

Acronis Access Advanced Administration Guide

Contents

- 1 Introduction6**
- 2 Quick Start.....7**
 - 2.1 Installation7
 - 2.2 Initial Setup8
- 3 Mobile Access17**
 - 3.1.1 Configuring the Default policy 17
- 4 Mobile Clients.....18**
 - 4.1 Sync&Share19
 - 4.1.1 Sync&Share Data Source 19
 - 4.1.2 LDAP Provisioning 20
 - 4.2 Web and Desktop clients21
- 5 Installing.....22**
 - 5.1 Requirements22
 - 5.1.1 Operating System Requirements 22
 - 5.1.2 Mobile Client Requirements..... 23
 - 5.1.3 Minimum Hardware Recommendation 23
 - 5.1.4 Network Requirements 24
 - 5.1.5 Desktop Client Requirements 25
 - 5.2 Installing Acronis Access Advanced on your server.....26
 - 5.3 Using the Configuration Utility28
 - 5.4 Using the Setup wizard31
 - 5.5 Clustering Acronis Access38
 - 5.6 Load balancing Acronis Access38
- 6 Upgrading.....39**
 - 6.1 Upgrading Acronis Access to a newer version.....39
 - 6.2 Upgrading to Acronis Access Advanced.....42
 - 6.3 Upgrading from mobilEcho 4.5 or earlier42
 - 6.4 Upgrading from activEcho 2.7 or earlier.....42
 - 6.5 Upgrading Gateway Clusters42
 - 6.6 Upgrading Load-balanced configurations.....44
- 7 Mobile Access53**
 - 7.1 Concepts53
 - 7.2 Policies55
 - 7.2.1 Adding a New Policy..... 56
 - 7.2.2 Modifying Policies 57
 - 7.2.3 Policy Settings..... 58
 - 7.2.4 Creating a Blocked Path list 71
 - 7.2.5 Allowed Apps..... 72
 - 7.2.6 Default Access Restrictions..... 74
 - 7.3 On-boarding Mobile Devices75

7.3.1	Server-side Management Enrollment Process	76
7.3.2	User-side Management Enrollment Process	79
7.4	Managing Gateway Servers	83
7.4.1	Registering new Gateway Servers	84
7.4.2	Server Details.....	86
7.4.3	Gateway Server Configurations	87
7.4.4	Licensing Gateway Servers	94
7.4.5	Cluster Groups.....	94
7.5	Managing Data Sources	96
7.5.1	Folders.....	97
7.5.2	Assigned Sources.....	100
7.5.3	Gateway Servers Visible on Clients.....	101
7.5.4	Legacy Data Sources.....	101
7.6	Settings	102
8	Sync & Share.....	104
8.1	General Restrictions.....	104
8.2	Sharing Restrictions	105
8.3	LDAP Provisioning	107
8.4	Quotas.....	108
8.5	File Purging Policies	108
8.6	User Expiration Policies	110
8.7	File Repository	110
8.8	Acronis Access Client	112
9	Users&Devices.....	114
9.1	Managing Mobile Devices.....	114
9.1.1	Performing Remote Application Password Resets	115
9.1.2	Performing Remote Wipes.....	116
9.2	Managing Users	117
9.3	Reassign Deleted User Content	120
10	Client Guides	120
11	Server Administration	121
11.1	Administering a Server.....	121
11.2	Administrators and Privileges.....	121
11.3	Audit Log.....	124
11.3.1	Log.....	124
11.3.2	Settings.....	127
11.4	Server.....	128
11.5	Web UI Customization	131
11.6	Web Previews & Editing	133
11.7	SMTP	134
11.8	LDAP.....	136
11.9	Email Templates.....	138
11.10	Licensing	140

11.11	Debug Logging	141
11.12	Monitoring	143
12	Maintenance Tasks	145
12.1	Disaster Recovery guidelines	145
12.2	Best Practices.....	147
12.3	Backing up and Restoring Acronis Access.....	148
12.4	Tomcat Log Management on Windows.....	151
12.5	Automated Database Backup	153
12.6	Automated Database Vacuum.....	155
12.7	Increasing the Acronis Access Tomcat Java Maximum Memory Pool.....	158
12.8	Migrating Acronis Access to another server.....	159
12.8.1	Before you begin	159
12.8.2	Migrating the Access Server and Gateway databases.....	160
12.8.3	Testing your new configuration	163
12.8.4	Cleanup of the original server	163
12.9	Upgrading PostgreSQL to a newer Major version	163
13	Supplemental Material	167
13.1	Conflicting Software	167
13.2	For the Access Server.....	167
13.2.1	Customizing the Web Interface through the API.....	167
13.2.2	Unattended desktop client configuration	168
13.2.3	Microsoft Azure Integration	172
13.2.4	Load balancing Acronis Access	184
13.2.5	Using Acronis Access with Microsoft Forefront Threat Management Gateway (TMG).....	191
13.2.6	Configuring Single Sign-On	208
13.2.7	Monitoring Acronis Access with New Relic	234
13.2.8	Using trusted server certificates with Acronis Access	235
13.2.9	How to support different Access Desktop Client versions	237
13.2.10	How to move the FileStore to a non-default location.....	238
13.2.11	Running Acronis Access Tomcat on multiple ports	239
13.2.12	Installing Acronis Access on a Microsoft Failover Cluster	240
13.2.13	Upgrading Acronis Access on a Microsoft Failover Cluster.....	266
13.2.14	Multi-homing Acronis Access	268
13.2.15	Deploy separate Web Preview servlets.....	269
13.2.16	PostgreSQL Streaming Replication.....	273
13.2.17	Configuring PostgreSQL for remote access	278
13.3	For the Mobile Clients	278
13.3.1	Using iOS Managed App Configuration features	279
13.3.2	Acronis Access for BlackBerry Dynamics	280
13.3.3	Microsoft Intune.....	298
13.3.4	MobileIron AppConnect support	300
14	Configuring an AppConnect tunnel between the Access Mobile client and the Access server via username/password authentication.....	313
15	Adding Kerberos Constrained Delegation Authentication	324
15.1.1	Using client certificate authentication.....	333
15.1.2	Using Kerberos Constrained Delegation authentication.....	334

16 What's New	342
16.1 What's New in Acronis Access Server	342
16.2 What's New in the Acronis Access app	372
17 Documentation for older versions	379

1 Introduction

This guide provides the documentation for Acronis Access Advanced and all of its features. For the client documentation, please visit the Client Guides (p. 120) section.

About Acronis Access Advanced

Acronis Access Advanced is a secure access, sync, and share solution that provides enterprise IT with complete control over business content to ensure security, maintain compliance, and enable BYOD. Acronis Access Advanced lets employees use any device - desktop, laptop, tablet or smartphone – to securely access and share content with authorized internal and external constituents, including employees, customers, partners, and vendors.

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

About Mobile Access

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

About Sync & Share

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

Acronis Access gives Enterprise IT control over who has access to files and lets IT determine whether file-sharing activities meet the compliance and security requirements of their organization. And, Acronis Access provides a level of visibility and monitoring not available from consumer-based solutions.

2 Quick Start

This guide is intended to provide the easiest and quickest way to install and have Acronis Access running. It is not suitable for custom configurations. For in-depth information and instructions for each component, please read the appropriate section of the full documentation.

In this section

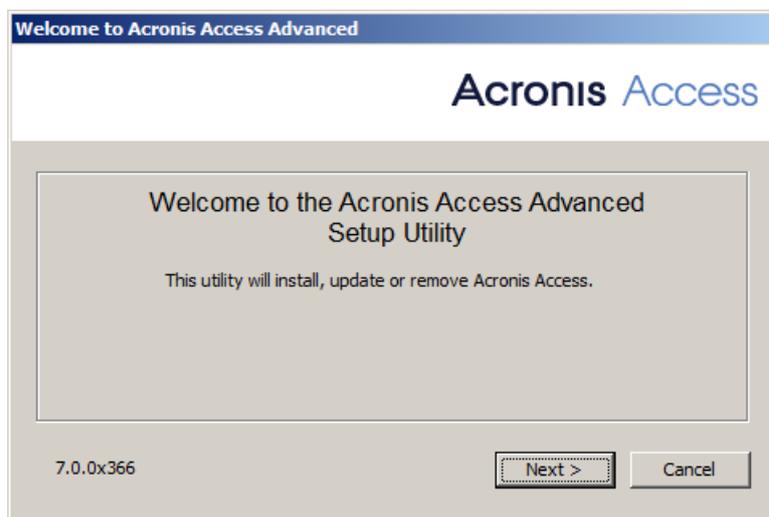
Installation	7
Initial Setup	8
Mobile Access	17
Sync&Share	19
Web and Desktop clients	21

2.1 Installation

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

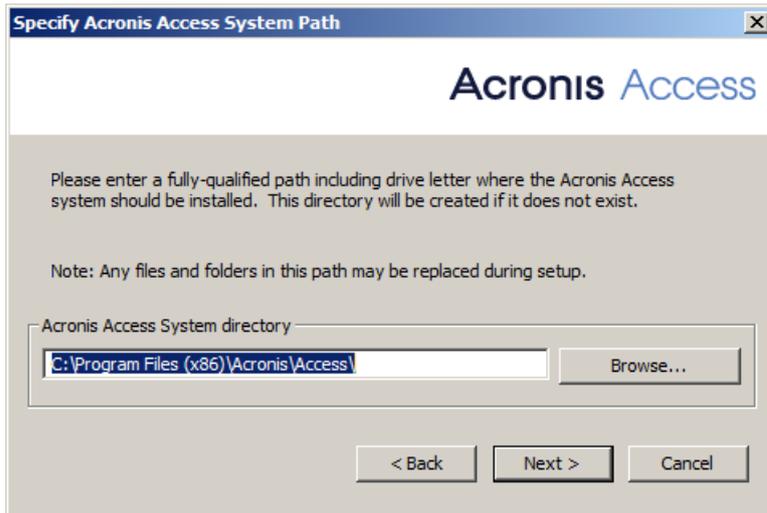
Using the Installer

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

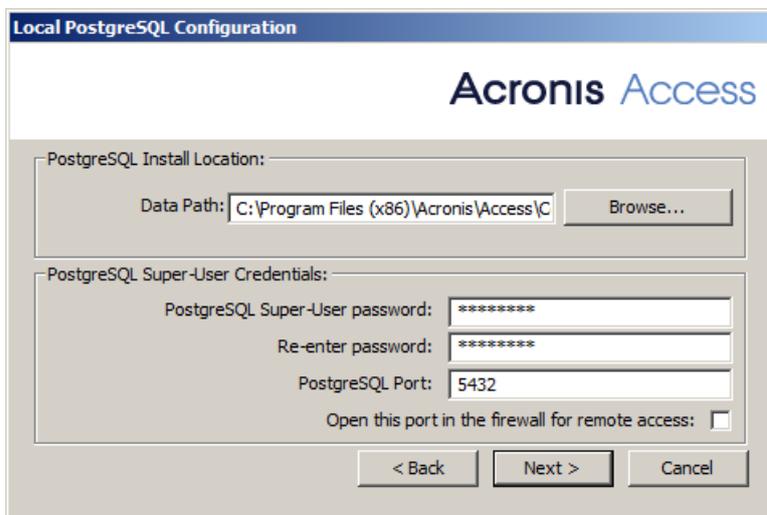


4. Press **Next** to begin.
5. Read and accept the license agreement.
6. Press **Install**.

7. Press **OK** to use the default path for the Acronis Access main folder.



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



9. A window displaying all the components which will be installed appears. Press **OK** to continue.
10. When the Acronis Access installer finishes, press **Exit**.
11. The configuration utility will launch automatically to complete the installation.
- 12.

Using the Configuration Utility

Note: The settings in the Configuration Utility can be changed later on.

Use the default values for each tab and press OK to start Acronis Access.

2.2 Initial Setup

The Setup Wizard takes the administrator through a series of steps to get the basic functionality of the server working.

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

Navigate to the Acronis Access's web interface using the IP address of your network adapter and the desired port. You will be prompted to set the password for the default administrator account.

Note: *If you run Acronis Access with the default certificates instead of using certificates from a Certificate Authority, you will get an error that the server is untrusted.*

Note: *All of the settings you see in the Initial Configuration page will also be available after you complete it. For more information on any of the settings, please visit the Server Administration (p. 121) articles.*

Note: *Internet Explorer 8 is not supported.*

Licensing

To start a trial:

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

Start trial Enter license key

Please register to start using the trial

First Name	<input type="text" value="John"/>
Last Name	<input type="text" value="Price"/>
Country	<input type="text" value="United States"/> ▼
State/province	<input type="text" value="Washington"/> ▼
Phone	<input type="text" value="+1000-755-332-12"/>
Select industry	<input type="text" value="Telecommunication"/> ▼
Company	<input type="text" value="Neucott Ltd."/>
Email	<input type="text" value="jprice@neucott.com"/>
<input type="button" value="Continue"/>	

- 2.

Start trial Enter license key

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

To license your Access Server:

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

General Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://access.yourcompany.com"/>
Audit Log Language	<input type="text" value="English"/> ▼

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

SMTP

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

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

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

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

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

LDAP information caching interval

Note: You can skip this section, and configure LDAP later but some of Acronis Access' functionality will not be available until you do.

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

Local Gateway Server

Acronis Access mobile app clients connect to the Access server using its Gateway Server address. Depending on server configuration, your desktop sync clients and web clients may also connect here. Your Gateway Server is currently running on 192.168.2.129:3000. It is recommended that you configure your clients to connect using an address that is reachable from all networks they will be connecting from. If your clients connect through a proxy, this address may actually be the DNS address of your proxy server. An example: gateway.mycompany.com

Address clients use to connect to the server:

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

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

File Repository

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

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

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

5. Press **Save**.

3 Mobile Access

In this section

Configuring the Default policy	17
Mobile Clients	18

3.1.1 Configuring the Default policy

All mobile clients enrolled in management with the Acronis Access server have their functionality governed and controlled by a User or Group policy. The Default policy is created automatically on installation and has the lowest priority (the highest being a personal User policy), but it affects all users that do not have a User policy and are not members of a Group policy. The Default policy is enabled by default.

Configuring the Default policy

1. Open the Acronis Access web console.
2. Navigate to **Mobile Access -> Policies -> Group Policies**.
3. Make sure that there is a check under the **Enabled** field and click on the **Default** policy.
4. View the settings and make changes if desired. For an in-depth overview of all the settings, please visit the Policies (p. 55) section.

4 Mobile Clients

When you run the Acronis Access app for the first time, you can either try the app in demo mode or you can enroll to your company's server.

To test out the app in the demo mode

Demo mode allows users to try the Acronis Access app even if their company doesn't have a Acronis Access Server. This is an environment setup for demonstration purposes only, not all features are accessible.

1. Install the app and open it.
2. After the welcome screen, select **Use our demo server**
3. You will be enrolled to the demo server.

Note: Once enrolled, you will have read-only access to a few shared folders on the demo server, as well as a couple of sync folders. These folders contain sample files, PDFs, image files, etc. You are able to browse, search, view & edit these available files and save edited files locally within the app if you so desire.

4. You can switch to your company's server at any point in time.

To enroll to your company's Access server

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

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

- Desktop and Web client
- iOS app
- Android app

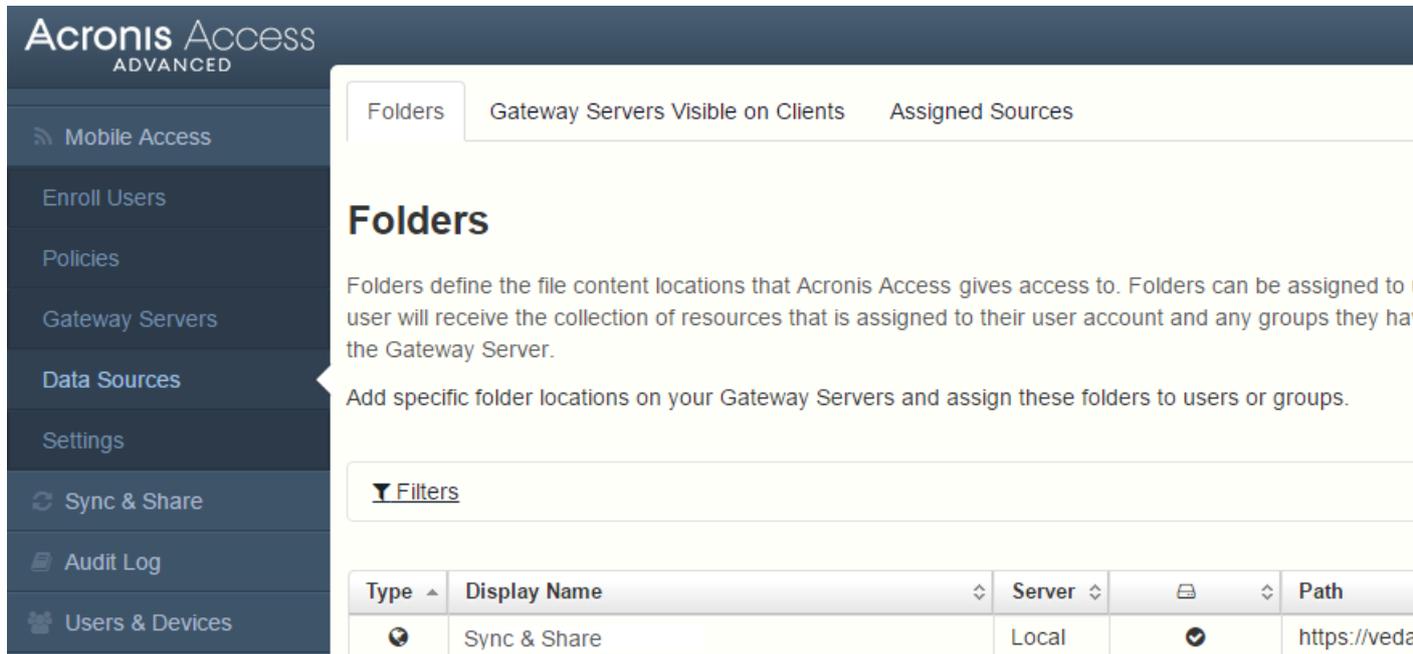
Windows mobile app

4.1 Sync&Share

4.1.1 Sync&Share Data Source

Once you install and configure Acronis Access, it will automatically create a Data Source called "**Sync&Share**" and will add the **Domain Users** group to the assigned users and groups list by default. At any time the administrator(s) can change or remove this Data Source folder.

This default Data Source will be available to all newly created users who are part of the **Domain Users** group and it is reachable via mobile, desktop and web clients.



The screenshot shows the Acronis Access Advanced web interface. The left sidebar contains navigation options: Mobile Access, Enroll Users, Policies, Gateway Servers, Data Sources (highlighted), Settings, Sync & Share, Audit Log, and Users & Devices. The main content area is titled 'Folders' and includes a sub-header 'Gateway Servers Visible on Clients' and 'Assigned Sources'. Below the title, there is explanatory text: 'Folders define the file content locations that Acronis Access gives access to. Folders can be assigned to user will receive the collection of resources that is assigned to their user account and any groups they have the Gateway Server.' and 'Add specific folder locations on your Gateway Servers and assign these folders to users or groups.' A 'Filters' section is visible above a table. The table has columns: Type, Display Name, Server, and Path. The first row shows a folder with Type 'Sync & Share', Display Name 'Sync & Share', Server 'Local', and Path 'https://veda'.

Type	Display Name	Server	Path
	Sync & Share	Local	https://veda

In this section

Sharing existing content only requires that you setup a Data Source for it and assign that Data Source to the desired users or groups.

Creating a Data Source

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

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

9. Based on your choice of location, enter the path to that folder, server, site or library.
10. Select the **Sync** type of this folder.
11. Enable **Show When Browsing Server** if you want this Data Source to be visible when Acronis Access mobile clients browse the Gateway Server.

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

12. Press the Save button.

By default, users cannot open NAS, File Servers and SharePoint resources from the Web client. However, enabling it is simple and grants more possibilities to the web users.

1. Open the Web Interface and browse to **Mobile Access --> Policies**. (Note even though policies primarily relate to the mobile app, the setting for web access is there too.)
2. Select the policy you want to change. If you haven't made any new ones, select the **Default** policy.
3. On the **Server Policy** tab, select the box **Allow File Server, NAS, and SharePoint Access from the Web Client**
4. Consider whether you want to also enable desktop syncing, for the chosen policy, using the sub-options **Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client** and **Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client**.
5. Click **Save**.

This is implemented as a per-policy setting to provide more flexibility. You may want to enable the setting for another group or some individual policies.

4.1.2 LDAP Provisioning

Enabling LDAP Provisioning allows your users to login with their LDAP credentials and have their accounts created automatically instead of the administrator having to invite each user (or group) individually. These accounts take up a license from your license pool so choose a specific LDAP group (or groups) for provisioning.

Enabling LDAP Provisioning

1. Open the Acronis Access web console.

2. Navigate to **Sync&Share -> LDAP Provisioning**.

LDAP Provisioning

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

LDAP Group

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

Remove

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

Find group that begins with

Search

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

The users in the selected group(s) will now have their Acronis Access accounts automatically generated the moment they try to login to Acronis Access with their LDAP credentials.

4.2 Web and Desktop clients

- The Web client allows all users with valid Acronis Access credentials to access and share files and folders from their preferred browser.
- The Desktop client enables users to share big files easily and ensures that their files are always up to date.

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

- Desktop and Web client
- iOS app
- Android app
- Windows mobile app

5 Installing

In this section

Requirements.....	22
Installing Acronis Access Advanced on your server.....	26
Using the Configuration Utility	28
Using the Setup wizard	31
Clustering Acronis Access.....	38
Load balancing Acronis Access.....	38

5.1 Requirements

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

In this section

Operating System Requirements.....	22
Mobile Client Requirements	23
Minimum Hardware Recommendation	23
Network Requirements.....	24
Desktop Client Requirements	25

5.1.1 Operating System Requirements

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

Note: Acronis Access 7.4.x is the last version that supports Windows XP and Vista. Newer versions of Acronis Access will not support connections from those operating systems.

Recommended:

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

Supported:

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

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

5.1.2 Mobile Client Requirements

Supported devices:

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

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

Supported OS's:

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

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

The Acronis Access app can be downloaded from:

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

5.1.3 Minimum Hardware Recommendation

Example deployments

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

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

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

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

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

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

Small Deployments

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

- RAM: 16 GB
- Disk Space: 100 GB

Medium Deployments

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

Large Deployments

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

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

5.1.4 Network Requirements

- 1 Static IP Address. 2 IP addresses may be needed for certain configurations.
- Optional but recommended: DNS names matching the above IP addresses.
- Network access to your Domain Controller if you plan on using Active Directory (LDAP).
- Network access to an SMTP server for email notifications and invitation messages.
- The address **127.0.0.1** is used internally by the Access Mobile Client and should not be routed through any kind of tunnel - VPN, MobileIron, Good Dynamics and etc.
- All machines running the Access Server or the Gateway Server need to be bound to the Windows Active Directory.

There are two components that handle HTTPS traffic, the Gateway Server and the Acronis Access Server. The Gateway Server is used by mobile clients to access both files and shares from the Data Sources. The Access Server provides the web user interface for Sync & Share clients, and is also the administration console for both Mobile Access and Sync & Share.

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

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

- **Port 443 access:** Acronis Access uses HTTPS for encrypted transport, so it fits in naturally with common firewall rules allowing HTTPS traffic on port 443. If you allow port 443 access to your Acronis Access server, authorized iPad clients can connect while inside or outside of your firewall. Acronis Access can also be configured to use any other port you prefer.

- **VPN:** The Access Mobile Client supports access through a VPN connection. Both the built in iOS VPN client and third-party VPN clients are supported. iOS management profiles can optionally be applied to devices using Mobile Device Management (MDM) systems or the Apple iPhone Configuration Utility to configure the certificate-based iOS “VPN-on-demand” feature, giving seamless access to Acronis Access servers and other corporate resources.
- **Reverse proxy server:** If you have a reverse proxy server set up, iPad clients can connect without the need for an open firewall port or a VPN connection. The Access Mobile Client app supports reverse proxy pass-through authentication, username / password authentication, Kerberos constrained authentication delegation and certificate authentication. For details on adding certificates to the Access Mobile Client app, visit the Using client certificates (p. 333) article.
- **Good Dynamics enabled Access Mobile Client app:** The Access Mobile Client app includes the ability to be enrolled in and managed by the Good Dynamics platform. In this configuration, all network communication between Access Mobile Clients and Gateway Servers is routed through the Good Dynamics secure communication channel and Good Proxy Server. For more details, see the Access Mobile Client for Good Dynamics (p. 280) manual page.
- **MobileIron AppConnect enrolled Access Mobile Client app:** If the Access Mobile Client application is enrolled with MobileIron's AppConnect platform, then all network communication between Access Mobile Client clients and Gateway Servers can be routed through the MobileIron Sentry. For more information see the MobileIron AppConnect (p. 300) manual page.

Certificates:

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

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

5.1.5 Desktop Client Requirements

Supported operating systems:

- Windows 7, Windows 8 and 8.1, Windows 10

Note: The Access desktop client version 7.4 is the last version that is compatible with Windows XP and Vista. If you want to use a newer version of the Acronis Access desktop client, you will have to update your Windows OS. Acronis Access 7.4 is the last server version to allow connections from Windows XP or Vista.

- Mac OS X 10.8 and higher with Mac compatible with 64-bit software.

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

Note: When installing the Acronis Access Desktop client, make sure that the sync-folder you create is not in a folder synchronized by another software. For a list of known conflicts visit [Conflicting Software \(p. 167\)](#).

Supported web browsers:

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

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

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

- Google Chrome 4.1.249.1042 and later.
- Safari 5.1.10 and later.

5.2 Installing Acronis Access Advanced on your server

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

Note: For upgrade instructions visit the *Upgrading* (p. 39) section.

Note: For instructions on installing on a cluster visit the *Installing Acronis Access on a cluster* (p. 240) section.

The installation of Acronis Access involves three steps:

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

Installing Acronis Access

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

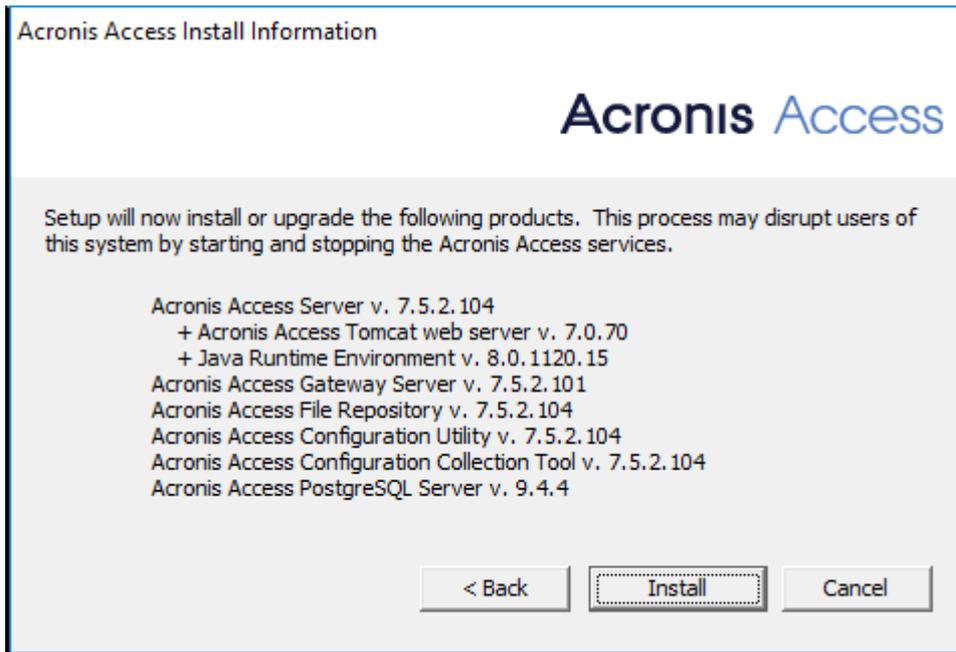
1. Download the Acronis Access installer.
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



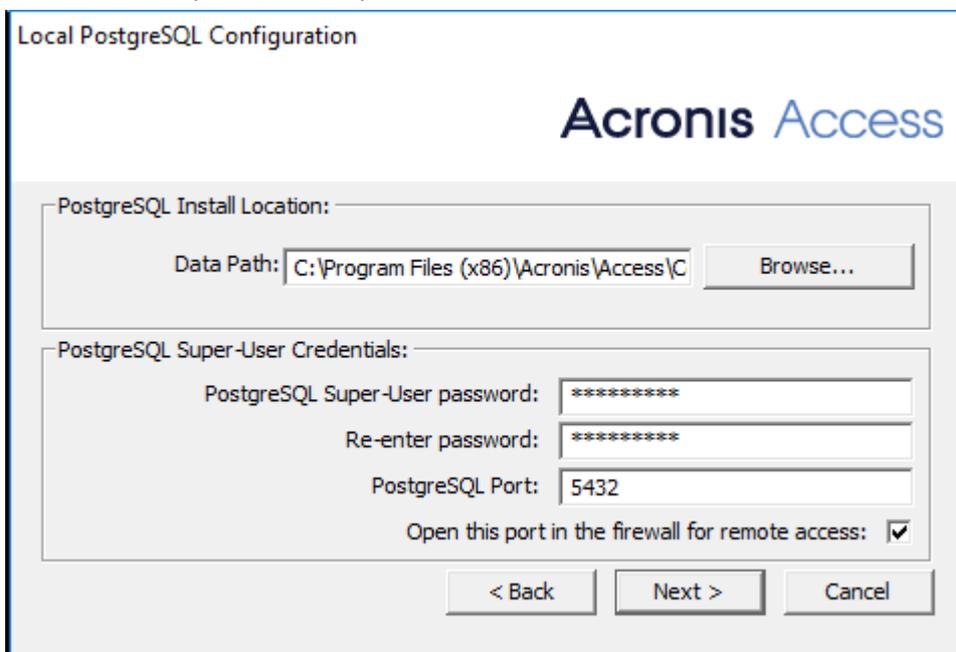
4. Press **Next** to begin.
Read and accept the license agreement.
5. Press **Install**.

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.

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



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



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

For instructions on using the Configuration utility, visit the Using the Configuration Utility (p. 28) page.

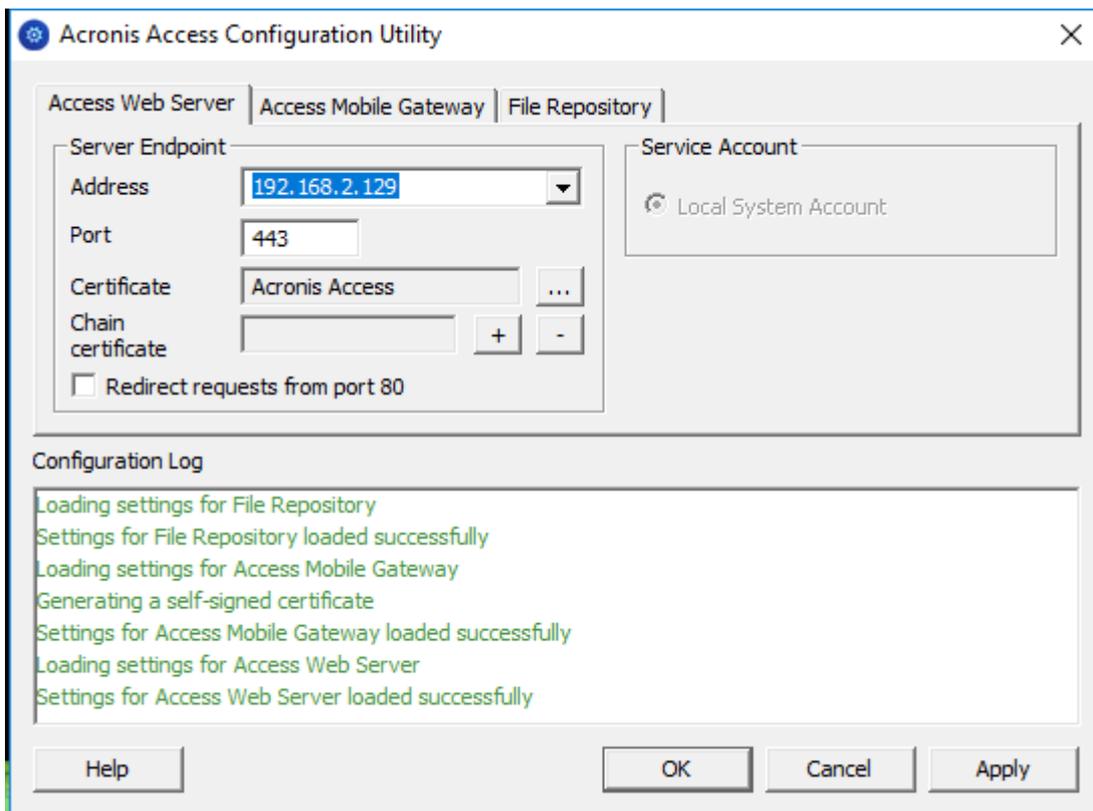
5.3 Using the Configuration Utility

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

Note: See the *Network Requirements* (p. 24) section for more information on best practices for the IP address configurations of Acronis Access.

Note: For information on adding your certificate to the Microsoft Windows Certificate Store, visit the *Using Certificates* (p. 235) article.

Access Web Server tab

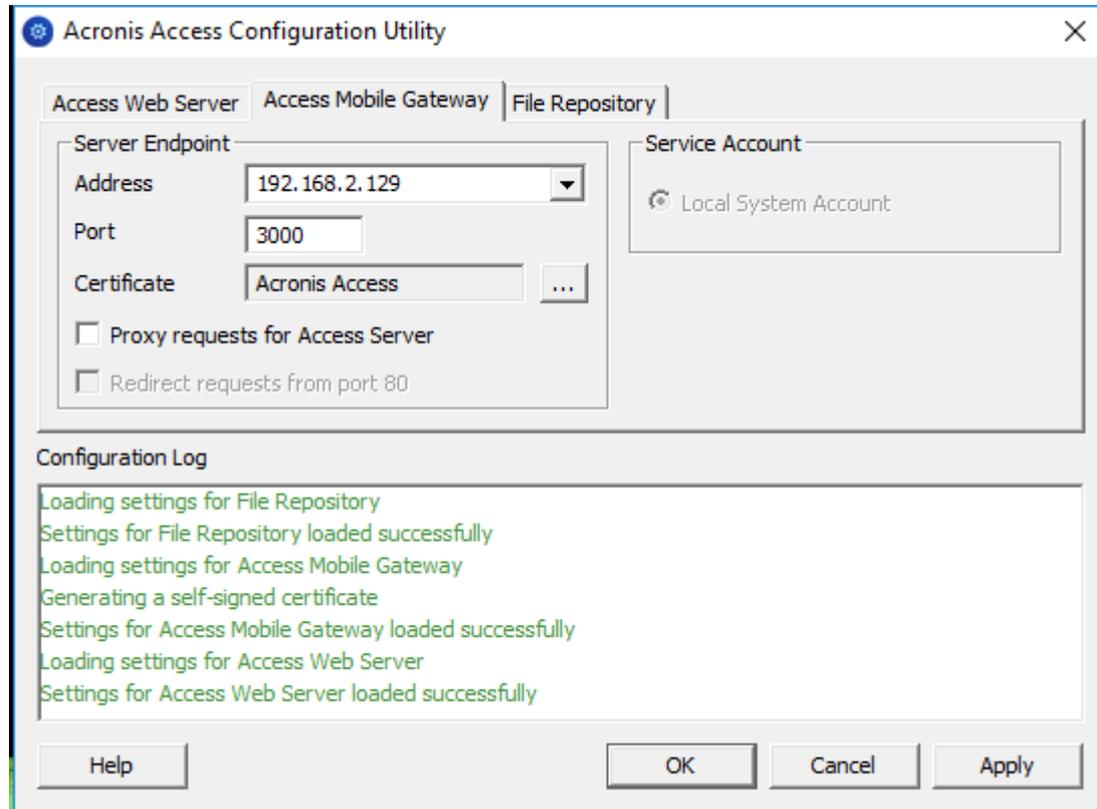


The Acronis Access Server provides the web user interface for Acronis Access clients, and is also the administration console for both Mobile Access (p. 53) and Sync & Share.

- **Address** - The IP address of your Web Interface or pick **All Addresses** to listen on all available interfaces.
- **Port** - The port of your Web Interface.
- **Certificate** - Path to the certificate for your Web Interface. You can choose a certificate from the Microsoft Windows Certificate Store.
- **Chain Certificate** - Path to the Intermediate certificate for your Web Interface. You can choose one from the Microsoft Windows Certificate Store. This certificate is only required if your Certificate Authority has also issued you an Intermediate certificate.
- **Redirect requests from port 80** - When selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.

- **Service Account** - This allows the Acronis Access Server service to run in the context of another account. This is normally not required in typical installations.

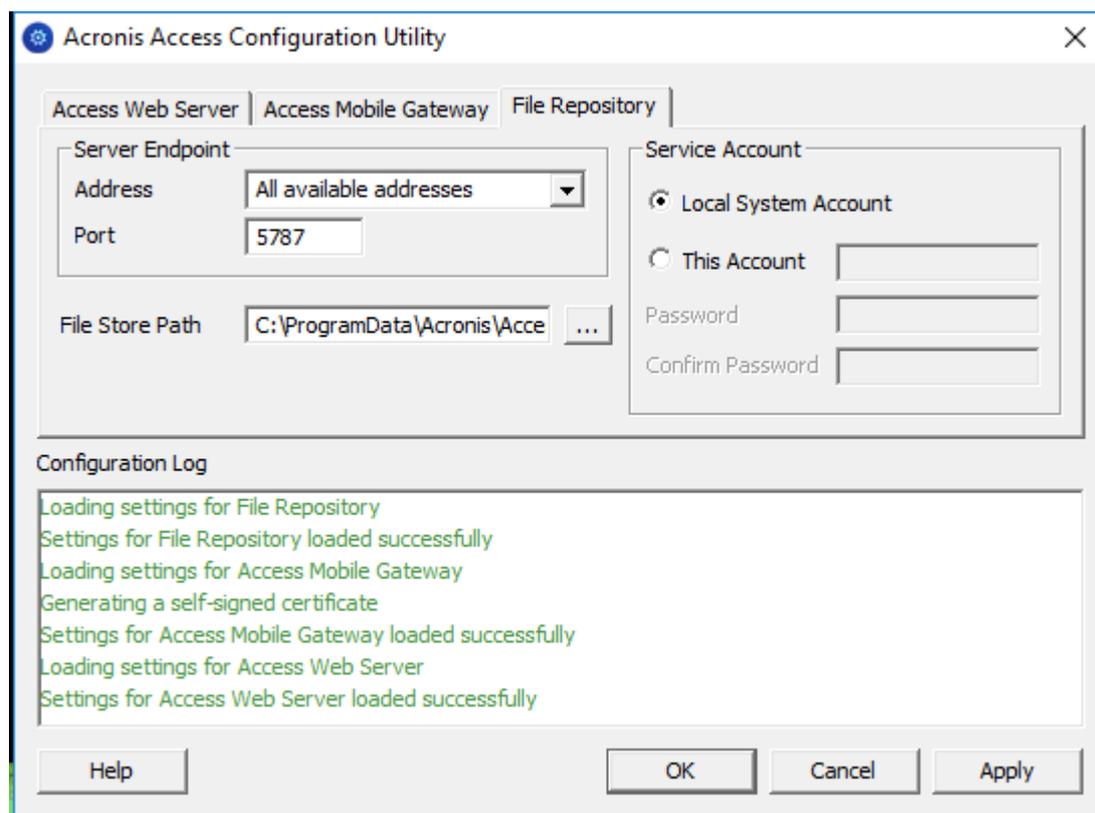
Access Mobile Gateway tab



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

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

File Repository tab



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

- **Address** - The IP address of your File Repository or pick **All Addresses** to listen on all interfaces. If you specify an IP or DNS address, the same address should also be specified in the **File Repository** section of the web interface. For more information on it, visit the File Repository (p. 110) article.
- **Port** - The port of your File Repository. The same port should also be specified in the **File Repository** section of the web interface. For more information on it, visit the File Repository (p. 110) article.
- **File Store Path** - UNC path to your File Store. If you change the File Store path, you **MUST** manually copy any files that are already in the original File Store location to your new location.

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

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

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

After you have filled in all the necessary fields, pressing **Apply** or **OK** will restart the services you have made changes to. It will take 30-45 seconds after the services have started before the Acronis Access Server is available.

At this point, a web browser will automatically launch and connect to the Acronis Access's IP address and port. On the login page, set the **administrator** password and then the Setup Wizard (p. 31) will guide you through the setup process.

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

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

5.4 Using the Setup wizard

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

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

Going through the initial configuration process

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

Note: Additional administrators can be configured later on, for more information visit the Server Administration (p. 121) section.

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

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

All of the settings you see in the Initial Configuration page will also be available after you complete it. For more information on any of the settings, please visit the Server Administration (p. 121) articles.

Licensing

To start a trial:

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

Start trial Enter license key

Please register to start using the trial

First Name	<input type="text" value="John"/>
Last Name	<input type="text" value="Price"/>
Country	<input type="text" value="United States"/> ▼
State/province	<input type="text" value="Washington"/> ▼
Phone	<input type="text" value="+1000-755-332-12"/>
Select industry	<input type="text" value="Telecommunication"/> ▼
Company	<input type="text" value="Neucott Ltd."/>
Email	<input type="text" value="jprice@neucott.com"/>
<input type="button" value="Continue"/>	

- 2.

Start trial Enter license key

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

To license your Access Server:

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

General Settings

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://access.yourcompany.com"/>
Audit Log Language	<input type="text" value="English"/> ▼

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

SMTP

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

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

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

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

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

LDAP information caching interval

Note: You can skip this section, and configure LDAP later but some of Acronis Access' functionality will not be available until you do.

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

Local Gateway Server

Acronis Access mobile app clients connect to the Access server using its Gateway Server address. Depending on server configuration, your desktop sync clients and web clients may also connect here. Your Gateway Server is currently running on 192.168.2.129:3000. It is recommended that you configure your clients to connect using an address that is reachable from all networks they will be connecting from. If your clients connect through a proxy, this address may actually be the DNS address of your proxy server. An example: gateway.mycompany.com

Address clients use to connect to the server:

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

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

File Repository

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

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

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

5. Press **Save**.

5.5 Clustering Acronis Access

Acronis Access allows the configuration of high-availability setups without needing third-party clustering software. This is configured through the new Cluster Groups feature introduced in Acronis Access 5.1. The setup procedure is simple, but provides high-availability for the Acronis Access Gateway Servers as they are the component under the heaviest load. All of these configurations are managed through the Acronis Access Server.

For more information and instructions on setting up a Cluster Group, visit the Cluster Groups (p. 94) article.

Although we recommend using the built-in Cluster Groups feature, Acronis Access also supports Microsoft Failover Clustering, for more information visit the Supplemental Material (p. 167) section.

5.6 Load balancing Acronis Access

Acronis Access supports load balancing. For more information please visit the Load Balancing Acronis Access (p. 184) and Cluster Groups (p. 94) articles.

6 Upgrading

In this section

Upgrading Acronis Access to a newer version	39
Upgrading to Acronis Access Advanced	42
Upgrading from mobilEcho 4.5 or earlier	42
Upgrading from activEcho 2.7 or earlier	42
Upgrading Gateway Clusters	42
Upgrading Load-balanced configurations	44

6.1 Upgrading Acronis Access to a newer version

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

Note: If you are upgrading from a version of Acronis Access earlier than 7.0, please contact Acronis support at <http://www.acronis.com/mobilitysupport/>

Note: Before upgrading, please review the Minimum Hardware Requirements (p. 23).

Note: Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Access and custom installations can affect the folder structures of your deployment.

Backup the vital components

The Apache Tomcat folder

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

We recommend that you backup the **web.xml** file before updating. Your **web.xml** file will be overwritten on upgrade. On versions 7.1.2 and newer, you can find a backup at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF\<timestamp>.previous.web.xml**. If you have made any specific changes that you wish to retain (excluding Single Sign On (p. 208), those changes are preserved) , you will have to manually copy and paste your changes from the old file.

Purge unnecessary audit logs

If you have not setup automatic log purging (p. 124), your server may have a lot of logs which may slow-down the backup process. We recommend exporting and purging the older logs before proceeding with the database backup.

The PostgreSQL database

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

1. Open a Command Prompt window and navigate to the **9.2\bin** folder located in the PostgreSQL installation directory.

e.g. `cd "C:\PostgreSQL\9.2\bin"`

2. Once your current Command Prompt directory is the **bin** folder, enter the following line:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Gateway Server(s) database(s)

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

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

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

The Acronis Access configuration file

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

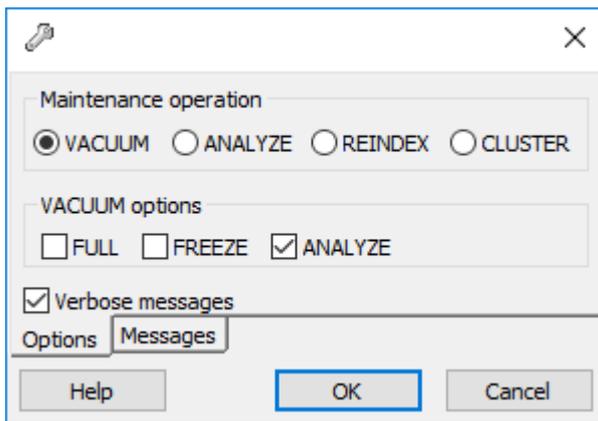
Note: *The default location is: C:\Program Files (x86)\Acronis\Access\Access Server*

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

Vacuum the database before upgrading

1. Open the Acronis Access PostgreSQL Administrator tool (can also be called PgAdmin) and double-click on **localhost** to connect to your server.

2. Right-click on the **acronisaccess_production** database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning! If your database is very large, the vacuum can take some time. This process should be run during periods of low load on the server.

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

Upgrade

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



3. Press **Next** to begin.
4. Read and accept the license agreement.
5. Press **Upgrade**.
6. Review the components which will be installed and press **Install**.
7. Review the installed components and close the installer.

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

6.2 Upgrading to Acronis Access Advanced

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

To do so:

1. Open the Acronis Access Web interface as an administrator.
2. Open the **General Settings** tab and click on **Licensing**.
3. Add your license.

Adding a new license

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

6.3 Upgrading from mobilEcho 4.5 or earlier

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

6.4 Upgrading from activEcho 2.7 or earlier

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

6.5 Upgrading Gateway Clusters

To upgrade an Acronis Access clustered configuration, you need to upgrade both the Acronis Access Server and the Gateway Servers in your Cluster Group (p. 94).

Note: For information on upgrading a Microsoft Failover Clustering configuration, visit the *Supplemental Material* (p. 167) section.

Note: For instructions on upgrading the Acronis Access Server, visit the *Upgrading from Acronis Access to a newer version* (p. 39) article

For each Gateway Server, you will need to do the following upgrade procedure:

Before performing any upgrades, please review our [Backup \(p. 148\)](#) articles and backup your configuration.

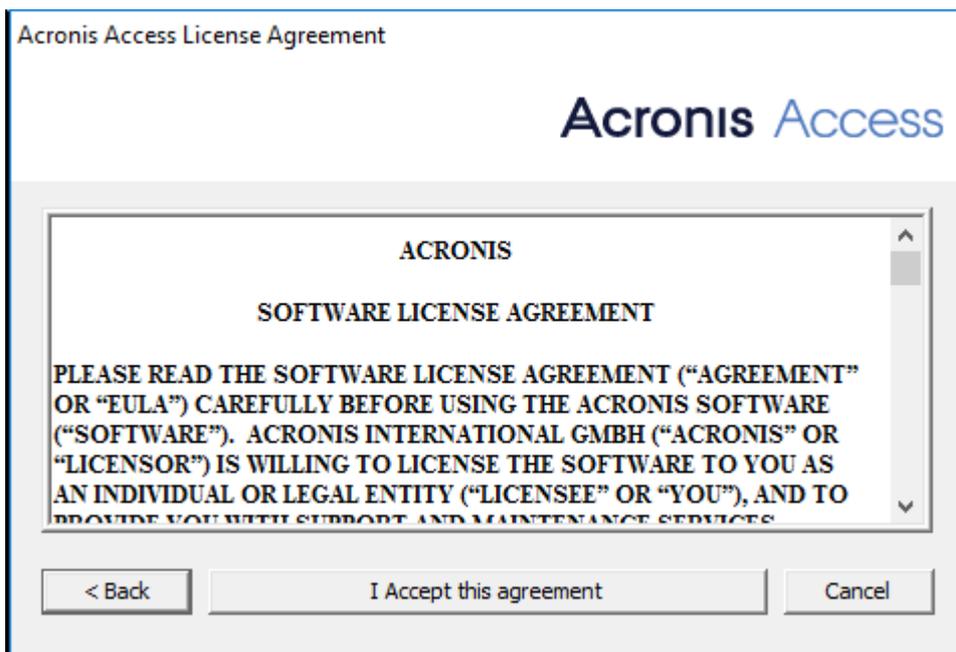
Note: Before upgrading, please review the [Minimum Hardware Requirements \(p. 23\)](#).

Note: Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Access and custom installations can affect the folder structures of your deployment.

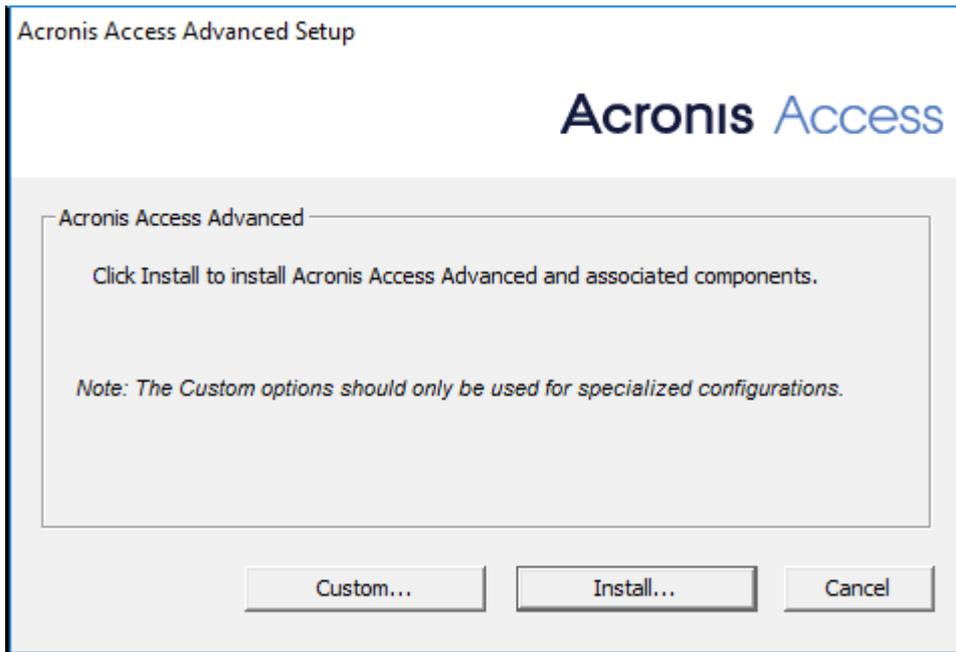
Upgrading a Gateway Server

Run the Acronis Access installer on the desired server.

1. Press **Next** on the **Welcome** screen.



2. Read and accept the license agreement.



- 3.
4. Select **Custom**.
5. Select only the **Acronis Access Gateway Server** component and press **Next**.
6. Review the components and press **Install**.
7. Once the installation finishes, review the **Summary**, and close the installer.
8. You will be prompted to open the **Configuration Utility**. Open it to review that all of your previous Gateway Server settings are in place. Make any changes if necessary and press OK.

6.6 Upgrading Load-balanced configurations

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

Before performing any upgrades, please review our Backup (p. 148) articles and backup your configuration.

Note: Before upgrading, please review the *Minimum Hardware Requirements (p. 23)*.

Note: Depending on your deployment, some of the paths used in this article might not be the same as yours. Upgrades from previous versions of Acronis Access and custom installations can affect the folder structures of your deployment.

In this section

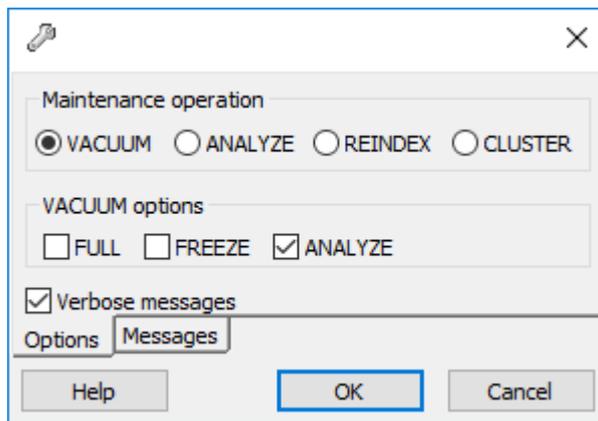
Pick one of the Acronis Access Server machines to act as the **Primary**. This machine is the **Primary** node only in the sense that it will be upgraded first and it will migrate any changes/settings to the PostgreSQL database. If the database is very large, these migrations can take several minutes.

Warning! *DO NOT* upgrade any other Tomcat servers until the **Primary** server is upgraded and you can log into the web interface to test it out.

Vacuum the database

This will help speed up the backup and restore process by optimizing your database

1. Open the Acronis Access PostgreSQL Administrator tool (can also be called PgAdmin) and double-click on **localhost** to connect to your server.
2. Right-click on the **acronisaccess_production** database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning! *If your database is very large, the vacuum can take some time. This process should be run during periods of low load on the server.*

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

For in-depth information on backup and restore procedures, please visit the [Backing up and Restoring Acronis Access \(p. 148\)](#) article.

Backup your PostgreSQL database

1. Stop all Acronis Access Tomcat services.
2. Open the Acronis Access PostgreSQL Administrator application and connect to the database server. You may be prompted to enter the password for your **postgres** user.
3. Expand **Databases** and right-click on the **acronisaccess_production** database.
4. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
5. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.
6. Close the PostgreSQL Administrator and open an elevated command prompt.
7. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"
8. Enter the following command: **pg_dumpall --host localhost --port 5432 --username postgres --inserts --file alldbs_inserts.sql**
 - **alldbs_inserts.sql** will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere

else - e.g. change the last part of the command above like so: **--file
D:\Backups\alldbs_inserts.sql**

- If you are using a non-default port, change **5432** to the correct port number.
- If you are not using the default PSQL administrative account **postgres**, please change **postgres** to the name of your administrative account in the command above.
- You will be prompted to enter the **postgres** user's password several times for this process. For each prompt, enter the password and hit Enter.

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

9. Copy the backup file to a safe location.
10. Do **NOT** shutdown the Postgres service as PostgreSQL itself will not be upgraded.

Backup additional important components

1. Backup the Tomcat **conf** and **logs** folders. By default located in: **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-<version>**

Note: *Replace <version> with the correct version of your Access Tomcat instance, e.g. **\apache-tomcat.70.0.70***

2. Backup the **acronisaccess.cfg** file. By default located in: **C:\Program Files (x86)\Acronis\Access\Access Server**
3. Backup all **web.xml** files. located by default in **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**.
4. Backup the **newrelic.yml** file. Its location depends entirely on where you have saved it. You can skip this step if you are not using New Relic monitoring.

Backup the Gateway Servers databases

1. Turn off all the Acronis Access Gateway services
2. Go to the Gateway database folders, by default **C:\Program Files (x86)\Acronis\Access\Gateway Server\database**
3. Make a backup of the **mobilecho.sqlite3** file.
4. Repeat these steps for each Gateway Server.

Stop all Acronis Access services on all machines

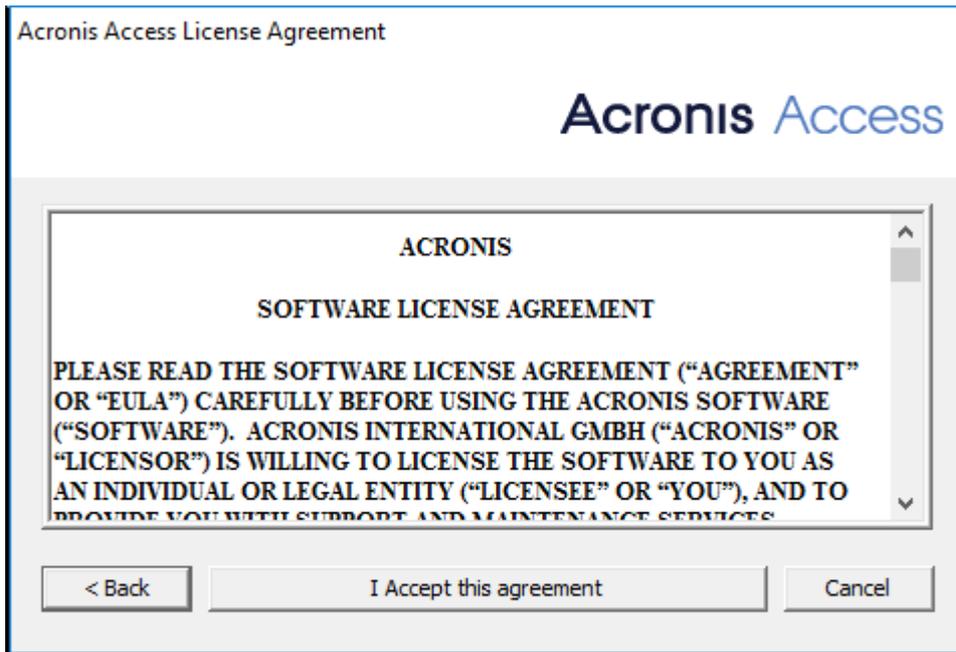
It is vital that all Access Tomcat services are stopped before you upgrade. We recommend also stopping all other Acronis Access services, except the PostgreSQL service as it must remain running.

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

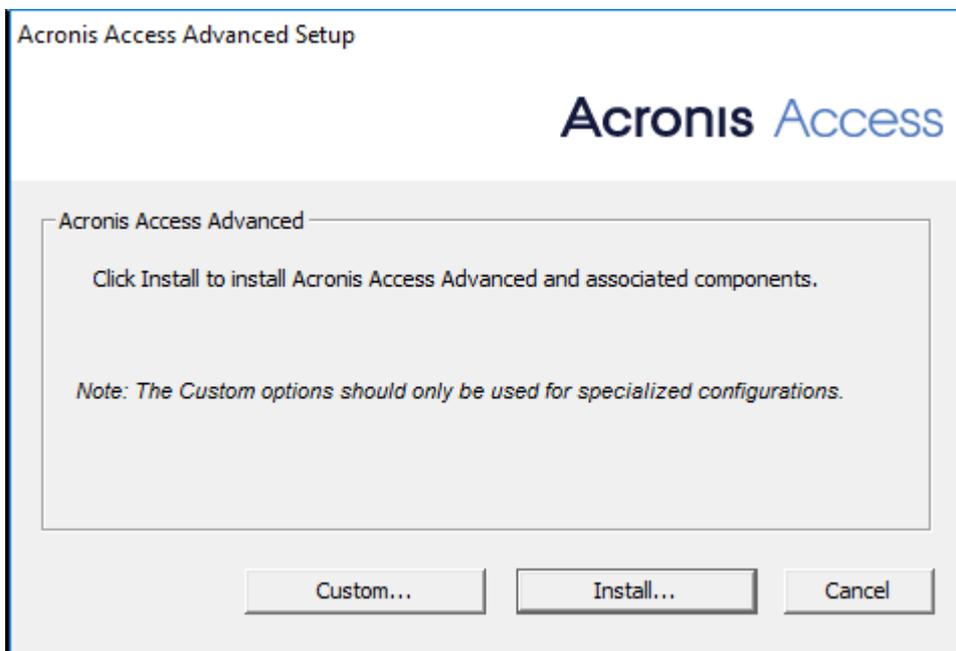
1. Copy the Acronis Access installer to the machine with the File Repository component and run the installer.

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

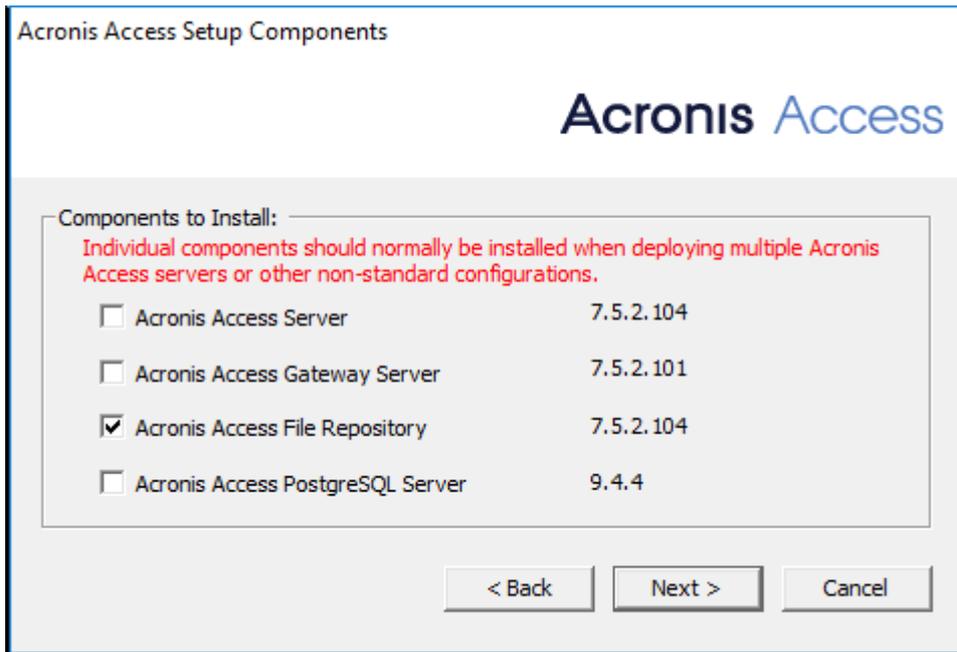
2. On the **Welcome** screen click **Next**.



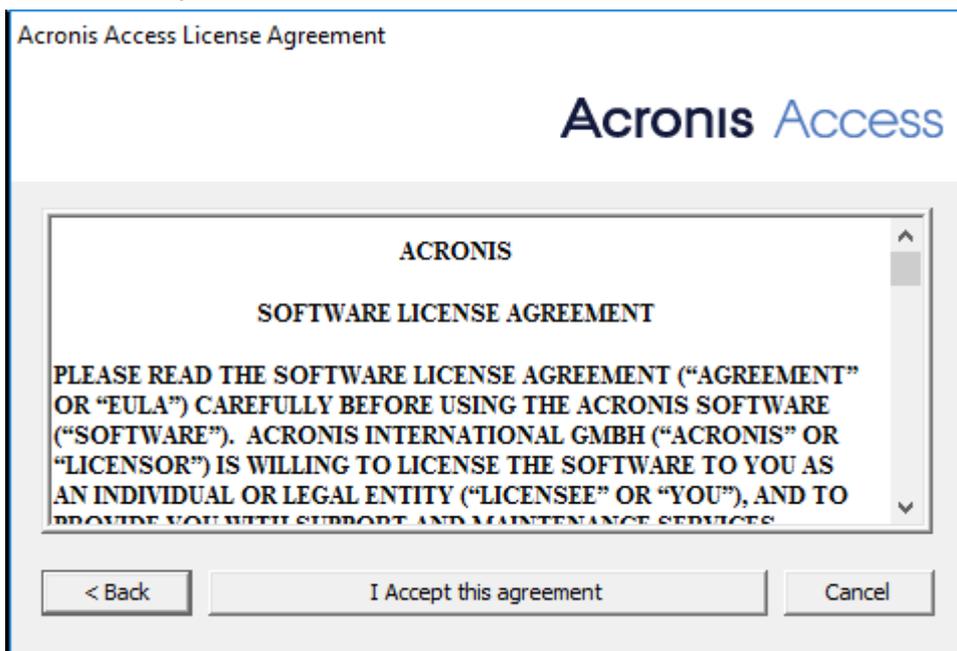
3. Accept the License Agreement.



- Choose **Custom...** and select only the **Acronis Access File Repository** to upgrade.

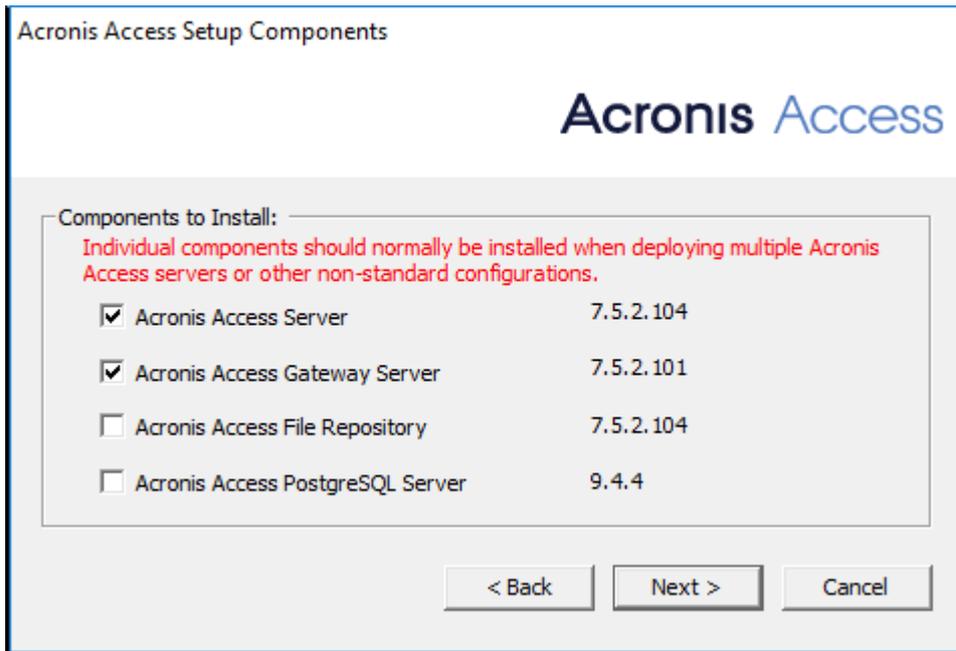


- Click **Next**, review what is going to be installed and click **Install**.
- When the upgrade is done, click **Exit**. When the Configuration Utility launches, click **OK**.
- Continue by upgrading your **Primary** Acronis Access Server on its corresponding machine.
 - Copy the Acronis Access Advanced installer to the **Primary** Acronis Access Server machine.
 - On the **Primary** node, start the Acronis Access installer.



- Press **Next** on the Welcome screen and then **Custom**. This will allow you to upgrade only the necessary services that are already installed on the machine, without installing others.

4. Select the Acronis Access services that you are going to upgrade. Choose only the Acronis Access Server and any components that are already present on the machine.



Note: Our installer will not update PostgreSQL. If you wish to update your version of PostgreSQL please view our article on the subject (p. 163) and contact Acronis support before proceeding.

5. Press **Install**, let the installer finish and launch the the **Configuration Utility**.

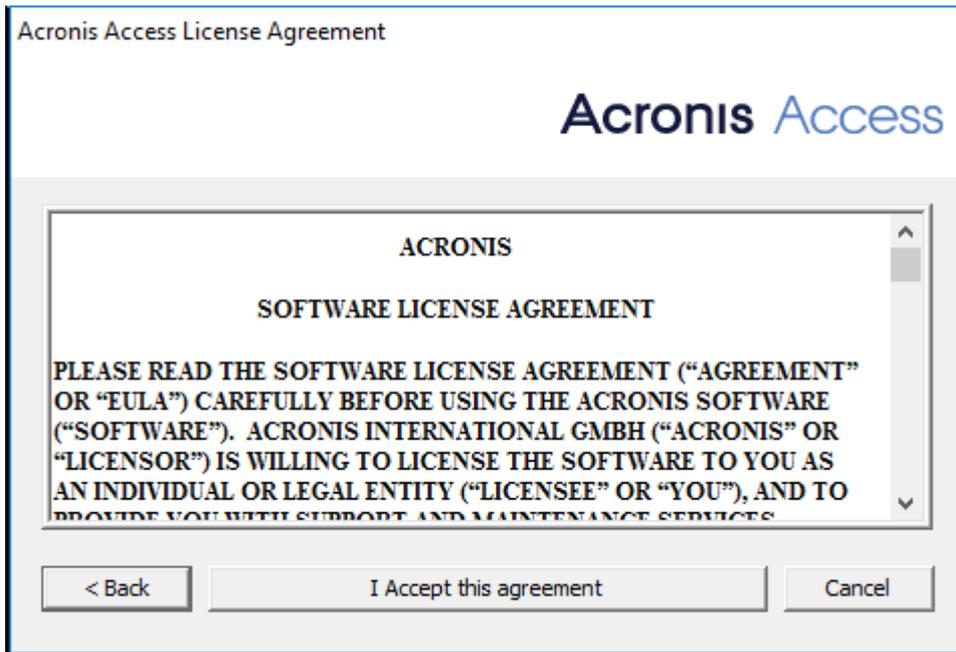
Note: Do not change any settings in the **Configuration Utility**! Changing settings can cause issues with your configuration.

6. Once the Configuration Utility starts all the necessary services, and the database migrations are finished, verify that Acronis Access web interface on the **Primary** server works as expected. A web browser will launch automatically and display the Access server log-in screen.
7. Log in as an administrator and verify that the settings are the same and there are no changes or issues.
8. Leave this instance of Acronis Access running while you update all other components.

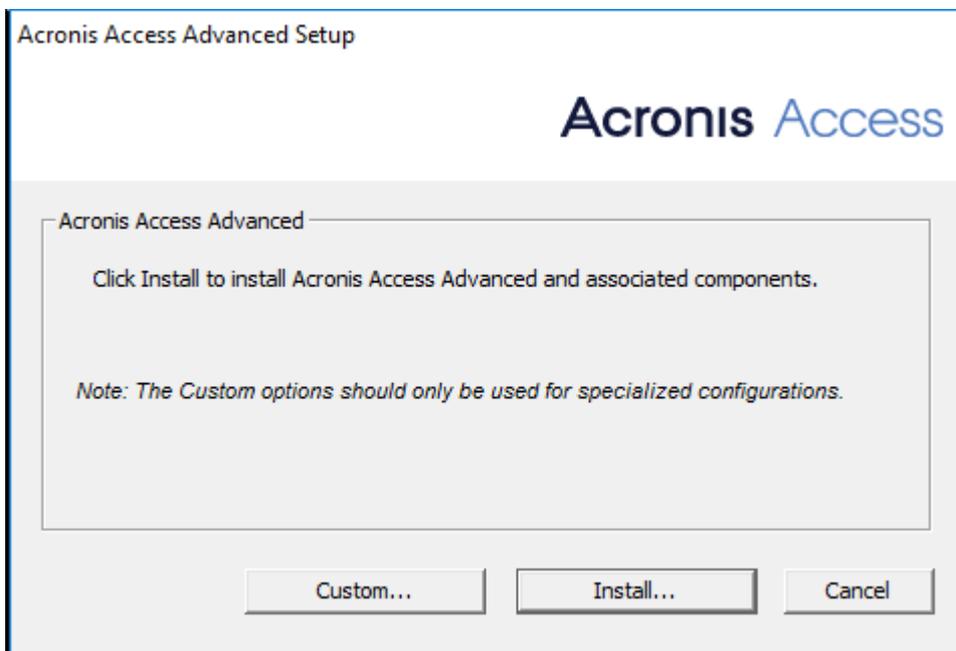
Warning! **DO NOT** upgrade or start any other Access Tomcat server until the **Primary** server is back up and you have verified that it is working correctly.

1. Copy the Acronis Access Advanced installer to any machine with only a Gateway Server and run the installer.

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



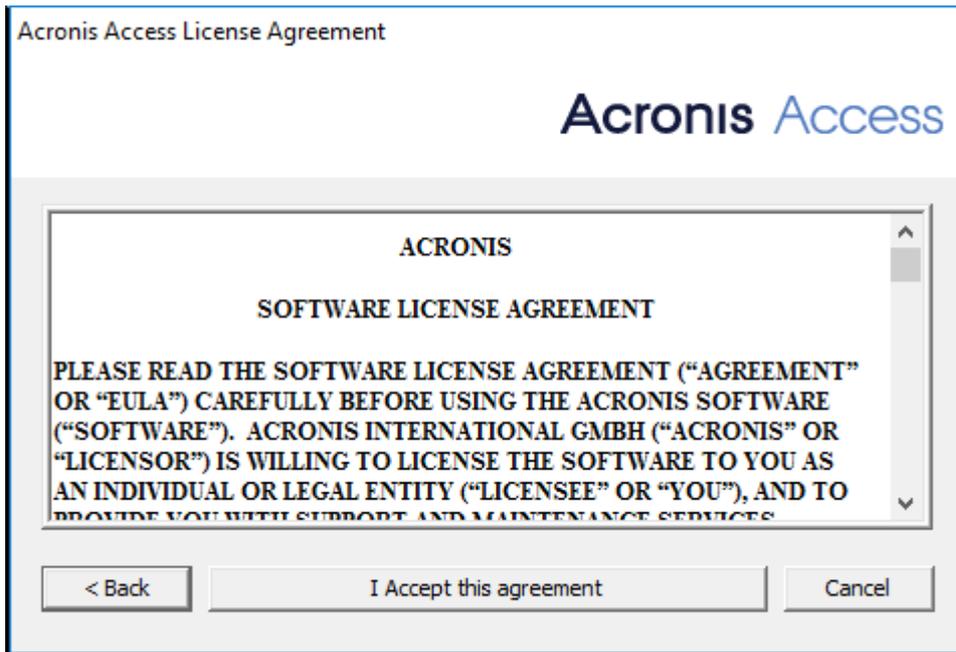
3. Accept the License Agreement.



4. Choose **Custom...** and select only the Acronis Access Gateway Server to upgrade.
5. Click **Next**, review what is going to be installed and click **Install**.
6. When the upgrade is done, click **Exit**. When the Configuration Utility launches, click **OK**.

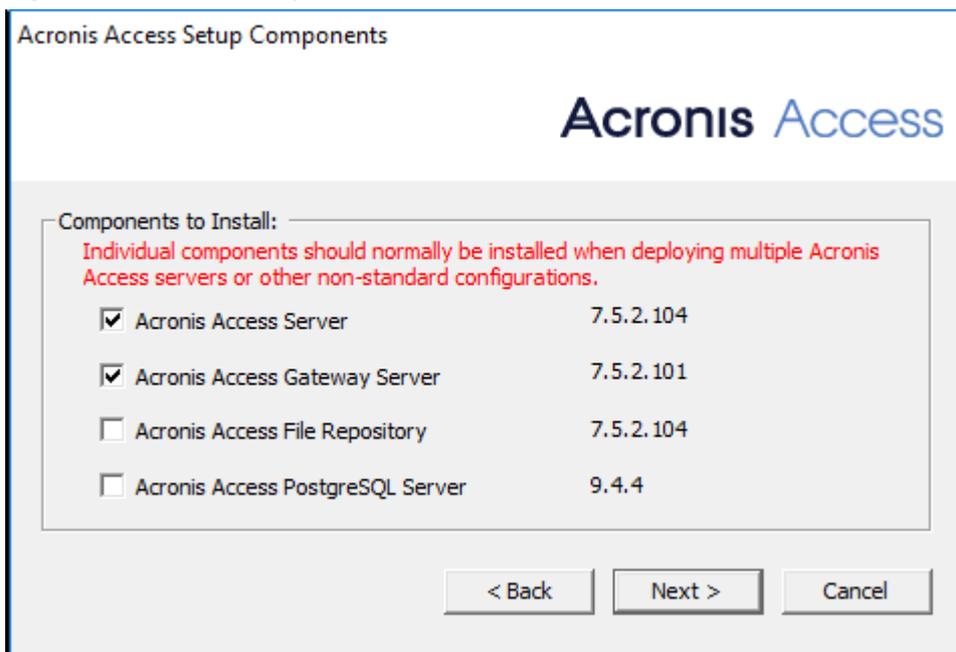
Once you have successfully updated the **Primary** Acronis Access node, all File Repository servers and all Gateway Servers, continue by upgrading the rest of the Acronis Access Servers.

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



2. Press **Next** on the Welcome screen and then **Custom**. This will allow you to upgrade only the necessary services that are already installed on the machine, without installing others.
3. Select any Acronis Access services that you wish to upgrade. Choose only the ones that are already present on the machine.
e.g. If there is only a Gateway server installed, select only the Gateway Server component in the installer.

e.g. If there is a Gateway Server and an Access Server, select both.



Note: Our installer will not update PostgreSQL. If you wish to update your version of PostgreSQL please view our article on the subject (p. 163) and contact Acronis support before proceeding.

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

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

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

7 Mobile Access

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

In this section

Concepts.....	53
Policies	55
On-boarding Mobile Devices	75
Managing Gateway Servers	83
Managing Data Sources	96
Settings.....	102

7.1 Concepts

Acronis 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 in the same network as existing file servers, allowing iPads, iPhones, Windows and Android devices to access files located on that network. These are typically the same files already available to PCs using Windows file sharing and Macs using Access Connect Server.

Clients access Acronis Access servers using their Active Directory user account. No additional accounts need to be configured within Acronis Access. The Acronis Access app 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 installed. This scenario allows Access users to connect to this single file server, and allows for client management on mobile devices. If client management is not needed, Data Sources can be setup on the local Gateway Server and the Acronis Access mobile clients will be able to access these Data Sources, but the users will be in control of their app settings.

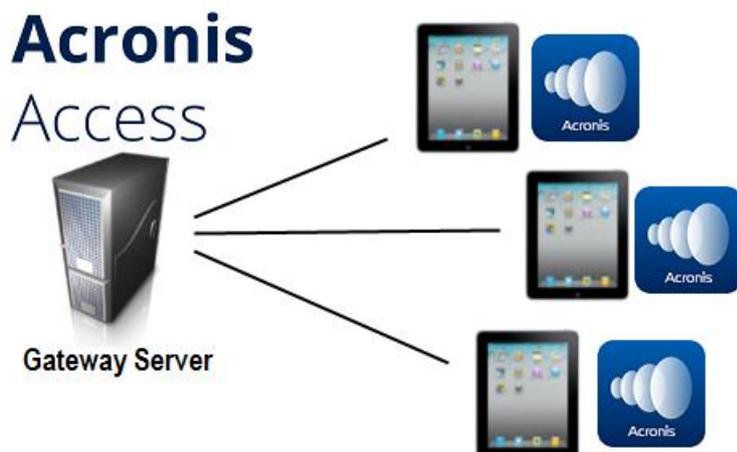


Fig 1. Single Acronis Access server with a Local Gateway Server

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

Note: Details on installing Acronis Access are included in the *Installing* (p. 22) section of this guide. Configuration of Gateway Servers and Data Sources is explained in the *Mobile Access* (p. 53) section.

If you wish to remotely manage your Access Mobile Clients, Acronis Access Management allows you to create policies per Active Directory user or group. Only one Acronis Access Server is required and these policies can:

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

A typical network employing client management includes one server with the Acronis 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. 55) and *Managing Mobile Devices* (p. 114) section of this guide.

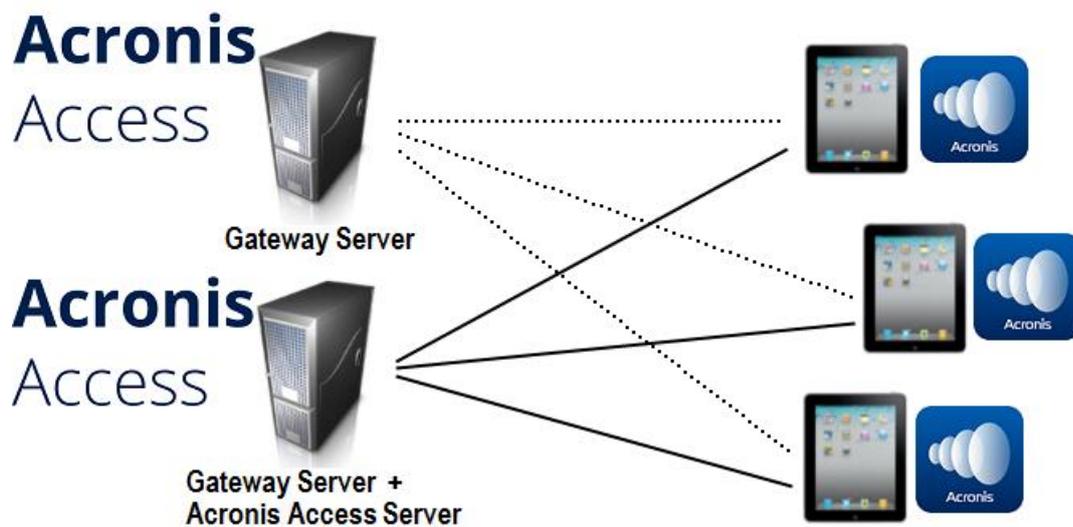


Fig 2. One Gateway Server, one Gateway Server + Acronis Access Server

7.2 Policies

Acronis Access 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

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

- Group Policies
- User Policies
- Allowed Apps
- Default Access Restrictions

Manage Group Policies

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

+ Add Group Policy

Filter by
Name
▼

Filter

Common Name / Display Name	Distinguished Name		Enabled
Default			<input checked="" type="checkbox"/>

In this section

Adding a New Policy.....	56
Modifying Policies	57
Policy Settings	58
Creating a Blocked Path list	71
Allowed Apps	72
Default Access Restrictions	74

7.2.1 Adding a New Policy

To add a new group policy:

1. Open the **Group Policies** tab.

2. Click the **Add new policy** button to add a new group policy. This will open the **Add a new group policy** page.

Add a New User Policy

Save

Search your directory and select a user for this policy.

Selected User John Doe

Find user that begins with Search

Copy Policy Settings from: Apply

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

3. In the **Find group** field, enter the partial or complete Active Directory group name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory groups. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the group name in the listed results.
5. Make the necessary configurations in each of the tabs (Security (p. 59), Application (p. 61), Sync (p. 66), Home Folders (p. 67) and Server (p. 69)) and press **Save**.

To add a new user policy:

1. Open the **User policies** tab.
2. Click the **Add new policy** button to add a new user policy. This will open the **Add a new user policy** page.
3. In the **Find user** field, enter the partial or complete Active Directory user name for which you'd like to create a policy. You can perform '**begins with**' or '**contains**' searches for Active Directory users. Begins with search will complete much faster than contains searches.
4. Click **Search** and then find and click the user name in the listed results.
5. Make the necessary configurations in each of the tabs (Security (p. 59), Application (p. 61), Sync (p. 66), Home Folders (p. 67) and Server (p. 69)) and press **Save**.

7.2.2 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.

Connectivity requirements

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

To modify 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.

7.2.3 Policy Settings

In this section

Security Policy	59
Application Policy	61
Sync Policy	66
Home Folders	67
Server Policy	69
Exceptions for policy settings	71

7.2.3.1 Security Policy

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

App Password Creation: **B M I**

- Optional
- Disabled
- Required

App Will Lock:

Allow User to Change This Setting

Minimum Password Length:

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

Require One or More Letter Characters

Mobile client app will be wiped after failed app password attempts

Wipe or Lock After Loss of Contact

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

Warn user starting days beforehand

App Crash Reporting: **i**

- Never send reports
- Allow user to choose to send reports
- Always send reports

Allow iTunes and iCloud to Back up Locally Stored Acronis Access Files **A B**

User Can Remove Mobile Client from Management

Wipe All Acronis Access Data on Removal

- **App password creation** - The Access Mobile Client application can be set with a lock password that must be first entered when launching the application.

- **Optional** - This setting will not force the user to configure an application lock password, but they will be able to set one from the **Settings** menu within the app if they desire.
- **Disabled** - This setting will disable the ability to configure an application lock password from the **Settings** menu within the app. This might be useful in the case of shared mobile devices where you prefer that a user cannot set an app password and will lock other users out of the Access Mobile Client.
- **Required** - This setting will force the user to configure an application lock password if they do not already have one. The optional application password complexity requirements and failed password attempt wipe setting only apply when **App password creation** is set to **Required**.
 - **App will lock** - This setting configures the application password grace period. When a user switches from the Access Mobile Client to another application on their device, if they return to the Access Mobile Client before this grace period has elapsed, they will not be required to enter their application lock password. To require that the password is entered every time, choose **Immediately upon exit**. If you would like the user to be able to modify their **App will lock** setting from within the Access Mobile Client settings, select **Allow user to change this setting**.
 - **Minimum password length** - The minimum allowed length of the application lock password.
 - **Minimum number of complex characters** - The minimum number of non-letter, non-number characters required in the application lock password.
 - **Require one or more letter characters** - Ensures that there is at least one letter character in the application password.
 - **Mobile Client app will be wiped after X failed app password attempts** - When this option is enabled, the settings and data in the Access Mobile Client app will be wiped after the specified number of consecutive failed app password attempts.
- **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 it's Acronis Access Server and prevent the lock or wipe.
- **App Crash Reporting** - Sends reports to Acronis if the mobile apps crash. No private data or identifying information is sent.
 - **Never send reports**
 - **Allow user to choose to send reports**
 - **Always send reports**

- **Allow iTunes and iCloud to back up locally stored Acronis Access files** - When this setting is disabled, the Access Mobile Client will not allow iTunes or iCloud to back up its files. This will ensure that no files within Acronis Access' secure on-device storage are copied into the backups.
- **User can remove Mobile Client from management**- Enable this setting if you would like your Acronis 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.

7.2.3.2 Application Policy

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

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

Require Confirmation When Deleting Files

Allow User to Change This Setting

Set the Default File Action **A**

Default Action: Show Action Menu

Allow User to Change This Setting

Allow Files to be Stored on This Device

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

Cache Recently Accessed Files on the Device

Maximum Cache Size: 100 MB

Allow User to Change This Setting

Content in My Files and File Inbox Expires after 21 days

- **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 Filesfolder, sync folders, recently accessed file caching) can be enabled or disabled using additional policy settings. If this option is disabled, no files will be stored on the device, ensuring that no corporate data is on the device if it is lost or stolen. If this setting is disabled, the user will not be able to save or sync files for offline use, cache files for improved performance, or send files from other applications to the 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 and have not changed, providing performance and bandwidth conservation benefits. **Maximum Cache Size** can be specified and the user can optionally be allowed to change this setting.
- **Content in My Files and File Inbox Expires after X days** - If this option is enabled, files in **My Files** will be deleted from the device after the set number of days.

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 server Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file creation.
- **File Deletes** - If this option is disabled, the user will not be able to delete files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file deletion.
- **File Moves** - If this option is disabled, the user will not be able to move files from one location to another on the Gateway Server, or from the server to the Access Mobile Client application's local My Files storage. This setting supersedes any NTFS permissions that client may have that allow file or folder moves.

- **File Renames** - If this option is disabled, the user will not be able to rename files from the Gateway Server. This setting supersedes any NTFS permissions that client may have that allow file renames.

Folder Operations

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

'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.

Hyperlinks in Documents

- **Allow Opening Hyperlinks in Documents** - When enabled, users will be able to open any hyperlinks that are saved in their documents.
 - **Allow User to Change These Settings** - When enabled, users will be able to enable or disable this feature based on their preference.

Open into:

- **Inline Browser** - Hyperlinks will be opened directly in the Acronis Access app.
- **Default Browser** - Hyperlinks will be opened in the default browser selected on your device.
- **MobileIron Web@Work** - Hyperlinks will be opened in the MobileIron Web@Work app.
- **Blackberry Access** - Hyperlinks will be opened in Good Access app.

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.
- **Allow use of Document Provider** - Allows mobile devices to use the Document Provider extension for Acronis Access. The Document Provider Extension can be affected by certain configurations:
 - a. If a client is managed by an older server, the Document Provider Extension is enabled unless either **Opening Acronis Access Files in Other Applications** is **disabled** or there is a black/white list **enabled**.
 - b. If a client is managed by a new server (version 7.3.1 and newer) and **Allow use of Document Provider** is enabled, even if **Opening Acronis Access Files in Other Applications** is **disabled** or there are white/black lists **enabled**, users will still be able to share files with other apps. Even specifically blocked ones.
 - c. If **Allow use of Document Provider** is enabled, but the creation of files is disabled, the Document Provider Extension will work but users will not be able to save files from other apps to any Acronis Access Data Sources.
- **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.
- **Importing Files from camera/photo library** - When enabled, users will be able to import photos and videos from their device's photo library directly into Acronis Access.
- **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.

***Note:** The Android platform does not have a built-in email app or function that can be disabled. To block users from moving files into emails, you must instead disable Opening Acronis Access files into Other Applications.*

- **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.

File Editing

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

PDF Annotation

- **Allow PDF annotation** - When this option is disabled, the Access Mobile Client will not be allowed to annotate PDFs.
 - **Allow Creation of Empty PDF Files** - When enabled, enables users to create empty PDF files which they can edit with Annotations.
- **Apply custom PDF view settings** - When enabled, all of the sub-settings will apply for all users, for all PDFs.
 - **Allow User to Change These Settings** - When enabled, users will be able to change their PDF viewing settings.
 - **Fit to Width** - When enabled, resizes the page so it will fit the width of your device's screen.
 - **Night Mode** - When enabled, the device uses the Night Mode color scheme for a more comfortable viewing experience in low-lit areas.
 - **Scroll Direction** - Lets you choose if the pages should change vertically or horizontally.
 - **Page Transitions** - Lets you choose the transition visual effects. **Slide** will just change the pages, **Continuous** will let you scroll through the pages as if they are 1 connected piece and **Curl** will flip the pages like a book.
 - **Page Display Mode** - Lets you choose if the PDF should be displayed as two pages or just one single page.
 - **Search Settings** - Lets you choose how search results will be displayed. **Simple** will highlight the results and you can scroll through them with the arrow icons, **Detailed** will display a drop-down of all results and you can navigate by tapping on them.
 - **Thumbnails** - Sets the size for the thumbnails of the pages when you open a PDF. You can choose between **Small**, **Large** and **None**.
 - **Search** - Configures the display format of the search results provided by the built-in PDF viewer.
 - **Hyperlink Highlighting** - Lets you choose the color that will highlight hyperlinks. You can also disable the highlighting by selecting **Disabled**.

7.2.3.3 Sync Policy

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

Allow User to Create Sync Folders

The following features are not supported by older mobile client apps. Please see this knowledge base article for details on the mobile client apps that support these features.

Only Allow 1-way Sync Folders to be Created ⓘ

Default Sync Folder Type ⓘ

Client is Prompted to Confirm before Synced Files are Downloaded:

Allow User to Change This Setting

Only Allow File Syncing While Device Is on WiFi Networks

Allow User to Change This Setting

Auto-Sync Interval:

Allow User to Change This Setting

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

Prevent device from sleeping during file sync ⓘ

Allow User to Change This Setting

- **Allow User to Create Sync Folders** - Allows the user to create their own sync folders.
 - **Only Allow 1-way Sync Folders to be Created** - Users will be able to create only 1-way sync folders.
 - **Default Sync Folder Type** - Sets either 1-way or 2-way as the default Sync folder type.
- **Client is Prompted to Confirm Before Synced Files are Downloaded** - Select the conditions under which the user must confirm before files in synced folders are downloaded. Options are: **Always**, **While on cellular networks only**, and **Never**. If **Allow User to Change This Setting** is enabled, clients will be able to change the confirmation options.
- **Only Allow File Syncing While Device is on WiFi Networks** - When this option is enabled, Acronis 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.

- **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.
- **Prevent device from sleeping during file sync** - When enabled, devices supporting this setting will not lock/sleep if you have file syncs in progress. If **Allow User to Change This Setting** is enabled, clients will be able to change the confirmation options.

7.2.3.4 Home Folders

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

Display the User's Home Folder

Display Name Shown on Client: Home Folder

Home Directory Type:

Active Directory Assigned Home Folder

Gateway Server used for access to Home Folders:

Local (192.168.2.129:3000) ▼

Custom Home Directory Path

Gateway Server: Not Selected

Home Folder Path: Not Selected

Sync to mobile client: None ▼

- **Display the user's home folder**- This option causes a user's personal home directory to appear in the Access Mobile Client app.
 - **Display name shown on client** - Sets the display name of the home folder item in the Access Mobile Client app. The **%USERNAME%** wildcard can be used to include the user's username in the folder name that will be displayed.

Note: The **%USERNAME%** wildcard cannot be used to display the user's username on any other type of data source. You can only use it on Active Directory assigned Home Folders.

- **Active Directory assigned home folder** - The home folder shown in the 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 for any data source type. **%USERNAME%** must be capitalized.
- **Sync to mobile client** – This option selects the type of sync of your Home Directory.

Note: *This option does **NOT** affect the user's ability to sync their Home Folder with the desktop client.*

7.2.3.5 Server Policy

Security Policy

Application Policy

Sync Policy

Home Folders

Server Policy

Required Login Frequency for Resources Assigned by This Policy:

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

Allow User to Add Individual Servers

- Allow Saved Passwords for User Configured Servers

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

Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client

Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client

Allow User to Add Network Folders by UNC path or URL

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

Local (192.168.2.129:3000) ▼

Block access to specific network paths

Blocked Path List:



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

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

Warn Client When Connecting to Servers with Untrusted SSL Certificates

Client Timeout for Unresponsive Servers: 30 seconds ▼

Allow User to Change This Setting

Trigger Intune Mobile Application Management enrollment

- **Required login frequency for resources assigned by this policy**- sets the frequency that a user must log into the servers that are assigned to them by their policy.

- **Once only, then save for future sessions** - The user enters their password when they are initially enrolled in management. This password is then saved and used for any file server connections they later initiate.
- **Once per session** - After launching the Access Mobile Client, the user is required to enter their password at the time they connect to the first server. Until they leave the Access Mobile Client application, they can then connect to additional servers without having to reenter their password. If they leave the Access Mobile Client for any period of time and then return, they will be required to enter their password again to connect to the first server.
- **For every connection** - The user is required to enter their password each time they connect to a server.
- **Allow user to add individual servers** - If this option is enabled, users will be able to manually add servers from within the Access Mobile Client application, as long as they have the server's DNS name or IP address. If you want the user to only have their policy **Assigned Servers** available, leave this option disabled.
 - **Allow saved passwords for user configured servers** - If a user is allowed to add individual servers, this sub-option determines whether they are allowed to save their password for those server.
- **Allow File Server, NAS and Sharepoint Access From the Web Client** - When enabled, Web Client users will be able to see and access mobile Data Sources as well.
 - **Allow File Server, Nas and SharePoint Folders to be Synced to the Desktop Client** - When enabled, desktop clients will be allowed to 1-way sync **Network** content.
 - **Allow Two-Way Syncing of File Server, Nas and SharePoint Folders to the Desktop Client** - When enabled, desktop clients will be allowed to 2-way sync **Network** content.

Note:** To enable the 2-way syncing of **Network** content for the desktop clients, you must also have allowed the following file and folder actions on the **Application Policy** tab: **Creation (Adding for folders), Copies, Deletes, Moves and Renames.

- **Allow User to Add Network Folders by UNC path or URL** - When enabled, the mobile client users will be able to add and access network folders and SharePoint sites not assigned to them or not accessible through the existing Data Sources. The selected Gateway Server must have access to those SMB shares or SharePoint sites.
 - **Block access to specific network paths** - When enabled, allows the administrator to create and use blacklists of network paths which the users shouldn't be allowed to self-provision.
- **Only allow this Mobile Client to connect to servers with third-party signed SSL certificates** - If this option is enabled, the Access Mobile Client will only be permitted to connect to servers with third-party signed SSL certificates.

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

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

able to change this through the Access Mobile Client app, check **Allow user to change this setting**.

7.2.3.6 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 AppConnect** 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.

7.2.4 Creating a Blocked Path list

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

To create a list:

1. Open the web interface as an administrator.
2. Open the Policies (p. 55) page.
3. Click on the desired User policy or Group policy.
4. Open the Server Policy (p. 69) tab.
5. Select the **Block access to specific network paths** check box.

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

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

To enable the blacklist for a User or Group policy:

1. Open the web interface as an administrator.
2. Open the Policies (p. 55) page.
3. Click on the desired User policy or Group policy.

4. Open the Server Policy (p. 69) 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.

7.2.5 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

Adding Apps Available for Lists	72
Finding an App's bundle identifier	73

7.2.5.1 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 app's bundle identifier exactly, or it will not white or blacklisted.
5. Click **Save**.

You can find the bundle identifier either by browsing the files on your device or you can view it in an iTunes Library.

Add a New App ×

Add any app you would like to include in a whitelist or blacklist.

In order for Acronis Access to identify an app, the app's unique "Bundle Identifier" is required. [Click here](#) for instructions on how to find an app's bundle identifier.

App Name:

Bundle Identifier:

7.2.5.2 Finding an App's bundle identifier

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

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

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

Finding an app's bundle identifier in an iTunes Library

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

1. Navigate to your iTunes Library and open the **Mobile Applications** folder.
2. On a Mac, this is typically in your home directory, in `~/Music/iTunes/Mobile Applications/`
3. On a Windows 7 PC, this is typically in `C:\Users\username\My Music\iTunes\Mobile Applications/`
4. If you have recently installed the app on your device, make sure you have performed an iTunes sync before you continue.

5. Locate the app that you require in the **Mobile Applications** folder.
6. Duplicate the file and rename the extension to .ZIP
7. Unzip this newly created ZIP file and you'll end up with a folder with the application name.
8. Inside that folder is a file called **iTunesMetadata.plist**
9. Open this PLIST file in a text editor.
10. Find the **softwareVersionBundleId** key in the list.
11. The **string** value below it is the bundle identifier value that you will need to enter for the app in Acronis Access. These are commonly formatted as: **com.companyname.appname**

7.2.6 Default Access Restrictions

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

Note: For information on setting custom access restrictions for your Gateway Servers visit the *Editing Gateway Servers (p. 87)* article in the *Managing Gateway Servers* section.

Configure the client enrollment status, client app types and authentication methods that can be used to connect to this Acronis 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 a 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 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 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 Blackberry Dynamics managed Android clients** – If you select this option, this Acronis Access server will allow users using the Android Access Mobile Client Good Dynamics managed client to connect. If you do not want to allow users with the Android Access Mobile Client Good Dynamics client 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 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 'iOS Managed App' iOS Client** – If you select this option, this Acronis Access server will allow users running the Acronis Access managed iOS Access app to connect. In order to be in this state, a client must received a Managed App Configuration (p. 279) containing at least one parameter. If you do not want to allow managed iOS users to access this Acronis Access server, you can uncheck this setting.
 - **Allow Blackberry Dynamics managed 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 Intune managed iOS clients** – If you select this option, this Acronis Access server will allow users using the iOS Access Mobile Client Intune managed client to connect. If you do not want to allow users managed by Intune to access this Acronis Access server, you can uncheck this setting.
 - **Allow AppConnect managed 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.
- **Allow Acronis Access Windows Mobile clients to access this server** -
 - **Allow Windows Phone client** - If you select this option, this Acronis Access server will allow phone users running the Windows Mobile Acronis Access app to connect. If you do not want to allow Windows Mobile users to access this Acronis Access server, you can uncheck this setting.
 - **Allow Windows Tablet / Desktop client** - If you select this option, this Acronis Access server will allow tablet users running the Windows Mobile Acronis Access app to connect. If you do not want to allow Windows Mobile users to access this Acronis Access server, you can uncheck this setting.

7.3 On-boarding Mobile Devices

To get started with the Acronis Access mobile client, users need to install the app through their respective App Store - iTunes, Google Play or Windows 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.....	76
User-side Management Enrollment Process	79

7.3.1 Server-side Management Enrollment Process

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

Enrollment Settings

Allow mobile clients restored to new devices to auto-enroll without PIN -

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

Device Enrollment Mode

Acronis 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 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.

Enrollment Invitations

Send an enrollment invitation to invite mobile clients to enroll with this Acronis Access server. This invitation will include their unique, required PIN number, instructions, and a shortcut to begin the enrollment process. If you choose to give your users their PIN number by other means, they can also initiate the enrollment process from the Acronis Access Mobile Client Settings menu or by opening this URL while on their device: `mobileEcho://avid.gililabs.com/enroll`

Filter by Username Filter Reset

Username	Display Name	Email Address	Distinguished Name	Expires	PIN	
mike	Michael Collins	mike@grouplogix.com	CN=Michael Collins,CN=Users,DC=gililabs,DC=com	2014-02-17 13:35:55	6PXXGAXN	✘
mike	Michael Collins	mike@grouplogix.com	CN=Michael Collins,CN=Users,DC=gililabs,DC=com	2014-02-17 13:35:55	WYN62CCA	✘
mike	Michael Collins	mike@grouplogix.com	CN=Michael Collins,CN=Users,DC=gililabs,DC=com	2014-02-17 13:35:54	P2R2JRQF	✘

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. 102)* section.

To generate a Acronis Access enrollment invitation:

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

7.3.2 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.

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

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

[Hide](#)

pam@gililabs.com,

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

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

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

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

[Tap here to install Acronis Access for Android](#)

2. Begin the enrollment process:

On iOS:

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

On Android:

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

PIN: D34WNNQ

Server Address: 192.168.1.72:3000

Username: pam@gililabs.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 enters their password to complete the enrollment process.

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

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

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

To enroll in management

Enroll automatically via enrollment email

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

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

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

Manual enrollment

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

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

Ongoing Management Updates

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

Connectivity requirements

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

Removing Management

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

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

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

To unmanage your device follow the steps below:

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

Note: *If your Acronis Access policy does not allow you to unmanage your client, the **Use Management** option will not be displayed on the **Settings** menu. In this case the only way to remove the device from management is by uninstalling the 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 app, follow the steps below:

For iOS:

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.

For Windows:

1. Tap and hold the app icon.

2. Select **Uninstall**.

For Android:

Note: Android devices software vary and you settings might look slightly different.

1. Open your App menu and select **Edit/Remove**.
2. Find the Access app and select it.
3. Press **Remove**.

7.4 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.

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

Note: If your IT administrator has not installed Windows Search, you will only be able to search **By Name**.

Support for content search of shared folders 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.

By Content search **requires** that the **Microsoft Windows Search** service is installed on the Acronis Access Gateway server machine and is configured to index any Data Sources where content search is enabled.

Windows Search is built into Windows Server 2008 but it is not enabled by default. To enable it, you have to add the Role called **File Services** in the Server Manager, and the **Windows Search Service** must be enabled. **Windows Search** can be configured to index the necessary Data Sources by right-clicking the Windows Search icon in the Start bar and selecting Windows Search Options. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

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

SharePoint

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

In this section

Registering new Gateway Servers.....	84
Server Details	86
Gateway Server Configurations	87
Licensing Gateway Servers.....	94
Cluster Groups	94

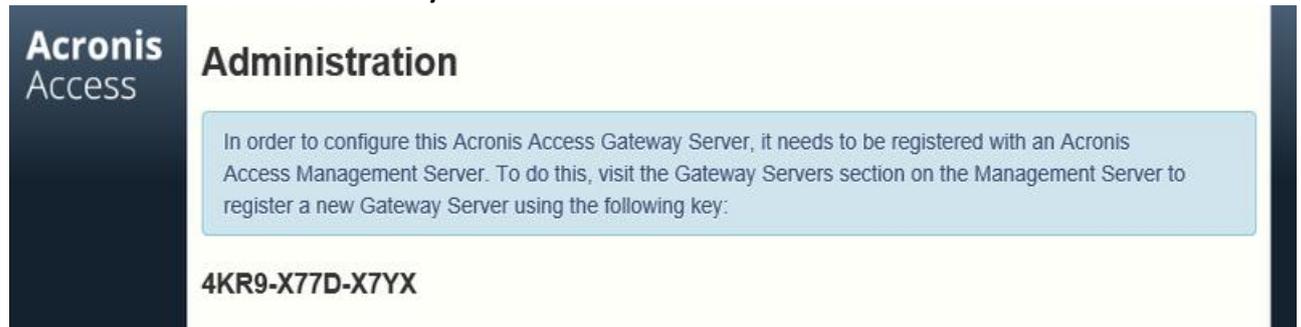
7.4.1 Registering new Gateway Servers

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/gateway_admin.

Note: The port 3000 is the default port. If you have changed the default port, add your port number after localhost.

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



The screenshot shows the Acronis Access Administration interface. On the left is the Acronis Access logo. The main heading is "Administration". A light blue box contains the following text: "In order to configure this Acronis Access Gateway Server, it needs to be registered with an Acronis Access Management Server. To do this, visit the Gateway Servers section on the Management Server to register a new Gateway Server using the following key:". Below this box, the Administration Key "4KR9-X77D-X7YX" is displayed.

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

Add New Gateway Server

Display Name:

Address for administration: ⓘ

Use alternate address for client connections ⓘ

Administration Key: ⓘ

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

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

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

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

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. 87) section.

7.4.2 Server Details

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

Status

Local ✕

Status Active Users

Display Name Local

Address for administration avid.gllilabs.com

Address for client connections avid.gllilabs.com

Operating System Microsoft Windows Server 2008 R2 Enterprise Edition Service Pack 1, 64-bit

Gateway Server version 7.0.0x160

Status Online

Last Contact 2014-11-11 07:41:25

Active Sessions 0

Licenses Used 0 of 500

Close

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

Active Users

Local ✕

Status Active Users



User	Location	Device	Model	OS	Client Version	Policy	Idle Time
fmedre	192.168.11.74:49325	T-Soft iPod touch 5G	iPod Touch 5G	iOS	6.1.0.158	Frank Medre	00:00:07
jprice	192.168.11.63:52087	iPad3	iPad 3 (WiFi)	iOS	6.1.0.158	John Price	00:00:13

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.

7.4.3 Gateway Server Configurations

In this section

.....89

You can use the default access restrictions set in the Policies (p. 55) section or you can set custom access restrictions for each Gateway Server.

Setting custom access restrictions for a specific Gateway Server

1. Press the Down arrow next to the **Details** button.
2. Select **Access Restrictions**.
3. Open the **Use Custom settings** tab.
4. Select the specific access restrictions you want for this Gateway Server.
5. Press **Apply**.

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.

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.

Edit Server: Local ×

General Settings **Logging** Search SharePoint Advanced

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

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

Audit Logging Archive Log File

Debug Logging

OK Apply Cancel

To enable Audit Logging for a specific gateway server:

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

To enable Debug Logging for a specific gateway server:

Note: The default location for the debug logs is: **C:\Program Files (x86)\Acronis\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 arrow next to the **Details** button and select **Edit**.

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

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

Note: *If your IT administrator has not installed Windows Search, you will only be able to search **By Name**.*

Support for content search of shared folders 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.

By Content search **requires** that the **Microsoft Windows Search** service is installed on the Acronis Access Gateway server machine and is configured to index any Data Sources where content search is enabled.

Windows Search is built into Windows Server 2008 but it is not enabled by default. To enable it, you have to add the Role called **File Services** in the Server Manager, and the **Windows Search Service** must be enabled. **Windows Search** can be configured to index the necessary Data Sources by right-clicking the Windows Search icon in the Start bar and selecting Windows Search Options. You can do Windows content searches on Windows reshares but the remote machine(s) must be in the same domain as the Gateway Server.

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

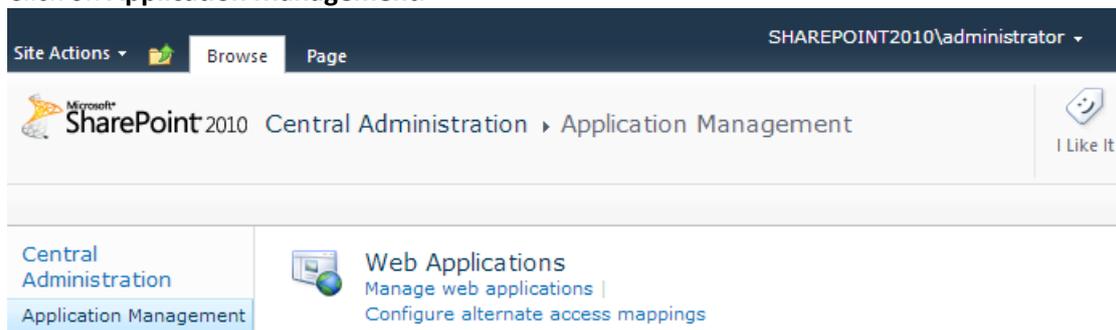
Entering these credentials is optional for general SharePoint support, but required to enumerate site collections. For example, say you have two site collections:

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

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

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

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



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

Web Application General Policy		Port
Define broad permissions policies.		
Name	URL	Port
SharePoint - 21815	http://sharepoint2010.gililabs.com:21815/	21815
SharePoint - 21816	http://sharepoint2010.gililabs.com:21816/	21816
SharePoint - 2229	http://sharepoint2010.gililabs.com:2229/	2229
SharePoint Claims - 23934	http://sharepoint2010.gililabs.com:23934/	23934
SharePoint - 80	http://sharepoint2010/	80
SharePoint - 25054	http://sharepoint2010:25054/	25054
SharePoint Central Administration v4	http://sharepoint2010:5869/	5869
SharePoint - 13537	https://sharepoint2010.gililabs.com:13537/	13537
SharePoint - 43224	https://sharepoint2010.gililabs.com:43224/	43224

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

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

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

Edit Users

Users

The policy for these users will be modified.

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

Permission Policy Levels

Choose the permissions you want these users to have.

Permissions:

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

Choose System Settings

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

Account operates as System

Save Cancel

- Press the **Save** button.

Edit Server: Local



General Settings

Logging

Search

SharePoint

Advanced

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

- Hide inaccessible items
 - Hide inaccessible items on reshares ⓘ
 - Hide inaccessible SharePoint sites
 - Minimum Android client version
 - Minimum iOS client version
 - Use Kerberos for SharePoint Authentication
 - Allow connections to SharePoint servers using self-signed certificates
 - Allow connections to Acronis Access servers using self-signed certificates
 - Accept self-signed certificates from this Gateway Server ⓘ
 - Show hidden SMB Shares
 - Use user principal name (UPN) for authentication with SharePoint Servers ⓘ
 - Perform Negotiate/Kerberos authentication in user-mode ⓘ
- Client session timeout in minutes

OK

Apply

Cancel

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

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

Note: Enabling this feature can have a significant negative impact while browsing folders.

- **Hide inaccessible SharePoint sites** - When enabled, SharePoint sites for which the user does not have the necessary permissions will not be shown.
- **Minimum Android client version** - When enabled, users connecting to this Gateway will be required to have this or a later version of the Acronis Access Android client app.
- **Minimum iOS client version** - When enabled, users connecting to this Gateway will be required to have this or a later version of the Acronis Access iOS client app..

- **Use Kerberos for SharePoint Authentication** - If your SharePoint server requires Kerberos authentication, you should enable this setting. You will also need to make an update to the Active Directory computer object for the Windows server or servers that are running the Gateway server software. The Acronis Access Windows server needs to be given permission to present delegated credentials to your SharePoint server on behalf of you users. Enabling the Acronis Access Windows server to perform Kerberos Delegation:
 1. In **Active Directory Users and Computers**, locate the Windows server or servers that you have the Gateway Server installed on. They are commonly in the **Computers** folder.
 2. Open the **Properties** window for the Windows server and select the **Delegation** tab.
 3. Select **Trust this computer for delegation to specified services only**
 4. Select **Use any authentication protocol**, this is required for negotiation with the SharePoint server.
 5. You must now add any SharePoint servers that you would like your users to be able to access using Acronis Access . If your SharePoint implementation consists of multiple load balanced nodes, you will need to add each SharePoint/Windows node to this list of permitted computers. Click **Add...** to search for these Windows computers in AD and add them. For each, you will need to select the "http" service type only.

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

- **Allow connections to SharePoint servers using self-signed certificates** - When enabled, allows connections from this Gateway to SharePoint servers using self-signed certificates.
- **Accept self-signed certificates from this Gateway Server** - When enabled, allows connections from this Gateway to Acronis Access servers using self-signed certificates.
- **Allow connections to Acronis Access servers with self signed certificates** - When enabled, allows connections to this other 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).
- **Perform Negotiate/Kerberos authentication in user-mode** - When enabled, the Gateway server will authenticate using the domain account set in the configuration utility. This is used for configurations requiring Kerberos, Single Sign-On and loadbalancing.

7.4.4 Licensing Gateway Servers

For more information on licensing your Gateway Servers, visit the Licensing (p. 140) section.

7.4.5 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 (p. 184) 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.

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. If necessary, select an alternative address for Acronis Access Server connections by enabling the checkbox and entering the address.
8. Mark the checkbox for each Gateway you want to be in the group.
9. Select the Gateway which will control the group's settings. All of the existing settings on that Gateway (including assigned Data Sources and excluding the address for administration) will be copied to every Gateway in the group.
10. Press **Create**.

Editing a cluster group:

Editing cluster groups does not differ from editing regular Gateways. For more information visit the Editing Gateway Servers (p. 87) article.

Adding members to an existing cluster group:

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

Changing the Master Gateway Server:

1. Open the web interface and navigate to **Mobile Access -> Gateway Servers**.
2. Expand the desired cluster group.
3. Find the Gateway Server that you want to promote to be the Master.
4. Press the **Actions** button and select **Become Group Master**.

7.5 Managing Data Sources

You can share NTFS directories located on your Windows server, on CMIS systems or on a remote SMB/CIFS file share for access by your Acronis Access users. When users connect, they will see these directories as file share volumes.

Access to SharePoint 2007, 2010, 2013, 365 content

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

SharePoint authentication methods supported

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

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

Access to OneDrive for Business content

Acronis Access can be setup to allow users access their personal OneDrive for Business content via a SharePoint data source. There are some requirements and limitations.

Changing Permissions for Shared Files and Folders

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

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

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

In this section

Folders.....	97
Assigned Sources.....	100
Gateway Servers Visible on Clients.....	101
Legacy Data Sources.....	101

7.5.1 Folders

Folders can be assigned to Acronis Access user and group policies, allowing them to automatically appear in a user's Acronis Access app. Folders can be configured to point to any folder residing on a Gateway Server, a remote share, a CMIS volume or even a SharePoint Library. This allows you to give a user direct access to any folders that might be important to them without users having to navigate to the folder or even knowing the exact server, shared volume name, and path to the folder.

Folders can point to any type of content that Acronis 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, a CMIS volume 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

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.

Syncing Folders

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

Note: This setting does not affect the desktop client.

- **None** - The folder will appear as a network-based resource in the Acronis Access 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 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 app. Its complete contents will initially be synced from the server to the device. If files in this folder are added, modified, or deleted, either on the device or on the server, these changes will be synced back to the server or device.

Creating a Data Source

1. Open the Acronis Access Web Interface.
2. Open the **Mobile Access** tab.
3. Open the **Data Sources** tab.
4. Go to **Folders**.
5. Press the **Add New Folder** button.

6. Enter a display name for the folder.
7. Select the Gateway Server which will give access to this folder.
8. Select the location of the data. This can be on the actual Gateway Server, on another SMB server, on a SharePoint Site or Library or on a Sync & Share server.

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

9. Based on your choice of location, enter the path to that folder, server, site or library.
10. Select the **Sync** type of this folder.
11. Enable **Show When Browsing Server** if you want this Data Source to be visible when Acronis Access mobile clients browse the Gateway Server.

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

12. Press the Save button.

Editing a Data Source

1. Open the **Data Sources** section and find the Data Source you want to edit.
2. Click on the **Pencil** icon for your Data Source at the right side of the table.
3. Change all desired parameters and press **Save**.

You can give easy access to SharePoint sites and libraries to your Acronis Access mobile 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

SharePoint Followed Sites

SharePoint Followed Sites can be enabled when creating the Data Source for your site. This is done with the Display Followed Sites checkbox. When enabled, all users that are following sites will see a folder "Followed Sites" in Acronis Access that will contain the resources they have permissions to access from those sites.

Note: *SharePoint Followed Sites cannot be synced.*

Creating a Data Source for a SharePoint Library

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

e.g. URL: `https://sharepoint.mycompany.com:43222`

e.g. Document Library Name: `My Library`

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

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

e.g. URL: `https://sharepoint.mycompany.com:43222`

e.g. Document Library Name: `Marketing Library`

e.g. Subpath: `Sales Report`

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

The 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. 87) article.

The supported CMIS volumes are **Alfresco (CMIS)** and **Documentum (CMIS)** volumes. You can also try using other CMIS vendors that use the **AtomPub** protocol with the **Generic CMIS (AtomPub)** option. This option may or may not work with your vendor and is not supported by Acronis.

We recommend having a Gateway server on the machine hosting the CMIS volumes to decrease timeouts on slow networks.

Note: *CMIS volumes have a limitation that does not allow copying folders.*

Since OneDrive for Business is SharePoint based, its content can be reached by creating a SharePoint Data Source in Acronis Access. As such however, there are some limitations.

- The Data Source **must** point to the wildcard for a user's main personal folder. You cannot create Data Sources pointing to sub-folders, but they are accessible and browsable from the main folder.
- These Data Sources will not work if the Gateway server is added manually in the app - they must be assigned through a policy.

- You Active Directory must be either linked with Office 365, use Federated AD Services or must be an Azure AD.
- Each user will only be able to see their own OneDrive data and will not have access to other users' data, regardless if it is shared and accessible through the Microsoft portal.

Creating the Data Source

1. Open the Acronis 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 the resources.
8. Enter the location of your OneDrive for Business main site, followed by the path for a personal folder, with the **%USERNAME%** wildcard.
e.g. **https://mycompany.sharepoint.com/personal/%USERNAME%**
9. Press the **Save** button.

Active Directory integration

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

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

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

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

7.5.2 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.
- The Folders table lists the Data Source's display name, Gateway Server, sync type, path and the policies to which this Data Source is assigned.
- By pressing the **Edit resources assigned to** button, the administrator can quickly edit the assignments for this policy.

7.5.3 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 app 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.
 - 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.

7.5.4 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.

Folders Assigned Sources Gateway Servers Visible on Clients Legacy Data Sources

Add New Legacy Folder

Legacy Data Sources

Some of the existing "Folders" configured on your mobilEcho Client Management Server prior to upgrading to mobilEcho 5.0, have been imported as "Legacy Folders". The Legacy Folders listed below point to locations on mobilEcho Gateway Servers that have not yet been upgraded to mobilEcho 5.0, or that have been upgraded to mobilEcho 5.0, but have not been registered to be administered from this Acronis Access Server. Once you upgrade these Gateway Servers to mobilEcho 5.0 and register them on the [Gateway Servers](#) page, their Legacy Folders will be imported into the standard [Folders](#) list.

If you need to add or edit folders located on these Gateway Servers prior to upgrading them to mobilEcho 5.0, you can do so from this page.

Type	Display Name	Server	Path	Sync	
	Management Projects	192.168.1.128:443	C:\Program Files (x86)\Acronis\Access\Gateway Server	None	

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.

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. 83) 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.

7.6 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.
- **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.

8 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

- General Restrictions104
- Sharing Restrictions105
- LDAP Provisioning107
- Quotas108
- File Purging Policies108
- User Expiration Policies110
- File Repository110
- Acronis Access Client112

8.1 General Restrictions

These restrictions apply to the usage of Sync & Share storage for all internal and external users

■ Maximum allowed file size 1024 MB

Blacklisted file types Specify file types not allowed, by file extension (e.g. mp3, exe).

+ Add

- Remove

You can set basic restrictions such as blacklisting file types and files over a certain size.

Maximum allowed file size - Allows you to set a maximum file size for all Sync & Share files.

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

To set a file type blacklist:

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

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

To set a maximum file size limit:

1. In the web console, expand the **Sync & Share** tab and open **General Restrictions**.
2. Select the **Maximum allowed file size** checkbox and enter the desired maximum file size in the text field (in MBs).
3. Press **Save**.

Note: Any preexisting files of a bigger size will no longer be synced and will not be movable. You can only manually download them or remove them.

8.2 Sharing Restrictions

- Allow Collaborators to Invite Other Users

Single File Sharing

- Enable Single File Sharing
 - Allow Public Download Links
 - Allow 'All Acronis Access Users' Download Links
 - Allow Only Internal (AD) Users to Download
 - Allow 'Shared to Users Only' Download Links
 - Require that Shared Files Links Expire
 - Maximum Expiration Time
 - Only Allow Sharing of Single-Use Download Links

Folder Sharing

- Require that Shared Folders Expire
 - Maximum Expiration Time

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

Enable Single File Sharing - When enabled, allows the sharing of single file links and lets you control how users access them and the duration for which they are accessible.

- **Allow Public Download Links** - When enabled, anybody can access the shared file if they have the link.
- **Allow 'All Acronis Access Users' Download Links** - When enabled, only users that possess credentials for Acronis Access will be able to access the shared file.
 - **Allow Only Internal (AD) Users to Download** - When enabled, only users that possess Active Directory credentials for Acronis Access will be able to access the shared file.
- **Allow 'Shared to' Users Only Download Links** - When enabled, allows the use of links usable only be the users that they are shared to.
- **Require that Shared File Links Expire** - When enabled, forces file links to have an expiration date.
 - **Maximum Expiration Time** - Controls the maximum amount of time (in days) before the file expires.
- **Only Allow Sharing of Single-Use Download Links** - When enabled, users will be able to send only single-use links. These links will be revoked after the first download.

Folder Sharing

Require that Shared Folders Expire - When enabled, all shared folders will be required to have an expiration date.

- **Maximum Expiration Time** - Controls the maximum amount of time (in days) before the folder expires.

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).

8.3 LDAP Provisioning

Members of the groups listed here will have their user accounts automatically created at first login. This simplifies the account creation process so the administrator doesn't have to send each user an invitation.

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

LDAP Group

CN=Domain Users,CN=Users,DC=t-soft-test,DC=biz

Remove

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

Find group that begins with

Common Name / Display Name	Distinguished Name
Domain Users	CN=Domain Users,CN=Users,DC=t-soft-test,DC=biz

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.

8.4 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?	<input checked="" type="checkbox"/>
Default quota notification interval	2 — days
Ad-hoc User Quota	2 — GB
LDAP User Quota	2 — GB
Enable admin-specific quotas?	<input checked="" type="checkbox"/>
Admin Quota	15 — GB

- **Enable Quotas?** - If enabled, limits the maximum space a user has by a quota.
 - **Default notification interval** - Time interval in days that sets how often users nearing their quota limit will receive notification emails.
 - **Ad-hoc User Quota** - Sets the quota for Ad-Hoc users.
 - **LDAP User Quota** - Sets the quota for LDAP users.
 - **Enable admin-specific quotas?** - If enabled, administrators will have a separate quota applied to them.
 - **Admin Quota** - Sets the quota for administrators.

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

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

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

8.5 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.

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
- Purge previous revisions older than
- Keep at least revisions per file, regardless of age
- Only keep revisions per file

Save

Purge scans run automatically every 60 minutes. However, you may **click here** to save your settings and run a purge scan immediately.

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.*

8.6 User Expiration Policies

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

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

External user sharing invitations and password reset requests expire after days

Expire pending invitations after days

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

Delete external users who have not logged in for days

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

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

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

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

8.7 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 (p. 28) 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.

These settings determine where files uploaded for syncing and sharing will be stored. In the default configuration, the file system repository is installed on the same server as the Acronis Access Server. The Acronis Access Configuration utility is used to set the file repository address, port and file store location. The 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. For more information, consult the [documentation](#).

File Store Type	<input type="text" value="Filesystem"/>
File Store Repository Endpoint	<input type="text" value="http://127.0.0.1:5787"/>
Encryption Level	<input type="text" value="AES-256"/>
File Store Low Disk Space Warning Threshold	<input type="text" value="50"/> <input type="text" value="GB"/>

File Store Status: Free space for file store http://127.0.0.1:5787 = 79.2 GB (85064871936.0 bytes)

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

- **File Store Type** - Select the storage location you would like to use for the virtual file system's repository. The options are File System, Acronis Storage, Microsoft Azure Storage, Amazon S3, Swift S3, Ceph S3 and Other S3-Compatible Storage.

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

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

8.8 Acronis Access Client

These settings are for the Access Desktop Client.

Force Legacy Polling Mode	<input type="checkbox"/>
Minimum Client Update Interval	<input type="text" value="60"/>
Client Notification Rate Limit	<input type="text" value="250"/>
Show Client Download Link	<input checked="" type="checkbox"/>
Minimum Client Version	<input type="text" value="7.0"/>
Prevent Clients from Connecting	<input type="checkbox"/>
Allow Client Auto-update to Version	<input type="text" value="Latest"/>

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

Note: As of Acronis Access Server version 7.5, only desktop clients newer than version 6.1 can connect.

- **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.

9 Users&Devices

In this section

- Managing Mobile Devices114
- Managing Users117
- Reassign Deleted User Content120

9.1 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.

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

Users & Devices

Users | **Devices** | [Reassign Deleted User Content](#)

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

Filters

Select: None | Actions | [Send Enrollment Invitation](#) | [Export](#)

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

- **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 it's settings), will be deleted. No other apps or OS data is effected.
 - **Remove from list** – This will remove the device from the **Device** list and it will un-manage 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	115
Performing Remote Wipes.....	116

9.1.1 Performing Remote Application Password Resets

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

When a password is lost, the only options are to perform a remote application password reset or to let the user uninstall Acronis Access from their device and reinstall it. Uninstalling 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.

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 it's settings database and allow the user to set a new app password.

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

1. An end user will contact you requesting to have their Acronis Access app password reset, they will give you their **Password Reset Code**.

2. Open the **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.

Reset App Password ×

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

Password Reset Code:

Generate Confirmation

Close

9.1.2 Performing Remote Wipes

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

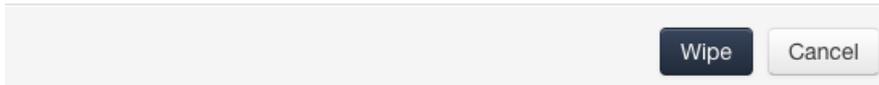
Queuing a Remote wipe

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

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

Remote Wipe ×

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



Connectivity requirements

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

9.2 Managing 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, but only if the user has Sync & Share access.

There are 3 types of Sync & Share user:

- **Free External** users can be created in several ways - via email invitation or via an invitation to a shared folder. Users will be sent a confirmation email and are required to activate their account through it. These users are not licensed by default and the administrator must convert them to licensed manually. If a user is not licensed, he can only create, edit, delete, and upload folders and files in the folders shared with him by other users. Non-licensed users cannot create or upload their own content and they cannot use the desktop client. Non-licensed users cannot **invite** or **view** other members even if they are given the rights. The user(s) must be licensed in order to use these features.
- 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. 107) 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. 121) article.
- **No Access** users are administrative users that don't have access to the Sync & Share Web Client and are not licensed by default. They can use the mobile app and Mobile Access features like regular users. These users can be either LDAP or Ad-Hoc.

Users & Devices

Users

Devices

Reassign Deleted User Content

Add Sync & Share User

Send Mobile Enrollment Invitation

Export ▾

▾ Filters

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

- **Name** – shows the name used to login to the server.
- **Email** - shows the email address of the user.
- **Sync & Share**
 - **Status** - displays the type of license used by the user.
 - **Usage** - shows the total size of the user's content.
- **Last Logged in** – time and date of last log in.
- **Actions**
 - **More Info** - Displays additional information about the user.
 - **Show Devices** - Displays information about the devices used by this user.
 - **Reset Sync & Share Password** - Sends a password resetting email.
 - **Convert to Licensed** - Converts a free user to a licensed user. This will use 1
 - **Edit User** - Allows you to edit this user.
 - **Delete** - Deletes the user.

Adding an Ad-Hoc user

1. Open the Acronis Access Web Interface.
2. Log in with an administrator account. 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. The user will receive an email to confirm their account. Once they open the link in the email, their account registration is complete.

Adding an LDAP 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 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.*

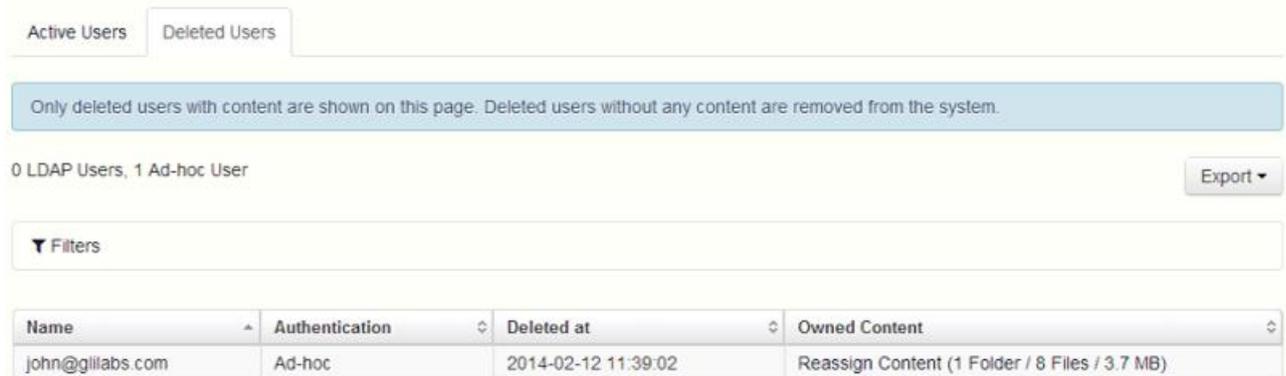
Setting a custom quota

You can set a custom quota for any user with Sync&Share access. To do so:

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

9.3 Reassign Deleted User Content

Deleted users without any content are completely removed. The content of users who had Sync&Share data (files, folders) will remain in the system and will be moved to this section. Administrators can access the list of content waiting to be reassigned or deleted. This content can be reassigned to another user, permanently deleted or left alone to be purged automatically by the system according to the purging policies in effect.



Active Users Deleted Users

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

0 LDAP Users, 1 Ad-hoc User Export ▾

Filters

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

When deleting a user, a window will ask you what to do with the user's content. This user's content can be reassigned to an existing user or deleted immediately. If you choose not to reassign or delete content now, you can reassign or delete it at a later time from the Reassign Deleted User Content page.

- **Save and reassign later** - The user's content will be left to be reassigned or purged.
- **Reassign to another user** - Immediately select another user and reassign the content to that user. That user will then have a Sync & Share folder called **Content inherited from DeletedUserName <deleteduseremail>** and he will also be the owner of all inherited content. This includes folders shared out by the deleted user.
- **Permanently delete** - Delete the account and the content.

10 Client Guides

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

- Desktop and Web client
- iOS app
- Android app
- Windows mobile app

11 Server Administration

In this section

Administering a Server.....	121
Administrators and Privileges	121
Audit Log	124
Server	128
Web UI Customization	131
Web Previews & Editing.....	133
SMTP	134
LDAP	136
Email Templates.....	138
Licensing.....	140
Debug Logging.....	141
Monitoring	143

11.1 Administering a Server

If you are an administrator logging in to the web interface, you can switch between **Administration** and **User** modes.

- To enter **Administration** mode, click on the user icon and press the **Administration Console**.
- To enter **User** mode, press the **Leave Administration** button at the top-right.



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

11.2 Administrators and Privileges

Administration page access restrictions

- **Only connections from configured IP address ranges will be allowed to access the Administration pages** - allows the administrator to allow only certain IP addresses to accessing the Administration web interface.
 - **IP addresses allowed to access the Administration pages** - the administrator enters the IP addresses that can access the **Administration** page. They can be comma-separated IPs, subnets or IP ranges.

e.g. 10.1.2.3, 10.4.*, 10.10.1.1-10.10.1.99

Note: Administrator access from localhost cannot be restricted.

Note: This feature does **not** work for servers that are using the Gateway Server to proxy requests for the Access Server.

Provisioned LDAP Administrator Groups

Provisioned LDAP Administrator Groups

Add Provisioned Group

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

LDAP Group	Full Rights	Manage Users	Manage Mobile Data Sources	Manage Mobile Policies	View Audit Log	
CN=Administrators,CN=Builtin,DC=t-soft,DC=biz	<input checked="" type="checkbox"/>	Actions				
CN=Users,CN=Builtin,DC=t-soft,DC=biz	<input checked="" type="checkbox"/>	Actions				

50 per page

Showing 1 to 2 of 2 groups

« < 1 > »

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:

Add Provisioned LDAP Administrator Group

Selected group:

Administrative Rights

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

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

Find group that begins with Search

Add Cancel

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.
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

Administrative Rights

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

- **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
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**.

11.3 Audit Log

11.3.1 Log

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

Note: *If you wish to configure a Gateway Server's logging and level of logging, please visit Gateway Server Logging (p. 88).*

▼ Filters

Filter by User:

Filter by Shared Projects:

Filter by Severity:

Filter by Gateway Server:

Filter by Device IP:

From:

To:

Search for Text:

Filter by Device Name:

- **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	Type	User	Message	Device Name
2017-05-31 08:09:59	Error		Error sending email ['Enroll user for mobile access' to 'johndoe@t-soft-test.biz']: 550 5.1.1 <johndoewhatisreallifetopwriting@mailinator.com>: Recipient address rejected: Unknown user: johndoewhatisreallifetopwriting@mailinator.com	
2017-05-31 08:06:57	Info		Free space for file store http://127.0.0.1:5787 = 80.2 GB (86096715776.0 bytes)	

< ||| >

25 per page Showing 1 to 2 of 2

<< < 1 > >>

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

If you have enabled Audit logging on a Gateway Server, you will also see the activity of your mobile clients. If you have allowed Desktop and Web clients to access mobile Data Sources, they will also be reflected in the log.

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

11.3.2 Settings

Acronis Access can automatically purge old logs and export them to files based on the policies below. It is recommended to export the log files to a folder outside the Acronis Access server directories so they will not be lost when the software is upgraded. The export file path must be a folder where the Acronis Access Tomcat Service user has read and write permissions.

Automatically purge log entries more than old

Export log entries to file as before purging

Export file path

Show timestamps in exported audit logs using:

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.

***Note:** We recommend exporting the logs to a folder that is outside of the Acronis Access installation folder so that they are not lost on upgrade. The folder you specify must have read/write access for the user account that the Acronis Access Tomcat service is running as. If you haven't changed the defaults, the account should be the Local System account.*

- **Show timestamps in exported audit logs using X** - Lets you choose if your audit logs should use the local server time or another time format (UTC).

11.4 Server

Server Name	<input type="text" value="Acronis Access"/>
Web Address	<input type="text" value="https://access.yourcompany.com"/>
Audit Log Language	<input type="text" value="English"/> ▼
Session Timeout in Minutes	<input type="text" value="15"/> —
Enable Sync and Share Support	<input checked="" type="checkbox"/>

Server Settings

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

Notifications

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

Email administrator a summary of errors?	<input checked="" type="checkbox"/>
Email Addresses	<input type="text" value="hristo@glilabs.com"/>
Notification Frequency	<input type="text" value="30"/> <input type="text" value="mins"/>

Notification Settings

- **Email administrator a summary of errors?** – If enabled, a summary of errors will be sent to specified email addresses.

- **Email Addresses** – one or more email addresses which will receive a summary of errors.
- **Notification Frequency** – frequency for sending error summaries. Sends emails only if errors are present.

In this section

An option for SMS two-factor authentication for web client login is included. You can use AD mobile phone numbers or user-provided phone numbers. Two-factor authentication can be required for every login, at a specified time interval, or only for login from new browsers.

Sending of SMS codes will require that an account is established with the Twilio SMS messaging service. For more information, please visit <https://www.twilio.com/sms>. For information on running a trial of Twilio, please visit [Twilio Free Trial](#).

Note: You only need 1 account with Twilio, and that account is used by the Acronis Access Server, you do not need accounts for every user.

Require web client SMS 2-factor authentication ▼

Require for Internal / LDAP users

Require for External users

Email mobile phone number recovery requests to

Twilio service settings for SMS messaging

In order to send 2-factor codes to users, you will need to establish a Twilio SMS messaging account and configure a messaging service that can be used by Acronis Access. [View more details](#)

Twilio Account SID

Twilio Auth Token

Twilio Messaging Service SID

Require web client SMS 2-factor authentication:

- **For initial login to new browsers** - Will require SMS authentication the first time when a new users opens the Acronis Access Server webpage. Once you enter the verification code and register your browser, you will not be prompted to enter an SMS code again unless you use a different browser or computer.

- **At a specified interval** - Will require SMS authentication at a specified time interval regardless of number of login attempts.
- **For every login** - Will require SMS authentication every time a user tries to connect.
- **Require for Internal / LDAP users:**
 - **Acronis Access account** - When selected, the users' phone numbers will be pulled from their Acronis Access accounts.
 - **Active Directory** - When selected, the users' phone numbers will be pulled from their Active Directory accounts.

Note: The phone number that is used is the **Mobile telephone** number, under the **Telephones** tab in the

Active Directory.

- **Fallback behavior:** - This option determines the default action if Active Directory is selected but the user does not have a phone number set.
 - **Use Acronis Access account** - Prompts the user to enter a phone number.
 - **Allow login without 2-factor authentication** - Allows logins without two-factor authentication.
 - **Do not allow login** - Users without phone numbers in the Active Directory will not be allowed to login.
- **Require for External users** - When enabled, external users will also be required to use SMS authentication.
- **Email mobile phone number recovery requests to** - All phone number recovery requests will be sent to this email address.

Twilio settings:

- **Twilio Account SID** - Your company's Twilio account security identifier (SID).
- **Twilio Auth Token** - Your company's Twilio authentication token.

Both of these can be found in the Twilio console at <https://www.twilio.com/console>

Console Dashboard

Account Summary

ACCOUNT SID AC4a7ac454eee8c255db64cc9d5947ff78

AUTH TOKEN 

[Account Details](#)

- **Twilio Messaging Service SID** - The SID of your Two-factor authentication messaging service. This SID is located at <https://www.twilio.com/console/sms/dashboard>. If you have multiple Twilio messaging services, use only the SID of the one you will use for two-factor authentication. When creating a Twilio messaging service, for **Use Case** leave it blank or select two-factor authentication.

Note: In the Twilio console, you will have to select the countries that are allowed to use the messaging service. Simply select the checkboxes for the desired countries.

The screenshot shows the Twilio Console interface. The main heading is 'Messaging Geographic Permissions'. Below the heading is a search bar labeled 'Filter by country name' and a red 'Filter' button. A list of countries is displayed, each with a checkbox: ASIA, Afghanistan (+93), Armenia (+374), Azerbaijan (+994), Bahrain (+973), Bangladesh (+880), Bhutan (+975), Brunei (+673), Cambodia (+855), and China (+86). The 'Armenia (+374)' checkbox is highlighted. The left sidebar contains navigation links: Home, Programmable SMS, Dashboard, Messaging Services, Short Codes, Tools, Logs, Insights, Add-ons Beta, Usage, and Settings (General, Geo Permissions).

11.5 Web UI Customization

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

Note: You can also make these customizations through the Access Advanced API, for more information check out [Web UI API customization](#).

Using custom logos

1. Open the Acronis Access web interface and login as an administrator.
2. Navigate to **General Settings** -> **Web UI Customization**.
3. Select the **Use Custom Logo** checkbox.
4. Choose the files for the logos you wish to change and make sure they are selected from the drop-down menu.

Note: The image size limits are written in brackets ().

5. Press **Save**.

Using a custom welcome message

1. Open the Acronis Access web interface and login as an administrator.
2. Navigate to **General Settings -> Web UI Customization**.
3. Select the **Display custom message on web login page** checkbox.
4. Enter the desired message in the text box and press **Save**.

Using color schemes

1. Open the Acronis Access web interface and login as an administrator.
2. Navigate to **General Settings -> Web UI Customization**.
3. Click on the **Color Scheme** drop-down and pick a scheme.
4. Press **Save**.

11.6 Web Previews & Editing

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

Web Previews & Editing

Acronis Access displays common types of documents and images within the web client interface, without requiring these files for viewing.

Enable Office Online integration

Office Online URL

Use Office Online for supported file types

Enable Microsoft services for Bing spelling, proofing and Smart Lookup

Enable built-in document previewer in web client

Only allow previews of files that do not require server-side rendering (PDF, images, text files)

Maximum cache size for recently rendered previews

Maximum concurrent generation calls

Allow connections to web preview services using self-signed certificates

Use custom URL for web preview service

Enable Office Online integration - Enables Office Online integrated functionality.

- **Office Online URL** - Enter your Office Online's WOPI discovery URL. For on-premises Acronis Access installations, you must be using an on-premises Office Online setup to be able to provide this URL. Microsoft's Office Online cloud service is limited to service provider use and is not publicly accessible without special certification and white listing.
- **Use Office Online for - Editing** allows you to edit Microsoft Office files - **DOCX, PPTX, XSLX**- while **Viewing and Editing** allows you to edit the mentioned files while also being able to preview **DOC, XLS** and **PPT** files as well.
- **Enable Microsoft services for Bing spelling, proofing and Smart Lookup** - Uses Microsoft's Bing services for spell-check capabilities.

Enable built-in document previewer in web client - Enables web previewing.

- **Only allow previews of files that do not require server-side rendering (PDF, images, text files)** - Decreases the load caused by web previews by only previewing files that do not require additional rendering. These files are PDFs, Images and simple text files.

- **Maximum cache size for recently rendered previews** - Sets the maximum size of the cache that is stored when you preview a file. This greatly increases the speed at which files open for preview if they have been recently opened.
- **Maximum concurrent generation calls** - Sets the maximum number of concurrent preview generation requests.
- **Allow connections to web preview services using self-signed certificates** - Allows you to contact web preview services that are using self-signed certificates. These are other Acronis Access Tomcat services.
- **Use custom URL for web preview service** - Enable if you have multiple Acronis Access servers and you wish to specify which one should handle the web previewing.

11.7 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.

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

SMTP Server Address

SMTP Server Port

Use secure connection?

From Name

From Email Address

Use SMTP authentication?

- **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

11.8 LDAP

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

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication
 Require exact match

LDAP information caching interval

Proactively Resolve LDAP Email Addresses

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

Include nested distribution group membership

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

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

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

11.9 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 Liquid. Please review the default templates to determine how best to customize your 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 **Liquid**. Please review the default templates to determine how best to customize your templates.

Select Language:

Select Email Template:

Available Parameters

invitation.email - User's email address

invitation.pin - User's PIN

invitation.display_name - User's display name

management_server_address - Acronis Access server address

expiration - PIN expiration date

url - Acronis Access URL

url_scheme - URL scheme to use for links (mobilecho://)

invitation.user - Username (User principal name)

app_name - App name ("Acronis Access" or "Acronis Access for Blackberry Dyna

is_good - True if application is for Blackberry Dynamics

send_ios_instructions - True if invitation should contain iOS instructions

send_android_instructions - True if invitation should contain Android instruction

send_windows_instructions - True if invitation should contain Windows instruct

has_web_access_to_shares - True if invited user has web access to network sh

email_templates_left_logo - URL to the image used for the left logo in the email templates

email_templates_right_logo - URL to the image used for the right logo in the email templates

locale - Locale code for this template

product_name - Product name (always displays as 'Acronis Access')

■ Use configured Server Name 'Acronis Access' as product name

Email Subject

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

Note: As of Acronis Access version 7.3, Liquid is the default template markup. If you have custom templates written in ERB, then ERB will be the default template markup for your server even if you upgrade.

Note: If you are using custom images in the email templates, these images should be hosted and must be somewhere accessible on the internet.

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

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

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

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

***Note:** Custom templates are **not** automatically updated when you update Acronis Access. If you want to use these updates introduced by Acronis, you must manually implement them in your custom templates. You will have to do this for all languages that you support and use.*

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

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

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

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

Different events have different available parameters.

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

11.10 Licensing

You will see a list of all your licenses.

- **License** - Type of the license (Trial, subscription etc).
- **Sync & Share Licensed Client Usage**- Currently used Sync & Share LDAP user licenses.
- **Sync & Share Free Client Usage** - Currently used Sync & Share free external user licenses.
- **Mobile Access Client Usage** - Currently used Mobile Client licenses.

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.

Note: Only Acronis Access Advanced licenses will be accepted. Acronis Access licenses will not work.

Adding a new license for a Gateway Server

Starting from 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

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

Legacy mobilEcho Licenses

Name	Address	License Type	Clients	Expiration Date	
Server	192.168.1.82	Enterprise	111	2014-08-24	Add License

25 per page Showing 1 to 1 of 1 entries

« < 1 > »

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**.

11.11 Debug Logging

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

Note: For information on enabling/disabling debug logging for a specific Gateway Server visit the *Editing Gateway Servers (p. 87)* article.

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

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

General Debug Logging Level

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

Available Debug Modules		Enabled Debug Modules
<ul style="list-style-type: none">active_recordauthenticationclustercometdatabase_connectionsemailencryptionexpiration	<div style="text-align: center;"><input type="button" value="Add +"/> <input type="button" value="Remove"/> <input type="button" value="Remove All"/></div>	

As of version 7.0 of the Acronis Access Server, the **exceptions** module has been removed from the list of available modules and is enabled at all times by default. Users that have upgraded from a previous version of Acronis Access may still see the **exceptions** module in the list. Once you make a change to the logging options and press **Save**, it will disappear.

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

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

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

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

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

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

11.12 Monitoring

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

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

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

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

Installing New Relic

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

1. Open <http://newrelic.com/> and create a New Relic account or log in with an existing account. Once that is done, proceed with your Application configuration.
2. For Application Type select **APM**.
3. For platform, select **Ruby**.
4. Download the New Relic script shown in Step 3 of the New Relic Starting Guide (newrelic.yml).
5. Open your Acronis Access web console.
6. Navigate to **Settings** -> **Monitoring**.
7. Enter the path to the newrelic.yml including the extension (e.g **C:\software\newrelic.yml**). We recommend you put this file in a folder outside of the Acronis Access folder so that it will not be removed or altered on upgrade or uninstall.
8. Click **Save** and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
9. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
10. You should be able to monitor you Acronis Access server via the New Relic website.

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

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

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

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

If you want to monitor the actual computer as well

1. Open <http://newrelic.com/> and log in with your account.
2. Press Servers and download the New Relic installer for your operating system.

3. Install the New Relic monitor on your server.
4. The New Relic server monitor requires Microsoft .NET Framework 4. The link the New Relic installer takes you to is only for the Microsoft .NET Framework 4 Client Profile. You will need to go to the Microsoft Download Center and download the entire .NET 4 Framework from the internet and install it before running the New Relic Server Monitor installer.
 - Wait until New Relic detects your server.

12 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. 145)* article.

In this section

Disaster Recovery guidelines	145
Best Practices	147
Backing up and Restoring Acronis Access	148
Tomcat Log Management on Windows	151
Automated Database Backup	153
Automated Database Vacuum	155
Increasing the Acronis Access Tomcat Java Maximum Memory Pool ...	158
Migrating Acronis Access to another server	159
Upgrading PostgreSQL to a newer Major version.....	163

12.1 Disaster Recovery guidelines

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

Introduction:

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

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

Description of the Acronis Access elements:

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

Acronis Access Gateway Server

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

Acronis Access Server

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

Acronis Access Configuration Utility

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

File Store

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

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

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

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

Resources needed to implement a fast recovery process

The resources needed to fulfill the disaster recovery process are:

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

The process

Backup Setup

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

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

Recovery

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

1. Boot up the recovery node. Adjust any network configuration like IP Address, Host Name if needed. Test Active Directory connectivity and SMTP access,
2. If needed restore the most recent Acronis Access software suite backup.
3. Verify that Tomcat is not running (Windows Control Panel/Services).
4. If needed, restore the FileStore. Make sure the relative location of the FileStore is the same as it was in the source computer. If this is not the case, the location will need to be adjusted by using the Configuration Utility.
5. Verify that the PostgreSQL service is running (Windows Control Panel/Services).
6. Restore the Acronis Access database.
7. Start the Acronis Access Tomcat service.
8. Migrate DNS to point to the new node.
9. Verify Active Directory and SMTP are working

12.2 Best Practices

1. Backup your database regularly

Keeping your database backed-up is one of the most important aspects of managing Acronis Access. The Backup process (p. 148) can be entirely automated (p. 153) to help you keep your backups up to date.

Deployments with very large Acronis Access server databases may want to use a different backup and restore method than the one provided.

Deployments with databases of several gigabytes and more may require some additional configurations during the **Backup&Restore** process to speed it up or otherwise improve it. For assistance with your specific configuration, please contact our technical support at <http://www.acronis.com/en-us/mobilitysupport/> for help and instructions.

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

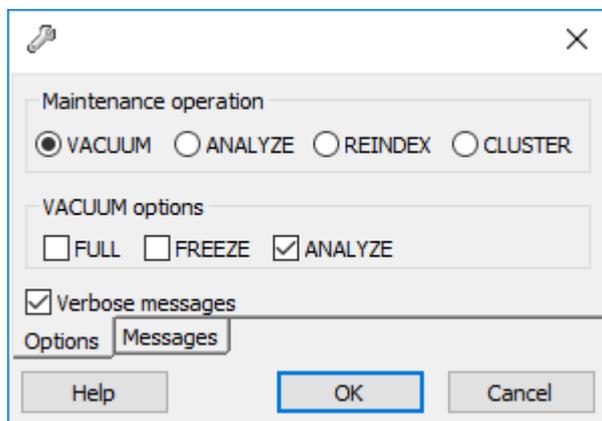
PostgreSQL databases require periodic maintenance known as **vacuuming**. The **VACUUM** command has to process each table on a regular basis to:

- Recover or reuse disk space occupied by deleted or updated rows.
- Protect against loss of very old data.
- Update data statistics and speed up index scanning.

The **ANALYZE** command collects statistics about the contents of tables in the database, and stores the results. Subsequently, the query planner uses these statistics to help determine the most efficient execution plans for queries.

To manually vacuum and analyze your database(s), do the following:

1. Open the Acronis Access PostgreSQL Administrator tool (can also be called PgAdmin) and double-click on **localhost** to connect to your server.
2. Right-click on the **acronisaccess_production** database and choose **Maintenance**.
3. Select the **VACUUM** radio button and the **ANALYZE** checkbox.



Warning! If your database is very large, the vacuum can take some time. This process should be run during periods of low load on the server.

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

To setup automatic vacuuming, please read our article at: **Automated Database Vacuuming (p. 155)**

3. For big deployments, you should consider running a load-balanced setup (p. 184) or clustering Gateway servers (p. 94).

12.3 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. For load-balanced configurations the process is almost entirely identical as a regular backup and restore. Any specifics will be added to the relevant steps.

Note: If your Acronis Access server database is very large, several gigabytes, you may want to use a different backup and restore method for your database. Please contact our technical support at <http://www.acronis.com/en-us/mobilitysupport/> for help and instructions.

We strongly recommend you perform a test backup/restore in a test environment before proceeding with backing up/restoring your production environment.

In this section

- 7.
1. Stop the Acronis Access Tomcat service.

Note: If you are load-balancing multiple Acronis Access Tomcat services, stop all of them.

2. Open the Acronis Access PostgreSQL Administrator application and connect to the database server. You may be prompted to enter the password for your **postgres** user.
3. Expand **Databases** and right-click on the **acronisaccess_production** database.
4. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
5. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.
6. Close the PostgreSQL Administrator and open an elevated command prompt.
7. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`
8. Enter the following command: `pg_dumpall --host localhost --port 5432 --username postgres --inserts --file alldbs_inserts.sql`
 - **alldbs_inserts.sql** will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: `--file D:\Backups\alldbs_inserts.sql`
 - If you are using a non-default port, change **5432** to the correct port number.
 - If you are not using the default PSQL administrative account **postgres**, please change **postgres** to the name of your administrative account in the command above.
 - You will be prompted to enter the **postgres** user's password several times for this process. For each prompt, enter the password and hit Enter.

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

9. Copy the backup file to a safe location.
 1. Stop the Acronis Access Gateway service.
 2. Go to the Gateway Server database folder, by default located at:
C:\Program Files (x86)\Acronis\Access\Gateway Server\database
 3. Copy the **mobileEcho.sqlite3** file to a safe location.
 4. If you have multiple Gateway Servers, repeat this process for each one and make sure the database files don't get mixed up.

If you've made changes to any of these files, it is recommended to make backups so you can transfer your settings when restoring or migrating your Acronis Access product.

- **web.xml** located by default at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**. Contains Single Sign-On settings.
 - **server.xml** located by default at **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.75\conf**. Contains Tomcat settings.
 - **krb5.conf** located by default at **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**. Contains Single Sign-On settings.
 - Your certificates and keys used for Acronis Access.
 - Custom color schemes located by default at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\customizations**.
 - **pg_hba.conf** located by default at **C:\Program Files\PostgreSQL\9.2\data**.
 - **newrelic.yml** file if you are using **New Relic** to monitor your Acronis Access server.
1. Open the **Services** control panel and stop the Acronis Access Tomcat service.

Note: For load-balanced configurations, stop all Acronis Access Tomcat services.

2. Open the Acronis Access PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called **acronisaccess_production**.
3. Right-click on the database and select **Refresh**.
4. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
 - If there are any tables in the database, right click on the database and rename it to **oldacronisaccess_production**. Finally, go to **Databases**, right-click and create a new database called **acronisaccess_production**.
5. Close the PostgreSQL Administrator and open an elevated command prompt.
6. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"
7. Copy the database backup file **alldbs_inserts.sql** (or whatever you have named it) into the **bin** directory.
8. In the command prompt, enter the following command: **psql -U postgres -f alldbs_inserts.sql**
9. Enter your **postgres** password when prompted for it.

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

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

10. Open the Acronis Access PostgreSQL Administrator application again and connect to the local database server.
11. Select **Databases**.
12. Expand the **acronisaccess_production** database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was in step 5 of the "Backup the Access Server's database" section.

Note: If the Acronis Access Server version you restore the database to is newer than the version from your database backup, and the Acronis Access Tomcat service has already been started, the number of tables in the new Acronis Access Server database could be larger than the number of tables you had when you did the backup.

1. Stop the Acronis Access Gateway service.
2. Copy the **mobliEcho.sqlite3** Gateway Server database backup into the new Gateway Server's database folder (by default **C:\Program Files (x86)\Acronis\Access\Gateway Server\database**) replacing the existing file.
3. Repeat this process for all Gateway Servers.

Make sure to copy any customizations made to Acronis Access' configuration files (web.xml, server.xml, krb5.conf, certificates, custom color schemes, email templates, pg_hba.conf or newrelic.yml), and move them to the new files.

After you have successfully performed a backup/restore or a migration to another machine, it's time to bring Acronis Access back online and to verify that all settings are correct.

Bringing regular deployments online

1. Start the Acronis Access Configuration Utility and make sure all settings found there are correct.
2. Press OK to start all services.

3. This should bring all services online simultaneously and restore all Acronis Access functionality.
4. If any of the components are on a separate machine, make sure to go to that machine and start them as well. In this case, the PostgreSQL service must be running in order for the Acronis Access Tomcat service to start without errors.

Bringing load-balanced deployments online

1. Pick one of your Acronis Access Servers to act as a Primary. It will be the Primary only in the sense that it will be brought online first.
2. If the PostgreSQL service is on another machine, make sure to start it first as it will affect the Acronis Access Server.
3. Go to the machine for the Primary Acronis Access Server and start the Acronis Access Configuration Utility.
4. Make sure all settings found there are correct. If there are no issues, press OK to start all services.
5. Open the Acronis Access web console and login as an administrator. Verify that all settings are correct.
6. Once you have verified your settings, proceed to go over each machine that has a Acronis Access component and starting it via the Configuration Utility.

12.4 Tomcat Log Management on Windows

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

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

Introduction:

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

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

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

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

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

A sample process:

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

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

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

```
ECHO OFF

REM Script: aETomcatLogsPurge.bat
REM 2012-05-12: Version: 1.0: MEA: Created

ECHO This script will delete files older than a number of days from a directory
ECHO Run it from the command line or from a scheduler

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

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

REM NumDays - Log files older than NumDays will be processed
set NumDays=14

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

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

REM ForFiles options:

REM     "/p": the path where you want to delete files.
REM     "/s": recursively look inside other subfolders present in the folder
mentioned in the batch file path
REM     "/d": days for deleting the files older than the present date. For instance
"/d -7" means older than 7 days
REM     "/c": command to execute to actually delete files: "cmd /c del @file".

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

:End

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

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

Steps:

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

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.
6. Define at what time the task should start. It is recommended to run this process when the system is not under extreme load or other maintenance processes are running.
7. Set the action type to "Start a program".
8. Click the Browse button, locate and select the script (batch) file.
9. When done, click Finish.
10. In the tasks list you may want to right click on the task, select properties and verify the task will run whether a user is logged on or not, for unattended operation.
11. You can verify the task is properly configured and running properly by selecting the task, right clicking on it and selecting "Run". The scheduler's log should report start, stop and any errors.

12.5 Automated Database Backup

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

Creating the database backup script

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

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

```

set datestr=%month%_%day%_%year%
echo datestr is %datestr%

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

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

```

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

Creating the scheduled task

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

On the General tab:

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

On the Triggers tab:

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

On the Actions tab:

1. Click **New**.
2. Select **Start a program** for **Action**.
3. For **Program/Script** press **Browse**, navigate to and select the **DatabaseBackup.bat** file.

4. For **Start in (optional)**, enter the path to the folder in which the script resides. e.g. If the path to the script is **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.3\PSQL.bat** enter **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.3**
5. Press **OK**.

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

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

12.6 Automated Database Vacuum

This guide will help you create a scheduled task that will run and vacuum the PostgreSQL database. Vacuuming is an important process especially if your deployment has a big database (several gigabytes).

Note: PostgreSQL is set to auto-vacuum in its configuration file. For deployments under high load it is possible that the auto vacuum will never run, as it is designed to not run when the server is under high load. For these cases, it is best to set up a scheduled task to run the Vacuum at least once a month.

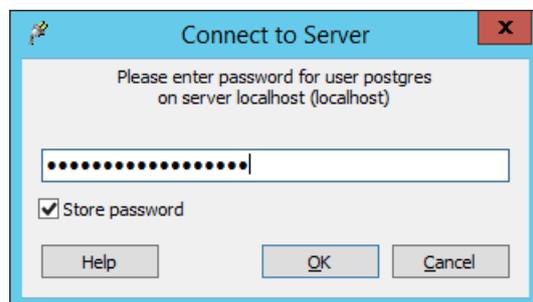
Configuring PostgreSQL and creating the script

Making sure the task will be able to run

You must make sure that you have the postgres user's password is saved into the pgpass file or the script won't be able to run. The easiest way to do this is from the Access PostgreSQL Administrator tool:

1. Open the Access PostgreSQL Administrator tool.
2. Connect to the database and on the dialog that opens to enter the password, enable the **Store Password** checkbox and click **OK**. This will save the postgres user's password to the pgpass file. This file will be created in **C:\Users\\AppData\Roaming\postgresql**.

Note: You may see a dialog with information on Saving passwords, this is expected. Press OK.



- Alternatively, you can manually create a file called **pgpass.conf** and enter the following text into the file and save it. Be sure to enter your **actual** postgres user password.
localhost:5432:*:postgres:yourpassword
3. For our example, we will copy the **pgpass.conf** file and place the copy in the **D:\Backup** folder. The user running the scheduled task, must have read access to the file.

Creating the script

In the example below, the PostgreSQL **bin** directory path is set to **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\bin**. You will need to edit the path to point to your PostgreSQL **bin** folder if you are using an older or a custom installation.

1. Create a folder where the log files will be stored and give the user running the task read, write and execute permissions to the folder. We recommend you use the machine's administrator as the user. In our example the log folder is **D:\Backup**.
2. Open the text editor of your choice (e.g. Notepad) and paste the following example script:

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

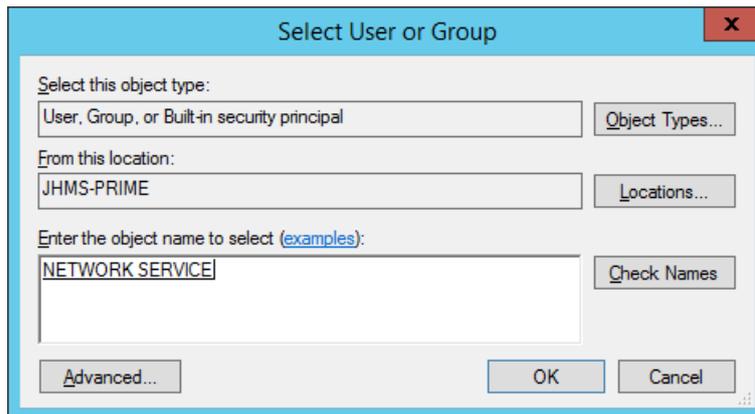
3. Edit this script to match your deployment.
 - Change the path to the **psql.exe** file with your path to the file.
 - Change the **--port** setting to the correct port number if you have changed the default.
 - If you are using a different PostgreSQL user, change **--username=** by replacing **postgres** with your desired user.
 - Change the **D:\Backup** part of the path for the logs to your desired log folder.
 - Change the **D:\Backup** part of the path for the pgpass.conf file to your path to the file.
4. Save the file as **vacuum.bat**. Make sure that you have selected **All types** under **Save as file type**.

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

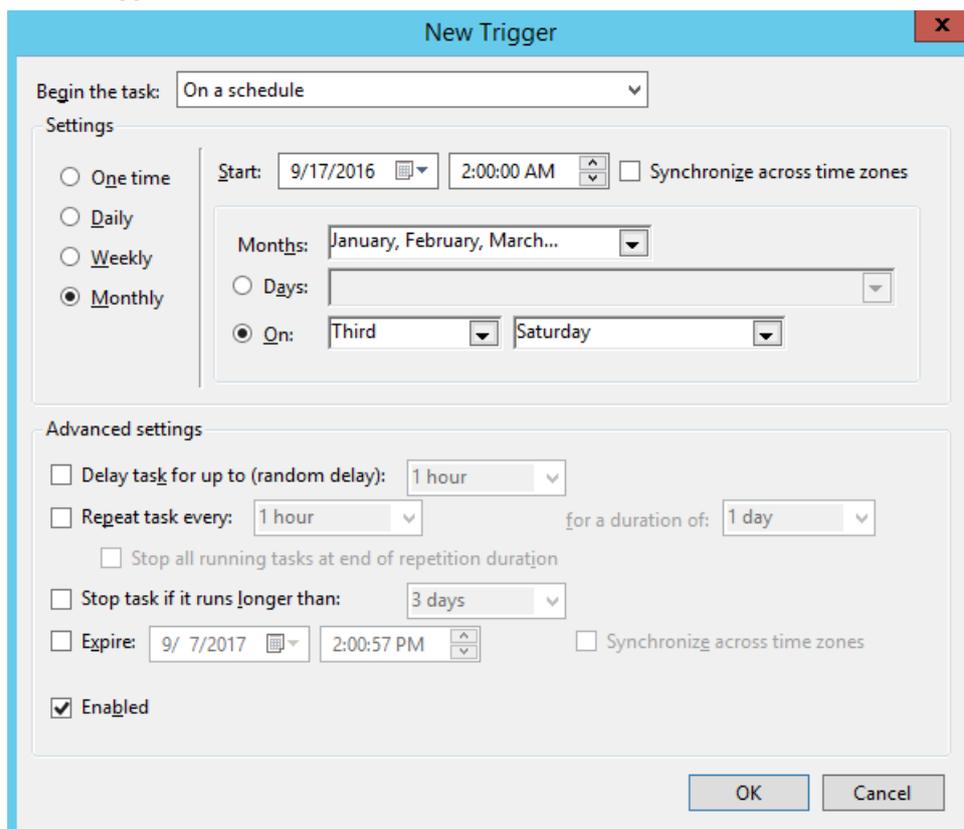
Configuring the Task Scheduler

1. Open the **Task Scheduler** from **Control Panel -> Administrative Tools -> Task Scheduler**.
2. Right-click on **Task Scheduler (local)** and select **Create Task**.
3. In the **General** tab:
 - Set the **Name** and **Description**.
 - Choose **Run whether user is logged on or not**.

- Set the **User account** as the user that will run this task. We recommend using the machine NETWORK SERVICE account.

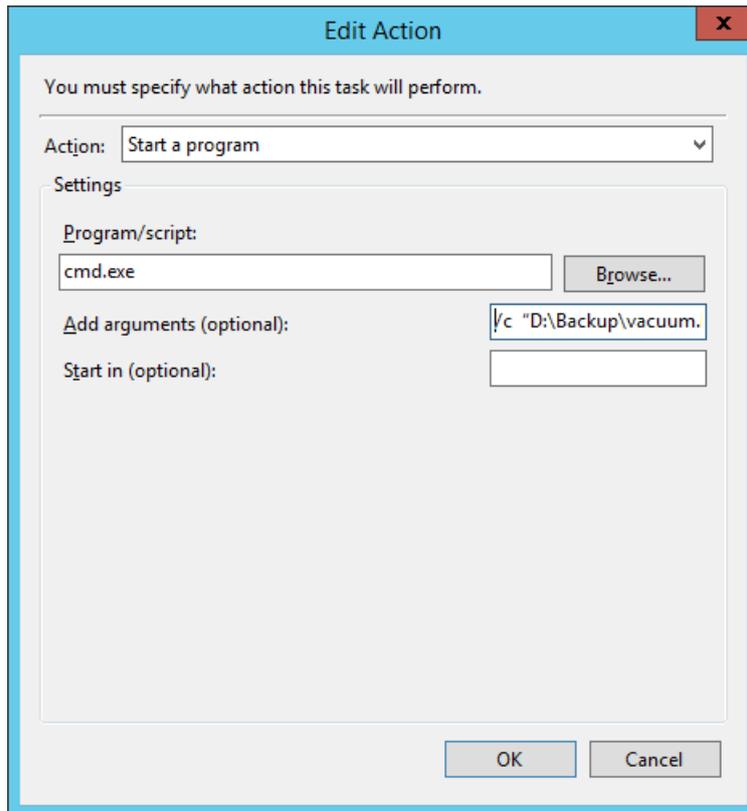


4. In the **Triggers** tab:



- Click **New** and set the schedule you want the vacuum to run on. This should be a time of low load on the server. We recommend running the vacuum at least once a month.

5. In the **Action** tab:



- Click **New** and for the **Action** select **Start a program**.
- For the **Program/script** enter `cmd.exe`
- In the **Add arguments** enter: `/c "C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\bin\vacuum.bat"`

Note: Make sure to edit the path in this command to reflect the path to your Postgres *bin* folder if you have a custom or older installation.

6. Leave all the defaults for the **Conditions** and **Settings** tabs.
7. Click **OK** to save the new task. It will prompt you to enter an administrator password.

Verify that the task works as expected

1. From the Task Scheduler, run the vacuum task manually to test it out and make sure it is writing the log file into the proper folder.
2. Check that the scheduled task runs at the time it is set for.

12.7 Increasing the Acronis Access Tomcat Java Maximum Memory Pool

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

To increase the maximum memory pool:

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

2. Click on the **Acronis Access Tomcat Configuration** tool shortcut.
3. Open the **Java** tab.
4. Change the **Maximum memory pool** to the desired size and press **OK**.
5. Restart the Acronis Access Tomcat service.

12.8 Migrating Acronis Access to another server

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

Before migrating the production server, we strongly recommend that these steps be performed in a test environment. The test deployment should have the same architecture as the production servers, along with a couple of test user desktop and mobile clients to ensure compatibility in the production environment.

In this section

Before you begin	159
Migrating the Access Server and Gateway databases	160
Testing your new configuration	163
Cleanup of the original server	163

12.8.1 Before you begin

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

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

- Are the Access Server, Postgres and the Gateway and File Repository all on one machine?
- Note the DNS, the IP and port of the Access server.
- Note the DNS, the IP and port of the Gateway server.
- Note the Address and Port of the File Repository.
- Note the location of the File Store.
- Note the PostgreSQL version number of your current server.

The easiest way to do this is to look at the folder name inside the main PostgreSQL folder (by default. C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL), the inside folder's name is the PostgreSQL major version number (e.g. **9.2**; **9.3**; **9.4**).

Much of this information can be found in the Configuration Utility.

Basic outline of the migration process:

Make sure that you are prepared to do all of these steps before you begin the migration.

1. Change the DNS entries to point to the new server machine.
2. Backup your current database files and certificates.
3. Move the database files and certificates to the new machine.
4. Migrate the File Store.
5. Install Acronis Access Advanced Server on the new machine.

6. Move certificates to the new machine.
7. Put database files into new Access Server installation.
8. Use Configuration Utility to start up new Access Server.
9. Confirm Gateway address is correct.
10. Test your new configuration.

12.8.2 Migrating the Access Server and Gateway databases

On the original server, where Tomcat/Gateway/PostgreSQL are running now:

Note: If your Acronis Access server database is very large, several gigabytes, you may want to use a different backup and restore method for your database. Please contact our technical support at <http://www.acronis.com/en-us/mobilitysupport/> for help and instructions.

1. Stop the Acronis Access Tomcat service
2. Open the Acronis Access PostgreSQL Administrator application and connect to the database server. You may be prompted to enter the password for your **postgres** user.
3. Expand **Databases** and right-click on the **acronisaccess_production** database.
4. Choose **Maintenance** and select the **Vacuum** radio button and the **ANALYZE** checkbox. Press **OK**.
5. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This can help you verify that the database restore is successful after a recovery.
6. Close the PostgreSQL Administrator and open an elevated command prompt.
7. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"
8. Enter the following command: **pg_dumpall --host localhost --port 5432 --username postgres --inserts --file alldbs_inserts.sql**
 - **alldbs_inserts.sql** will be the filename of the backup. It will be saved in the PostgreSQL bin directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: **--file D:\Backups\alldbs_inserts.sql**
 - If you are using a non-default port, change **5432** to the correct port number.
 - If you are not using the default PSQL administrative account **postgres**, please change **postgres** to the name of your administrative account in the command above.
 - You will be prompted to enter the **postgres** user's password several times for this process. For each prompt, enter the password and hit Enter.
 - **Note:** Typing the password will not result in any visual changes in the Command Prompt window.
9. Copy the backup file to the new machine that will host the Access Server.
10. Copy the certificates you use for the Access Server to the new machine.
11. If you plan to migrate the File Store, copy over those files. For a large File Store this could take some time. For more information, read *Moving the FileStore to a different location* (p. 238).

Backup the Gateway Server's database

1. Stop the **Acronis Access Gateway** service.
2. Go to the Gateway Server database folder, by default located at:
C:\Program Files (x86)\Acronis\Access\Gateway Server\database

3. Copy the **mobilecho.sqlite3** file to the new machine that will host the Gateway Server.

If you've made changes to any of these files, it is recommended to make backups so you can transfer your settings when restoring or migrating your Acronis Access product.

- **web.xml** located by default at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**. Contains Single Sign-On settings.
- **server.xml** located by default at **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.75\conf**. Contains Tomcat settings.
- **krb5.conf** located by default at **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**. Contains Single Sign-On settings.
- Your certificates and keys used for Acronis Access.
- Custom color schemes located by default at **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\customizations**.
- **pg_hba.conf** located by default at **C:\Program Files\PostgreSQL\9.2\data**.
- **newrelic.yml** file if you are using **New Relic** to monitor your Acronis Access server.

On the new server that will be hosting the Acronis Access Server, perform the following steps:

Install Acronis Access

1. Start the Acronis Access Advanced installer and press **Next**. Read and accept the license agreement.
2. Choose **Install** and follow the installer screens.

***Note:** If the Access Server, PostgreSQL, Gateway are going on separate machines, choose **Custom** and select the desired component(s).*

3. On the PostgreSQL Configuration screen enter the same password for the PostgreSQL Super-User that was used on the original server. Press **Next**.
4. Review the components being installed and press **Install**.
5. Once the installer is done, press **Exit** and dialog will come up telling you the Configuration Utility will run next.
6. When the Configuration Utility comes up, leave it open without pressing **OK** or **Apply**.

1. Open the **Services** control panel and stop the Acronis Access Tomcat service.

***Note:** For load-balanced configurations, stop all Acronis Access Tomcat services.*

2. Open the Acronis Access PostgreSQL Administrator application, connect to the local database server, select **Databases**, and confirm there is a database called **acronisaccess_production**.
3. Right-click on the database and select **Refresh**.
4. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
 - If there are any tables in the database, right click on the database and rename it to **oldacronisaccess_production**. Finally, go to **Databases**, right-click and create a new database called **acronisaccess_production**.

5. Close the PostgreSQL Administrator and open an elevated command prompt.
6. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"
7. Copy the database backup file **alldbs_inserts.sql** (or whatever you have named it) into the **bin** directory.
8. In the command prompt, enter the following command: **psql -U postgres -f alldbs_inserts.sql**
9. Enter your **postgres** password when prompted for it.

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

10. After the restore is complete, close the command prompt window.
11. Open the **Acronis Access PostgreSQL Administrator** application again and connect to the local database server.
12. Select **Databases**.
13. Expand the **acronisaccess_production** database, expand **Schemas** and expand **Public**. Verify that the number of **Tables** is the same as it was in step 5 of the "**Backup the Access Server's database**" section.

***Note:** If the Access Server version you restore the database to is newer than the Access Server version from your database backup, and the Acronis Access Tomcat service has already been started, the number of tables in the new Access Server database could be larger than the number of tables you had when you did the backup.*

Restore the Gateway Server database

1. Copy the **moblIEcho.sqlite3** Gateway Server database that came from the old server into the new Gateway Server's database folder (by default **C:\Program Files (x86)\Acronis\Access\Gateway Server\database**) replacing the existing file.

Configure your new server

***Note:** It is highly recommended that you do not change the DNS names used by Acronis Access, only the IP addresses they are pointing to. The following instructions assume you are re-using the DNS names of the previous instance of Acronis Access.*

1. Go back to the Acronis Access Configuration Utility that you left open and set the settings for the Gateway Server, Access Server and File Repository.
2. Click **Apply**, and then **OK**. At the next dialog click **OK** and a browser will launch with the Acronis Access web interface.
3. Log into the Access server.
4. Click on **Administration**. Navigate to the **Mobile Access -> Gateway Servers** page.
5. In the list of Gateway Servers you should see your Gateway server listed.
6. If the address for your gateway server is a DNS entry you should not need to make any changes to the server as long as the DNS entry is now pointing to your new server machine. If the address for your gateway is an IP address, then you will need to edit the gateway server.

Verify Acronis Access administrative settings

Once you have successfully finished your database's restoration, we highly recommend that you login to the web interface and verify that your settings have carried over and that they are still relevant before proceeding with anything else. Here are some examples of important items to check:

- Audit Logging - Make sure that the new Acronis Access logs folder has all the necessary permissions so that logs can be written.
- New Relic - If you are using New Relic, copy the **newrelic.yml** file from the old machine to this one and make sure that the path in the Acronis Access web interface points to the file.
- Administration settings - Make sure all your LDAP, SMTP and general administrative settings are correct.
- Gateway Servers and Data Sources - Make sure all your Gateway Servers are still reachable on the correct addresses and check if all your Data Sources have valid paths.

12.8.3 Testing your new configuration

After you have the new server set up, make sure that everything is working by doing a couple of simple actions:

- Navigate the web interface and check if everything is working as expected. Check if your settings are there and haven't been modified.
- Upload a file through the web interface to the Sync and Share section and do the same for any Network nodes you have set up (if any).
- Connect to the new server with a desktop client and a mobile client applications.
- Upload and download some files through the desktop and/or mobile clients.

12.8.4 Cleanup of the original server

Once you have verified that your new server is running correctly and you do not intend to use the old server again, we recommend you uninstall Acronis Access from the old machine.

Open the Acronis Access installer, accept the license agreement and click Uninstall. Select all components and press uninstall. This will remove all Acronis Access components from your machine.

Note: *If you don't have an Acronis Access installer, open the control panel, uninstall the Acronis Access PostgreSQL Server, Acronis Access Gateway Server, and the Acronis Access File Repository Server, Acronis Access Server, Acronis Access Configuration Collection Tool, the Acronis Access Configuration Utility and LibreOffice.*

- The PostgreSQL server will not automatically remove its **Data** directory. Manually remove the entire PostgreSQL directory found here by default: C:\Program Files\Acronis\Access\Common\PostgreSQL\
- You may also want to remove the Java that was installed for the Access Server. Java can also be removed from the control panel.

12.9 Upgrading PostgreSQL to a newer Major version

Major PostgreSQL releases often add new features that change some of the internal workings of PostgreSQL. There are two main ways to upgrade your PSQL instance - by dumping your entire

database and then re-inserting it in the new instance (**pg_dumpall**) or with the new **pg_upgrade** command. Both methods have their benefits and their drawbacks.

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

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

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

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

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

- Are the Access Server and PostgreSQL server on the same machine?
- What port is PostgreSQL running on?
- What is the locale of your current PostgreSQL installation? You can check this by opening the PostgreSQL Administration tool and clicking on the `acronisaccess_production` database. On the right, under Properties, you will see the **Encoding** and **Character type**.

Warning: Make sure that your new PostgreSQL installation has the same **Encoding** and **Character type**, otherwise you will not be able to upgrade successfully.

- What is the IP and/or DNS name of the machine running PostgreSQL?
- What is the PostgreSQL version number of your current server. The easiest way to find this is to look at the folder name inside the main PostgreSQL folder (by default. `C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL`), the inside folder's name is the PostgreSQL major version number (e.g. 9.2; 9.3; 9.4).
- Make sure that all necessary permissions in the file system(s) are configured.
- Make sure that access between the two instances is allowed via the **pg_hba.conf**. This is very important if your new PostgreSQL instance is not on the same machine.

Dumping the database from the old instance

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

1. Stop the Acronis Access Tomcat service
2. Make sure that the Old instance of PostgreSQL is running and that the New instance is stopped.
3. Open the Acronis Access PostgreSQL Administrator application and connect to the database server. You may be prompted to enter the password for your **postgres** user.
4. Expand **Databases** and right-click on the **acronisaccess_production** database.
5. Choose **Maintenance** -> **Vacuum** and press **OK**.
6. Expand the database, expand **Schemas** and expand **Public**. Take note of the number of the **Tables** section. This will help you verify that the database transfer is successful.
7. Close the PostgreSQL Administrator and open an elevated command prompt.
8. In the command prompt, navigate to the PostgreSQL bin directory.
e.g. `cd "C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.3\bin"`

9. Enter the following command: **pg_dumpall --host localhost --port 5432 --username postgres --inserts --file alldbs_inserts.sql**
 - **alldbs_inserts.sql** will be the filename of the backup. It will be saved in the PostgreSQL **bin** directory. You can use a path in the above command if you wish to save it somewhere else - e.g. change the last part of the command above like so: **--file D:\Backups\alldbs_inserts.sql**
 - If you are using a non-default port, change **5432** to the correct port number.
 - If you are not using the default PSQL administrative account **postgres**, please change **postgres** to the name of your administrative account in the command above.
 - You will be prompted to enter the **postgres** user's password several times for this process. For each prompt, enter the password and hit **Enter**.

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

10. Once you verify that the dump process is finished, stop the Old PostgreSQL instance and start the New one.

Inserting the database in the new instance

1. Make sure that the New instance of PostgreSQL is running and that the Old instance is stopped.
2. Open the Acronis Access PostgreSQL Administrator application, connect to the local database server, select **Databases**, and check if there is a database called **acronisaccess_production**. If there isn't one, you will have to create it.
3. Right-click on the database and select **Refresh**.
4. Expand it and expand **Schemas**, expand **Public** and verify that there are zero (0) **Tables**.
5. If there are any tables in the database, right click on the database and rename it to **oldacronisaccess_production**. Finally, go to **Databases**, right-click and create a new database called **acronisaccess_production**.
6. Close the PostgreSQL Administrator and open an elevated command prompt.
7. Copy the database backup file **alldbs_inserts.sql** (or whatever you have named it) into the bin directory of the new instance.
8. In the command prompt, navigate to the PostgreSQL **bin** directory.
e.g. **cd "C:\Program Files\Acronis\Access\Common\PostgreSQL\9.3\bin"**
9. Enter the following command: **psql -U postgres -f alldbs_inserts.sql**
10. Enter your **postgres** password when prompted for it.

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

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

Verify that the new instance has the correct database

1. Open the Acronis Access PostgreSQL Administrator application and connect to the New database server. You may be prompted to enter the password for your **postgres** user.
2. Expand **Databases** and right-click on the **acronisaccess_production** database.
3. Expand the database, expand **Schemas** and expand **Public**.
4. Verify that the **Tables** section contains the same number of tables as the one you saw before.

The upgrading process

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

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

7. Open an elevated command prompt and navigate to the New PostgreSQL **bin** directory with the **cd** command.

e.g. **cd C:\Program Files(x86)\Acronis\Access\Common\PostgreSQL\9.5\bin**

8. Use the **pg_upgrade** command with the following parameters:

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

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

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

Verify that the new instance has the correct database

1. Open the Acronis Access PostgreSQL Administrator application and connect to the New database server. You may be prompted to enter the password for your **postgres** user.
2. Expand **Databases** and right-click on the **acronisaccess_production** database.
3. Choose **Maintenance -> Vacuum** and press **OK**.
4. Right-click on the **acronisaccess_production** database again.
5. Choose **Maintenance -> Reindex** and press **OK**.
6. Expand the database, expand **Schemas** and expand **Public**.
7. Verify that the **Tables** section contains the same number of tables as the one you saw before.

13 Supplemental Material

In this section

Conflicting Software.....	167
For the Access Server.....	167
For the Mobile Clients.....	278

13.1 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.
- **Anti-virus software** should not scan sync folders, as it may cause conflicts with the sync process. It is recommended that the Acronis Access Filestore folder is added to your anti-virus' ignore or white list. Unless you have turned off encryption, all the items in the Filestore folder will be encrypted and the anti-virus will not be able to detect anything but it may cause issues with some items.

13.2 For the Access Server

In this section

Customizing the Web Interface through the API.....	167
Unattended desktop client configuration	168
Microsoft Azure Integration.....	172
Load balancing Acronis Access.....	184
Using Acronis Access with Microsoft Forefront Threat Management Gateway (TMG)	191
Configuring Single Sign-On.....	208
Monitoring Acronis Access with New Relic.....	234
Using trusted server certificates with Acronis Access	235
How to support different Access Desktop Client versions.....	237
How to move the FileStore to a non-default location.	238
Running Acronis Access Tomcat on multiple ports.....	239
Installing Acronis Access on a Microsoft Failover Cluster.....	240
Upgrading Acronis Access on a Microsoft Failover Cluster.....	266
Multi-homing Acronis Access.....	268
Deploy separate Web Preview servlets	269
PostgreSQL Streaming Replication.....	273
Configuring PostgreSQL for remote access.....	278

13.2.1 Customizing the Web Interface through the API

Using the API to update your web interface's color scheme can be done easily and without having to restart any services or have any downtime. Some of these customizations can be done through the web interface of Acronis Access (p. 131).

1. You will need to install Curl in order to use any API commands.

- a. Download Curl from the official site at: <https://curl.haxx.se/download.html>

Note: Make sure to download a version that supports SSL!

- b. Follow the prompts from the Curl installer until the installation is finished or just extract the Curl archive.
2. Open an elevated command prompt and enter the following command:
 - `curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@<path_to_file> -F customization_settings[color_scheme_client_scss_file]=@<path_to_file> -F customization_settings[color_scheme]=<name_of_scheme> -u <user>:<password> 'https://<your_site>/api/v1/settings/customization'`

The above command will change the color scheme of the website to the one you selected.

Note: If you only wish to change one of the color scheme .css files, when entering the above command, use the current scheme for the item you do not want to change.

3. Here is an example of how the command looks if you want to upload a **testUI.css** for the Administration part of the UI and **test_client_UI.css** for the web client that are located in **D:\WebUI** and pick **Custom** as the color scheme that will get updated:
 - `curl -X PUT -F customization_settings[color_scheme_administration_css_file]=@D:\WebUI\testUI.css -F customization_settings[color_scheme_client_scss_file]=@D:\WebUI\test_client_UI.css -F customization_settings[color_scheme]=Custom -u administrator:123456 'https://myCompany.com/api/v1/settings/customization'`

13.2.2 Unattended desktop client configuration

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

Creating and configuring 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.

Unattended installation of the client

This section will help you install the Acronis Access Desktop client silently on user login on all desired machines.

Creating an installer distribution point

All computers that will have the client installed, must have access to the installer. This is done by creating a folder, sharing it with the desired user group and placing the installer in it.

1. Right-click on the folder with the installer and select **Properties**.
2. Open the **Sharing** tab and press **Share**.
3. Enter the domain group, OU or users that you will install the Access client on. This group (or etc.) should be the same as the one you select for the **Group Policy Object**.
4. Press **OK/Done** and close all remaining dialogs.

Note: Make sure that the installer is reachable by the desired machines by its network address (e.g. `\\WIN2008\Software\AAClientInstaller.msi`)

Getting the installer on the user's machine

1. On the domain controller, expand the **Group Policy Objects** section and right click on your new Policy Object.
2. Select **Edit** and expand **User Configuration -> Preferences -> Windows Settings -> Files**.
3. Right-click on Files and select **New -> File**.
4. Select **Create** for **Action**.
5. For **Source file(s)** either click on the browse button and navigate to the Access client installer or enter the full path to it. (e.g. `\\WIN2008\Software\AAClientInstalelr.msi`)
6. For **Destination file** enter the destination folder and destination filename. This will copy the Access client installer from the network share and will place it in the destination folder on the user's machine on logon.

Note: e.g. If you enter `C:\Folder\ThisFile.msi`, the client installer will get placed in the user's **C** drive, in the folder `Folder` and will be named `ThisFile.msi`.

7. Press **OK**.

Installing the client

Making the installation script

1. Create an empty text file and paste the following script into it:

```
msiexec /i "C:\AAC.msi" /quiet
sleep 180
DEL /F /S /Q /A "C:\AAC.msi"
```

This script will open a command prompt, install the Access client without displaying anything and delete the Access client installer after 3 minutes.
2. Change the path `C:\AAC.msi` in both places, to the path you entered in the **Destination File** field and press **File -> Save As...**
3. Enter a name for the script and make sure it ends with **.bat**. For the **Save as type:** field, select **All Files**. Make sure that the file is either on the domain controller or is reachable by it. This file is important and must not be changed or deleted so place it in a specific location that won't get changed.

Using the script on user logon

1. Open the **Group Policy Manager** and expand the **Group Policy Objects** section and right click on your new **Policy Object**.
2. Select **Edit** and expand **User Configuration -> Policies -> Windows Settings -> Scripts (Logon/Logoff)**.
3. Double-click on **Logon** and press **Add**.
4. In the **Add Script** dialog, press **Browse (...)** and navigate to the folder where you saved the script.
5. Select the script and press **Open**.
6. Press **OK** and press **OK** again on the following dialog.
7. Done. All users in the specified group or OU will now get the Acronis Access client installed on logon.

Creating the folder and registry entries:

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

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

Creating the sync folder:

1. Right-click on **Folders** and select **New -> Folder**.
2. Set the **Action** to **Create**.
3. For the path, enter the following token: **%USERPROFILE%\Desktop\AAS Data Folder**

Creating the registry:

1. Right-click on **Registry** and select **New -> Registry Item**.
2. Set the **Action** to **Create**.
3. For **Hive**, select **HKEY_CURRENT_USER**.
4. For the path, enter the following: **Software\Group Logic, Inc.\activEcho Client**
5. Now do the following for the desired entries:
6. For the Username:
 - a. For **Value name** enter **"Username"**.
 - b. For **Value type** select **REG_SZ**.
 - c. For **Value data** enter the following token: **%USERNAME%@%USERDOMAIN%**

Note: If you wish to use **Single Sign-on**, do **not** configure the Username token. Instead, do the following:

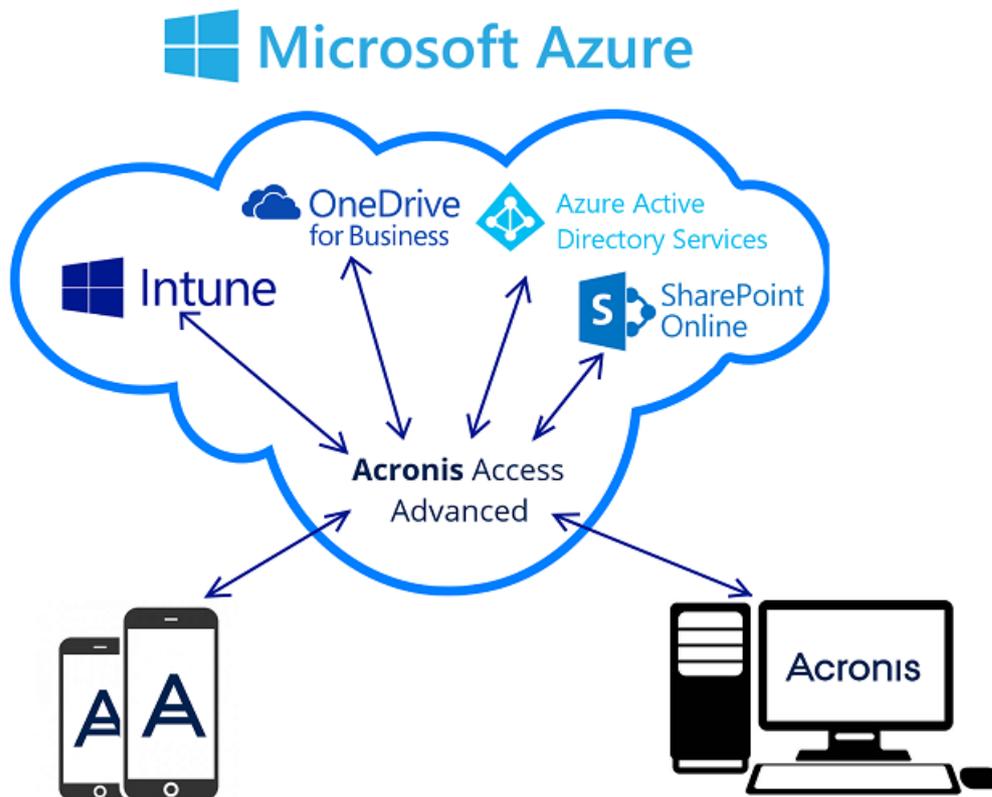
- For **SSO**:
 - a. For **Value name** enter **"AuthenticateViaSSO"**.
 - b. For **Value type** select **REG_SZ**.
 - c. For **Value data** enter **1**.

7. For the Server URL:
 - a. For **Value name** enter "**Server URL**".
 - b. For **Value type** select **REG_SZ**.
 - c. For **Value data** enter the address of your 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.

13.2.3 Microsoft Azure Integration

Integrating Acronis Access in Microsoft Azure

Microsoft Azure offers Enterprise customers an easy method to deploy their preferred software in the cloud, with huge support of different operating systems and software, while still keeping their users in control. Integrating Acronis Access in Microsoft Azure lets you get the full benefit of Acronis Access' features without having any dedicated physical machines. The whole product can be run from within the Microsoft Azure cloud without any lack in functionality.



13.2.3.1 Before you begin

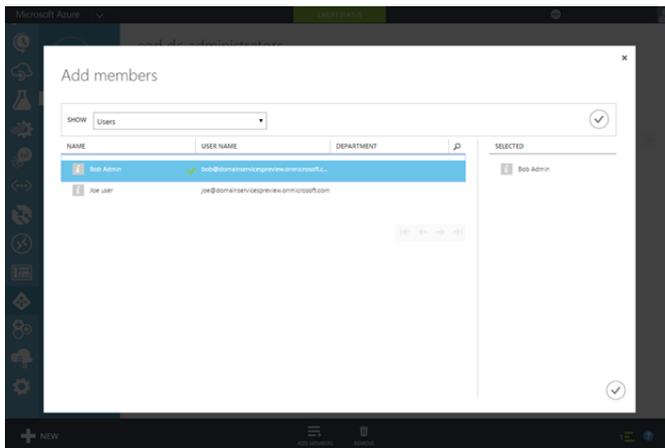
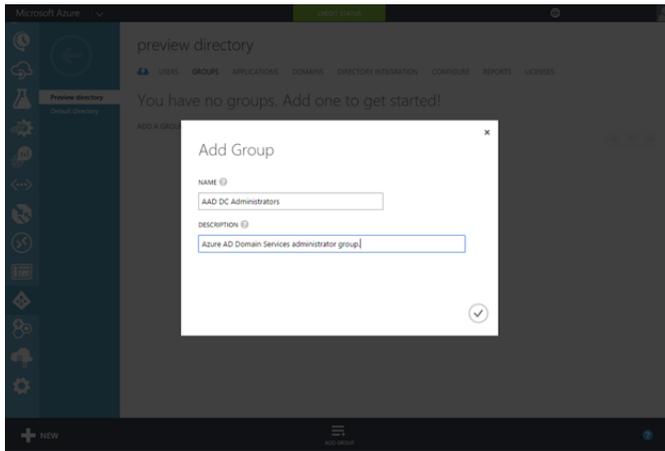
There are some important items that you need to make sure are already setup and running before installing Acronis Access:

- When creating the Azure Virtual Machine that will host Acronis Access, we recommend Windows Server 2012 R2 or Windows Server 2008 R2.
- A Virtual Network that the Virtual Machine will use. Azure Directory Services requires Virtual Network (**classic**) in order to be functional and you must configure the Virtual Machine to be able to work with Virtual Network (**classic**).
- You will need the "AAD DC Administrators" group. If you do not have this group already created, you will have to create it. The users in that group will be able to bind machines to the domain.
- In Azure, you must have a Directory Service running, so you can bind the Virtual Machine, on which Acronis Access will be running, to your Azure Active Directory.

13.2.3.2 Managing the Azure Active Directory Service

Create the 'AAD DC Administrators' group

Using the Azure management portal, create a group called 'AAD DC Administrators' and add all users who need to be administrators on the managed domain to it. These administrators will be able to join machines to the domain and to configure group policy for the domain.



13.2.3.3 Select or Create the Azure virtual network

Select (or create) the Azure virtual network in which to enable Azure AD Domain Services

When enabling Azure AD Domain Services, you will need to specify which Azure virtual network you'd like to make domain services available in. Ensure you pick a virtual network that satisfies the following criteria:

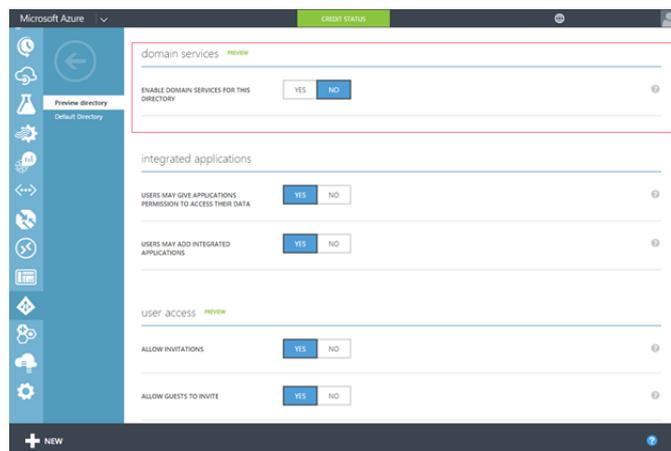
- Azure Directory Services require a Virtual Network (**classic**) in order to be functional.
- The virtual network belongs to a region supported by Azure AD Domain Services. See the region page for details.
- Ensure the virtual network is a regional virtual network and doesn't use the legacy affinity groups mechanism.
- Ensure your workloads deployed in Azure Infrastructure services are connected to this virtual network.
- Make a note of the virtual network's name for later.

13.2.3.4 Enable Azure AD Domain Services for your Azure AD tenant

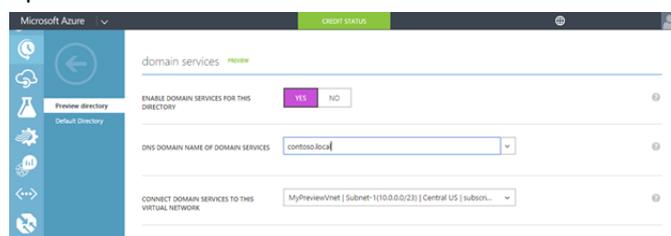
Enabling Azure AD Domain Services for your Azure AD tenant is a simple process.

Note: You can also Sync your Active Directory instance with Azure AD Connect. For more information, please consult Microsoft Azure's documentation on the subject.

1. Navigate to the Azure AD tenant and click on the **Configure** tab of your directory. You will notice a new section titled **Domain Services**.

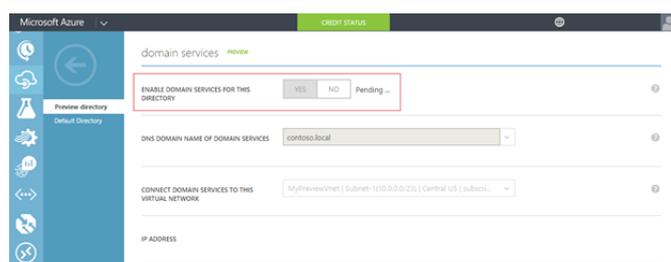


2. Flip the toggle titled **Enable Domain Services for this directory** to **Yes** to see other configuration options.



3. Specify a domain name for the domain you're creating using Azure AD Domain Services. You may choose to use the built-in domain name (*.onmicrosoft.com) or any of the domain names available in the domains tab of your directory. Optionally, you can also specify a custom domain name by typing it into the textbox.
4. In the drop down, select the virtual network in which domain services should be made available.
5. When you are done, hit **Save** at the bottom of the page.
6. At this point, Azure AD Domain Services will start to provision a domain for your tenant and the page should display a 'Pending...' state. Under the covers, domain services are being provisioned and connected to the virtual network you've selected.

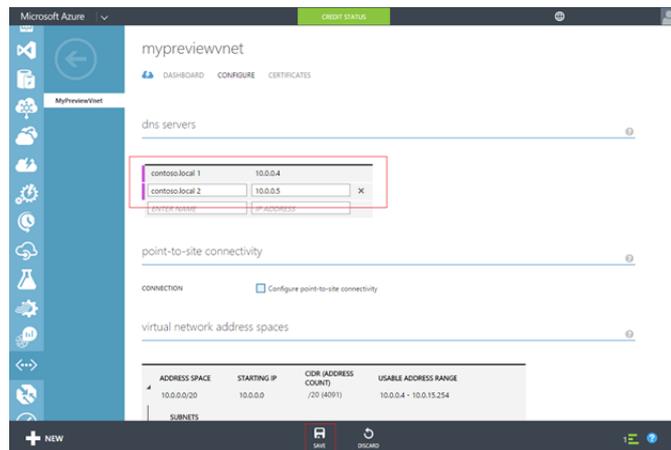
Note: Restarting **Domain Services** after Acronis Access has been configured and has active users is not recommended as the Access server cannot account for the inner workings of Microsoft Azure's Domain Services.



7. You will notice the IP addresses of the Azure AD Domain Services start to appear on the page as these come online. Azure AD Domain Services provide high availability and you should expect to see two IP addresses when the services are fully provisioned for your domain. It can take 20-30

minutes for the first IP address to be displayed and another 20-30 minutes for the second IP to be available.

- At this point, you can set these IP addresses as the DNS servers for the virtual network in which you had enabled Azure AD Domain Services. This enables virtual machines within that virtual network to 'see' the domain and connect to it for domain join, LDAP, authentication etc.



Note: For any further information and help with the Active Directory, please contact Microsoft Technical Support.

13.2.3.5 Creating a Acronis Access Virtual Machine through the Azure Marketplace

The easiest way to get started with a Acronis Access subscription is to use an image straight from the Azure marketplace. The image has Acronis Access already installed and you will only have to configure it to suit your deployment.

Creating a Virtual Machine with a Acronis Access image

Creating the Virtual Machine:

- Open the Azure portal and log in.
- Open the **Virtual Machines** tab and press **Add**.
- Enter **Acronis Access** in the search field and hit **Enter**.
- Select **Acronis Access Advanced**.
- Press **Create**. Make sure that **Resource Manager** is the **Deployment Model**.

Configuring the Virtual Machine's settings:

Note: All of these settings are controlled by Microsoft. If you are experiencing issues or do not understand some of the options, please consult Microsoft Azure documentation or Microsoft support.

Basics:

- Enter a name for the Virtual Machine.
- Select a disk type - SSD or HDD.
- Enter a username and password for the Virtual Machine. These will be used to connect to it via remote desktop.

4. For **Subscription**, select **Pay-As-You-Go**.
5. Either use an existing **Resource group** or select **Create new** and enter a name for the group.
6. Select the **Location** that is closest to your geographical location. This will improve the performance and the connectivity.
7. Press OK when satisfied with the **Basic** settings.

Size:

Choose one of the recommended sizing plans. If none of the recommended plans will suffice for your deployment, press **View All** and select one of those.

Note: The plan you choose should *NOT* be smaller than the recommended ones! For more information, please read the Acronis Access hardware requirements (p. 23).

Settings:

- **Storage**
 - Select an existing Storage account or create a new one.
- **Network**
 - Select an existing Virtual network or create a new one.
 - Select a Subnet for the Virtual network.
 - Set a Public IP address if you want the virtual machine to be reachable from outside the virtual network.
 - Select a Network security group for the VM.
- **Extensions**
 - Add any Azure virtual machine extensions or leave this setting at **No Extensions** if you are unfamiliar with Extensions.
- **High availability**
 - Select the desired Availability set, if any.
- **Monitoring**
 - Disable or enable diagnostics for your the virtual machine.
 - If using diagnostics, select a diagnostics storage account.

Review the virtual machine's parameters and subscriptions. If everything is as desired proceed on to buying.

Configuring Acronis Access

1. Once the virtual machine has been created, you can log into it and you will be greeted by an open browser with the Acronis Access console open.
2. Choose a password for the administrator account.
3. You will be presented with the Acronis Access setup wizard.

13.2.3.6 Configuring Acronis Access

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

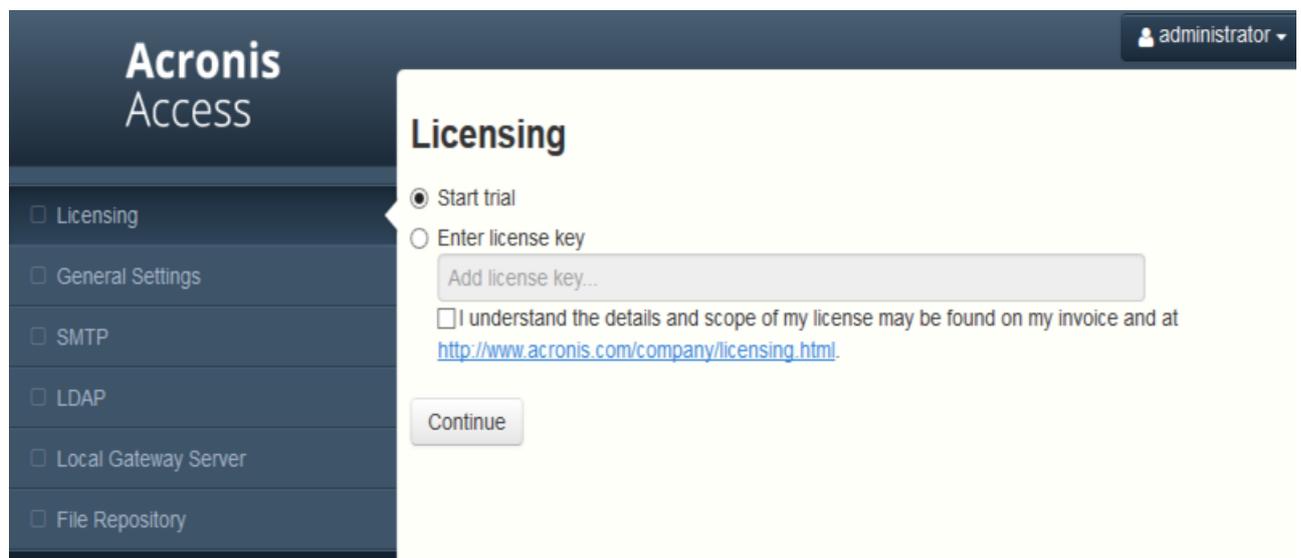
Note: After the configuration utility has run, it will take 30-45 seconds for the server to come up the first time.

Navigate to the Acronis Access's web interface using the DNS name/IP address given to the Virtual Machine and the port specified in the Configuration Utility. You will be prompted to set the password for the default administrator account.

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

Going through the initial configuration process

Licensing



- To start a trial:
 - a. Select **Start Trial**, enter the required information and press **Submit**.
- To license your Access Server:
 - a. Select **Enter license keys**.
 - b. Enter your license key and mark the checkbox.
 - c. Press **Save**.

General Settings

Server Settings

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

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

SMTP

SMTP

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

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

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

1. Enter the DNS name or IP address of your SMTP server

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

LDAP

LDAP

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

Enable LDAP?

LDAP Server Address

LDAP Server Port

Use Secure LDAP Connection?

LDAP Username

LDAP Password

LDAP Password Confirmation

LDAP Search Base

Domains for LDAP Authentication

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

Require exact match

LDAP information caching interval

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

1. Mark **Enable LDAP**.

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

Local Gateway Server

Local Gateway Server

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

Address clients use to connect to the server:

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

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

File Repository

1. Select a file store type. Use **Filesystem** for a file store on your computers and Acronis Storage S3, Swift S3, Ceph S3, Amazon S3 for a file store in the cloud. Other S3 compatible storage services can be used, but we cannot guarantee their functionality.
2. Enter the DNS name or IP address for the file repository service.

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

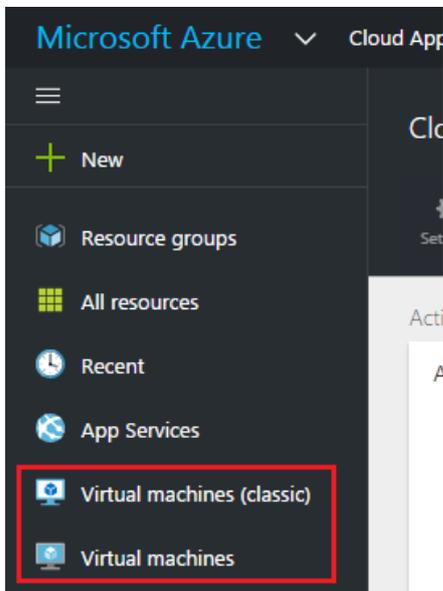
3. Select an encryption level. Choose between None, AES-128 and AES-256.
4. Select the minimum free space available before your server sends you a warning.

5. Press **Save**.

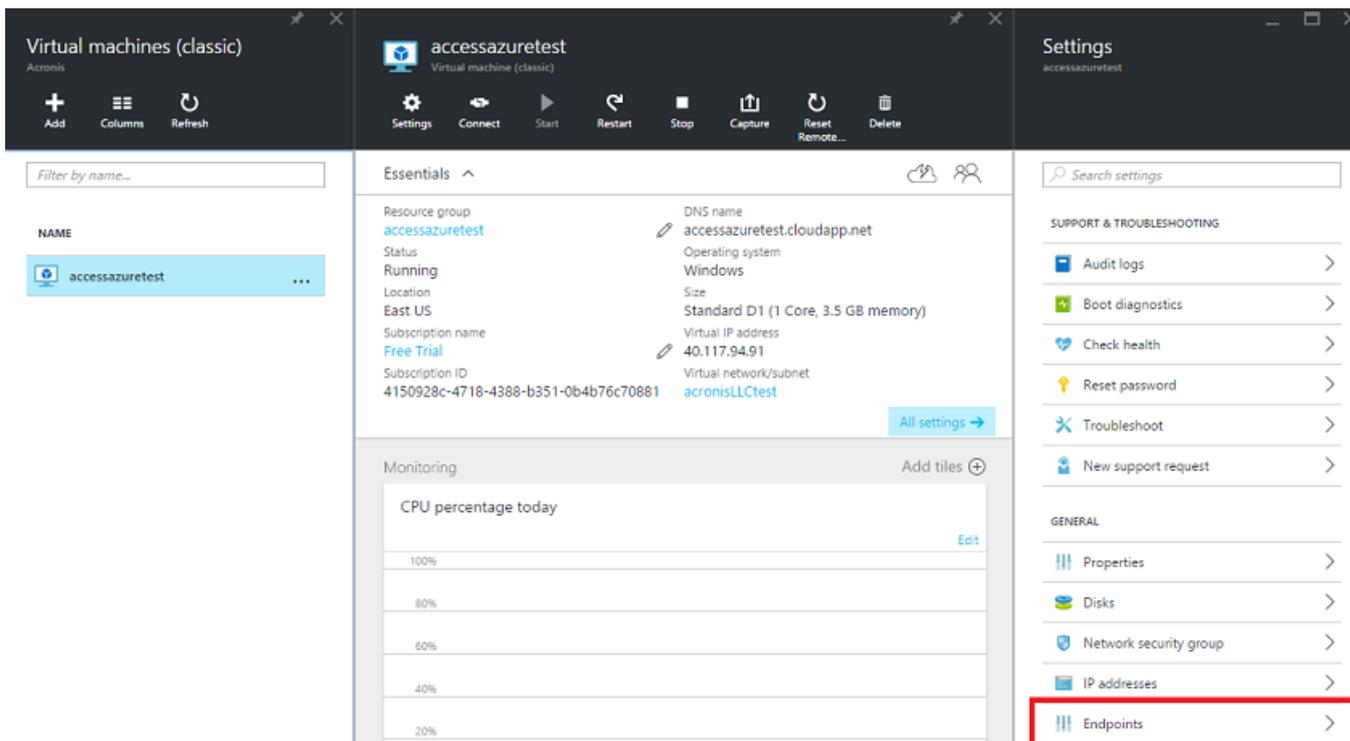
13.2.3.7 Opening the necessary ports on Azure

In order for Acronis Access to be reachable from outside the private Virtual Network, you need to setup some **Endpoints**.

1. Login to Microsoft Azure and open the Virtual Machines tab. If you have both Virtual Machines (classic) and Virtual Machines, please open the proper tab depending on your Virtual Machine type.



2. Click on the Virtual Machine that hosts Acronis Access.
3. From the **Settings** menu on the right side, select **Endpoints**.



4. Press **Add**, enter a name for the endpoint and select TCP as the protocol.

5. Enter the Ports used by your Acronis Access Services. You will need 1 endpoint for each service. (Acronis Access Tomcat and Acronis Access Gateway). By default, <PROCUT_NAME> uses port 443 for the Access Tomcat service and port 3000 for the Access Gateway service.

Add endpoint
accessazuretest

* Name

Protocol TCP UDP

* Public port

* Private port

Floating IP address Disabled Enabled

Access control list

ORDER	NAME	ACTION	REMOTE SUBNET
<input type="text"/>	<input type="text"/>	deny	<input type="text" value="0.0.0.0/0"/> ...

13.2.3.8 SharePoint Online and OneDrive for Business integration

Acronis Access supports both SharePoint Online and OneDrive for Business. To integrate these services, you have to add them as Data Sources.

Adding SharePoint Online as a Data Source

1. Open the Acronis Access web interface and login as an administrator.
2. Open the **Mobile Access** tab and click on **Data Sources**.
3. Press **Add New Folder**.
4. Enter a name for the **Folder**.
5. Select the Gateway that will handle the connections. Usually, this should be the locally installed one.
6. Select SharePoint site as the **Data Location** and enter the link to your team's SharePoint Online site. E.g. **https://company.sharepoint.com**
7. Select the **Sync** type and if the **Folder** should be visible when someone is browsing the server.
8. Enter the name of and select the users/groups that will have this Folder assigned to them.
9. Press **Save**.
10. If 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://company.sharepoint.com:43222**
e.g. **Document Library Name: Projects**

Adding OneDrive for Business as a Data Source

The procedure is almost entirely the same as adding a SharePoint site but since this product is for personal use for the employees, there isn't a universal link that can be used for everyone. You will have to use a wildcard (%USERNAME%). The link that you must enter will look like this:

https://YOURDOMAIN-my.sharepoint.com/personal/%USERNAME%_YOURDOMAIN_onmicrosoft_com

This creates a Data Source that allows all users to work with their OneDrive items through Acronis Access.

Note: Enter the whole URL in the SharePoint Site field, do not use the Subpath or Library fields.

Note: The device has to be managed by Acronis Access or the wildcard will not work and users will not be able to access OneDrive items.

Another important thing to note is due to the use of the wildcard, users cannot give access to their files, to other users. Administrators can create a Data Source for each user on a user-by-user basis and then administer who can share with whom if they so desire.

13.2.4 Load balancing Acronis Access

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

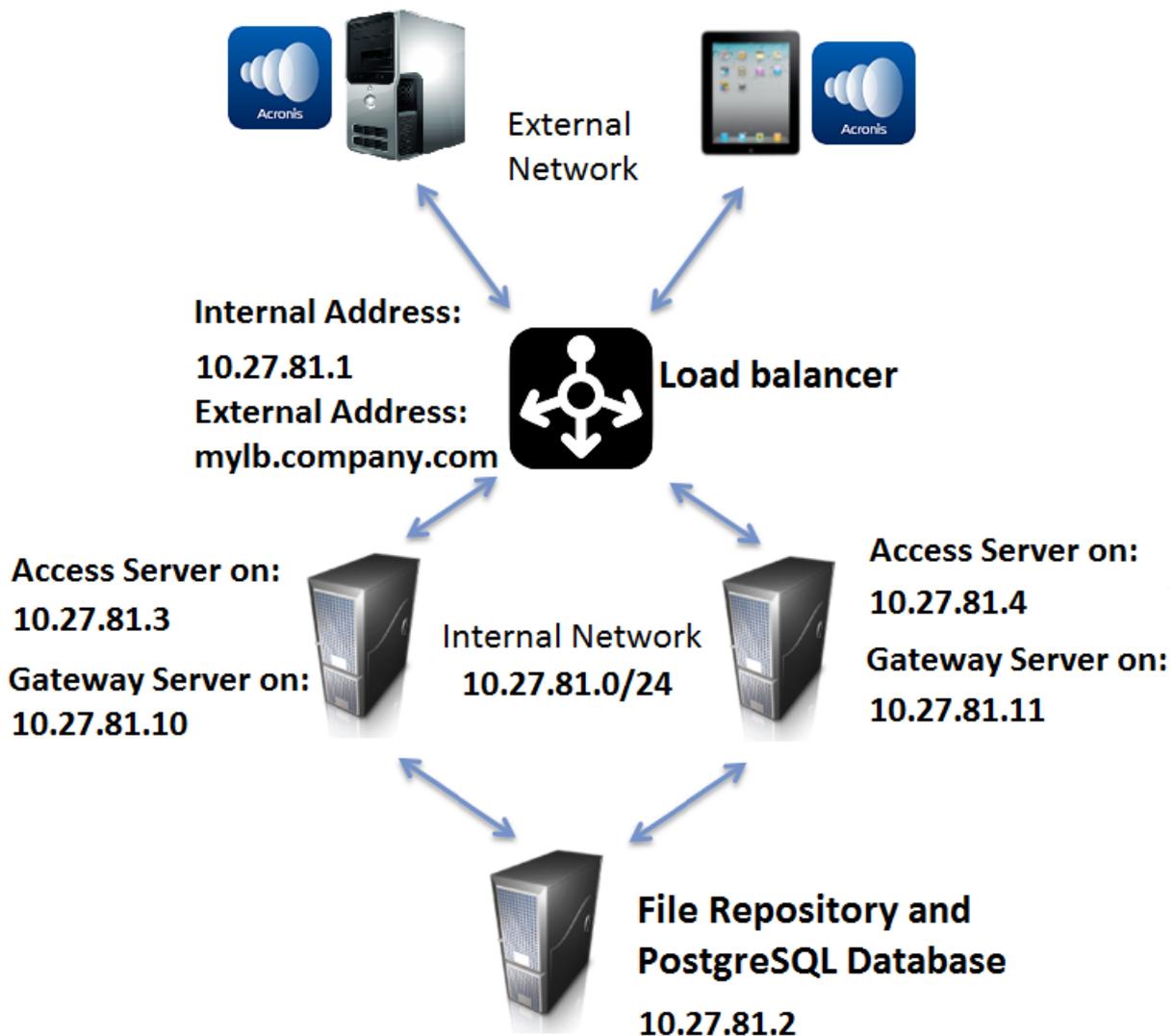
Load balancing only the Gateway Servers

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. 94) 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.

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.

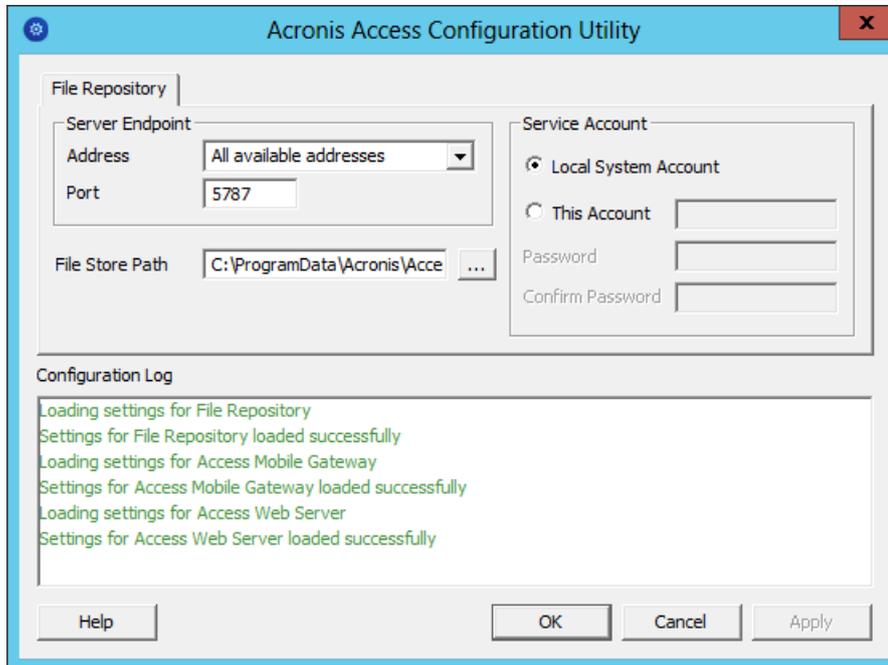
On the server that will be hosting your PostgreSQL database and File Repository, perform the following steps:

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 (p. 28).
 - 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.

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 \(p. 28\)](#) and [File Repository \(p. 110\)](#) 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
# First Acronis Access & Gateway server
host all all 10.27.81.3/32 md5
# Second Acronis Access & Gateway server
host all all 10.27.81.4/32 md5
```

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

9. If you wish to enable remote access to this PostgreSQL instance, you will have to edit the **postgresql.conf** file. Follow the steps below:
 - a. Navigate to and open the **postgresql.conf**. By default it is located at: **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\Data\postgresql.conf**
 - b. Find the line **#listen_addresses = 'localhost'**
 - c. Enable this command by removing the **#** symbol at the start of the line.

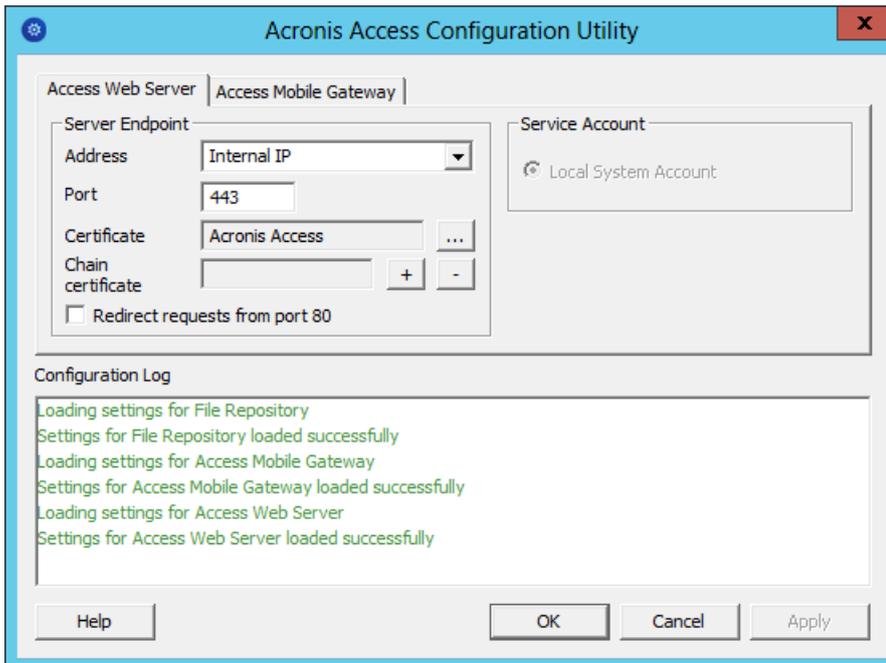
- d. Replace **localhost** with ***** to listen on all available addresses. If you want PostgreSQL to listen only on a specific address, enter the IP address instead of *****.
 - e.g. **listen_addresses = '*'** - This means that PostgreSQL will listen on all available addresses.
 - e.g. **listen_addresses = '192.168.1.1'** - This means that PostgreSQL will listen only on that address.
 - e. Save any changes made to the **postgresql.conf**.
 - f. Restart the Acronis Access PostgreSQL service.
10. 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**.

Note: PostgreSQL uses port 5432 by default. Make sure that this port is open in any firewall or routing software.

On the two servers that will be acting as both 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 (p. 28).
 - a. You will be prompted to open the Configuration Utility. Press **OK**.
 - b. **On the Access Server tab:**
 - 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**.

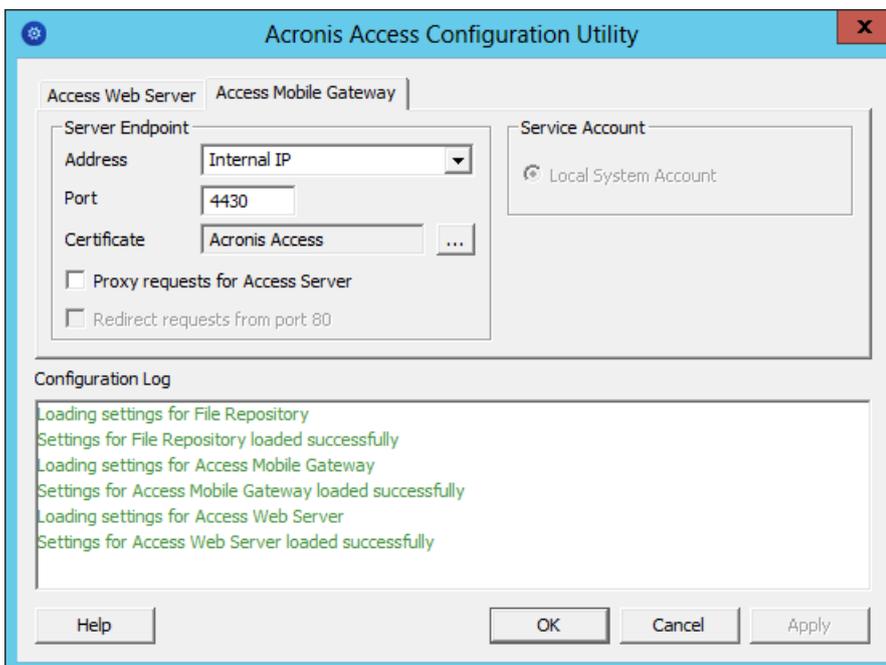
Note: If you don't have a certificate, a self-signed certificate will be created by Acronis Access. This certificate should NOT be used in production environments.



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.

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 its 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 (p. 31).
 - 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**.

- Enter your LDAP credentials, with the domain. (e.g. acronis\hristo).
 - 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. 84) 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. 94) 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.

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.

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

In this section

Overview	191
Known Issues.....	192
Introduction	192
Install the SSL Server Certificate	195
Create a New Web Listener	196
Create a New Web Site Publishing Rule.....	201
Configure an External DNS Entry for the Acronis Access Gateway Server	207
Using the Access Mobile Client with a TMG reverse proxy server	207
Using the Access Desktop Client with a TMG reverse proxy server.	207

13.2.5.1 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:

Note: The Acronis Access app for Windows phones and tablets does not support reverse proxy and will not work with TMG.

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

13.2.5.2 Known Issues

Microsoft's TMG product has a bug/limitation where it closes push notification (i.e., long-running TCP socket) connections, which affects Acronis Access in the following ways:

- All the Access desktop clients that connect through it cannot use push notifications and will be forced to use the legacy polling mode (p. 207). The clients therefore cannot sync Network nodes because that requires a working push notification connection to the Access server for technical reasons.

Using legacy polling is inefficient and generates a significant additional load on the Access server.

This is not an Acronis Access bug and therefore we cannot fix it.

You can either escalate a case with Microsoft support to investigate the configuring of the TMG to support push notification connections, or you can switch to a different firewall that properly supports push notification connections.

- The Acronis Access app for Windows phones and tablets does not support reverse proxy.

13.2.5.3 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.

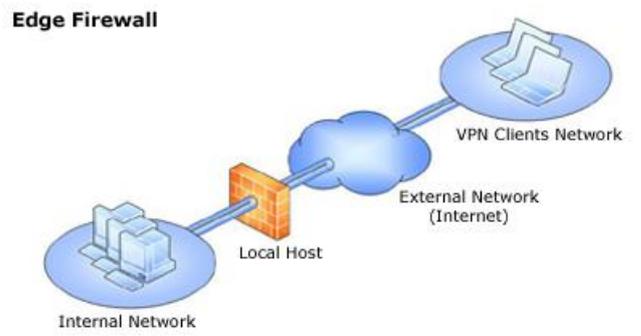
In this section

Understanding Forefront Threat Management Gateway (TMG) Network Topology 193
 Understanding Forefront Threat Management Gateway authentication 194

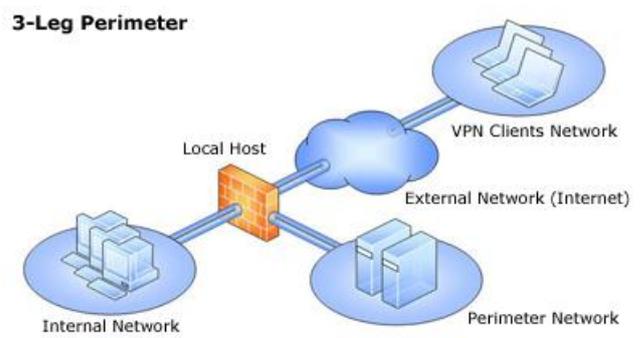
Understanding Forefront Threat Management Gateway (TMG) Network Topology

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.

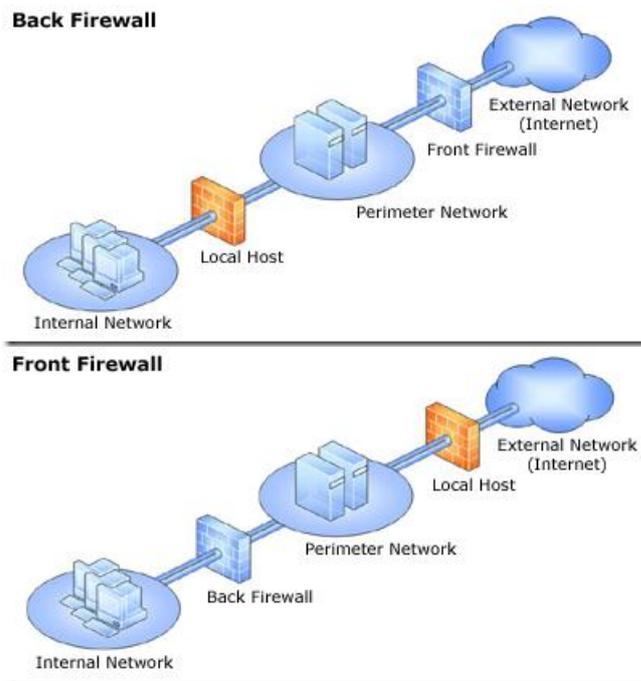
- **Edge Firewall** - In this topology, Forefront TMG is located at the network edge, where it serves as the organization's edge firewall, and is connected to two networks: the internal network and the external network (usually the Internet).



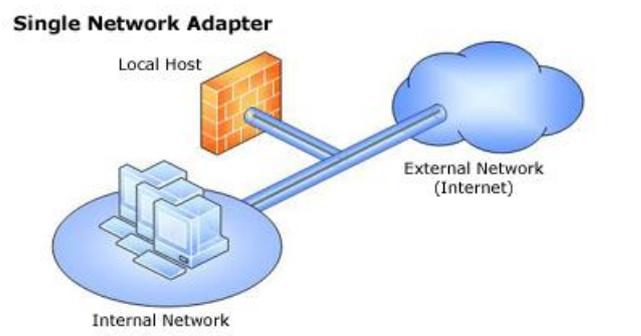
- **3-Leg Perimeter** - This topology implements a perimeter (DMZ) network. Forefront TMG is connected to at least three physical networks: the internal network, one or more perimeter networks and the external network.



- **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>.

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>

13.2.5.4 Install the SSL Server Certificate

Request and install an SSL certificate using the FQDN for each Gateway 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:

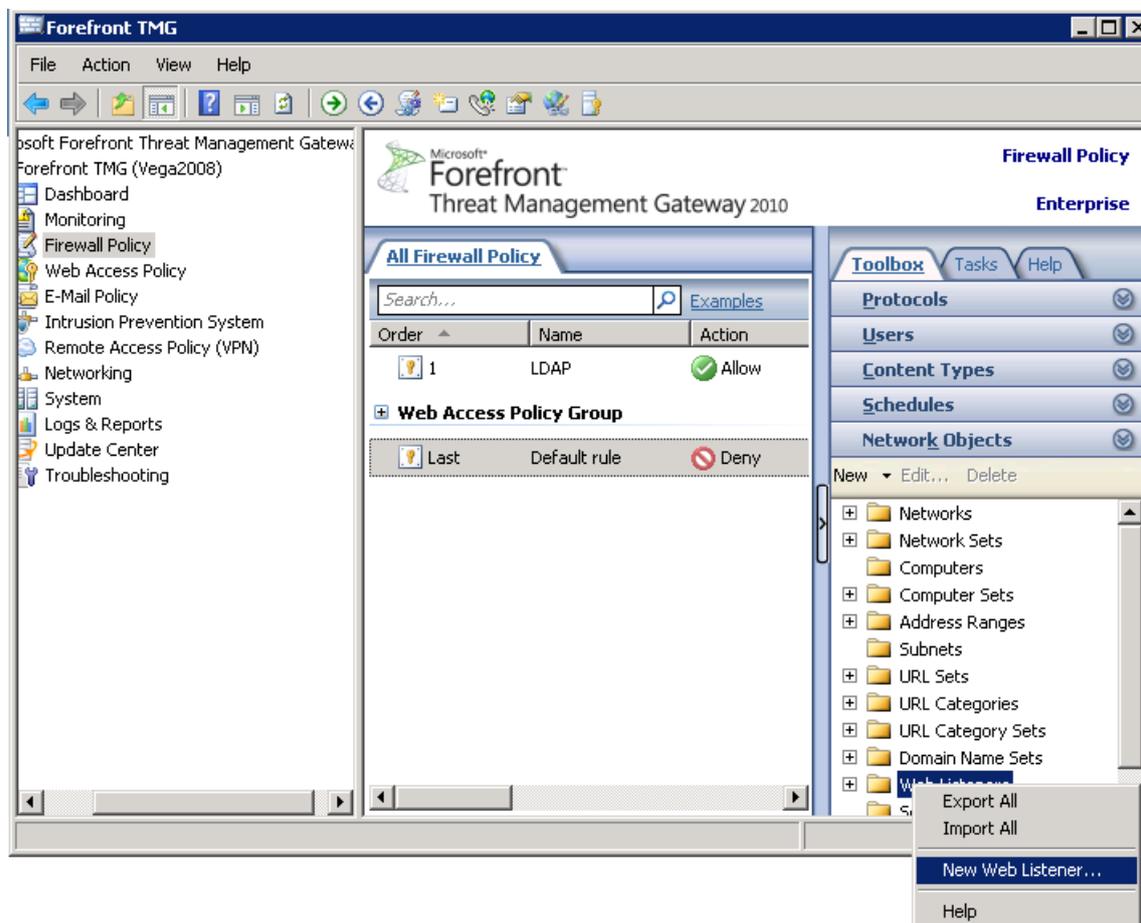
1. On the TMG computer, click **Start**, type **mmc**, and then press **Enter** or click **OK**.
2. Click the **File** menu and then click **Add/Remove Snap-in** or press **Ctrl+M**. Under **Available Snap-ins**, click **Certificates** and then click **Add**.
3. Select Computer Account and then click **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.
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.

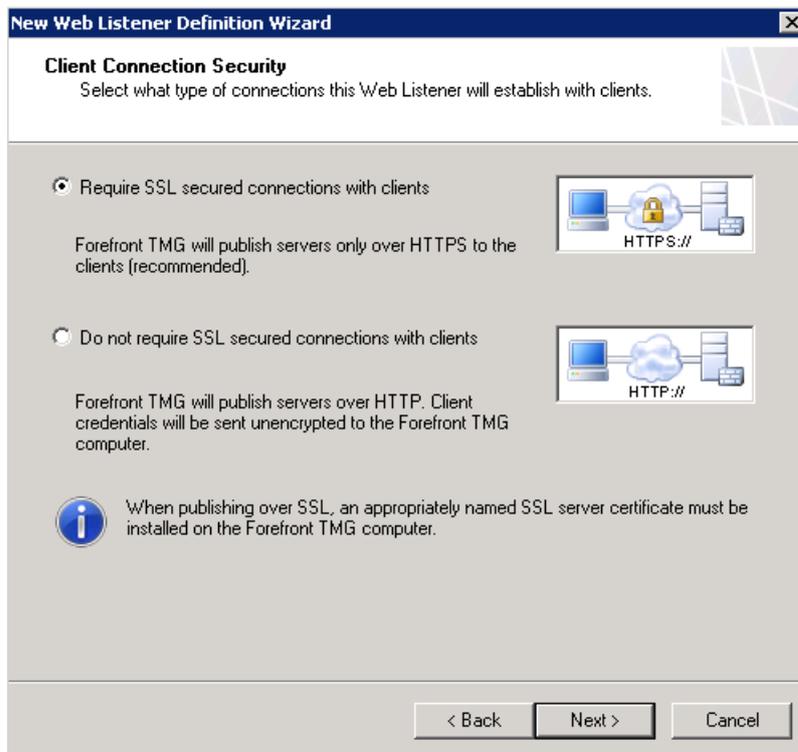
13.2.5.5 Create a New Web Listener

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.

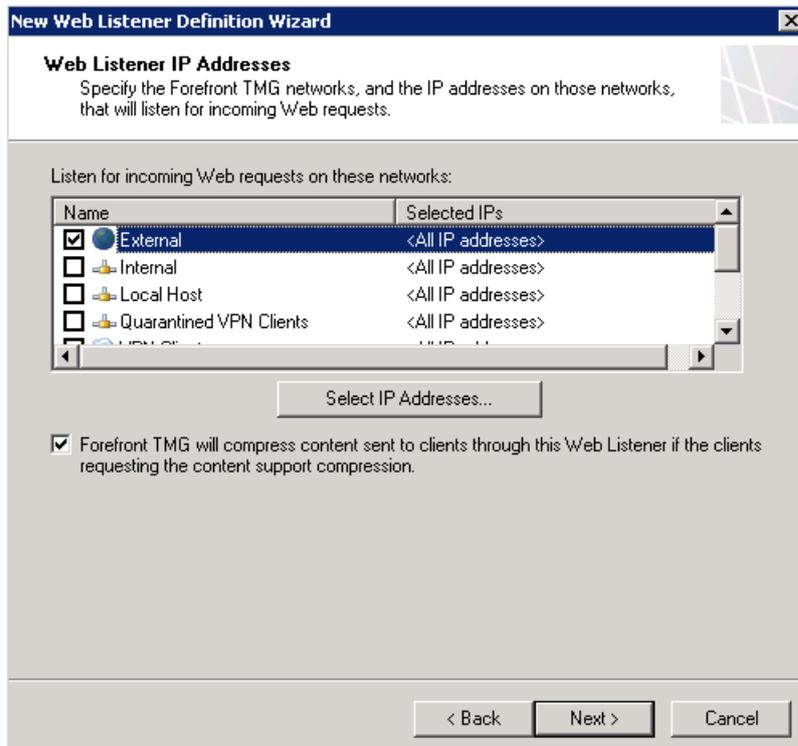


4. The **Welcome to the New Web Listener Wizard** page appears. Give a name to the **Web Listener** (e.g. Access WL) and click **Next**.

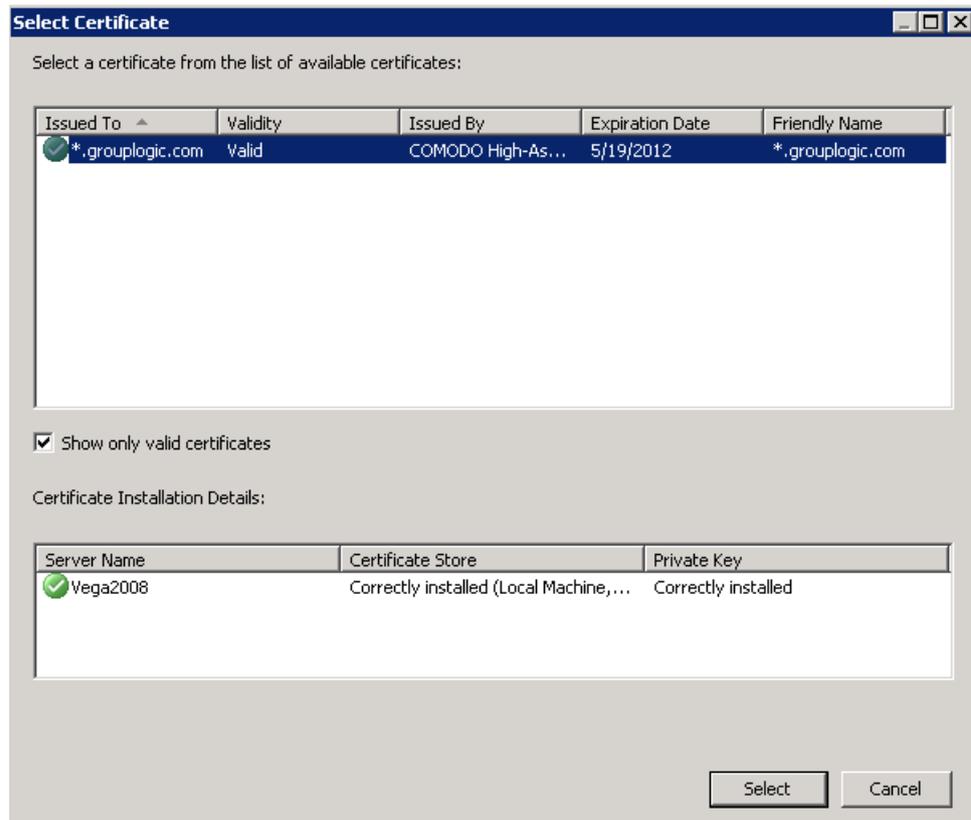
- On the **Client Connection Security** page select **Require SSL secured connections with clients** and click **Next**.



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



- 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.



- Confirm that the correct certificate appears on the **Listener SSL Certificates** page and click **Next**.
- 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**.

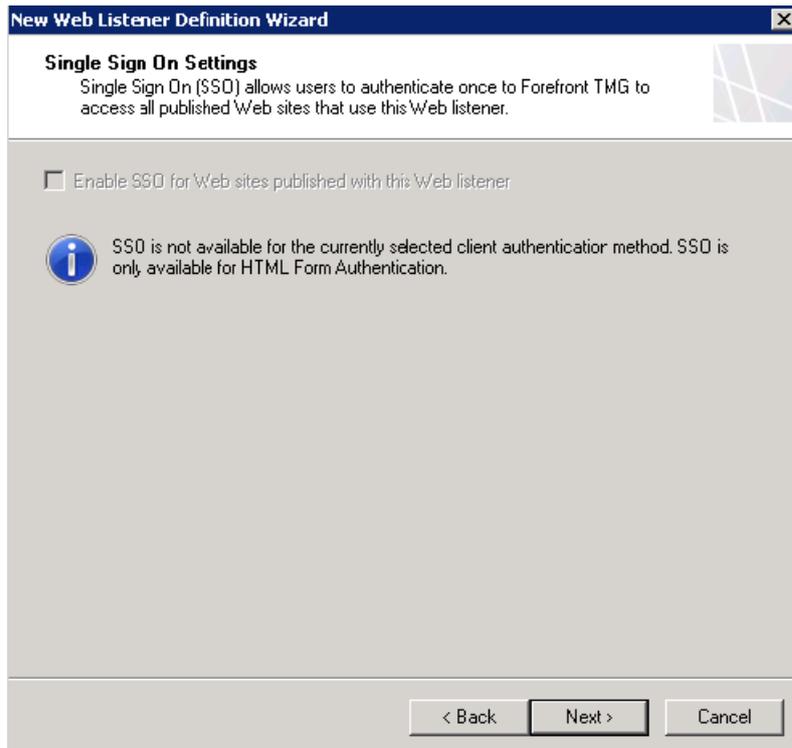
Acronis Access mobile client supports:

- **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.

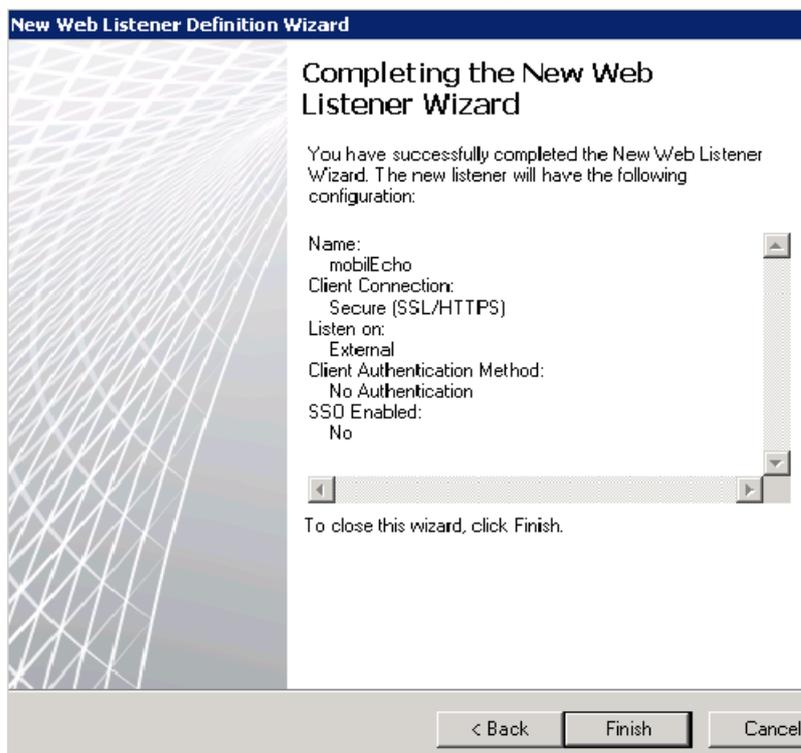
- **SSL Client Certificate Authentication** - Use this option if you'd like the Access Mobile Client app to authenticate with the TMG reverse proxy with an SSL user identity certificate. This certificate must be added to the Access Mobile Client app (p. 333) before the user can authenticate with the TMG reverse proxy server. Additional instructions can be found here. <http://support.grouplogic.com/?p=3830>

The screenshot shows a Windows-style dialog box titled "New Web Listener Definition Wizard" with a close button (X) in the top right corner. The main heading is "Authentication Settings". Below the heading is a descriptive text: "Select how clients will authenticate to Forefront TMG, and how Forefront TMG will validate their credentials." To the right of this text is a small graphic of a grid. The main content area is divided into two sections. The first section is titled "Select how clients will provide credentials to Forefront TMG:" and contains a dropdown menu. The dropdown menu is currently open, showing five options: "HTTP Authentication", "HTML Form Authentication", "HTTP Authentication", "SSL Client Certificate Authentication" (which is highlighted with a blue background), and "No Authentication". The second section is titled "Select how Forefront TMG will validate client credentials:" and contains five radio button options arranged in two columns. The first column has three options: "Windows (Active Directory)" (which is selected), "LDAP (Active Directory)", and "RADIUS". The second column has two options: "RADIUS OTP" and "RSA SecurID". At the bottom of the dialog box are three buttons: "< Back", "Next >", and "Cancel".

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



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



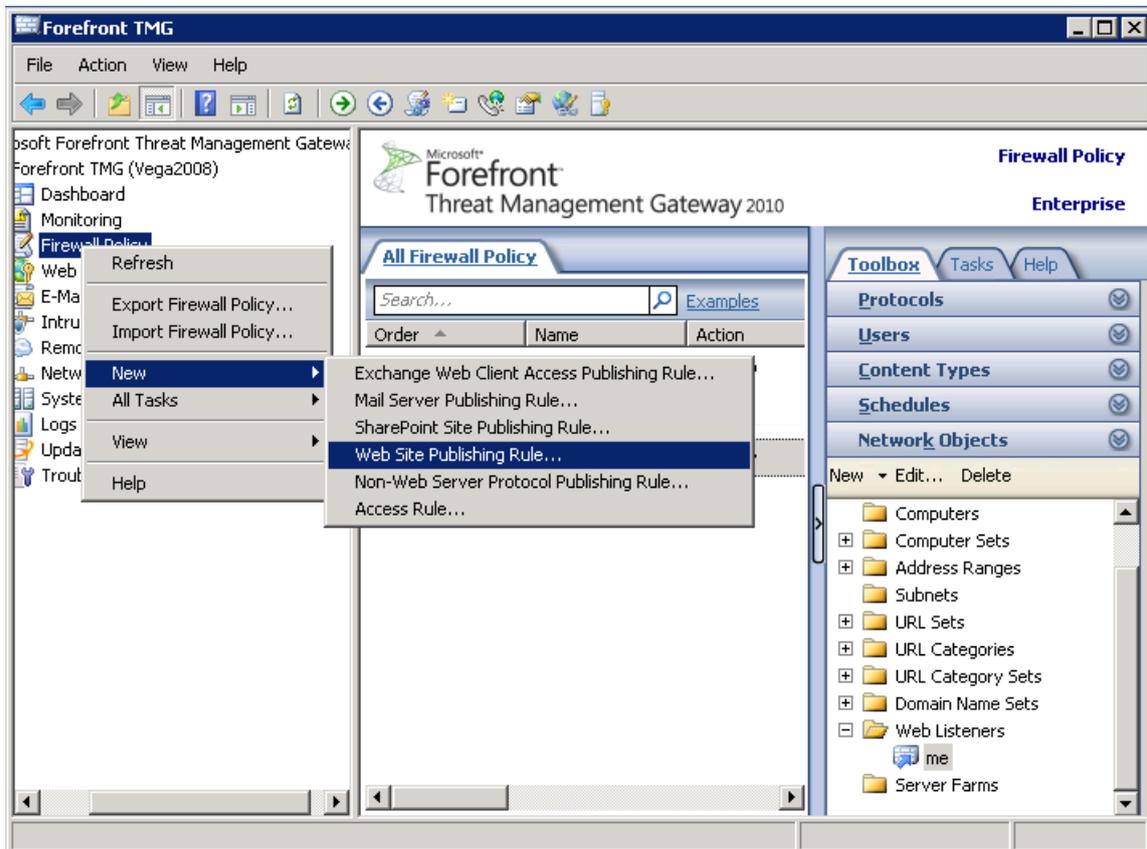
12. Click the **Apply** button to commit the changes.



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).

13.2.5.6 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.
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**.

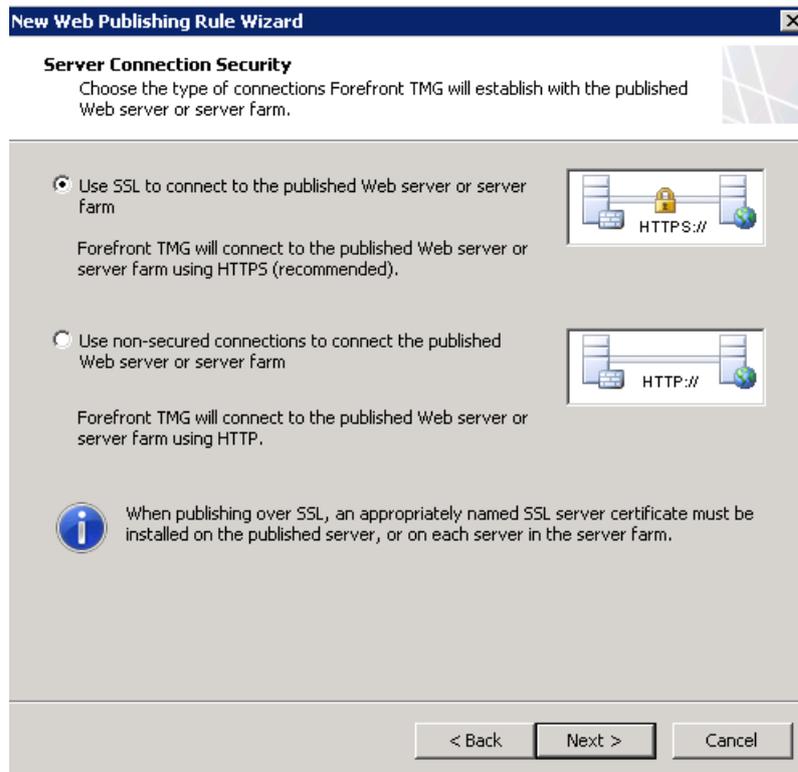
4. On the **Select Rule Action** page verify that the **Allow** option is selected and click **Next**.

The screenshot shows a dialog box titled "New Web Publishing Rule Wizard" with a close button (X) in the top right corner. The main heading is "Select Rule Action" with the instruction "Specify how you want this rule to respond when the rule conditions are met." Below this, the text "Action to take when rule conditions are met:" is followed by two radio button options. The first option, "Allow", is selected and includes the text "With this option selected, incoming requests matching the rule conditions will be allowed." The second option, "Deny", is unselected and includes the text "With this option selected, incoming requests matching the rule conditions will be denied and the traffic will be blocked." At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

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

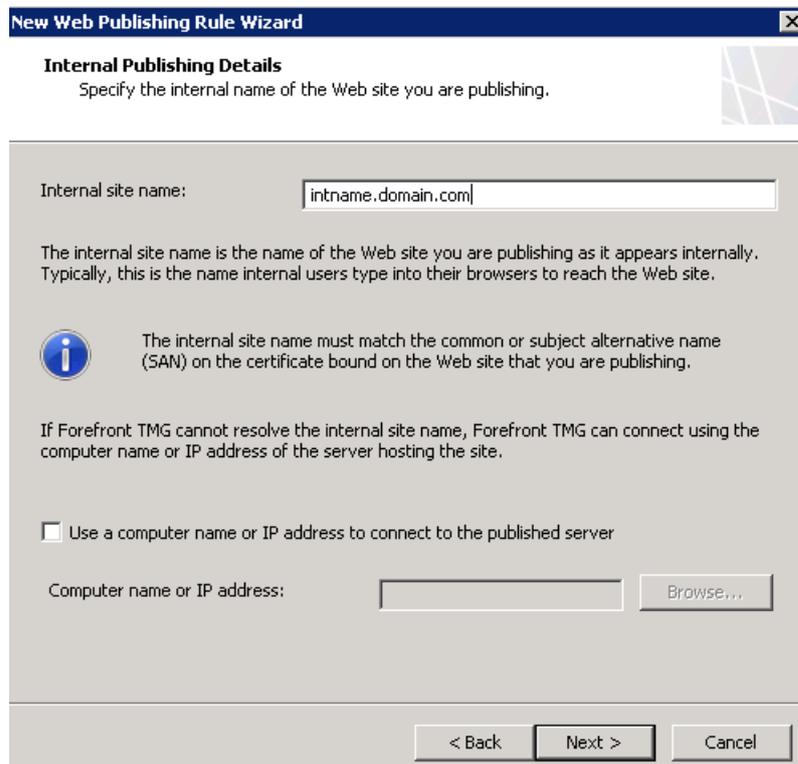
The screenshot shows a dialog box titled "New Web Publishing Rule Wizard" with a close button (X) in the top right corner. The main heading is "Publishing Type" with the instruction "Select if this rule will publish a single Web site or external load balancer, a Web server farm, or multiple Web sites." Below this, there are three radio button options. The first option, "Publish a single Web site or load balancer", is selected and includes the text "Use this option to publish a single Web site, or to publish a load balancer in front of several servers." and a help link "Help about publishing a single Web site or load balancer". The second option, "Publish a server farm of load balanced Web servers", is unselected and includes the text "Use this option to have Forefront TMG load balance requests between a server farm (mirrored servers)." and a help link "Help about publishing server farms". The third option, "Publish multiple Web sites", is unselected and includes the text "Use this option to publish more than one Web site. A new rule will be created for each site published." and a help link "Help about publishing multiple Web sites". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

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 "inname.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 inname 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.

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



- 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**.

New Web Publishing Rule Wizard

Internal Publishing Details
Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder.

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use **/***. Example: folder/*.

Path (optional):

Based on your selection, the following Web site will be published:

Web site:

Forward the original host header instead of the actual one specified in the Internal site name field on the previous page

< Back Next > Cancel

- 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**.

New Web Publishing Rule Wizard

Public Name Details
Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for:

Only requests for this public name or IP address will be forwarded to the published site.

Public name:
Example: www.contoso.com

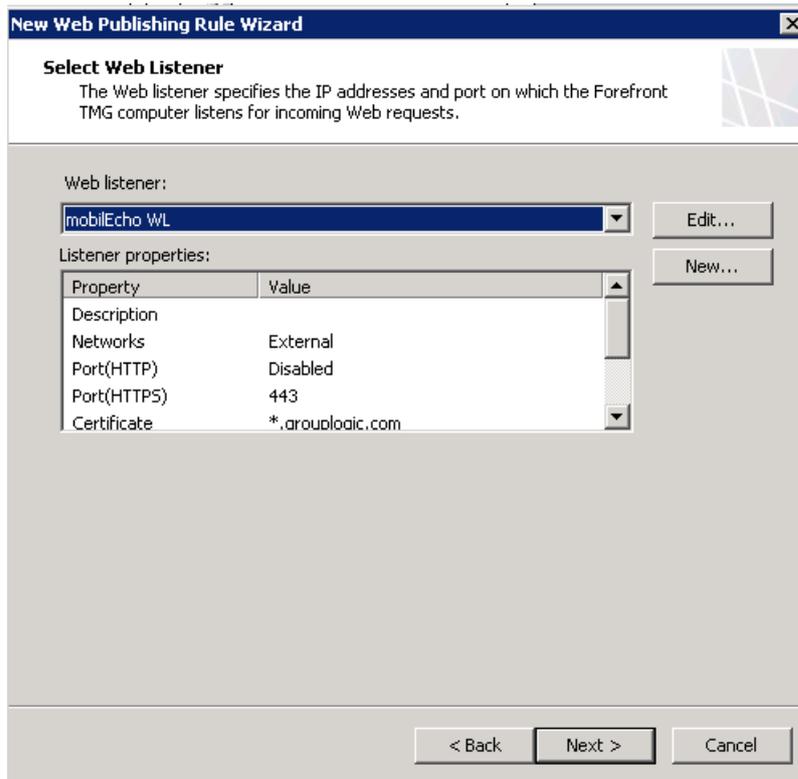
Path (optional):

Based on your selections, requests sent to this site (host header value) will be accepted:

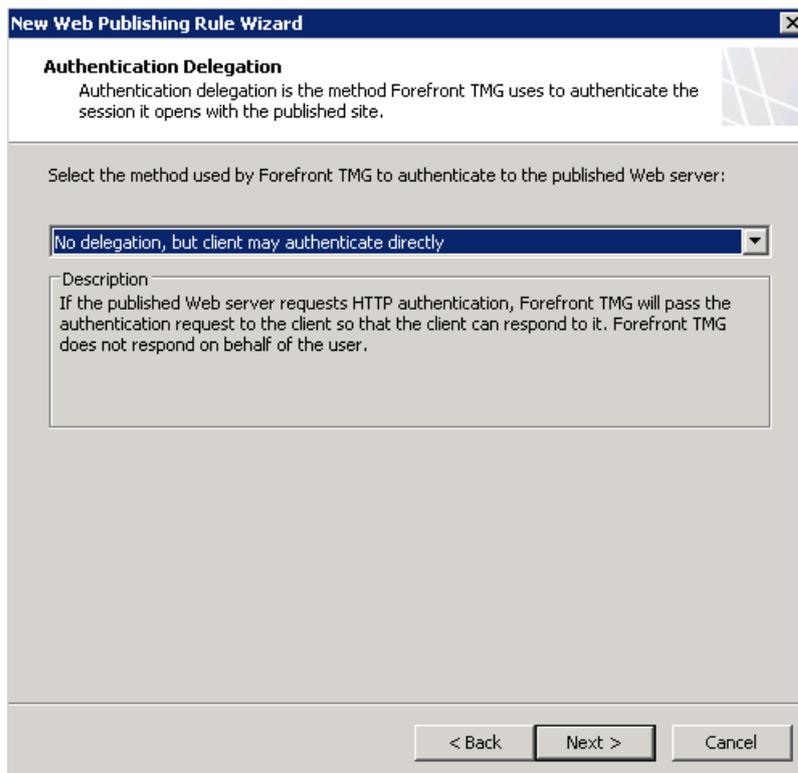
Site:

< Back Next > Cancel

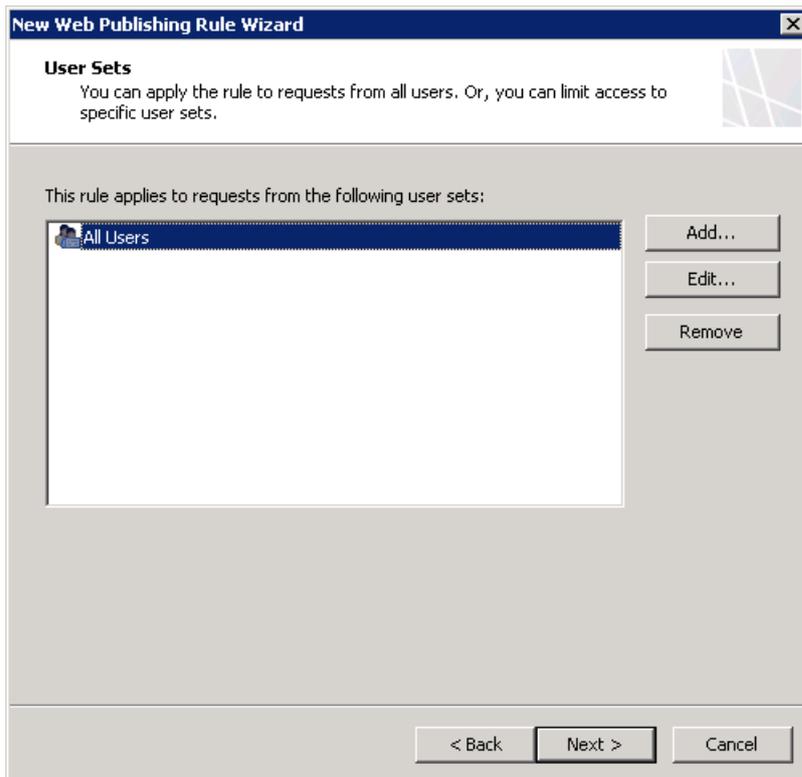
10. On the **Select Web Listener** page select the web listener that you have created for Acronis Access from the drop-down menu and click **Next**.



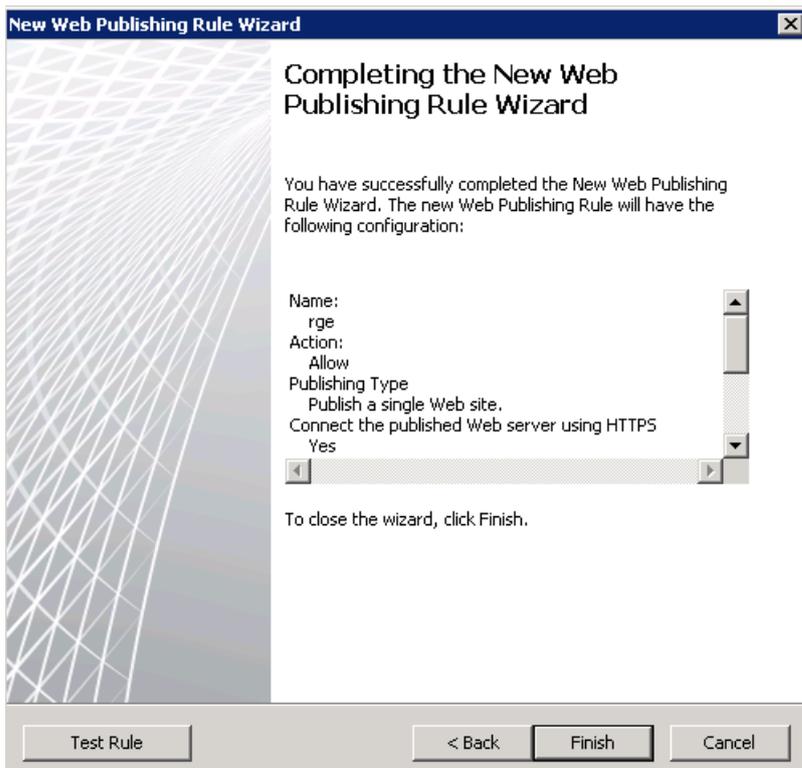
11. On the **Authentication Delegation** page select the **No delegation, but client may authenticate directly** option from the drop-down menu and click **Next**.



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



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).

13.2.5.7 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.

13.2.5.8 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.
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**.

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

This feature is built-in and requires little to no configuration. You will need to use Legacy polling because of a known issue in Microsoft TMG. For more information, please check the Known Issues (p. 192) section.

Enabling Legacy polling mode and disabling syncing:

1. Open the web interface and expand **Sync&Share**.
2. Click on **Access Desktop Client** and select the **Force Legacy polling mode** checkbox. and press **Save**.

Note: The default polling time is 30 seconds. To reduce load on the server you can increase that time to 60 or 90 seconds or higher. That time is how often the client will call up to the server to ask if there are any changes.

3. Click on the **Mobile Access** tab and click on **Policies**. Click on the policy that your desktop clients use.
4. Open the **Server** policy tab and make sure the boxes **Allow File Server, NAS and SharePoint Folders to be Synced to the Desktop Client** and **Allow Two-Way Syncing of File Server, NAS and SharePoint Folders to the Desktop Client** are unchecked and press **Save**.
These syncs are not possible in a configuration without push notifications.

Using the desktop client:

Note: The desktop client cannot sync Network Data Sources in this configuration.

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!

13.2.6 Configuring Single Sign-On

This guide will lead you through an advanced configuration to enable Single Sign On functionality with Acronis Access.

Note: Single Sign-On is only usable in a working domain.

Note: Single Sign-On does **NOT** work when you are running Acronis Access in a single port configuration (when the Gateway Server is proxying the requests for the Access Server).

Note: Single Sign-On does **NOT** work if Acronis Access is installed on the Domain Controller. In addition, even disregarding the SSO limitations, it is highly recommended for performance reasons that the Access server not be installed on a Domain Controller.

The Single Sign-On functionality allows all valid LDAP users to login to the web interface and desktop client without having to enter their credentials. The user must have an Acronis Access account or LDAP Provisioning must be enabled on the server.

- Acronis Access displays a link on the login page that will log in the user with the account that was used to login into this computer.

Note: You have to open the Acronis Access interface using its FQDN (e.g. https://access.company.com) for SSO to work. Single Sign-on does NOT work if you open the interface via IP address.

- For the Desktop Client, there is a new radio button that enables SSO. The users will only have to enter the Access server's URL. It will automatically log them in with the account that they have used to login into the computer.

Note: This will work only for the Windows client. Mac support will come in a follow-up release.

In this section

Access and Gateway on the same machine.....	209
Access and Gateway on separate machines	214
Acronis Access in a Domain Forest	219
Verify that an SPN is registered	230

Using SMB or SharePoint Data Sources	230
Using mobile clients with client certificate authentication	231
For Load Balanced environments	232

13.2.6.1 Access and Gateway on the same machine

This configuration is the most common and consists of 1 Access server and 1 Gateway server, with both residing on the same machine. This is the default Acronis Access installation.

In this section

On any user's machine	212
-----------------------------	-----

This is a one-time step that must be performed in order to register the Access Server with the Kerberos server on the domain. We will use 'setspn.exe' to specify which LDAP account will be queried for SSO authentication checks.

Note: If you want to use **mobile clients with certificate authentication**, the DNS entries for the Access and Gateway servers must **NOT** be the name of the computer. If the Access Server's SPN is just the name of the machine, the Gateway server will treat the Access Server as "on my machine", and will not attempt to perform Kerberos authentication.

e.g. machineAccess.domain.com / machineGW.domain.com will work

e.g. machine.domain.com / computer.domain.com will NOT work

Configuring the LDAP account that will handle SSO

Note: If you want to use SMB or SharePoint Data Sources, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources. For more information, please visit the *Advanced Delegation Configurations (p. 231)* article.

1. Open a command prompt.

Note: You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command **setspn -s HTTP/computername.domain.com account name**

e.g. If your Access server is installed on **ahsoka.acme.com** and you want to use **john@acme.com** as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:

setspn -s HTTP/ahsoka.acme.com john

Note: The LDAP account name used in the command above **MUST** match the account which you will specify by the **spnego.preauth.username** property in **web.xml**.

Note: This account will typically match the LDAP account specified by the administrator in the Acronis Access web interface at **General Settings -> LDAP -> LDAP Username / LDAP Password**, but this is not mandatory.

3. If your Access server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.

e.g. If your server is running on port 444, the command will be:

setspn -s HTTP/ahsoka.acme.com:444 john

*Note: The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.*

4. Go to the domain controller and open **Active Directory Users and Computers**.
5. Find the user that you used in the above commands (in this case - **john**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.
7. Press **OK**.

Configuring the SPN for the Gateway Server

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running `setspn` and specifying the hostname of the server on which it is running as the 'user' in the `setspn` command.

For this configuration to work, you will need to set an additional DNS entry for your Gateway server.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (**A record**) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
e.g. codygw.acme.com
3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Access Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.
5. Go back to the machine with Acronis Access.
6. Open the command prompt.
7. Enter the following `setspn` command: **`setspn -s HTTP/gatewaydns.domain.com computername`**
For example, if your gateway server is running on host '**cody**' in the domain and your DNS entry is **codygw.acme.com**, run this command:
`setspn -s HTTP/codygw.acme.com cody`
8. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
`setspn -s HTTP/codygw.acme.com:444 cody`
9. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created in step 4.

Setting the domain account that will be used for Single Sign-on authentication

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**
2. Find and open the file **web.xml**. In this file you will set the domain username and password that the SSO service will run under. This account **must** match the account that you used to register the HTTP service with Kerberos in the **On the Domain** section.
3. In **web.xml** there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

```

<init-param>
  <param-name>spnego.preauth.username</param-name>
  <param-value>yourusername</param-value>
</init-param>
<init-param>
  <param-name>spnego.preauth.password</param-name>
  <param-value>yourpassword</param-value>
</init-param>

```

4. Replace **yourusername** with the desired LDAP username.
5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, **'**, or **<**, you will have to properly escape them in the XML document. To do so, you will have to replace them with the following:

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

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

Setting the Kerberos domain lookup

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**
2. Find and open the file **krb5.conf**
3. In **krb5.conf** there are only two properties that are needed from the administrator:
 - a. The domain for single sign-on (e.g., **ACME.COM**). Please note that this is the name of your domain, **not** the DNS name of the server.

Note: The domain in **krb5.conf** must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

- b. The Kerberos Key Distribution Center's address (typically matches the address of your primary domain controller; e.g., **acmedc.ACME.COM**)
4. The **krb5.conf** file that we install looks like this:

```

[libdefaults]
    default_realm = ACME.COM
    default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
    default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
    permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc

[realms]
    ACME.COM = {

```

```
kdc = acmedc.ACME.COM
default_domain = ACME.COM
```

```
[domain_realm]
```

```
.ACME.COM = ACME.COM
```

5. Replace all instances of **ACME.COM** with your domain (**in uppercase!**). Please note that this is the name of your domain, **not** the DNS name of the server.
6. Replace the value for "**kdc =**" with the name of your domain controller. The domain must be written in uppercase. e.g. **kdc = yourdc.YOURDOMAIN.COM**
7. After the above configuration files are updated the Access Server (the Acronis Access Tomcat service) must be restarted in order for the changes to take effect.

Enabling Single sign-on in the web interface:

1. Open the Acronis Access web interface and log in as an administrator.
2. Expand the **General Settings** tab and open the **LDAP** page.
3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials**.
4. Press **Save**.

Note: These steps work only if the machines that will host the Gateway Servers are in the same domain as the Access Server.

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running `setspn` and specifying the hostname of the server on which it is running as the 'user' in the `setspn` command.

For any Gateway Servers that reside on a different machine from the Access Server

1. Open the command prompt.
2. Enter the following `setspn` command: **setspn -s HTTP/computername.domain.com computername**
For example, if you gateway server is running on host '**cody**' in the domain, run this command:
setspn -s HTTP/cody.acme.com cody
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
setspn -s HTTP/cody.acme.com:444 cody
4. Repeat this section for all additional Gateway servers.

On any user's machine

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

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

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

Windows:

For Internet Explorer:

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

For Chrome:

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

1. Open the registry editor (**regedit32.exe**)
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome**
3. Create the **Google\Chrome** keys if they don't already exist.
 - a. Right click on the Policies folder and select **New -> Key**.
 - b. Type in **Google** for the folder name.
 - c. Right click on the **Google** folder and select **New -> Key**.
 - d. Type in **Chrome** for the folder name.
 - e. Click on the Chrome folder and in the white panel on the right, right-click and select **New -> String Value**.
 - f. Enter the key name: **AuthNegotiateDelegateWhitelist**.
4. Set your domain name (e.g. **ahsoka.acme.com** or ***.acme.com**) as the value for the **AuthNegotiateDelegateWhitelist** registry key.
5. Restart Chrome.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

*Note: To add all subdomains use the format ".example.com" (NOT *.example.com)*

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

Mac:

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

For Safari:

It will just work.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

Note: To add all subdomains use the format **".example.com"** (NOT ***.example.com**)

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

For Chrome:

1. Using the **Ticket Viewer** application (**/System/Library/CoreServices/Ticket Viewer**), you can check if you have a Kerberos ticket and create one if it hasn't been created automatically.

Note: You also can create a ticket via the **Terminal** by entering **kinit** and then your password.

2. To configure Chrome's whitelist to allow authentication against any domains you will be using, open the **Terminal** and run the following commands:

```
$ defaults write com.google.Chrome AuthServerWhitelist "*.acme.com"  
$ defaults write com.google.Chrome AuthNegotiateDelegateWhitelist  
"*.acme.com"
```
3. Restart the Chrome browser.

13.2.6.2 Access and Gateway on separate machines

In this section

On any user's machine218

This is a one-time step that must be performed in order to register the Access Server with the Kerberos server on the domain. We will use 'setspn.exe' to specify which LDAP account will be queried for SSO authentication checks.

Note: If you want to use **mobile clients with certificate authentication**, the DNS entries for the Access and Gateway servers must **NOT** be the name of the computer. If the Access Server's SPN is just the name of the machine, the Gateway server will treat the Access Server as "on my machine", and will not attempt to perform Kerberos authentication.

e.g. **machineAccess.domain.com / machineGW.domain.com** will work

e.g. **machine.domain.com / computer.domain.com** will NOT work

Configuring the LDAP account that will handle SSO

Note: If you want to use **SMB or SharePoint Data Sources**, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources. For more information, please visit the **Advanced Delegation Configurations (p. 231)** article.

1. Open a command prompt.

Note: You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command **setspn -s HTTP/computername.domain.com account name**
e.g. If your Access server is installed on **ahsoka.acme.com** and you want to use **john@acme.com** as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:

setspn -s HTTP/ahsoka.acme.com john

Note: The LDAP account name used in the command above **MUST** match the account which you will specify by the **spnego.preauth.username** property in **web.xml**.

Note: This account will typically match the LDAP account specified by the administrator in the Acronis Access web interface at **General Settings -> LDAP -> LDAP Username / LDAP Password**, but this is not mandatory.

3. If your Access server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.

e.g. If your server is running on port 444, the command will be:

setspn -s HTTP/ahsoka.acme.com:444 john

Note: The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.

4. Go to the domain controller and open **Active Directory Users and Computers**.
5. Find the user that you used in the above commands (in this case - **john**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**.
7. Press **OK**.

Configuring the SPN for the Gateway Server

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running **setspn** and specifying the hostname of the server on which it is running as the 'user' in the **setspn** command.

For any Gateway Servers that reside on a different machine from the Access Server

1. Open the command prompt.
2. Enter the following **setspn** command: **setspn -s HTTP/computername.domain.com computername**
For example, if your gateway server is running on host '**cody**' in the domain, run this command:
setspn -s HTTP/cody.acme.com cody
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
setspn -s HTTP/cody.acme.com:444 cody
4. Repeat this section for all Gateway servers.

If there is a Gateway Server on the same machine as the Access Server

This is required only if you have a Gateway Server on the same machine as the Access Server. If you do not, skip this section. For this configuration to work, you will need to set an additional DNS entry for your Gateway server.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (**A record**) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
e.g. codygw.acme.com
3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Access Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.
5. Go back to the machine with Acronis Access.
6. Open the command prompt.
7. Enter the following **setspn** command: **setspn -s HTTP/gatewaydns.domain.com computername**

For example, if you gateway server is running on host 'cody' in the domain and your DNS entry is **codygw.acme.com**, run this command:

```
setspn -s HTTP/codygw.acme.com cody
```

8. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
setspn -s HTTP/codygw.acme.com:444 cody
9. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created in step 4.

Editing the web.xml file:

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**
2. Find and open the file **web.xml**. In this file you will set the domain username and password that the SSO service will run under. This account **must** match the account that you used to register the HTTP service with Kerberos in the **On the Domain** section.
3. In **web.xml** there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

```
<init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>yourusername</param-value>
</init-param>
<init-param>
    <param-name>spnego.preauth.password</param-name>
    <param-value>yourpassword</param-value>
</init-param>
```

4. Replace **yourusername** with the desired LDAP username.
5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, **'**, or **<**, you will have to

properly escape them in the XML document. To do so, you will have to replace them with the following:

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

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

Editing the krb5.conf file:

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**
2. Find and open the file **krb5.conf**
3. In **krb5.conf** there are only two properties that are needed from the administrator:
 - a. The domain for single sign-on (e.g., **ACME.COM**)

Note: The domain in **krb5.conf** must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

- b. The Kerberos Key Distribution Center's address (typically matches the address of your primary domain controller; e.g., **acmedc.ACME.COM**)
4. The **krb5.conf** file that we install looks like this:

```
[libdefaults]
    default_realm = ACME.COM
    default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
    default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc
    permitted_enctypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5
des-cbc-crc

[realms]
    ACME.COM = {
        kdc = acmedc.ACME.COM
        default_domain = ACME.COM

[domain_realm]
    .ACME.COM = ACME.COM
```

5. Replace all instances of **ACME.COM** with your domain (**in uppercase!**).
6. Replace the value for "**kdc =**" with the name of your domain controller. The domain must be written in uppercase. e.g. **kdc = yourdc.YOURDOMAIN.COM**
7. After the above configuration files are updated the Access Server (the Acronis Access Tomcat service) must be restarted in order for the changes to take effect.

Enabling Single sign-on in the web interface:

1. Open the Acronis Access web interface and log in as an administrator.
2. Expand the **General Settings** tab and open the **LDAP** page.
3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials**.
4. Press **Save**.

On any user's machine

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

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

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

Windows:

For Internet Explorer:

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

For Chrome:

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

1. Open the registry editor (**regedit32.exe**)
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome**
3. Create the **Google\Chrome** keys if they don't already exist.
 - a. Right click on the Policies folder and select **New -> Key**.
 - b. Type in **Google** for the folder name.
 - c. Right click on the **Google** folder and select **New -> Key**.
 - d. Type in **Chrome** for the folder name.
 - e. Click on the Chrome folder and in the white panel on the right, right-click and select **New -> String Value**.
 - f. Enter the key name: **AuthNegotiateDelegateWhitelist**.
4. Set your domain name (e.g. **ahsoka.acme.com** or ***.acme.com**) as the value for the **AuthNegotiateDelegateWhitelist** registry key.
5. Restart Chrome.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

*Note: To add all subdomains use the format ".example.com" (NOT *.example.com)*

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

Mac:

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

For Safari:

It will just work.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

*Note: To add all subdomains use the format ".example.com" (NOT *.example.com)*

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

For Chrome:

1. Using the **Ticket Viewer** application (**/System/Library/CoreServices/Ticket Viewer**), you can check if you have a Kerberos ticket and create one if it hasn't been created automatically.

*Note: You also can create a ticket via the **Terminal** by entering **kinit** and then your password.*

2. To configure Chrome's whitelist to allow authentication against any domains you will be using, open the **Terminal** and run the following commands:

```
$ defaults write com.google.Chrome AuthServerWhitelist "*.acme.com"  
$ defaults write com.google.Chrome AuthNegotiateDelegatedWhitelist  
"*.acme.com"
```
3. Restart the Chrome browser.

13.2.6.3 Acronis Access in a Domain Forest

As of Windows Server 2012, Microsoft have added Resource **Based Kerberos Constrained Delegation**, which allows cross-forest constrained delegation. This enables deployments to use Single sign-on

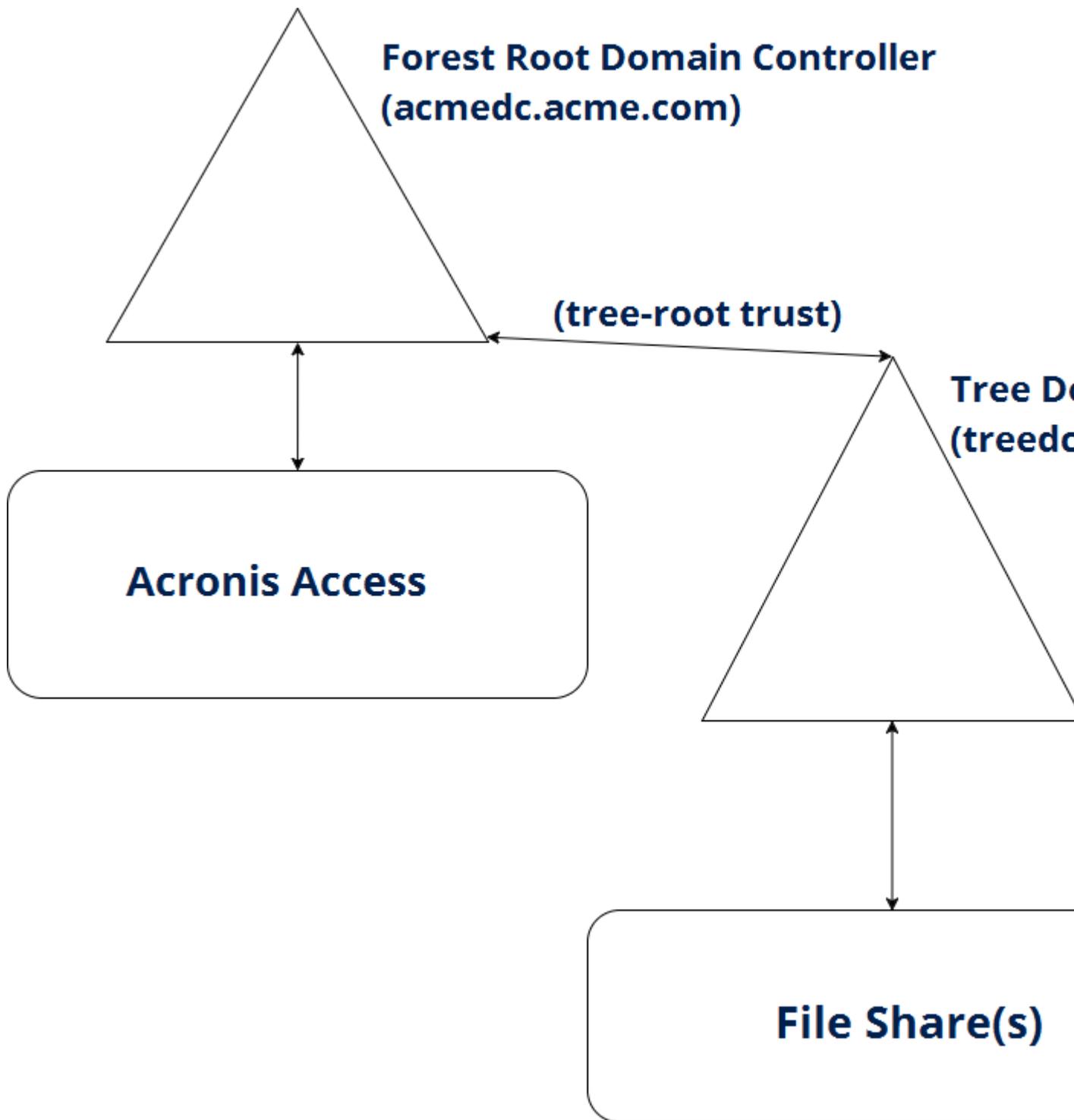
even if they have resources in multiple domains (within the same Forest), without having to install a Gateway server on the resources.

Note: *In order to make use of this feature, all of your domains in the forest must run in **domain functional level 2012** or higher.*

This article will guide you through:

- Setting up your Acronis Access server for SSO.
- Setting up your Gateway server(s) for SSO.
- All Configurations on your domain in order to get cross-forest constrained delegation working.

- The setup users have to do in order to use SSO.



In this section

Requirements.....222
 On any user's machine222
 For the Access Server223
 For the Gateway Server226

Requirements

This guide is intended for multi-domain configuration running in a single Forest. As such, we assume that your LDAP is properly configured, users can login to the domain without issue and that the connectivity between the domains inside the forest is properly configured.

- This type of Constrained Delegation is available only in domain controllers running in **domain functional level 2012** or higher. Windows Server 2012 is the first to allow Resource Based Kerberos Constrained Delegation.
- You need to have **Global Catalog** enabled and running.

On any user's machine

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

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

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

Windows:

For Internet Explorer:

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

For Chrome:

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

1. Open the registry editor (**regedit32.exe**)
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome**
3. Create the **Google\Chrome** keys if they don't already exist.
 - a. Right click on the Policies folder and select **New -> Key**.
 - b. Type in **Google** for the folder name.
 - c. Right click on the **Google** folder and select **New -> Key**.
 - d. Type in **Chrome** for the folder name.
 - e. Click on the Chrome folder and in the white panel on the right, right-click and select **New -> String Value**.
 - f. Enter the key name: **AuthNegotiateDelegateWhitelist**.
4. Set your domain name (e.g. **ahsoka.acme.com** or ***.acme.com**) as the value for the **AuthNegotiateDelegateWhitelist** registry key.
5. Restart Chrome.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

*Note: To add all subdomains use the format ".example.com" (NOT *.example.com)*

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

Mac:

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

For Safari:

It will just work.

For Firefox:

1. Type **about:config** in the address bar and press enter.
2. Find and edit the preference **network.negotiate-auth.trusted-uris** and add **https://ahsoka.acme.com** , or just **.acme.com**, [the list is comma-separated].

*Note: To add all subdomains use the format ".example.com" (NOT *.example.com)*

3. To enable Network **Data Sources** support, you will need to also edit **network.negotiate-auth.delegation-uris** by adding **ahsoka.acme.com** or just the domain name - **acme.com**.
4. Restart **Firefox**.

For Chrome:

1. Using the **Ticket Viewer** application (**/System/Library/CoreServices/Ticket Viewer**), you can check if you have a Kerberos ticket and create one if it hasn't been created automatically.

*Note: You also can create a ticket via the **Terminal** by entering **kinit** and then your password.*

2. To configure Chrome's whitelist to allow authentication against any domains you will be using, open the **Terminal** and run the following commands:

```
$ defaults write com.google.Chrome AuthServerWhitelist "*.acme.com"  
$ defaults write com.google.Chrome AuthNegotiateDelegatedWhitelist  
"*.acme.com"
```
3. Restart the Chrome browser.

For the Access Server

In this section

4.

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Access Server\Web Application\WEB-INF**
2. Find and open the file **web.xml**. In this file you will set the domain username and password that the SSO service will run under.

This account **must** match the account that you will use to register the **HTTP** service with Kerberos in the following sections, so we recommend writing it down.

3. In **web.xml** there are two properties that need to be set - the domain username and password that the SSO service will use. Find the following lines:

```
<init-param>
    <param-name>spnego.preauth.username</param-name>
    <param-value>yourusername</param-value>
</init-param>
<init-param>
    <param-name>spnego.preauth.password</param-name>
    <param-value>yourpassword</param-value>
</init-param>
```

4. Replace **yourusername** with the desired LDAP username.
5. Replace **yourpassword** with the LDAP password for the LDAP account specified above. If you have one of these five special characters in your password: **&**, **>**, **"**, **'**, or **<**, you will have to properly escape them in the XML document. To do so, you will have to replace them with the following:

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

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

1. Navigate to **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**
2. Find and open the file **krb5.conf**
3. In **krb5.conf** there are only two properties that are needed from the administrator:
 - a. The domain for single sign-on (e.g., **ACME.COM**).
 - This must be the domain where your Acronis Access Server and Gateway servers reside.
 - Please note that this is the name of your domain, **not** the DNS name of the server.

Note: The domain in **krb5.conf** must always be in **UPPERCASE** or Kerberos ticket lookups may fail.

- b. The Kerberos Key Distribution Center's address (typically matches the **DNS** address of your primary domain controller; e.g., **acmedc.ACME.COM**). This is the address of the domain controller in the domain where Acronis Access and its components reside.
4. The **krb5.conf** file that we install looks like this:

```
[Libdefaults]
    default_realm = ACME.COM
```

```
default_tkt_encypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5  
des-cbc-crc
```

```
default_tgs_encypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5  
des-cbc-crc
```

```
permitted_encypes = aes128-cts rc4-hmac des3-cbc-sha1 des-cbc-md5  
des-cbc-crc
```

```
[realms]
```

```
ACME.COM = {  
    kdc = acmedc.ACME.COM  
    default_domain = ACME.COM
```

```
[domain_realm]
```

```
.ACME.COM = ACME.COM
```

5. Replace all instances of **ACME.COM** with your domain (**in uppercase!**). Please note that this is the name of your domain, **not** the DNS name of the server.
6. Replace the value for "**kdc =**" with the DNS name of your domain controller. The domain portion must be written in uppercase. e.g. **kdc = yourdc.YOURDOMAIN.COM**
7. After the above configuration files are updated the Access Server (the Acronis Access Tomcat service) must be restarted in order for the changes to take effect.
 1. Open the Acronis Access web interface and log in as an administrator.
 2. Expand the **General Settings** tab and open the **LDAP** page.
 3. At the bottom of the page, enable the checkbox **Allow log in from the web client and desktop sync client using existing Windows/Mac login credentials**.
 4. Press **Save**.

Configure an additional DNS entry for your Access server

If you have a Gateway server on this machine, you must have a separate DNS entry for your Access Server.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (**A record**) for the Access server.
2. Enter a name. This will be the DNS address that will be used to reach the Access server.
e.g. ahsokaccess.acme.com
3. Enter the IP address of the Access Server (without the port). If you're running the Gateway and the Access Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.

Setting the SPN for the Access Server

1. On the machine where Acronis Access is running, open a command prompt.

Note: You must be logged in with a domain account and have the rights to use **setspn**

2. Enter the command **setspn -s HTTP/access_DNS_name.domain.com account name**

Note: The LDAP account name used in this command **MUST** match the account which you have specified in the `web.xml` file.

- e.g. If your Access server is installed on `ahsoka.acme.com` and you want to use `john@acme.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:
`setspn -s HTTP/ahsokaaccess.acme.com john`
- e.g. If your Access Server is installed on `ahsoka.acme.com` and you want to use `jane@tree.com` as the pre-authenticated LDAP account to grant Kerberos tickets, the command will look like this:
`setspn -s HTTP/ahsokaaccess.acme.com tree\jane`

Note: This account will typically match the LDAP account specified by the administrator in the Acronis Access web interface in the **LDAP settings**, but this is not mandatory.

3. If your Access server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number.

e.g. If your server is running on port 444, the command will be:

```
setspn -s HTTP/ahsokaaccess.acme.com:444 john OR
setspn -s HTTP/ahsokaaccess.acme.com:444 tree\jane
```

Note: The **HTTP** in the commands above refer to the **HTTP** service class, not the **HTTP** protocol. The **HTTP** service class handles both **HTTP** and **HTTPS** requests. You do not need to, and **should NOT**, create an SPN using **HTTPS** as a service class name.

4. Go to the domain controller where your users reside and open **Active Directory Users and Computers**. If you have multiple domains with users, open the one which contains the user used in the previous steps.
5. Find the user that you used in the above commands (in this case - **john** or **jane**).
6. Click on the **Delegation** tab and select **Trust this user for delegation to any service (Kerberos only)**. Enabling this setting allows the LDAP object to delegate authentication to any service. In our case that is the Gateway Server service.
7. Press **OK**.

Verify you can log into Access

1. Go to a machine other than your Domain Controller or your Acronis Access server.
2. Open your Acronis Access web console and use the link under the password field on the login page.

Note: You need to be logged into the machine with a domain user that was either invited to Access, has already logged in or is a member of a Provisioned LDAP group.

Note: You must complete the *On any user's machine* section in order for your browser to accept SSO requests.

For the Gateway Server

In this section

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the Gateway server, the gateway service must be registered with the KDC server by running **setspn**

and specifying the hostname of the server on which it is running as the 'user' used in the **setspn** command.

Configure an additional DNS entry for your Gateway server

In order for this configuration to work, you must have a separate DNS entry for your Gateway Server as well.

1. On your DNS server, open the **Forward Lookup Zones** for your domain, right-click and create a new **Host** entry (**A record**) for the Gateway server.
2. Enter a name. This will be the DNS address that will be used to reach the Gateway server.
e.g. codygw.acme.com
3. Enter the IP address of the Gateway Server (without the port). If you're running the Gateway and the Access Servers on the same IP address, enter that IP address.
4. Select **Create associated pointer (PTR) record** and press **Add Host**.

Configure the SPN for the local Gateway Server

1. Go to the machine with Acronis Access.
2. Open the command prompt.
3. Setup the SPN for the Gateway Server:
 - a. If your Gateway Server is running as the Local System account, the command is:
setspn -s HTTP/gatewaydns.domain.com computername
 - b. **setspn -s HTTP/codygw.acme.com cody**
For example, if you gateway server is running on host '**cody**' in the domain and your DNS entry is **codygw.acme.com**, run this command:
setspn -s HTTP/codygw.acme.com cody
 - c. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
setspn -s HTTP/codygw.acme.com:444 cody
4. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created (i.e. **codygw.acme.com**).

Verify that the SPNs were set correctly for the Gateway

1. If you have a local volume for the local Gateway, you can verify that the SPNs and delegation are working by logging in with SSO. This must be done on a machine other than the Acronis Access server and the Domain Controller, otherwise SSO will not work.
2. Browse the local Gateway Server's volume. If that works, you can proceed forward, otherwise please verify you have successfully configured the proper SPNs for the proper objects.

Note: If you try a volume on a remote file server, you should get an Access Denied error.

Note: This type of Constrained Delegation is available only in domain controllers running in domain functional level 2012R2 or higher. Windows Server 2012 is the first to allow cross-domain Kerberos Constrained Delegation.

You can use Resource Based Constrained Delegation to grant users access to file servers or other network resources located in another domain.

1. Go to the domain controller for the domain where your file server resides and open **PowerShell**.
2. If your Gateway Server is running as the **LocalSystem** account:
 - a. **\$computer1 = Get-ADComputer -Identity <gateway_server_computer> -server <domain_controller_for_this_domain>**
 e.g. **\$computer1 = Get-ADComputer -Identity cody -server dc.acme.com**
 This command gets the computer object for the gateway server, specifies the AD Domain Services instance to connect to and saves this information in the **\$computer1** variable.
 - b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount \$computer1**
 e.g. **Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount \$computer1**
 This command sets the property **Principals Allowed To Delegate To Account** of the file server computer object, to the computer object for the gateway server. This allows the gateway server's computer to delegate to the file server's computer.
3. If your Gateway Server is running as a **User Account**:
 - a. **\$user1 = Get-ADUser -Identity <logon_user_of_the_gateway_service> -server <domain_controller_for_this_domain>**
 e.g. **\$user1 = Get-ADUser -Identity jane -server dc.acme.com**
 This command gets the user object for the user that the gateway server runs as, specifies the AD Domain Services instance to connect to and saves this information in the **\$user1** variable.
 - b. **Set-ADComputer <file_server_computer> -PrincipalsAllowedToDelegateToAccount \$user1**
 e.g. **Set-ADComputer cody -PrincipalsAllowedToDelegateToAccount \$user1**
 This command sets the property **Principals Allowed To Delegate To Account** of the file server computer object, to the user object that the gateway server runs as. This allows the selected user to delegate to the file server's computer.
4. To verify the Gateway user account was added as an account allowed to be delegated credentials to, you can run the following:
Get-ADComputer <file_server_machine> -Properties PrincipalsAllowedToDelegateToAccount
 e.g. **Get-ADComputer omega -Properties PrincipalsAllowedToDelegateToAccount**
5. Repeat these steps for all your File Servers.

It will take some time for the delegation to be propagated – 10 to 15 minutes for small LDAP deployments and even more for larger structures.

Note: *These steps work only if the machines that will host the Gateway Servers are in the same domain as the Access Server.*

In order for the KDC ("Key Distribution Center") Kerberos server to be able to authenticate users to the gateway server, the gateway service must be registered with the KDC server by running **setspn** and specifying the hostname of the server on which it is running as the 'user' in the **setspn** command.

For any Gateway Servers that reside on a different machine from the Access Server

1. Open the command prompt.
2. Enter the following **setspn** command: **setspn -s HTTP/computername.domain.com computername**
 For example, if you gateway server is running on host '**cody**' in the domain, run this command:
setspn -s HTTP/cody.acme.com cody
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

```
setspn -s HTTP/cody.acme.com:444 cody
```

4. Repeat this section for all additional Gateway servers.

If you do not have access to **Resource Based Kerberos Constrained Delegation**, another way to configure SSO to remote shares and resources located in another domain is by installing a Gateway Server on a machine in that domain. This allows you to use regular Kerberos Constrained Delegation and **works on domains in functional level 2008**.

Install a Gateway Server on a machine in the desired domain

1. Download the Acronis Access installer and move it to the machine.
2. Start the Acronis Access installer, accept the license agreement and press **Next**.
3. Select **Custom...** installation and select only the Gateway Server's checkbox.
4. Press **Install**. After the installation finishes, close the installer.
5. In the **Configuration Utility**, set the IP address of the gateway and the port.

Make the Gateway service run as a User Account

1. Open **Control Panel** -> **Administrative Tools** -> **Services**.
2. Find the Acronis Access Gateway Server service, right-click on it and select **Properties**.
3. Select the **Log On** tab and select the **This account** radio button.
4. Select the User that the service will run as either by pressing **Browse** and searching or just by entering the username and password of the user. The user **must** be from the domain where Acronis Access is installed. We recommend using a dedicated account and not the one used for the Access Server's SPNs.
5. Press **OK** and can close the **Services** control panel. Do not restart the service yet, as without the necessary permissions for the user account, the service will not start.

Grant the selected User the necessary rights

1. In order for the service to run as a user, that user must be granted **Act as part of the operating system** and must be a part of the Local Administrators group.
2. Open the **Local Security Policy** and navigate to **Local Policies** -> **User Rights Assignment**. You may have to make this change in the **Group Policy Manager** depending on your deployment.
3. Open the **Act as part of the operating system** object and press **Add User** or **Group**.
4. Select the dedicated user for the Gateway service.
5. Close all open dialogs and open **Control Panel** -> **User Accounts** -> **Manage Accounts**.
6. Press **Add** and enter the domain and username of the dedicated account.
7. You can now restart the Acronis Access Gateway service in the **Services** control panel.

Configure the SPN for the remote Gateway Server

1. Go to any machine in the domain where the Acronis Access Server resides.
2. Open the command prompt.
3. To configure the SPN, the command is: **setspn -s HTTP/gatewaydns.domain.com useraccountfor_gw**

e.g. If your gateway server is running on host '**magpie**' in the **tree.com** domain and is running as the **peter** user account from the **acme.com** domain, run this command:

```
setspn -s HTTP/magpie.tree.com peter
```

If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:

```
setspn -s HTTP/magpie.tree.com:444 peter
```

4. If you haven't done so already, you have to change your desired Gateway Server's **address for administration** to be the Gateway Server DNS entry you created (i.e. **magpie.tree.com**).
5. Make sure that the Gateway Server has **Perform Negotiate/Kerberos authentication in user-mode** (p. 87) enabled. You have to restart the Acronis Access Gateway service after you enable this setting.
6. When creating **data sources** for the resources in the second domain, make sure to use the Gateway Server that resides in that domain.

e.g. If you want to grant your users access to the files on **repository.tree.com**, you will have to pick the gateway server that is located in **tree.com** (e.g. **magpie.tree.com**)

Verify that the SPNs were set correctly for the Gateway

1. If you have a local volume for the local Gateway, you can verify that the SPNs and delegation are working by logging in with SSO.
2. Browse the local Gateway Server's volume. If it doesn't work please verify you have successfully configured the proper SPNs for the proper objects.
3. Delegation changes might take some time to propagate (e.g. 10-15 minutes for small LDAP deployments and more for larger ones).

13.2.6.4 Verify that an SPN is registered

To query whether the desired SPN is registered properly:

1. Open an elevated command prompt.
2. Enter the **setspn -Q HTTP/computername.domain.com** command.
e.g. **setspn -Q HTTP/ahsoka.acme.com**
3. To query the SPNs registered to a particular domain user, use the **-l** (lowercase **L**) switch;
e.g. **setspn -l john**
4. After registering the SPN, before you can authenticate to it with SSO you will need to either reboot the client machine or run this command on the client machine:

```
klint purge
```

13.2.6.5 Using SMB or SharePoint Data Sources

If you want to use SMB or SharePoint Data Sources, you must configure the Active Directory account to permit Kerberos delegation to each of your SMB and SharePoint data sources.

For network shares and SharePoint servers, do the following:

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

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

2. Find the computer object corresponding to the Gateway server.

Note: *If you are running the Gateway server under a **User** account, select that **User** object instead.*

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

13.2.6.6 Using mobile clients with client certificate authentication

This is an additional step that you have to perform. You need to set up delegation from the Gateway Server to the Access Server regardless if they are on the same machine or not.

Kerberos Constrained Delegation

This type of delegation will work if the Access Server and the Gateway Server are in the same domain.

1. To do this, open the Active Directory on the domain controller.
2. Find and edit the Gateway server's computer object and go to the delegation tab.
3. Select **Trust this computer for delegation to specified services only** and **Use any authentication protocol**.
4. To select the Access Server's SPN, click Add and enter the username of the account that's associated with the Access Server's **HTTP** SPN.

Note: *Do not search for the computer that the Access Server is running on - you'll have to do the lookup by username.*

Note: *Kerberos authentication to the Access Server is not compatible with single port mode.*

5. Once you search for the user, you should see the **HTTP** services, so select them (there might be two if you registered the SPN twice - once with the port and once without).
6. Press **Apply** and close all dialogs.

Resource Based Kerberos Constrained Delegation

This type of delegation will work even if the Access and Gateway servers are in separate domains in a domain forest.

Note: In order to make use of this feature, all of your domains that Acronis Access will have access to must run in **domain functional level 2012** or higher.

1. Double-check that the DNS entry dedicated for the Access Server and for which you have set an SPN is in fact set as the address for your S&S volume in the Data Sources page.
2. Configure delegation between the Gateway Server and the Access Server. This time the delegation will be from the Gateway Server to the Access Server.
3. Execute the following commands for the following users:

```
$pc1 = Get-ADComputer -Identity <name_of_gateway_machine>
```

```
Set-ADUser <Access_SSO_user_account> -PrincipalsAllowedToDelegateToAccount $pc1
```

```
e.g: $pc1 = Get-ADComputer -Identity ahsoka
```

```
Set-ADUser john -PrincipalsAllowedToDelegateToAccount $pc1
```

4. If your Gateway is running as a user account you will need to set the delegation to be between the two user accounts, with the following commands:

```
$user1 = Get-ADUser -Identity <Gateway_User_Account>
```

```
Set-ADUser <Access_SSO_user_account> -PrincipalsAllowedToDelegateToAccount $user1
```

```
e.g: $user1 = Get-ADUser -Identity gwuser
```

```
Set-ADUser john -PrincipalsAllowedToDelegateToAccount $user1
```

It will take some time for the delegation to be propagated – 10 to 15 minutes for small LDAP deployments and even more for larger structures.

13.2.6.7 For Load Balanced environments

The Gateway Server has the option to perform all HTTP authentication in user mode rather than have the web server attempt to do Kerberos/Negotiate authentication. This is required to get SSO working for the Gateway(s) running behind a load balancer.

To enable this feature, Open the web interface and go to **Mobile Access -> Gateway Servers**, click the **Edit** option in the cluster group, go to **Advanced** and enable the checkbox "**Perform Negotiate/Kerberos authentication in user-mode**"

Enabling Network Nodes

In order to be able to access Network nodes in the Web, while using SSO, several changes will be required. Since the Gateway Servers are running behind a load balancer, registering with Kerberos will need to happen with a user account, not computer name.

For this to work, the gateway services will need to run under a user account. You can either use the same LDAP user under which the Access Tomcat server is registered, or you can select a new one, dedicated to your Gateway services.

Either way, the user you choose will need to be given the right to act as part of the operating system on the machines where the Gateway Servers are installed.

Selecting a user to act as part of the operating system

1. On the machine with the Gateway server, click **Start -> Run**
2. Type **gpedit.msc** and press **OK**

3. Expand **Windows Settings** and expand **Security Settings**.
4. Expand **Local Policies** and click on **User Rights Assignment**.
5. Right-click on **Act as part of the operating system** in the list and select **Properties**.
6. In this window, you can add users and groups or remove them. Enter the desired username and press OK.
7. Close all remaining windows and restart the server for the change to take effect.

Running the Gateway Server's service as the selected user account

Once you have added the user you will be running the service as, you must set the Gateway service to run as them. To do so, complete the following steps:

1. On the machine where the Gateway Server is installed, click **Start** and select **Run**.
2. Type in **services.msc** and click **OK**. Alternatively, open the **Control Panel** and go to **Administrative Tools** -> **Services**.
3. Right-click **Acronis Access Gateway** in the list and select **Properties**.
4. Click on the **Log On** tab.
5. Select the radio button for **This account:** and enter the credentials of the user you granted operating system rights to.
6. Click **OK** and close all windows

Configuring the SPNs for the Gateway Cluster

In order for the Key Distribution Center Kerberos server to be able to authenticate users to the gateway cluster, each Gateway Server and the load balancer for the Gateways must be registered with the KDC server by running **setspn** and specifying the account name as which the service will be running as.

1. Open the command prompt.
2. Enter the following command:
setspn -s HTTP/computername.domain.com username
 For example, if you gateway service is running as user **john**, the command will be:
setspn -s HTTP/gatewayserver1.acme.com john
3. If your gateway server is running on a non-default port (i.e., a port other than 443), you should also register an SPN using the port number; e.g., if your gateway server is running on port 444:
setspn -s HTTP/gatewayserver1.acme.com:444 john
4. Repeat these steps for each Gateway Server and for the load balancer. The SPN for the load balancer should look like this:
setspn -s HTTP/gwloadbalancerdns.acme.com john
 - Desktop or Web client users must be on a separate machine from the one running the Access Server (but in the domain) or SSO will not work.
 - You must access the server using the exact same FQDN as the SPN is using; e.g., **https://ahsoka.acme.com** . You cannot use other DNS names or IP addresses e.g., **https://localhost** or **https://10.20.56.33**.
 - Verify that you can log in to the Access Server without using SSO by entering the exact same LDAP credentials as your client windows machine uses. This will verify that your account credentials are valid for Acronis Access regardless of SSO configurations.

- Verify that you can access all Data sources without using SSO and using the same credentials as your LDAP login account.
- If you are unable to log in via SSO, double-check that you have configured your Web browser for SSO to the FQDN to which you are connecting, and you are logged in on your client machine using a domain account.
- Single Sign-On will not work if the Acronis Access Server is running on the Domain Controller.
- Acronis Access will not work with SSO if you are trying to access it from the machine that is the Domain Controller.

Note: Due to how Kerberos works, you cannot authenticate via SSO from a client application or Web browser running on the Domain Controller or the Access server.

Additionally, the Access server cannot authenticate to the Domain Controller when the Access server is running on the Domain Controller.

- If you get a **401 Error** when trying to log in using SSO, check the username and password in the **web.xml** file and make sure that any special characters are escaped properly. The special characters are: **&**, **>**, **"**, **'**, or **<**, for information on how to escape them, please see **step 5** of the **Editing the web.xml file** section.

13.2.7 Monitoring Acronis Access with New Relic

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

1. Open <http://newrelic.com/> and create a New Relic account or log in with an existing account. Once that is done, proceed with your Application configuration.
2. For Application Type select **APM**.
3. For platform, select **Ruby**.
4. Download the New Relic script shown in Step 3 of the New Relic Starting Guide (`newrelic.yml`).
5. Open your Acronis Access web console.
6. Navigate to **Settings -> Monitoring**.
7. Enter the path to the `newrelic.yml` including the extension (e.g `C:\software\newrelic.yml`). We recommend you put this file in a folder outside of the Acronis Access folder so that it will not be removed or altered on upgrade or uninstall.
8. Click **Save** and wait a couple of minutes or until the **Active application(s)** button becomes active on the New Relic site.
9. If more than 10 minutes pass, restart your Acronis Access Tomcat service and wait a couple of minutes. The button should be active now.
10. You should be able to monitor you Acronis Access server via the New Relic website.

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

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

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

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

If you want to monitor the actual computer as well

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

13.2.8 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.*

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

Note: *If prompted by your vendor to select a server type, choose IIS. The certificates must be installed in the Windows Certificate Store before Acronis Access can use them.*

Generating a certificate request via IIS:

For more information on this procedure, please refer to the following Microsoft Knowledge Base article: [http://technet.microsoft.com/en-us/library/cc732906\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx)

Generating a certificate request via OpenSSL:

Note: *For this guide you need to have OpenSSL installed.*

Note: *Contact your preferred certificate vendor for more information or help with this procedure.*

To generate a pair of private key and public Certificate Signing Request (CSR) for the web server "AAServer":

1. Open an elevated command prompt and enter the following command:

```
openssl req -new -nodes -keyout myserver.key -out AAServer.csr -newkey rsa:2048
```

This creates a two files. The file **myserver.key** contains a private key; do not disclose this file to anyone. Be sure to backup the private key, as there is no means to recover it should it be lost. The private key is used as input in the command to generate a **Certificate Signing Request (CSR)**.

Note: *In case you receive this error: **WARNING: can't open config file: /usr/local/ssl/openssl.cnf** run the following command: **set OPENSSL_CONF=C:\OpenSSL-Win64\bin\openssl.cfg** change the path, depending on where you installed OpenSSL. After you have completed this procedure, attempt step 1 again.*

2. You will now be asked to enter details to be entered into your CSR. Use the name of the web server as **Common Name (CN)**. If the domain name is **mydomain.com** append the domain to the hostname (use the fully qualified domain name).
3. The fields email address, optional company name and challenge password can be left blank for a web server certificate.
4. Your CSR will now have been created. Open the **server.csr** in a text editor and copy and paste the contents into the online enrollment form when requested by the certificate vendor.

Requirements

The certificate you are using must contain its private key. The certificate file must be in either the **.PFX** or **.P12** format. It doesn't matter which one since **.PFX** is the predecessor of **.P12** and the data inside is usually stored in the same format making them interchangeable.

Note: If your Certificate Vendor provided you with a certificate and a key as two separate files, you can combine them into one **.PFX** file with the following command:

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

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

This command requires OpenSSL to be installed.

Installing your certificate to your Windows certificate store

Note: If your Access and Gateway Servers are using different certificates, repeat these steps for both.

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

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

14. If the certificate has a password, type the password on the **Password** page, and then click **Next**.
15. Check the following boxes:
 - a. **Mark this key as exportable**

b. **Include all extended properties**

16. On the **Certificate Store** page, click **Place all certificates in the following store**, and then click **Next**.
17. Click **Finish**, and then click **OK** to confirm that the import was successful.

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

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. There should be a shortcut in the Windows Start menu.

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

2. On the **Access Web Server** tab, press the [...] button and select your certificate from the list.
3. On the **Access Mobile Gateway** tab, press the [...] button and select your certificate from the list.
4. Click **Apply**. This will restart the web services and after about a minute they should be back online and using your certificate. You can check to confirm they are serving the correct certificates.

If the Certificate Authority has issued you an Intermediate certificate along with your certificate, it must also be added to the Acronis Access Server through the Configuration Utility.

Note: The Configuration Utility only searches in the **Intermediate Certificates** certificate store. If your certificate was installed in one of the other stores, open **certmgr.msc** and move your Intermediate certificate from the store it is in, to the **Intermediate Certification Authorities -> Certificates** store.

1. Launch the Acronis Access Configuration Utility. There should be a shortcut in the Windows Start menu.

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

2. On the **Access Web Server** tab, press the [...] button and select your certificate from the list.
3. Press the plus (+) button next to the **Chain Certificate** field and select the **intermediate certificate** you wish to use from the list. If the desired certificate is not in the list, please check if it was properly installed and which store it was installed in.
4. On the **Access Mobile Gateway** tab, press the [...] button and select your certificate from the list. No additional steps are required for intermediate certificates.
5. Click **Apply**. This will restart the service and after it comes back online, you can check to confirm it is serving the selected certificates.

13.2.9 How to support different Access Desktop Client versions

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

1. Download the version of Access Desktop Client which you want to use. Make sure you have these 4 files:

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

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

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

Note: Before proceeding, please log-in to the web interface 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.

The service is running as the Local System account

1. Go to the machine on which Acronis Access is installed.
2. Stop the **Acronis Access File Repository Server** and **Acronis Access Tomcat** services.
3. You will find the current **FileStore** in the folder which you selected with the **Configuration Utility**. The default location is **C:\ProgramData\Acronis\Access\FileStore**.
4. Copy or move the entire **FileStore** folder with all of its contents to the desired location.
e.g. **D:\MyCustom Folder\FileStore**

Note: If the **File Store** is on a remote network share, the computer on which the **File Repository** service is running must have full permissions to the **File Store** folder on the network share.

5. Open the **Configuration Utility**.
6. In the **File Repository** tab, change the path of the **FileStore** to the new path where you've moved the **FileStore** folder.
7. 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. 110) settings.
8. Start **Acronis Access File Repository Server** service.
9. Start the **Acronis Access Tomcat** service and close the **Services** control panel.

The service is running as a User account

1. Go to the machine on which Acronis Access is installed.

2. Stop the **Acronis Access File Repository Server** and **Acronis Access Tomcat** services.
3. You will find the current **FileStore** in the folder which you selected with the **Configuration Utility**. The default location is **C:\ProgramData\Acronis\Access\FileStore**.
4. Copy or move the entire **FileStore** folder with all of its contents to the desired location.
e.g. **D:\MyCustom Folder\FileStore**
5. Open the **Configuration Utility**.
6. In the **File Repository** tab, change the path of the **FileStore** to the new path where you've moved the **FileStore** folder.
7. 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. 110) settings.
8. If the **File Store** is on a remote network share, the user account as which the **File Repository** service is running must have full permissions to the **File Store** folder on the network share.
9. The account must also have read and write access to the local **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 and close the **Services** control panel.

13.2.11 Running Acronis Access Tomcat on multiple ports

While the Configuration Utility supports setting the Tomcat service to only one port, Tomcat itself can be configured to run on multiple ports. This can be done by adding additional Connectors with the desired ports in the Tomcat server.xml file. Upgrades and restarting the Tomcat service using the CU will not affect the new connectors.

Note: We recommend performing this configuration after you have already run the Configuration Utility once and the Tomcat service has started successfully.

Configuring an additional Tomcat Connector

1. Stop the Acronis Access Tomcat service if it is running.
2. Navigate to and open the **server.xml** file. By default it is located at **C:\Program Files (x86)\Acronis\Access\Common\apache-tomcat-7.0.59\conf**.

Note: The number in the path (7.0.59) might be different depending on your version of Tomcat.

3. Browse the file until you see the **Connector** section that looks like this:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="$${catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="443"/>
```

Note: Depending on your text editor, you will most likely see the code above displayed in a single line when you open **server.xml**.

Note: If you have selected a port other than **443** in the **Configuration Utility**, your **Connector** will have that port listed in the example shown above.

4. Copy the entire **Connector** section and paste the copy right below the original one. Both sections should be on the same level of indentation.
5. Replace **443** (or whatever port you have chosen in the **Configuration Utility**) with the desired second port that Tomcat will run on. e.g.:

```
<Connector maxHttpHeaderSize="65536" maxThreads="150"
enableLookups="false" disableUploadTimeout="true" acceptCount="100"
scheme="https" secure="true" SSLEnabled="true"
SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" SSLCertificateFile="$
{catalina.base}/conf/AAServer_LocalHost.crt"
SSLCertificateKeyFile="{catalina.base}
/conf/AAServer_LocalHost.key" SSLHonorCipherOrder="true"
SSLCipherSuite="ECDH+AESGCM:ECDH+AES256:ECDH+AES128:RSA+AESGCM:RSA+AES:
!aNULL:!eNULL:!LOW:!3DES:!RC4:!MD5:!EXP:!PSK:!SRP:!DSS"
connectionTimeout="-1" URIEncoding="UTF-8" address="0.0.0.0" port="4430"/>
```

Note: Make sure that the code for the new **Connector** is written the same way as the existing one. i.e. if the old one is written as a single line, make sure the new one is as well.

6. Open the Acronis Access web interface and navigate to **General Settings** -> **Server Setting**.
7. In the **Web Address** field make sure that the address provided is using one of the ports for the Connectors. This is the address users will see in email invites and you can choose only 1 port for it.

13.2.12 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 2008 (R2) Microsoft Failover Cluster	240
Installing Acronis Access on a Windows 2012 (R2) Microsoft Failover Cluster	254

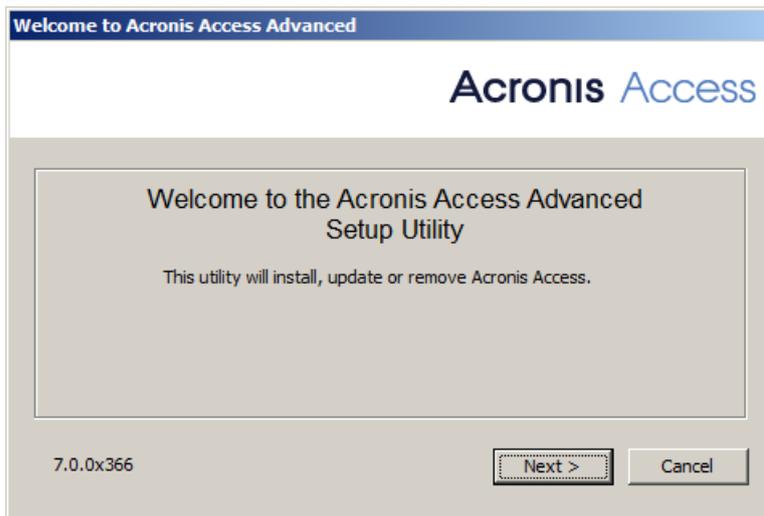
13.2.12.1 Installing Acronis Access on a Windows 2008 (R2) Microsoft Failover Cluster

Installing Acronis Access

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

1. Download the Acronis Access installer.

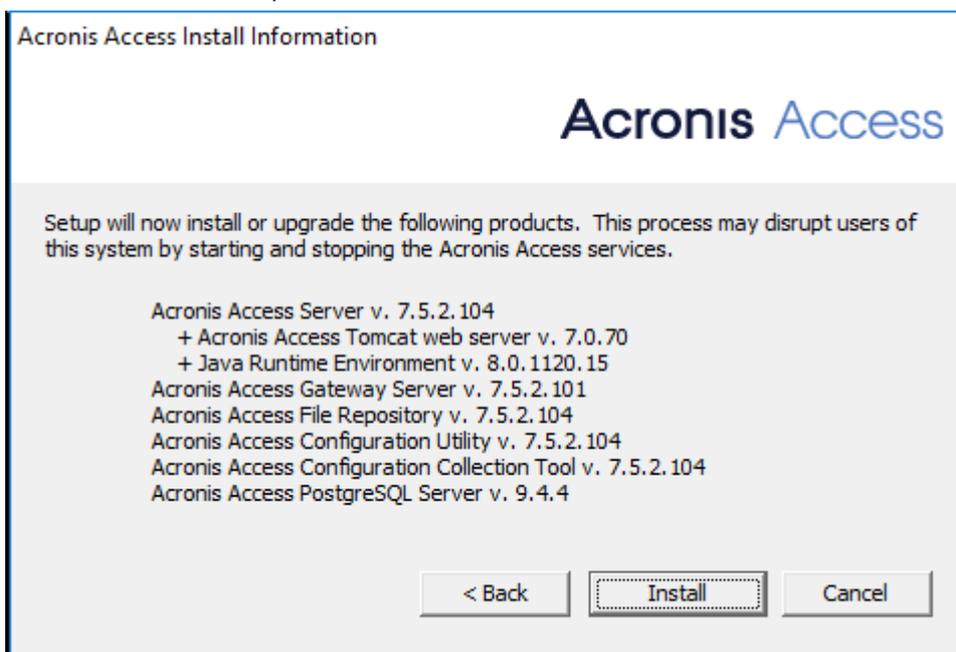
2. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
3. Double-click on the installer executable.



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

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



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

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

Local PostgreSQL Configuration

Acronis Access

PostgreSQL Install Location:

Data Path: S:\PSQL Browse...

PostgreSQL Super-User Credentials:

PostgreSQL Super-User password: *****

Re-enter password: *****

PostgreSQL Port: 5432

Open this port in the firewall for remote access:

< Back Next > Cancel

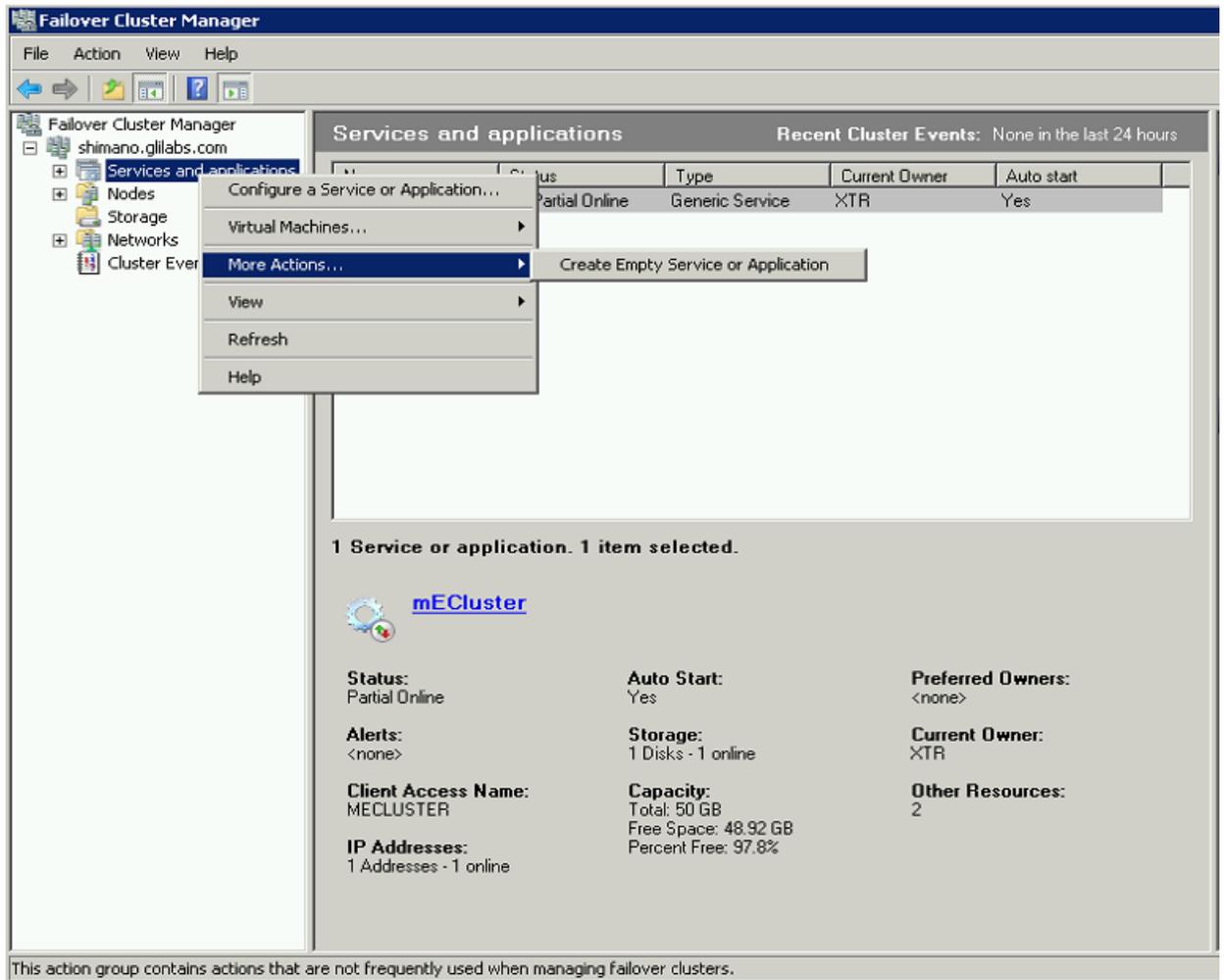
9. A window displaying all the components which will be installed appears. Press **OK** to continue.

When the Acronis Access installer finishes, press Exit.

Creating the Service group

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

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



Configurations on the Active node

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

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

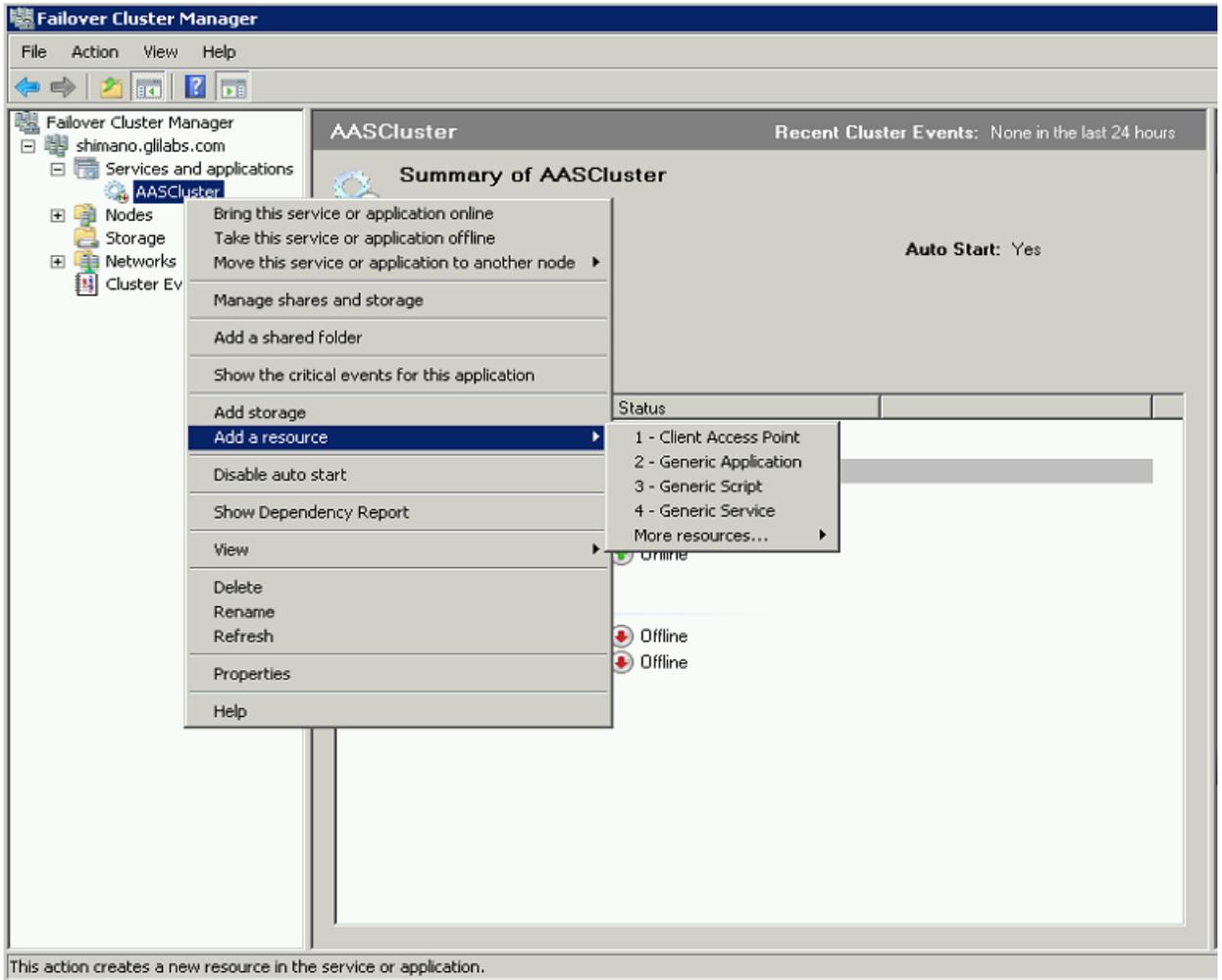
Note: You can copy the configured database.yml from the first node and paste it to the second node.

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

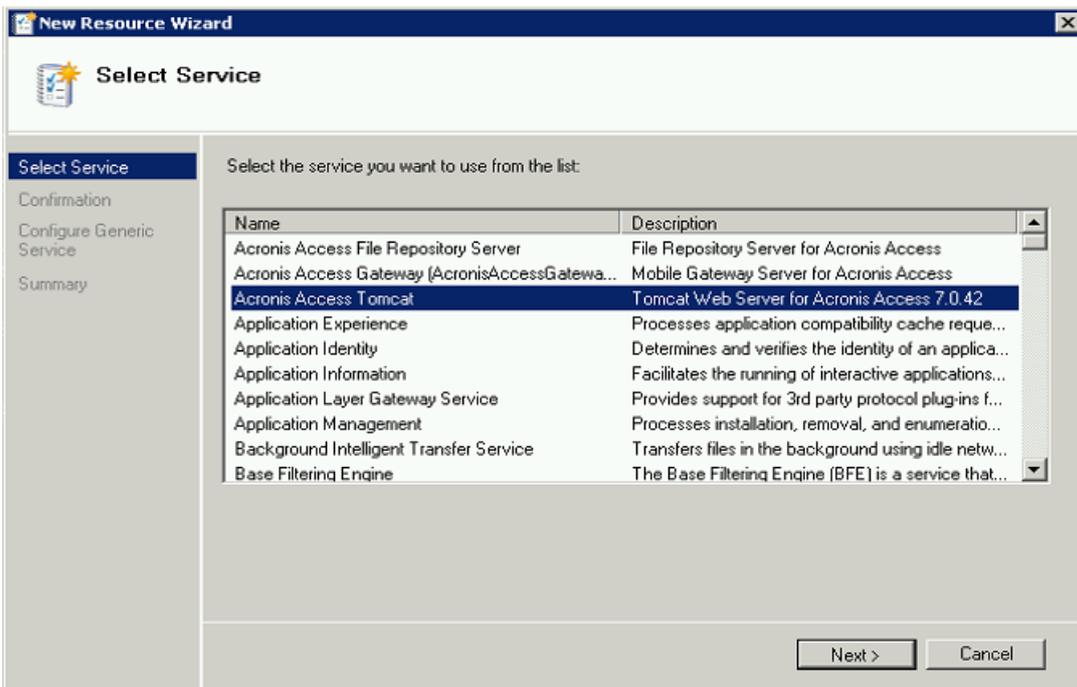
Complete the following procedure for each of the following services: AcronisAccessGateway, AcronisAccessPostgreSQL (this may be different depending on the version of Acronis Access), AcronisAccessRepository and AcronisAccessTomcat

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

2. Select **Generic Service**.



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

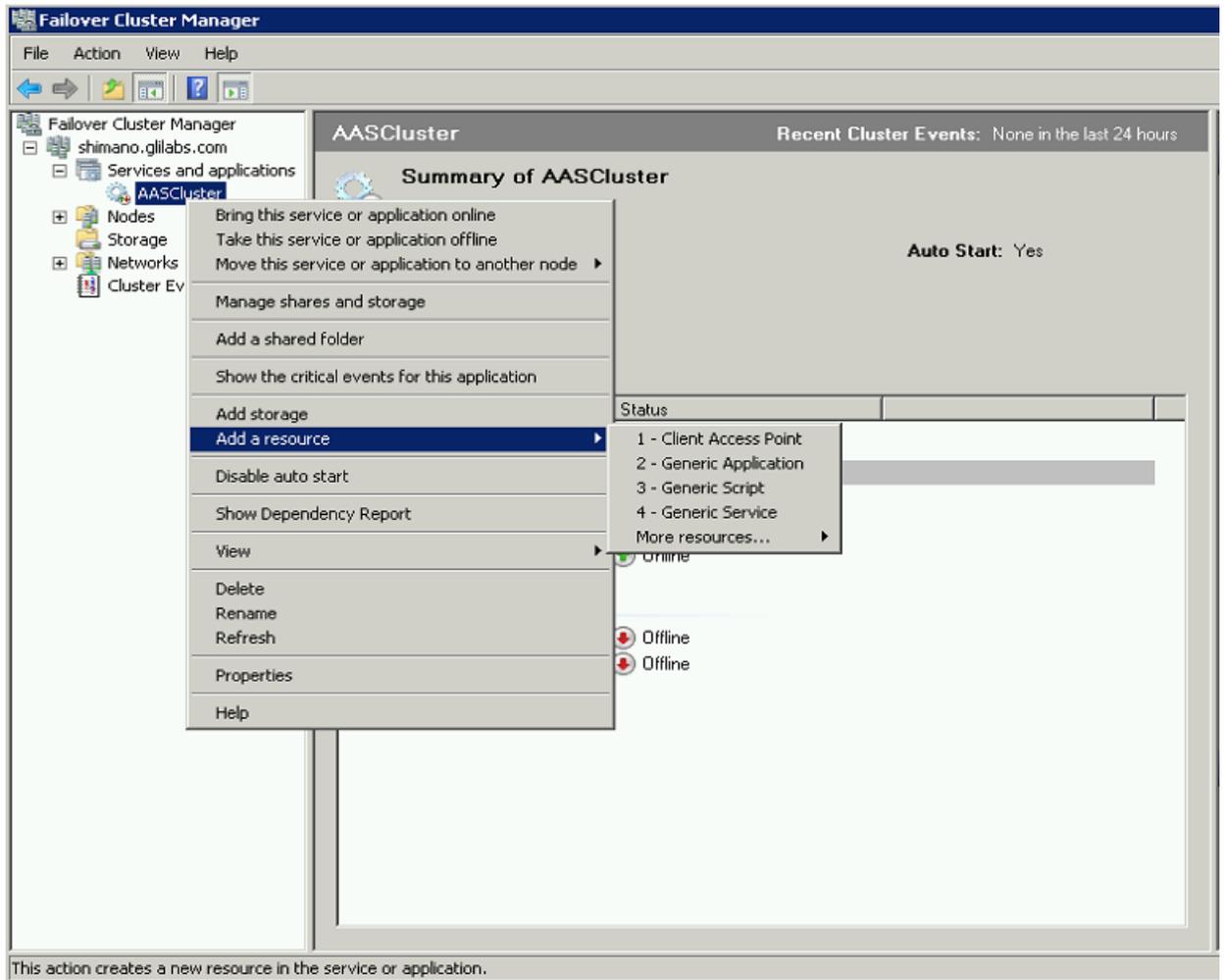


4. On the confirmation window press **Next**.

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

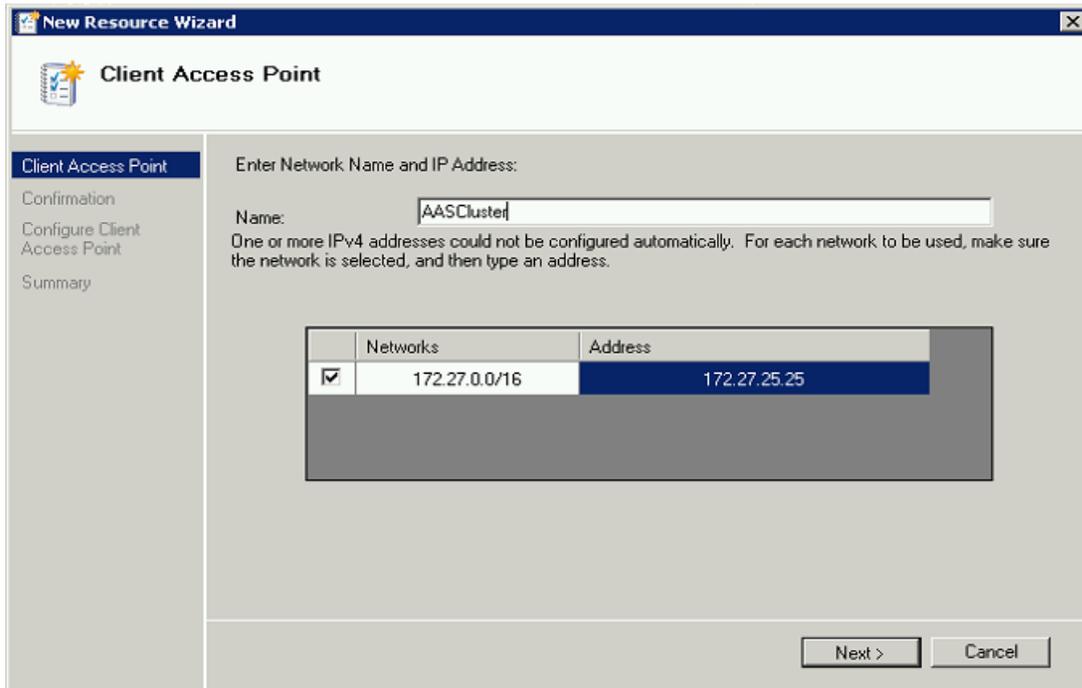
Setting a Client Access Point

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



3. Enter a name for this access point.

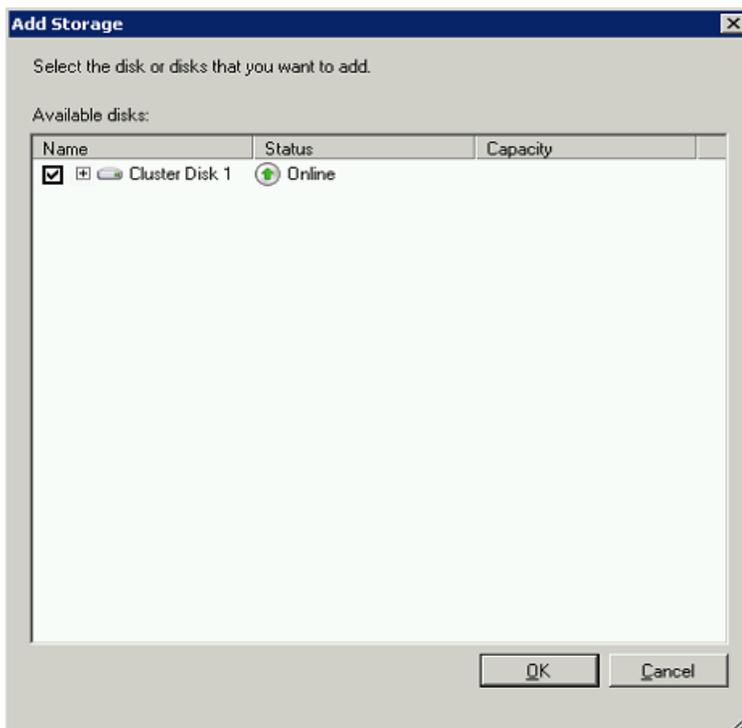
4. Select a network.



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

Adding a shared disk

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



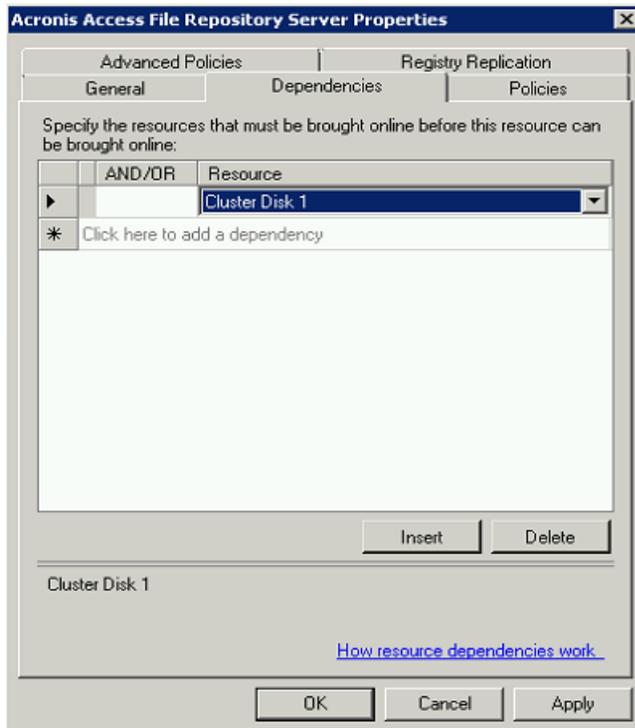
3. On the Confirmation window press **Next**.
4. On the summary window press **Finish**.

Configuring dependencies

1. Double click on the Acronis Access Service group.

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

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

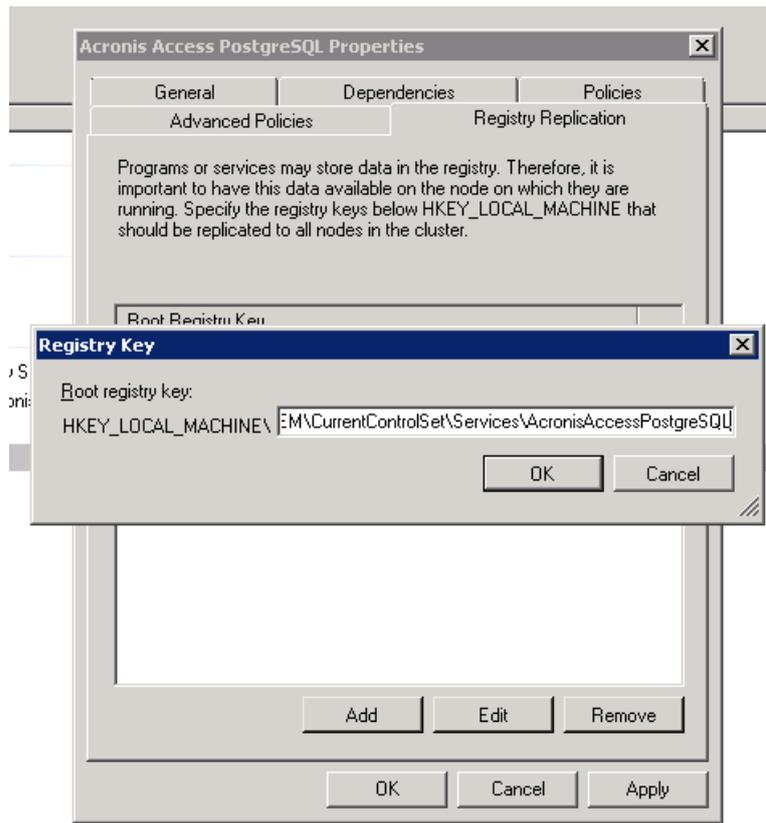


4. Press **Apply** and close the window.

For PostgreSQL also do the following:

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

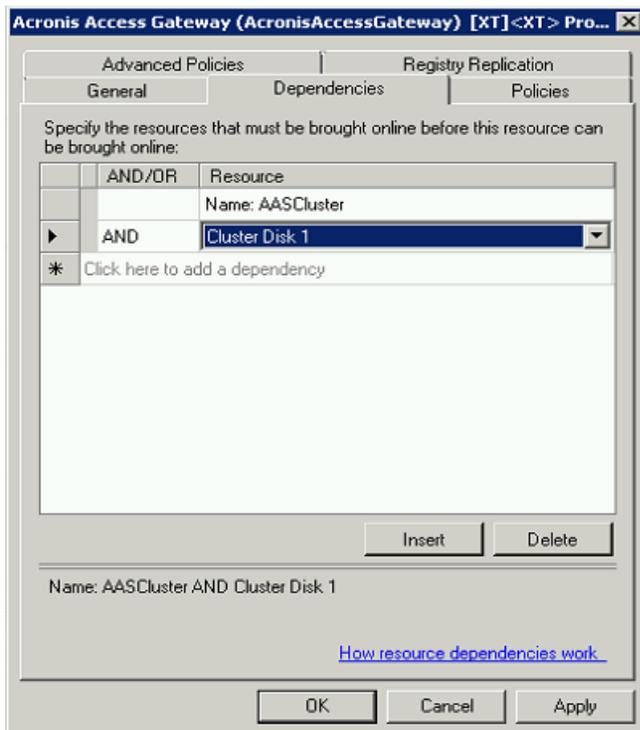
2. Press **Add** and enter the following:
SYSTEM\CurrentControlSet\Services\AcronisAccessPostgreSQL(For older versions of Acronis Access the service may be different. e.g. **postgresql-x64-9.2**)



For the Acronis Access Gateway Server service do the following:

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

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

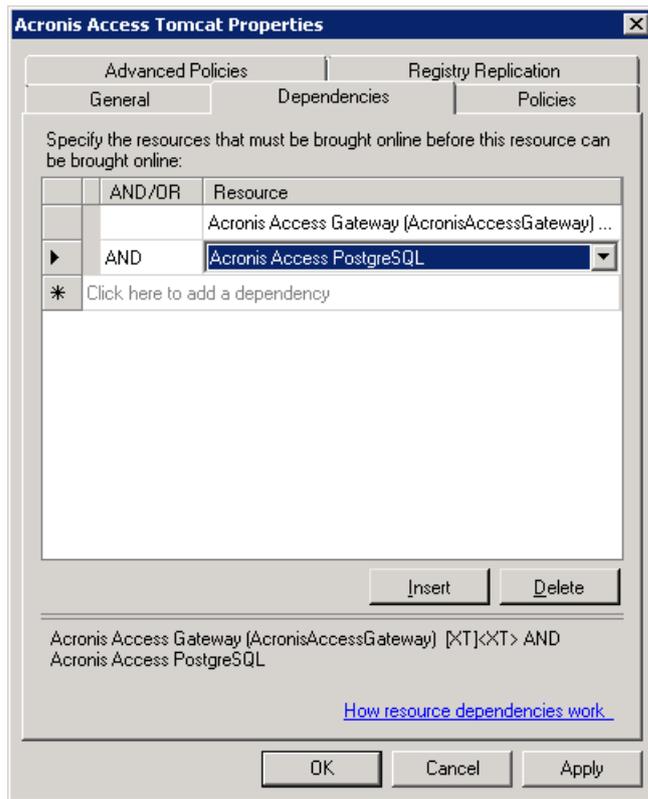


4. Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

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

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

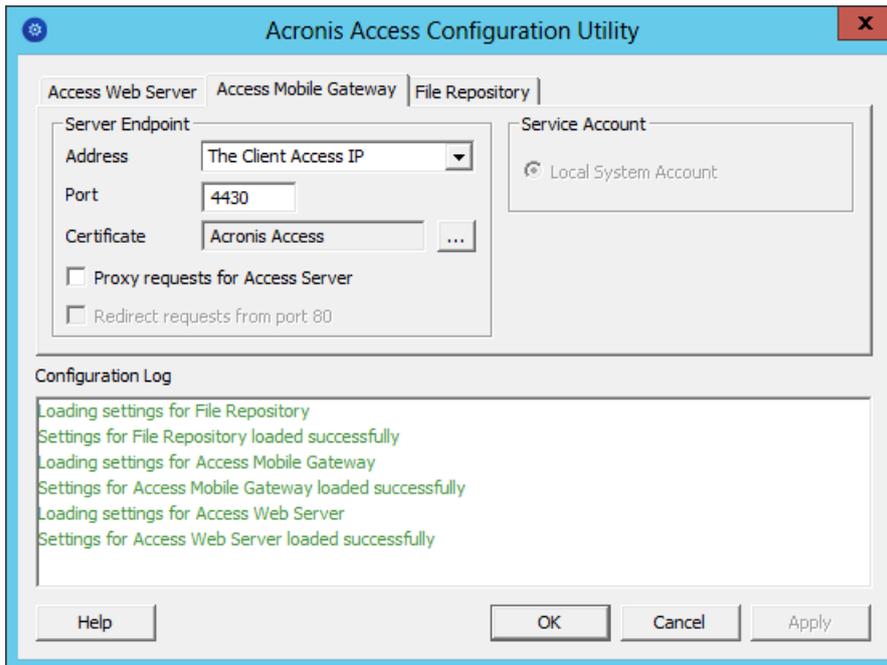


Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access Service group and set it as a dependency for the network name.

Bringing the service group online and using the Configuration Utility

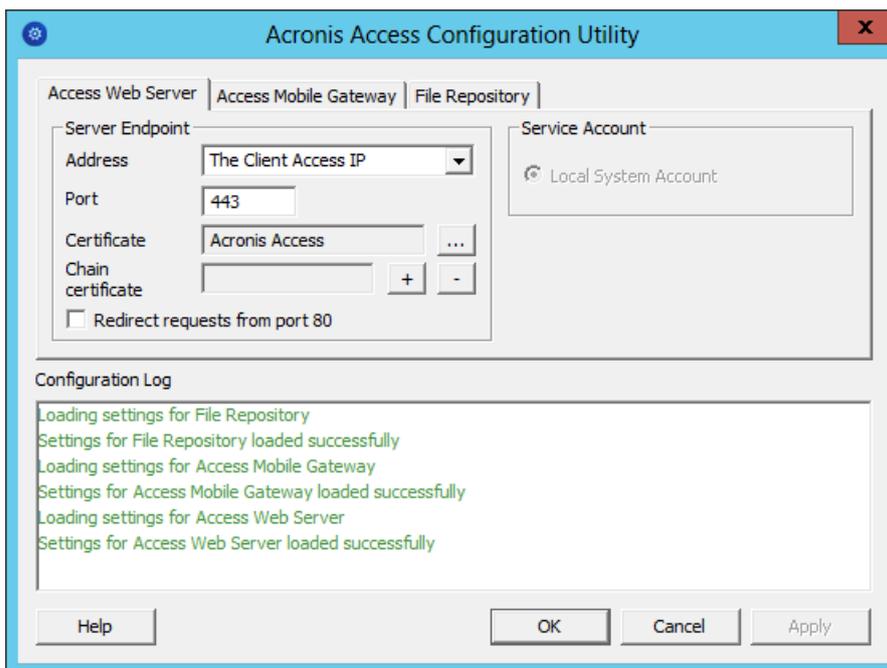
1. Right-click on the Acronis Access service group and press **Bring this application or service group online**.
2. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

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

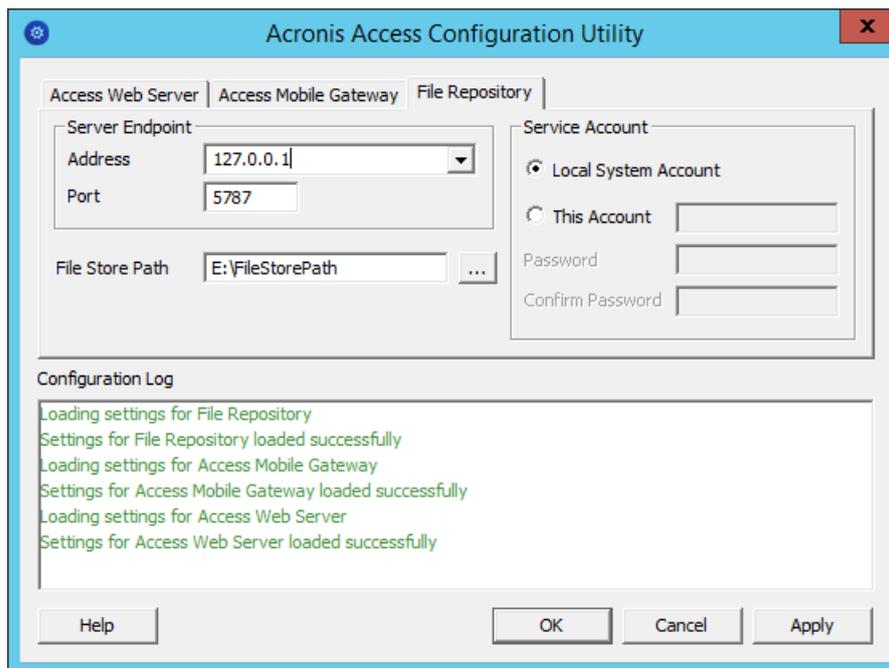


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.



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



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

Installation and configuration on the second node

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

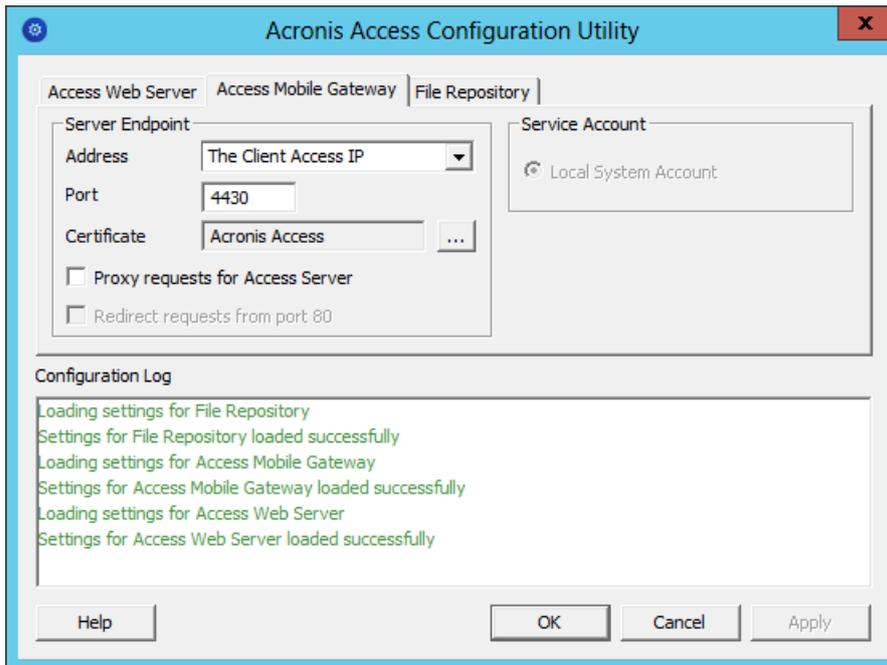
Note: Use slashes(/) as a path separator.

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

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

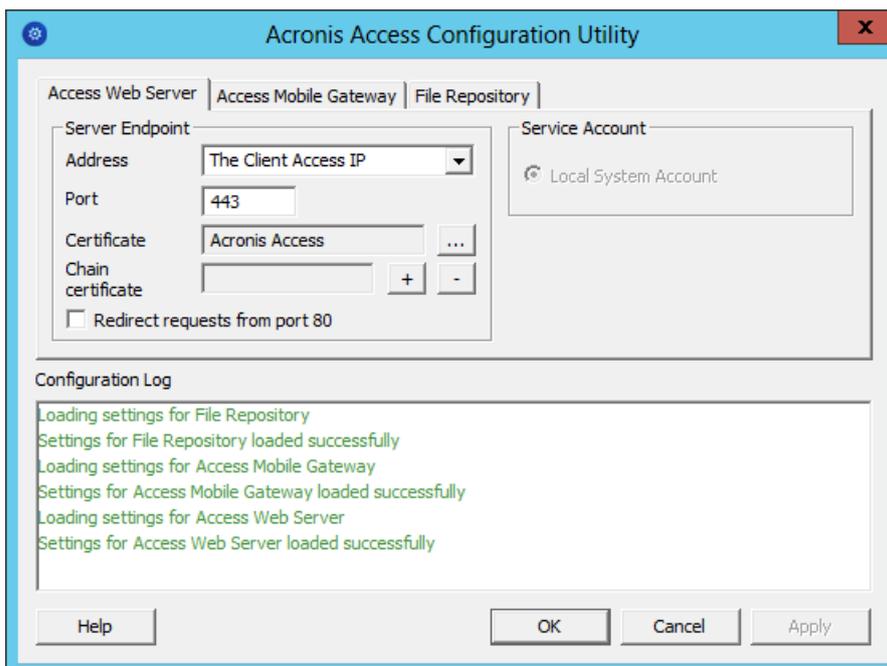
- Move the Acronis Access service group to the second node. To do so, right-click on the service group and click on **Move to the second node**.
- Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

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

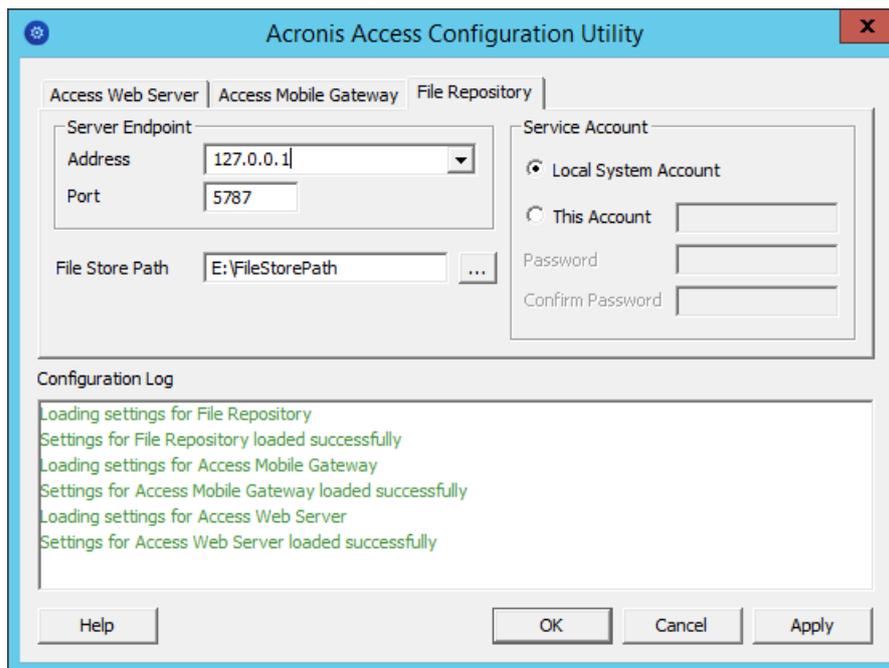


8. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.



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



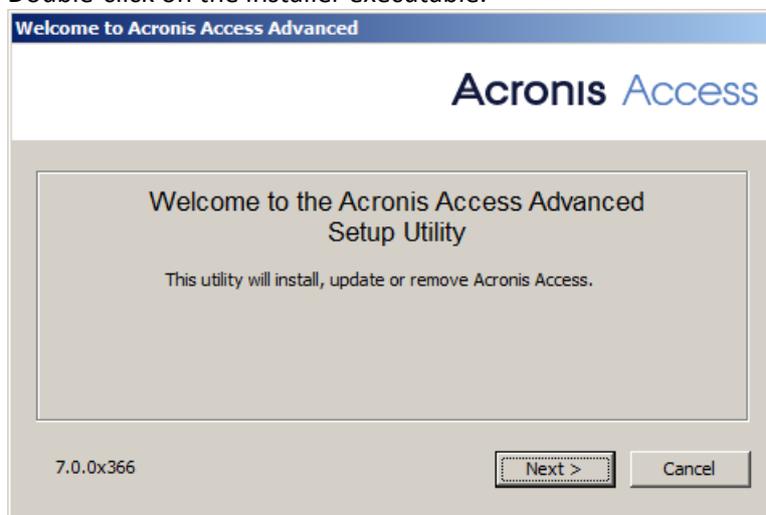
- Click **OK** to complete the configuration and restart the services.

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

Installing Acronis Access

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

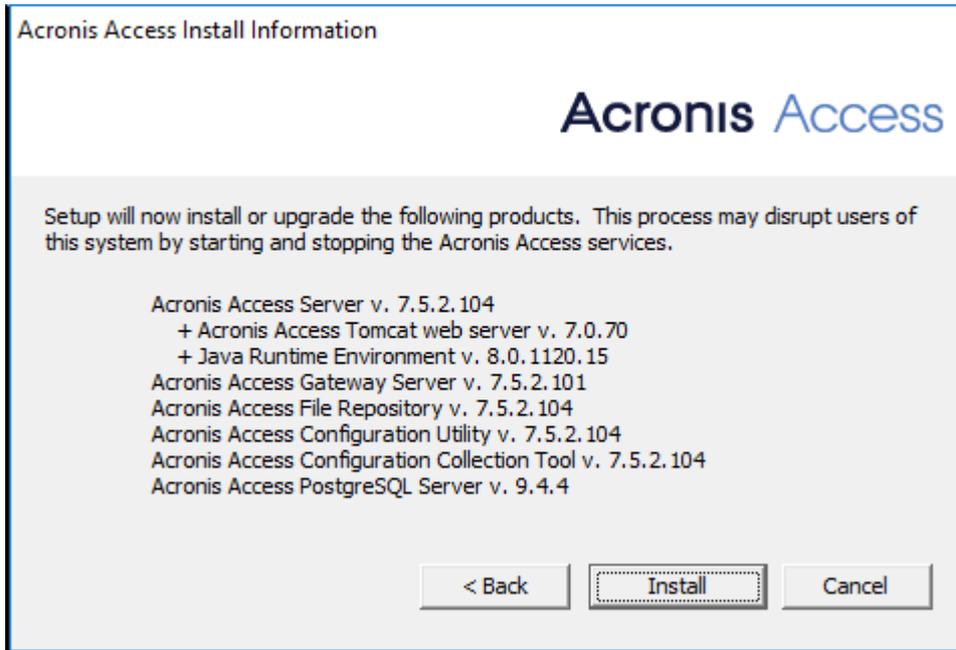
- Download the Acronis Access installer.
- Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
- Double-click on the installer executable.



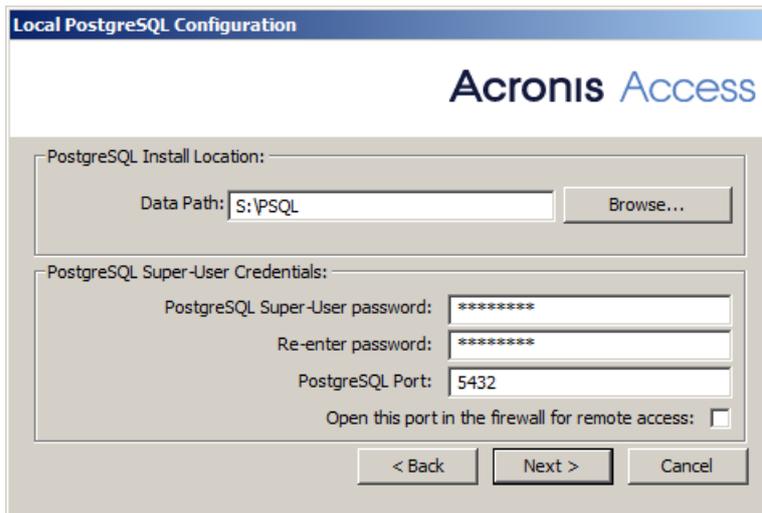
- Press **Next** to begin.
Read and accept the license agreement.
- Press **Install**.

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.

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



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

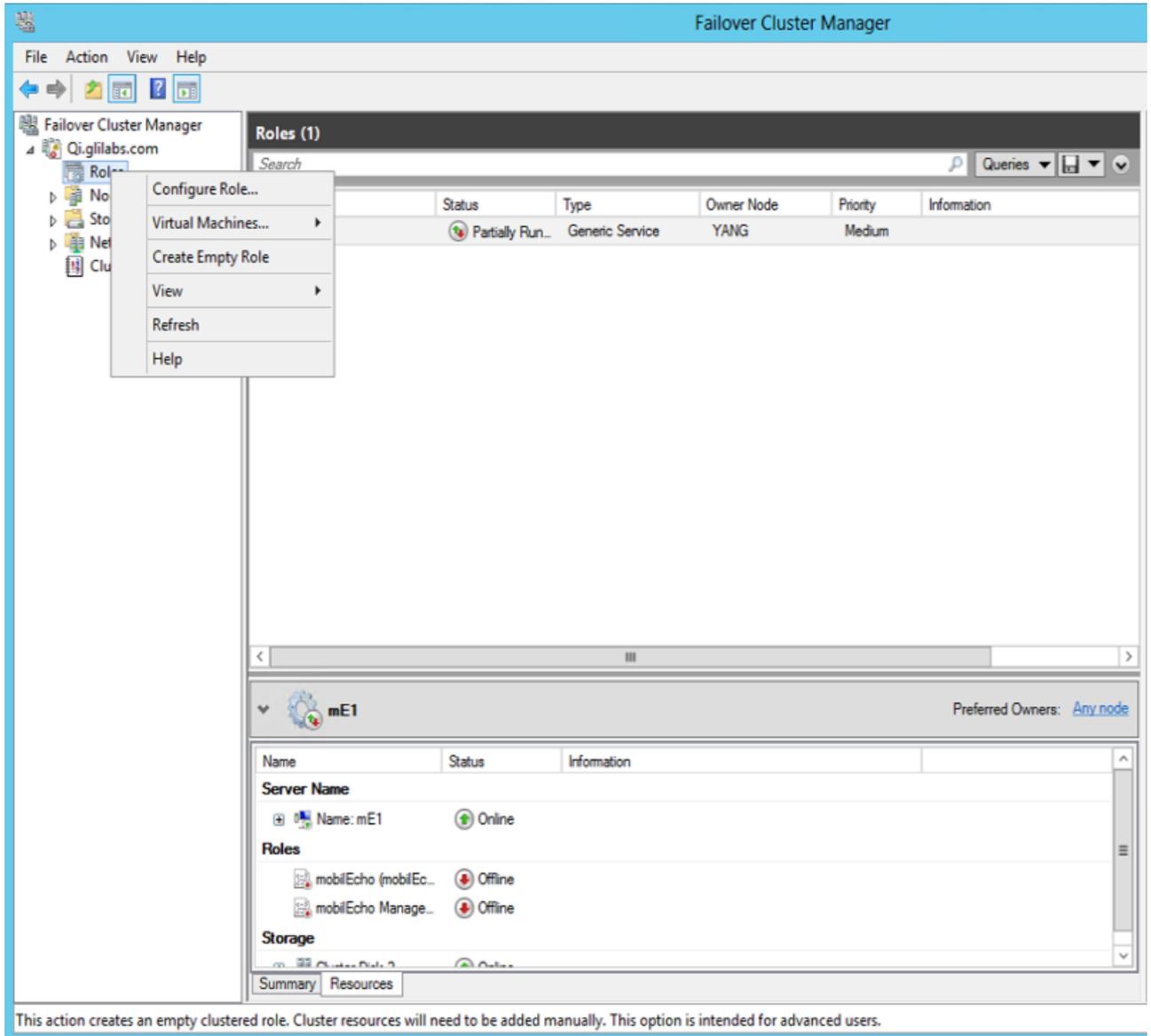


9. A window displaying all the components which will be installed appears. Press **OK** to continue. When the Acronis Access installer finishes, press **Exit**.

Creating the role

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

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



Configurations on the Active node

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

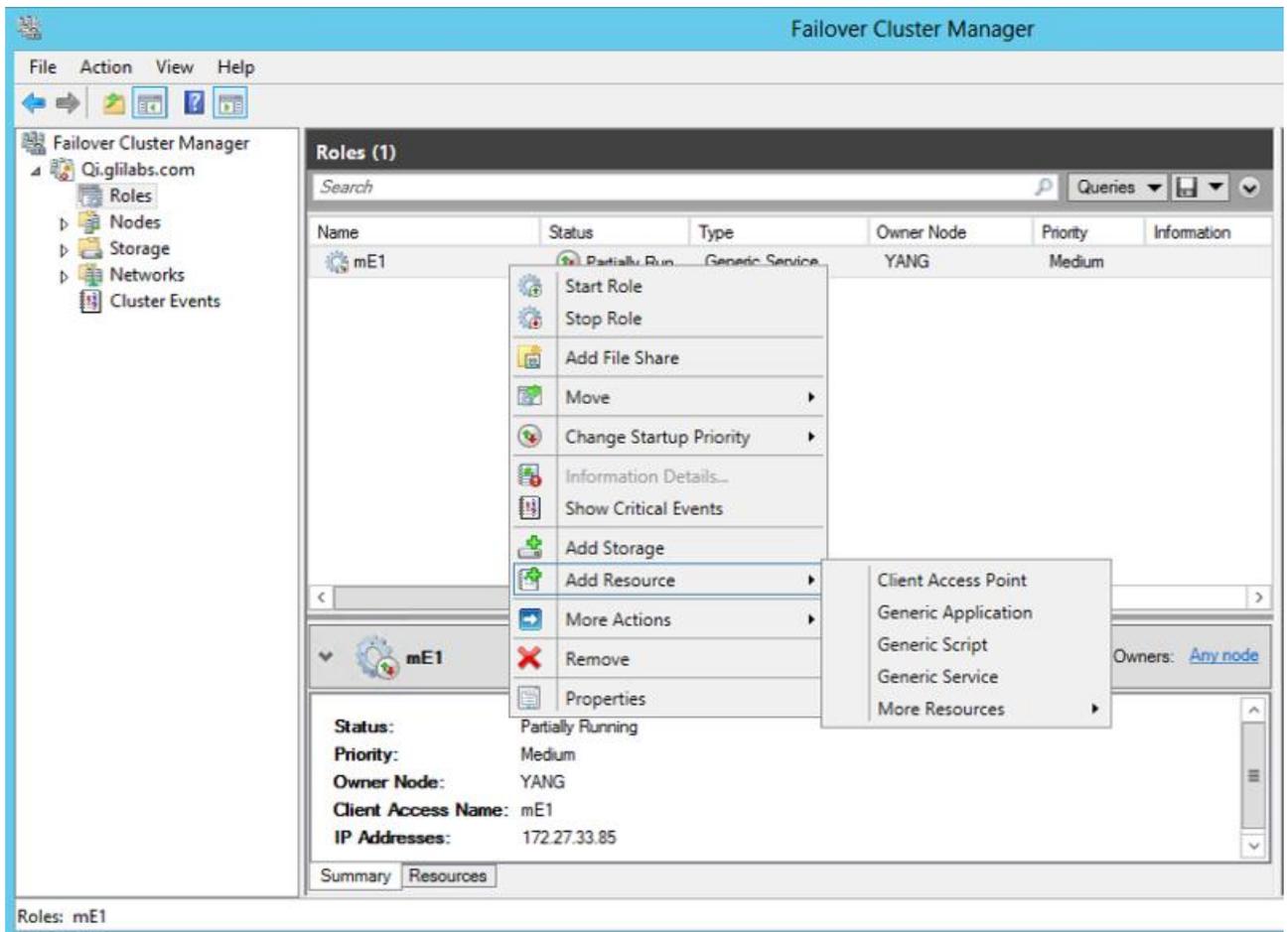
Note: Use slashes(/) as a path separator.

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

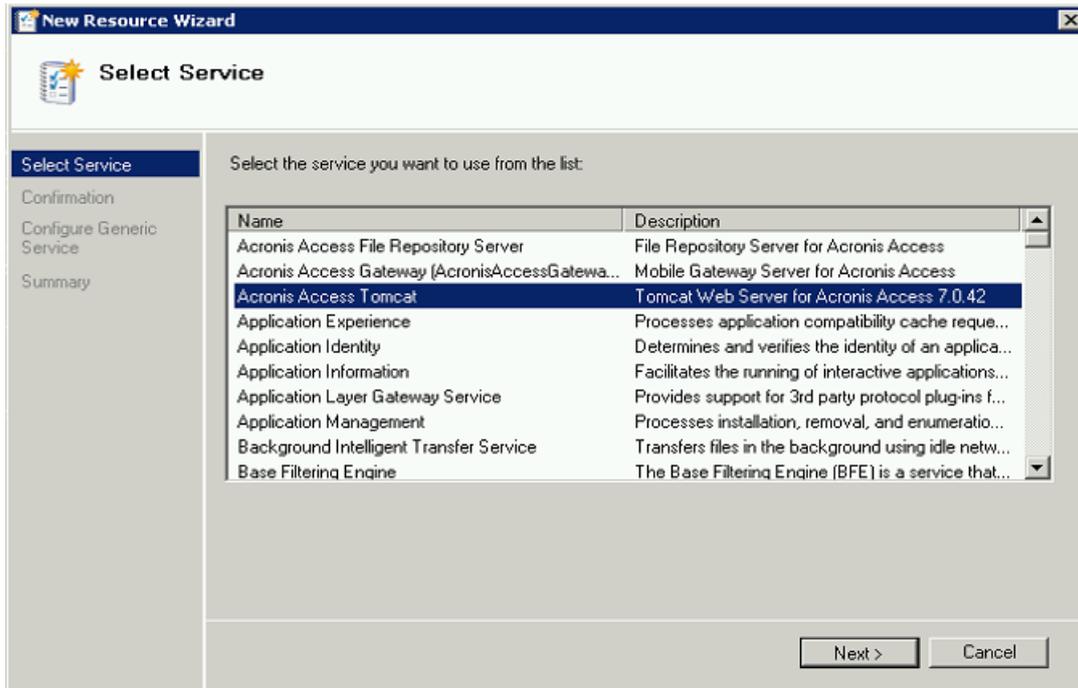
Adding all of the necessary services to the Acronis Access role

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

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



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

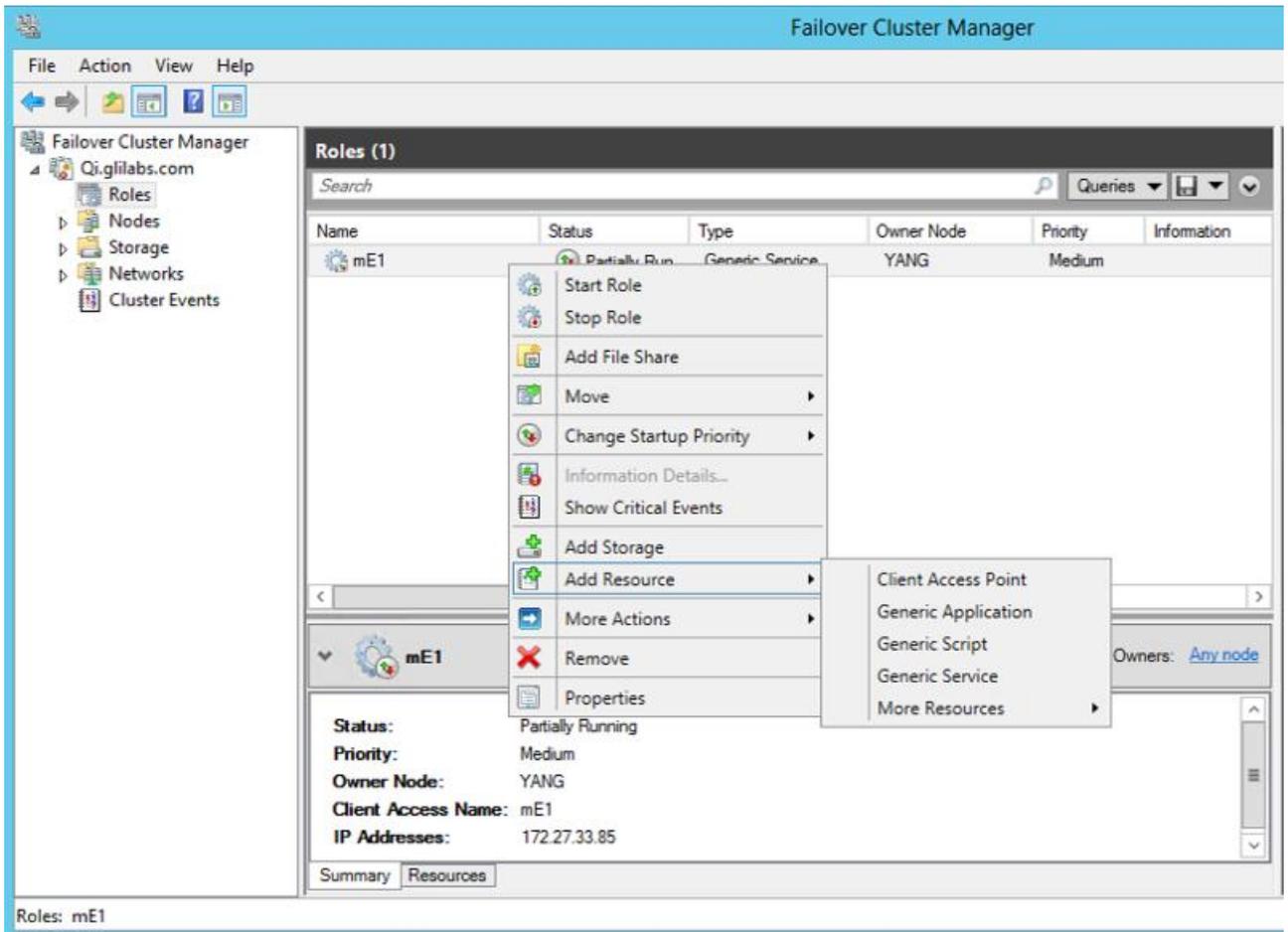


4. On the Confirmation window press **Next**.
5. On the summary window press **Finish**.

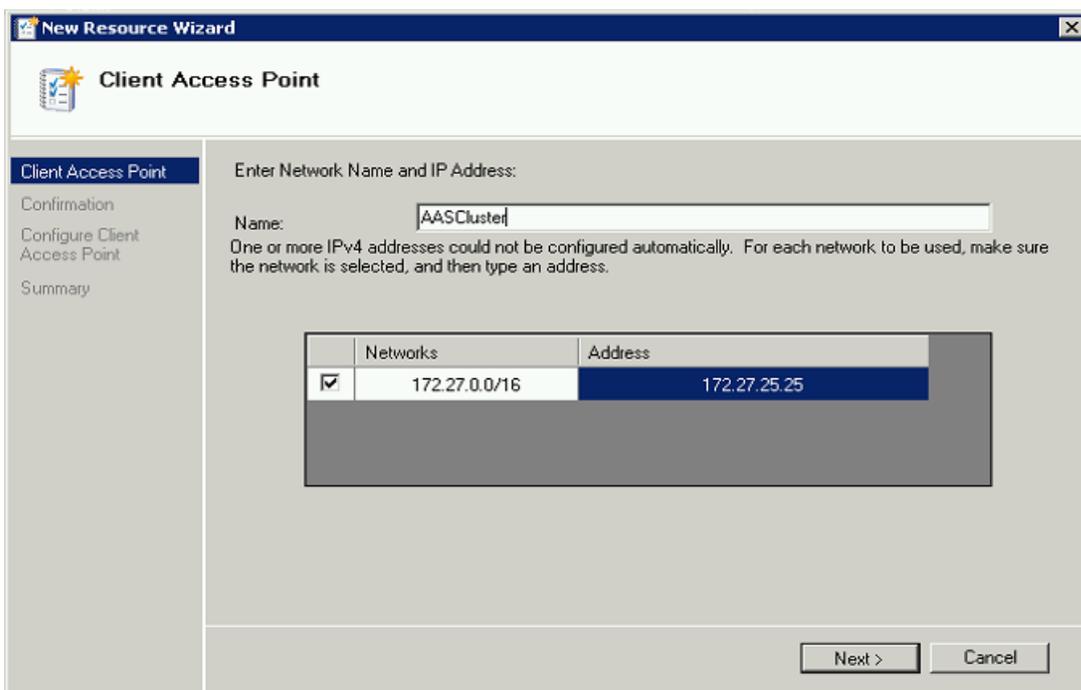
Setting an Access Point

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

2. Select **Client Access Point**.



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

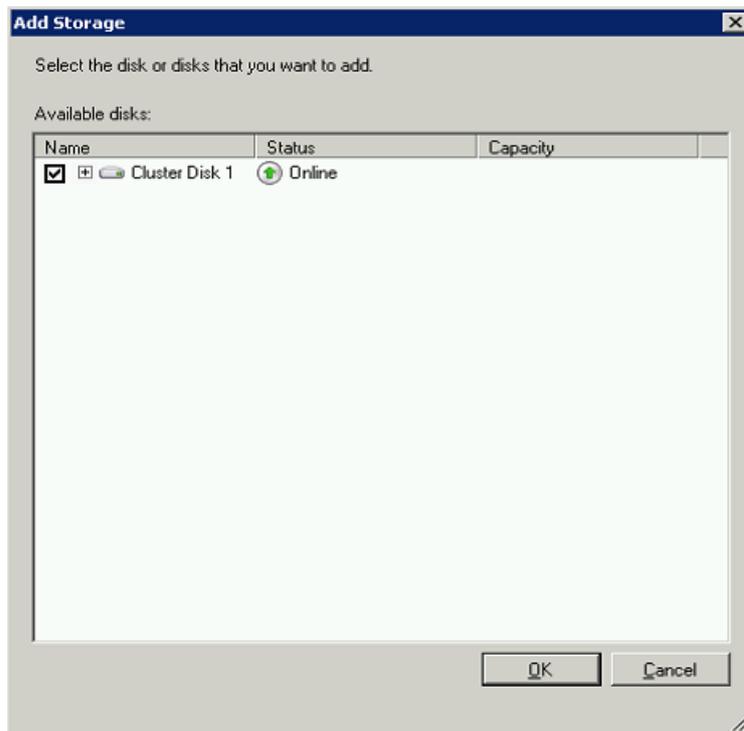


5. Enter the IP address and press **Next**.
6. On the Confirmation window press **Next**.

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

Adding a shared disk

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



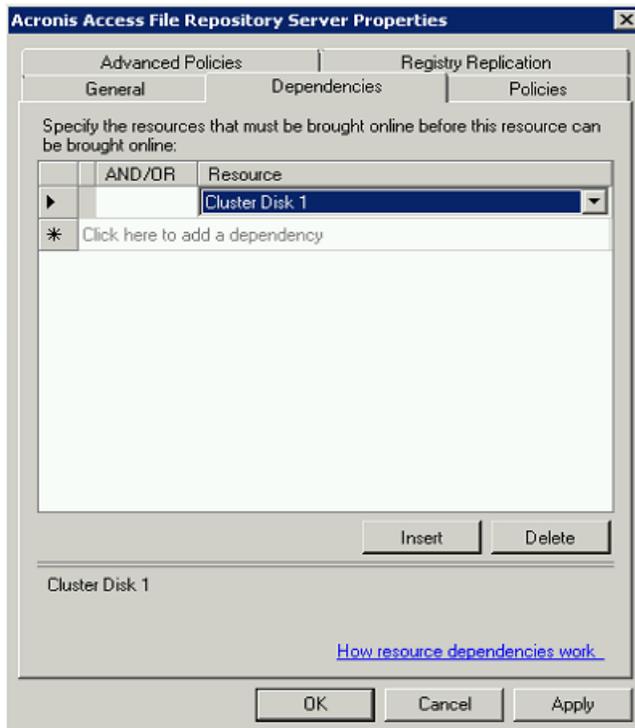
Configuring dependencies

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

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

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

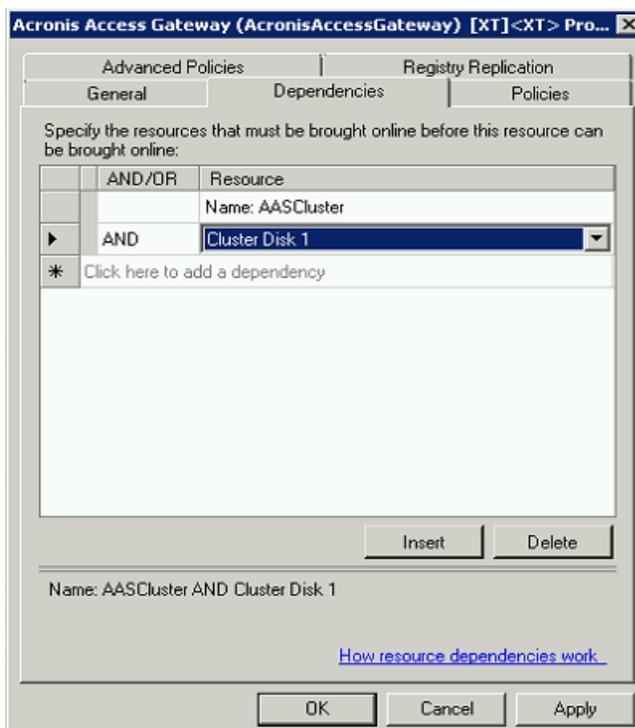
3. Click on **Resource** and select the shared disk you have added.



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

For the Acronis Access Gateway Server service do the following:

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

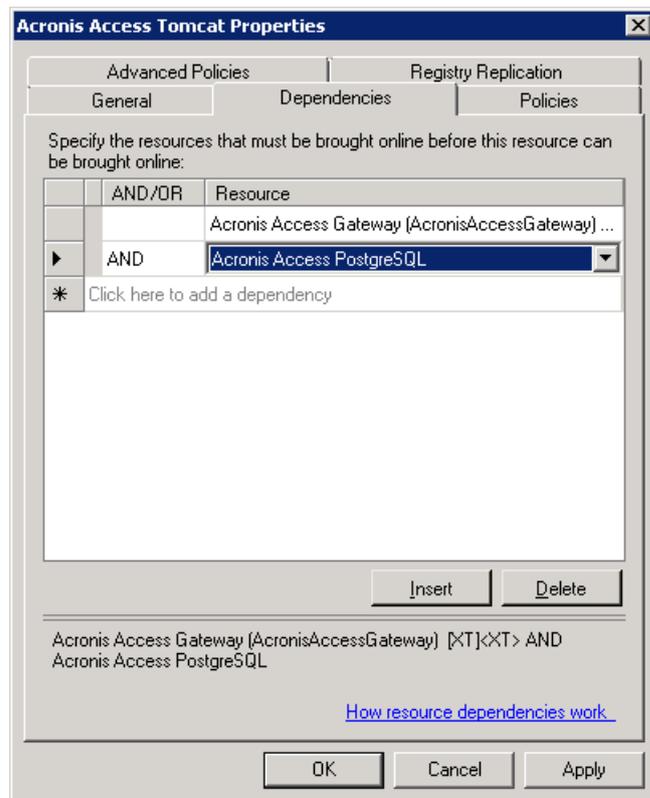


4. Press **Apply** and close the window.

For the Acronis Access Tomcat service do the following:

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

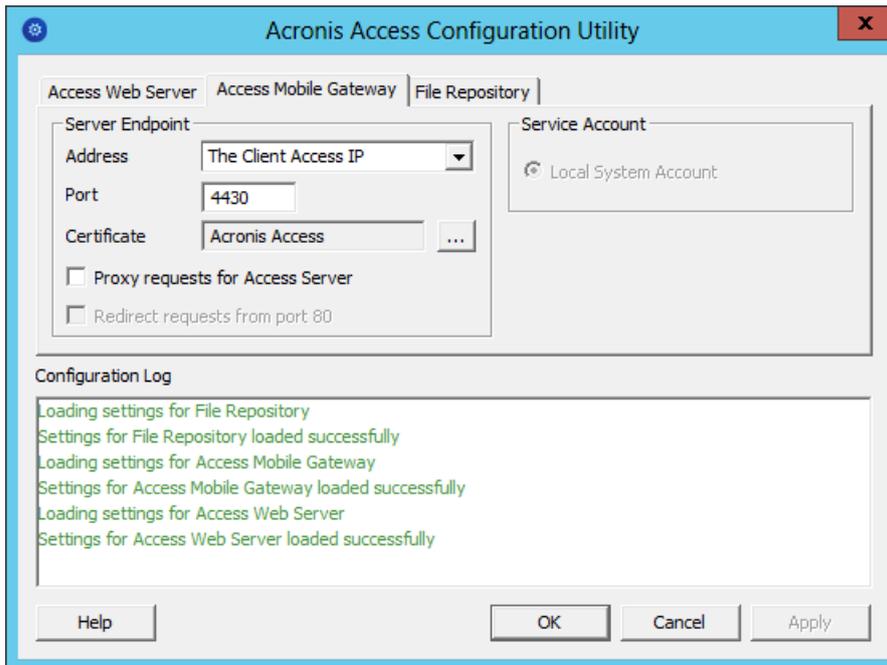
Note: If you want to run the Gateway and Access servers on different IP addresses add the second IP as a resource to the Acronis Access role and set it as a dependency for the network name.



Starting the role and using the Configuration Utility

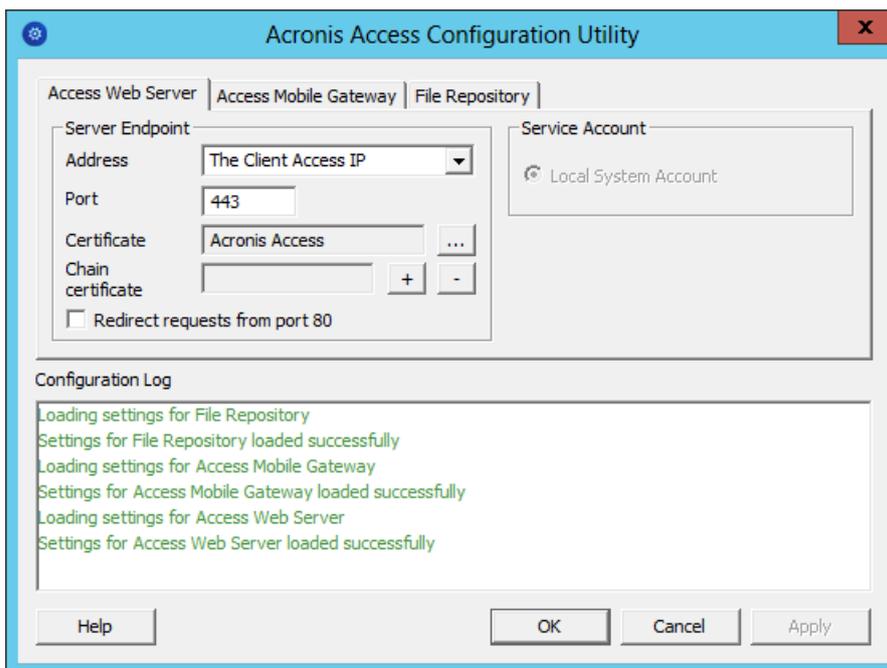
1. Right-click on the Acronis Access role and press **Start role**.
2. Launch the Configuration Utility. On a clean install, this is generally located at **C:\Program Files (x86)\Acronis\Access\Configuration Utility**

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

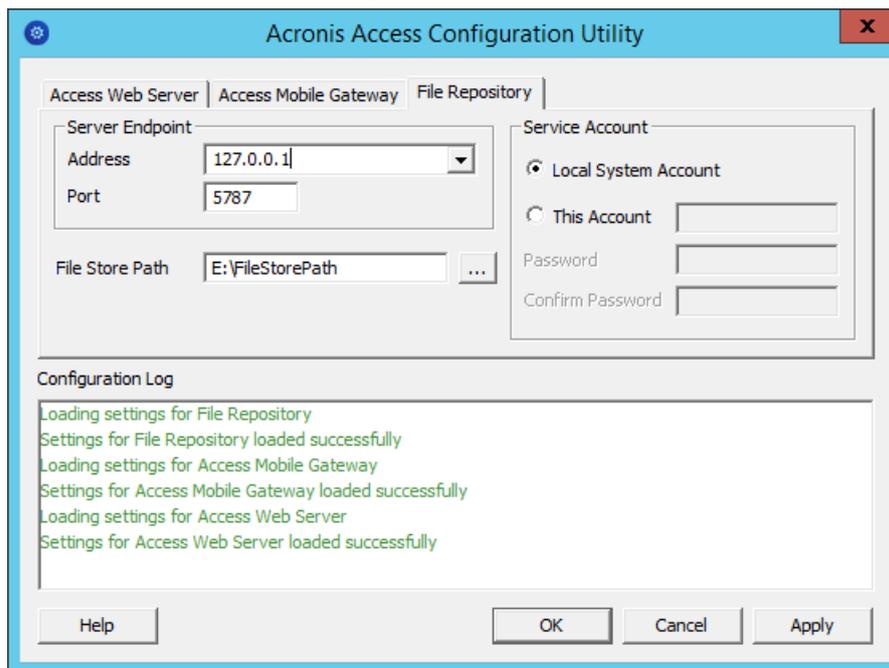


4. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.



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



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

Installation and configuration on the second node

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

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

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

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

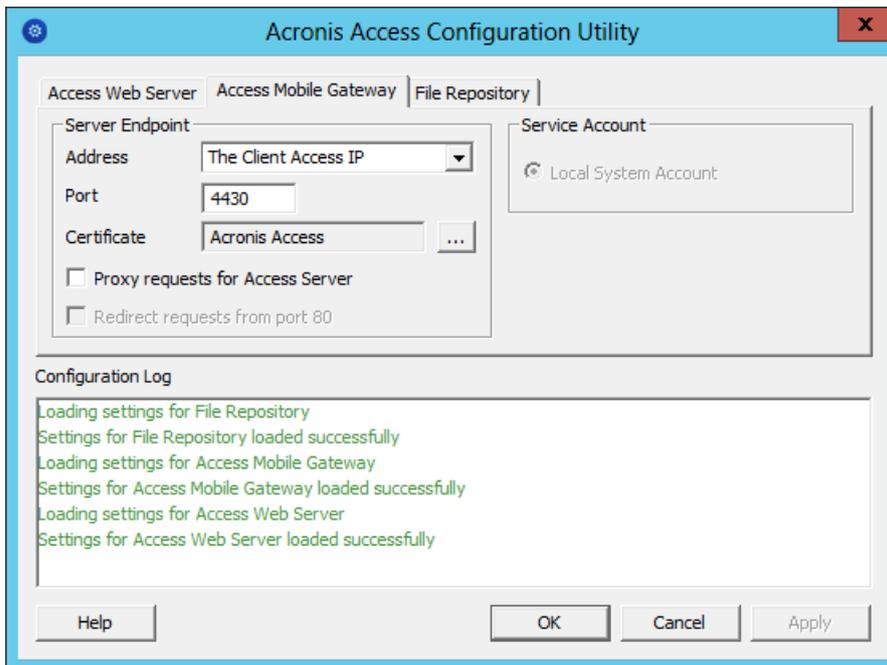
For PostgreSQL do the following:

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

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

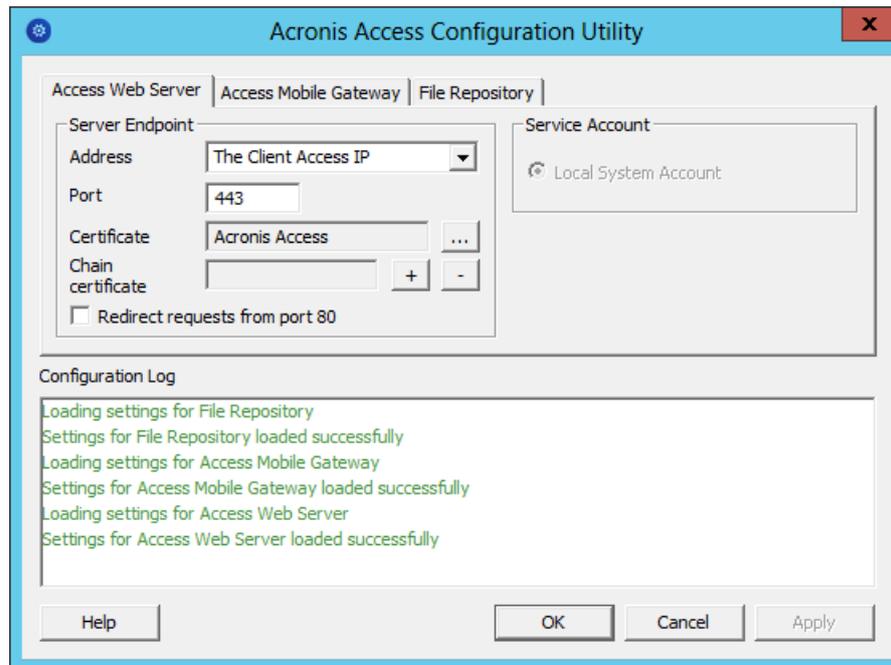
Using the Configuration Utility on the second node

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

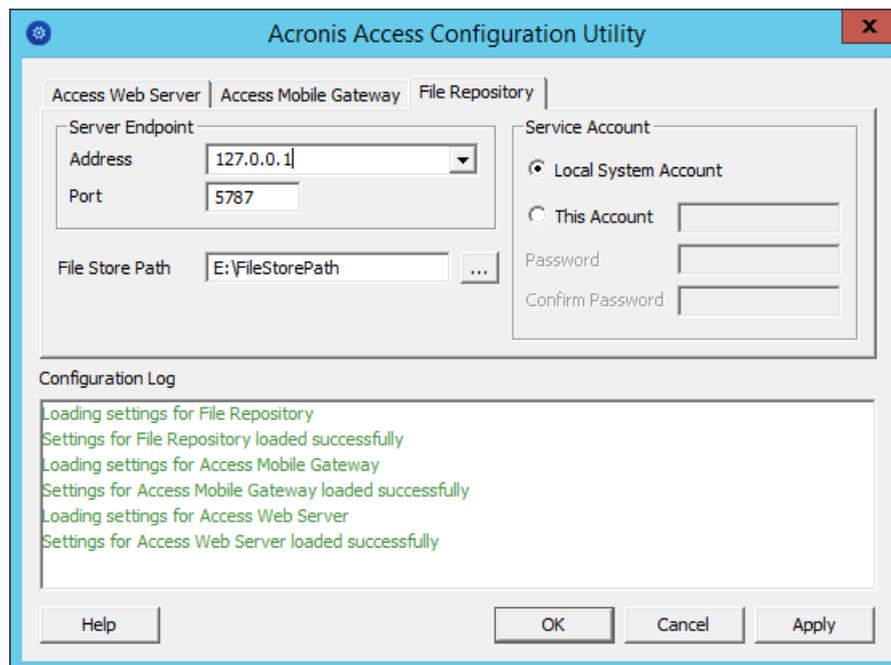


3. Configure the Acronis Access Server service to listen on the IP address(es) for the Acronis Access Service group.

Note: If **Redirect requests from port 80** is selected, Tomcat will listen for incoming traffic on the unsecure port 80 and redirect it to the HTTPS port you have specified above. If you have another program listening on port 80, do not check this box.



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



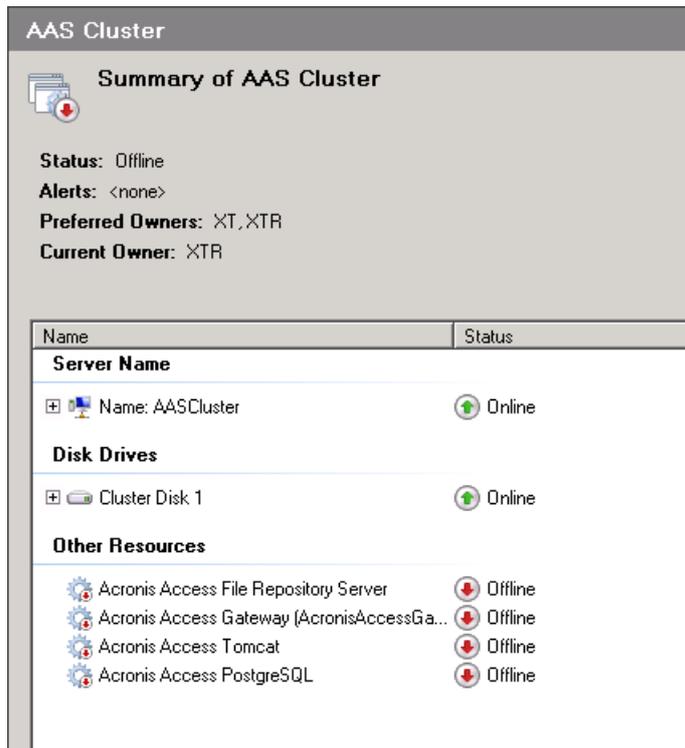
5. Click **OK** to complete the configuration and restart the services.

13.2.13 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.

Note: Before performing any upgrades, please review our *Backup (p. 148)* articles and backup your configuration.

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

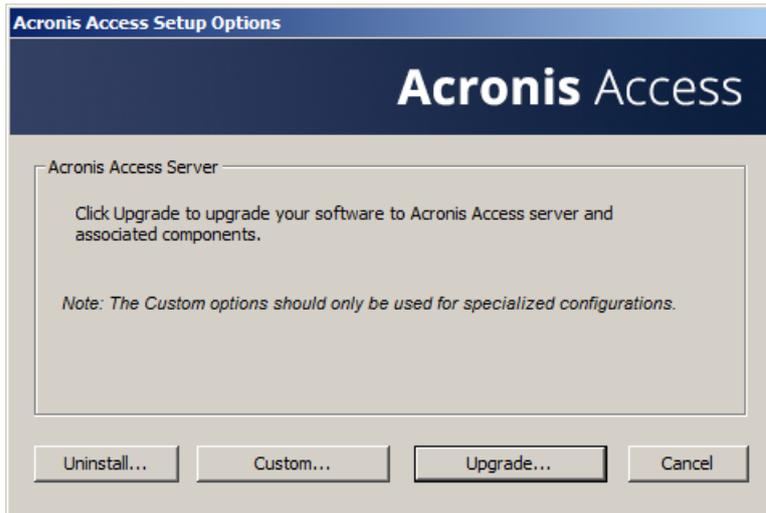


4. Disable any anti-virus software you have or it may interrupt the installation procedure resulting in a failed installation.
5. Double-click on the installer executable.

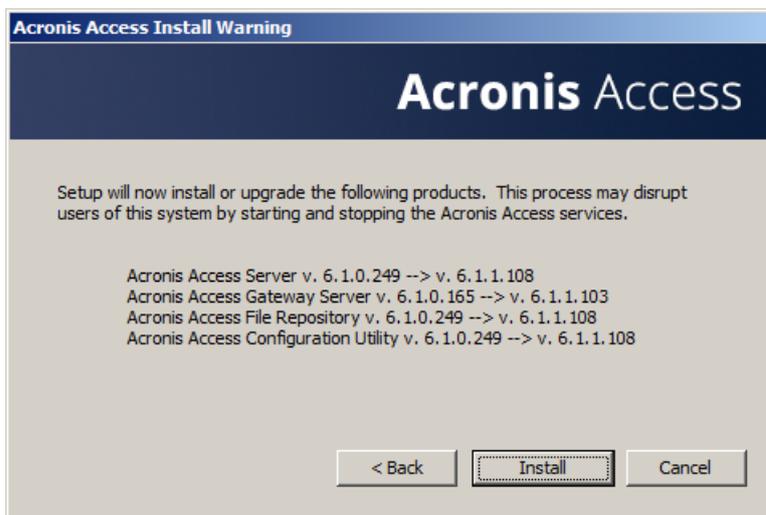


6. Press **Next** to begin.
7. Read and accept the license agreement.

8. Press **Upgrade**.



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



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

Warning! Do not bring the cluster group online!

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

13.2.14 Multi-homing Acronis Access

Multi-homing the Acronis Access Gateway and Access servers is a simple task done through the Configuration Utility.

The only requirement is that you have 2 separate network interfaces and IP addresses.

Configuring multi-homing

1. Open the Acronis Access Configuration Utility.
2. Open the **Access Server** tab and enter the first IP address and the 443 port.

3. Open the **Gateway Server** tab and enter the second IP address and the 443 port.
4. Press **OK**.

Note: Microsoft completely changed how the TCP/IP stack behaves in Windows Server 2008. A single IP transport now supports multiple layers and there is no longer a 'Primary' IP address. So, when multiple IP addresses are assigned to a single interface, all of the addresses are treated evenly and are all registered into DNS. In other words, this behavior is not a bug, but by design. However, the behavior causes issues because unless you do something about it, the IP address used will be round-robin (DNS).

You can work around this by disabling dynamic DNS registration on the NIC and then creating the host DNS entry manually. Another easier work around is to install the HotFix referenced on **KB975808**: <http://support.microsoft.com/?kbid=975808>. Once you have installed the HotFix, you will be able to use the `netsh skipassource` flag. When using this flag while adding new addresses you tell the stack that the new address is not used for outgoing packets. Therefore, these IP addresses will not be registered on the DNS servers. For example:

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

13.2.15 Deploy separate Web Preview servlets

The Web Preview functionality of Acronis Access allows users to view file contents without having to download the whole file. With a lot of users, this can slow down your deployment's performance. To counter this, you can setup additional Tomcat servers with our Web Preview Servlet, which can handle the web previewing and assist your main Acronis Access Advanced Server(s).

A load balancer can be put in front of a series of Tomcat servers to further balance the load for the web preview servlets. The preview requests do not need any state, so no special configuration of the load balancer is needed.

In this section

Installing and configuring the servlet.....	269
Access Server Configurations.....	272
Load-balancing your Web Preview servlets.....	272

13.2.15.1 Installing and configuring the servlet

Tomcat Installation

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

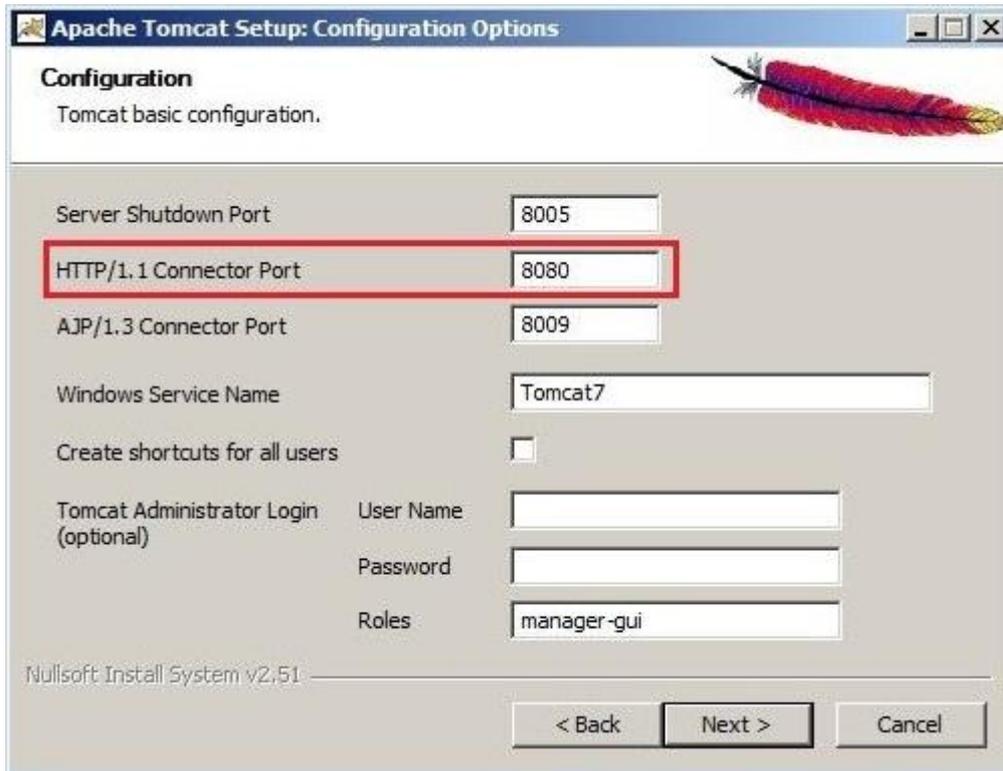
Requirements for both scenarios:

1. Make sure you have a 64bit Java Runtime Environment (JRE) version installed. A 64bit Java Development Kit (JDK) will also work. Java must be version 8 or later.
2. Download a 64bit version of Apache Tomcat 7. Make sure the version you plan to use is not newer than the one supported by Acronis Access. The version used by Acronis Access is listed in the What's New (p. 342) section.

In this section

- 3.

1. Download an installation file with the 64bit version of Apache Tomcat 7. You can find the list of versions at Apache Tomcat's site. Find the desired version and click on it, then open the bin folder and download the .exe file (e.g. **apache-tomcat-7.0.50.exe**).
2. Start the installer and follow the steps of the installation wizard. You can use all of the default settings. You can change the listen port if necessary, the default is 8080.



Note: The installer will pick up the Java installation folder automatically.



3. Once the installation is done, go to your machine with Acronis Access and navigate to your Acronis Access installation folder (by default **C:\Program Files (x86)\Acronis\Access\Access Server**).
4. Copy the **AccessPreviewServlet** folder to the new machine with Apache Tomcat installed and paste it in your Tomcat's **webapps** folder. (by default C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps)
5. Navigate to the **conf** folder of your Apache Tomcat installation (by default C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf) and backup the **server.xml** file.
6. Now open the file, find the lines: **<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">** and place the following right under them:

```
<!-- for Access Web preview -->
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\AccessPreviewServlet">
</Context>
```

Note: If you have installed Apache Tomcat in a location different than the default, you will have to edit the **docBase=""** path to reflect the correct path of your installation.

7. Save and close the file.
8. To start the Tomcat service, open **Control Panel -> Administration Tools -> Services** and start the Apache Tomcat service.

1. Download a **.zip** file with the 64bit version of Apache Tomcat 7. You can find the list of versions at Apache Tomcat's site. Find the desired version and click on it, then open the bin folder and download the core .zip file (e.g. **apache-tomcat-7.0.50.zip**).
2. Extract the contents of the archive to your preferred location. e.g. **C:\Program Files\Apache Tomcat**.
3. Navigate to **C:\Program Files\Apache Tomcat\apache-tomcat-<version>** and open the **bin** folder.

Note: The extracted folder name contains a version number, replace **<version>** with the version of your Tomcat. e.g. **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75**

4. Open **startup.bat** with a text editing program and find the line **setlocal**.
5. Add the following lines below it:

```
set "CATALINA_HOME=Your Tomcat Folder"
e.g. set "CATALINA_HOME=C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75"
```

Note: This sets the default Tomcat folder for all settings. Use the proper path for your Apache Tomcat folder.

```
set "JRE_HOME=Java main folder location"
e.g. set "JRE_HOME=C:\Program Files\Java\jre1.8.0_112"
```

Note: This sets the default JRE folder for all settings. Use the proper path for your Java folder.

Note: If you're using a JDK, the command is **JAVA_HOME** instead of **JRE_HOME**.

6. Save any changes made to the file.
7. Once that is done, go to your machine with Acronis Access and navigate to your Acronis Access installation folder (by default **C:\Program Files (x86)\Acronis\Access\Access Server**).

8. Copy the **AccessPreviewServlet** folder to the new machine with Apache Tomcat and paste it in your Tomcat's **webapps** folder. (by default **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps**).
9. Navigate to the **conf** folder of your Apache Tomcat installation (e.g. **C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\conf**) and backup the **server.xml** file.
10. Now open the file, find the lines: **<Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">** and place the following right under them:

```
<!-- for Access Web preview -->
<Context path="/AccessPreviewServlet" docBase="C:\Program Files\Apache Tomcat\apache-tomcat-7.0.75\webapps\AccessPreviewServlet">
</Context>
```

11. Edit the **docBase=""** path to reflect the correct path of your installation. Save and close the file.

*Note: If you do not change the default port the server is listening on, the servlet will be listening on **8080**. To change the port, find the following lines in the **server.xml** file:*

```
<Connector port="8080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

*Replace **8080** with the desired port number.*

12. To start the Tomcat service, navigate to the bin folder and double-click on the **startup.bat** file. The black DOS window must remain open while the Tomcat is running.

13.2.15.2 Access Server Configurations

1. Open the Acronis Access web interface and open **General Settings -> Web Previews**.
2. Enable **Use custom URL for web preview service** and enter the address for your new web preview servlet. (e.g. **http://accesswp.company.com:8080**). The port number must be present in the URL you provide. If you're using a load-balanced or clustered setup, the URL will be the address of your loadbalancer.
3. Depending on the number of servers you set up to run the web preview servlet, you may want to increase the number of **Maximum concurrent generation calls** the Access server is set to.
4. Find the setting **Maximum concurrent generation calls** setting and set it to the appropriate value.

The default value is 2. Rendering of a document can utilize the majority of one processor core. The number of rendering threads should be set to no greater than 50% of your available processor cores. Exceeding this recommendation can result in degradation of other services on the server.

13.2.15.3 Load-balancing your Web Preview servlets

Your **Web Preview** servlets must be placed behind a load-balancer.

1. Enable duration-based session stickiness (or your load balancer's equivalent) on your load balancer and configure it to not expire.
2. If a health-check is required (looking for an HTTP status of 200 to be returned), a ping to **http://servername.yourdomain.com:port/AccessPreviewServlet/generate_preview/** will satisfy it.

e.g. **https://servlet1.acme.com/AccessPreviewServlet/generate_preview** and **https://servlet2.acme.com/AccessPreviewServlet/generate_preview**.

- Using a browser, open the address of your load balancer to verify the configuration is working.
e.g. <https://loadbalancer.yourdomain.com>

13.2.16 PostgreSQL Streaming Replication

The purpose of this document is to provide a step-by-step procedure on how to configure streaming replication between two PostgreSQL servers. Streaming replication is one of the many methods that exist to keep a PostgreSQL database online, but other methods won't be addressed in this document.

Note: *This document does not describe the installation process of PostgreSQL or Acronis Access but only the streaming replication configuration.*

Streaming replication

The streaming replication process is based on Write-Ahead Logging (WAL) segment. WAL, is a standard method for ensuring data integrity. WAL's central concept is that changes to data files (where tables and indexes reside) must be written only after those changes have been logged, that is, after log records describing the changes have been flushed to permanent storage. If we follow this procedure, we do not need to flush data pages to disk on every transaction commit, because we know that in the event of a crash we will be able to recover the database using the log: any changes that have not been applied to the data pages can be redone from the log records.

Using WAL results in a significantly reduced number of disk writes, because only the log file needs to be flushed to disk to guarantee that a transaction is committed, rather than every data file changed by the transaction. The log file is written sequentially, and so the cost of syncing the log is much less than the cost of flushing the data pages.

WAL also makes it possible to support on-line backup, point-in-time recovery and replication. Streaming replication refers to continuous sending of WAL records over a TCP/IP connection between a primary server and a standby server, using the walsender protocol over replication connections. Although streaming replication can be synchronous, and considering the resources needed and the impact on performances of a synchronous process, we've decided to only consider asynchronous streaming replication as a valid scenario.

Requirements:

- Two PostgreSQL servers: the active server will be called "primary server" and the passive server will be called "standby server" in the procedure.
- PostgreSQL 9.4: We will implement features like "replication slot" that require PostgreSQL 9.4. This version is actually embedded with Acronis Access Advanced 7.2 and is installed only during new installations (and not upgrades).
- One virtual IP (optional): this virtual IP will be used in all frontends that run Access Server role and should always be owned by to the active host (the primary server).
- We recommend that Acronis Access is already installed and the primary server's database has been initialized.

13.2.16.1 On the Primary Server

Create a replication user

This user will be used by the replication process to send WAL from the Primary server to the Standby server. For security reasons, it is recommended to create a dedicated user, with replication permissions, instead of using the default superuser account (i.e. **postgres**).

1. On the Primary server, run the following command:

```
psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -U postgres
```

This command can also be run remotely using the following options:

```
psql -c "CREATE USER replicator REPLICATION LOGIN ENCRYPTED PASSWORD 'XXXXX';" -h <IP_OF_PRIMARY_SERVER> -U postgres
```

*Note: PSQL is located in the **bin** sub-folder of PostgreSQL's installation folder. Depending on your **PATH** environment variable, you may need to specify the path to reach the command or move to the right directory before executing the command. This note also applies for the next commands used in this procedure.*

Configure access

Edit the access control on the Primary Server to allow the connection from the Standby Server.

1. This can be done by editing the **pg_hba.conf** file (located in the **data** sub-folder) and adding the following line:

```
host replication replicator <IP_OF_STANDBY_SERVER>/32 trust
```

2. If more security is needed between the database servers, then authentication can require the client to supply an encrypted password (md5) and/or only allow SSL encryption (**hostssl**) e.g.:

```
host replication replicator <IP_OF_STANDBY_SERVER>/32 md5
```

```
hostssl replication replicator <IP_OF_STANDBY_SERVER>/32 md5
```

Configure streaming replication

1. Navigate to the PostgreSQL installation folder. By default, it is located in **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4**
2. Navigate into the **Data** folder and modify the **postgresql.conf** file. Find and edit the following lines:

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

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

3. Restart the PostgreSQL service after making the above changes.

Create a replication slot

1. On the Primary Server, run the following command:

```
psql -U postgres -c "SELECT * FROM pg_create_physical_replication_slot('access_slot');"
```
2. Verify that the slot is created using the following command:

```
psql -U postgres -c "SELECT * FROM pg_replication_slots;"
```

13.2.16.2 On the Standby Server

Verify that all necessary servers have access to each other

In case of a fail-over, the Standby server will be promoted to be the Primary server and will reply to all Access Servers' requests.

It is recommended to configure the access to the Standby server for all Access Servers now, so that you won't be required to reboot the PostgreSQL service on any Standby server during the fail-over process.

Note: When the Standby server is in standby mode, the database is in read-only mode (hot standby). It is not possible to configure and use the Standby server as the production database by mistake.

1. Edit the access control on the Standby server to allow the connection from all Access Servers.
2. This can be done by navigating to the PostgreSQL installation folder and editing the **pg_hba.conf** file (located in the **data** sub-folder) and by adding the following line for each server:

```
host replication replicator <IP_OF_ACCESS_SERVER_1>/32 md5
host replication replicator <IP_OF_ACCESS_SERVER_2>/32 md5
```

Configure streaming replication

1. Navigate to the PostgreSQL installation folder. By default, it is located in **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4**
2. Navigate into the **Data** folder and modify the **postgresql.conf** file. Find and edit the following lines:

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

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

The **hot_standby** setting specifies whether or not you can connect and run queries during streaming replication. When it is enabled, the database will accept read-only request and it is then possible to look at the database and check that replication process works by looking at the database tables' content.

Note: When using *md5* or *password* as the authentication method specified in **pg_hba.conf**, a password will be required for that connection. To "enter" this password, you have to add the following command to the **recovery.conf** file on the Standby server.

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

e.g. this is how it would look for Postgres running on IP 10.0.0.1, port 5432, with user **replicator** and password 1234: **primary_conninfo = 'host=10.0.0.1 port=5432 user=replicator password=1234'**

3. **Stop the PostgreSQL service on the Primary server to do the initial seeding of the database and start the streaming replication process.**

Backup configuration files

Make a backup of all the **.conf** configuration files, including: **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**. These files will be overwritten by the initial seeding process and you will need to restore them after this step.

Clean the data directory

Delete (or just rename) the **data** sub-folder. Renaming the folder is a good way to keep a copy of a previous configuration and be able to revert back the Standby server's database to a consistent state in case an issue occurs during the initial seeding or at the database startup.

Initial seeding

The initial seeding is done using a backup of the Primary database to a folder located on the Standby server.

1. Make sure that the Primary server is not in active use. The easiest way to do this is stop the Acronis Access Tomcat service, and then start it when the seeding is complete.
2. To start the initial seeding at Standby server level use the following command:
pg_basebackup.exe -h <IP_OF_PRIMARY_SERVER> -D <PATH_TO_NEW_DATA_DIR> -U replicator -v -P --xlog-method=stream

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

Restore configuration files

Copy of all the **.conf** configuration files (including **pg_hba.conf**, **postgresql.conf**, **pg_ident.conf**) from the backup folder to the new **Data** folder and overwrite all existing files.

Streaming replication controls

1. Open the Data folder and create (or modify) the **recovery.conf** file.
2. Add the following lines if they don't already exist:
 - **standby_mode = 'on'**

- `primary_conninfo = 'host=<IP_OF_PRIMARY_SERVER> port=5432 user=replicator password= <PASSWORD_USED_FOR_REPLICATOR_USER>'`
 - `primary_slot_name = 'access_slot'`
 - `trigger_file = '<PATH_TO_TRIGGER_FILE>' # As an example 'failover.trigger'`
 - `recovery_min_apply_delay = 5min`
3. Start the PostgreSQL service on the Standby server after saving the above changes.

*Note: In case of a fail-over, the **recovery.conf** file will be renamed to **recovery.done**.*

Additional Information

- The **standby_mode** setting specifies to start the PostgreSQL server as a standby. In this case, the server will not stop the recovery when the end of archived WAL is reached, but will keep trying to continue the recovery by fetching new WAL segments connecting to the Primary server as specified by the **primary_conninfo** setting (that specifies a connection string to be used for the Standby server to connect with the Primary server).
- We use the replication slot created during the previous steps on the Primary server, by using the **primary_slot_name** setting.
- The **trigger_file** setting specifies a trigger file whose presence ends recovery on the Standby server and makes it the Primary server. This will be used during the fail-over process.
- Optionally, **recovery_min_apply_delay** settings can be set. By default, a Standby server restores WAL records from the Primary server as soon as possible. It may be useful to have a time-delayed copy of the data, offering opportunities to correct data loss errors. This parameter allows to delay recovery by a fixed period of time, measured in milliseconds if no unit is specified. For example, if you set this parameter to 5 min, the Standby server will replay each transaction commit only when the system time on the standby is at least five minutes past the commit time reported by the primary server.

It is possible that the replication delay between servers exceeds the value of this parameter, in which case no delay is added. Note that the delay is calculated between the WAL timestamp as written on the Primary Server and the current time on the standby server. Delays in transfer because of network lag or cascading replication configurations may reduce the actual wait time significantly. If the system clocks on the Primary Server and the Standby Server are not synchronized, this may lead to recovery applying records earlier than expected; but that is not a major issue because useful settings of this parameter are much larger than typical time deviations between servers.

13.2.16.3 Testing the fail-over

We recommend that you test the above settings and make sure the fail-over works, before implementing it in your production setup.

If the Primary server is not down, make sure to stop it before configuring the Standby server to take that role. This is done to avoid the Primary server from processing further queries leading to issues.

You can turn the Standby server into the Primary server by creating the trigger file that was mentioned in the **recovery.conf**. Now that Standby server has taken over the role of the Primary server, make sure that your Acronis Access servers are configured to use it.

*Note: Once the fail-over process is triggered and completes successfully, the **recovery.conf** file will be renamed to **recovery.done**.*

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

13.2.17 Configuring PostgreSQL for remote access

Remote access can help you if you are managing multiple instances of PostgreSQL or you just prefer to manage your database remotely.

To enable remote access to this PostgreSQL instance, follow the steps below:

1. Navigate to the PostgreSQL installation directory: **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\Data**
2. Edit **pg_hba.conf** with a text editor.
3. Include host entries for each computer that will have remote access using their internal address and save the file. The **pg_hba.conf** (HBA stands for host-based authentication) file controls client authentication and is stored in the database cluster's data directory. In it you specify which servers will be allowed to connect and what privileges they will have. e.g.:

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

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

4. Navigate to and open the **postgresql.conf**. By default it is located at: **C:\Program Files (x86)\Acronis\Access\Common\PostgreSQL\9.4\Data**
 - a. Find the line **#listen_addresses = 'localhost'**
 - b. Enable this command by removing the **#** symbol at the start of the line.
 - c. Replace **localhost** with ***** to listen on all available addresses. If you want PostgreSQL to listen only on a specific address, enter the IP address instead of *****.
 - e.g. **listen_addresses = '*'** - This means that PostgreSQL will listen on all available addresses.
 - e.g. **listen_addresses = '192.168.1.1'** - This means that PostgreSQL will listen only on that address.
5. Save any changes made to the **postgresql.conf**.
6. Restart the Acronis Access PostgreSQL service.

Note: PostgreSQL uses port 5432 by default. Make sure that this port is open in any firewall or routing software.

13.3 For the Mobile Clients

In this section

Using iOS Managed App Configuration features	279
Acronis Access for BlackBerry Dynamics.....	280
Microsoft Intune	298
MobileIron AppConnect support	300

Using client certificate authentication.....	333
Using Kerberos Constrained Delegation authentication	334

13.3.1 Using iOS Managed App Configuration features

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

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

We support the use of the following keys:

- **enrollmentServer** - The value of this key should be set to the DNS address of the Acronis 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. This PIN requirement is configured on the **Settings** page (p. 102) of the **Acronis Access** web console.
- **userName** – 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 variable to autocomplete this value with the specific user's username.

Creating a plist file

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

Creating the plist file

1. Open a text editor of your choice.
2. Enter the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    Enter your desired keys here
  </dict>
</plist>
```

Example:

```
<dict>
  <key>enrollmentServer</key>
```

```

<string>server.example.com</string>
<key>userName</key>
<string>username</string>
  <key>enrollmentPIN</key>
  <string>11Y9KL</string>
</dict>

```

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

Uploading the plist file to MobileIron

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

Uploading the plist file to Microsoft Intune

Note: For an in-depth guide, please visit the [Microsoft Intune Documentation on the subject](#).

1. In the Microsoft Intune administration console, choose **Policy > Overview > Add Policy**.
2. In the list of policies, expand **iOS**, choose **Mobile App Configuration**, and then choose **Create Policy**.
 - In the General section of the **Create Policy** page, supply a name and an optional description for the mobile app configuration policy.
 - In the Mobile App Configuration Policy section of the page, in the box, enter or paste an XML property list that contains the app configuration settings.
3. Click **Validate** to ensure that the XML that you entered is in a valid property list format.
4. When you are done, click **Save Policy**.

13.3.2 Acronis Access for BlackBerry Dynamics

In this section

For iOS.....	280
For Android	291

13.3.2.1 For iOS

In this section

Introduction	281
Testing a trial version of Acronis Access for BlackBerry Dynamics.....	281
Requesting and configuring Acronis Access within BlackBerry Control	282
BlackBerry Dynamics Policy Sets and Acronis Access	285
Granting Acronis Access access to a BlackBerry Dynamics User or Group	286
Enrolling the Acronis Access client app in BlackBerry Dynamics	288
Side-loading Acronis Access	289

Introduction

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

The components of the BlackBerry Dynamics platform include:

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

Acronis Access for BlackBerry Dynamics requires:

- **Acronis Access for BlackBerry Dynamics client app** - The Acronis Access for BlackBerry Dynamics client app available on the Apple App Store <http://www.grouplogic.com/web/megoodappstore> is specifically designed as a BlackBerry Dynamics integrated application. When first installed and run on a device, the Acronis Access for BlackBerry Dynamics app will prompt the user to activate the app in BlackBerry Dynamics. This activation is required before the user can proceed with enrolling the app with their Acronis Access server and accessing file.
- **Acronis Access server** - Acronis Access for BlackBerry Dynamics uses the same server-side software as standard Acronis Access. No server-side changes are required for Acronis Access servers to work with BlackBerry 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 BlackBerry Dynamics.

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

Testing a trial version of Acronis Access for BlackBerry Dynamics

The process of trialing Acronis Access for BlackBerry 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 Acronis site. 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 (p. 7) to assist in initial setup.

- 2. The Acronis Access for BlackBerry Dynamics client app is a free download from the Apple App Store <http://www.grouplogic.com/web/megoodappstore>.
<http://www.grouplogic.com/web/meappstore>

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

Requesting and configuring Acronis Access within BlackBerry Control

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

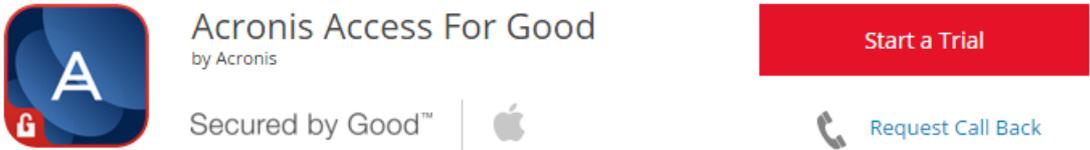
In this section

.....282
.....283

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

On the Acronis Access for <https://begood.good.com/gd-app-details.jspa?ID=248978> BlackBerry app page, click the Start Trial button to request a trial or get the licensed version of the app. <https://begood.good.com/gd-app-details.jspa?ID=248978>

Good Dynamics Marketplace > Acronis Access For Good



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

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

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

Manage Apps



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

Allowing access from your domain

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

Client Connections

▼ ALLOWED DOMAINS *. 

Route All 

DOMAIN	PRIMARY GP CLUSTER	SECONDARY GP CLUSTER	ACTIONS
*(All Domains)	-- Not set --	-- Not set --	 
*.acronisdemo.com	First	-- Not set --	  
*.glilabs.com	First	-- Not set --	  
*.glilabs2008.com	First	-- Not set --	  
*.grouplogic.com	First	-- Not set --	  

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

Assigning your domain as a default domain for connections

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

Allowing specific servers to connect

▼ ADDITIONAL SERVERS  

SERVER	PORT	PRIMARY GP CLUSTER	SECONDARY GP CLUSTER	ACTIONS
ae.grouplogic.com	443	First	-- Not set --	  
ae.grouplogic.com	8043	First	-- Not set --	  
avid.glilabs.com	443	First	-- Not set --	  

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

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Additional Servers**.
3. Press the plus (+) icon and enter the DNS name and port of the server you want to grant access to. Repeat this step for all Acronis Access servers you want your Good clients to connect.

BlackBerry Dynamics Policy Sets and Acronis Access

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

These settings include:

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

Data Leakage Protection effects and limitations

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

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

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

Acronis Access for BlackBerry Dynamics includes a BlackBerry Dynamics feature called "Secure Docs". This allows files to be transferred between the Acronis Access for BlackBerry Dynamics app and the BlackBerry for

Enterprise app. Once a file is opened into the BlackBerry for Enterprise app, it can then be opened into other 3rd party BlackBerry Dynamics enabled apps that include this feature. This functionality will be available, even with the BlackBerry Control **Data Leakage Protection** policy setting enabled.

Granting Acronis Access access to a BlackBerry Dynamics User or Group

Before a user can enroll their Acronis Access app in BlackBerry 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 BlackBerry Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you manage access on the user level, when new versions of Acronis Access for BlackBerry are released, you will need to return to the users' BlackBerryControl configuration and add the new version before they are allowed to run that version.

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

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

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

Manage User

Resend Welcome Email Remove User Refresh

Hristo Ilchev hristo.ilchev@grouplogic.com

Policy Set Good Default Policy

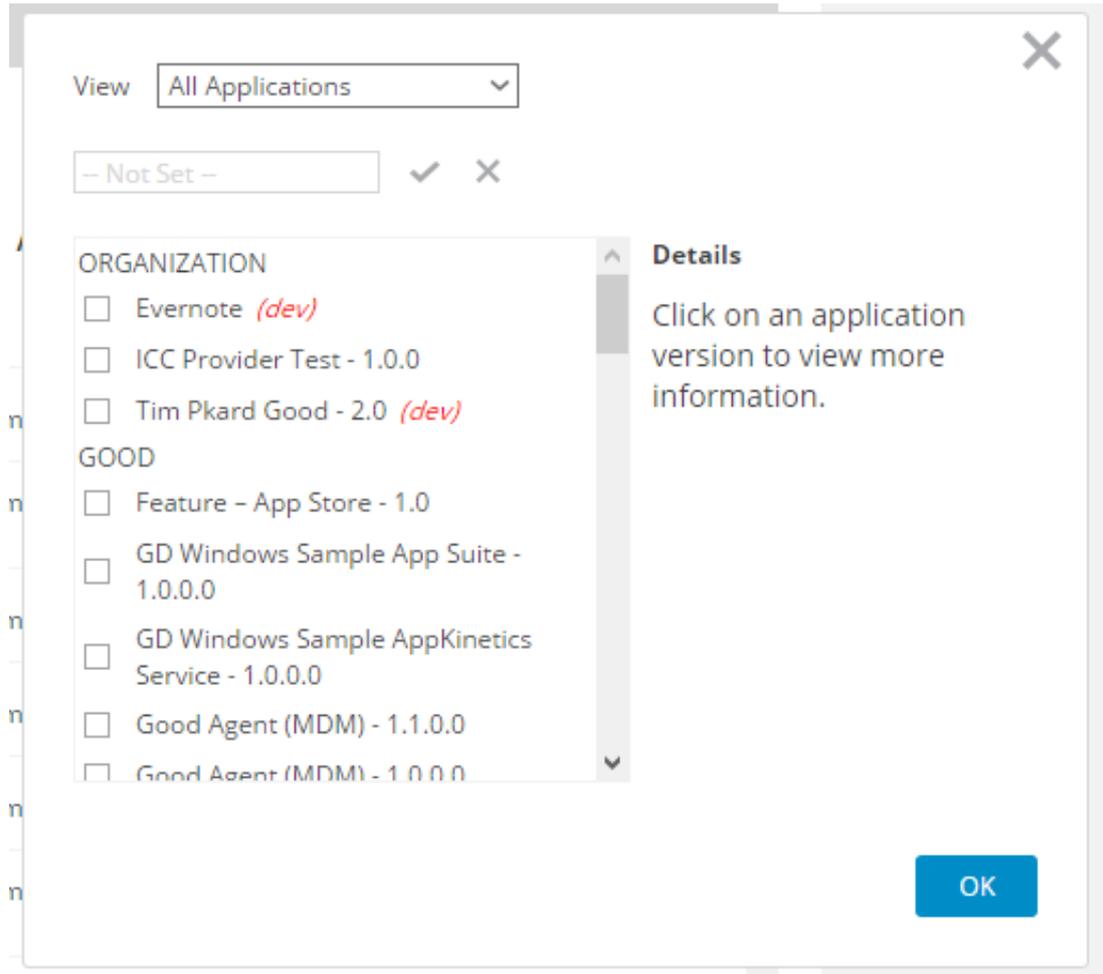
App Groups

DEVICES | APPS | ACCESS KEYS

ENTITLED ENTERPRISE APPS

APP / GD VERSION	GD APP ID	GD
Good Access		

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



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

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

3. On the **Access Keys** tab, press **New Access Key**.

The screenshot shows the 'Manage User' interface for a user named Hristo Ilchev. At the top, there are three buttons: 'Resend Welcome Email', 'Remove User', and 'Refresh'. Below the user name, there are fields for 'Policy Set' (set to 'Good Default Policy') and 'App Groups' (with a pencil icon). A navigation bar at the bottom of the user management section has three tabs: 'DEVICES', 'APPS', and 'ACCESS KEYS', with 'ACCESS KEYS' being the active tab. Below the navigation bar are four buttons: 'Delete', 'Resend keys', 'New Device Enrollment Key', and 'New A...'. The main content area is titled 'PROVISIONED ACCESS KEYS' and contains a table with one row of data.

<input type="checkbox"/>	KEY	TYPE	STATUS
<input type="checkbox"/>	zf1v4-c7pvq- [REDACTED]	Access Key	Expires on Dec 27, 2015 at 6:09 PM.

0 of 1 selected

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

Enrolling the Acronis Access client app in BlackBerry Dynamics

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

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

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

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

3. Progress will be displayed as your app is enrolled with BlackBerry Dynamics.
4. If required by your BlackBerry Dynamics policy, you will be asked to set an application lock password. If you are also using BlackBerry for Enterprise, Acronis Access may require that you log into BlackBerry for Enterprise in order to gain access to the Acronis Access app. Once this process is completed, you will be taken to the Acronis Access application's home screen.

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

Aside from that requirement, Acronis Access for BlackBerry Dynamics functions the same way that the standard Acronis Access app does. Some features in the app may be restricted based on your BlackBerry 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.

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

Side-loading Acronis Access

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

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

Note: *The Acronis Access app is not actively involved in the iTunes File Sharing file transfer process.*

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

Preparing Documents for Side Loading

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

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

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

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

Sync the items through iTunes

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

Enrolling and importing the side-loaded documents

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

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

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

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

Important notes

- Any assigned sync folders that do not have a corresponding folder in the To Import folder will be silently ignored and will perform a standard, full over-the-air initial sync after the import process completes.
- Any folders in the To Import folder that do not match an assigned network sync folder will be silently ignored and deleted from the device.
- If the user leaves the app while the import is executing, it will continue to run in the background for up to 10 minutes. This time period is depended on iOS app management out of Acronis Access control. If the Acronis Access app is shut down by iOS or the end user, the import process will continue where it left off the next time the app is started.
- After the preloaded files and folders have been copied into the appropriate sync folders, the app will perform an over-the air sync. During this first sync, the app will consider any files side-loaded into the app as up-to-date as long as the server version of that file has the same file size. The

timestamps on the files will not be expected to match, so if the sizes match, the local file's timestamp will be updated so that it matches the server version. If the sizes do not match, the file will be automatically synced down from the server and replaced. This will not trigger any conflict detection behavior.

- A policy setting will be added to the BlackBerry Dynamics application policy section for Acronis Access (on the BlackBerry Control server) that governs whether this side-loading behavior is active. By default, this feature will be disabled. If disabled in the BlackBerry Dynamics policy, the enrolled/activated Acronis Access for BlackBerry app will delete any files and folders that are copied into the Documents folder via iTunes File Sharing, each time the app starts up.

13.3.2.2 For Android

In this section

Introduction	291
Requesting and configuring Acronis Access within BlackBerry Control	292
BlackBerry Dynamics Policy Sets and Acronis Access	295
Granting Acronis Access access to a BlackBerry Dynamics User or Group	296

Introduction

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

The components of the BlackBerry Dynamics platform include:

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

Acronis Access for BlackBerry Dynamics requires:

- **Acronis Access for BlackBerry Dynamics client app** - The Acronis Access for BlackBerry Dynamics client app available on the Apple App Store <http://www.grouplogic.com/web/megoodappstore> is specifically designed as a BlackBerry Dynamics integrated application. When first installed and run on a device, the Acronis Access for BlackBerry Dynamics app will prompt the user to activate the app in BlackBerry Dynamics. This activation is required before the user can proceed with enrolling the app with their Acronis Access server and accessing file.

- **Acronis Access server** - Acronis Access for BlackBerry Dynamics uses the same server-side software as standard Acronis Access. No server-side changes are required for Acronis Access servers to work with BlackBerry 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 BlackBerry Dynamics.

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

Requesting and configuring Acronis Access within BlackBerry Control

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

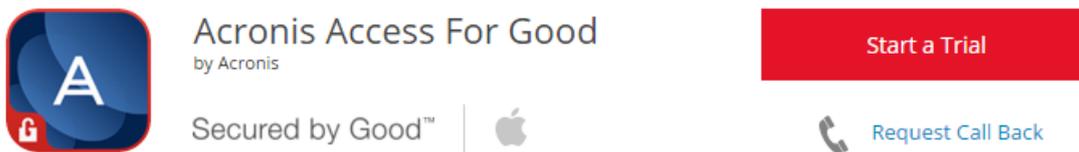
In this section

.....	292
.....	293

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

On the Acronis Access for <https://begood.good.com/gd-app-details.jspa?ID=248978> BlackBerry app page, click the Start Trial button to request a trial or get the licensed version of the app. <https://begood.good.com/gd-app-details.jspa?ID=248978>

Good Dynamics Marketplace > Acronis Access For Good

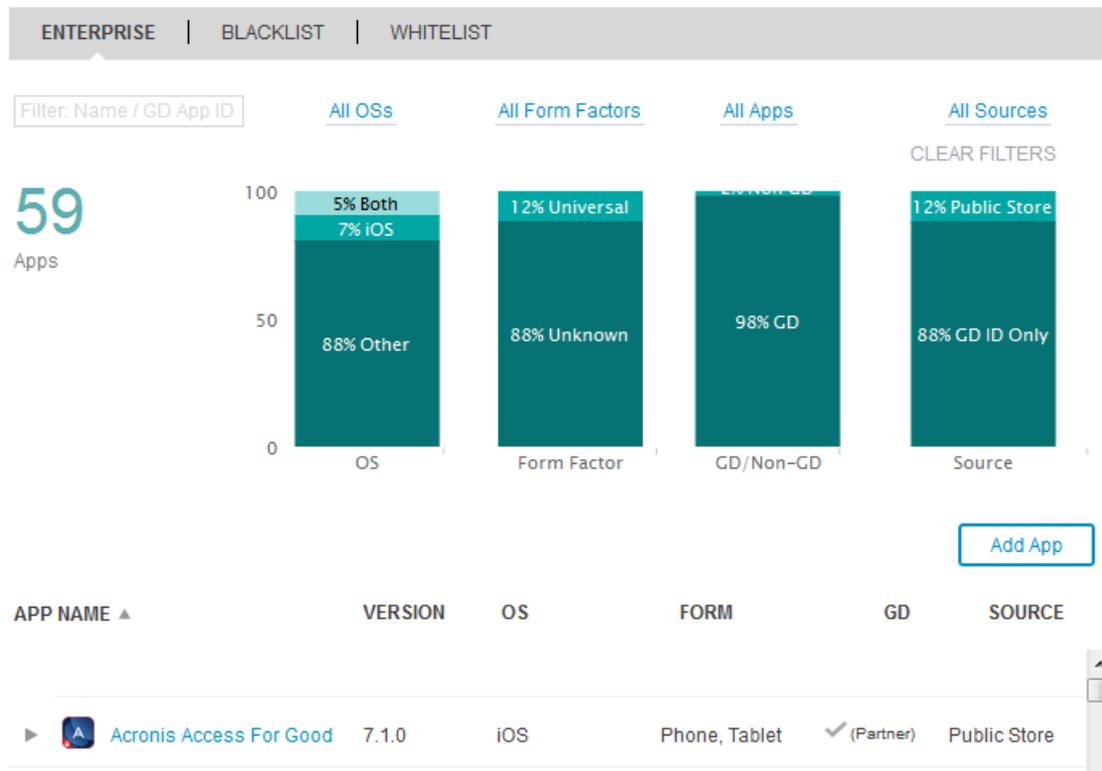


If you select a trial version of the app, your access should be granted within a few minutes. You should receive a notification from the BlackBerry site when your request has been accepted and notify you that the **Acronis Access for BlackBerry** app as been published to your BlackBerry Control server.

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

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

Manage Apps



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

Allowing access from your domain

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

Client Connections

▼ ALLOWED DOMAINS *. 

Route All 

DOMAIN	PRIMARY GP CLUSTER	SECONDARY GP CLUSTER	ACTIONS
*(All Domains)	-- Not set --	-- Not set --	 
*.acronisdemo.com	First	-- Not set --	  
*.glilabs.com	First	-- Not set --	  
*.glilabs2008.com	First	-- Not set --	  
*.grouplogic.com	First	-- Not set --	  

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

Assigning your domain as a default domain for connections

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

Allowing specific servers to connect

▼ ADDITIONAL SERVERS  

SERVER	PORT	PRIMARY GP CLUSTER	SECONDARY GP CLUSTER	ACTIONS
ae.grouplogic.com	443	First	-- Not set --	  
ae.grouplogic.com	8043	First	-- Not set --	  
avid.glilabs.com	443	First	-- Not set --	  

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

1. Open the **Client Connections** settings from the lefthand menu.
2. Expand **Additional Servers**.
3. Press the plus (+) icon and enter the DNS name and port of the server you want to grant access to. Repeat this step for all Acronis Access servers you want your Good clients to connect.

BlackBerry Dynamics Policy Sets and Acronis Access

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

These settings include:

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

Data Leakage Protection effects and limitations

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

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

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

Acronis Access for BlackBerry Dynamics includes a BlackBerry Dynamics feature called "Secure Docs". This allows files to be transferred between the Acronis Access for BlackBerry Dynamics app and the BlackBerry for

Enterprise app. Once a file is opened into the BlackBerry for Enterprise app, it can then be opened into other 3rd party BlackBerry Dynamics enabled apps that include this feature. This functionality will be available, even with the BlackBerry Control **Data Leakage Protection** policy setting enabled.

Granting Acronis Access access to a BlackBerry Dynamics User or Group

Before a user can enroll their Acronis Access app in BlackBerry 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 BlackBerry Dynamics applications to individual users, you are required to select specific version numbers of the app to allow. If you manage access on the user level, when new versions of Acronis Access for BlackBerry are released, you will need to return to the users' BlackBerryControl configuration and add the new version before they are allowed to run that version.

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

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

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

Manage User

Resend Welcome Email Remove User Refresh

Hristo Ilchev hristo.ilchev@grouplogic.com

Policy Set [Good Default Policy](#)

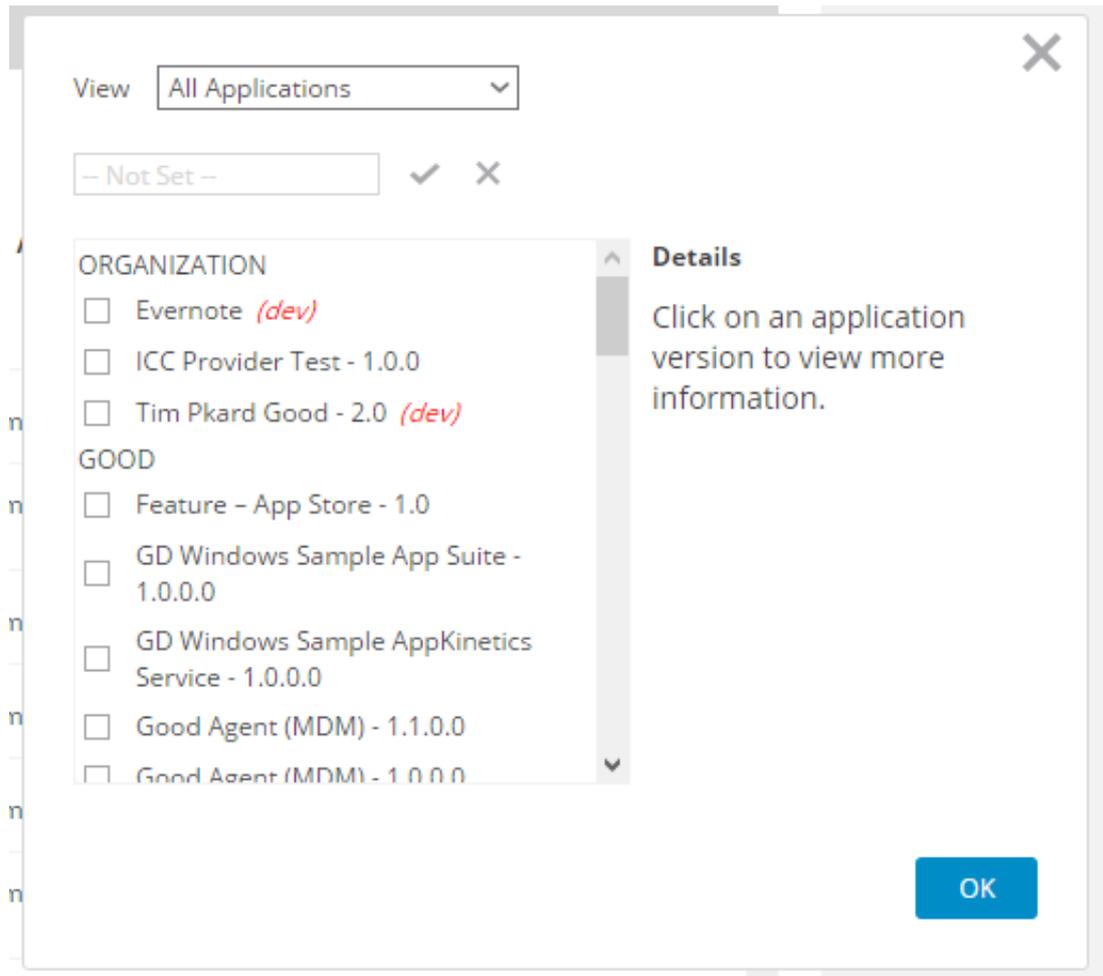
App Groups

DEVICES | **APPS** | ACCESS KEYS

ENTITLED ENTERPRISE APPS

APP / GD VERSION	GD APP ID	GD
Good Access		

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



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

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

3. On the **Access Keys** tab, press **New Access Key**.

The screenshot shows the 'Manage User' interface. At the top, there are three buttons: 'Resend Welcome Email', 'Remove User', and 'Refresh'. Below these, the user's name 'Hristo Ilchev' and email 'hristo.' are displayed. The 'Policy Set' is 'Good Default Policy'. Under 'App Groups', there is a pencil icon. A navigation bar at the bottom of the user profile section has three tabs: 'DEVICES', 'APPS', and 'ACCESS KEYS', with 'ACCESS KEYS' being the active tab. Below the navigation bar are four buttons: 'Delete', 'Resend keys', 'New Device Enrollment Key', and 'New A...'. The main content area is titled 'PROVISIONED ACCESS KEYS' and contains a table with one row of data.

<input type="checkbox"/>	KEY	TYPE	STATUS
<input type="checkbox"/>	zf1v4-c7pvq- [REDACTED]	Access Key	Expires on Dec 27, 2015 at 6:09 PM.

0 of 1 selected

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

13.3.3 Microsoft Intune

Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure. To enroll mobile devices you must set Intune as your mobile device authority and then configure the infrastructure to support the platforms you want to managed. This requires establishing a trust relationship with the device.

Note: This feature is only supported by the iOS Acronis Access client version iOS 7.0.5 or newer.

Note: In order for Acronis Access to be managed by Intune, it must be installed through the **Microsoft Intune Company Portal** application.

In this section

.....	299
.....	299
.....	299

4.

1. In the Azure portal, select **More Services** from the left sidebar and enter **Intune**.
2. Select **Intune**, open **Mobile Apps** and open **Apps**.
3. Press **Add** and click on the **App type** drop-down.
4. Select **iOS store app** and click on **Search the App Store**.
5. Enter **Acronis Access** to find the app, select the standard Acronis Access app and press **OK**.
6. Click on **App information** and tweak how the app will appear in the Intune app store (e.g. name, icon, device type and etc.).
7. After all steps are completed, press **Add**. The app will now be available in the management portal for configurations and policies and in the Intune store for download by users.

1. Open the **Azure** management portal and open the **Groups** page.
2. Select **All Groups** and press **New Group**.
3. Enter the name and description of the group.
4. Select the **Membership type**. **Assigned** will let you select the users that will be invited to the group.
5. Press **Create** when ready. Your group is now created and ready.

Mobile App Configuration Policy

This policy affects only the Acronis Access app.

1. Open the **Azure** management portal and open **Intune -> Mobile Apps -> App configuration policies** page.
2. Press **Add**, enter a **Name** and select **Enrolled with Intune**.
3. Select **iOS** as the platform and select Acronis Access from the list of apps.
4. Click on **Configuration Settings** and select **Use configuration designer** from the drop-down.
5. Enter the desired managed app configuration keys. You can see the Acronis Access supported ones at Using iOS Managed App Configuration features (p. 279). For information on how to set them up, please check Microsoft Intune documentation.
6. When you're satisfied with all the settings, press **Add**.

Mobile Application Management Policy

1. Open the **Azure** management portal and open **Intune -> Mobile Apps -> App protection policies** page.
2. Press **Add policy**, enter a **Name** and select **iOS** for the **Platform**.
3. Select Acronis Access from the list of apps.
4. Click on **Settings** and select all desired settings. You can use the defaults by pressing **OK**.
5. Press **Create**.

Once all of the configuration of **Groups** and **Policies** is complete, all that's left is to deploy the app to your users.

Managing deployment

1. Open the **Intune** management portal and open the **Apps** page.
2. Click on the Acronis Access app and select **Manage Deployment** from the menu.
3. Select the groups which will receive the app and press **Next**.
4. Select what the deployment will be for each user or group. The options are:
Required (mandatory install), **Available** (users install from the company portal on demand), **Not Applicable** (the app is not installed or shown in the company portal), **Uninstall** (the app will be uninstalled from targeted devices).
You can also set a deadline for the **Required** installations. Press **Next** when all configurations are done.
5. Select the **Mobile Application Management Policy** for each user and group. This step requires that you have a policy setup and is mandatory. Press **Next**.
6. Skip the **VPN Profile** settings by pressing **Next**.
7. Select the **Mobile App Configuration Policy** for each user and group and press **Finish**.

13.3.4 MobileIron AppConnect support

In this section

Introduction	300
Testing a trial version of Acronis Access with AppConnect	301
Integrating the Acronis Access Android client with MobileIron	301
Integrating the Acronis Access iOS app with MobileIron	303
Creating an AppConnect configuration and policy for Acronis Access on your MobileIron VSP	304
Activating the Acronis Access iOS client with AppConnect	309
Ongoing AppConnect management of Access Mobile Clients.....	310
Using AppConnect with Kerberos Constrained Delegation	311

13.3.4.1 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 Android app** - A special MobileIron version of the app is required. It can be downloaded from http://support.grouplogic.com/?page_id=4566. This version of the app must be added to your **Apps@Work** store.
- **Acronis Access Server** - The standard version of Acronis Access Server (version 5.0 or later), is fully compatible with mobile clients managed by AppConnect.

13.3.4.2 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>
3. The Acronis Access Android app is a free download from one of our support sites
http://support.grouplogic.com/?page_id=4566.
4. The Acronis Access mobile apps need to have an AppConnect configurations and policies created on your MobileIron Virtual Smartphone platform (VSP) before they can be auto-configured for access to your Acronis Access Gateway server(s).
5. Mobile devices also need to have the MobileIron Mobile@Work app installed before any AppConnect-enabled apps can be activated and before the Acronis Access app can be installed. Mobile@Work is a free download from both the Apple app store and the Google Play store.
6. When you are ready to activate Access Mobile Clients with AppConnect, please proceed to the following sections of this document.

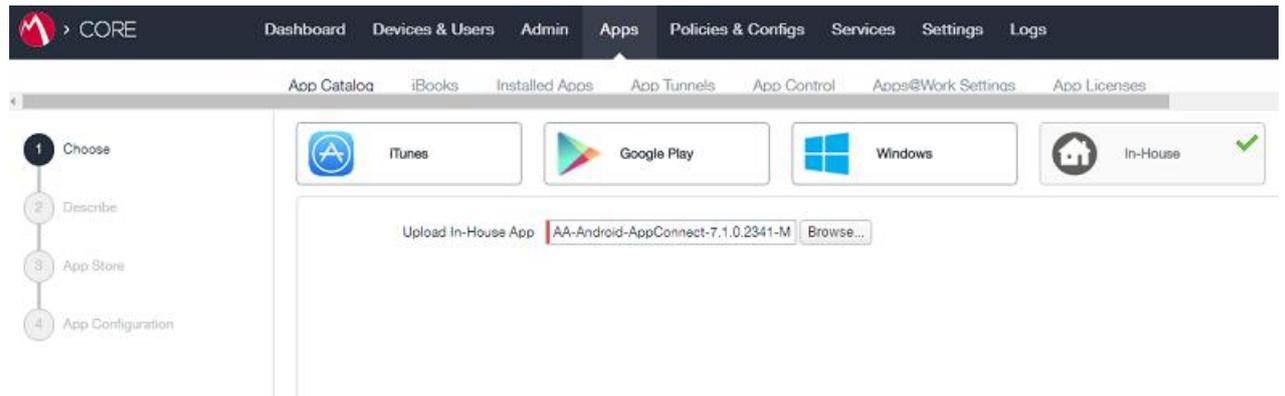
13.3.4.3 Integrating the Acronis Access Android client with MobileIron

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

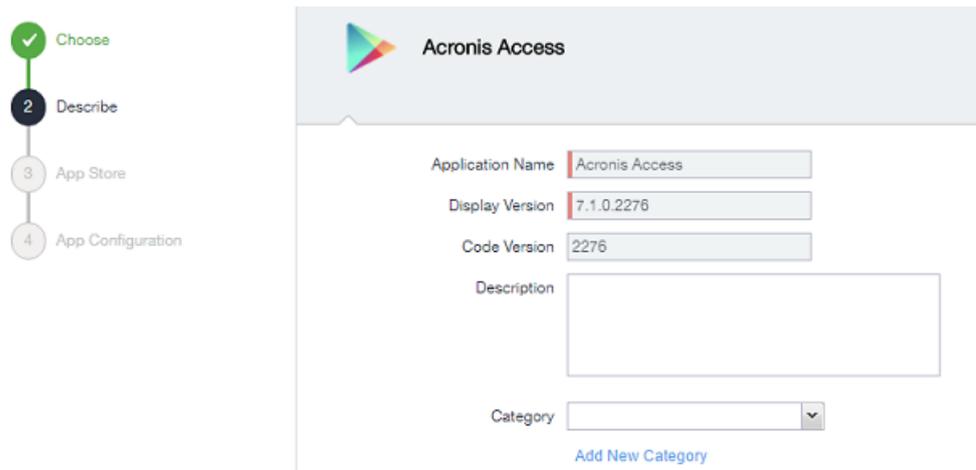
Note: Make sure that the version you download is compatible with your version of MobileIron's **Secure Apps Manager**.

2. Log in to your MobileIron Core console.
3. Open the **Apps** tab and select **App Catalog**.
4. Press **Add+** and select **In-House**.

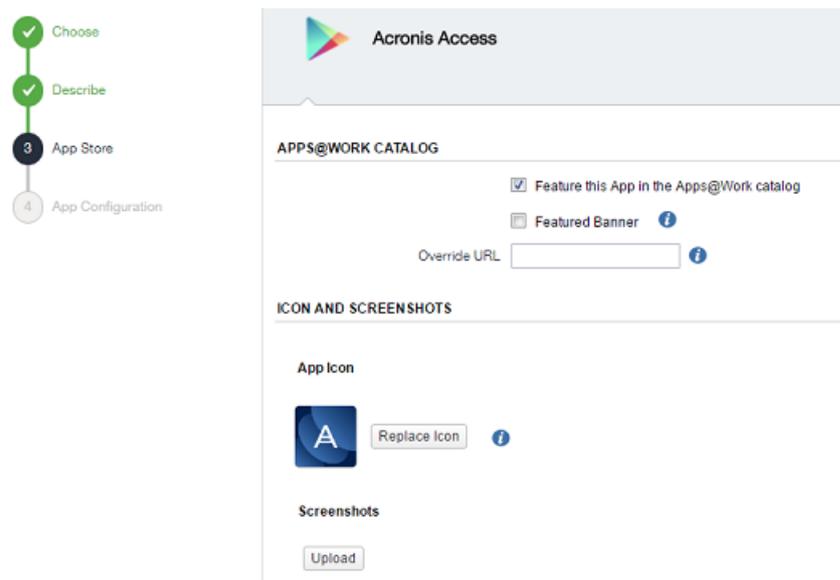
- Press **Browse**, navigate to and select the **Acronis Access Android .apk**.



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



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



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

Choose

Describe

App Store

4 App Configuration

Acronis Access

APP INSTALLATION SETTINGS

Mandatory

Silently install

Enforce this version

PER APP VPN SETTINGS

Per App VPN by Label Only

License Required

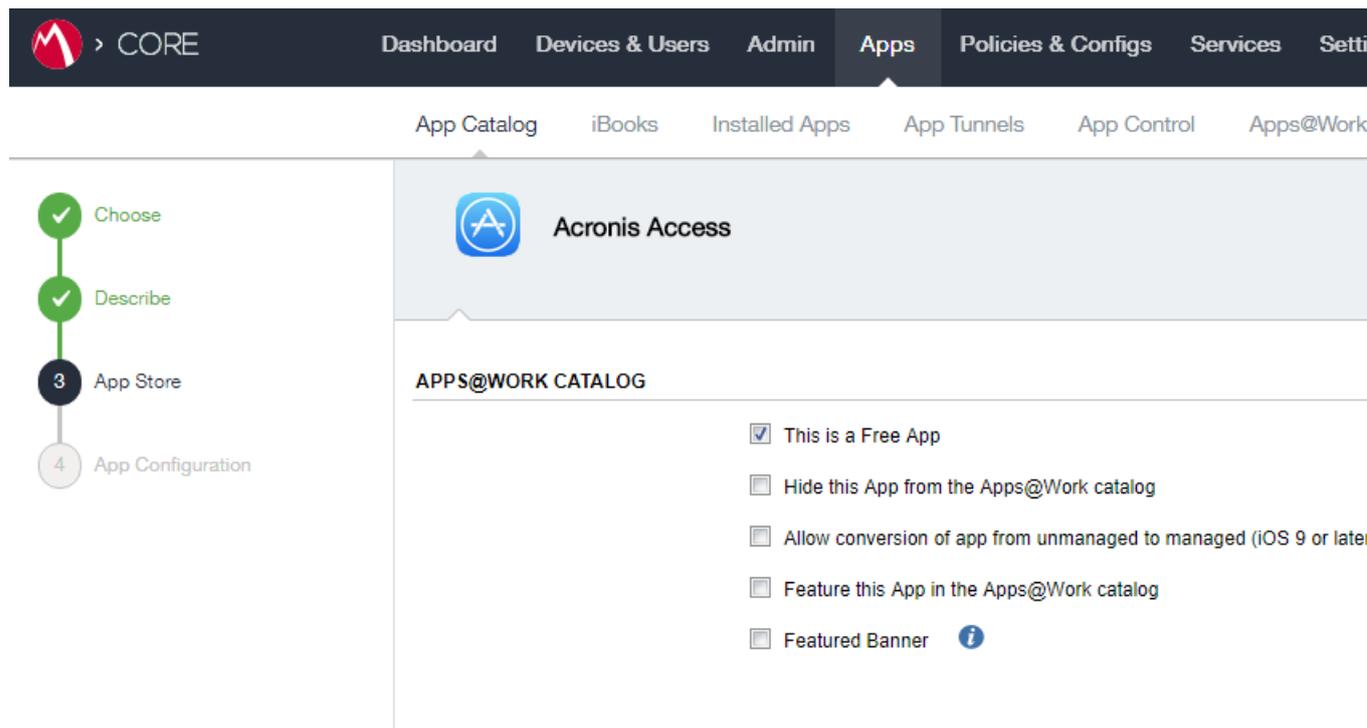
Back Skip Finish

13.3.4.4 Integrating the Acronis Access iOS app with MobileIron

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

1. Log in to your MobileIron Core console.
2. Open the **Apps** tab and select **App Catalog**.
3. Press **Add+** and select **iTunes**.
4. Enter **Acronis Access** in the search-box and press **Browse**, select the latest version of Acronis Access.
5. Press **Next**. Enter a description for the app and press **Next**.

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



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

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

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

Before you can start on-boarding Acronis Access users (p. 75). You will need to create two items on your MobileIron VSP:

- 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.
- 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.....	304
Creating a Acronis Access app Container Policy	307
Assign labels to the new Configuration and Container Policy	309

Creating a Access Mobile Client app Configuration

- Log into your MobileIron VSP web console and select the **Policies & Configs** tab.
- Click on the **Configurations** tab and press Add New.

3. In the drop-down menu, navigate to **AppConnect** and select **App Configuration**.

The screenshot shows the Acronis CORE interface. At the top, there is a navigation bar with the CORE logo and menu items: Dashboard, Devices & Users, Admin, Apps, and Policies. Below this, there are tabs for Configurations, Policies, ActiveSync Policies, and Com. The main content area displays a table of configurations. A dropdown menu is open over the 'Add New' button, listing various categories: Android, Exchange, Email, Wi-Fi, VPN, AppConnect, Certificates, Certificate Enrollment, Docs@Work, Web@Work, iOS and OS X, and Windows. The 'AppConnect' category is selected, and a sub-menu is open showing 'App Configuration' and 'Container Policy'. The table below the menu has columns for Name, Package ID, Description, # Phones, and Labels.

Name	Package ID	Description	# Phones	Labels
Access 7 Enterprise MA...	acronis.acce...		0	
Access 7 Enterprise Poli...	acronis.acce...		0	
Access 7 Proto	grouplogic.ac...		0	
Access 7.0.5	grouplogic.m...		0	
Access Android Config			0	
Access Android Policy			0	
Access Beta In-House 9		Appli...	0	
Access Beta In-House d		Appli...	0	
Acronis Access Beta Act		Appli...	0	
Acronis Access Beta File		Appli...	3	
Acronis Access Enterpri		Appli...	0	

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

New AppConnect App Configuration

Name:

Description:

Application:

AppTunnel Rules
Enter the tunneled hosts and their target Sentry services. Drag host rules in the order that should be evaluated.

SENTRY	SERVICE	URL WILDCARD	PORT		
misentry.giliabs.com	avid	*.company.com	3000	=	×

Identity Certificate:

App-specific Configurations

KEY	VALUE	
enrollmentPIN		×
enrollmentUserName		×
enrollmentServerName	access.company.com	×

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

Description – This can be any description you like.

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

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

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

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

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

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

App-specific Configurations – This section allows you to specify values that will be used to auto-complete the Acronis 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. 102) 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**
- **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 MobileIron's **\$USERID\$** wildcard, which will auto-complete the field with the username which the user has entered when setting up their Mobile@Work app.
- **enrollmentPassword** – This key is optional. The value of this key will be inserted into the Password field in the Acronis Access enrollment form. You can use MobileIron's **\$PASSWORD\$** wildcard, which will auto-complete the field with the password which the user has entered when setting up their Mobile@Work app.

Creating a Acronis Access app Container Policy

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

4. Within this new **Container Policy**, enter the following information:

New AppConnect Container Policy

An app is authorized only if an AppConnect container policy for the app is present on the device. This policy also allows you to define app-specific settings.

Name

Description

Application 

Exempt from AppConnect passcode policy 

SECURITY POLICIES

▼ **iOS Data Loss Prevention**

- Allow Print
- Allow Copy/Paste To
- Allow Open In

▼ **Android Data Loss Prevention** 

- Allow Screen Capture

[Cancel](#) [Save](#)

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

Description – This can be any description you like.

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

Exempt from AppConnect passcode policy - Select this option if you would like users to be able to open Acronis 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.

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**.

13.3.4.6 Activating the Acronis Access iOS client with AppConnect

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

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

Once the needed Configuration and Container Policy have been created on the MobileIron VSP, you are ready to install and configure Acronis 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, but has not yet been enrolled with a Acronis Access Server
- Acronis Access has already been installed on the device, and has already been enrolled with a Acronis Access Server
- Acronis Access has not yet been installed on the device310

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.

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.

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.

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

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

Acronis Access has not yet been installed on the device

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

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.

13.3.4.7 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.

13.3.4.8 Using AppConnect with Kerberos Constrained Delegation

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

The Android and Windows mobile apps do not support this configuration.

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

As this is a complex setup in order to reduce errors and simplify troubleshooting, it will be accomplished in two phases. The first phase will establish an AppTunnel using username/password to authentication to the Acronis 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 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 be able to authenticate to Network shares, Sync&Share folders and SharePoint sites.

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 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 and
 Adding Kerberos Constrained Delegation Authentication.....324

14 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 multi-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

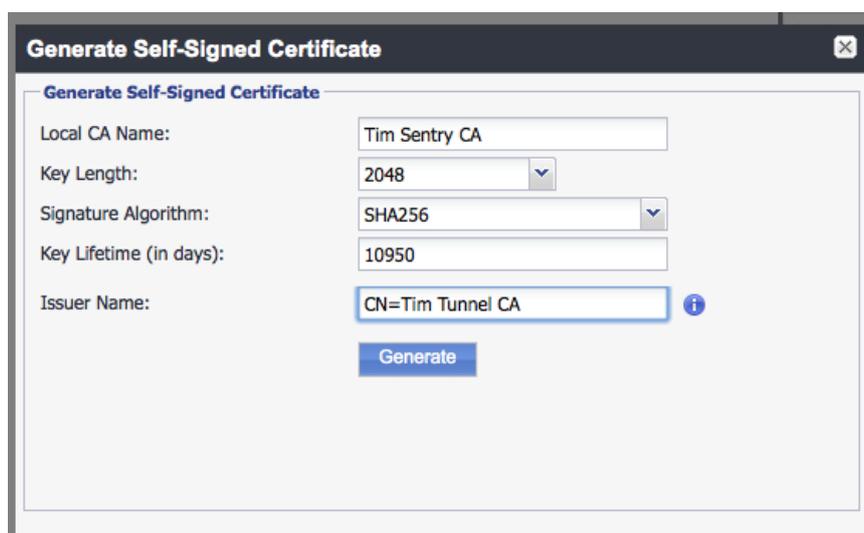
You may have an alternate Certificate Authority (CA) and Simple Certificate Enrollment Protocol (SCEP) provider but this guide assumes you do not for completeness sake. Please consult MobileIron documentation for configuring a third party CA and SCEP provider.

In this section

Configuring Acronis Access on the VSP	316
Verify AppTunnel usage	322

5.

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



The screenshot shows a window titled "Generate Self-Signed Certificate" with a close button in the top right corner. Inside the window, there is a form with the following fields and values:

- Local CA Name: Tim Sentry CA
- Key Length: 2048 (selected from a dropdown menu)
- Signature Algorithm: SHA256 (selected from a dropdown menu)
- Key Lifetime (in days): 10950
- Issuer Name: CN=Tim Tunnel CA (with an information icon to the right)

At the bottom of the form is a blue "Generate" button.

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

4. Click **Generate**.

Certificate Template ✕

CA Certificate

CA Certificate: [0]

```

Version: 3
SerialNumber: 5021272919645868630
IssuerDN: CN=Tim Tunnel CA
Start Date: Wed May 07 10:28:26 PDT 2014
Final Date: Fri Apr 29 10:28:26 PDT 2044
SubjectDN: CN=Tim Tunnel CA
Public Key: RSA Public Key
modulus:
94452d641eb39cd7a7af97ed816c0af5fd0a56c9bd472afce7f7cc4f2f4548a6ceee
0c7f6b411cd65bfb05f3c228c1bae1203450565e08b6f313131aa3e3022762c82a62
b3a789043d11158da4e7e960c39c5355e3accb0f2860d2934b0e9847b5750d5b3858
984f2bd99c7f82e04e3deb7565b16afa9b46a34ddc8323fac5f1b5e34d4fc7265a8f
11953d66296d0bdf75776913ee075c96267511189460223903fbf9f5238a6c6d54cb
0c147f375e4941bfab8fe7d30058afa34335d518bcd91e5a5213762cb701d8713e81
ec53ea25e1884eb7e6324c8410a2527f59613eec6812d1dd5f7c1fb64c5e719f1743
56fc4be1ffdd25d23633bd1267a3ef9b79a7
public exponent: 10001

Signature Algorithm: SHA256WITHRSA
Signature: 68335d3616d0dc761b5525284c8b21bf745931f9
91609930b5db931d8e921760e46c1f2b4797c5c6
          
```

CRL Distribution Point URL:

Cert URL:

CRL Lifetime (hours):

Client Certificate Template

Hash Algorithm:

Minimum Key size Allowed:

Key Lifetime (days):

Enhanced Key Usage:

CLIENT_AUTHENTICATION

IPSEC

SMART_CARD_LOGON

Custom OIDs:

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**.

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

The screenshot shows the 'New SCEP Setting' dialog box with the following configuration:

- Name: Tim Sentry SCEP
- Description: (empty)
- Enable Proxy:
- Cache locally generated keys on the VSP:
- User Certificate: Device Certificate:
- Setting Type: Local
- Local CAs: Tim Sentry CA
- Subject: CN=tunnelingSentry
- Subject Common Name Type: None
- Subject Alternative Name Type: None
- Subject Alternative Name Value: (empty)
- Key Size: 2048
- CSR Signature Algorithm: SHA1
- Key Usage: Signing Encryption

- **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**.

The screenshot shows the 'New Standalone Sentry' dialog box with the following configuration:

- Sentry Host Name / IP: timsentry.no-ip.biz
- Sentry Port: 9090
- Enable ActiveSync: Enable App Tunneling:
- Device Authentication: Identity Certificate
- Trusted Root Certificate Upload: Upload Certificate, View Certificate
- Check certificate revocation list (CRL):
- Certificate Field Mapping: Subject Alternative Name Type: (empty), Value: (empty)

- **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

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**.

New AppConnect Container Policy

An app is authorized only if an AppConnect app policy for the app is present on the device. AppConnect app Policy allows to define app specific policy.

Name:

Description:

Application:

Exempt from AppConnect passcode policy

Data Loss Prevention Policies

iOS

Print **Allow**

Copy/Paste To **Allow**

All apps

AppConnect apps

Open In **Allow**

All apps

AppConnect apps

Whitelist

Android

Screen Capture **Allow**

- **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**.

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

Modify AppConnect App Configuration

Name: Acronis Access app config

Description:

Application: com.grouplogic.mobilecho

App Tunnel

Tunneled hosts and their target Sentry services. Drag host rules in the order that should be evaluated.

URL Wildcard	Port	Sentry	Service
oppenheimer.gillabs.com	443	timsentry.no-ip.biz	ACCESS_GATEWAY

Identity Certificate
Credentials for establishing the app tunnel.
Tim Sentry SCEP

App-specific Configurations

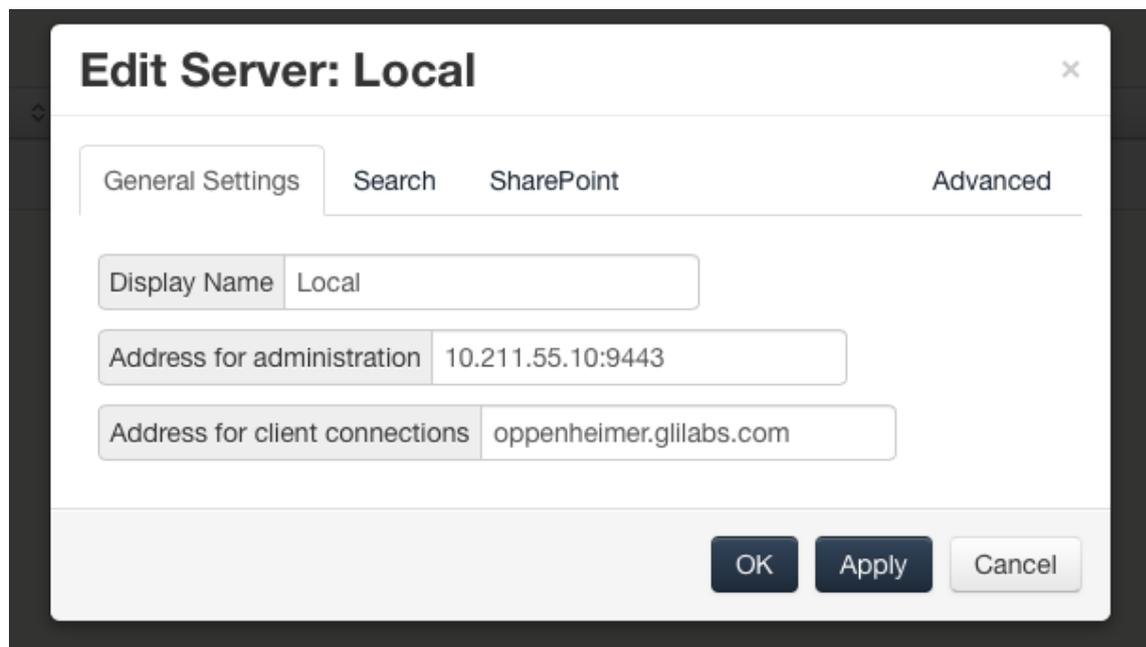
Key	Value
-----	-------

Save | Cancel

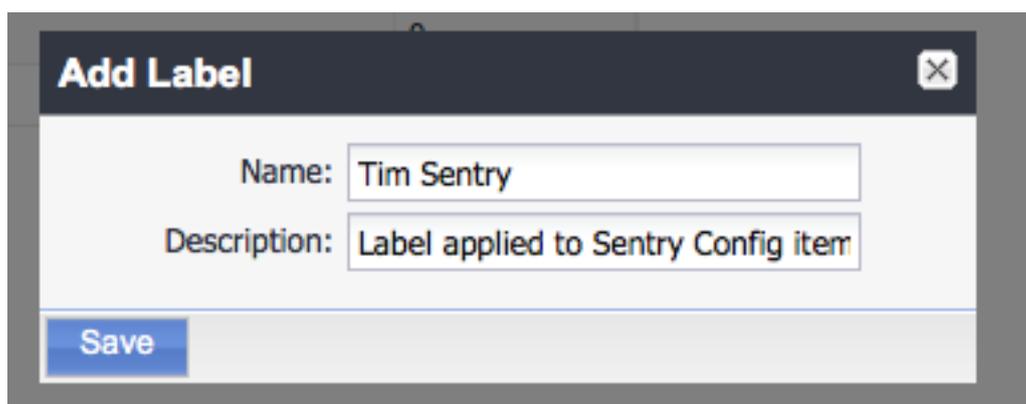
- **Name:** Enter a name based on your preference.
- **Application:** Enter com.grouplogic.mobilecho. This is the Bundle ID as seen in the Apple store.
- **App Tunnel**
 - **URL Wildcard:** The URL that the client will try to contact the Acronis Access gateway server on. This must match the "Address 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**.

*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.

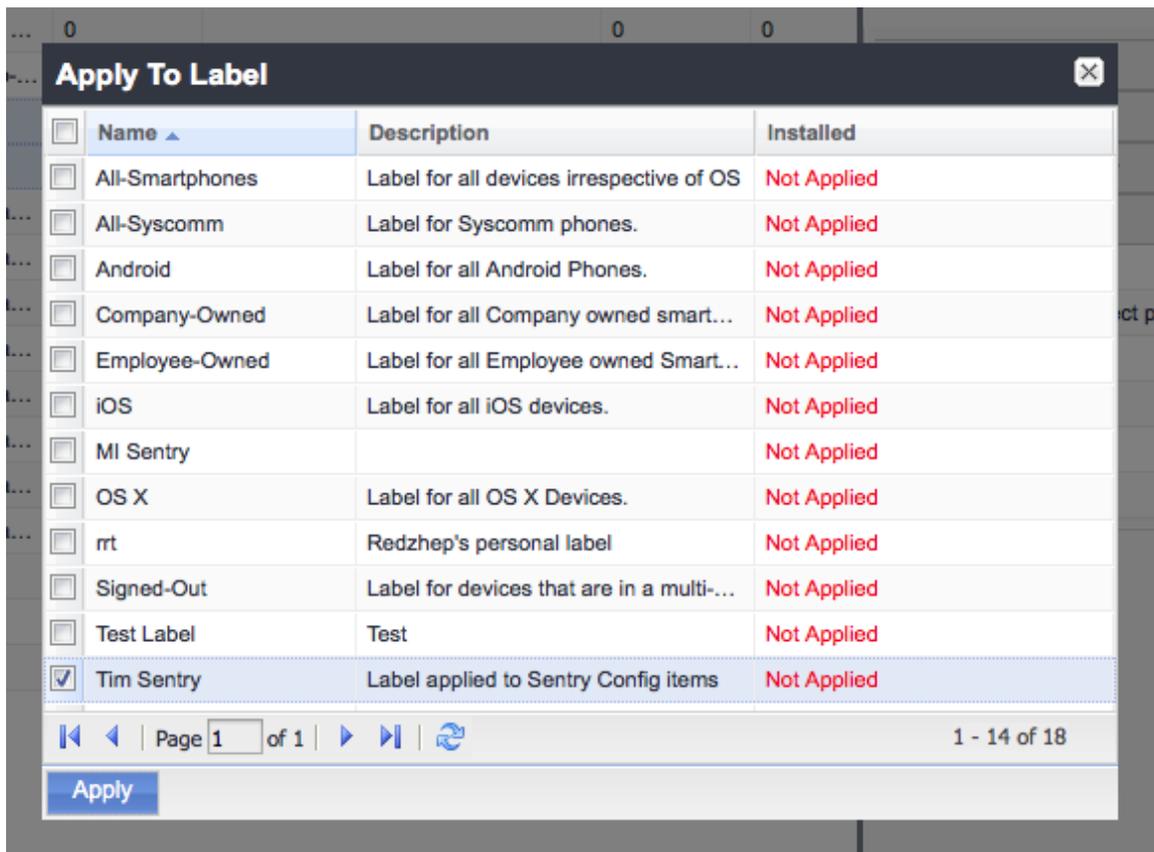


1. Still within the MobileIron VSP Admin Portal, select **Users & Devices** and open **Labels**.
2. Press **Add new**.



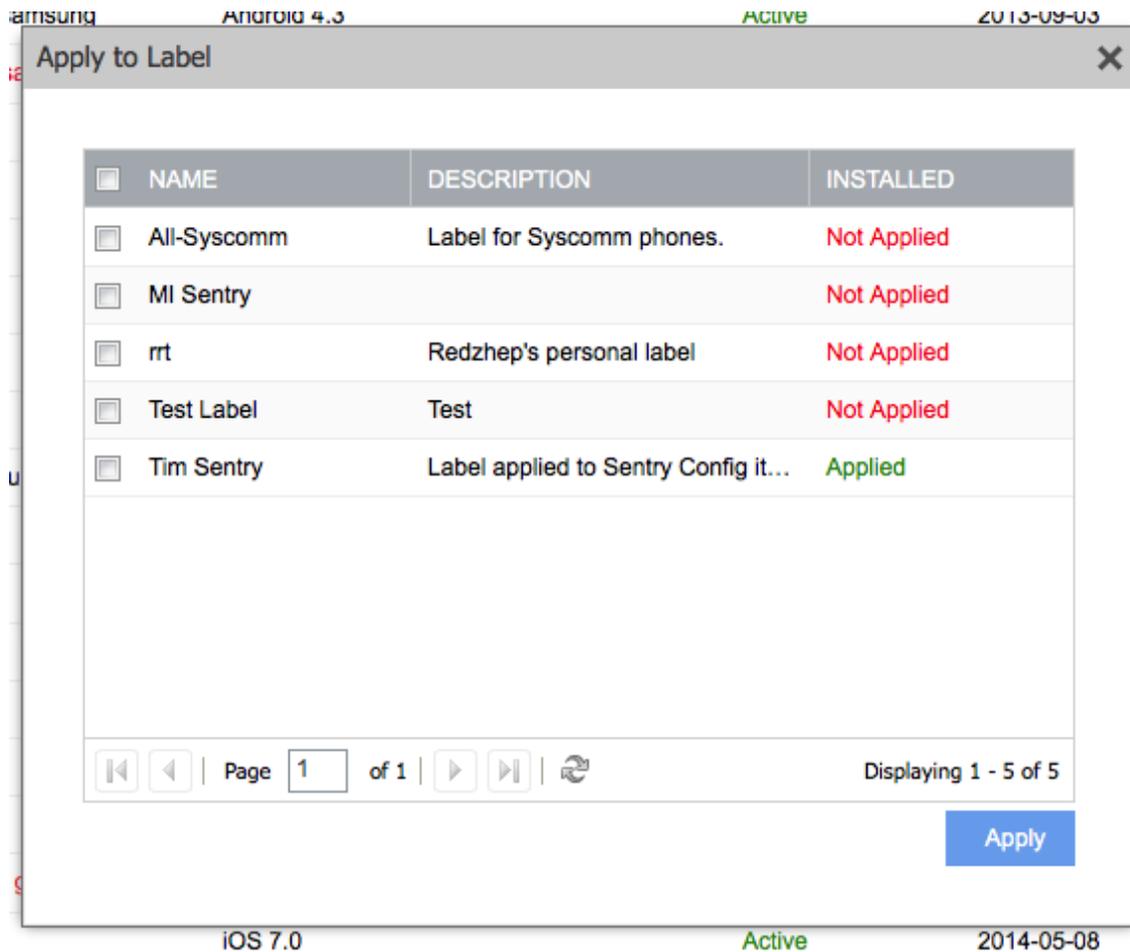
- **Name:** Enter a name based on your preference.
 - **Description:** Enter a description based on your preference.
3. Click **Save**.
 1. Still within the MobileIron VSP Admin Portal, select **Policies & Configs**.

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

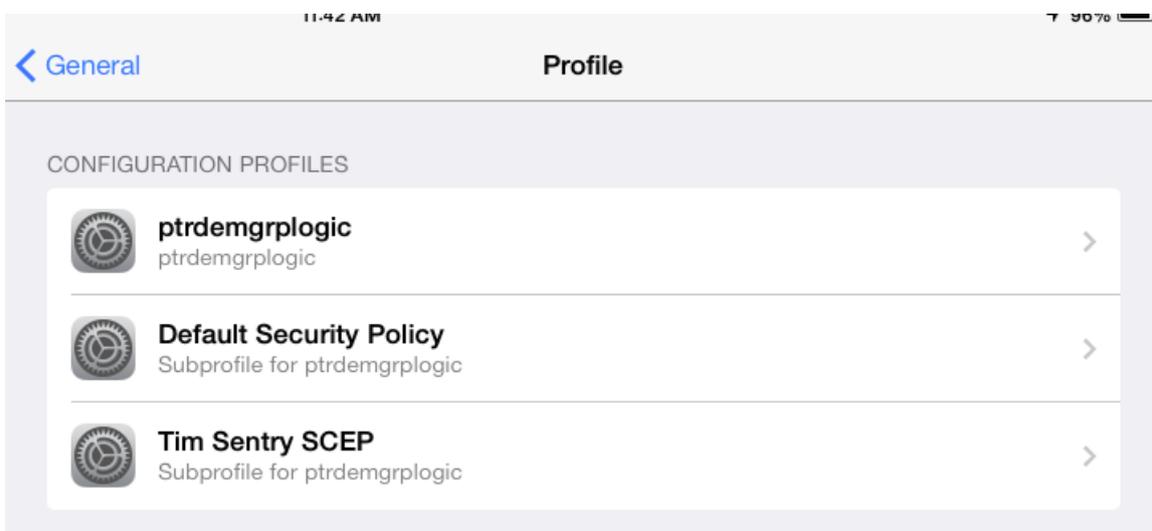


3. Press **More Actions** and select **Apply to Label**.
4. Mark the Label created in "Create a new label".
5. Click **Apply**.
1. Still within the MobileIron VSP Admin Portal, Select **Users & Devices** and open **Devices**.

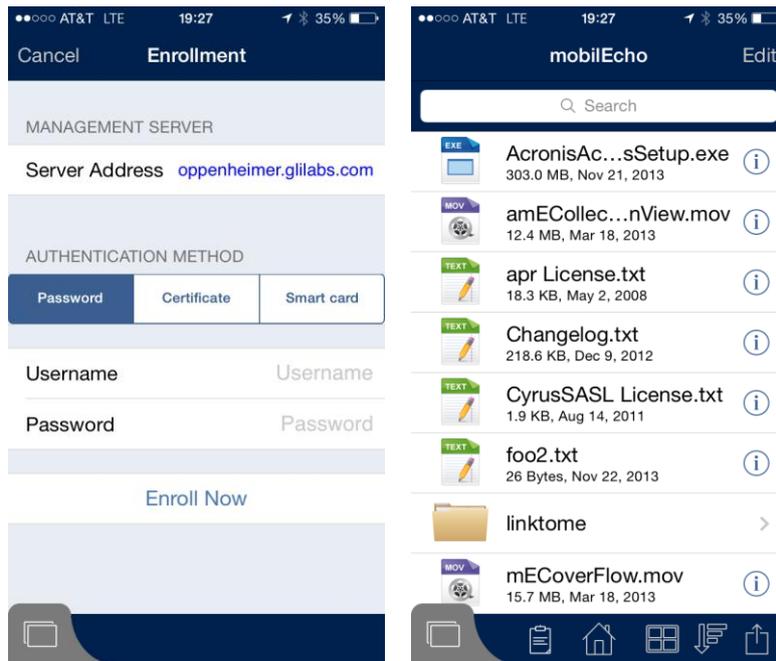
2. Mark the iOS device to be used for Sentry testing.



3. Select **Actions** -> **Apply to Label**.
 4. Check Label created in "Create a new label".
 5. Click **Apply**.
1. Open the Mobile@Work app and open the **Settings**.
 2. Tap on Check for Updates.
 3. Tap on **Force Device Check-In**. If this is successful the SCEP configured in this document should show up in the device settings at **Settings** -> **General** -> **Profiles**.



4. Install Acronis 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 **AppConnect Configuration**. For a true test this URL should not be reachable by the mobile client (use cellular 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."

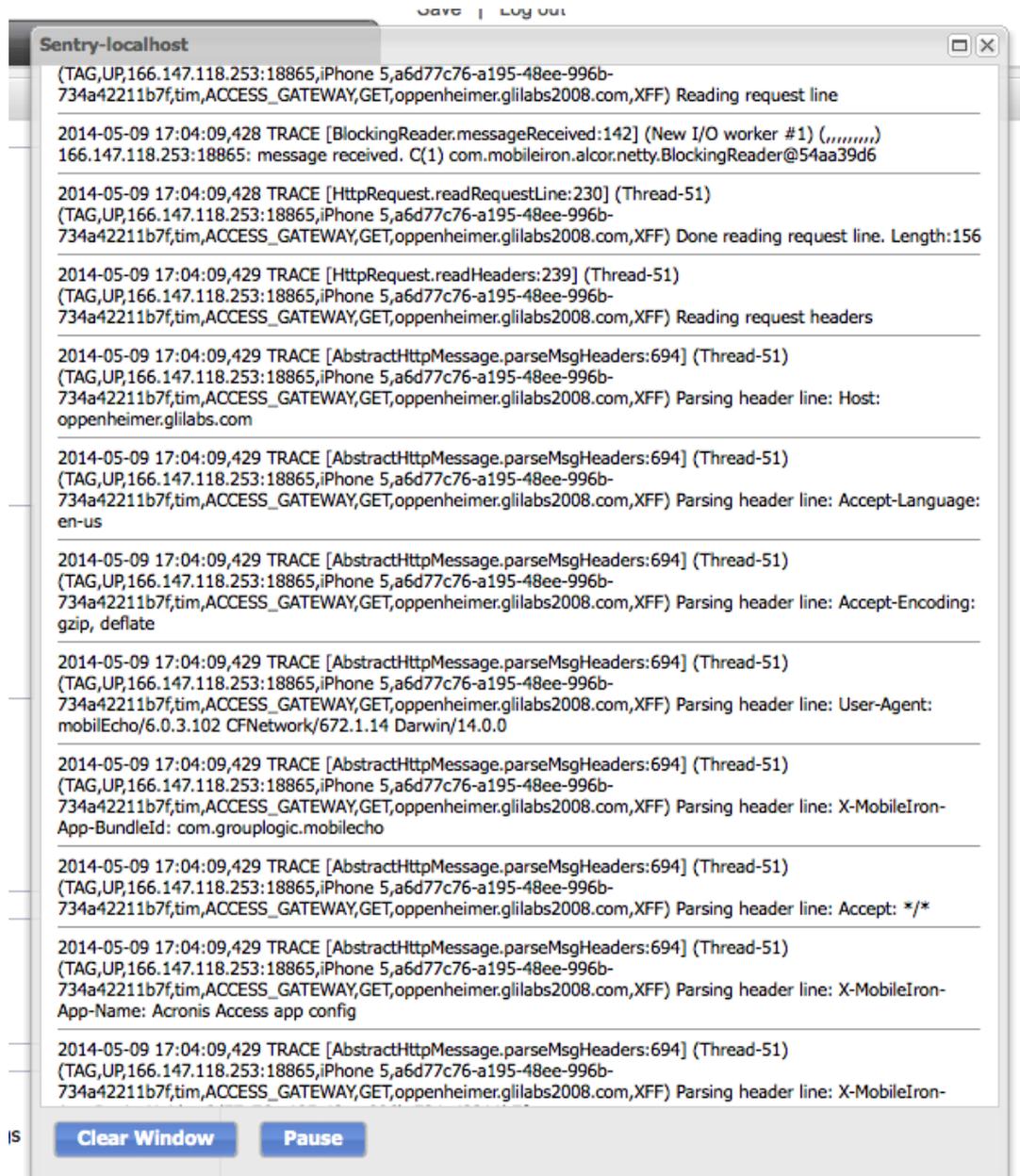
If the data sources in your profile are all part of the Acronis Access Gateway that has been configured to route through the sentry you should be able to browse those sources via the AppTunnel also at this point.

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**.

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



```
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Reading request line
2014-05-09 17:04:09,428 TRACE [BlockingReader.messageReceived:142] (New I/O worker #1) (,,,,,,)
166.147.118.253:18865: message received. C(1) com.mobileiron.alcor.netty.BlockingReader@54aa39d6
2014-05-09 17:04:09,428 TRACE [HttpRequest.readRequestLine:230] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Done reading request line. Length:156
2014-05-09 17:04:09,429 TRACE [HttpRequest.readHeaders:239] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Reading request headers
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: Host:
oppenheimer.gllilabs.com
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: Accept-Language:
en-us
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: Accept-Encoding:
gzip, deflate
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: User-Agent:
mobilEcho/6.0.3.102 CFNetwork/672.1.14 Darwin/14.0.0
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: X-MobileIron-
App-BundleId: com.grouplogic.mobilecho
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: Accept: */*
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: X-MobileIron-
App-Name: Acronis Access app config
2014-05-09 17:04:09,429 TRACE [AbstractHttpMessage.parseMsgHeaders:694] (Thread-51)
(TAG,UP,166.147.118.253:18865,iPhone 5,a6d77c76-a195-48ee-996b-734a42211b7f,tim,ACCESS_GATEWAY,GET,oppenheimer.gllilabs2008.com,XFF) Parsing header line: X-MobileIron-
```

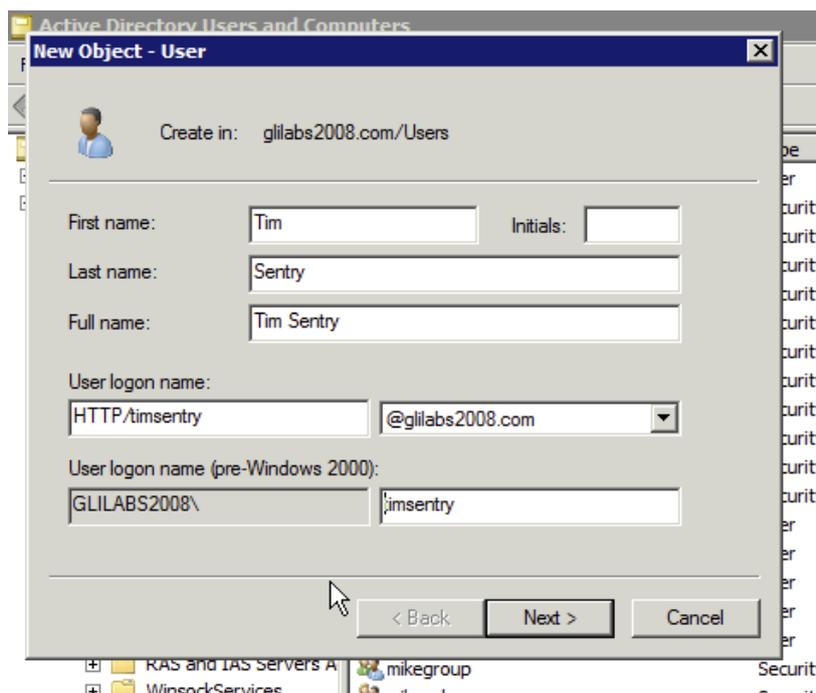
15 Adding Kerberos Constrained Delegation Authentication

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 datasources configured on that gateway. Additional delegation will be required for additional Gateways, Sharepoint servers, and reshares.

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

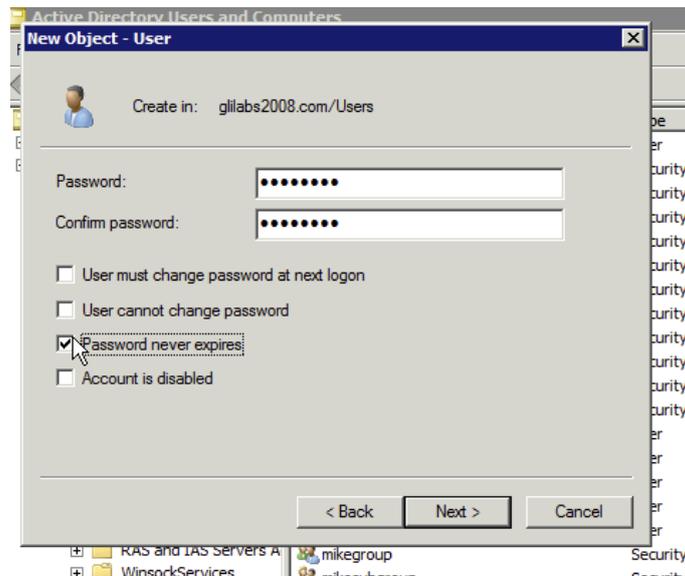
1. Log in to your KDC server as an administrator.
2. From the Windows Start menu, select **All Programs**, select **Administrative Tools > Active Directory Users and Computers**.
3. In the newly opened console, expand the domain (Kerberos refers to a domain as a realm).
4. Right-click **Users** and select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



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

- 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**

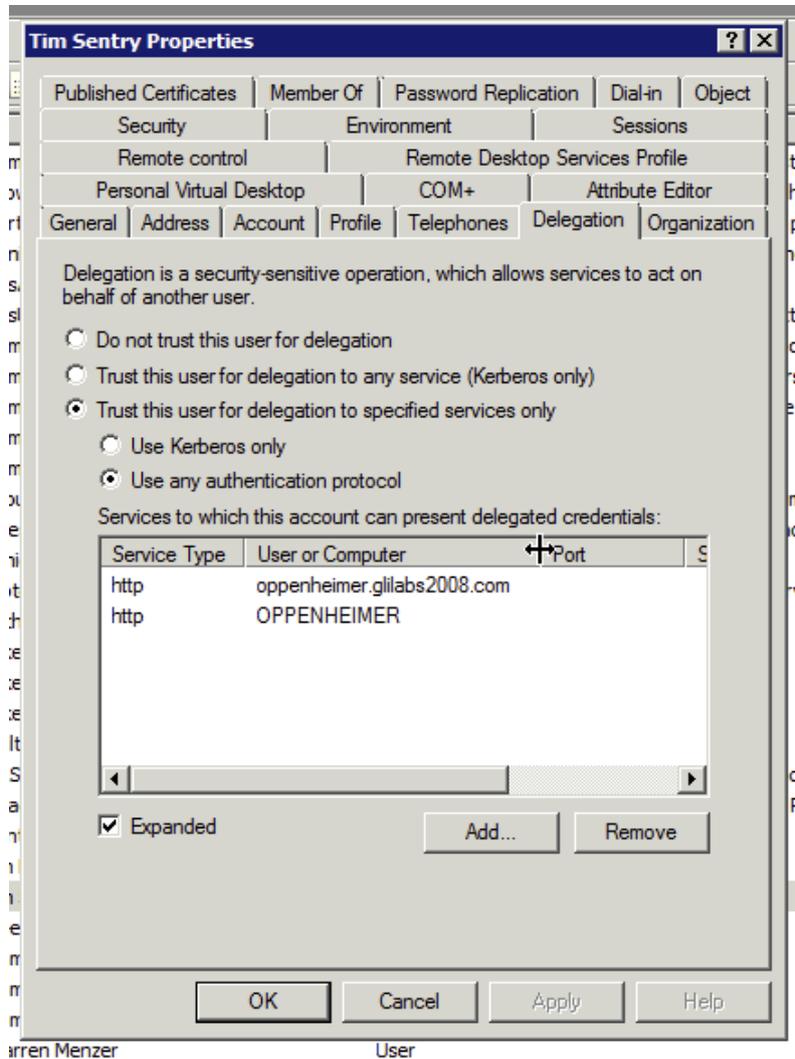
E.g. `ktpass /out timsentry.keytab /mapuser timsentry@glilabs2008.com /princ HTTP/timsentry@glilabs2008.com /pass 123456`

```
C:\Users\Administrator>ktpass /out timsentry.keytab /mapuser timsentry@glilabs2008.com /princ HTTP/timsentry@glilabs2008.com /pass [REDACTED]
Targeting domain controller: dc.glilabs2008.com
Using legacy password setting method
Successfully mapped HTTP/timsentry to timsentry.
WARNING: ptype and account type do not match. This might cause problems.
Key created.
Output keytab to timsentry.keytab:
Keytab version: 0x502
keysize 65 HTTP/timsentry@glilabs2008.com ptype 0 <KRB5_NT_UNKNOWN> vno 3 etype
0x17 <RC4-HMAC> keylength 16 (0x5c875e4d5257b48f74cc445af903ea89)
```

This warning can be ignored.

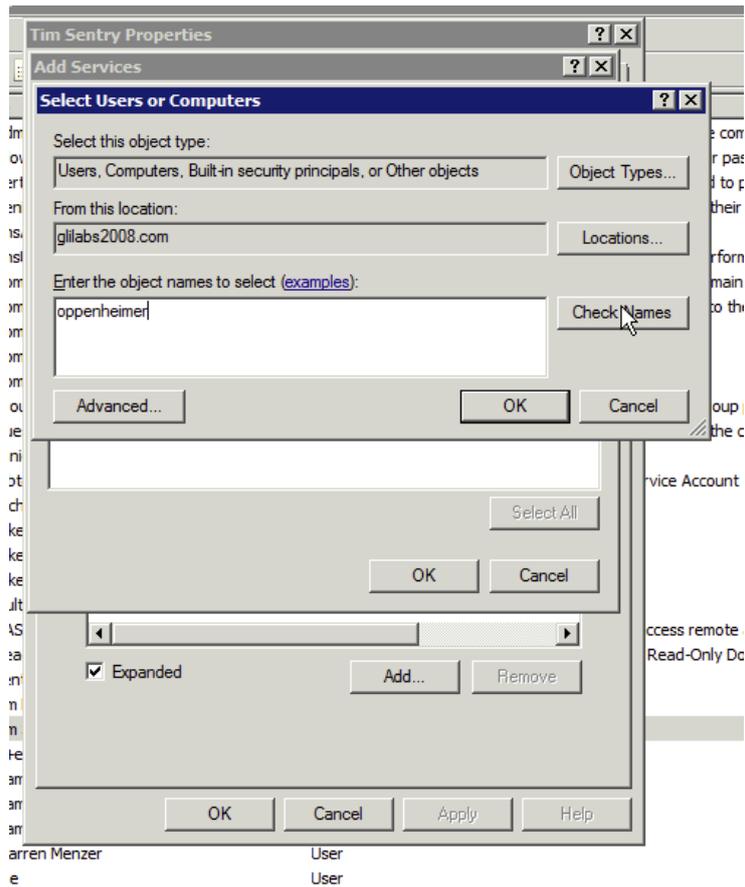
1. From the Windows Start menu, select **All Programs** and open **Administrative Tools > Active Directory Users and Computers**.
2. In the newly opened console, expand the realm (domain).
3. Click on **Users**.

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**.



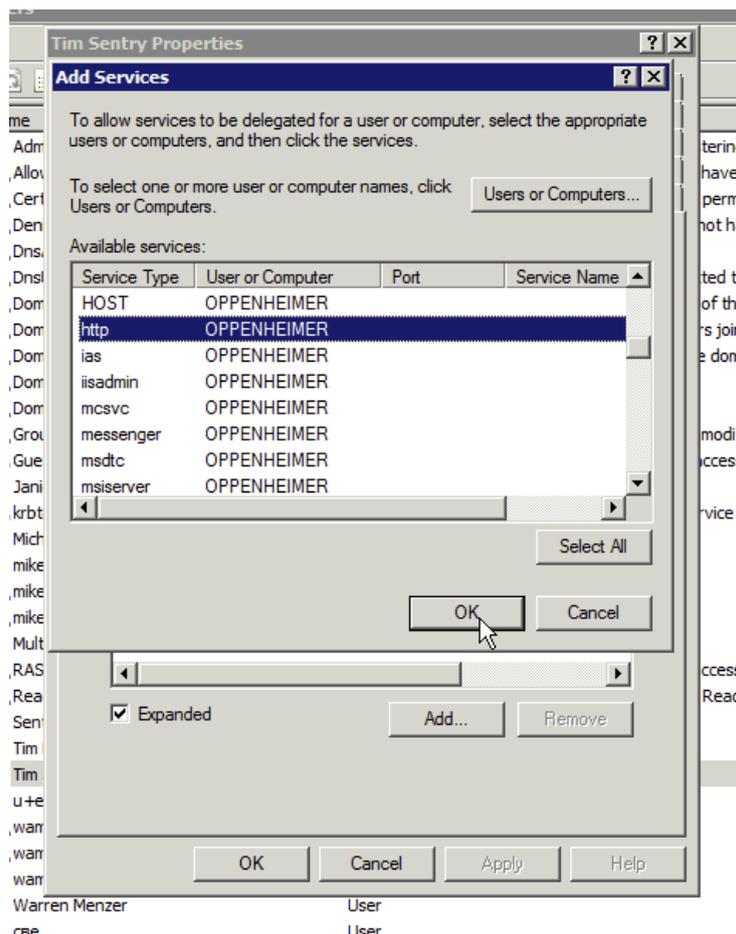
6. Press **Add...**
7. Press **Users or Computers...**
 - Enter the computer name of the Acronis Access Gateway Server.
 - Click on **Check Names**.

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



8. Click **OK**.

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



- 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.

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

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

Modify SCEP Setting

Description:

Enable Proxy:

Cache locally generated keys on the VSP ⓘ

User Certificate Device Certificate

Setting Type: Local

Local CAs: Tim Sentry CA

Subject: CN=tunnelingSentry

Subject Common Name Type: None

Subject Alternative Name Type: NT Principal Name

Subject Alternative Name Value: \$USER_UPN\$ ⓘ

Distinguished Name

Subject Alternative Name Value: \$USER_DNS\$ ⓘ

None

None

Key Size: 2048

CSR Signature Algorithm: SHA1

Key Usage: Signing Encryption

Issue test certificate: ⓘ

Save | Cancel

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

***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**.

Save SCEP Setting

Please confirm that you want to remove cached user/device certificates generated using this profile. Note that all existing cached certificates will be removed and all clients will need to be provisioned with new certificates. Also note that Android clients should be upgraded to version 5.6 or higher before taking this action.

Save

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

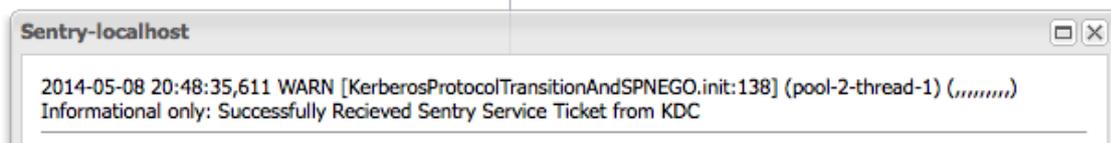
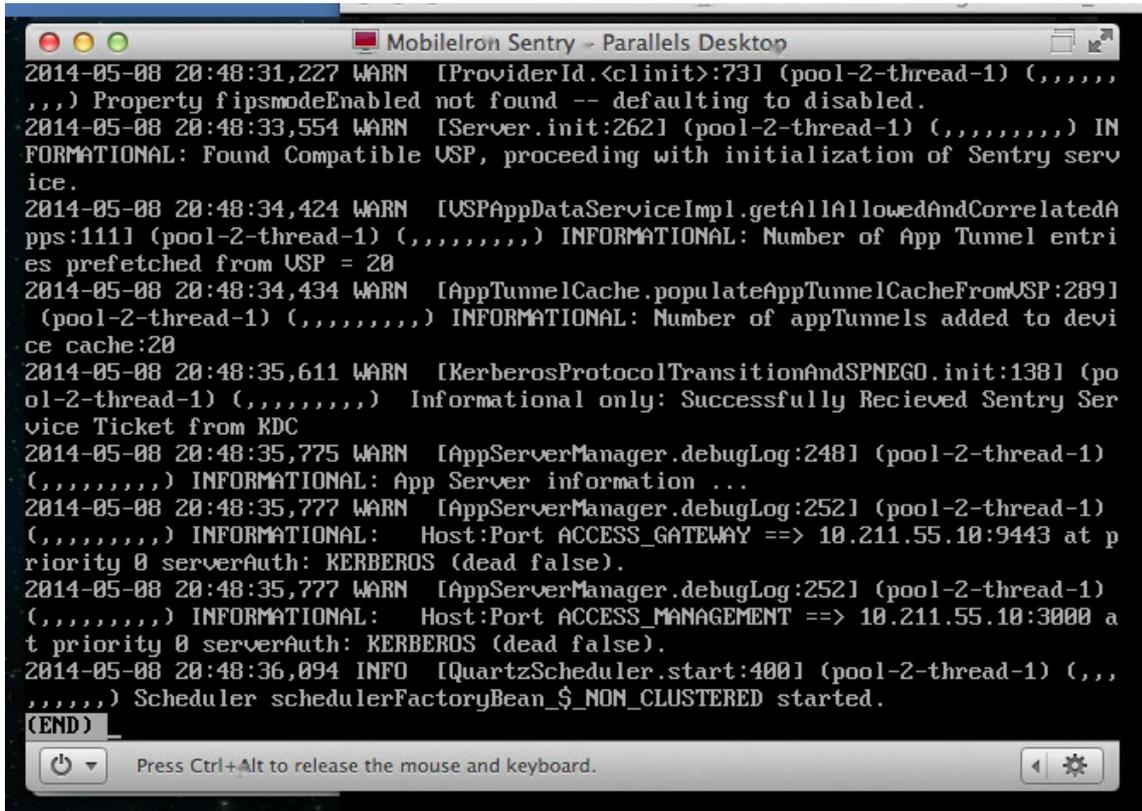
1. Still in the MobileIron VSP Admin Portal, select **Settings** and open **Sentry**.
2. Find the **Sentry** created in "Add and Configure the Sentry".
3. Click on the **Edit** icon.

- 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 Authentication 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**.

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.

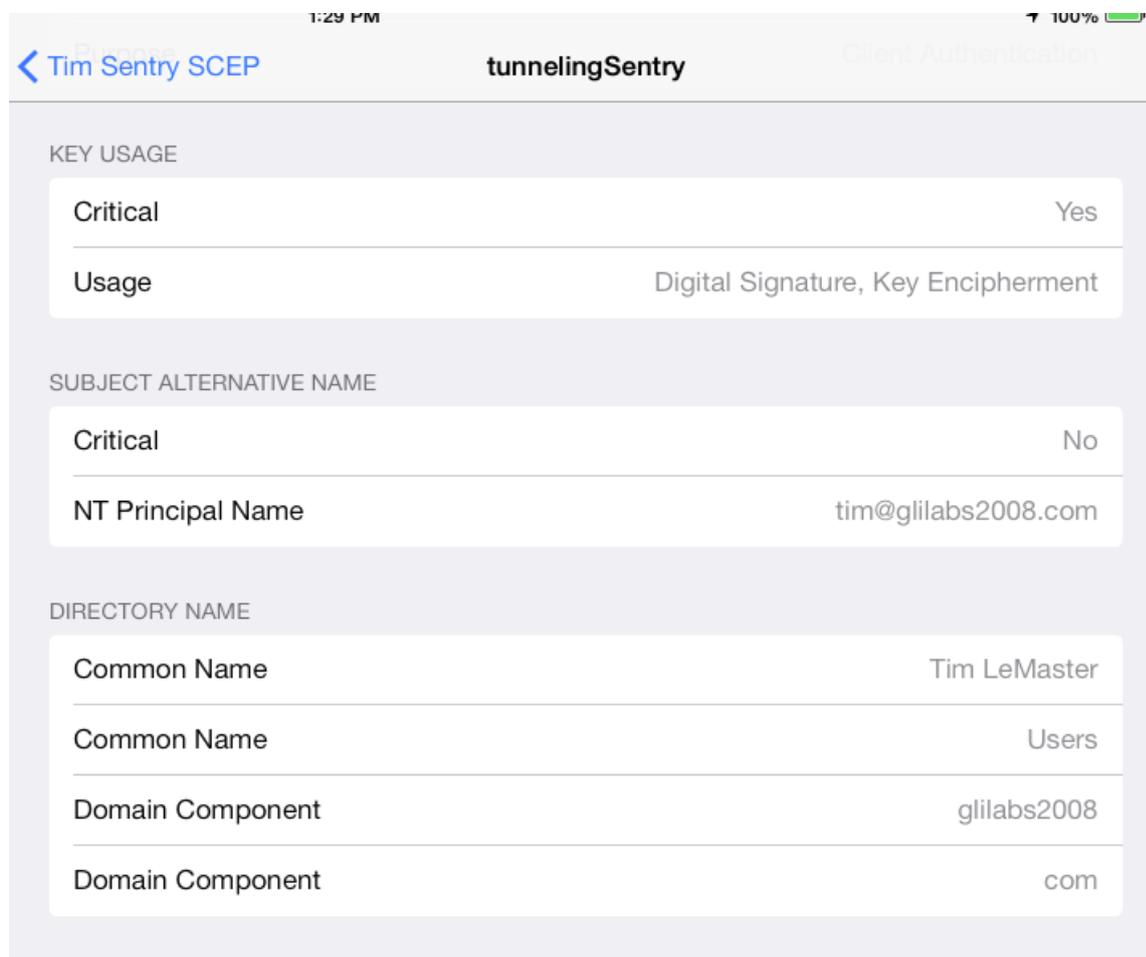
Find the line "**Informational only: Successfully Received Sentry Service Ticket from KDC**". This verifies the Sentry is able to reach and communicate with the KDC.



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.

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.

Delegation for network shares and SharePoint

This article will help you configure MobileIron credential delegation methods with network shares and SharePoint sites. This guide requires that you have already configured both MobileIron and Acronis 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**.
2. Find the computer object corresponding to the Gateway server.

Note: If you are running the Gateway server under a **User** account, select that **User** object instead.

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

15.1.1 Using client certificate authentication

Acronis Access accepts SSL user identity certificates for authentication with a Acronis Access Server or an HTTPS Reverse Proxy server.

If you have enabled certificate authentication as your Acronis Access or HTTPS Reverse Proxy login method, the Access Mobile Client app will be automatically challenged for a user identity certificate when it attempts to connect to a Gateway server. In order for authentication to take place, an SSL user identity certificate must be added to the Access Mobile Client app.

Mobile Device Management (MDM) solutions, including the Apple iPhone Configuration Utility, allow you to add certificates to an iOS device. Certificates added in this way are placed in an Apple specific section of the iOS Keychain and are only available to built in Apple services and applications, such as VPN and the Mail app. In order for the Acronis Access app to get access to a certificate, it must be added to the device through the Acronis Access app itself.

Presently, the process for adding a certificate to Acronis Access requires that the certificate file is transferred to the device and then opened into Acronis Access. The easiest way to perform this is by emailing the certificate file to the user.

Server side prerequisites

In order to use client certificate authentication you must have a Gateway server installed on the same machine as the Acronis Access Server and the mobile clients must enroll using the Gateway Server's address.

Note: When using this method, if the Gateway Server service crashes or is disabled, clients enrolled with it will not be able to connect to the management server even though the Acronis Access Server is still running.

Note: When using this form of authentication, mobile clients cannot access Sync&Share Data Sources.

Warning! You will not be able to use client certificate authentication if your mobile client is enrolled into management directly to the Acronis Access Server.

Example scenario: If your Acronis Access is on 192.168.1.1:3000 and your Gateway is on 192.168.1.1:443, in order to use client certificate authentication, your users have to enroll in client management with 192.168.1.1:443. The Acronis Access Server is still the management server, but the requests are proxied through the Gateway Server.

To prepare a certificate for the Acronis Access app:

You must have a certificate authority established with which you will issue certificates. Creating certificates is not a function of Acronis Access.

The certificates you generate must be associated with your users' Active Directory accounts. Acronis Access will query AD to match these certificates to the relevant user account at the time of authentication. This mapping of certificates to AD user accounts may be handled by your Microsoft Certificate Authority, or may need to be performed manually if you are using another type of certificate authority.

Using your certificate authority, generate a user identity certificate that includes a private key and is in the PFX or P12 format. This certificate will require a password when it is created. This password will need to be entered by the user when the certificate is installed in the Acronis Access client app. This certificate file should have a .PFX or .P12 extension by default.

Once the certificate file has been created, remove its extension completely by deleting the ".PFX" or ".P12" from the file name. This is required so that the file can be opened into Acronis Access using the standard iOS "Open In" function.

To send and install the file using email:

1. Compose an email to the user and attach the certificate file to the email. Ensure that you've removed the extension from the certificate file, as described above.
2. When the user receives the email on their device, they simply have to tap the attached file and choose "Open in Acronis Access" from the pop-up menu.
3. Acronis Access will start and the user will be prompted to confirm they want to add the certificate to Acronis Access .
4. The user will then be prompted to enter the private key password
5. Once the password is entered, the certificate is added to Acronis Access and the client will be able to perform certificate authentication with a Gateway server and HTTPS reverse proxy server.

The status of the installed certificate can be viewed by opening the **Settings** menu in the Acronis Access app.

15.1.2 Using Kerberos Constrained Delegation authentication

Gateway Servers in Acronis Access 5.1 or newer support authentication using Kerberos Constrained Delegation.

This can be used in scenarios using Kerberos Constrained Delegation to authenticate Acronis Access iOS clients through a reverse proxy using client certificates (e.g. TMG). In this scenario you will need to install a user certificate (p. 333) in the Access Mobile Client app. This certificate needs to be bound to Active Directory.

Another scenario is to authenticate mobile devices with client certificates using MobileIron AppTunnel. In this scenario you must have Acronis Access and Mobile@Work installed on your device and a MobileIron Sentry setup on a server. The Sentry is a standalone component which provides access control and tunneling. It provides the secure infrastructure that AppTunnel uses for app data. You don't have to install a client certificate in the Acronis Access app, as the MobileIron AppTunnel will take care of that.

The Android and Windows mobile apps do not support this configuration.

Note: Please visit the *Using AppConnect with Kerberos Constrained Delegation (p. 311)* section for more information on configuring MobileIron and Acronis Access with Kerberos Constrained Delegation.

The Apache Tomcat used by the Acronis Access Server does not support either Kerberos or client certificate authentication. In order to use any of these authentication methods, you must have a Gateway server installed on the same machine as the Acronis Access Server and the mobile clients must enroll using the Gateway Server's address. When a user enrolls with the Gateway Server instead of the Access Server, all authentication is done by the Gateway Server, thus allowing the use of Kerberos Constrained Delegation and client certificates. All management features are still enforced by the Acronis Access Server but the authentication is done by the Gateway Server.

Note: When using this method, if the Gateway Server service crashes or is disabled, clients enrolled with it will not be able to connect to the management server even though the Acronis Access Server is still running.

In this section

Configurations in the Active Directory.....	335
Delegation for network shares and SharePoint.....	340

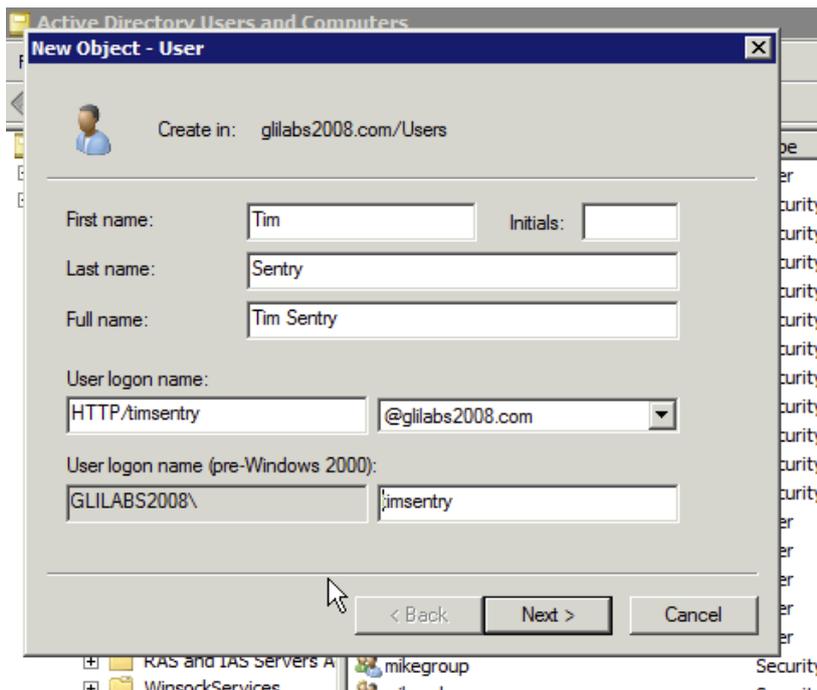
15.1.2.1 Configurations in the Active Directory

This guide will help you configure the Windows Active Directory elements needed for Kerberos Constrained Delegation authentication.

Create a Kerberos Service Account

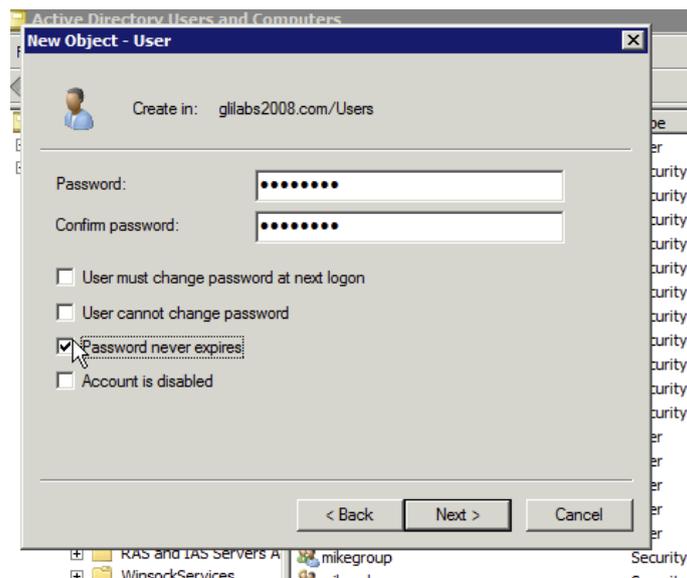
1. Log in to your KDC server as an administrator.
2. From the Windows Start menu, select **All Programs**, select **Administrative Tools > Active Directory Users and Computers**.
3. In the newly opened console, expand the domain (Kerberos refers to a domain as a realm).

- Right-click **Users** and select **New > User**.



- Enter a **Name** and a **User Logon Name** for the Kerberos service account. Use standard alphanumeric characters with no whitespace for the **User Logon Name**, as it is entered in a command prompt later in the guide. 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.

- 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.

- Click **Next**.
- Click **Finish**.

Create a keytab for the Kerberos Service Account

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

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

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

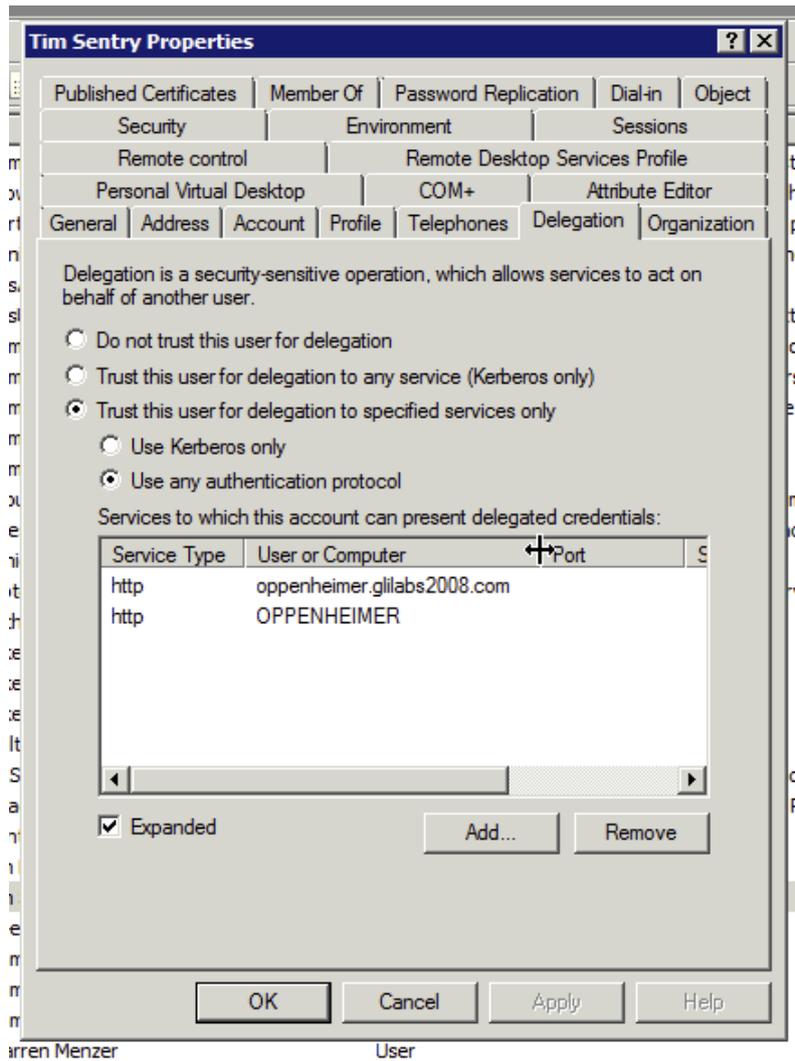
```
C:\Users\Administrator>ktpass /out timsentry.keytab /mapuser timsentry@glilabs2008.com /princ HTTP/timsentry@glilabs2008.com /pass ██████████
Targeting domain controller: dc.glilabs2008.com
Using legacy password setting method
Successfully mapped HTTP/timsentry to timsentry.
WARNING: ptype and account type do not match. This might cause problems.
Key created.
Output keytab to timsentry.keytab:
Keytab version: 0x502
keysize 65 HTTP/timsentry@glilabs2008.com ptype 0 <KRB5_NT_UNKNOWN> vno 3 etype
0x17 <RC4-HMAC> keylength 16 <0x5c875e4d5257b48f74cc445af903ea89>
```

This warning can be ignored.

Delegate HTTP service to the Acronis Access server

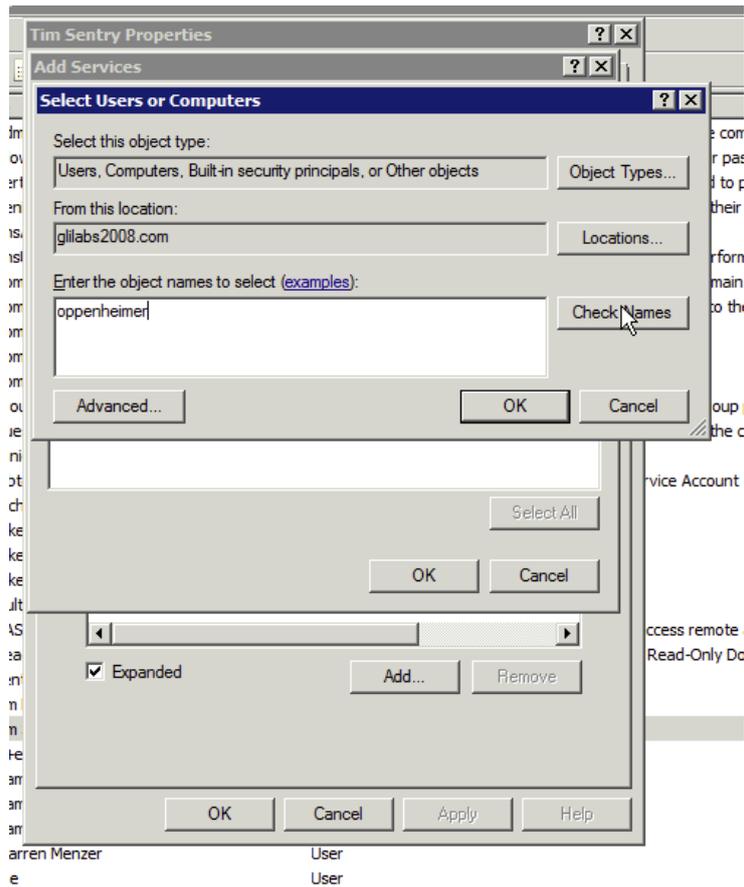
1. From the Windows Start menu, select **All Programs** and open **Administrative Tools > Active Directory Users and Computers**.
2. In the newly opened console, expand the realm (domain).
3. Click on **Users**.
4. Find and select the Kerberos user account that you created in "Create a Kerberos Service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

- Select **Use Any Authentication Protocol**.



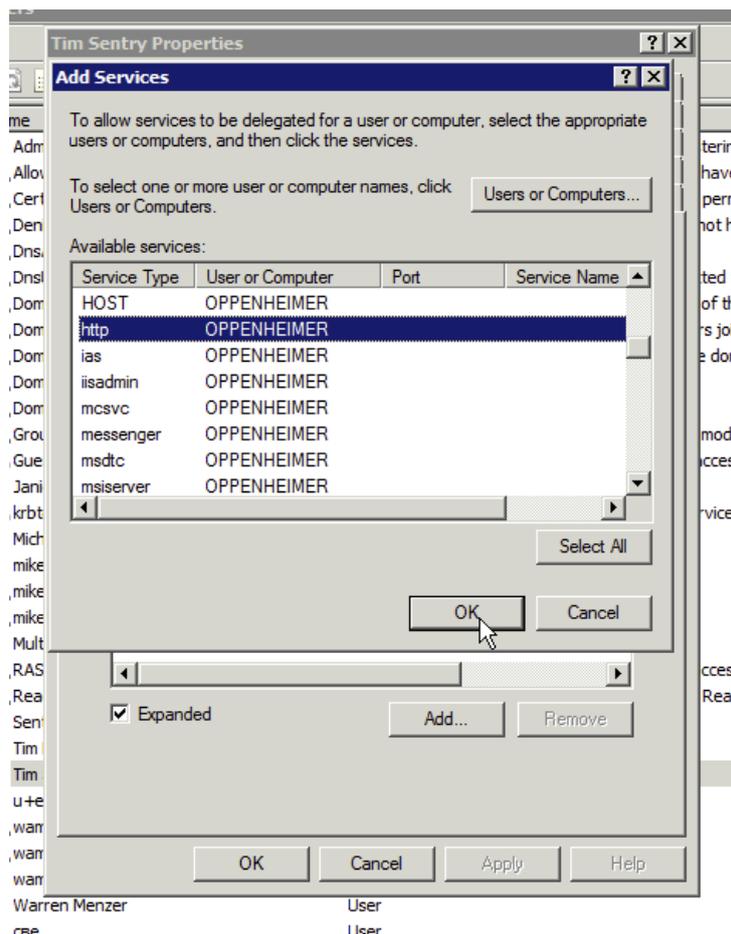
6. Press **Add....**
7. Press **Users or Computers....**
 - Enter the computer name of the Acronis Access Gateway Server.
 - Click on **Check Names**.

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



8. Click **OK**.

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



10. Click **OK**.

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

15.1.2.2 Delegation for network shares and SharePoint

This article will help you configure credential delegation methods with network shares and SharePoint sites. This guide requires that you have already configured Acronis Access and its Active Directory account that delegates 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**.
2. Find the computer object corresponding to the Gateway server.

Note: If you are running the Gateway server under a **User** account, select that **User** object instead.

3. Right-click on the user and select Properties.
4. Open the **Delegation** tab.

5. Select **Trust this computer for delegation to specified services only**.
6. Under that select **Use any authentication protocol**.
7. Click **Add**.
8. Click **Users or Computers**.
9. Search for the sever object for the SMB share or SharePoint server and click **OK**.
 - For SMB shares, select the **cifs** service.
 - For SharePoint, select the **http** service.
10. Repeat these steps for each server that the Acronis 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.

16 What's New

In this section

What's New in Acronis Access Server342

What's New in the Acronis Access app372

16.1 What's New in Acronis Access Server

Note: Numbers such as "[ASRV-2345, DE1013, US552]" refer to Acronis' internal change tracking system.

Included in the latest version of Acronis Access are: **Tomcat** version: 7.0.70; **Java** version: 8u112; **PostgreSQL** version: 9.4

Acronis Access 8.0 (Released: September 21, 2017)

Acronis Access 8.0 and newer will no longer support Internet Explorer 8. Acronis Access 7.5 is the last version that supports Internet Explorer 8.

Enhancements:

- Added support for an optional Microsoft Office Online integration that enables file viewing and editing using **Office Online** from within the Web Client. Office Online supports **DOCX**, **XLSX** and **PPTX** files. **DOC**, **XLS** and **PPT** files are also supported, but will ask to be converted to the newer format for editing. For on-premise installations, this feature requires that an Office Online Server is available. ASRV-357, ASRV-4714, ASRV-4664
- New Office files can now be created in the Web Client, for editing with Office Online.
- Added support for multi-select of items in the Web Client using item selection check boxes and shift, command/ctrl keyboard options. ASRV-4723, ASRV-353
- Subfolders of existing Sync & Share shared folders can now be shared independently to separate audiences. ASRV-1635
- Subfolders of root level Sync & Share folders can now be synced to the desktop client.
- Added a mobile policy setting to initiate and require Acronis Access iOS app enrollment with Intune Mobile Application Management. This allows the Acronis Access iOS app to have Intune MAM applied, without requiring that the mobile device is managed by Intune MDM. ASRV-4510
- During an upgrade installation, administrators will be notified if mandatory database migrations will increase the time it takes to perform the upgrade. ASRV-5269

Bug fixes:

- Improved the reliability of desktop client sync.
- Fixed an issue with folder sorting in the Web Client with Chinese characters. ASRV-4487
- Miscellaneous localization fixes.

Acronis Access 7.5.4 (Released: May 19th, 2017)

BUG FIXES:

- Fixed an issue where files added to shared folders might not be visible to non-owner members.
- Fixed an issue where file download links shared by non-owner members of shared folders may not function correctly.
- Fixed an issue where the file purging process could generate an error.

Acronis Access 7.5.3 (Released: April 21st, 2017)

BUG FIXES:

- Miscellaneous fixes and improvements
- Fixed an issue with the desktop sync client on Mac OS 10.9

Acronis Access 7.5.2 (Released: February 11th, 2017)

BUG FIXES:

- Fixed an issue with duplicate display of admin users in the web admin console.
- Fixed a potential issue where a Tomcat setting could be changed to an unsupported value upon upgrade, causing service issues.

Acronis Access 7.5.1 (Released: January 25th, 2017)

BUG FIXES:

- Fixed an issue where the search field in the web UI could be incorrectly positioned if you are using the “Custom” color scheme option.
- Fixed an issue with paging on the web admin console audit log page.
- Fixed an “internal error” that could occur while browsing Sync & Share storage that contains expired shared folders.
- Changed the logging of gateway CURL connection errors from WARN level to DEBUG level.
- SMS 2-factor authentication compatibility improvements.

Acronis Access 7.5 (Released: January 12th, 2017)

ENHANCEMENTS:

- If you are upgrading to Acronis Access Advanced 7.5 or later from a version before 6.0, you will need to take additional steps to upgrade. Please contact Acronis Mobility Support for details on performing this upgrade. ASRV-350
- The web and desktop clients are now localized in Spanish.
- Microsoft Azure Storage is now supported as a location for the Sync & Share file repository. ASRV-3489
- An option for SMS 2-factor authentication for web client login is included in this release. Options are provided to use AD mobile phone numbers or user-provided phone numbers. 2-factor authentication can be required for every login, at a specified time interval, or only for login from new browsers. Sending of SMS codes will require that an account is established with the Twilio SMS messaging service. ASRV-296

- File and folder search is now available in the web client. Options for filtering results based on file type, file modification date and file owner are provided. Windows File Server network data sources with Windows Search enabled will also display an option to search by file name or file contents. ASRV-1421
- File contents searches of Windows File Server data sources with Windows Search enabled will now return matches based on Windows Explorer tags, in addition to file contents. This applies to searches from the web client or mobile apps. ASRV-4221
- The "Administration" link to the web admin console has been moved from the top level of the web client into the "User menu". Users with admin privileges will see a new user icon in the web UI that includes a star on the bottom right. ASRV-4093
- All "Good Dynamics" settings in the administration console have been renamed to "Blackberry Dynamics". ASRV-4074
- Added a new mobile gateway Access Restriction option to allow or deny connections from the upcoming Acronis Access for Blackberry Dynamics Android app. ASRV-3795
- Added a new mobile policy option to configure the display format of search results provided by the built-in PDF viewer. ASRV-3791
- Added a new mobile policy option to allow or deny editing of password protected Office files. Viewing and editing of password protected Office files will be supported in upcoming versions of the Access Advanced mobile clients. Editing a password protected file will remove the password upon saving. For this reason, this capability is disabled by default, but may be enabled if you choose. ASRV-3729
- The LibreOffice service, used in previous releases for rendering Office files for viewing in the web client, has been replaced with a new internal rendering library offering enhanced performance. Files are now rendered incrementally for more responsive viewing. The LibreOffice service will be automatically uninstalled when you upgrade to version 7.5 or later. ASRV-3867
- Added an option to delete a user's Sync & Share content immediately at the time you delete their account. ASRV-2848
- The owner of a Sync & Share folder that has been shared to you is now displayed in the web client when you mouse over the shared folder's icon. ASRV-3123
- In Sync & Share "Show Deleted" mode, a deleted folder is no longer displayed if all contents of the folder have been previously purged from the server. ASRV-16253
- The included version of Java has been updated to version 8u112. ASRV-3409
- Added an option to not send an email notification to affected end users when adding and removing users from a Sync & Share shared folder using the Acronis Access Server API. ASRV-3888

BUG FIXES:

- Fixed an issue where network folders could appear as read-only in the web UI when the user actually has read-write permissions. ASRV-4200

Acronis Access 7.4.1 (Released: October 18th, 2016)

- Miscellaneous fixes and improvements.

Acronis Access 7.4 (Released: September 15th, 2016)

ENHANCEMENTS:

- Added the ability to preview a file that was shared to you using a download link directly on the shared file landing page. Options for View and Download are now displayed. This feature requires that web client document previewing is enabled on the server. ASRV-3051
- Added a new mobile policy option to enable or disable the ability to create empty PDF files for PDF annotation note taking. ASRV-3620
- Added a new mobile policy option that determines how URL's in documents will be opened by the Acronis Access app. Options include: "Default Browser", "Inline Browser", "MobileIron Web@Work", "Good Access", or blocking the opening of URLs. ASRV-3452
- Added a new mobile policy option to allow enabling or disabling the import of files from the camera/photo library. ASRV-2821
- Added a new mobile policy option to allow enabling or disabling use of the iOS document provider extension feature added to the 7.6 version of the Acronis Access for iOS client app. This setting will default to disabled, unless your existing policy allows "Opening Acronis Access files in other applications" without whitelist or blacklist restrictions. ASRV-2490
- Sync & Share storage quotas can now be configured to be smaller than 1 GB. ASRV-1439
- Added an "Open Log Folder" button to the Mac and Windows desktop sync clients Preferences dialog. ASRV-2025
- Shared folder change notification emails now include a link to directly navigate to the folder in question. This change is in the 'User notification' email template. If you have customized this email template, these changes will need to be manually added to the template if desired. ASRV-1577
- Improved the rendering of the width of columns in Excel files displayed in the web previewer. ASRV-3007
- Increased the reliability and speed of the Mac desktop sync client recovering from network interruptions and sleep. ASRV-3582, ASRV-3353, ASRV-139
- Updated included Tomcat to version 7.0.70.
- Updated included Java to version 8u92.

BUG FIXES:

- Fixed an issue where it may not have been possible to reassign a deleted user's Sync & Share data. ASRV-3149
- Fixed an issue where multiple conflict resolution files could be created when Office files are open and repeatedly saved on multiple clients. ASRV-3024

Acronis Access 7.3.1 (Released: June 20th, 2016)

ENHANCEMENTS:

- Added a new mobile 'Application Policy' setting to allow the iOS Document Provider Extension feature released in the 7.6.0 version of the Acronis Access iOS app to be enabled or disabled. This policy setting will default to enabled on upgraded servers if the "Opening Acronis Access Files in Other Applications" policy is enabled and no app blacklist or whitelist is in use. It will be disabled

by default on upgraded servers if an app blacklist or whitelist is in use or if the "Opening Acronis Access Files in Other Applications" policy is disabled. ASRV-2490

- Added a new mobile 'Sync Policy' setting that can be used to prevent a mobile device from auto-locking while the Acronis Access app is syncing files. This setting is **off** by default and currently supported by Acronis Access for iOS version 7.6.0 or later. Support for Android and Windows Mobile will follow in future app releases. ASRV-2988
- Added a new option in Audit Log - Settings to choose whether you would like exported audit logs to show timestamps in the Access Server's local time zone or the UTC time zone. ASRV-3096
- Added additional 'Auto-Sync Interval' options to the mobile 'Sync Policy'. These new options are 8, 12, 24 and 48 hours. This setting is currently supported by Acronis Access for iOS version 7.6.0 or later. Support for Android and Windows Mobile will follow in future app releases. ASRV-3130
- Added a new policy setting to enable or disable app crash reporting to Acronis via the Fabric reporting library. This reporting is disabled by default and can only be activated if you opt in with the server-side policy, but we encourage you to enable it. These reports allow Acronis to improve the Access apps and are only sent when the app encounters a crash. They contain no private data or identifying information. This reporting feature and policy setting only apply to Acronis Access for Android version 7.0.0 or later. Support for iOS and Windows Mobile will follow in future app releases. ASRV-3138
- Acronis Access will not be affected by **Compatibility Mode** settings for **Internet Explorer**. Both the administration portal and the web user interface will work as expected. ASRV-3194

BUG FIXES:

- Fixed an issue that could cause an Acronis Access iOS client that is configured to use Kerberos single sign on to unnecessarily prompt for a password. ASRV-3111

Acronis Access 7.3 (Released: May 5th, 2016)

ENHANCEMENTS:

- Added support for Italian localization to Access Advanced Server.
- Added an option to use Acronis Storage as your Sync & Share 'File Repository' storage location. ASRV-1519
- Added options to use Swift S3, Ceph S3 and "Other S3-Compatible Storage" as your Sync & Share 'File Repository' storage location. ASRV-2774
- Acronis Access can now display SharePoint "followed sites" within SharePoint network data sources. They are displayed in a "Followed Sites" folder within the root of the data source. Users can "follow" sites from within SharePoint's web client. This feature is disabled by default and can be enabled in a SharePoint data source's settings in the Acronis Access web admin. ASRV-2423
- Within Sync & Share storage, users now have the option to restore a deleted folder and all of its contents in a single operation. In addition, navigating into a deleted folder to browse for and restore a specific deleted file is also supported. ASRV-451
- The Windows and Mac desktop clients now allows syncing of files with file paths greater than 260 characters. Files with paths over this length may not be accessible using Windows Explorer. ASRV-439
- The desktop sync client will now compare the file contents of server-side and desktop files to avoid uploading or downloading an unchanged file, even if the files' modification dates differ. If a user uploads an identical file or if the desktop sync client is uninstalled and later reinstalled to

use the same local sync folder, existing files will be compared and reused without further upload or download. Sync & Share files uploaded by Acronis Access mobile or web clients will now be compared with existing server-side files to prevent unnecessary revisions when uploaded files are identical to existing files. ASRV-2734

- The default TCP/IP ports used in new installations of Acronis Access Advanced have been changed. The Acronis Access web client/admin service will now be installed on port 443 by default. The Acronis Access Gateway service will now be installed on port 3000 by default. Upgrade installs on existing Acronis Access Advanced servers will maintain the present port configuration. ASRV-2810-
- Sync & Share shared file URLs have been simplified to a shorter format. ASRV-1157
- A user will no longer receive Sync & Share email notifications for actions they personally took (download, upload, unsubscribe, etc.) ASRV-39
- Added a new option to the Web Previews web admin settings page that enables web client preview of only files that do not require server-side rendering. If this option is enabled, Microsoft Office files cannot be previewed within the web client. ASRV-2644
- The Mobile Access policy setting "Allow File Server, NAS and SharePoint Access From the Web Client" now defaults to being enabled for new Acronis Access Advanced installations and in newly created Mobile Access policies. ASRV-2818
- Added as new option on the Email Templates page to use the configured "Server Name" for the product_name variable in email contents. ASRV-1942

BUG FIXES:

- Fixed an issue that could result in the sync folder size for certain network data sources to be shown as zero when adding a sync folder within the web client. ASRV-2473
- Fixed an issue where the processing of a large number of database items could cause the Acronis Access Gateway service to time out at startup. ASRV-2400
- Free external users will now be displayed with a "Guest" icon next to their name on the Sync & Share folder "Members" dialog. ASRV-1940
- Fixed an issue where Excel files opened in the web previewer may not properly display hyperlinks in the file contents. ASRV-2798
- Fixed an issue where paths to the file repository would not work if they contained Chinese characters. ASRV-2810

Acronis Access 7.2.3 (Released: February 29th, 2016)

ENHANCEMENTS:

- Added mobile client policy options to configure view setting in the new and improved PDF viewer / annotation tool that was added to the Acronis Access iOS app (version 7.5). ASRV-2103

BUG FIXES:

- Fixed a sync issue that could occur when deleting or moving a folder within the Sync & Share desktop client folder and then immediately replacing it with a new folder of the same name. ASRV-1706

Acronis Access 7.2.2 (Released: February 2nd, 2016)

ENHANCEMENTS:

- EMC Documentum is now supported by Acronis Access as a data source. Acronis Access users connect to Documentum using the CMIS protocol. Documentum now appears in the data source type options when configuring a network data source. ASRV-1012
- Added a new gateway access restriction setting that allows restricting mobile access to Microsoft Intune managed iOS clients. These clients are allowed to connect by default upon upgrade from previous versions of Acronis Access. They can be disallowed within the gateway server 'Access Restrictions' settings.. ASRV-1686
- Added a new mobile client management policy option that only allows users to create 1-way sync folders. ASRV-1846
- Added a new mobile client management policy option that configures the sync folder type (1-way or 2-way) that is selected by default in the mobile client during sync folder creation. ASRV-1846
- Text files are now rendered by the web client previewer as plain text, rather than converting them to PDFs. ASRV-1855
- The web previewer file render timeout has been increased to 120 seconds to accommodate larger files. ASRV-1868
- Added web previewer support for .rtf, .ini, .log, .csv, .ico, .jpe and Open Office files (.ods, .odt and .odp). ASRV-1852

BUG FIXES:

- Improved speed of accessing SharePoint data sources when Microsoft Online login service is not reachable by the Access Server. ASRV-374
- Improved the speed of loading PDF files within the web client previewer on Internet Explorer 11.
- Fixed an issue where expired shared file links could be unnecessarily audit logged multiple times. ASRV-1737
- Fixed an issue where the user who deleted a file or folder might not be specified in shared folder change notifications. This change is in the "User notification" template. Customers who have customized email templates will need to manually added these changes to the customized templates, if desired. ASRV-1964
- Fixed an issue where Alfresco file modification dates might not match other Access Server modification dates. ASRV-1586
- Fixed an issue where conflict resolution files could be created erroneously when syncing network node files. ASRV-2141
- Fixed an issue where the web client previewer would fail to render and display Office files if the Access Server's DNS name was not resolvable by internal DNS. ASRV-1887
- Fixed an issue refreshing the audit log page in the IE11 browser. ASRV-1624

Acronis Access 7.2.1 (Released: December 10th, 2015)

ENHANCEMENTS:

- Improved email address validation during trial activation. ASRV-2037

BUG FIXES:

- Fixed a bug where using Single Sign-On could break the desktop client's sync functionality.

Acronis Access 7.2 (Released: November 17th, 2015)

ENHANCEMENTS:

- Added the ability to view Office files, PDFs, text files and images directly within the Acronis Access web browser client without downloading. This feature is enabled by default upon upgrade and can be configured in a new "Web Previewer" section of the server "General Settings".
- Added the ability to give access to content management system data sources via the CMIS protocol. Acronis Access now includes a supported data source setting for Alfresco and a 'Generic CMIS' option. Documentum support will be included soon in a followup release. [ASRV-1012]
- A "Download Mobile Client" page that includes details on the available Acronis Access mobile apps has been added to the web user menu. [ASRV-1463]
- When sharing Sync & Share file download links, you may now restrict access to only those users the links are emailed to by the Access Server. [ASRV-330]
- A new link properties dialog allows viewing the link URL, 'Shared to' users, access restrictions, and expiration settings of existing shared download links. These sharing settings can also be edited in this dialog. [ASRV-1011]
- New external users invited to Sync & Share files or folders will now be required to activate their Acronis Access account via an activation email link, before gaining access to their account. [ASRV-1184]
- When Acronis Access web client users are prompted with the option to sync a newly-shared folder, they will now be notified if they do not have any desktop sync clients registered. [ASRV-1509]
- Acronis Access mobile clients can now access Sync & Share data sources using certificate or Kerberos authentication. [ASRV-466]
- Added new gateway server "Access Restrictions" option to allow or deny connections from Microsoft Intune managed Acronis Access iOS client apps. [ASRV-312]
- Added new gateway server "Access Restrictions" option to allow or deny connections from Acronis Access iOS client apps managed by "iOS Managed App" functionality. [ASRV-1026]
- Access to the Acronis Access administration console can now be restricted to specific IP addresses or IP ranges. [ASRV-1183]
- Improved page load performance of the user "Log" page. [ASRV-1209]
- Improved email type ahead lookup performance. [ASRV-1468]
- The trial period for Acronis Access Server is now 30 days. [ASRV-1228]
- Added a gateway 'Cluster Group' configuration option to "Use alternate address for Access Server connections" for cases when the Acronis Access web server needs to connect to the Cluster Group using a different network address than mobile clients. [ASRV-243]
- Acronis Access now preserves custom Tomcat 'temp' directory settings on upgrade. [ASRV-378]
- Added support for TLSv1.2. [ASRV-1281]
- Updated PostgreSQL to version 9.4.4-3. [ASRV-379]
- Updated to Java to version 8u60. [ASRV-1327]

BUG FIXES:

- Fixed an issue where desktop client users could encounter a login failure when the Access Server is configured to "Force Legacy Polling Mode" for desktop clients. [ASRV-278]
- Fixed an issue with unattended uninstall of the Acronis Access Windows Desktop client. [ASRV-1192]
- Fixed an issue that could cause an error during Acronis Access Windows Desktop client installation if the Window autorun registry key could not be found. [ASRV-1496]
- Fixed an issue where temporary files might not be deleted from the server if web client file uploads to network folders are canceled before completion. [ASRV-1516]
- Fixed an issue where the custom service account used to run the Acronis Access gateway server service would revert to 'Local System' after modifying settings in the Acronis Access Configuration Utility. [ASRV-1503]
- Fixed an issue where Single Sign On could fail if a user's implicit and explicit user principle names (UPN) are different. [ASRV-1497]
- Fixed an issue where the Acronis Access web client UI would revert to IE8 mode for newer versions of Internet Explorer, if they have "compatibility mode" enabled. [ASRV-1346]
- Fixed an issue where auto-update of the Acronis Access Windows Desktop Sync Client could fail if the Windows language was set to French. [ASRV-1229]
- Fixed an issue where the Acronis Access Windows Desktop Sync Client could fail due to an incompatibility displaying notifications while the Photo Gallery screensaver was active on Windows 10. [ASRV-111]
- Fixed an issue where configuring a shared file download link expiration limit of greater than days 999999 would result in a web page error. [ASRV-1219]
- Fixed an issue where custom Tomcat web.xml settings for Single Sign On would not be preserved when the Acronis Access Server was upgraded. [ASRV-1059]
- Fixed an issue where Network Home Folders with very large numbers of items could appear empty for mobile clients. [ASRV-1054]
- Fixed an issue where the Acronis Access Windows Desktop Client could become stuck downloading a file if the client was stopped or computer was rebooted during download. [ASRV-1546]

Acronis Access 7.1.2 (Released: August 4th, 2015)

ENHANCEMENTS

- Users will now be notified in the web UI when their session is about to expire and be given the option extend it. If they do not, they will be automatically logged out. US3869, DE14304
- Sync & share files which are deleted and have been purged from the repository will no longer be shown when "show deleted" is enabled. US10696
- There is now a setting available for filtering the file links that are displayed on the "Links" web page. US10812
- Users can now modify the days until expiration of a link from the link details dialog. US10820
- Users can now modify the public or private status of file links from the link details dialog. US10821

- Users can now modify the 1-time download setting for a link from the link details dialog. Note that if a multiple-use link is converted to a single-use download, only one additional download will be permitted of that file, not one download per user it was shared to. US10822
- When a multiple-use file link is shared to multiple users, each user will receive the same file link, not one unique link per user. This was done to improve the usability of the shared links dialogs.
- The Access Server API now offers an option to delete all content when deleting a user. US10644
- Updated the icons on mobile policies to reflect the features supported in the latest Android client app.

BUG FIXES

- File links can now be shared without an expiration date, if the Access Server's 'Sharing Restrictions' settings allow it. DE12851, DE13461
- If a user no longer has access to a folder, the file links shared from that folder will no longer be shown on the shared "Links" page. DE14574
- If a file is moved from its original location, all shared links to that file will be automatically revoked. DE14610
- Users who lose write access and thus 'can invite other users' access to a share will have all file links they shared in that folder revoked. DE14615, DE14623
- A File link will no longer permit downloads if the user who shared the file link no longer has access to the file. This might happen if "User A" shared a link to a file in a shared folder owned by "User B", and then "User B" later removed "User A" as a member of that shared folder. DE14560
- A user will no longer receive an email that he no longer has access to a share if he has unsubscribed himself. US10770
- When a user connects to download a login-required file link shared with Access and uses SSO to authenticate, the user will be directed to the proper page after authenticating. DE14539
- The SSO login link is no longer displayed on iOS devices and Windows phones. DE14554
- SharePoint subpaths will now be resolved properly when added in the web client. DE14423
- Scrolling is now enabled in the left sidebar if there are enough Network data sources to require it. DE14429
- Improved text wrapping of footers in default email templates. DE14436
- Self-provisioned folders can now be deleted successfully from mobile clients. DE14517
- Improved word wrap in Korean language for Internet Explorer and Firefox. DE14522
- Fixed an authentication issue preventing users without a UPN (User Principal Name) from authenticating from the mobile client. DE14624
- Fixed an issue where users could encounter an error accessing files shared via a link if the file has a single quote in the name. DE14633
- A new setting is available to specify the address the Access Server should use to contact Access Gateway cluster groups. By default, this value will be identical to the address for client connections. DE14636
- Optimized memory usage on the Gateway Server when uploading thousands of files. DE14589
- The desktop client will automatically reauthenticate with the Access Server when using SSO and syncing network content if the Kerberos ticket expires. US10900

Acronis Access 7.1.1 (Released: July 8th, 2015)

BUG FIXES

- Fixed an issue where some menu items on the Mac desktop clients were not properly localized for some languages.
- Fixed a rare issue which could prevent the Access Server from successfully upgrading from older versions.
- When selecting a file in the web UI that was shared with a link, a **Notifications** option will no longer appear in the righthand menu. This option does not apply to files shared by links.
- Fixed an issue where clients authenticating with Single Sign-On would fail to be able to browse network nodes after their Kerberos ticket expired.

Acronis Access 7.1

ENHANCEMENTS

- Acronis Access now supports integrated desktop authentication (single sign-on) for the web client and the Windows desktop client. When single sign-on is enabled, users who already authenticated to the domain when logging into their computer will not need to reenter their username and password to authenticate when logging into the web interface or in the Windows desktop client. Support for this feature in the Mac desktop sync client will be included in a subsequent update. This feature requires additional configuration, please read the Configuring Single Sign-On (p. 208) article for more information. [US10595]
- An option has been added to allow users to share file download links that expire after a single download. [US7172]
- Users can now configure shared Sync & Share folders to expire. After the expiration date, all members of the share will lose access to the shared folder. [US6314, US8531]
- New administrative options are available to limit the size and types of files that can be uploaded to Sync & Share. Administrators can enable these limits and specify the maximum file size and disallowed file types on the Sync & Share => General Restrictions page of web administration. [US10587]
- A new "**Links**" page is available showing users all Sync & Share files they have shared with "Send link" or "Get link". This list allows users to revoke access to these file links or navigate to the files in the Sync & Share hierarchy. [US10809]
- Users can now view a detailed list of the individual file links shared for a specific file, including to whom the link was sent, what the limitations of the link are, and when it expires. These individual links can be revoked. [US10814]
- Sync & Share files which have been shared with "Send link" or "Get link" will now have an icon next to them in the file and folder list. Clicking this icon will allow users to view and modify the details of the file's shared links. [US10816]
- Acronis Access is now localized for Korean. [US10638]
- When a user is disabled, all their shared file links will be temporarily disabled. When a user is deleted, their shared file links will be disabled until their content is reassigned. When the user's content is reassigned, the file links will be re-enabled and owned by the new owner of the content. [US9870]
- Administrators can configure a custom message to be displayed on the web login page. This message can be configured on the Settings => Web UI customization page. [US10319, US10660]

- The default user notification emails will now include a link to allow the user to unsubscribe from the Sync&Share shared folder notification emails. [US10423]
- When a file link is shared to multiple users at the same time, all the users receiving a passkey link will receive the same link. Previously, each user would get a different, individualized link. The only exception to this is one-time use links. If a one-time use link is shared to multiple users, each user will get a unique link which will allow a single download. [US10808]

BUG FIXES

- Mobile device enrollment time has been significantly reduced. [US10712]
- Gateway clusters with a client connections address that is not accessible from the Access Server can now be administered (using the server address). [DE13147]
- A new user who first logs in from a mobile device and is a member of a Sync & Share LDAP provisioned group will now be granted Sync & Share access without having to first log in via the web interface. [DE13215]
- Pending users with access to Sync & Share data sources can now successfully enroll from a mobile device. [DE13379]
- Active Directory users whose passwords contain a colon can now successfully authenticate to get access to synced network data sources from the desktop client. [DE14294]
- Fixed an issue starting the Access Server if the PostgreSQL password contained single quotes, colons, percent, high Unicode, or other special characters. [DE14355]
- Dashes are no longer considered invalid in server names defined in the Access Restrictions list for allowable enrollment servers.[DE14414]
- The modification date reported when downloading a Sync & Share file via a direct link is now listed in the server's time zone. [DE14418]
- Deleted users are no longer listed in the type ahead lists for email suggestions. [DE14508]
- The Access Server installer will no longer fail to complete successfully when the PostgreSQL password contains a colon, single quote, high Unicode, or other special characters. [DE14433]
- Fixed a rare issue in the desktop client where a file getting locked on disk immediately after download during the sync operation could cause the sync could hang. [DE14197]

KNOWN ISSUES

- Acronis Access 7.1 comes with Java version 8u31 but is certified with 8u45. There is a known issue with Java versions later than 8u31 causing problems with the Single Sign-On feature. If you have upgraded your Java and wish to use SSO, please read this article: <https://kb.acronis.com/content/56367>

Acronis Access 7.0.5

ENHANCEMENTS

- Acronis Access is now localized for traditional and simplified Chinese. US10350
- Improved performance when browsing contents of network data sources containing many subfolders. US10622
- Acronis Access supports device certificate authentication. US10697

BUG FIXES

- Fixed an issue where some SharePoint data sources could not be added if the path was very long. DE14339
- Fixed an error that could occur on startup after upgrades to Access Server 7.0.4 if there were users without a username specified. DE14352
- Fixed problems that could occur uploading files with Internet Explorer 9. US10636
- Fixed an issue where opening the desktop sync dialog for a synced network folder and saving without making any changes could change a 2-way synced folder to a 1-way synced folder. DE14398, DE14415
- Fixed an issue where syncing new network folders could be delayed if other users were syncing many network folders and files. DE14406
- Fixed an issue where the desktop sync client might not immediately update a network folder's sync type (from a 1-way sync to a 2-way sync, or vice versa) when changes were made in the web interface. DE14413
- Fixed an issue where the Access Server could fail to retrieve audit logs from Gateway servers. DE14414
- Fixed an issue with Kerberos authentication to SharePoint. DE13289, DE14272
- Fixed a rare issue where desktop clients would receive an obscure Unicode error instead of a clear explanation on the desktop client when a sync could not be completed because a file being synced was open on that computer in another application. DE14151, DE14289
- Fixed an issue which could occur when desktop clients were upgraded directly from version 2.x to version 7.0.4 or later. DE14336
- Fixed an issue where files could be duplicated on the server if Visual C# projects were saved in the Sync & Share folder on the desktop client. DE14353

Acronis Access 7.0.4

ENHANCEMENTS

- Mobile client '**Access restrictions**' now offer options for limiting access from Windows mobile clients. Options for including instructions & install links for Windows clients are also now available on the enrollment invitations page and in enrollment emails. US8788, US10558
- Access web interface has improved usability on mobile devices with lower screen resolutions. US10270
- The gateway server option to allow connection using self-signed certificates can now be changed even if the gateway server is offline. US10318
- When using the web UI to choose to sync a folder to the desktop client, users are now shown the total size of the folder to be synced. This will help users to make an informed decision when syncing large shares to their desktop. US10414
- The Configuration Utility now allows a UNC path to be provided for the location of the Access File Repository. DE13733
- The Configuration Utility now allows intermediate certificates to be configured. US10315
- The email address options shown during auto-complete when inviting users to a share is now limited to the members of shares they are members of. In addition internal AD users will also be able to see all other internal AD users. DE13387

- Direct file download links created with "**Send Link**" or "**Get Link**" can now be configured to require Access user login before a file can be downloaded. New options are available on the '**Sharing Restrictions**' settings page to allow administrators to define whether public links and login-restricted download links are permitted. If both types of links are permitted, users will be able to choose which type of link they would like when sharing it. There is also an administration setting available to limit access to login-restricted links to internal users only. US10499

CHANGES

- **Web administration pages can no longer be accessed with Internet Explorer 8.** US10471

BUG FIXES:

- Fixed a bug which caused unhandled errors to sometimes be reported when attempting to invite a large AD group for mobile enrollment. US10511
- The %USERNAME% variable is now supported in the name and description of home directory data sources in the web interface. DE13651
- A small pop-up window should no longer appear when downloading files from the web UI with Safari. DE13699
- Notifications now include the user who created the shared file link, when files are downloaded with a direct file download link. DE13811
- The list of data sources will now appear even if some data sources are inaccessible. The inaccessible data sources will simply not be shown in the list. DE13896
- Color schemes are now used for the file download link landing page. DE14072
- AD users with accounts that do not have a UPN (User Principal Name) configured can now access network data sources using the Access web interface. DE14089
- Conflict resolution now supports users whose names contain a forward slash. When creating conflict files, any forward slashes in usernames are now replaced with an underscore, since slashes are invalid characters on the Windows file system. DE14133
- Files and folders on network volumes that were uploaded by a Mac and contain a forward slash can now be synced to Mac and Windows desktop clients. DE14141
- Addressed issues that could keep the Access Server from properly ingesting Gateway audit log messages. DE14146, DE14152
- Fixed an issue where file purging could encounter errors and fail after an upgrade to Access 7.0.3. DE14195, DE14015, DE14101
- Fixed a licensing issue that could occur causing a single user session to temporarily use more than one license on the Gateway Server. DE14275, DE14142
- The PostgreSQL service will now be stopped before upgrade on clusters, preventing errors which prevent the cluster from being upgraded. DE11927
- When saving Microsoft Office files rapidly, the desktop client will no longer create multiple copies of the file in Access. DE14014

Acronis Access 7.0.3

ENHANCEMENTS:

- The API documentation for web clients has been updated, including support and documentation for network files and folders.
- The color scheme of the Acronis Access website can be configured to a variety of preset color schemes. Alternatively, administrators can develop their own custom color scheme. The color scheme can be configured by administrators through the Web UI Customization (p. 131) page.
- Custom logos can now be uploaded to modify the look of the web UI. Three image sizes are used for the various locations the logo appears. On upgrade, the existing custom logo (if any) will be used for all the custom logo locations, but properly sized logos can be uploaded on the Web UI Customization (p. 131) page.
- If a user's mobile access policy allows access from the web client, the default enrollment invitation email will now include a link to the Acronis Access web site. For customers who have customized their enrollment invitation email template, this additional text will need to be manually added to the customized template if desired.
- Users can now download the contents of the folder they are currently browsing with the "**Download folder**" option.
- Administrators of Acronis Access will no longer be prompted to explicitly specify the gateway server's address on a new installation during the Initial configuration (p. 31). The gateway address will be automatically set to the same address as the Access server.
- Minor changes were made to the default enrollment invitation email template to prepare for an upcoming mobile client release. Users who have custom email templates will need to update them manually, if desired.
- Improved login performance and general web application performance by caching some settings in memory.
- Various improvements to increase performance and throughput when uploading and downloading Sync & Share files.
- Acronis Access now installs with Java 8u31.

BUG FIXES:

- Fixed LDAP caching errors which could occur if **ldap_caching** debug logging was enabled.
- Fixed a problem with New Relic monitoring.
- Fixed a problem where a user's desktop synced network folder might not be removed when the server-side network folder was removed from their assigned data sources.
- Fixed an issue where gateway file shares could not be browsed from the web portal if a management server is required and the management server is listening on a non-standard port.
- When a user upgrades from Acronis Access 6.x, if a user tries to reset their password before they have successfully logged in against Access 7.x, they will no longer encounter an error.
- Renaming a top-level 1-way sync folder on the desktop client will no longer produce a warning.
- Fixed a timeout error that could occur when downloading large files via the mobile client.

KNOWN ISSUES:

- If you have end-users running Internet Explorer 8, please consider upgrading to a more secure browser. Administrators can change the SSL bindings to support Internet Explorer 8 users with the following limitations (DE12649):

- Users running Internet Explorer 8 are automatically redirected to the Access 6 style web client interface.
- Internet Explorer 8 will be not supported by the redesigned Access 7 web interface.
- These users will not have access to file server, NAS and SharePoint data sources from the web client interface.
- Server Administration from Internet Explorer 8 is not supported.

Acronis Access 7.0.2

ENHANCEMENTS:

- Acronis Access Server and Desktop Clients for Mac and PC are now localized in Polish.
- Acronis Access now allows syncing file server, NAS & SharePoint folders to a Mac or PC via the Access Desktop Client. This feature can be enabled or disabled in the "Mobile Access" policy and requires that Access Web Client access to these data sources is also enabled.
- Enhancements to user/email address entry in the sharing dialog box in the Access Web Client.
- Access Web Client now displays a multi-level breadcrumb trail.
- SMB network shares are now selectable as File Repository destinations in the Access Server Configuration Utility (DE13472).
- The Access Server Configuration Utility will now default to a self-signed certificate if no suitable certificates are available in Computer\Personal certificate store. (DE12983)
- GOST encryption is supported in Russian localization of Access Server 7.0.2 (US9922).
- Access to Network Home Folders is now included in the Web Client (US9733).
- Network data sources with %username% wildcards in their path are now supported in the Web Client (DE13206).
- Web Client upload now allows uploading more than 10 files simultaneously. (DE12719)
- Java 7 Update 71 is used in this release.

BUG FIXES:

- Fixed an issue emailing Sync & Share file download links via the iOS mobile client (DE13177).
- Links to landing pages and folders from notification emails and from the Desktop Client Finder/Explorer contextual menus no longer sometimes require the user to log in.
- Fixed an issue when upgrading from mobilEcho 4.5 where legacy data sources might not be converted (DE13188).

KNOWN ISSUES:

- Due to a bug in the included 3rd party Java installer, an issue may occur during installation on non-English Windows Servers. Please refer to <https://kb.acronis.com/content/54518> to address this issue. (DE13473)
- If you have end-users running Internet Explorer 8, please consider upgrading to a more secure browser. Administrators can change the SSL bindings to support Internet Explorer 8 users with the following limitations (DE12649):
 - Users running Internet Explorer 8 are automatically redirected to the Access 6 style web client interface.

- Internet Explorer 8 will be not supported by the redesigned Access 7 web interface.
- These users will not have access to file server, NAS and SharePoint data sources from the web client interface.
- Server Administration from Internet Explorer 8 is not supported.

Acronis Access 7.0.1

ENHANCEMENTS:

- Various improvements to the Web Client interface.
- Acronis Access Server and Acronis Access Desktop Clients for Mac and PC are now localized in Russian.
- Apache Tomcat 7.0.57 is used in the release (DE11653).
- Java 7 update 71 is used in the release.
- The allowed minimum expiration time for shared file download links now defaults to 1 day or more on new installations of Acronis Access Server. Previously the minimum link expiration default was 30 days. (DE13079).
- Browsing network data sources via the Web Client is improved for folders with large number of items (DE13056).
- Improved conflict resolution behavior.

BUG FIXES:

- Fixed usage of “¥” symbol for logging in to Access Server Web Client (DE13031).
- Upgrading to Acronis Access 7.0.1 from mobilEcho 4.5 is now supported. (DE12984).
- Fixed shortcut to Acronis Access Tomcat service configuration tool in the Start menu after the upgrade from Acronis Access 6.1 (DE12966).
- Shared Folders now have Notifications in the right hand menu (DE12948).
- If you have end-users running Internet Explorer 8, please consider upgrading to a more secure browser. Administrators can change the SSL bindings to support Internet Explorer 8 users with the following limitations (DE12649):
 - Users running Internet Explorer 8 are automatically redirected to the Access 6 style web client interface.
 - Internet Explorer 8 will be not supported by the redesigned Access 7 web interface.
 - These users will not have access to file server, NAS and SharePoint data sources from the web client interface.
 - Server Administration from Internet Explorer 8 is not supported.
- Fixed occasional crashes in Access Desktop Client for Mac (DE12879).

KNOWN ISSUES:

- When using single port Access Gateway Server configuration, there could be an issue with handling paths longer than 256 characters. Please visit the following KB article to resolve the issue (DE12405): <http://support.microsoft.com/kb/820129>

Acronis Access 7.0

ENHANCEMENTS

- Redesigned and enhanced Access web client user interface.
- **Acronis Access** is now named **Acronis Access Advanced** and is the upgrade path for existing users of Acronis Access 6 or earlier. A new version tailored for small/medium businesses with simpler requirements has been also introduced. This new version is named Acronis Access.
- During new installations, the configuration wizard now attempts to detect and system configuration options, such as SMTP server and Active Directory (LDAP) server.
- During installation, Acronis Access and Acronis Access Advanced can now be configured to operate using a single open port for client connections. In this configuration, all Access clients (mobile app, desktop sync client, web client interface) use the same network address and port to connect to the Access server.
- Folders and files residing on file servers, NAS and SharePoint Servers can now be browsed and accessed from within the Access web client interface. This capability can be enabled or disabled on a user or group basis.
- Updated graphic design of default email templates. Redesigned notification and invitation email templates.
- The Users administration page and Devices administration page are now unified into a single admin console page.
- Access now provides conflict resolution for Sync & Share files and folders. If users' file modifications overlap and cause conflicts, the conflicting files will be renamed with the users name and the current date, so that the conflicting file is obvious and can be handled as needed. Previous to Access 7.0, these conflicting files would have been saved as new versions.
- Sync & Share files can now be copied between Sync & Share folders using the web client interface.
- Sync & Share file download links can be now be generated and copied for use, without requiring an email to be sent by the Access server. The file download links feature can be enabled or disabled.
- Usernames can now be assigned to 'Ad-hoc' external users. All Sync & Share users are generally referred to by user names instead of just email addresses.
- Access Client Version is now displayed in the Users and Devices section of Access Server administration page. (US8696)
- Java version 7 U71 is used in this release. (US9486)
- Improved audit logging when files are downloaded from direct download link. (DE10961)
- Sorting files by type is now allowed in the web client interface. (US6836)
- Postgres can now be removed using the 'Add/Remove Programs' control panel. (US8270)
- There is now a global setting to disable the ability to share files using direct download links. (US8347)
- The default threshold and interval for user notification as they approach their quota for Sync & Share can now be configured. (US8605)
- Apache Tomcat 7.0.56 is used in this release. (US9801)
- OpenSSL version 1.0.1i is used in this release. (DE11653)
- Added support for batch operations in the Devices table (remote wipe, cancel remote wipe, etc.). (US8875)

BUG FIXES

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

KNOWN ISSUES

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

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

Acronis Access 6.1.3

ENHANCEMENTS

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

- Installer includes Java Version 7 Update 51.
- Apache Tomcat updated to 7.0.55. (US9392)

BUG FIXES

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

Acronis Access 6.1.2

ENHANCEMENTS

- Fixed a potential issue with uploading large files via Access web client interface.
- "**Require exact match**" option has been added to "**Domains for LDAP authentication**". When Access sharing invitation emails are sent to users whose email address domain matches the domains listed in '**Domains for LDAP authentication**' setting, they will be instructed to log in with their internal LDAP (Active Directory) credentials. Users who do not match '**Domains for LDAP authentication**' will be invited to create an Acronis Access external user account. Users whose email domain is a subdomain of an entry in '**Domains for LDAP Authentication**' will receive emails with internal user LDAP instructions, unless this '**Require exact match**' checkbox is **checked**. This checkbox is unchecked by default and for upgrades.
- Adjusted the **Application Policy** administration page to reflect changes in the Acronis Access for Android 3.2.3 application.
- In addition to being denied access and redirected, an error message will now be displayed when trying to access a Sync & Share folder you do not have access to via a URL.
- The audit log now allows the owner of a shared folder to see when a member of the shared folder sends download links to others.
- Configuration utility updated to use OpenSSL 1.0.1h.
- Tomcat version updated to 7.0.54.
- Java 7 Update 51 is used in this release.

BUG FIXES

- Fixed an issue with downloading **Sync & Share** files from an Amazon S3 repository.
- Fixed an issue with distinguishing multiple ad-hoc Access Server administrators that do not have associated email addresses.
- Fixed an issue with populating the **owner_name** value in the exported logs.
- Fixed an issue where some provisioned administrator groups were unable to log in after an upgrade.
- Fixed possible request timeout issue when enrolling a mobile client in a large Active Directory.
- Fixed an automatic service startup issue when installed on a Windows Server that is not a member of a domain.

- Fixed a licensing message issue with running multiple Gateway servers on the same network using the same serial number.
- Fixed intermittent SSL errors in the mobile Acronis Access app when accessing **Sync & Share** folders.
- Fixed some Java detection issues in the installer.
- Fixed the issue with the client reporting a python exception instead of an error indicting the actual problem.

KNOWN ISSUES

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

Acronis Access 6.1.1

ENHANCEMENTS

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

BUG FIXES

- Users with the reserved string "data" in their username are now able to complete mobile app enrollment.
- Fixed an issue where an Acronis Access Gateway Server could be listed multiple times in the Access mobile app if the Gateway Server was configured to be visible and multiple data source folders were also assigned.
- Fixed enabling/disabling logging for an Access Server cluster group.
- Addressed a dependency issue that could prevent the Access Gateway service from starting automatically after a reboot on Windows Server 2008R2.

Acronis Access 6.1

ENHANCEMENTS

- Web Services API for the Acronis Access Server administration. The API documentation is packaged within the Access server and is accessible by administrators. The link can be found in the footer.
- The Acronis Access audit log can now be configured to automatically export and purge old log entries. Preferences for export and purge settings can be set on the Audit Log => Settings page.
- New Acronis Access configuration summary tool to collect relevant server configuration details for sending to Acronis support.

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

BUG FIXES

- The active session count will be refreshed when the Gateway Servers page is reloaded.
- Type-ahead search for selecting users to invite to shared files and folders is now supported on Internet Explorer 8.
- The Acronis Gateway Server service is now dependent on other key services so it should be assured to start properly when the server starts up.
- When a Cluster Group is disbanded, any policies that were using that Cluster Group as the Gateway Server used to access “My Network Folders” (locations added by the user) will be updated to instead use the last Gateway Server that was a member of the Cluster Group.
- Fixed an issue with email address filtering for enrolled users.
- Administrators should no longer get a fatal error page when changing the language setting after receiving an error message.
- Administrators should no longer encounter problems applying trial extensions after upgrading an expired server.
- LDAP sync and share users should now always be listed as LDAP once they have successfully authenticated, even if their email domain does not match the domains for LDAP authentication. Administrators can be added from LDAP even if the email domain is not included in domains from LDAP authentication.

- When administrators add new users or administrators, they will receive an immediate error message if adding a user with an invalid email address.
- Pending invitations will now be properly resolved to grant sync and share access to existing administrative users.
- Exports of the users table will now include the the "Licensed" field.
- Sending a download link will now respect the blacklist and whitelist restrictions.
- Searching for new LDAP users to enroll should be much faster.
- New users who are in both a LDAP provisioned administrators group and a LDAP provisioned sync and share group will get the combined permissions.
- Mapping a home directory to an existing data source now works properly if the available data source uses the %USERNAME% wildcard.
- LDAP searches no longer display built-in groups which are not valid choices for group memberships.
- Slow home directory lookups will no longer cause mobile users to fail to enroll.
- Fixed an issue which could cause authenticating and accessing assigned sources with certificates on Windows 2003 R2 to fail.
- Unlicensed adhoc users are now properly restricted from connecting with the client to the server.
- Information in the Gateway Servers table is now updated immediately, instead of when you open the details tab for the server.
- The cosmetic "from" address in emails sent by Acronis Access now appears as the actual sender's email address.
- Old Acronis Access serial numbers are now removed when a new base serial number is applied.
- The installer will no longer create multiple Gateway server entries in Programs and Features on upgrade.
- Fixed memory leak in Gateway server.

Acronis Access 6.0.2

BUG FIXES

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

Acronis Access 6.0.1

ENHANCEMENTS

- Added a new policy to specify which gateway or cluster group will be used to share users' Active Directory assigned home folders. Active Directory assigned home folders will now automatically be shared by a gateway without the need to manually 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.
- Self-provisioned folders now can be added and removed successfully when the profile is configured to use either a gateway server or a cluster group, regardless of whether or not the server or cluster group is online.
- Policy priority order will be respected, so users will receive the highest priority group policy to which they are entitled.
- Clients who do not have sync and share enabled will no longer be incorrectly reported as "unmanaged" in the audit log.
- Files with Japanese or other characters in their filenames should no longer have the filenames changed when downloaded with Internet Explorer.
- Administrators should no longer see unresolvable errors when subscription licenses expire.
- The Access Desktop Client minimum version list now correctly includes 3.0 client versions, and will be honored for both old and new desktop clients.
- Home directories should no longer be inaccessible after upgrades from pre-5.0 versions of mobilEcho.
- Miscellaneous localization bug fixes.

Acronis Access 6.0.0

ENHANCEMENTS

- The mobilEcho and activEcho products have been combined into a single new product called Acronis Access Server. This changes the branding and product names in the mobile and desktop clients as well as the web application. Acronis Access Server 6.0 can be installed as an upgrade to mobilEcho and/or activEcho and existing licenses will continue to work. Customers are entitled to exchange their existing mobilEcho and/or activEcho license(s) for a new Acronis Access license that will enable the full functionality of the combined product. To request this upgrade, please **submit this web form**.
- Active Directory-based Administrator users are no longer required to have an email address assigned. Administrator users can also be added without configuring the Acronis Access Server for SMTP.
- A new checkbox is provided on the Server Settings that allows Sync & Share functionality to be turned on or off. By default when upgrading from mobilEcho to Acronis Access Server Sync & Share (formerly known as activEcho) is disabled.
- Active Directory distribution groups can now be invited to Sync & Share folders.
- Inviting many users to Sync & Share folders is now significantly faster.
- The Configuration Utility now includes more status / progress messages when it is setting up the server.
- The Configuration Utility will now generate an error if the repository is located on a remote network volume but the Repository Service is configured to run under the Local System account. The Repository Service needs to run under an account with permissions to the remote network volume.
- The Configuration Utility will now present an error if an SSL certificate is selected that does not have an embedded private key.
- Java has been upgraded to Version 7 Update 51.
- The Server Settings "Server Name" is now used as the title of the web site that appears to end users.
- The LDAP Cache refresh interval has been changed from 60 to 15 minutes.
- A new Advanced Setting for Gateway Servers has been added that, if enabled, users will authenticate with their UPN (example: username@domain.com). Otherwise, users will authenticate with their separate domain and usernames (example: domain\username). This is sometimes needed when authenticating to some federated scenarios, i.e., SharePoint 365.

BUG FIXES

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

Acronis Access 5.1.0

ENHANCEMENTS

- The Configuration Utility now provides the ability to control whether the Access Server should bind to HTTP port 80 and redirect automatically to the configured HTTPS port. Previously this was enabled by default, but now the administrator must enable it on clean installations.
- When editing email templates a new option allows the administrator to view the default value for the email subject.
- Users with mobilEcho 5.1 or later on iOS can now create their data sources directly from the application to access any file share or SharePoint location. Users enter UNC paths or SharePoint URLs from the client. New policy settings have been introduced on the management server to control whether clients are allowed to create these data sources, and which Gateway Servers are used for these requests.
- Multiple Gateway Servers can now share a common configuration via a Cluster Group. Changes to the settings and policies assigned to the Cluster Group are automatically pushed to all members of the Group. This will typically be used when multiple Gateway Servers are placed behind a load balancer for high availability.
- Gateway Servers now support authentication using Kerberos. This can be used to in scenarios using Kerberos Constrained Delegation to authenticate mobilEcho iOS clients through a reverse proxy using client certificates. It also can be used to authenticate mobile devices with client certificates using MobileIron AppTunnel. Note that when using this form of authentication, mobile clients cannot access activEcho shares.
- The required data sources are now automatically created when assigning home folders to a user or group policy. Previously administrators needed to manually create a data source for the server hosting the home directory.
- The address of a legacy Gateway Server can now be modified
- The policy exceptions for Android have been updated to reflect the functionality of the mobilEcho Android 3.1 client

BUG FIXES

- Exporting a large set of records from the audit log now completes significantly faster.
- Error messages from some dialogs are now properly cleared when the error condition is resolved.
- Only one instance of the Configuration Utility can now be run at a time.
- On Windows Server 2003, the uninstall process no longer reports that PostgreSQL was not installed by the Acronis Access Server installer.
- The Configuration Utility now generates an error if the Gateway Service is configured to bind to all address on a port and the Access Server on a specific address with the same port.
- By default on clean installs Tomcat is now configured to not listen for shutdown requests on port 8005. This prevents conflicts with other instances of Tomcat on a server. Because the Access Server Tomcat instance runs as a service, shutdown requests over network ports are not needed.
- Miscellaneous localization improvements.
- Improved performance displaying the log for non-administrative users
- Expired license notifications will no longer appear when activEcho is disabled via the Access Server administrator

- New users that receive an invite email now receive a message to set their initial password instead of changing the password
- The Upload New Files dialog no longer shows an extra field when using Internet Explorer 8 or 9
- The Windows Desktop Client will no longer re-upload content in some situations when the user's password expires and is re-entered
- Miscellaneous fixes to the file sync logic in the Desktop Client
- Removing a user or group policy with a custom home folder now properly removes the volume on the Gateway Server.
- Displaying Assigned Sources for a user now displays sources assigned to that user through their group memberships.
- Improved the ordering of the tabs in the Data Sources administration page.
- Changing a Gateway Server administration address no longer dismisses the edit dialog when clicking Apply.
- mobilEcho clients enrolling for management using client certificates will no longer fail periodically if the user was not already in the server's LDAP cache.
- Adding white space to Gateway Server addresses no longer prevents the Gateway Server from being properly managed.
- Notes in the Device Information dialog are now saved properly.
- When policies are disabled, they now appear grayed out in the policy list.
- On upgrade from mobilEcho Server 4.5 the mobilEcho users are now imported properly even if the wrong LDAP search base is entered in the configuration wizard.
- License keys starting with YD1 are now displayed properly as trials with an expiration date on the licensing page, instead of perpetual licenses.
- Enrollment email invitations now have proper links for Android clients.
- Editing SharePoint credentials for a Gateway Server is now disabled if the Gateway Server does not have a license supporting SharePoint connectivity.

Acronis Access 5.0.3

ENHANCEMENTS

- Acronis Access Server can now be installed on a Windows Failover Cluster, for Windows Server 2003 SP2, 2008/2008R2 and 2012/2012R2. Please see [Installing Acronis Access on a cluster \(p. 240\)](#) and [Upgrading Acronis Access on a cluster](#) for instructions on how to install or upgrade in this configuration.

BUG FIXES

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

Acronis Access 5.0.2

ENHANCEMENTS

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

BUG FIXES

- Localization improvements.
- Choosing to uninstall from the installer application now works on Windows Server 2003.
- Installer will now enforce that a minimum of 1GB of free disk space is available before installing.
- Upgrades from activEcho 2.7 now work properly on non-English PostgreSQL installations.
- Clients can now access data sources with a colon in their name.
- Upgrades from mobilEcho 4.5 now properly handle migrating SharePoint data sources.
- After an upgrade, the Assigned Sources tab in Data Sources now properly displays resources assigned to a user.
- Sorting the Active Users table by Policy or Idle Time no longer generates an error.
- Clients can now access Gateway Servers that are provisioned to be visible on clients and that have different addresses for client connections.
- Fixed a bug where home folders could fail to open in the mobilEcho client if the Access Server contained data sources with similar paths (for example "\\homes" and "\\homes2")

Acronis Access 5.0.1

BUG FIXES

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

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

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

Acronis Access 5.0.0

ENHANCEMENTS

- Acronis Access Server is a new shared server platform used by both mobilEcho and activEcho. Both products now use the same shared backend infrastructure. Functionality for each product is determined and enabled based on licensing.
- New integrated platform installer. Acronis Access server, mobilEcho and activEcho are included in the installer. Installer run time installation options allow administrator to determine what elements are deployed.
- Acronis Access Server automatically installs Java JRE and the required Java Cryptographic Engine policy files.
- New Server Configuration Utility allows administrators to set base configuration options like binding to specific IP addresses and ports, handling local machine firewall rules, installation of SSL certificates.
- Acronis Access Server is localized in English, German, Japanese and French.
- New startup wizard simplifies initial configuration of the server
- Redesigned, updated user and management web interfaces, including responsive design with support for mobile devices.
- New paging tables support display, sorting and filtering of much larger sets of data. The log filtering has been improved, including filtering by typing partial user names, by message type, etc.
- Redesigned, easier to use Projects view for end users.
- activEcho Clients (Mac/Windows) have been localized in German, Japanese and French.
- Support for HTML5 drag and drop file uploading directly to the web interface. One or many files can be uploaded via Drag and Drop in a single operation.
- Improved file upload handling, including progress indicators in the web interface and the ability to cancel uploads.
- Folders can be downloaded as a ZIP file from the Projects view in the Web UI.
- Individual files can be shared with other users. Those users will get a link to download the files, which can be configured to expire.
- Sharing invitation dialogs now support type-ahead against both local users and users in Active Directory / LDAP.
- The previous revisions feature for finding / downloading / restoring previous versions of files has been redesigned and is more flexible. Previous revisions can be selected to be "made current".
- activEcho desktop clients (Mac/Windows) now show progress indicators files being synchronized.
- New "unsubscribe" button is available in folders shared to you.
- Sorting criteria chosen by the end user is now saved when browsing project folders.
- Event Notifications can now be configured globally as default settings for all shares. Users can override the defaults for individual shares.
- Notifications can now be configured to be sent when a file is downloaded / synced.
- activEcho clients on Windows now perform validation of SSL certificates using the built-in Windows certificate store. This improves compatibility with 3rd party certificate authorities.
- Improved user interface responsiveness for re-assigning content when there are 1000s of users in the system.
- The Amazon S3 access key no longer displayed in plain text on the administration pages.

- Improved page load times when there are many users and/or files, especially when quotas are in use.
- Improved support for email invitations using different formats of email addresses.
- Wildcards can now be used in domains for sharing black and whitelists.
- Administrators can now globally hide the checkbox "Allow collaborators to invite other collaborators".
- New Administration mode toggles between a user's individual project / log views and the administration console.
- mobilEcho client management has been fully integrated into a common web administration interface. This can be used for managing mobile clients for activEcho, or if a mobilEcho license is provided the single console can manage all mobilEcho and activEcho functions.
- Users list can now be exported.
- The mobilEcho Client Management Server is integrated with Acronis Access Server and built on Apache Tomcat and PostgreSQL database for improved scalability and resilience.
- The mobilEcho Administrator previously used to manage individual mobilEcho servers has been removed; Access Gateway Servers (formerly mobilEcho File Access Servers) are now managed directly within the Acronis Access Server web administration user interface.
- mobilEcho Client Management Server configuration file has been removed; configuration settings previously in the configuration file are automatically migrated and are now managed through the Acronis Access Server web administration user interface.
- Configuration of data sources (formerly assigned "Folders") to be shared to mobile devices has been redesigned.
- New "Assigned Sources" capability allows administrators to get a report of all of the assigned resources that a particular Active Directory user or group will receive.
- Audit logging can be enabled to report on mobile user activity across multiple Acronis Access Gateway Servers.
- Administrators can now be granted different permissions for administrative activity, including managing users, data sources, mobile policies or viewing the audit log. This can be based on individual users and/or membership in Active Directory groups.
- Devices operations such as remote wipe or removing devices from the device list can now be performed in batches.
- A catch-all "default" policy can be configured which applies to all users that don't match configured Active Directory user or group policies.
- New policy options allow specification that content on the device within the "My Files" and "File Inbox" folders expires and is removed after a certain amount of time.
- When sending an enrollment invitation to an Active Directory group, users who are already enrolled through another group can be filtered out.
- A warning is presented if a user is invited for enrollment but does not match any existing user/group policy.
- The devices table now lists the user or group policy in use for each device.
- Cached Active Directory / LDAP information about users is now updated periodically in the background.
- Content searching is now available against remote Windows file shares running Windows Search.
- A policy cannot be deleted if a device is being managed by it
- mobilEcho enrollment invitation templates can be modified directly from within the web administration console. Multiple languages for each template are supported.

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

BUG FIXES

- Improved support for exporting Unicode characters to TXT or CSV files.
- Folders that cannot be shared no longer have the Invite... option.
- Users can now remove themselves from the share even if they do not have permission to invite other users to the share.
- If a file or folder cannot be downloaded to a Windows client because the name is too long, unchecking the Sync to devices option in the web interface now resolves the error on the client by removing the entire shared folder.
- activEcho clients properly handle error when uploading files and user is out of quota space.
- Users can now be deleted even if they are listed on the black list.
- Files can be uploaded to the repository when encryption is disabled.
- Home directory configuration is now retrieved properly when LDAP is configured to use the global catalog.
- Improved handling of Active Directory lookups when trailing spaces are used.
- The "Enrolled at" date is now formatted properly when exporting to .CSV file.
- Improved support for displaying Unicode via the web administration user interface.
- SharePoint folders ending with a space can now be enumerated by clients.
- SharePoint libraries that have extra slashes now support file deletion and copy properly.

16.2 What's New in the Acronis Access app

Note: Acronis Access 7.5 for iOS and later will no longer support iOS 7. Customers on this platform can continue to download the existing application using Apple's "latest compatible version" functionality.

Access Mobile Client 7.8 [iOS]

ENHANCEMENTS:

- Added in-app web browser.
- Added support for opening password protected Office documents.
- Improved tutorial functionality.

Access Mobile Client 7.7.1 [iOS]

BUG FIXES:

- Fixed various issues related to camera capture.
- Fixed an issue when using Touch ID in share and action extensions.

Access Mobile Client 7.7 [iOS]

ENHANCEMENTS:

- Added in-app camera capture.
- Added new Sync & Share data source section.
- Added support for Sync & Share invitation date expiry and language.
- Added new search mode to PDF viewer.
- Added bookmark saving to PDF viewer.
- Added new setting to choose how hyperlinks are opened.
- Added Touch ID authentication to share and action extensions.
- Made minimized file drawer available application-wide.
- Made commonly accessed view settings directly available in PDF viewer.
- Improved application performance during sync checking.

BUG FIXES:

- Fixed minor display issues on iPad Pro.

Access Mobile Client 7.6.1 [iOS]

ENHANCEMENTS:

- Added support for iOS 10.
- Added the minimized file drawer to all file viewers.
- Improved performance of PDF viewer.
- Fixed an issue that would cause printing to not be available in PDF viewer.

Access Mobile Client 7.6 [iOS]

ENHANCEMENTS:

- Added document provider extension for seamless read/write access to Acronis Access storage from third-party applications.
- Added action extension for streamlined saving of files from third-party applications back into Acronis Access storage.
- Added support for SharePoint Followed Sites.
- Added support for iOS multi-tasking.
- Improved support for iPad Pro devices.

Access Mobile Client 7.5.1 [iOS]

ENHANCEMENTS:

- Various improvements to PDF toolkit including performance, stability, and functionality

- Improved e-mail address validation to better conform to RFC-822
- Improved handling of PDFs containing errors

BUG FIXES:

- Fixed an issue when authenticating through a reverse proxy
- Fixed an intermittent crash when importing images into PDFs

Access Mobile Client 7.5 [iOS]

Removed support for iOS 7. Customers on this platform can continue to download the existing application using Apple's "latest compatible version" functionality.

ENHANCEMENTS

- All-new PDF annotation toolkit that also allows annotation from iPhone.
- Added support for CMIS data sources.
- Added a 'press and hold' gesture that opens the edit menu.
- Improved generation and handling of cross-platform file and folder links.

Access Mobile Client 7.2 [iOS]

ENHANCEMENTS

- Improved Japanese text rendering in the Office editor. ACIOS-3119
- Added support for Touch ID. ACIOS-930
- Added Italian localization. ACIOS-3458
- Added options to the Sync & Share invitation dialog for "Allow to invite other members" and "Allow to view other members of this share." ACIOS-2093
- Added a policy restriction to allows users to create 1-way sync folders only. ACIOS-3382
- Improved support for volumes containing special characters in their names. ACIOS-3004
- Added support for custom fonts when editing Office documents. ACIOS-3453
- Improved timing and stability of application startup when using MDMs.

BUG FIXES:

- Fixed an issue that would cause enrollment to fail and loop when an incorrect password was supplied via MDM auto-enrollment. ACIOS-3217
- Fixed an issue that would cause a sync folder to have to resync its content if the display name was changed.
- Fixed an issue with copying and moving files with colons in their names. ACIOS-3222
- Reduced the number of messages received when launching the application in Airplane Mode with sync folders. ACIOS-2364
- Fixed an issue that would corrupt file links in Excel documents. ACIOS-3118

- Fixed the display of the number formatting toolbar in the Office editor. ACIOS-3121
- Fixed an issue that would cause Bookmarks to be deleted when unmanaging. ACIOS-3002
- Fixed an issue that would not allow media files to be previewed when using mobilecho:// links. ACIOS-2823
- Fixed an issue that could cause Powerpoint presentations with hidden objects to render incorrectly.

Access Mobile Client 7.0.5

ENHANCEMENTS:

- Added support for Microsoft Intune mobile application management.
- Added the ability to unzip compressed files.
- Added a setting to disable hyperlink underlining in PDFs.

Access Mobile Client 7.0.4

ENHANCEMENTS:

- External (ad-hoc) Sync & Share users can now successfully add an Access Server using the app first-run setup process

BUG FIXES:

- Fixed issue related to bookmarks pointing to folders that have ":" in the name
- Fixed an issue where mobilEcho:// links didn't work on iOS 9
- Fixed an issue with mobilEcho:// links to resources residing on user-added gateway servers
- Fixed an issue writing to the root of certain datasources
- Fixed an issue with copy operations between data sources if "Once per session" login frequency is set on the server

Access Mobile Client 7.0.2

BUG FIXES:

- App enrollment to server names that contain a path after server address, e.g. "proxy.example.com/access", is now supported.
- App enrollment will now succeed if the Access gateway server's port is explicitly specified and the "Require that client is enrolled with an Acronis Access server" policy is enabled

Access Mobile Client 7.0.0

ENHANCEMENTS:

- Brand new design and style
- Pop-up use guide for first time run on the app
- Restyled office editing tool

- Collapsible left hand menu
- Support for portrait orientation file browsing on the iPad
- Much faster thumbnail preview generation
- Increased speed & performance when working with files within the app
- New 'Edit mode' for selecting and working with multiple files
- New 'Paste bar' for copying and moving files
- All files now open immediately into Preview mode when tapped. Office files and text files can then be edited by tapping the Edit icon (a pencil icon) in the menu bar. PDFs can be immediately annotated at any time.
- Pull down on the file list/grid to reveal sort options and view options (list or thumbnail/grid)
- When viewing a folder, the process of adding new folders, files, photos, video to that folder and syncing and bookmarking the folder are all handled through the "+" button in the menu bar
- Adding new Access Servers and "Network folders" are done with the "+" button while browsing the top level "Network" item
- Bookmarks are now displayed in the "Favorites" section. This section will be expanded with more features in later releases. For example, the display of recently opened and newly added/synced files.
- There is no longer a "File Inbox" folder. All files sent to the Access app from other apps can be quickly saved to the folder of the user's choice using the 'Paste bar'.

Access Mobile Client 6.1.5

BUG FIXES:

- Fixed an issue that could occur while manual starting syncs of multiple folders simultaneously.
- Fixes an issue displaying Japanese and Chinese fonts while editing Office files on iOS 8.2
- Fixes an issue displaying Korean and Thai fonts while editing Office files on iOS 8.2

Access Mobile Client 6.1.4

BUG FIXES:

- Fixed an issue that could occur while syncing a home directory folder.
- Fixed an issue where documents with protected fields could encounter compatibility issues when saved by SmartOffice.

Access Mobile Client 6.1.3

BUG FIXES:

- Fixed an issue with Asian fonts not displaying correctly in SmartOffice.
- Fixed an issue with hyperlinks not working in SmartOffice when created by a script.
- Fixed an issue that could occur while saving a presentation in SmartOffice.
- Fixed an issue that could result in loss of MobileIron AppConnect configuration.

Access Mobile Client 6.1.2

BUG FIXES:

- Fixed an issue that could cause the app to crash on iOS 8.

Access Mobile Client 6.1

ENHANCEMENTS

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

Access Mobile Client 6.0.1

BUG FIXES

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

Access Mobile Client 6.0

ENHANCEMENTS

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

mobilEcho 5.1

ENHANCEMENTS

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

mobilEcho 5.0

ENHANCEMENTS

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

mobilEcho 4.5.2

ENHANCEMENTS

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

mobilEcho 4.5.1

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

mobilEcho 4.5

ENHANCEMENTS

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

17 Documentation for older versions

For older versions of Acronis Access documentation, please check the links below:

Note: *Your preferred language might be unavailable for older documentation.*

7.5.x

7.4.x

7.3.x

7.2.x

7.1.x

7.0.x

6.0.x

5.0.x