Microsoft SQL Server Backup to Windows Azure Tool

# Overview:

SQL Server 2012 and SQL Server 2014 have built in capability to back up to Windows Azure storage. The SQL Server Backup to Windows Azure tool provides the same functionality to previous versions of SQL Server. It can also be used to specify encryption and compression for your backups.

Using the 3-step wizard, you can specify a rule or set of rules that are applied to any SQL Server backup. One example of a rule could be to redirect all local backups to the specified Windows Azure storage. Another example of a rule would be to use compression or encryption for backups stored in a specific location.

Once you configure the rules, these rules are applied to SQL Server Backup files. If the rule is set to use Windows Azure storage account, the tool redirects the backups to the specified Windows Azure storage account, but leaves a stub file with metadata information to be used during restore.

## Benefits:

* Support for backups to Windows Azure Storage for SQL Server versions that do not have the built-in capability. Using Windows Azure storage for your backups has several benefits off-site storage for disaster recovery, ability to access from any location, etc. For more information, see [SQL Server Backup and Restore with Windows Azure](http://go.microsoft.com/fwlink/?LinkId=327759).
* Encryption and Compress support for SQL Server versions that do not have the built in capability. Currently only SQL Server 2014 has encryption support, and SQL Server 2008 or later support compression during backup. SQL Server 2008 supports compression in Enterprise edition only, but for SQL Server 2008 R2 and later encryption is supported on Standard editions or higher.

# Installing the Tool:

The setup is simple and involves the following steps:

1. From the download page, download the MSI (x86/x64) to your local machine that has the SQL Server Instances installed. If your production machines do not have access outside of your organization, download to a local share and use the MSI to install the tool on your production machines.
2. Double click the MSI file to start the installation.
3. Read and accept the terms of the license agreement, and click **Install** to start the installation process.

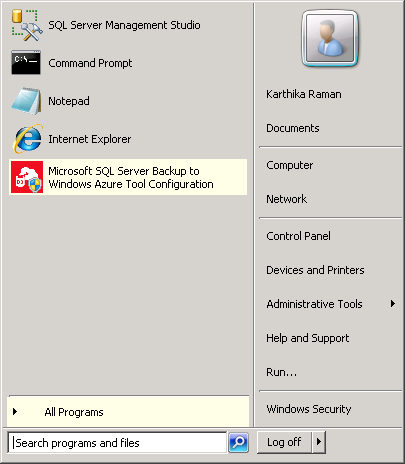
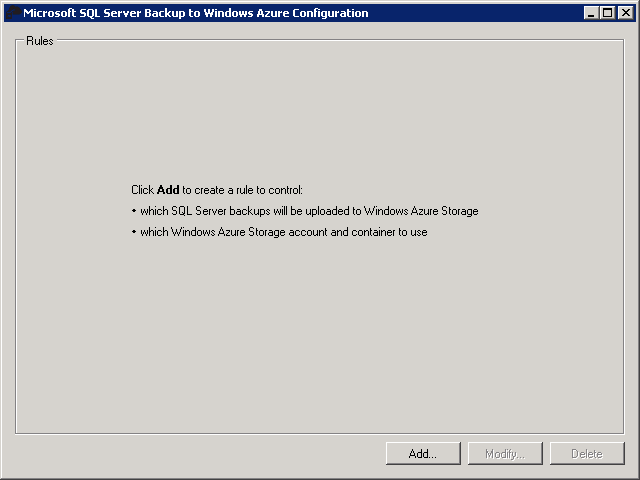
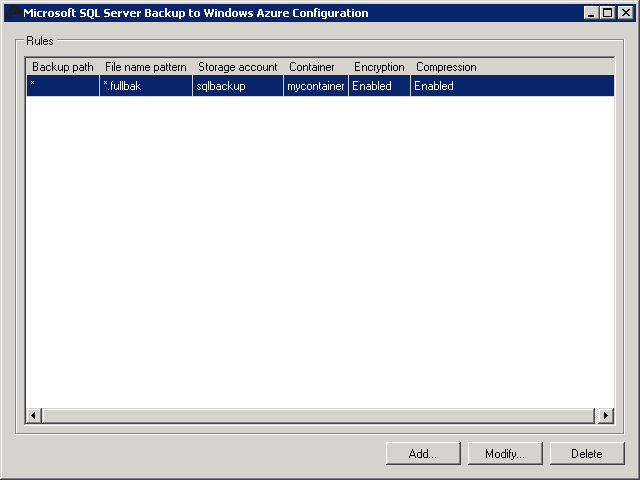
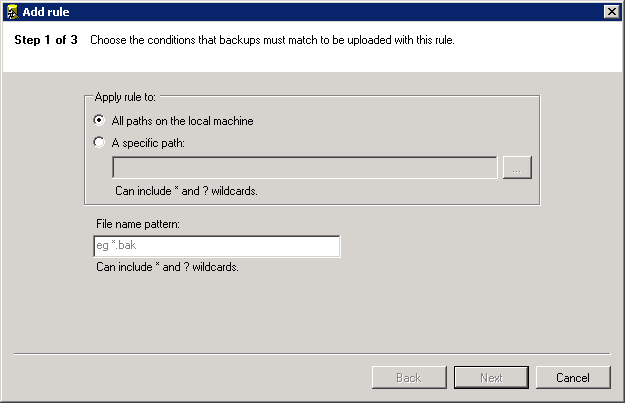
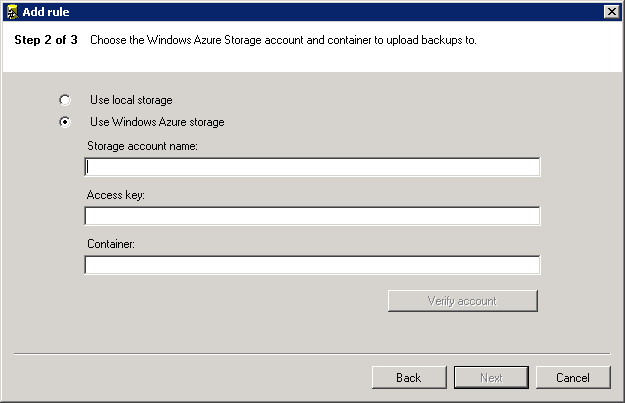
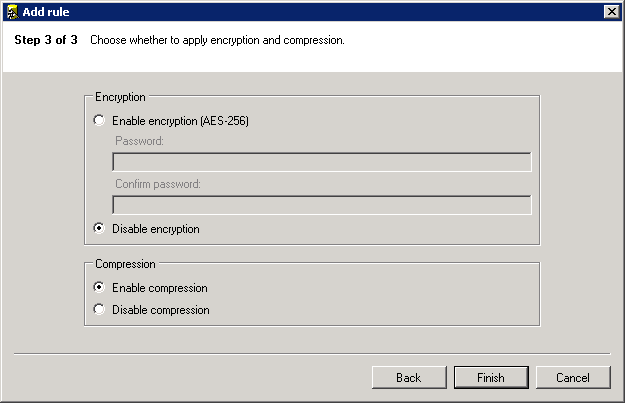
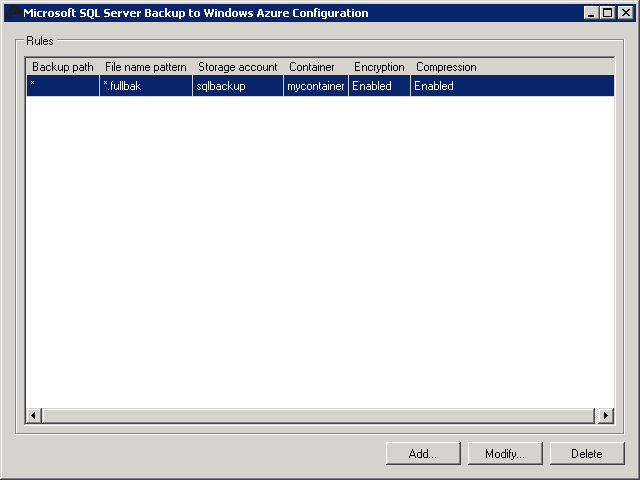
## SQL Server and Operating Systems Support:

This tool is supported on SQL Server 2005 or later, and Operating System versions: Windows Server 2008 or later for Servers, and Windows 7 or later for Client Operating Systems.

# Prerequisites:

* Windows Azure subscription and a Windows Azure Storage Account.
  + You can log in to the [Windows Azure Management Portal](https://manage.windowsazure.com/) using your Microsoft account. If you do not have a Microsoft account, [visit Windows Azure 3-Month free trial](http://go.microsoft.com/fwlink/?LinkId=271927).
  + To create a Windows Azure storage account, see [How to Create a Windows Azure Storage Account](http://www.windowsazure.com/en-us/develop/net/how-to-guides/blob-storage/#create-account).
* A Windows Azure Blob Storage Container: SQL Server uses the Windows Azure Blob storage service and stores the backups as blobs. A container is a grouping of blobs an all blobs must live in a container.

## How to Use the Tool to Create Rules:

1. Once installed the Tool, the tool should be appear on the Programs list. Here is a screen shot from a Windows Server 2008 R2 machine: 
2. Click on the “**Microsoft SQL Server Backup to Windows Azure**…” to start the Wizard.
3. On the **Rules** page, click **Add** to create a new rule. NOTE: Only the **Add** button is enabled if you are using this tool for the first time. Once you have created one or more rules, you will see the existing rules and the option to **Modify** or **Delete** the rule as shown below. 
4. On the **Add Rule (Step 1 or 3)** page, you can either choose to apply the rule to all paths to the local machine or to one specific location. You must also specify the file name pattern that this rule should apply to. For example, if you want to apply this rule to all files with the extension .bak, you would specify \*.bak in the File name pattern field. 
5. **On the Add Rule (Step 2 of 3)** page, you can specify the Windows Azure storage account information, so the backups you specified in Step 1 can be redirected to use the Windows Azure storage as the backup destination. Alternatively, you can choose to keep the local storage as the backup destination.
   1. For Windows Azure Storage, you must specify the name of the account, the storage access key, and the name of the container. You can retrieve the name of the storage account and the access key information by logging into the Windows Azure management portal. The storage name and access key are used to authenticate to the storage account, the container. Click **Verify account** to ensure that the information specified is valid and the tools is able to connect to the storage account. 
6. **On the Add Rule (Step 3 or 3)** page, you can enable or disable encryption or compression. If you enable encryption, you must specify a password. Once you specify the options, click **Finish** to create the rule. 
7. On clicking Finish you will see the following page with the rule configuration. 

# Restoring a Database from backups in Windows Azure Storage:

The SQL Server Backup to Windows Azure Tool creates a ‘stub’ file with some metadata to use during restore. Use this file to point your restore operations to. SQL Server uses the metadata from this file and the backup on Windows Azure storage to complete the restore.

# Additional Resources:

[SQL Server Backup and Restore with Windows Azure](http://go.microsoft.com/fwlink/?LinkId=327759).