BackupVault Management Console

USER MANUAL
For Microsoft Windows

backupvault.co.uk

BACKUPVAU

Copyright Notice & Proprietary Information

Trademarks

® - Microsoft, Windows, Microsoft Windows, Microsoft Windows Server, Microsoft Server, Microsoft Volume Shadow Copy Service, MS Windows, MS SQL, MS Exchange, Internet Explorer, and Windows Explorer are registered trademarks of Microsoft Corporation.

Instruction Symbols

The following icons appear in the document:

***Note**: Important additional information.*

***Example**: Practical illustration of a process or procedure.*

***Tip**: Suggestion or hint to guide or assist users performing a task.*

***Warning**: Warning against potential mistakes and actions that could cause critical error.*

Contents

1. Introduction

Congratulations on choosing the BackupVault Storage Platform. BackupVault minimises risk, maximises productivity and allows businesses to regain control of their most valuable asset - their data.

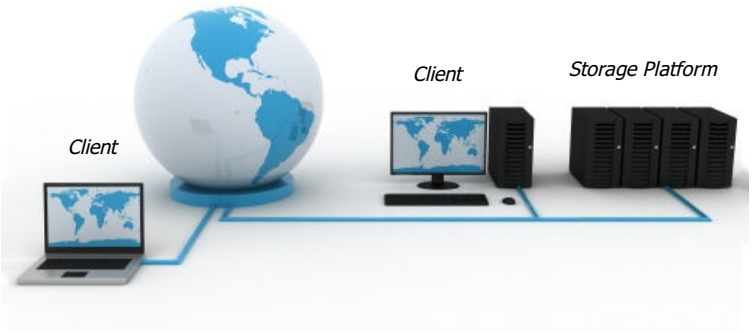
For technical support, please contact your software provider.

Product overview

The BackupVault Storage Platform Console is a management tool that enables you to manage the Storage Platform and all the elements within the larger backup environment. The BackupVault storage solution, the Storage Platform and the Storage Platform Console are explained in more detail below.

Storage solution

Within a BackupVault storage solution setup, Backup Clients (Desktop & Laptop [DL], Server Edition [SE] and/or Enterprise Server Edition [ESE]) connect and back up data to the Storage Platform.



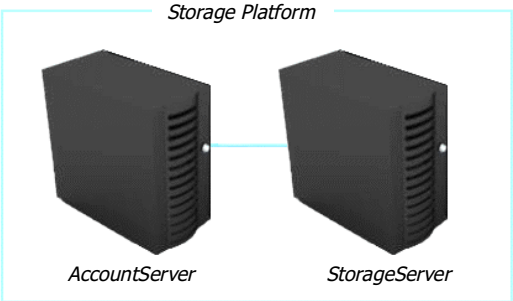
This diagram illustrates a common scenario:

Files and folders stored on one or more machines running DL, SE or ESE can be backed up to a Storage Platform over an Internet connection or within a Local Area Network.

In the event of data loss or corruption on the server, data can be retrieved from the Storage Platform and restored to the original or another Backup Client in just a few easy steps.

Storage Platform

A BackupVault Storage Platform (SP) consists of an AccountServer (AS) connected to one or more StorageServer[s] (SS). The AccountServer manages user authentication information and Backup Group management. This information is distributed to individual StorageServers and is used by the ESE Backup Clients to connect directly to StorageServers; DL and SE Backup Clients connect to the AccountServer. The StorageServer is the file storage location for Clients' encrypted data.



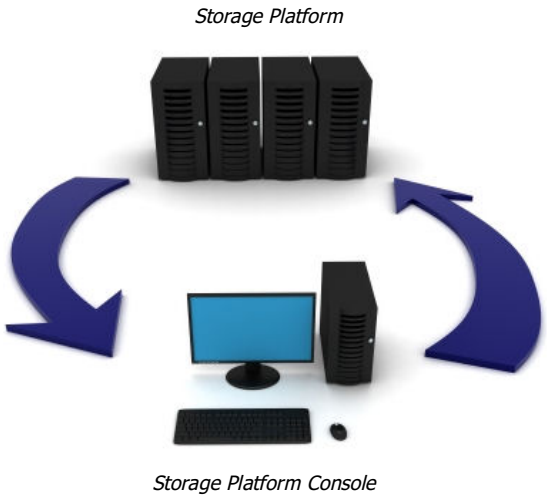
The diagram on the left represents a common scenario:

When an AccountServer is connected to one or more StorageServer(s), together they function as a Storage Platform.

***Note**: These components (AS & SS) may run on the same or separate physical platforms.*

Storage Platform Console

The BackupVault Storage Platform Console (SP Console) is used to manage and administer all the elements within the storage solution.



The diagram on the left represents a simplified scenario:

The Storage Platform Console connects to the Storage Platform and enables the management of the entire backup environment (Backup Accounts, Backup Clients and the Storage Platform).

2. Getting started

This chapter is a Quick Guide to getting the Storage Platform Console up and running.

***Note**: For more detailed information on using the SP Console, see Chapters 3 to 9 later in this manual.*

How to set up an SP Console

Follow the steps outlined below to set up the SP Console to access and control the Storage Platform and Backup Accounts (i.e. the backup environment):

Step 1: Install the SP Console

To install the SP Console on a Windows operating system:

1. Ensure that the machine on which you wish to install the Console meets the minimum system requirements listed in Chapter 3, “Installation”.
2. Run the Console installer issued to you by your software provider.
3. Follow the Setup Wizard steps.

***Note**: For detailed information on each of the wizard steps, see The Setup Wizard in Chapter 3, “Installation”.*

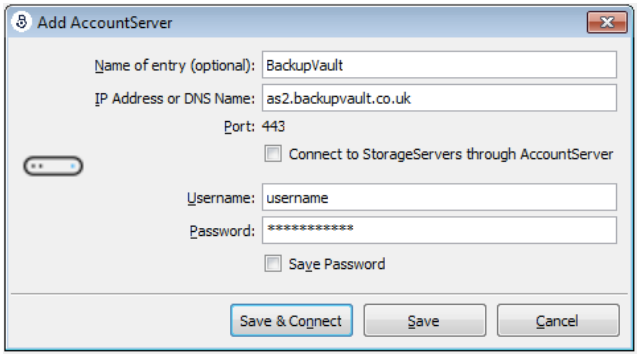
After completing the wizard, the SP Console will be installed. The next step is to connect to the Storage Platform.

Step 2: Connect to the Storage Platform

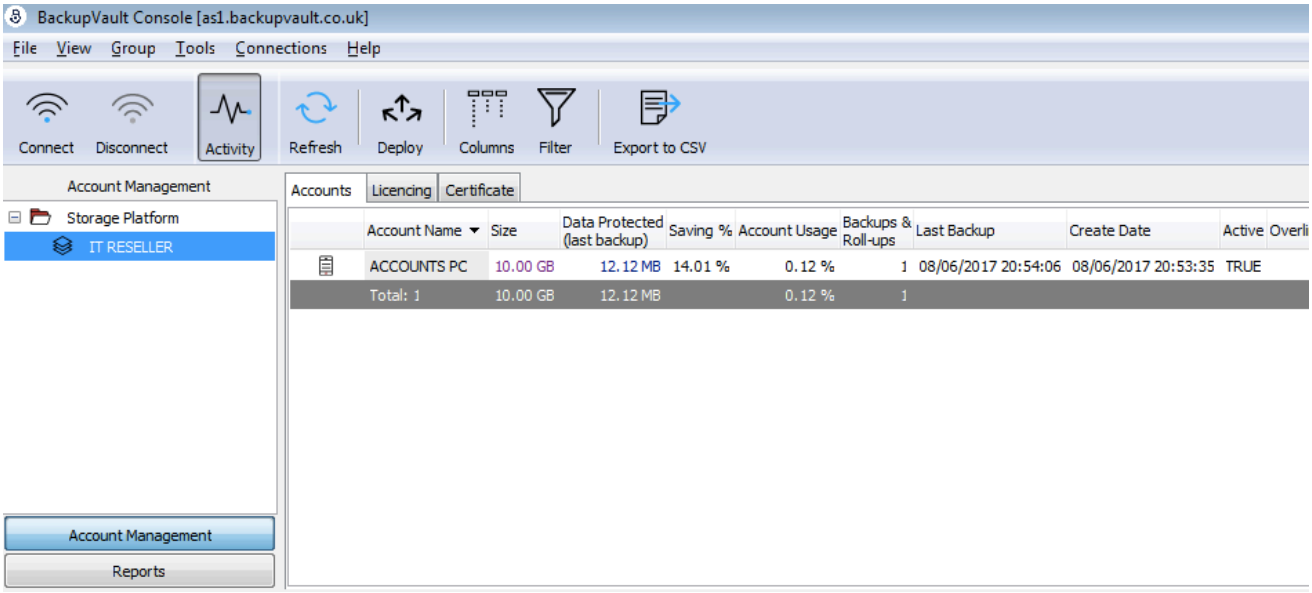
The SP Console can connect to an AccountServer to perform Storage Platform-wide administrative functions. However, it can also connect directly to MirrorServers with limited administrative functions should the AccountServer be unavailable.

To connect to a Storage Platform from the AccountServer for the first time:

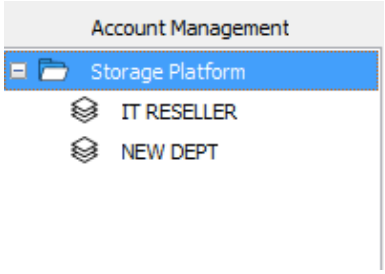
1. In the **Add AccountServer** dialog box that appears when you open the SP Console for the first time, enter the details of the AccountServer you wish to connect to in the boxes provided.
2. Click **Save and Connect.**



Once connected, the SP Console opens in Account Management view by default.



If there are any Collections or Backup Groups already created on the AccountServer, they will display in the Account Management tree, under the **Storage Platform** node.



An SP Console user with the correct permissions can configure the Storage Platform, create and configure Collections and Backup Groups and manage any Backup Accounts that already exist on the Storage Platform.

***Note**: The configuration options available depend on your user access rights. As an Admin user, you have full access rights. For a detailed description of the rights available, see Chapter 9, "User Access Management".*

As every Backup Account needs to belong to a Backup Group, you need to add at least one Backup Group to the SP Console. For more information, see *Adding and deleting Groups* in Chapter 6, "Account Management".

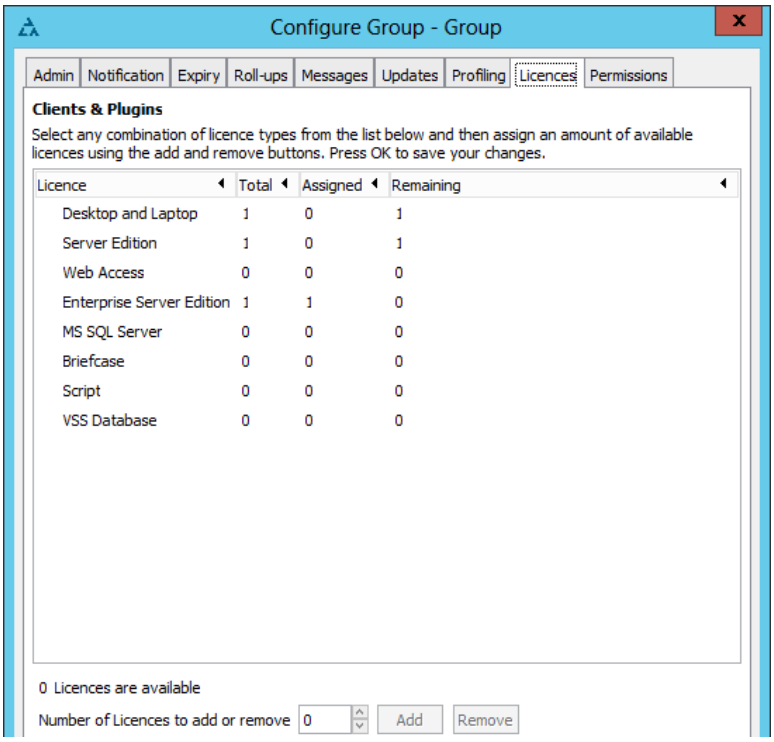
Once you have added a Backup Group, you need to add the appropriate licences to allow users to add new Backup Accounts to it.

***Note**: New Backup Accounts are created via the Account Wizard that runs immediately after a Backup Client installation is complete. For more information, please refer to the relevant Backup Client User Manual (Desktop & Laptop or Server Edition).*

Step 3: Add licences to Backup Groups

Before Backup Accounts can be created on the Storage Platform, appropriate licences need to be added to the relevant Backup Group. These must be added from the pool of purchased licences available.

***Note**: To purchase additional licences, please contact your software provider.*



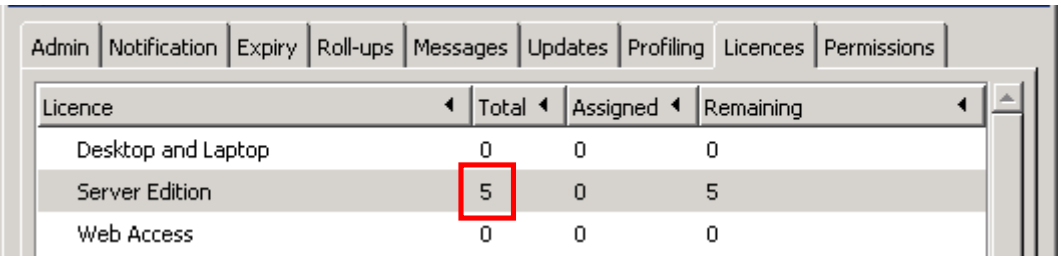
To add licences to a Backup Group:

1. In the Account Management view, expand the **Storage Platform** node in the Account Management tree.
2. Double-click the Backup Group name. Alternatively, right-click the name, and then click **Configure**.
3. In the **Configure Group** dialog box that appears, click the **Licences** tab.
4. Select the type of licence to add to the Backup Group. E.g. **Server Edition**.
5. In the **Number of Licences to add or remove** box, type the number of licences to add.
6. Click the **Add** button.

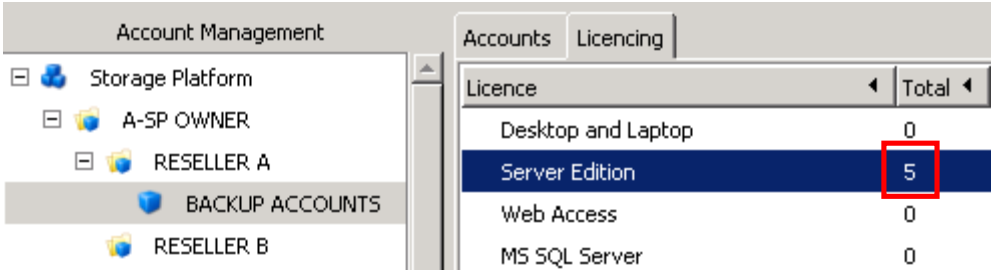
   ***Tip**: If the **Add** button is disabled, ensure that the Backup Collection to which the Group belongs has sufficient licences assigned to it.*

7. Click **OK**.

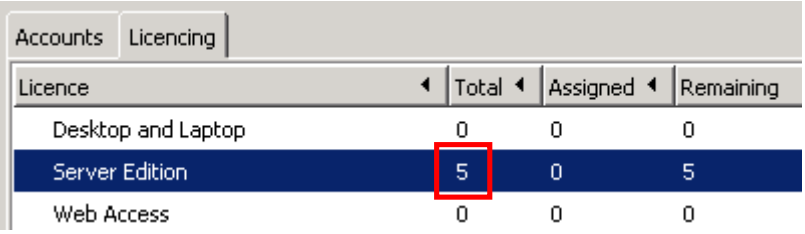
The number of licences added to the Backup Group will display in the **Total** column on the **Licences** tab in the **Configure Group** dialog box:



The number of licences will also display in the **Total** column on the **Licencing** tab in the Account Management view:



Now that licences have been added to the Backup Group, a deployment MSI (installer) file can be created from that Backup Group and used to install Backup Clients onto desktop, laptop or server machines. Those installations will enable users to create new Backup Accounts that belong to the Backup Group from which the MSI was deployed. For each Backup Account created, one licence is assigned and the number of remaining licences available for use displays in the **Remaining** column.

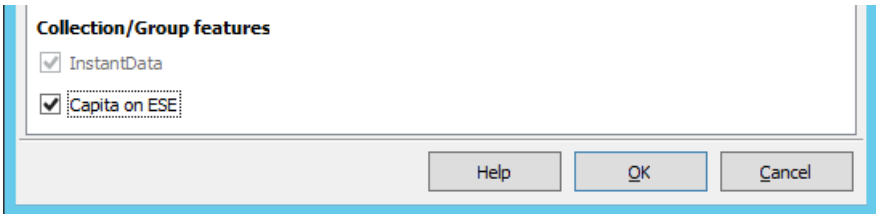


Collection/Group feature licences

Take note of the additional licences that can be allocated to groups at the bottom of the **Licences** tab.

***Note**: These licences must be enabled on the Collection first before they can be enabled on the Group.*

The licences are:

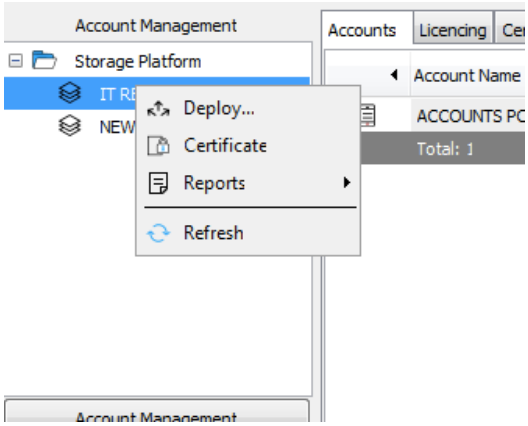


- **InstantData.** Allows connecting to a Backup Account with the InstantData application (see the "InstantData User Manual" for more information)
- **Capita for ESE.** Allows the ESE Backup Client to configure and back up data from the Capita modules.

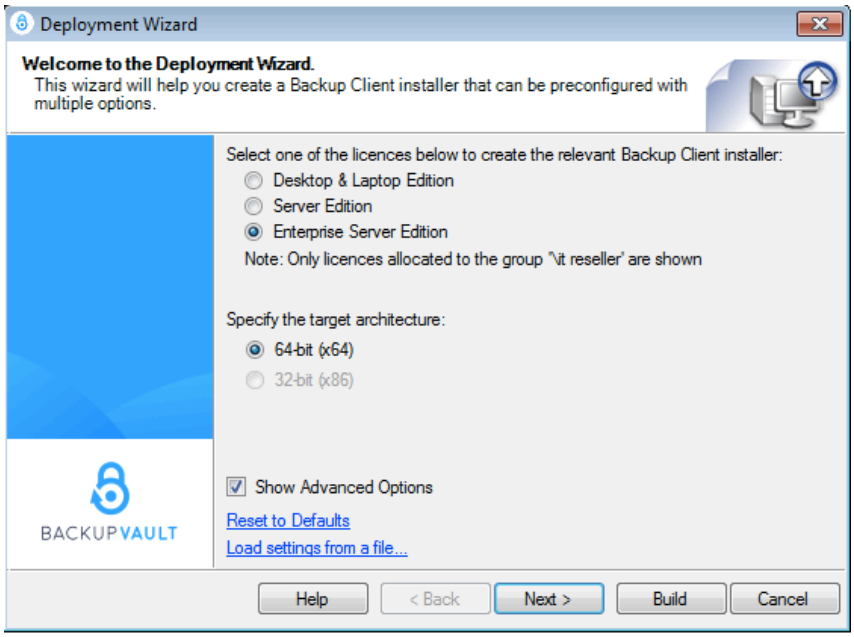
Step 4: Deploy an MSI (installer) file

To deploy an MSI file:

1. In the Account Management view, expand the **Storage Platform** node in the Account Management tree.
2. Right-click the name of the Backup Group to which the new user(s) should belong and then click **Deploy**. The Deployment Wizard will launch.



3. Select the type of Backup Client installation to create, select the folder in which to save the installation, click **Next** and then complete the Deployment Wizard.

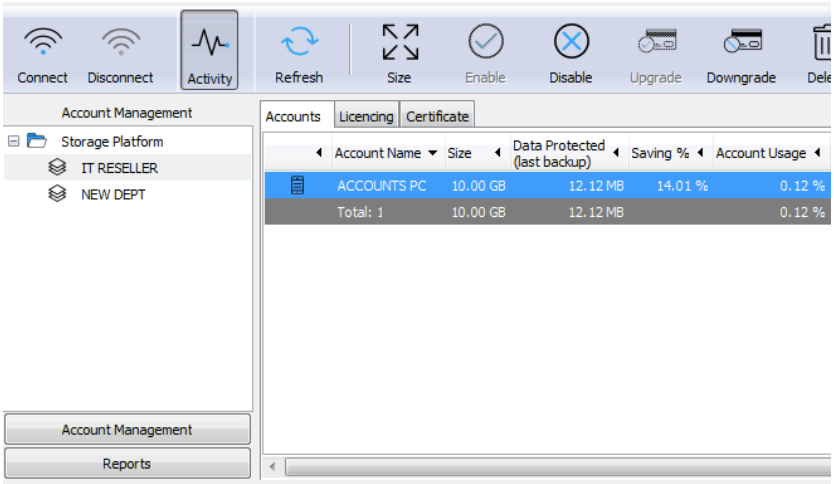


For more information, see *Deployment Wizard* in Chapter 6, “Account Management”.

After completing the Deployment Wizard, an MSI file will be created. This file can be used to install the BackupVault Client application, create a Backup Account and initiate the first backup.

***Note**: For more information on installing the Backup Client application and creating Backup Accounts, please refer to the relevant User Manual (BackupVault Desktop & Laptop, Server Edition and Enterprise Server Edition User Manuals).*

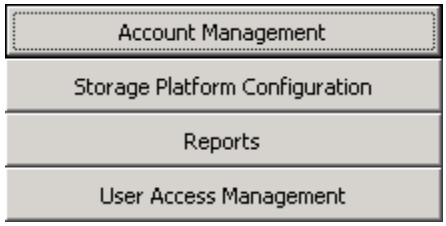
Once the new Backup Account is created via the Backup Client, the Account name will display on the Accounts tab in the Account Management view and users with the correct permissions will be able to manage those Backup Accounts.



***Note**: If a new Account is added while you are working on the **Accounts** tab, you may need to refresh the tab to view the latest list. To do this, click the **Refresh** button on the toolbar.*

Step 5: Start managing the backup environment

To manage the backup environment:



1. Depending on the type of management to be performed, click the relevant view button in the view selector.

   ***Note**: The views available depend on the user access rights assigned to you by your Backup Administrator. As an Admin user, you have access to all the options described below.*

2. Use the management tools available in the selected view to manage the backup features. For more information on tools, tasks and views, see:

   - Chapter 6, “Account Management”
   - Chapter 7, “Storage Platform Configuration”
   - Chapter 8, “Reports”
   - Chapter 9, “User Access Management”

3. Installation

Installing the SP Console on a computer enables its users to manage the Storage Platform. User Access Management enables you to provide SP access to everyone involved in its administration, with the option of limiting the functionality available to each user.

***Note**: For the latest system requirements and compatibility information, please refer to the **System Requirements and Compatibility Matrix**.*

Setup Wizard

To install the Storage Platform Console:

1. Run the SP Console installer issued to you by your software provider. This will launch the SP Console Setup Wizard.
2. Follow the Setup Wizard steps as described below.

***Note**:*

- *The SP Console installer will automatically detect if an earlier version is installed. If so, it will launch any necessary updates. The updated SP Console will retain the display and connection settings of the previous version and use the same directory locations (unless different locations are specified during the installation, in which case it will store the settings in the new Console locations).*
- *The SP Console installer will run automatically after the Storage Platform installation if located in the same folder as the Storage Platform installer.*

The Setup Wizard typically consists of six steps that guide you through a relatively complex task in a simple, step-by-step manner and allow you to undo previous operations by navigating backward.

Step 1 of 6: Start the wizard

To start the Setup Wizard:

Click **Next** to begin the installation setup.

Step 2 of 6: Select a destination location

To specify where the SP Console should be installed:

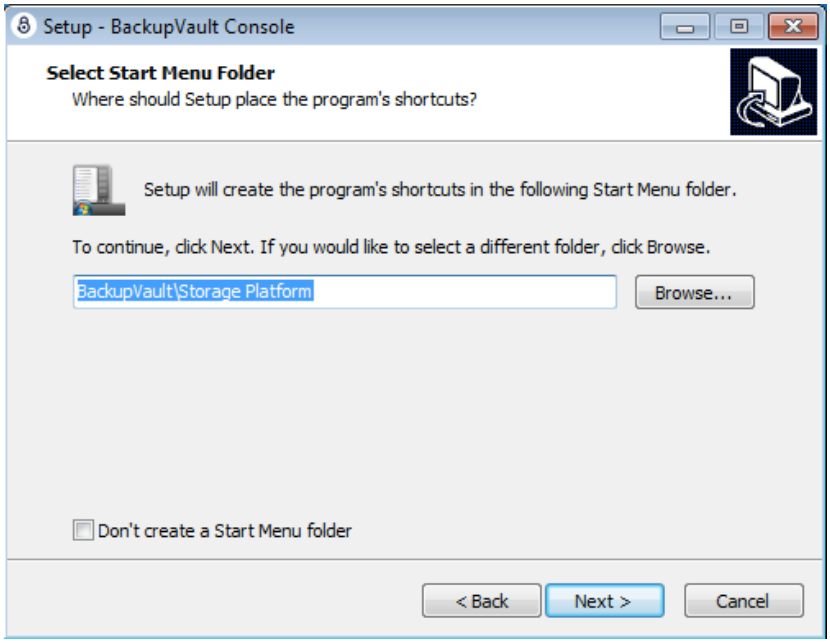
- Either accept the default location by clicking **Next**;
- Or click the **Browse** button, specify a different location, and then click **Next**.

Step 3 of 6: Select a Start menu folder

To select the Start menu location:

- Either accept the default location by clicking **Next**;
- Or click the **Browse** button, specify a different location, and then click **Next**.

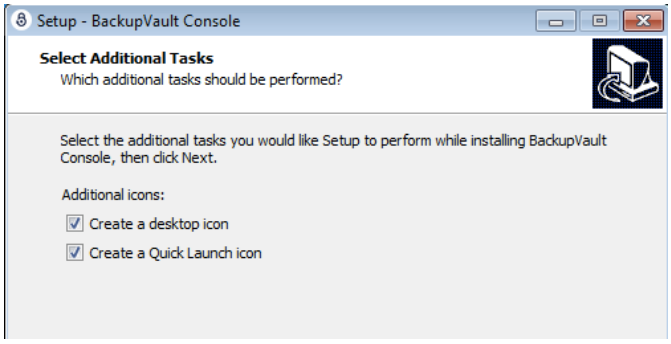
***Tip**: If you do not wish to add an SP Console menu item to the Start Menu, select the **Don't create a Start Menu** folder check box at the bottom of the wizard screen.*



Step 4 of 6: Select additional tasks

To create additional icons:

1. Select whether a Desktop icon should be created.
2. Click **Next** to continue.

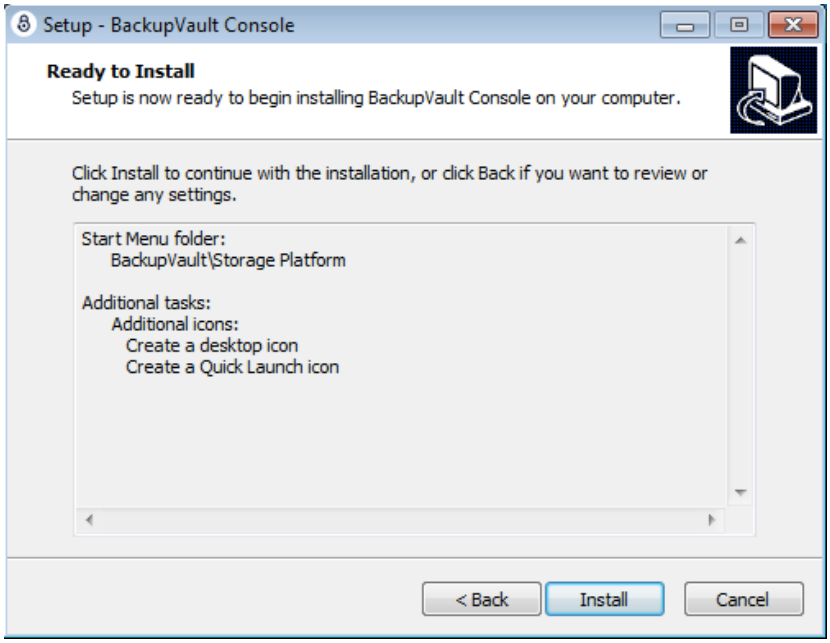


***Note**: A Desktop icon can also be pinned to the Start bar after the installation.*

Step 5 of 6: Begin the installation

To begin the installation:

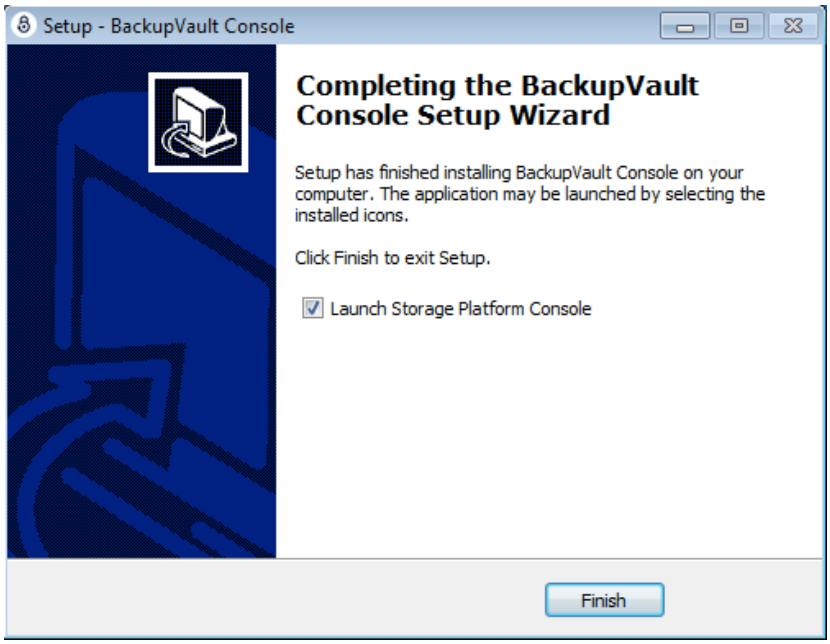
Click **Install**.



Step 6 of 6: Close the wizard

To close the wizard:

1. Ensure that the **Launch Storage Platform Console** check box is selected.
2. Click **Finish**.



4. Connection

Once the Storage Platform Console is installed on a computer, you can open the Graphical User Interface (GUI) and connect to a Storage Platform (via the AccountServer) or directly to a MirrorServer. You can access the GUI via the:

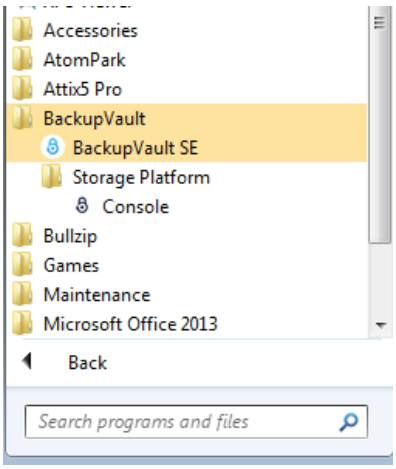
- **Start** menu
- Desktop

***Note**: Whether Desktop shortcut is available depends on the option selected during the installation process (see Step 4 of 6: Select additional tasks in Chapter 3, "Installation").*

Opening the GUI

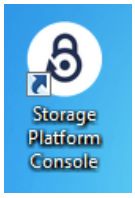
To open the SP Console GUI from the Start menu:

Simply type the word "Console" while in the Start menu.



To open the SP Console from the Desktop:

Double-click the **Storage Platform Console** icon.

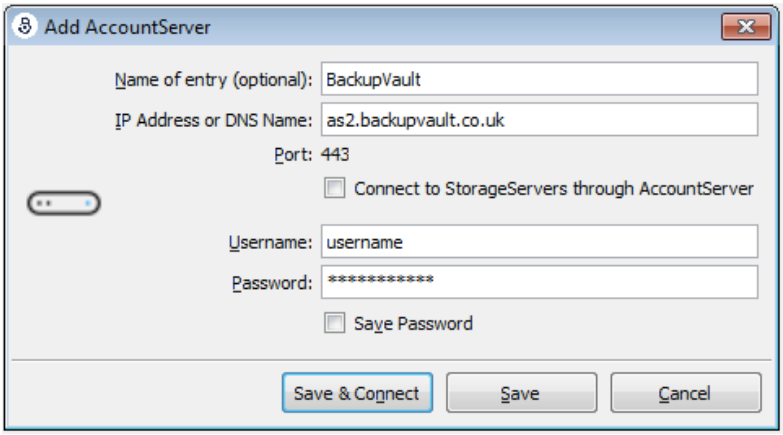


Connecting to a Storage Platform

You can use the SP Console to connect to the Storage Platform via the AccountServer. This ensures that you have access to all the rights and permissions assigned to your Access user role. For more information, see Chapter 9, “User Access Management”.

To connect to a Storage Platform for the first time:

1. When opening the SP Console for the first time, an **Add AccountServer** dialog box appears, enabling you to add the details of the AccountServer to connect to. Type the necessary information in the boxes provided.
2. Select the **Save Password** check box if you wish the SP Console to pre-populate the **Password** box for future connections.
3. Click **Save and Connect** to save the connection details for future use and connect to the AccountServer.



***Note**: The **Save** button allows you to add multiple AccountServers to the connection list without having to connect to each AccountServer.*

Once a connection is established, the SP Console management interface appears, displaying all Backup Account Groups created on the Storage Platform and a host of related management options. For more information on the options available, see “SP Console interface” later in this chapter.

5. Graphical User Interface (GUI)

You can open the Graphical User Interface using the:

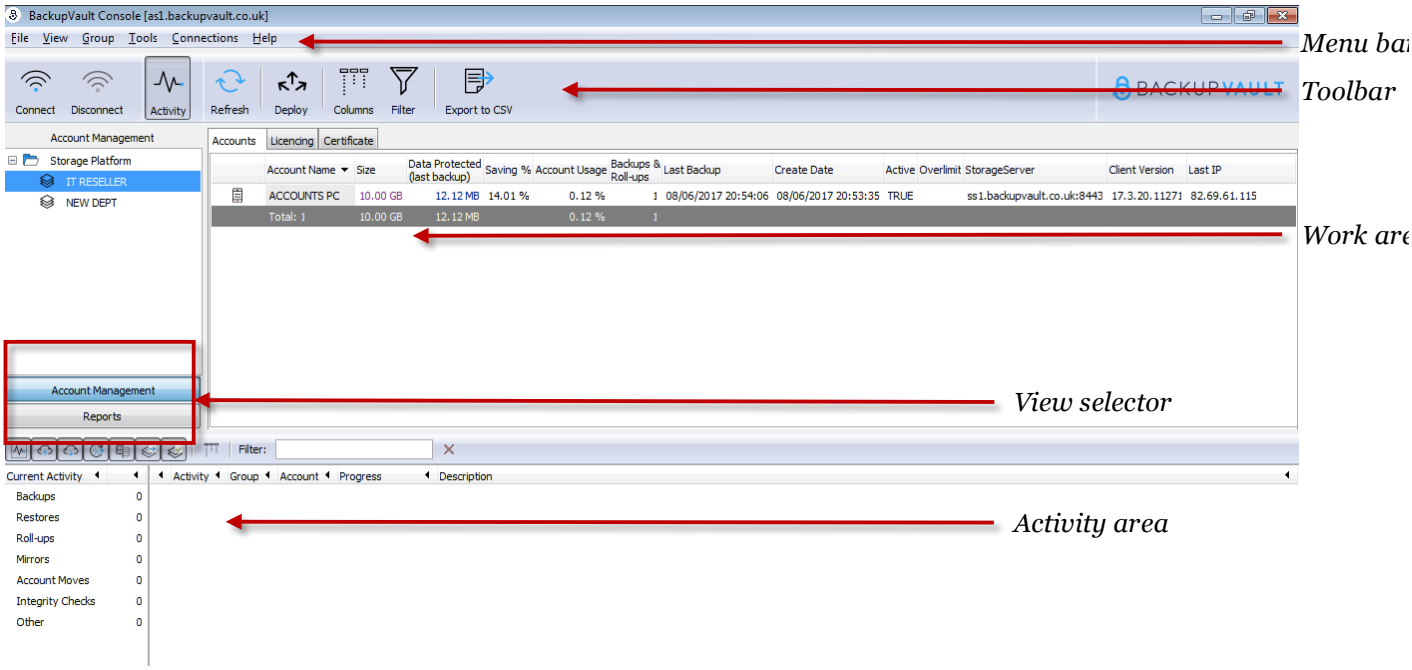
- SP Console **Start** menu item;
- SP Console Desktop icon or

***Note**: Whether a Desktop shortcut is available depends on the option selected during the installation process (see Step 4 of 6: Select additional tasks in Chapter 3, "Installation").*

For more information on opening the GUI, see Chapter 4, "Connection".

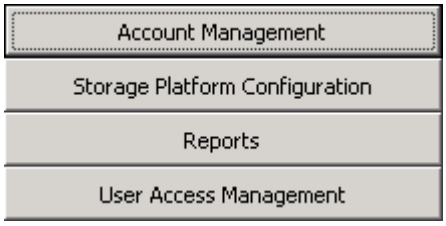
SP Console interface

SP Console features and functions are grouped in an easy-to-use layout:



View selector

The view selector enables you to select the SP Console view you wish to work in by clicking the appropriate button.



There are four views available to the admin user.

***Note**: The views available depend on the user access rights assigned to you by your Backup Administrator. Admin user rights will grant you access to all the views described below. For more information on user permissions, see Chapter 9, "User Access Management".*

SP Console views

Account Management view

Click the **Account Management** button in the view selector to manage Collections, Backup Groups, Backup Accounts, and licensing.

Storage Platform Configuration view

Click the **Storage Platform Configuration** button in the view selector to configure the AccountServer, Storage Pool(s) and StorageServer(s) as well as any MirrorServers and/or Slave AccountServers that form part of your backup environment.

Reports view

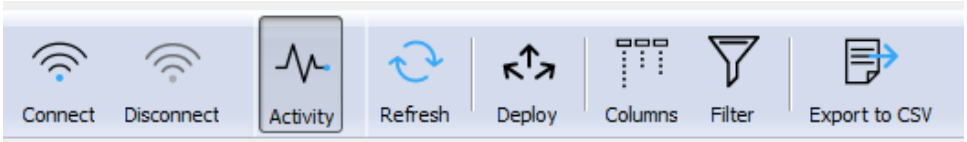
Click the **Reports** button in the view selector to manage Standard and Enterprise Reports (if licensed).

User Access Management view

Click the **User Access Management** button in the view selector to configure Storage Platform user access permissions.

***Note**: Only the functions and permissions enabled by the Backup Administrator will be available to the user logging in with an audit trail logged. For more information on user permissions, see Chapter 9, "User Access Management".*

Menu bar and toolbar buttons



Menus available in all views

Five menus always display on the menu bar, regardless of the view being worked in:

- File
- View
- Group
- Tools
- Connections
- Help

The following tables provide descriptions of the options available in each menu and screenshots of buttons where applicable.

File menu:

Options	Description	Button
Exit	Click **Exit** to disconnect from the SP and close the SP Console.	Exit

View menu:

Use the **View** menu to switch between different views and show or hide the Activity and Diagnostics areas.

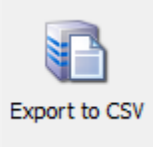
***Note**: For detailed information on each of the views and areas, see Chapters 5 - 8 as well as "Activity area" and "Diagnostics area" later in this chapter.*

Options	Description	Button
Account Management	Click **Account Management** to switch to the Account Management view.	Account Management
Storage Platform Configuration	Click **Storage Platform Configuration** to switch to the Storage Platform Configuration view.	Storage Platform Configuration
Reports	Click **Reports** to switch to the Reports view.	Reports
User Access Management	Click **User Access Management** to switch to the User Access Management view.	User Access Management
Activity	Select **Activity** to show the Activity area. Deselect **Activity** to hide the area. For more information on the Activity display options, see "Activity area" later in this chapter.	Activity
Diagnostics	Select **Diagnostics** to show the Diagnostics area. Deselect **Diagnostics** to hide the area. For more information on the Diagnostics display options, see "Diagnostics" later in this chapter.	
Customise Columns	Click **Customise Columns** to access the list of columns available for display in the work area. All columns display by default. To hide any columns, clear the check boxes next to their column heading names.	Columns

Options	Description	Button
Filter Accounts	Click **Filter Accounts** to access the **Select Licences to Display in Groups** dialog box. You can use the options available to filter the Groups/Accounts that display based on the licences they possess. ***Note**: This option is only available when a Backup Group/Account is selected in the Account Management view.*	Filter

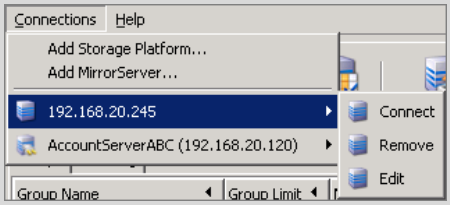
Tools menu:

Options	Description	Button
Options	Click **Options** to access the **Options** dialog box, which allows you to configure the SP connection, display, and fixed views settings. **Connection tab:** The **Connection** tab allows you to specify the Internet connection settings. Select the type of configuration to use, specify additional information if required, and then click **OK** to save your settings. **Display tab:** The **Display** tab provides a range of different display settings. • In the **Colour Options** area, you can configure the SP Console to provide a visual alert when certain parameters are met in the Account Management pane by displaying items in particular colours. These colours may be changed according to your preferences by clicking the relevant colour box, selecting a new colour, and then clicking **OK**. Colour options and default settings: ○ **Number of days since last backup** with 7 days and **red** as the default ○ **Percentage of account limit used** set to 90% and **orange** as the default. ○ **Disabled group** with **red** selected as the default ○ **Disabled account** with **grey** selected as the default ○ **User over limit** with **yellow** selected as the default ○ **Grid Lines** with a very light blue (#F0F0FF) selected as the default • In the **Plug-ins** area, you can choose how plug-in information displays in the Account Management view's **Plug-ins** column. The default selection, **Combo box**, displays the plug-in names in a drop-down list if more than one plug-in is installed. The **List** option displays plug-in names in a list format; one plug-in name per line. • In the **Main Toolbar** area, you can specify the preferred style of the toolbar. (E.g. Select **Icons Only** to remove the toolbar text.) **Fixed Views tab** The **Fixed Views** tab enables you to choose whether the **Activity** and	Options

Options	Description	Button
	Diagnostics areas must be displayed as additional views in the view selector or whether they should always be visible at the bottom of the Storage Platform Console. As with the main toolbar, you can change the style and icon size. You can also choose the layout of the two sections in the **Orientation** area. For more information on the Activity and Diagnostics areas, see “Activity area” and “Diagnostics area” later in this chapter.	
Export to CSV	Click **Export** to CSV to export the Backup Groups and Backup Accounts information on the **Accounts** tab to a CSV file. ***Note**: This option is only available when a Backup Group or Account is selected in the Account Management view.*	

Connections menu:

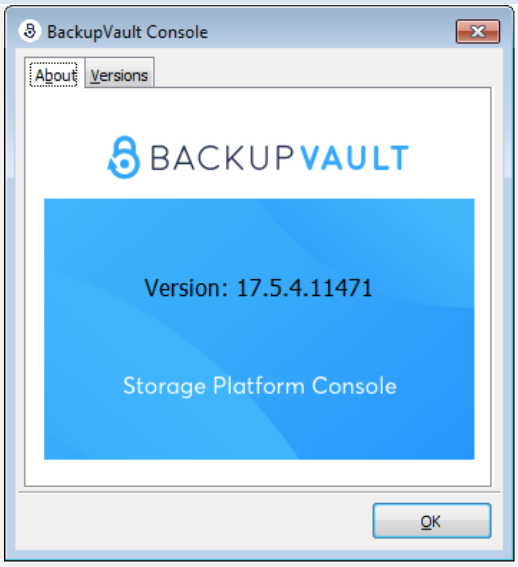
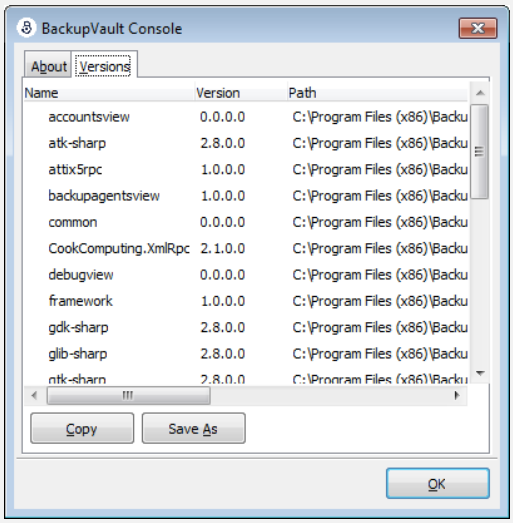
The Connections menu enables you to add, remove and edit AccountServers within the Storage Platform.

Options	Description	Button
Add Storage Platform	Click **Add Storage Platform** to add a Storage Platform connection to the SP Console.	
Add MirrorServer	Click **Add MirrorServer** to add a MirrorServer connection to the SP Console.	
<AccountServer>	The **Connections** menu lists all AccountServers that the SP Console has been configured to connect to. Point to the name of an AccountServer to access **Connect**, **Remove** and **Edit** options. For more information, see AccountServer in Chapter 7, “Storage Platform Configuration”.	

Help menu:

The Connections menu enables you to add, remove and edit AccountServers within the Storage Platform.

Options	Description
Product Help	Click **Product Help** to open the Storage Platform Console Product Help panel. This panel, which displays to the right of the work area (see “SP Console interface” earlier in this chapter), provides intuitive help related to the pane you are working in.
About	Click **About** to view the BackupVault Storage Platform Console splash screen and to access the **Versions** tab, which contains a list of all installed DLLs and their version numbers. **Splash screen:**

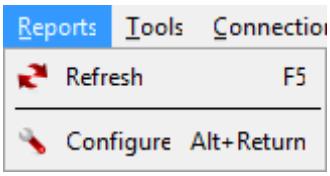
Options	Description
	 **Versions tab:**  **Copy button:** Click the **Copy** button to copy the contents of the tab to the Clipboard. You can then paste it into another text application such as Notepad. **Save As button:** Click the **Save As** button to save a text version of the **Versions** tab contents.
Manage Updates	After you have manually updated the AccountServer, you can use the **Manage Updates** option to update associated StorageServers and MirrorServers from the SP Console.

Options	Description
	Note: • *Slave ASs and shared MirrorServers cannot be selected to update. However, if a single SS/MS is selected, all Slave AccountServers/StorageServers/MirrorServers on the same server will be updated.* • *Only StorageServers and MirrorServers installed via the Storage Platform installer can be updated using this feature.* • *Only MirrorServers that are mirrored to using the "admin" account can be updated using this feature.* Click **Manage Updates** to launch the Storage Platform Version Report in a web browser. ***Note***: *A certificate error is expected at this point. It is safe to proceed.* The report details the latest version of the Storage Platform that is available (the version of the AccountServer that you manually updated) as well as the versions of all the StorageServers (grouped per Storage Pool) and MirrorServers linked to the AccountServer. It provides the option to update each component that is not on the latest version. The report also supplies a range of other information, such as the components' IP and port, online status, version and update status. **Report from AccountServer: WIN-SP4L3FMMTGO** **Latest version available: 8.15.604.9532** Selection (all/none) Account Servers Server / Ip and Port / Online / Version / Status / Selection (all/none) AccountServer / 0.0.0.0:443 / Online / 8.15.604.9532 / ✓ / ☐ SlaveAccountServer / Develop1:443 / Online / 8.15.603.14502 / Outdated / ☐ Storage Servers in Storage Server / Ip and Port / Online / Version / Status / Selection (all/none) StorageServer / develop1:8446 / Online / 8.15.603.14502 / Outdated / ☑ StorageServer / develop1:8447 / Online / 8.15.603.14502 / Outdated / ☑ StorageServer / WIN-SP4L3FMMTGO:8447 / Online / 8.15.604.9532 / ✓ / ☐ Storage Servers in Storage Pool 2 Server / Ip and Port / Online / Version / Status / Selection (all/none) StorageServer / develop1:8445 / Online / 8.15.603.14502 / Outdated / ☐ To update a StorageServer or MirrorServer, select it in the **Selection** column and click **Update**. You can cancel any updates by selecting the appropriate component and clicking **Cancel**. ***Note***: *While an update is in progress, the online status will change to offline for the duration of the upgrade.* The status column can show one of the following: • Check mark – Indicates that the component is using the latest version

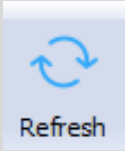
Options	Description
	• Queued – Indicates that the component is queued for update • Outdated – Indicates that there is a newer version available

Reports menu (Reports view)

In the Reports view, the **Reports** menu is available on the menu bar.

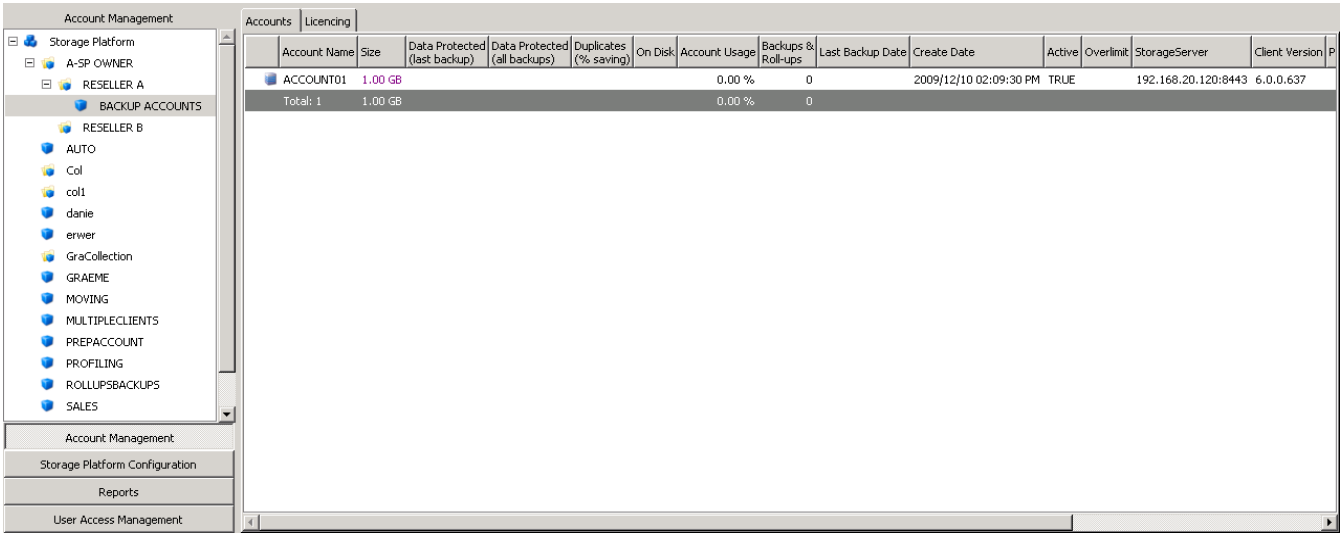


Reports menu

Options	Description	Toolbar Button
Refresh	Click **Refresh** to retrieve the latest figures from the AccountServer and update the information displayed in the work area accordingly.	
Configure	Click **Configure** to modify the general report properties or to configure a specific report's settings: Modifying general report properties: 1. In the Reports tree, select **Standard** or **Enterprise** and then click Configure. 2. In the **General Report Properties** dialog box that appears, configure the SMTP Settings, and then click **OK**. Enabling and configuring a specific report: 1. In the Reports tree, select a specific report (e.g. **Licence Report**) and then click Configure. 2. In the **Report Properties** dialog box that appears, select the **Enable this report** check box. 3. Modify/configure the report's E-mail settings and SyncSchedule using the options available. 4. Click **OK**.	

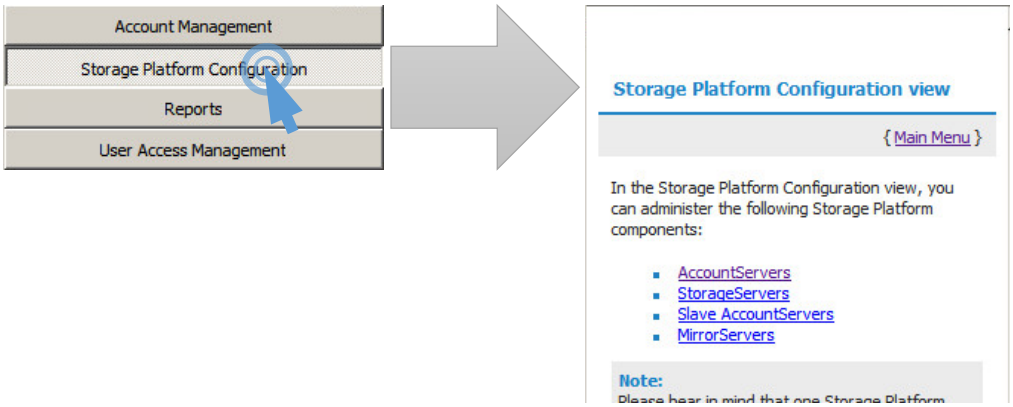
Work area

This area displays information relevant to the selected view. For more information on each view, see "View selector" earlier in this chapter.



Product Help

Access the SP Console Help by clicking **Product Help** on the **Help** menu.

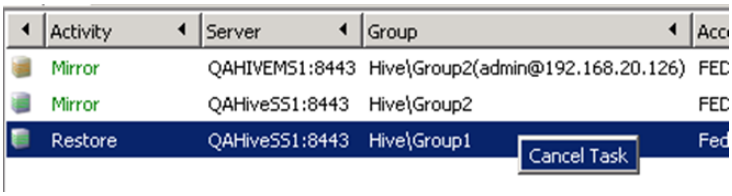


This Help pane displays information relating to the view open in the Console.

Activity area

The Activity area displays information relating to all current connections and activities on the Storage Platform. Information displayed:

- **Backups** (displayed in **Blue**)
- **Restores** (displayed in **Fuchsia**)
- **Roll-ups** (displayed in **Teal**)
- **Mirrors** (displayed in **Green**)
- Account Moves (displayed in Purple)
- Integrity Checks (displayed in Red)



Activity-related buttons are available on a small Activity toolbar:

Tip:

- *You can click the **Show All** button if all activities are not displayed.*
- *Columns can be sorted by clicking on the column headers.*
- *You can filter activities to only display a particular Backup Group(s) - Use the **Filter by Group** button on the toolbar (see below).*
- *While a process is being performed, a progress bar displays. You can right-click the progress bar and then click **Cancel** to stop the process.*

6. Account Management

You can use the SP Console to manage Backup Accounts and their connections to the Storage Platform. You can also place the Accounts into Backup Groups and Collections and deploy Client installation files to enable the creation of new Accounts within those Groups and Collections. See below for more information.

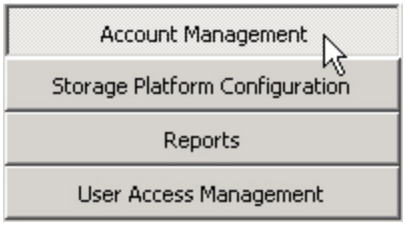
Account Management view

In the Account Management view, you can administer the following:

- Collections
- Backup Groups
- Backup Accounts
- Backup Client deployments
- Backup Clients (Remote Management)

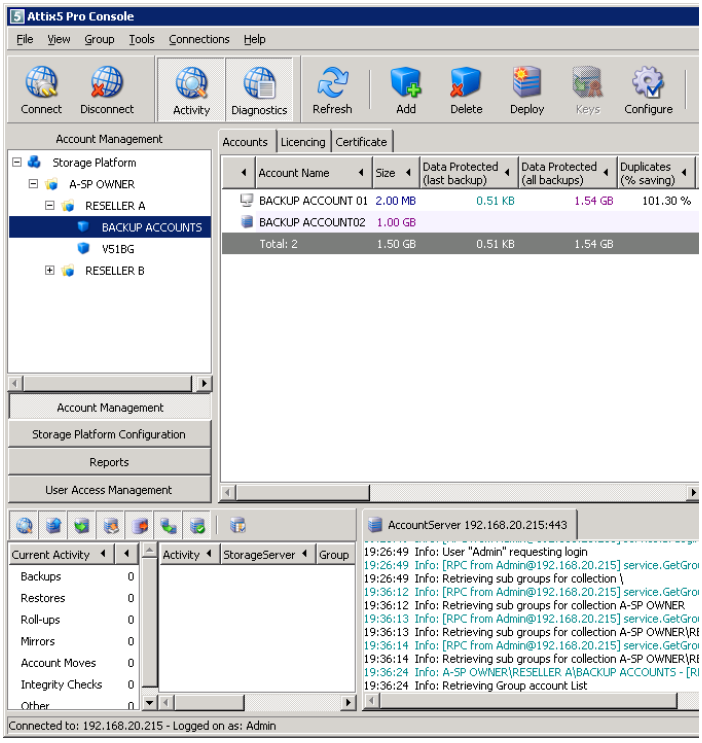
To access the Account Management view:

1. Open the SP Console and connect to the Storage Platform. [See Chapter 4, “Connection”.]
2. In the view selector on the left of the SP Console, click the **Account Management** button.



A summary of all Collections and Backup Groups configured on the Storage Platform will be displayed by default. This provides you with an overview of the default settings configured in each Collection/Backup Group.

When viewing this Backup Group summary, you can adjust the way that the information displays by adding/removing columns and filtering Backup Groups according to the licences they possess.

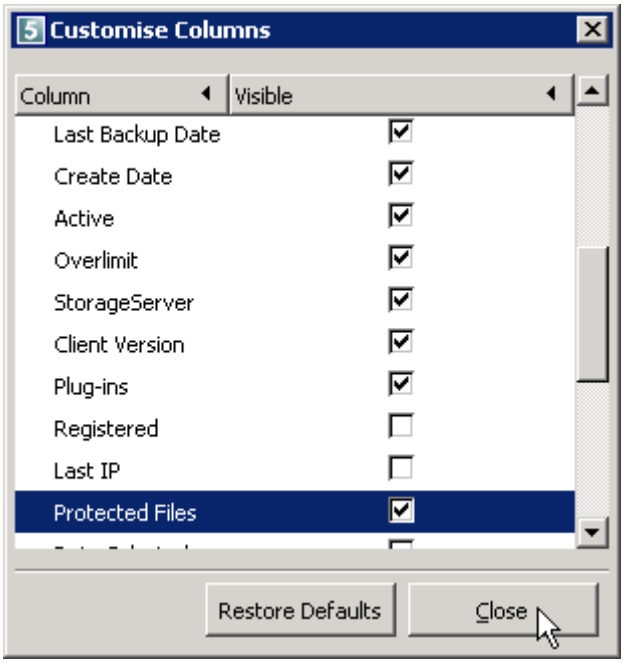


To add/remove columns:

1. On the **View** menu, click **Customise Columns**. Alternatively, click the **Customise Columns** button on the main toolbar.
2. In the **Customise Columns** dialog box that appears, specify which columns you wish to add/remove by selecting/clearing the check boxes next to the column names.
3. Click **Close**.

***Note**:*

- *You can click the **Restore Defaults** button to revert to the default column selections.*
- *The columns available depend on whether a Collection or Backup Group is selected.*



When a Collection is selected, the following columns are available by default in the Groups tab:

- **Group Name** – The name of the Backup Group.
- **Group Limit** – The storage space allocated to the Backup Group.
- **Max Accounts** – The maximum number of Backup Accounts the Backup Group can hold. If this is zero, the number of Backup Accounts is unlimited.
- **Roll-ups** – The number of roll-ups that are retained for Accounts in the Backup Group.
- **Expiry Date** – The date on which the Backup Group expires. If this column is empty, the Backup Group does not have an expiry date.
- **Mirror Enabled** – Mirroring is either enabled or disabled.
- **Enabled** – The Backup Group is either enabled or disabled.

- **Type** – The Backup Group is either a registered or evaluation group.
- **Updates** – Automatic updates are either on, off or on the SP default setting.
- **Profiling** – Profiling is either enabled or disabled.
- **HSM Enabled** – Hierarchical Storage Management is either enabled or disabled.
- **Default Account Size** – The default storage space allocated to Backup Accounts in the Backup Group.
- **Overspill (%)** – The percentage of the Account limit that Accounts in the Backup Group may exceed during the backup process.

When a Backup Group is selected, the following columns are available by default in the Accounts tab:

- **Account Name** – The name of the Backup Account.
- **Size** – The storage space allocated to the Backup Account.
- **Data Protected (last backup)** – The amount of uncompressed data protected by the last backup.
- **Data Protected (all backups)** – The amount of data protected by all backups. The sum of the uncompressed size of all the files (excluding unchanged files) in all backups. If there are multiple copies of the same file, they will all contribute to the final size. If a file is patched, the new uncompressed file size (resulting size) is used.
- **Saving** – Saving due to compression, patching, and Account-level de-duplication. It is the difference between Data Protected (all backups) and On Disk.
- **Saving %** – Saving as a percentage of Data Protected (all backups), i.e. Saving / Data Protected (all backups) * 100.
- **On Disk** – The amount of disk space used to store all backups on the StorageServer (excluding index files). This is generally less than the Data Protected columns due to compression, patching and SIS.
- **Account Usage** – The percentage of the Backup Account being used.
- **Backups & Roll-ups** – The number of backups and roll-ups that are available to restore from.
- **Last Backup** – The date and time at which the last backup started.
- **Create Date** – The date on which the Account was created.
- **Active** – The Backup Account is either active or disabled.
- **Overlimit** – The amount of data that the Backup Client attempted to back up. If the amount of data is within the allowed overspill, the backup will be successful; otherwise it will fail.
- **StorageServer** – The IP address of the StorageServer to which the Account backs up.
- **Client Version** – The version of the Backup Client associated with the Account.
- **Plug-ins** – Lists the plug-ins installed on the Backup Client. Depending on the settings, the plug-ins will either appear as a list with each plug-in on a separate line or in a drop-down list on a single line. If the column contains "…", select the Account and then click on the Plug-ins column to view the drop-down list.
- **GUID** – The Globally Unique Identifier of the Account.

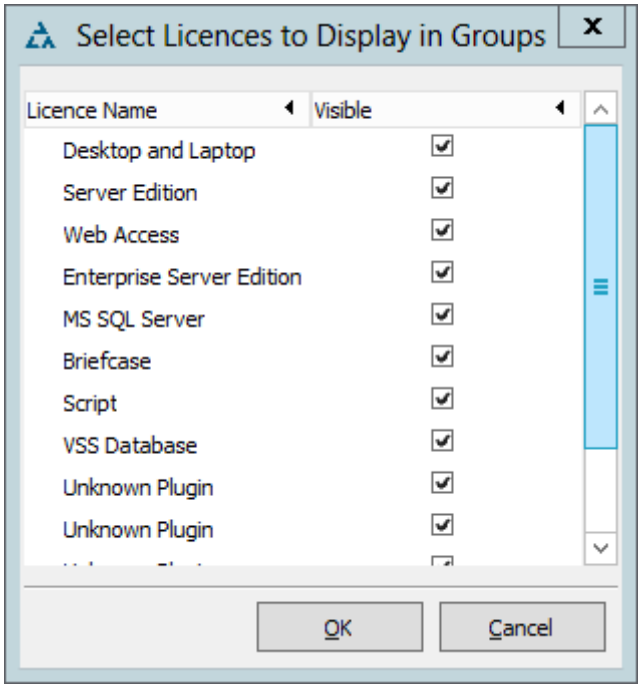
- **StorageServer IP Override** – If true, the Account is temporarily being directed to a different StorageServer (the IP of which is shown in the StorageServer column) from its usual one.
- **Restorable Data** – Restoring a full, uncompressed copy of each backup and adding up the size of all the data restored will result in this figure.

To filter Groups according to licences:

1. On the **View** menu, click **Filter Accounts**. Alternatively, click the **Filter** button on the main toolbar.

   ***Note**: This option is only available when viewing a Backup Group's **Accounts** tab. Click the Backup Group name in the Account Management tree and then ensure that the **Accounts** tab is selected in the work area (right-hand pane).*

2. In the **Select Licences to Display in Groups** dialog box that appears, all licences are selected by default. Clear all check boxes except those belonging to the licences you wish to filter by.
3. Click **OK**.



Account Management view icon legend

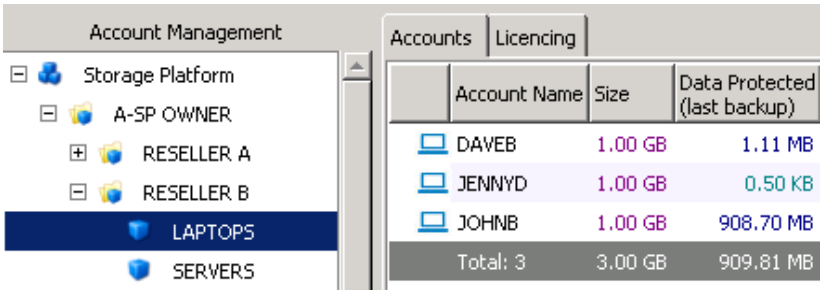
Icon	Location	Description
	Account Management tree	Storage Platform Collection (top level)
	Account Management tree	Collection
	Account Management tree	Group
	Account Management tree	Disabled Group
	Accounts tab	Server Edition Backup Client Account
	Accounts tab	Desktop & Laptop Edition Backup Client Account
	Accounts tab	Enterprise Server Edition Backup Client Account

For more information on configuring Backup Groups, see “Backup Groups” later in this chapter.

Collections

In the Account Management tree, you can create a Collection and then move or add Backup Groups to it. This is especially useful to administrators managing multiple Backup Groups that can be categorised.

***Example**: A Collection can be used to manage Groups representing different categories of Backup Accounts (e.g. departments, teams, resellers, Backup Account types):*



You can perform the following actions on Collections using the SP Console:

- Add/Delete Collections
- Configure Collection settings
- **Add/Delete/Configure Groups** (See *Adding and deleting Groups* later in this chapter.)

Adding and deleting Collections

To add a Collection:

1. In the Account Management view, expand the Account Management tree and select the node you wish to add the Collection to.
2. On the **Storage Platform** or **Collection** menu, click **Add Group or Collection**. Alternatively, click the **Add** button on the main toolbar or right-click the node and then click **Add Group or Collection** in the shortcut menu that appears.

   ***Note**: You can add a Collection to the **Storage Platform** Collection or to any other Collection but you cannot add a Collection to a Group.*

3. In the **Add New Group or Collection** dialog box that appears, select **Collection**.
4. In the **Name** box, type a display name for the Collection.

   ***Note**: The following characters are not supported in Collection names: "*", "/", "\", "|", "<", ">", "?", ":", "_", "&", "#", "@" and "!".*

5. In the **Storage Limit** box, enter storage limit for the Collection.

   ***Note**: Set the amount to "0" to use the maximum storage available in the parent Collection. However, note that the sum of the Storage Limits of Collections within a Collection, cannot exceed the Storage Limit set on the parent Collection.*

6. Click **OK**.

   ***Note**: After creating a Collection, you need to make licences available to any Backup Groups you may wish to add to it. To do this, you'll need to assign licences to the Collection. The Console will prompt you to do this after creating the Collection. For instructions, see "Account Management Licencing" later in this chapter.*

To delete a Collection:

1. In the Account Management tree, click the Collection name.
2. On the **Collection** menu, click **Delete Collection**. Alternatively, click the **Delete** button on the main toolbar or right-click the Collection name and then click **Delete Collection** on the shortcut menu that appears.
3. In the confirmation dialog box that appears, click **Yes**.

Configuring Collection settings

Settings configured for a Collection will determine the default settings assigned to all new Backup Groups added to that Collection.

To configure Collection settings:

1. In the **Account Management** view, expand the tree and then select the Collection name.
2. On the **Collection** menu, click **Configure**. Alternatively, click the **Configure** button on the toolbar or right-click the Collection name and then click **Configure** on the shortcut menu that appears.
3. In the **Configure Collection** dialog box that appears, configure the options as required, and then click **OK**.

Special considerations

All configuration options available for Backup Groups are available for Collections. (For more information on Backup Group configuration options, see “Configuring Group settings” later in this chapter.) However, certain values set on the Collection, will affect its Groups regardless:

Group Storage Limit: While most Collection settings affect only the default values of new Backup Groups, the Group Storage Limit (in the Admin tab) applies to the sum of all Backup Group limits within the Collection. Ensure that the Collection’s limit accommodates the limits applied to all the Backup Groups it will contain.

Allowed Storage Overspill: The percentage overspill on an underlying Group cannot be higher than the Allowed Storage Overspill percentage (set in the Admin tab) on the Collection.

Exporting the list of Accounts

You can generate a CSV file of all Backup Accounts belonging to a Backup Group. This file can then be opened in a spreadsheet editor.

To export a list of all Backup Accounts belonging to a Backup Group:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Accounts belong.
2. On the **Tools** menu, click **Export CSV**. Alternatively, click the **Export to CSV** button on the main toolbar.
3. In the **Choose export location** dialog box that appears, type a name for the CSV file in the **Name** box or accept the default name provided.
4. Use the **Save in folder** drop-down list and, if necessary, the **Browse for other folders** function to select a location in which to save the file or accept the default location.
5. Click **Save**.

A CSV file containing a list of all the Backup Accounts in the Group will be saved to the specified location and can be opened in any spreadsheet program.

Example:

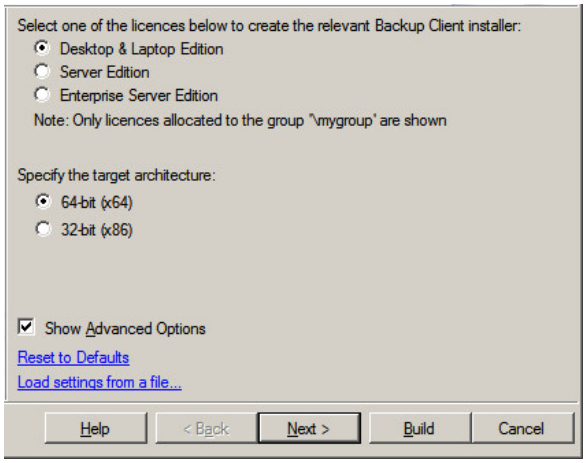
MANUAL.csv

	A	B	C	D	E	F	G	H
1	Account Name	Size	Data Protected	On Disk	Account Usage	Archives	Last Backup Date	Create Date
2	2007EX32VM	1024	0	0	0	0	N/A	2009/07/14
3	MACKIE	1024	0	0	0	1	2009/07/14 13:21	2009/07/14
4	QAWIN2003	1024	0	190948723	0	182	2009/07/13 10:15	2009/07/10
5	XPDLV51	1024	0	155189074	0	216	2009/07/10 18:09	2009/07/10
6								

MANUAL

Creating Backup Client deployments

You can create Backup Client deployments to enable users to create Backup Accounts belonging to a particular Backup Group. These deployments can contain pre-configured Backup Account Setup information. For more information, see “Deployment Wizard” later in this chapter.



Warning: *Certain antivirus programs may result in deployment failures. In such cases, you may need to disable antivirus scanning for the duration of the deployment process.*

Working with Group Certificates

As a Backup Administrator, you may find it useful to have access to the encryption keys used by Backup Accounts. You can gain access to these by requesting a Group Certificate from BackupVault and then uploading it to the Storage Platform using the SP Console.

Note:

- *BackupVault requires a formal letter of request from a Company Director before a Group Certificate will be issued.*
- *This functionality is only available to users with full SP Console Administrative rights. For more information on user permissions, see Chapter 9, “User Access Management”.*

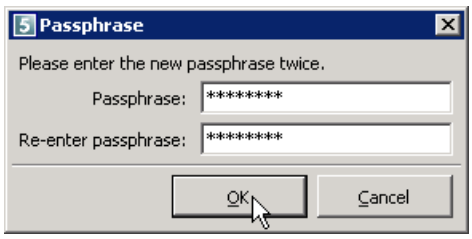
When you request a Group Certificate, a public and private key pair is generated. The public key is used to encrypt the users’ encryption key and only the private key can decrypt it. This key pair is stored on your machine, protected by a passphrase, which you will be prompted to choose when requesting the Group Certificate. The public key is then included in a Group Certificate signed by the BackupVault LicenceServer, and stored with the Group on the Storage Platform.

As users back up data, their encryption keys are encrypted with the public key that is stored in the Group Certificate. These encrypted versions of the keys are then stored on the Storage Platform. You can download the encrypted keys and decrypt them on your machine using an SP Console that has the matching Group Certificate private key. In order to do that, you will need to provide the passphrase that decrypts the private key stored on your machine. Since the keys can only be decrypted by the private key, it is only possible for the person in possession of the private key and the passphrase to view them.

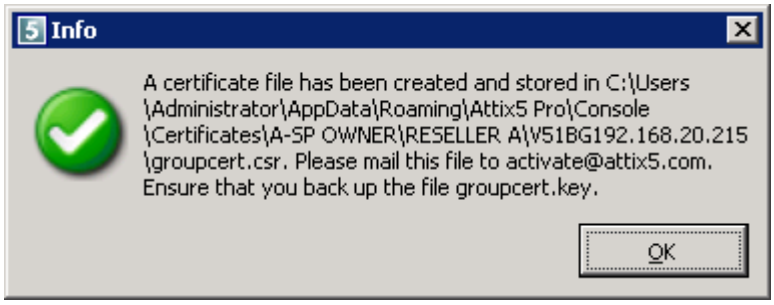
To request a Group Certificate:

1. In the Account Management tree, select the Group name.
2. On the **Group** menu, click **Certificate**. Alternatively, right-click the Group name and then click **Certificate** on the shortcut menu.
3. In the **Group Certificate** dialog box that appears, click **Request Certificate**.
4. In the Information box that appears, click **OK**.
5. In the **Passphrase** dialog box that appears, type a passphrase in the boxes provided, and then click **OK**.

***Warning**: Please remember your passphrase..*



6. An Information dialog box will indicate that a file called “groupcert.csr” has been saved in a particular location. Navigate to that location, zip the groupcert.csr file and email it to **backup@backupvault.co.uk**.



BackupVault will now send you a Group Certificate file called “groupcertsigned.crt”. Once received, you need to upload this file to the SP Console. See below.

To upload a Group Certificate to the SP Console:

1. Navigate to the certificate on the machine running the SP Console.

***Tip**: The default certificate location is located in:*
C:\Users\[Current user]\AppData\Roaming\BackupVault\Console\Certificates

2. The **Certificates** folder contains subfolders for each Collection and/or Backup Group on the Storage Platform. Paste the groupcertsigned.crt file into the relevant Group folder.

***Tip**: The format of the folder is GroupnameAccountServerIP.*

***Example**: With a Collection called **A-SP OWNER**, another Collection, **RESELLER A**, within it, and a Backup Group named **BACKUP ACCOUNTS** within that, the folder would be called **BACKUPACCOUNTS192.168.20.120** and the path would be: Certificates\A-SP OWNER\RESELLER A\BACKUPACCOUNTS192.168.20.120.*

3. In the SP Console, expand the Account Management tree and then select the Group name.
4. On the **Group** menu, click **Certificate**. Alternatively, right-click the Group name and then click **Certificate** on the shortcut menu.
5. In the **Group Certificate** dialog box that appears, click **Upload Group Certificate**.

***Note**: This process must be authorised by your Service Provider before a certificate will be generated.*

Each Backup Account user's encryption key will be captured when the Account performs a successful backup.

To confirm when a Group Certificate expires:

1. In the SP Console, expand the Account Management tree and then select the Group name.
2. In the work area, click the **Certificate** tab. The Group Certificate Information will be displayed in the top half of the tab with the expiry dates.

To reactivate the Group Certificate:

1. Locate the certificate files on the machine running the SP Console. (See ***Tips*** in "To upload a Group Certificate to the SP Console" above.)

   There are 3 files in the Backup Group's folder:

   - groupcert.csr
   - groupcert.key
   - groupcertsigned.crt
2. Zip the groupcert.csr file and email it to **backup@backupvault.co.uk**. In the message body, mention that this is a re-activation of an existing groupcert. A new groupcertsigned.crt file will be sent back (zipped).
3. Unzip the new file and replace the existing one.
4. Open the SP Console, right-click on the Backup Group in the Account Management tree and then click **Certificate**.
5. Click **Upload Group Certificate** and supply the passphrase.

The re-activated certificate will be uploaded and you can then view any encryption keys captured before the certificate expired.

Warning**: When an existing Group Certificate has expired, do not request a new one. Please zip the contents of the certificate folder and send it to **backup@backupvault.co.uk** with a request that it be renewed. **If you request a new group certificate, the current encryption keys will be lost.

After requesting a new group certificate, new key pairs are created that will not match the current groupcert loaded on the Storage Platform and the key capture will not work. In such an event, you need to delete the current groupcert on the AccountServer.

To delete the Group Certificate on the AccountServer:

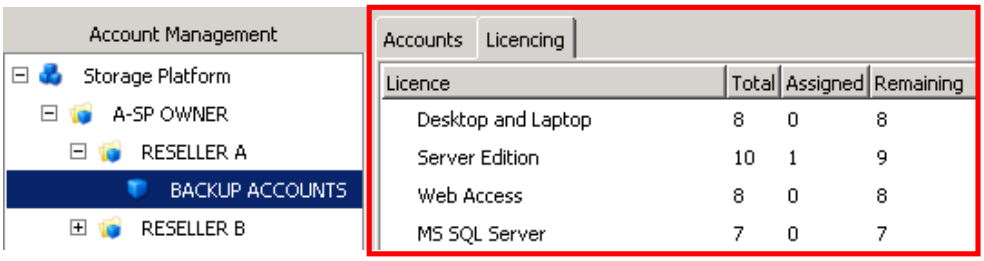
1. In the Account Management tree, select the Group name.
2. On the **Group** menu, click **Certificate**. Alternatively, right-click the Group name and then click **Certificate** on the shortcut menu.
3. In the **Group Certificate** dialog box that appears, click **Delete Certificate**.
4. In the Confirmation dialog box that appears, click **Yes**.

***Note**: You may wish to delete the Group Certificate if:*

- *you requested a new groupcert after the previous one expired (See Warning above)*
- *you cannot find the Certificate folder mentioned above*
- *you cannot recall the passphrase to access the keys*

Account Management licencing

A **Licencing** tab that displays in the work area when you select a Group or Collection in the Account Management tree provides you with a summary of all licences allocated to the Storage Platform.



***Note**: You can add/remove licences that belong to the pool of licences purchased from BackupVault. To purchase additional licences, please contact your software provider.*

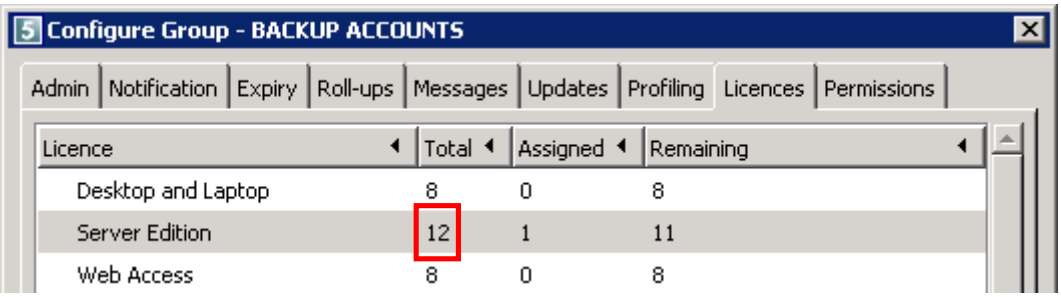
To add/remove licences:

1. In the Account Management tree, select the Group or Collection name.
2. On the **Group** or **Collection** menu, click **Configure**. Alternatively, click the **Configure** button on the main toolbar or right-click the Group or Collection name and then click **Configure** on the shortcut menu that appears.
3. In the **Configure Group** dialog box that appears, click the **Licences** tab.
4. In the Licences list, select the name of the licence you wish to add/remove.
5. Type the number of licences to add/remove in the **Number of Licences to add or remove** box.
6. Click the **Add**/**Remove** button.

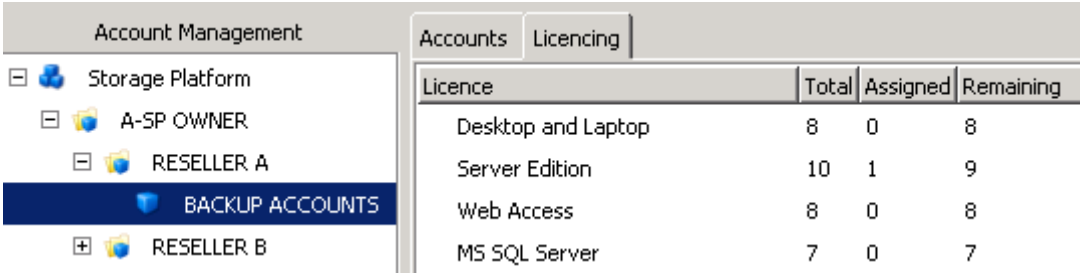
7. Click **OK**.

***Note**: When you add licences to a Group or Collection, the number of available licences in the parent Collection is updated accordingly.*

The number of licences assigned to the Backup Group will display in the **Total** column on the **Licences** tab in the **Configure Group** dialog box.



The number of licences will also display in the **Total** column on the **Licencing** tab in the Account Management view.



Once licences have been added to a Backup Group, a deployment MSI (installer) file can be created from it and used to install Backup Clients onto desktop, laptop or server machines. Those installations will enable users to create new Backup Accounts that belong to the Backup Group from which the MSI was deployed. For each Backup Account created, one licence is assigned and the number of remaining licences available for use displays in the **Remaining** column.

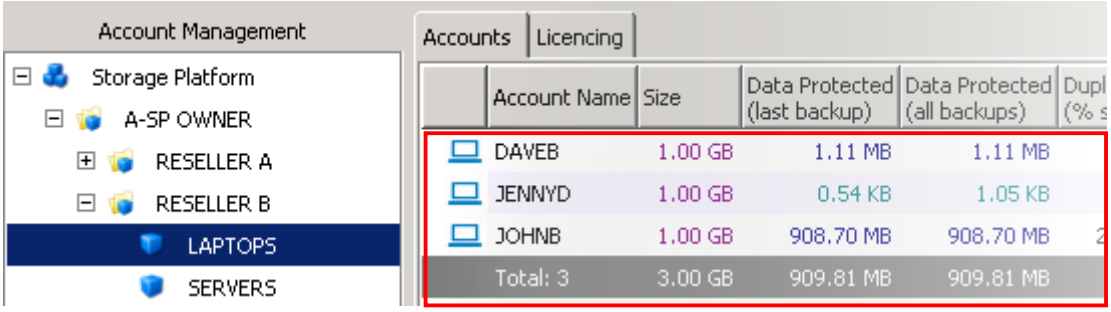
Access often-used reports

To access often-used Backup Group reports:

1. In the Account Management view, expand the Account Management tree and right-click the Backup Group whose reports you want to access.
2. Point to **Reports**, and then select the report that you want to access.

Backup Accounts

If a Backup Group is selected in the Account Management tree, a list of all the Backup Accounts belonging to that Group will display in the work area along with individual Account data such as the Account limit, last backup size, total backup size, etc.



***Note**: The Access User with Admin rights has full control of the Backup Accounts. For more information on Access Users, see "Permissions tab" earlier in this chapter.*

You can perform the following actions on Backup Accounts using the SP Console:

- Delete Account

  ***Note**: For information on creating Backup Accounts, please refer to the relevant Backup Client User Manual (Desktop & Laptop User Manual, Server Edition User Manual or Enterprise Server Edition User Manual).*

- Change Account size
- Enable/Disable Account
- Upgrade/Downgrade Account
- Rename Account
- Connect to Backup Client (See "Remote Management" later in this chapter)
- Change User Password
- Change Group (Move Account)
- Export Account list to CSV

The following additional and advanced options are also available when you right-click on a Backup Account.

- Import Backup Snapshot
- Export Restore Snapshot
- Initiate/Schedule Integrity Check
- Change the StorageServer it connects to
- Override StorageServer IP address
- Copy Account GUID to Clipboard
- Access often-used reports

***Tip**:*

- *Multiple Accounts in the same Backup Group can be highlighted by using the **Shift** or **Ctrl** keys and then selecting them with your mouse.*
- *The actions most commonly performed by administrators can be initiated using the buttons on the toolbar.*

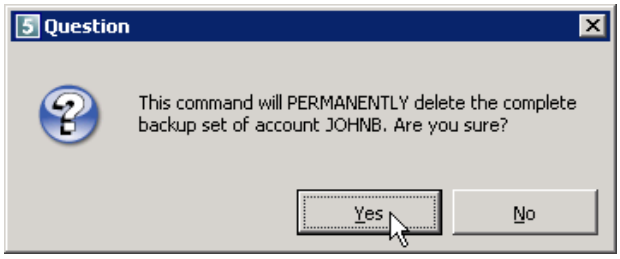
Adding and deleting Accounts

Adding Backup Accounts

Backup Accounts are created during the Account Wizard. For more information, please refer to the relevant Client User Manual (BackupVault Desktop & Laptop User Manual or Backup Edition Server Edition User Manual).

To delete an Account:

1. In the Account Management view, expand the Storage Platform tree and select the name of the Group to which the Account belongs.
2. In the work area, ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to delete.
4. On the **Accounts** menu, click **Delete**. Alternatively, click the **Delete** button on the main toolbar or right-click the Account name and then click **Delete** on the shortcut menu.
5. In the confirmation box that displays, click **Yes**.



***Warning**:*

- *This command will PERMANENTLY delete the complete set of backed up files belonging to the Backup Account. If unsure about whether or not to delete the Backup Account, please consider disabling the Backup Account instead. (See "Disabling Accounts" later in this chapter.)*
- *If the Backup Account is being mirrored, by default it will be deleted from the MirrorServer as soon as the delete command is issued.*

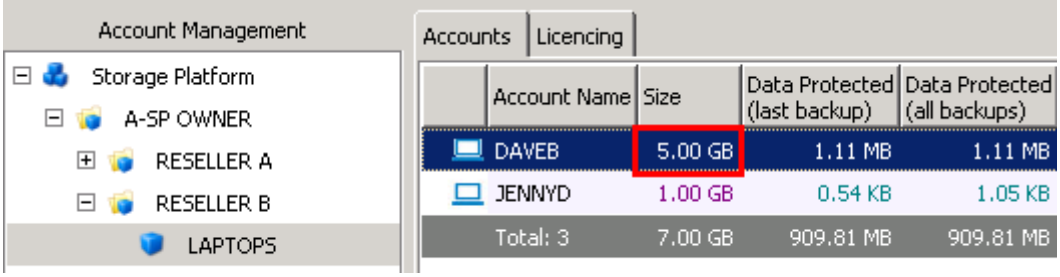
Changing an Account's size

As the Backup Administrator, you may wish to change the backup limit for Accounts. You can increase or decrease the disk space allowed for each Account's backups by changing the Account size in the Console.

To change the Account size:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. In the work area, ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to modify.
4. On the **Accounts** menu, click **Change Account Size**. Alternatively, click the **Size** button on the main toolbar or right-click the Account name and then click **Change Account Size** on the shortcut menu that appears.
5. In the **Change Account Size** dialog box that appears, type the new Account limit (in Gigabytes) in the **Enter a new size in GB** box, and then click **OK**.

The Account size limit will be updated on the Storage Platform and the new maximum value will display in the **Size** column on the **Accounts** tab.



Enabling an Account

Using the SP Console, you can enable an Account that was previously disabled, thereby allowing it to back up to the Storage Platform again.

***Note**:*

- *A Backup Account could have been disabled as a result of manual disabling (see below) or an action such as a Backup Snapshot (see Importing a Backup Snapshot later in this chapter).*
- *A Backup Snapshot created using the ESE Backup Client will only result in the Backup Account being locked for further backups. File/folder restores can still be performed as usual.*

To enable an Account:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. In the work area, ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to enable.
4. On the **Accounts** menu, click **Enable**. Alternatively, click the **Enable** button on the main toolbar or right-click the Account name and then click **Enable** on the shortcut menu that appears.

The Account will be enabled and a message logged in the **Diagnostics** area:

192.168.20.120

```
15:51:36  Info: A-SP OWNER\RESELLER B\LAPTOPS - [RPC from Admin@192.168.20.215] group.UpdateUsersEnabled
15:51:36  Info: 1 Account enabled in group A-SP OWNER\RESELLER B\LAPTOPS
```

The user of this Backup Account will now be able to back up to the Storage Platform.

***Tip**: Enabled Accounts display as active on the **Accounts** tab. Disabled Accounts are greyed out.*

Accounts | Licencing

	Account Name	Size	Data Protected (last backup)	Data Protected (all backups)
	DAVEB	5.00 GB	1.11 MB	1.11 MB
	JENNYD	1.00 GB	0.54 KB	1.05 KB
	JOHNB	1.00 GB	908.70 MB	908.70 MB
	Total: 3	7.00 GB	909.81 MB	909.81 MB

Disabling an Account

Using the Console, you can disable an Account, preventing any further backups to the Storage Platform from that Account.

To disable an Account:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. In the work area, ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to disable.
4. On the **Accounts** menu, click **Disable**. Alternatively, click the **Disable** button on the main toolbar or right-click the Account name and then click **Disable** on the shortcut menu that appears.

The Account will be disabled and a message logged in the **Diagnostics** area:

192.168.20.120

```
15:52:25  Info: 1 Account disabled in group A-SP OWNER\RESELLER B\LAPTOPS
15:52:34  Info: A-SP OWNER\RESELLER B\LAPTOPS - [RPC from Admin@192.168.20.215] group.UpdateUsersEnabled
```

The user of this Backup Account will no longer be able to back up to the Storage Platform but you can enable the Account again at any time to allow further backups. For more information, see “Enabling an Account” above.

***Tip**: Disabled Accounts are greyed out on the **Accounts** tab.*

Accounts | Licencing

	Account Name	Size	Data Protected (last backup)	Data Protected (all backups)
	DAVEB	5.00 GB	1.11 MB	1.11 MB
	JENNYD	1.00 GB	0.54 KB	1.05 KB
	JOHNB	1.00 GB	908.70 MB	908.70 MB
	Total: 3	7.00 GB	909.81 MB	909.81 MB

Upgrading an Account

Using the SP Console, you can upgrade an Account to change its status from Evaluation to Registered.

Note:

- *In cases where Backup Accounts have been created within Evaluation Groups, they will automatically be created as Evaluation Accounts. If the Group is later upgraded to "Registered", its Accounts will remain "Evaluation" Accounts until manually upgraded as described below.*
- *Once an Account is registered, it is advised to move it out of the Evaluation Group and into a Registered one.*
- *Evaluation Accounts display an advertisement in the form of a banner at the bottom of the application window. This banner cannot be closed by the user.*

To upgrade an Account:

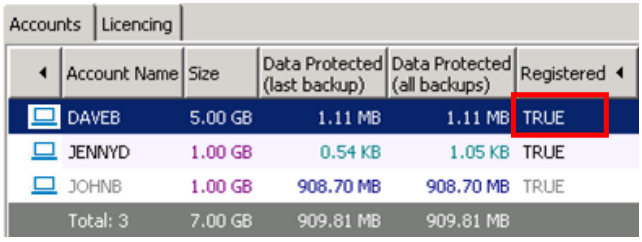
1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. In the work area, ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to upgrade.
4. On the **Account** menu, click **Upgrade**. Alternatively, click the **Upgrade** button on the main toolbar or right-click the Account name and then click **Upgrade** on the shortcut menu that appears.
5. Click the button on the toolbar. Alternatively, on the **Accounts** menu, click **Upgrade**.

The Account status will be changed from Evaluation to Registered and a record of the change will display in the **Diagnostics** area:

192.168.20.120

```
17:02:10  Info: A-SP OWNER\RESELLER B\LAPTOPS - [RPC from Admin@192.168.20.215] group.UpdateUsersType
17:02:10  Info: Type changed for account DAVEB in group A-SP OWNER\RESELLER B\LAPTOPS
```

Tip: *The Account status will display on the* ***Accounts*** *tab's* ***Registered*** *column:*



Account Name	Size	Data Protected (last backup)	Data Protected (all backups)	Registered
DAVEB	5.00 GB	1.11 MB	1.11 MB	TRUE
JENNYD	1.00 GB	0.54 KB	1.05 KB	TRUE
JOHNB	1.00 GB	908.70 MB	908.70 MB	TRUE
Total: 3	7.00 GB	909.81 MB	909.81 MB	

To change a Backup Account's status from Registered to Evaluation, you need to *Downgrade* the Account.

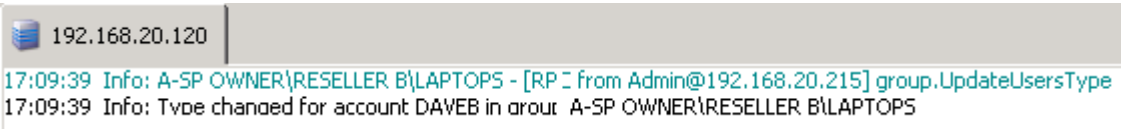
Downgrading an Account

Using the SP Console, you can downgrade an Account to change its status from Registered to Evaluation.

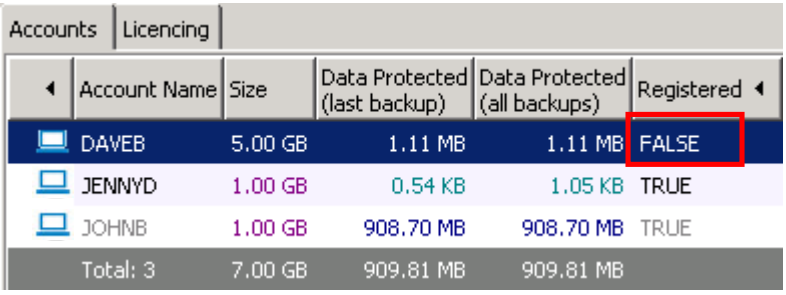
To downgrade an Account:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. Ensure that the **Accounts** tab is selected.
3. Select the name of the Account you wish to downgrade.
4. Click the **Downgrade** button on the toolbar. Alternatively, on the **Accounts** menu, click **Downgrade**.

The Backup Account status will be changed from Registered to Evaluation and a record of the change displays in the **Diagnostics** area:



The Account status will display on the **Accounts** tab's **Registered** column:



Account Name	Size	Data Protected (last backup)	Data Protected (all backups)	Registered
DAVEB	5.00 GB	1.11 MB	1.11 MB	FALSE
JENNYD	1.00 GB	0.54 KB	1.05 KB	TRUE
JOHNB	1.00 GB	908.70 MB	908.70 MB	TRUE
Total: 3	7.00 GB	909.81 MB	909.81 MB	

Tip:

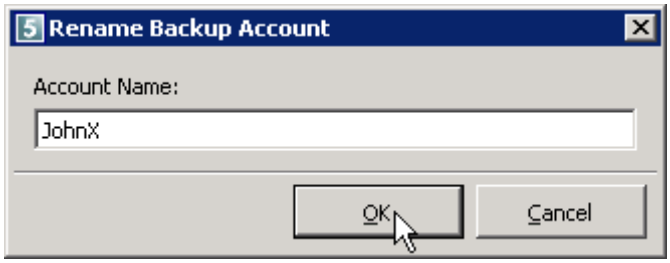
- *If you do not see the **Registered** column on the **Accounts** tab, click **Customise Columns** on the **View** menu or click the Columns button on the main toolbar, select the **Registered** check box, and then click **Close**.*
- *You can then move the column to the position that best suits your management needs by clicking the column heading and using a drag-and-drop operation.*

Renaming a Backup Account

You can rename a Backup Account using the SP Console.

To rename a Backup Account:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Account you wish to rename.
4. On the **Account** menu, click **Rename**. Alternatively, right-click the Account name and then click **Rename** in the shortcut menu that appears.
5. In the **Rename Backup Account** dialog box that appears, type a new name for the Account.
6. Click **OK**.



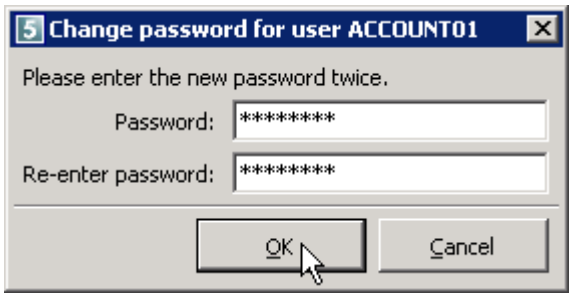
At the next backup or restore, the Client will adopt the new name and update its details accordingly.

Changing a user password

You can change the user password associated with a Backup Account using the SP Console.

To change a user password:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Account you wish to change the user password for.
4. On the **Account** menu, click **Change user password**. Alternatively, right-click the Account name and then click **Change user password** on the shortcut menu.
5. In the **Change password for user <username>** dialog box that appears, type the new password in the **Password** box and then re-type it in the **Re-enter password** box.
6. Click **OK**.



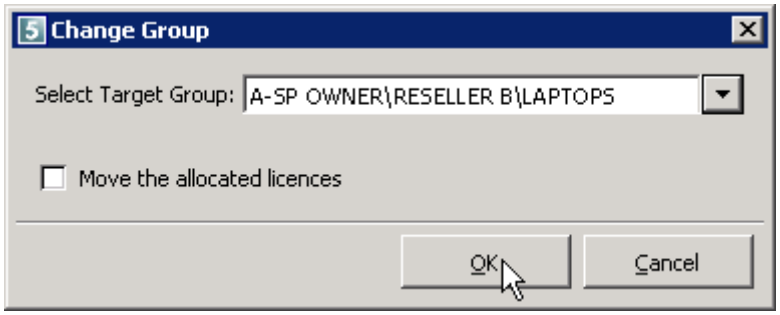
Once the Backup Client user changes the password on the client-side, he/she will be able to back up data to the Storage Platform using the new password.

Changing the Backup Group (moving a Backup Account)

Using the SP Console, you can move a Backup Account from one Backup Group to another.

To change the Backup Group that a Backup Account belongs to:

1. In the Account Management view, expand the Account Management tree and select the name of the Backup Group to which the Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Backup Account you wish to move.
4. On the **Account** menu, click **Change Group**. Alternatively, right-click the Backup Account name and then click **Change Group** on the shortcut menu.
5. In the **Change Group** box that appears, use the **Select Target Group** arrow to select a new Backup Group name.
6. Select the **Move the allocated licences** check box to ensure that all associated licences are moved with the Account.
7. Click **OK**.



The Backup Account will disappear from the Group's Accounts list and be listed under the new Backup Group name in the Account Management tree. Select the name of the new destination Backup Group in the Account Management tree to view and continue managing the Backup Account.

***Note**: If you move the Backup Account from a Backup Group configured for mirroring to a Group that is not configured for mirroring, the Account will be deleted from the MirrorServer after the retention period set on the MirrorServer has elapsed (the default is 24 hours).*

If you move the Backup Account from a Backup Group on a StorageServer that is configured for

mirroring to a Group on another StorageServer (also configured for mirroring but to a different MirrorServer), the Backup Account will be moved between MirrorServers automatically. No manual MirrorServer configuration is necessary.

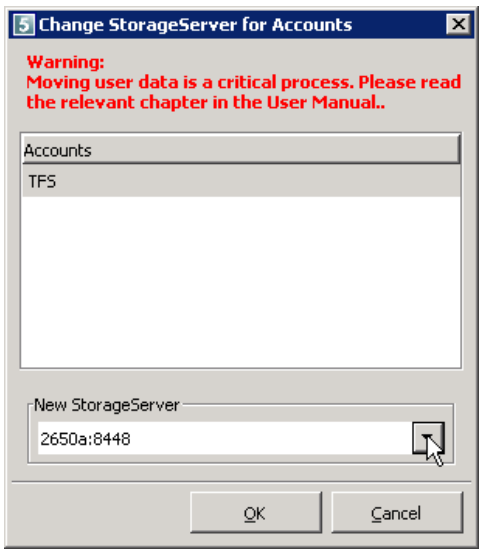
Changing the StorageServer

Using the SP Console, you can move a Backup Account from one StorageServer to another.

***Note**: You will only see this option on your **Account** menu if you manage more than one StorageServer with the SP Console.*

***Warning**: When moving a Backup Account between StorageServers, the major and minor versions of the destination StorageServer must be the same as the source StorageServer, or later. If this is not the case, the move will fail with an appropriate message appearing in the StorageServer log. For example: In V6.2.3, 6 is the major version and 2 is the minor version. Therefore, if the source StorageServer is V6.2.3, the Backup Account can be moved to a V6.2.2 StorageServer, but not to a V6.1.1 StorageServer.*

To move a Backup Account to another StorageServer:



1. In the Account Management view, expand the Account Management tree and select the name of the Backup Group to which the Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Backup Account you wish to move.
4. On the **Account** menu, click **Change StorageServer**. Alternatively, right-click the Backup Account name and then click **Change StorageServer** on the shortcut menu.
5. In the **Change StorageServer** box that appears, select a Backup Account in the Accounts list.
6. Use the **New StorageServer** arrow to select a destination StorageServer.
7. Click **OK**.

The Backup Account will be moved to the new StorageServer.

Advanced actions

Advanced actions can be accessed from the menu bar or by right-clicking on an Account name and then pointing to **Advanced** in the shortcut menu.

Importing a Backup Snapshot

The Backup Snapshot feature in DL, SE and ESE Backup Clients enables users to create a backup of all selected files on the Client for transferral to the Storage Platform using a removable storage device.

***Tip**: This feature is useful when the amount of data to be transferred to the Storage Platform is too great to transfer over the Internet.*

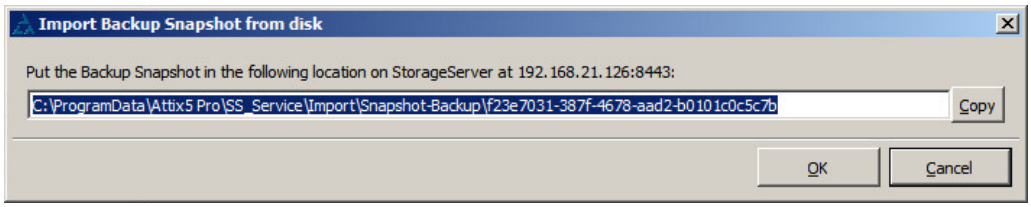
After creating a Backup Snapshot using a Backup Client (see the relevant Backup Client User Manual), you can import the data to a StorageServer using the SP Console as described below.

***Note**: The Backup Account will remain disabled until the Backup Snapshot has been imported. This means that backups cannot be performed until the account is enabled again.*

***Tip**: If for some reason the Snapshot from an ESE Backup Client will not be imported, the Backup Account can be enabled manually.*

To import a Backup Snapshot:

1. In the Account Management view, expand the Account Management tree and then select the name of the Group to which the Client's Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Account that you wish to import the Snapshot for.
4. On the **Account** menu, point to **Advanced**, and then click **Import Backup Snapshot**. Alternatively, right-click the Account name, point to **Advanced**, and then click **Import Backup Snapshot** on the shortcut menu.
5. In the **Import Backup Snapshot from disk** dialog box that displays, click the **Copy** button to copy the StorageServer location path.



***Note**: Alternatively for steps 5-7, if for some reason it is not possible to open the location path in a Windows Explorer window, the entire GUID-labelled folder on the storage device can be transferred to the appropriate folder on the StorageServer:*

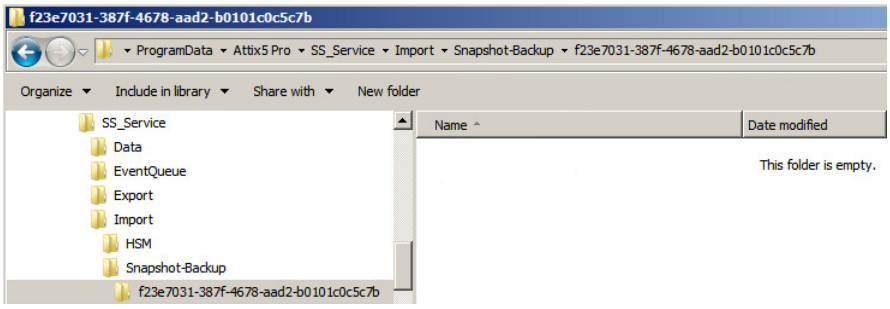
%ProgramData%\<product folder>\<SS_Service>\Import\Snapshot-Backup

For example:

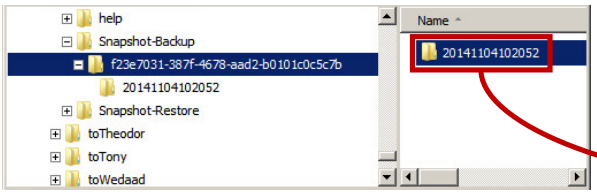
*E:\Snapshot-Backup**f23e7031-387f-4678-aad2-b0101c0c5c7b** is transferred to*

*C:\ProgramData\Attix5 Pro\SS_Service\Import**Snapshot-Backup****f23e7031-387f-4678-aad2-b0101c0c5c7b***

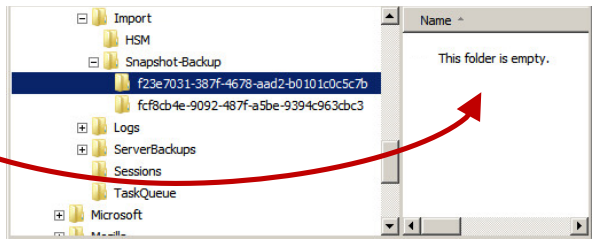
6. Access the StorageServer on which the Account resides, open Windows Explorer, paste the location path into the Address bar, and then press **Enter**.



7. Transfer the dated Snapshot folder (e.g. 20100506xxxxxx, created on the 06th May 2010) within the GUID-labelled folder to the destination folder of the same GUID on the StorageServer. (As per the location provided in step 6.)



Backup Snapshot on storage device



StorageServer destination

8. Once the Snapshot data is in the correct location, click **OK** in the SP Console's **Import Backup Snapshot from disk** dialog box.

9. In the **Info** dialog box that appears, click **OK**. When the process has completed, it will be logged in the StorageServer's Diagnostics window, for example:.

   16:13:34 Info: A-SP OWNER\RESELLER A\SERVERS\SERVER01 - Backup Snapshot Import completed successfully.

The StorageServer has now been updated with the latest Backup Client data and the Backup Account will be re-enabled automatically. The Backup Client user can now continue backing up data as usual.

Exporting a Restore Snapshot (Disaster Recovery)

The Restore Snapshot feature enables you to take data from the Storage Platform and make it available to the Backup Client for restores using a mobile storage device.

***Tip**: This feature is useful when the amount of data to be transferred to the Backup Client is too great to transfer over the Internet within a limited time frame (e.g. in a Disaster Recovery scenario).*

To export a Restore Snapshot to a mobile storage device:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Client's Backup Account belongs.

2. Ensure that the **Accounts** tab is selected in the work area.

3. In the Accounts list, select the name of the Account for which you wish to export a Restore Snapshot.

4. On the **Accounts** menu, point to **Advanced**, and then click **Export Restore Snapshot**. Alternatively, right-click the Account name, point to **Advanced,** and then click **Export Restore Snapshot** on the shortcut menu that appears.
5. In the **Snapshot recovery from Disk** dialog box that appears, select a backup to restore using the **Backup to restore** arrow.
6. If the encryption key is not currently available, an **Encryption key** box will prompt you for it.

***Note**: To enable the Console to export the Restore Snapshot upon clicking OK, as described in step 8 below, enter the key and then proceed to the next step. Leaving this box blank will result in the Restore Snapshot being queued until the Backup Client performs its next backup.*

***Tip**: If the key is currently available, the **Encryption key** box will NOT be displayed, and the snapshot export will be performed upon clicking **OK** in step 8 below.*

7. Click the **Copy** button to copy the Restore Snapshot location to the Clipboard or make a note of the Restore Snapshot location to refer to later.
8. Click **OK**. Once complete, the StorageServer Diagnostics window will log a "Snapshot Restore completed successfully" message.

***Warning**: Ensure that your Snapshot location has enough free space.*

9. On the StorageServer machine, open Windows Explorer, paste the Restore Snapshot location into the Address bar (or navigate to it), and then press **Enter**.
10. Copy the Snapshot and paste it into the desired location on your mobile storage device.

You can now transfer the snapshot data from the storage device or server to another machine and import the backup information to the Backup Client, enabling the user to restore any/all files via the **Restore** tab. For more information, please refer to the relevant Backup Client User Manual.

***Tip**: You can also restore data using the SP Console's Remote Management feature. See "Remote Management" later in this chapter.*

Preparing a Recovery Server for a Snapshot

Another option for recovery to site is to use a dedicated StorageServer, acting as a Recovery StorageServer, which can be made locally available to the site (especially useful if the site has experienced major data loss over multiple Backup Accounts). This can be done by recovering from a typical MirrorServer that hosts the same Backup Account data required for such a disaster recovery. For more information and assistance with the process, please contact BackupVault.

Importing HSM data

To make a Backup Account's HSM data available for restore via the Backup Client, you need to import the relevant HSM data.

***Note**:*

- *HSM data consists of roll-ups that have been archived before being deleted from the Storage Platform. For more information on roll-ups, see Roll-ups tab in the Backup Groups section of Chapter 6, "Account Management".)*
- *The ESE Backup Client can import HSM data directly without it having been imported through the Storage Platform. Follow the "Restore Snapshots" procedure in the ESE Backup Client manual to achieve this.*

To import a Backup Account's HSM data:

1. Navigate to the StorageServer's HSM Export folder.

   ***Tip**: The location is defined on the **HSM** tab of the **Configure StorageServer** dialog box. See HSM tab in Chapter 7, "Storage Platform Configuration".*

2. Note the name of the Backup Group to which the Backup Account belongs and then open the matching folder in the HSM location.

   ***Tip**: The matching HSM folder names follow the syntax: **GroupName_AccountName**, e.g. **ALLSERVERS_SERVER6**.*

3. HSM folders are named according to the last backup date contained in the roll-up. Open the folder containing the roll-ups you wish to make available to the Client for restoring.

   ***Tip**: Roll-up folders names follow the syntax: **YearMonthDayHourMinuteSecond**. E.g. **20100614115403** (which represents 14th June 2010, 11:54:03).*

4. In the archived roll-up folder, you'll find either an HSM folder (with a folder name that matches that of the Backup Account GUID) or a single HSM Tar file.
   a. If a full HSM folder is available, copy it to the Clipboard (the folder name should match that of the Backup Account GUID.)
   b. If a single Tar file is available, you first need to untar the file and then copy the untarred files and folders to the Clipboard.

5. Paste the HSM data (GUID folder name) into the StorageServer's HSM Import folder.

   ***Tip**:*

   - *The **Import** folder location is defined on the **HSM** tab of the **Configure StorageServer** dialog box. See HSM tab in Chapter 7, "Storage Platform Configuration".*
   - *To import multiple HSM archives, paste the HSM data (GUID folder name) for each archive that you want to import into the StorageServer's HSM Import folder. If you are informed that the folder already exists and asked whether you want to merge the folders, click **Yes**.*

The HSM data should now be available for restore from the Backup Client.

Initiating/Scheduling Integrity Checks

You can do an Integrity Check on a specific Backup Account, which is useful if you suspect that the data may be corrupt on the Storage Platform. During each monthly roll-up, should any data be corrupt, an automatic Integrity Check will occur to fix or retransmit corrupt data.

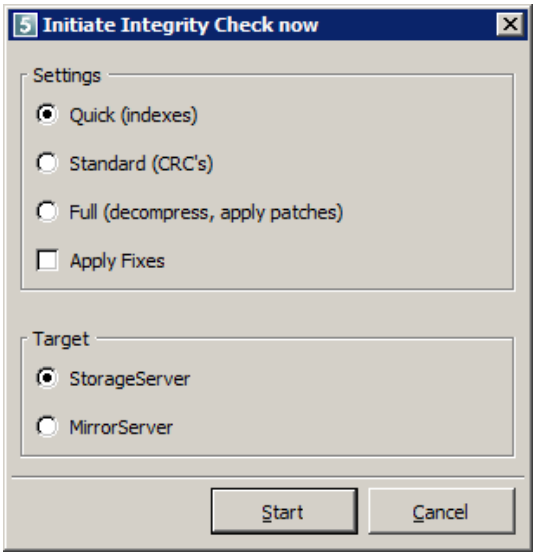
***Warning**:*

- *An Integrity Check may take some time to complete and may result in high processor usage.*
- *For ESE Backup Accounts - the Integrity Check with the "Apply Fixes" option set, will not run in the following instances:*
  - *A backup or restore process is in progress*
  - *A partial or incomplete backup exists that has not been finalised (Use the 'Purge Partial Backups' option in the SP Console before running the Integrity Check)*
  - *A StorageServer roll-up is in progress*

***Tip**: You can monitor the progress of an Integrity Check in the StorageServer Diagnostics window (at the bottom of the screen).*

You can initiate an Integrity Check manually or schedule automatic Integrity Checks.

To initiate an Integrity Check manually:

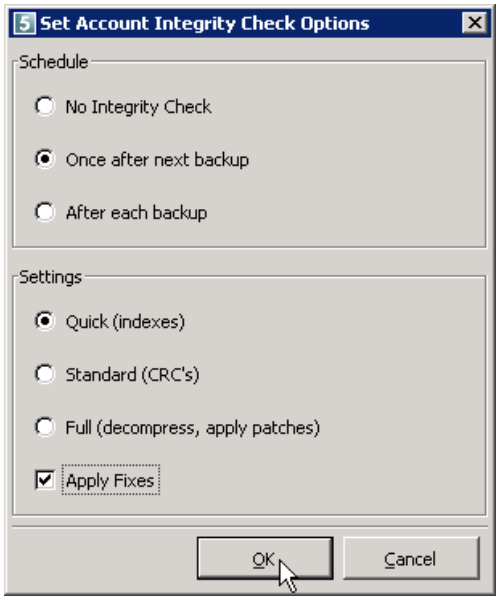


1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Backup Account on which you wish to perform an Integrity Check.
4. On the **Account** menu, point to **Advanced**, point to **Integrity Checks**, and then click **Initiate Integrity Check now**. Alternatively, right-click the Backup Account name, point to **Advanced**, point to **Integrity Checks**, and then click **Initiate Integrity Check now** on the shortcut menu that appears.
5. In the **Initiate Integrity Check now** dialog box that appears, select the checks to be performed, whether or not to apply fixes and whether to run the Integrity Check on the StorageServer or MirrorServer.

   ***Note**:*

   - *The MirrorServer target will be greyed out if the Backup Account's StorageServer or Backup Group is not mirrored.*
   - *If you choose to run the Integrity Check on the MirrorServer, you must be logged in to the SP Console with the "admin" account and the MirrorServer must be set to use the Master password and not a Mirror Account.*
6. Click **Start**.

To schedule an Integrity Check:



1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the name of the Account on which you wish to perform an Integrity Check.
4. On the **Account** menu, point to **Advanced**, point to **Integrity Checks**, and then click **Schedule an Integrity Check**. Alternatively, right-click the Account name, point to **Advanced**, point to **Integrity Checks**, and then click **Schedule an Integrity Check** on the shortcut menu that appears.
5. Select one of the following options:
   - Once after next backup
   - After each backup

   ***Tip**: **After each backup** is less processor intensive than the other options as it will only verify the latest backup and not all available backups on the Storage Platform.*
6. In the **Settings** area, specify the level that should be checked and whether or not fixes should be applied.
7. Click **OK**.

***Warning**:*

- *Note that the only way for the Integrity Check to fix a problem is to remove the problem file from the backups. If this happens, the Backup Client will receive an error during the next backup which will flag the particular file for a full backup.*
- *Only a small number of Integrity Checks can be run at the same time so some checks may be postponed until the next backup if too many are running.*

Overriding the StorageServer IP

This feature does not move the Backup Account data. It is used when the StorageServer IP address or host name has changed or to temporarily send the data of the next backup to a different StorageServer.

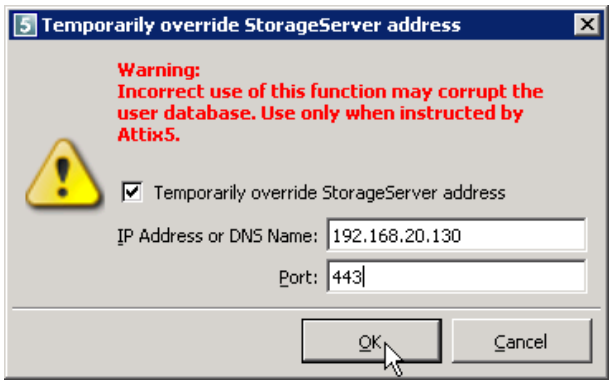
***Warning**: Changing the StorageServer IP address will cause ALL Backup Clients that connect to it to use the new address. Incorrect use of this feature may corrupt the user database.*

***Note**: You will only see this option if you manage more than one StorageServer with the SP Console.*

Tip: You can use this feature to back up to a snapshot server. See "Preparing a Recovery Server for a Snapshot".

To override the StorageServer IP:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, select the Account(s) you wish to move.
4. On the **Account** menu, point to **Advanced**, and then click **Override StorageServer IP**. Alternatively, right-click the Account name, point to **Advanced**, and then click **Override StorageServer IP** in the shortcut menu.
5. In the Temporarily override StorageServer address dialog box that appears, select the **Temporarily override StorageServer address** check box.

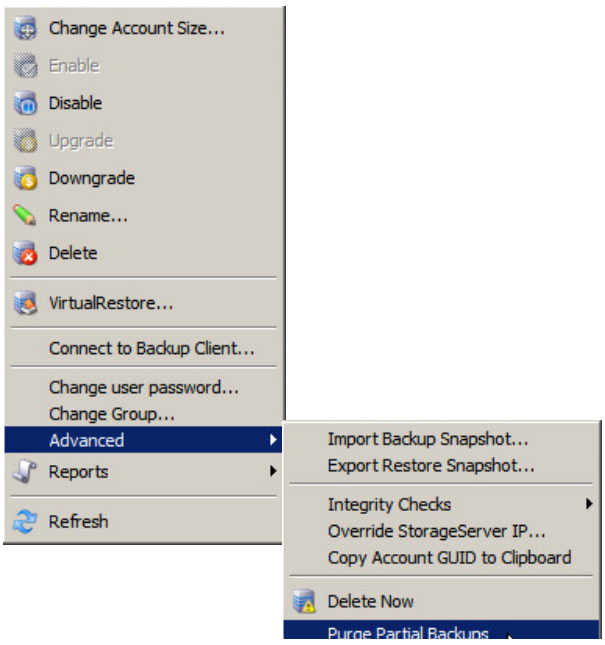


6. In the **IP Address or DNS** name box, type the IP address or DNS name of the StorageServer you wish to move the Account to.
7. In the **Port** box, type the port number the SP Console must use to connect to the Storage Platform.
8. Click **OK**.

Purging Partial Backups

Partial backups are unfinalised backup processs on the Storage Platform. This occurs when staged backups are interrupted or are cancelled unexpectedly so that the backup can be resumed at a later stage. This also occurs when streaming backups are interrupted where the "retry" attempts are still in progress.

This also prevents integrity checks from being run or for integrity problems to be corrected (see "Initiating/Scheduling Integrity Checks" earlier in this section). To correct this, these "partial" backups should be removed from the StorageServer.



To purge partial backups:

1. In the Account Management view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, right-click the Backup Account(s) whose partial backups need to be purged.
4. Select **Advanced** and then **Purge Partial Backups**.
5. Click **OK** on the warning dialog that appears.

Note:

- *For ESE Backup Accounts, the Purge instruction will automatically be performed every 24 hours.*
- *ESE Backup Clients cannot resume partial backups unless the retry attempts haven't been exhausted. Therefore, the Purge task will automatically be run if a backup fails or is cancelled.*
- *Any data received for a Backup Account during a partial backup will need to be backed up again.*

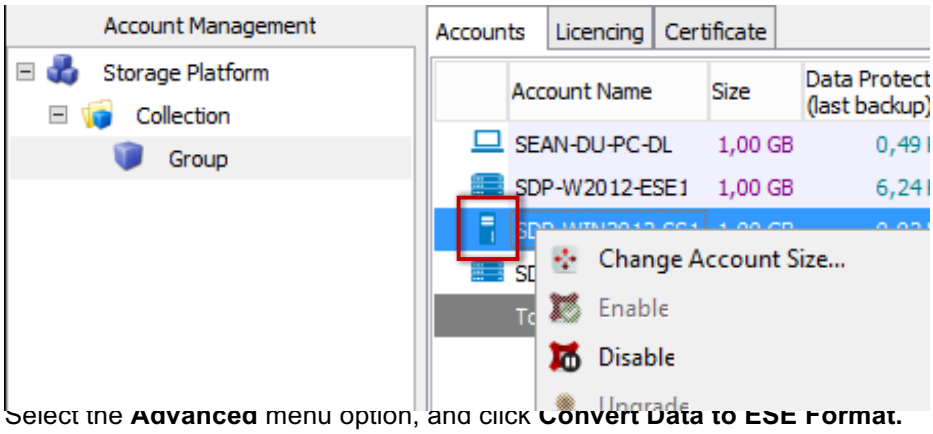
Converting SE Accounts to the ESE data format

In order to facilitate upgrading existing Server Edition (SE) Backup Clients to Enterprise Server Edition (ESE), existing SE Backup Accounts on the Storage Platform can be converted to the data format used by ESE. Only then can the newly installed ESE Backup Client connect to the same account.

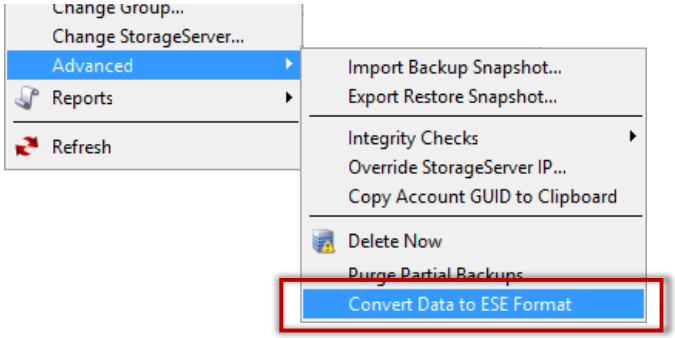
To convert Backup Accounts:

Note: *You'll need Storage Platform or Group Administrator permissions to view the menu item below.*

1. In the **Account Management** view, expand the Account Management tree and select the Group contain the SE account(s) to be converted.
2. Select one or many Backup Accounts. (Multiple Accounts are selected by using the “CTRL” key while left-clicking the Account.)
3. Right-click on a selected SE Account to bring up the context-menu.



4. Select the **Advanced** menu option, and click **Convert Data to ESE Format.**



A wizard will be initiated guiding you through the rest of the process. Take note of the prompts and requirements displayed on the screen.

***Note**: ESE licences will automatically be allocated to newly converted ESE Accounts' Backup Clients once an Account has been converted. However, it is recommended that you allocate the appropriate number of ESE licences to affected Backup Groups for effective Storage Platform licence maintenance.*

***Tip**: Run the "SE to ESE Conversion" report (located in the **Reports** view, under "Enterprise > Other") to list all converted Accounts and those that haven't yet been connected to with the ESE Backup Client.*

(See the section, "SE Backup Account Conversion" later in this chapter for details on the conversion process.)

Accessing often-used reports

To access often-used Backup Account reports:

1. In the **Account Management** view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
2. Ensure that the **Accounts** tab is selected in the work area.
3. In the Accounts list, right-click the Backup Account(s) whose reports you want to access.

4. Select **Reports** and then select the report that you want to access.

SE Backup Account Conversion

In order to facilitate upgrading existing Server Edition (SE) Backup Clients to Enterprise Server Edition (ESE), existing SE Backup Accounts on the Storage Platform can be converted to the data format used by ESE. Only then can the newly installed ESE Backup Client connect to the same account.

How does it work?

When the conversion of an Account is initiated, a new task on the Storage Platform is started. This task will sequentially convert each Account in the selected list, one after the other. At a high level, the process is as follows:

1. The Account is prepared by purging any partial backups and running a quick integrity check to correct any data discrepancies.

   *(The "conversion" task on the StorageServer can still be cancelled. See the section, "**Error! Reference source not found.**", in Chapter 7, "Storage Platform Configuration".)*

2. Backup indexes and files are converted to the new format resulting in "duplicate" copies.

   *(The "conversion" task on the StorageServer can **not** be cancelled.)*

   ***Note**: This uses additional disk space on the affected StorageServer.*

3. At this point the Account is also disabled and locked to prevent any other Storage Platform tasks from being performed on it, such as backups.
4. Once the conversion has taken place the data is verified with another quick integrity check.
5. The original SE-format Account data is deleted, an ESE licence is reserved on the Backup Group, and the ESE Backup Client is able to connect to the converted Account.
6. If a MirrorServer is affected by this Account, a conversion task for the relevant Account will be performed immediately.

Before converting an Account

1. Restrictions

Limitations exist that will prevent an SE Backup Account from being converted:

- **Plug-ins.** If the Backup Client of the Account uses plug-ins that are not provided or supported in ESE. The following plug-ins will not prevent the Account from being converted:
  - Email Notification (Plug-in ID 19)
  - Script [(Plug-in ID 20)
  - VSS [(Plug-in ID 29)
  - System State (using WSB) (Plug-in ID 36)
  - UNC (Plug-in ID 100)
  - Workspace (Plug-in ID 1000)

  Take note of the prompts on the screen. All data, however, will still be accessible for restores from the Backup Client after the Account has been converted.

- **Operating system compatibility.** If the operating system of the Account's Backup Client currently resides on an operating system not supported by ESE.

2. Requirements

- Ensure that you have at least 1GB of RAM available on the StorageServer for every 1 million files in the Backup Account that is to be converted.

***Note**: This is over and above the minimum 4GB required by normal StorageServer operation.*

- Because of Step 2 mentioned above, ensure that sufficient disk space is available on the StorageServer containing the Accounts that are to be converted – 10% more than what as currently used by the Account in question.

***Note**: Post conversion, the SE-format Account data is deleted.*

Converting SE Backup Accounts

To convert Backup Accounts, see the section above “Converting SE Accounts to the ESE data format” under “Advanced Actions”.

Remote Management

You can connect to and administer BackupVault DL and SE Backup Clients using the Storage Platform Console’s Remote Management feature.

***Note**:*

- *Remote Management is not available for ESE Backup Clients.*
- *Remote Management must be enabled in the Backup Client before you can connect to it. (For more information, please refer to the relevant Client User Manual.)*
- *If Multiple Backup Sets are enabled on the Client, only the Default backup set will be accessible using the Remote Management feature.*

***Tip**: This feature is especially useful if you do not have GUI access via the Client (e.g. if the Client is installed on a Linux operating system with the GUI feature disabled.)*

Two connection options are available:

- Connect using your Storage Platform Access Account
- Connect using the standard Remote Management username and password

***Note**: A user connecting with Access Account credentials will only have access to the Remote Management functionality assigned to his/her Role. Users connecting with the standard Remote Management username and password will have full access to all Remote Management functionality. For more information, see Chapter 9, “User Access Management”.*

By using this feature, you can initiate backups and restores, modify the backup selection, view log files and configure a number of options ranging from the backup schedule to file exclusions and patching settings.

Connecting to a Backup Account

To connect to a Backup Account:

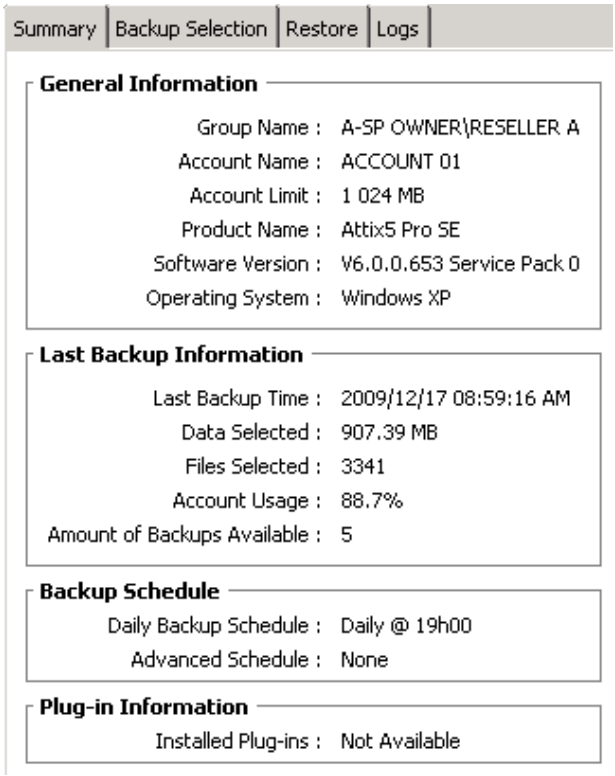
1. Ensure that Remote Management is enabled in the Backup Client. (For more information, please refer to the relevant Backup Client User Manual.)
2. In the **Account Management** view, expand the Account Management tree and select the name of the Group to which the Backup Account belongs.
3. On the **Account** menu, click **Connect to Backup Client**. Alternatively, double-click the Account name or right-click it, and then click **Connect to Backup Client**.
4. In the **Connect to Backup Client** dialog box that appears, ensure that the correct IP Address and the Storage Platform port number display the boxes provided.
5. Select the type of credentials you wish to use.

   ***Note**:*

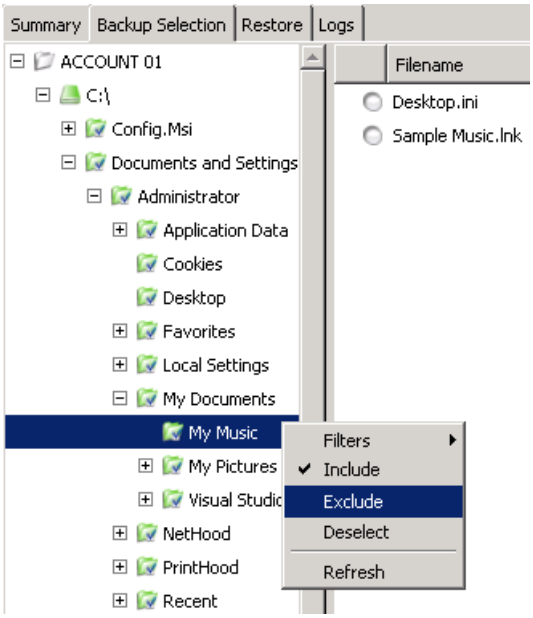
   - *If **Allow SP controlled** access was selected when Remote Management was enabled on the Client, you will be able to use the Storage Platform credentials to connect to the Client.*
   - *If **Allow custom access** was enabled and a particular username and password were specified in the Client, you need to select **Use these credentials** and type those credentials in the boxes provided.*
6. Select **Remember these details** to keep these connection settings configured for your next Remote Management connection.
7. Click **OK**.

Once connected to a Backup Client, four tabs are displayed: **Summary**, **Backup Selection**, **Restore** and **Logs**.

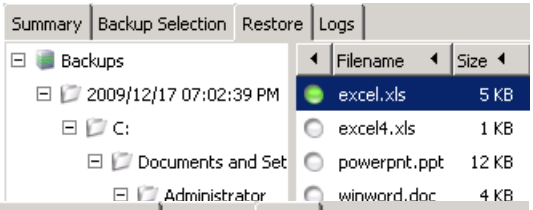
The **Summary** tab displays Backup Account information and configuration settings (a summary of the Backup Client with information ranging from the Account limit, software version and Operating System to the Backup Schedule and installed plug-ins).



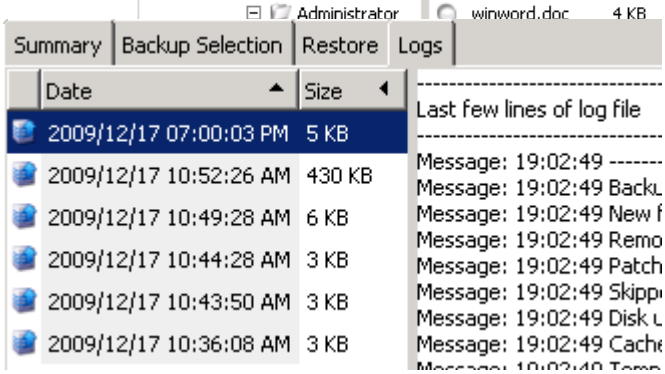
You can use the **Backup Selection** tab to modify the backup selection on the remote machine. Right-click the files and/or folders and use the shortcut menus to change their selection statuses. Click the **Backup** button on the main toolbar to initiate the backup process. If the previous backup failed for any reason, the Storage Platform Console will prompt whether the previous backup must be resumed.



You can use the **Restore** tab to restore files and folders. Select the folders to restore and then click the **Restore** button on the main toolbar to initiate the restore process.



On the **Logs** tab, you can view Backup and Restore Logs. To view only a summary of the logs, click the **Summary** button on the main toolbar.



__Tip__: While a Backup or Restore process is running, you can use the __Cancel__ button to stop the process.

Configuring a Backup Account

__Warning__: Please read through this section carefully before changing any of the settings. Incorrect settings could cause serious problems or even stop the Backup Client from functioning.

To configure a Backup Client via Remote Management:

1. Click the **Options** button on the main toolbar.
2. In the **Backup Agent Properties** dialog box that appears, configure the tabs as desired. For more information on the tabs available, see sections below.
3. Click **OK**.

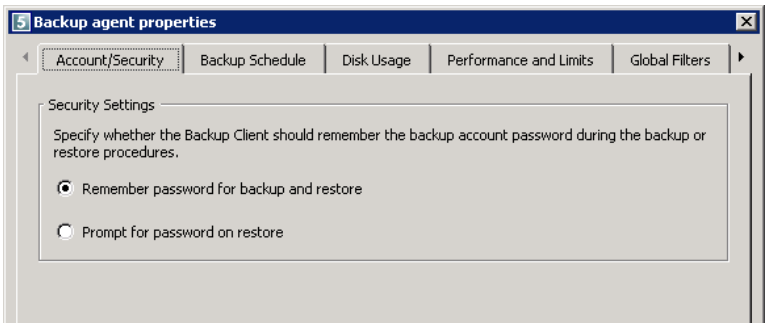
Backup Agent dialog box

The **Backup Agent** dialog box provides you with Backup Client properties also available in the Backup Client's **Options and Settings** dialog box. The tabs described below enable you to modify these properties from within the SP Console.

Account/Security tab

Security Settings

The Account/Security tab allows you to select whether or not the Backup Client is to remember the Backup Account password during backups and restores. Two options are available:

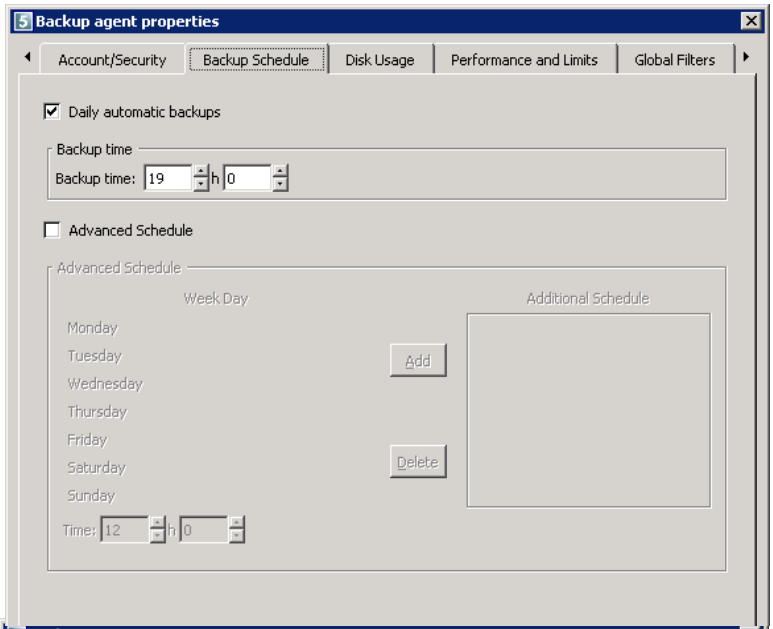


- Remember password for backup and restore: The Backup Client remembers the user password when doing a backup or restore. This is the default setting.

- Prompt for password on restore: The Backup Client prompts for the user password during the restore process.

Backup Schedule tab

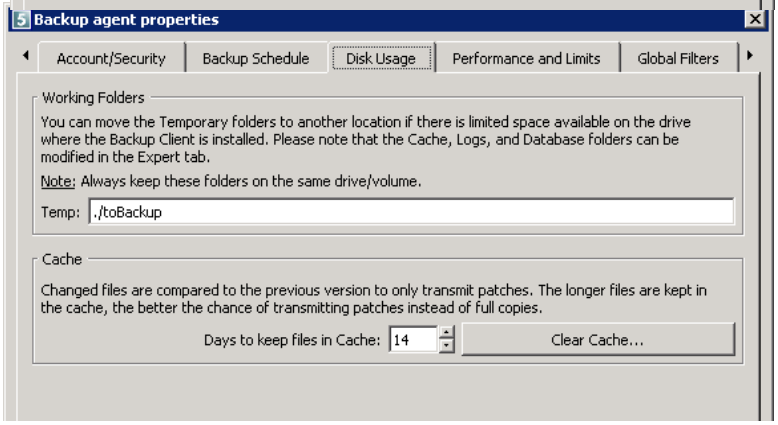
You can modify the backup schedule on the **Backup Schedule** tab. Settings on this tab are identical to those available in the Backup Client's **Options and Settings** dialog box. For more information on configuring backup schedules, please refer to the relevant Backup Client User Manual.



***Warning**: If disabling automatic backups, all backups will have to be initiated manually.*

Disk Usage tab

You can use the **Disk Usage** tab to change the **Temp** folder location and the number of days that files are to be kept in the cache.



Working Folders section

If there is limited space on the drive where the Backup Client is installed, you can move **Temp** folder, which is used as a temporary workspace for backups and restores, to another location.

***Note**: **Cache**, **Logs** and **Database** folders can be moved using the **Expert** tab.*

***Warning**:*

- *The **Cache** and **Temp** folders must reside on the same drive/volume.*
- *If the database or any of the folders are stored on a network share, please ensure that the Backup Service has the correct permissions to connect and write to that share.*

Cache section

When modifications are made to a file, the Backup Client only transmits changes to that file, as opposed to transmitting the complete file again. This is accomplished by the use of a local cache.

By default, recently modified files are kept in the Cache for 20 days, after which they will be deleted. Once a file has been flushed from the cache, a full copy will be backed up when any modifications are made to the file. The longer files are kept in the Cache, the better the chance of only transmitting patches instead of full copies and thus reducing the amount of data that needs to be transmitted. If there is limited disk space available, consider shortening the time files are kept in the cache.

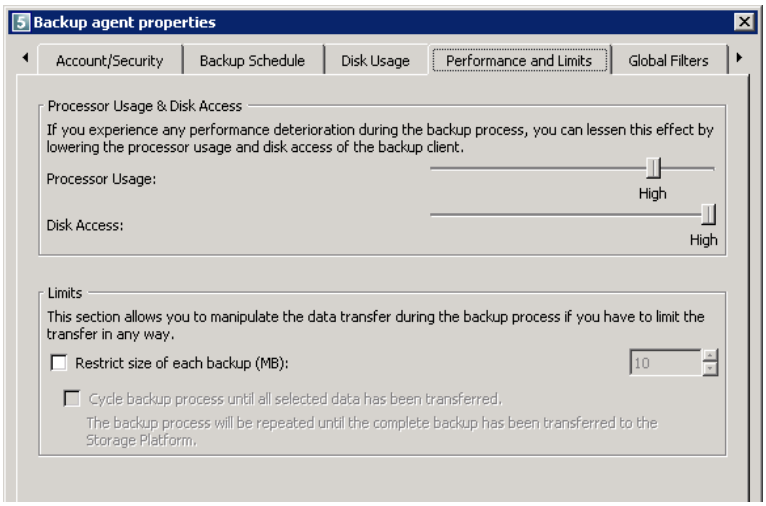
***Warning**: If 0 days are specified for caching, patching is disabled. All files in the **Cache** will be deleted and full copies of changed files will be backed up to the server during each backup.*

To delete the current cache, click the **Clear Cache** button. If the cache is deleted, full copies of the selected files will be re-sent to the Storage Platform during the next backup.

***Note**: The Backup Client will log the message **Doing monthly cache cleanup** once a month. This maintenance task is to ensure that there are no redundant files in the Cache.*

Performance and Limits tab

On the **Performance and Limits** tab, you can change the processor usage, disk access and data transfer limits.



Processor Usage and Disk Access section

The Backup Client uses a fair portion of the available processor power to patch, compress and encrypt files during the backup process. If the computer is being used at the same time, the user may experience some performance deterioration. You can lessen this effect by lowering the Client's processor usage and disk access.

To lower the Backup Client processor usage:

Move the **Processor Usage** slider to the left.

***Warning**: If the highest **Processor Usage** setting is used, it will affect server performance during the backup.*

To lower the Backup Client disk access:

Move the **Disk Access** slider to the left.

***Tip**: The process will take longer if this setting is lowered but other disk-intensive applications will perform better.*

***Warning**: If the **High** setting is used, the Backup Client will continuously use all available disk access to read and write to the disk. This will, however, ensure that the process completes as fast as possible.*

Limits section

You can use the **Limits** tab to limit data transfer speed and/or the size of each backup.

To limit data transfer speed:

1. Select the Limit outgoing transfer speed (Kbyte/s) to check box.
2. Type a value in Kbytes/second in the box provided.
3. Click **OK**.

To limit the size of each backup:

1. Select the Restrict size of each backup (MB) check box.
2. Type a maximum value amount of data that may be transferred during each backup.
3. If you wish to enable a backup cycle, select Cycle backup process until all selected data has been transferred.
4. Click **OK**.

***Note**: If this option is enabled, it may take several backups before all files are backed up to the Storage Platform. This feature is especially useful when using a slow Internet connection and there are problems with transferring large backups.*

Global Filters tab

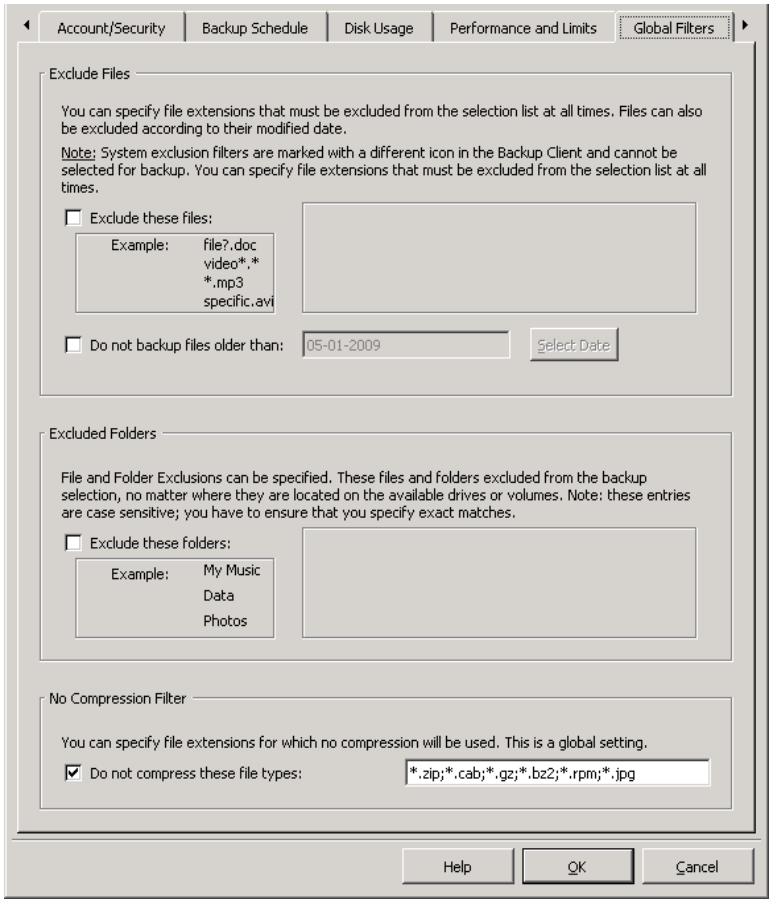
Global Filters enables you to exclude files and/or folders globally and set up a No Compression filter.

Exclude Files section

Exclude these files enables you to specify that files with certain file names, extensions or last modified dates be excluded from all backup selections.

***Tip**: You can use wildcards. E.g. *.mp3 will exclude all MP3 files from backups.*

***Example**: To exclude all MP3 and AVI files, type: *.mp3;*.avi in the text box. (Separate entries with a semicolon.)*



You can also exclude files based on their *last modified* date by selecting the **Do not back up files older than** check box and specifying a date in the box provided.

***Note**: The **Date Exclusions** Filter uses the file modify date as a reference and not the file create date.*

Exclude Folders section

Exclude these folders enables you to exclude certain folders from all backup selections.

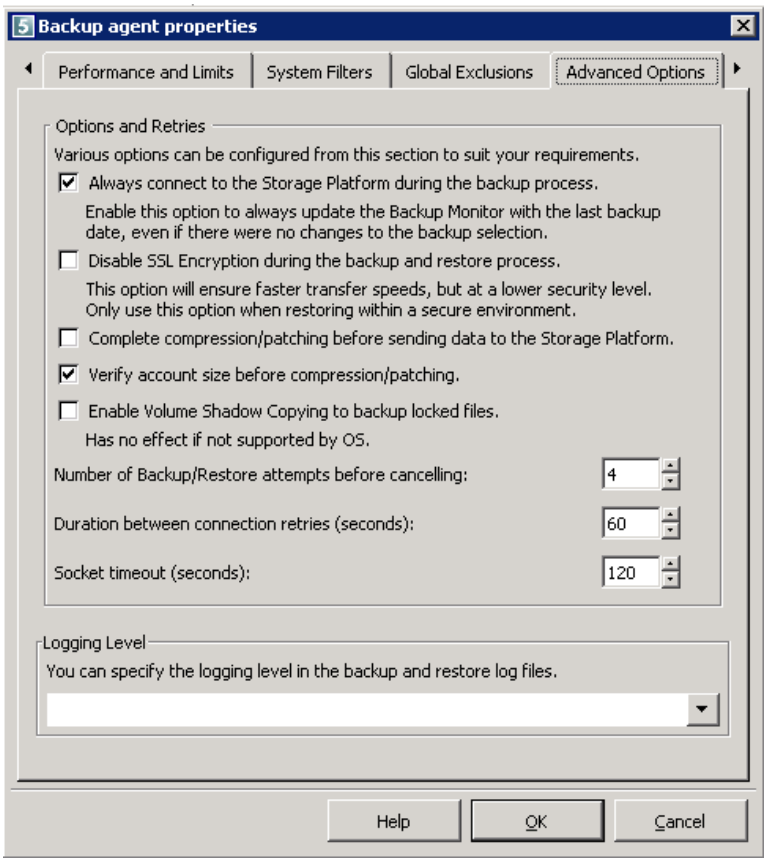
***Note**: The **Date Exclusions** Filter uses the file modify date as a reference and not the file create date.*

No Compression Filter section

Compression is not effective on all file types as some files may already be compressed or cannot be compressed at all. The Backup Client could increase processor usage and spend some time trying to compress these files. This filter enables you to specify a list of file extensions that must not be compressed during the backup process. The list of file types specified by default are types known for not compressing well.

Advanced Options tab

Options and Retries section



- Always connect to the Storage Platform...

  When the **Always connect to the Storage Platform** check box is selected, the Backup Client will connect to the Storage Platform during each backup, whether or not changes were made. This updates the last backup date stamp, even if there were no changes made to the backup set, ensuring that the Storage Platform always reflects the latest backup date.

- Complete compression/patching before sending data to the Storage Platform

  During the backup process, BackupVault SE compresses and patches files and places them in a queue to be transmitted. This queue allows transmission and compression/patching to occur in parallel, reducing the total backup time significantly.

  Select this option to disable multiple thread backups. This option is typically needed when using a dial-up account. With this setting enabled, the Backup Client will compress all new files and patch all modified files before starting to transmit data to the Storage Platform.

- Verify account size before compression/patching

  With this setting enabled, the Backup Client verifies the Backup Account size limit on the Storage Platform before starting with the compression and/or patching. It is useful to flag Account limit issues before starting these possibly time-consuming processes.

- Enable Volume Shadow Copying to back up locked files

  Microsoft Volume Shadow Copy Service (VSS) provides a solution by creating a snapshot of the data at any given point in time without any interruption to any applications. Using this option enables the backup of open or locked files.

***Warning**: When using the SE Backup Client, please use relevant plug-ins to back up databases, otherwise, the ESE Backup Client also backs up SQL Server databases securely using VSS.*

- Use VSS to update the cache

  Using this option will increase the speed of the cache update process.

***Warning**: This setting will increase the load on VSS and may cause VSS to fail on servers with heavy I/O (like file servers), resulting in cache update failures.*

- Number of Backup/Restore attempts before cancelling

  By default, the Backup Client tries to connect to the Storage Platform 4 times before cancelling the backup process. It is advised to increase the number of attempts when using a slow Internet connection. The backup will continue from the previous point of failure and not resend the entire backup.

- Duration between connection retries

  By default, if the connection is dropped, the Backup Client will try to reconnect to the Storage Platform after 60 seconds. This setting enables the Backup User to increase/decrease the duration between the retries.

- Socket Timeout

  The default socket timeout is 60 seconds. If the Backup Client is connected to the Storage Platform and there is no communication between the two, the time specified in this box (in seconds) is how long the Backup Client will stay connected before dropping the connection.

Logging Level section

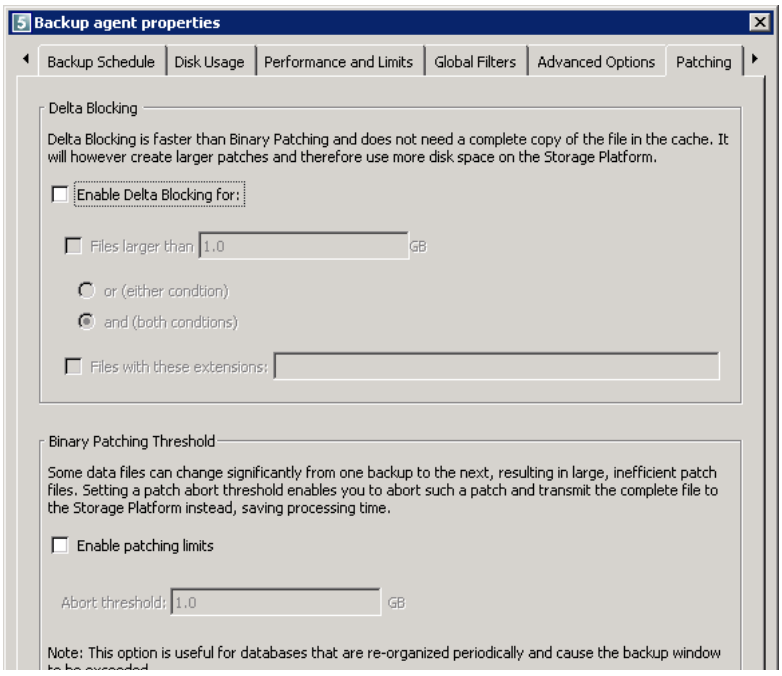
You can specify the level of information that must be included in the log files. Choose between:

- Log all messages
- Suppress detail
- Log errors and warnings

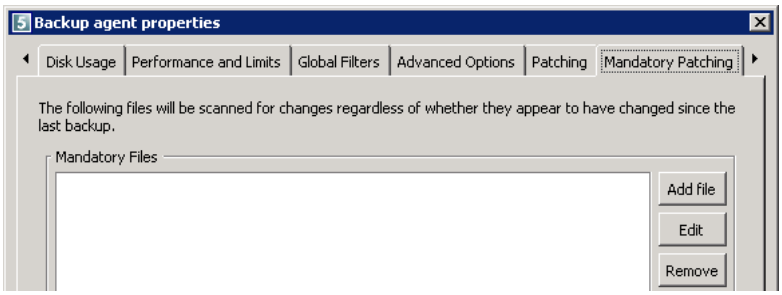
Patching tab

Patching is the process of extracting only the differences between files. This process minimizes the amount of data that has to be transferred to the Storage Platform. There are two types of patching available: Binary Patching (enabled by default) and Delta Blocking.

If you are not accustomed with this functionality, please refer to the Client User Manual for additional information before changing these settings.



Mandatory Patching tab



A file is considered modified if the timestamp or size changes. The Backup Client can, however, be configured to patch certain files and folders regardless of whether or not they appear to have changed since the last backup.

Files selected for mandatory patching display on the Client's **Backup Selection** tab with a green icon containing the letter "M": .

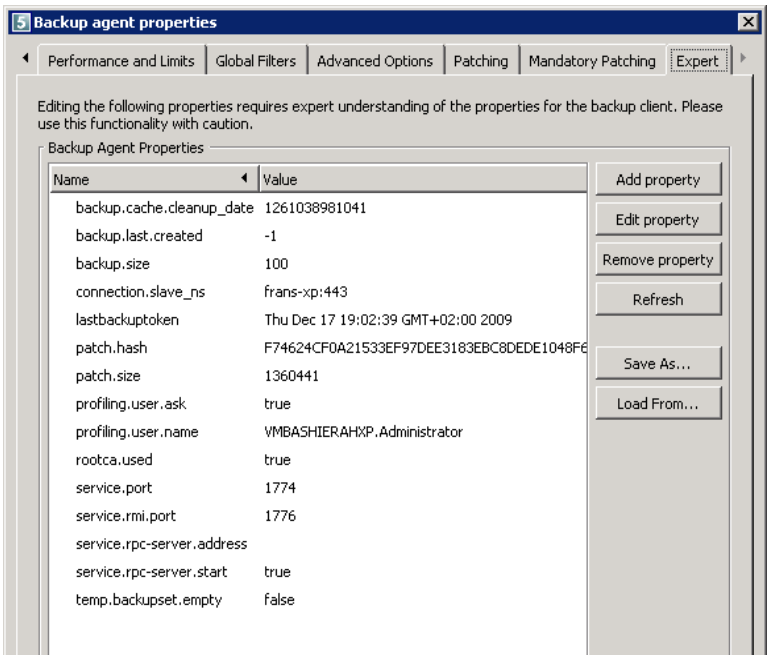
***Note**: Files selected for mandatory patching can be excluded by the Backup Client user. For more information, please refer to the Client User Manual.*

***Tip**: Mandatory Patching is especially useful in situations where files are held open by an application (internally the file changed, but the change is not reflected in the last modified date on the file system or in the size of the file itself).*

To select files for mandatory patching:

1. Click the **Add file** button.
2. In the **Add file** dialog box that appears, type the name of the file.
3. Click **OK** to save the settings.

Expert tab



The **Expert** tab contains all variable settings not found on any of the other Backup Client configuration tabs. These entries are saved in the **a5backup.properties** file and the file also includes plug-in settings, if installed.

***Warning**: Please use this tab with caution. Incorrect use may alter the backup and restore procedures.*

Use the buttons on the right to **Add**, **Edit** or **Remove** properties. Settings can be imported and exported by using the **Save As** and **Load From** buttons, and the **Refresh** button will update the Backup Client Properties section with any recent changes.

Backup Client Updates

Updating Backup Clients manually can be a time consuming exercise. BackupVault allows you to automate this process. Desktop & Laptop Edition, Server Edition and Enterprise Server Edition can be updated automatically with the latest software version (like new releases and service packs) and brand changes during backups.

Performing automatic updates requires the following:

- Auto-updates are enabled on the AccountServer
- The AccountServer is up to date with the latest Backup Client upgrade files (for distribution to Backup Client machines)

***Note**: Backup Clients are always updated to the latest version and service pack available on the Storage Platform. If the version is too old to be updated, the update must be done manually.*

For ESE Backup Clients, the update pack is distributed in two files per Storage Platform: one for brand updates and one for core Backup Client updates; for all other Backup Clients, one file per Storage Platform is distributed.

A separate update for each brand and operating system is created. If you have different branded Backup Clients connecting to your Storage Platform, they will be updated with their own branding.

Backup Client update activities are displayed in the Diagnostics area of the Storage Platform Console.

Enabling Auto-Updates

You can enable Auto-Updates for the complete Storage Platform (from the AccountServer) or per Collection or Group.

***Warning**: If a Backup Client plug-in has been deprecated, the Backup Client will only be updated to the latest version in which the plug-in was still supported.*

To enable Auto Updates for the entire SP's Backup Accounts:

1. Access the **Storage Platform Configuration** view by clicking the **Storage Platform Configuration** button in the view selector.
2. Click the AccountServer node in the Storage Platform Configuration tree and then click the **Configure** button on the toolbar. Alternatively, right-click the AccountServer node and then click **Configure**.
3. Navigate to the **Updates** tab and select the **Auto-update Backup Client** check box. Ensure that the **Update File Search Path** is correct and then click **OK**.

Auto Updates are now enabled. Since all Backup Groups are set to use the Storage Platform's default Auto Update setting by default, Auto Updates are now enabled for all Backup Groups.

To enable Auto Updates at Collection/Group level:

1. Access the Account Management view by clicking the **Account Management** button in the view selector.
2. Select the Collection or Backup Group name and then click the **Configure** button on the toolbar. Alternatively, right-click the Collection or Group name and then click **Configure**.

3. Click the **Updates** tab and then select the applicable **Auto Update Backup Client** option.
    a. **Storage Platform Default** – The setting enabled on the AccountServer (see procedure above) will be applicable
    b. **Yes** – Auto-updates are enabled (Overrides AccountServer setting)
    c. **No** - Auto-updates are disabled (Overrides AccountServer setting)

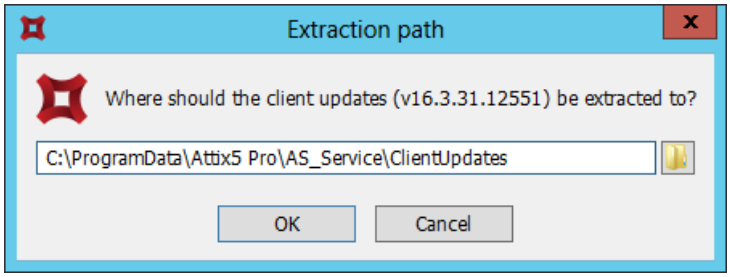
***Warning**: When setting the Auto-Update Backup Client option on Collection level, the setting will only be applicable for new Groups i.e. the option is not automatically propagated to existing Backup Accounts.*

Update AccountServer with core Backup Client upgrades

Once an updated Backup Client upgrade file has been extracted on the AccountServer it will be available for distribution when Backup Clients request updates during the backup process.

To extract the upgrade file:

1. Run the "…**ClientUpdates**….**exe**" file where the AccountServer is installed.
2. Confirm the extraction path in the dialog box provided or enter a new one:



***Note**: The path must correspond to the **Update File Search Path** specified in the "Enabling Auto-Updates" procedure above.*

3. Click **OK**.

The latest client updates will be extracted and can be requested by Backup Clients. However, for Enterprise Server Edition Backup Clients, updates are distributed to the respective StorageServers from where it can be requested by Backup Clients.

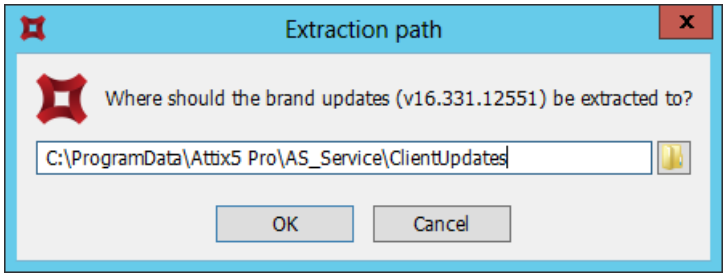
***Note**: The latest supported Java version is also supplied with the core Backup Client updates.*

Update AccountServer with brand changes

For Enterprise Server Edition Backup Clients only, once the file with updated brand changes has been extracted on the AccountServer it will be available for distribution when Backup Clients request updates during the backup process.

To extract the upgrade file:

1. Run the "...BrandUpdates...exe" file where the AccountServer is installed.
2. Confirm the extraction path in the dialog box provided or enter a new one.



***Note**: The path must correspond to the Update File Search Path specified in the "Enabling Auto-Updates" procedure above.*

3. Click **OK**

The brand updates will be extracted on the AccountServer and distributed to the respective StorageServers from where it can be requested by Backup Clients.

Plug-in Auto-Update process

During the backup process, the Storage Platform will compare the plug-in versions received from the Backup Client with the latest versions available on the Storage Platform. If newer versions are available, the Backup Client will be able to download the files and automatically update the installed plug-ins.

Deployment Wizard

The Deployment Wizard is used to create a single installation file (MSI) that can be preconfigured with file selections and backup permissions to install **Desktop & Laptop Edition, Server Edition** or **Enterprise Server Edition** Backup Client software on a computer.

***Warning**:*

- *Certain anti-virus programs may result in deployment failures. In such cases, you may need to disable antivirus scanning for the duration of the deployment process.*
- *To prevent ESE Backup Client deployments from failing, ensure that both the Update AccountServer with core Backup Client upgrades and Update AccountServer with brand changes have been extracted on the AccountServer.*

Creating a Backup Client deployment file

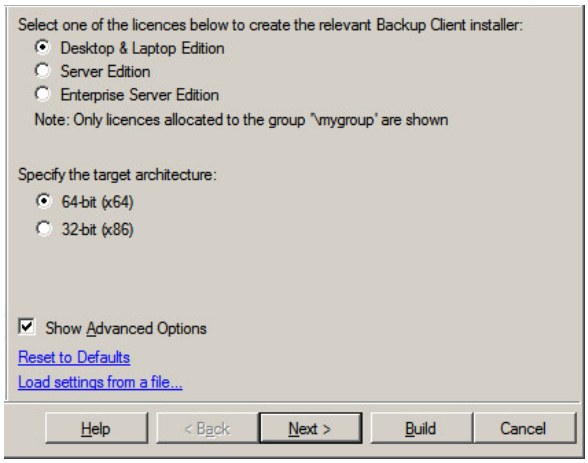
To create a deployment file for a Backup Group:

1. In the Account Management view, expand the relevant Collection in the Account Management tree.
2. Right-click the name of the Backup Group to which the new Backup Accounts will belong, and then click **Deploy**.

3. The Deployment Wizard will be initiated. Follow the wizard steps described below to create the deployment file. A custom MSI installer will be built according to your wizard selections.

Step 1 of 11: Start the Deployment Wizard and specify the initial settings

1. Select the type of Backup Client installer that you wish to create.
2. Select **64-bit** or **32-bit** as the target architecture.



***Note**: If you have access to multiple branded Backup Clients, you will be able to choose which brand to deploy during this step. The brands available depend on the brands that your Access User has been given access to. Admin users have full access to all brands.*

If you have access to multiple Storage Platforms, the latest Backup Client version relevant to that Storage Platform will be used to create the deployment.

***Warning**: Please note the following and ensure that you configure the MSI installer for the correct architecture:*

- *64-bit installers cannot run on 32-bit operating systems. However, 32-bit installers can run on 64-bit operating systems.*
- *System State and Exchange plug-ins can only function with 64-bit SE Backup Clients running on 64-bit operating systems.*
- *An available licence is required in order to create a corresponding Backup Client installer.*

3. Select the **Show Advanced Options** check box if you wish to view the Deployment Wizard's advanced options.

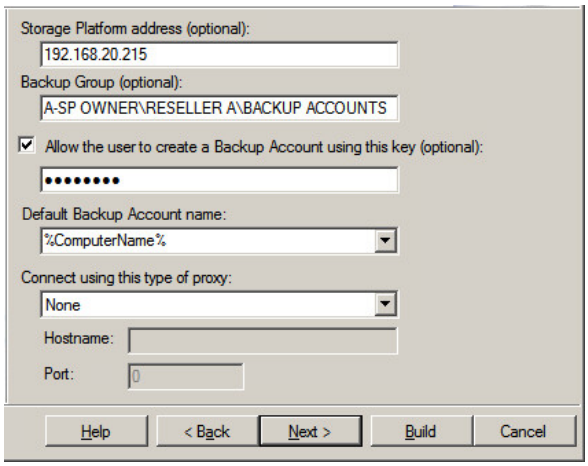
***Note**:*

- *The **Reset to Defaults** option at the bottom of the Deployment Wizard will reset all settings currently populated to the default settings.*
- ***Load settings from a file...** enables you to load settings from a previously created deployment file (you have the option to save the settings in an xml file for future use in the final step of the Deployment Wizard).*

4. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 2 of 11: Specify the Backup Account and connection details

1. Specify the correct Storage Platform and Backup Group details.



Warning:

- *Please ensure that you enter the correct settings, or the Backup Client will not be able to function correctly.*
- *If the AccountServer is bound to a port different from the default, ensure you specify the* ***Storage Platform address*** *with the port number appended e.g.:*

  192.168.20.215:223

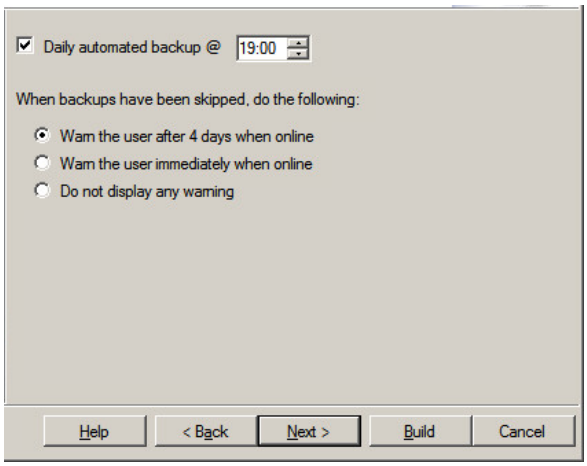
Note: *If you initiated the Deployment Wizard from within the Storage Platform Console, these entries will already be populated with the correct settings. If you leave these entries blank, the Backup Account Setup Wizard will prompt the user for the details.*

2. If you wish to disable the creation of new Backup Accounts, deselect the **Allow the user to create a Backup Account using this key** check box. The Backup Client will then only allow reconnects to existing Backup Accounts available on the Storage Platform.

Note: *The* ***Default Backup Account*** *name box allows you to specify whether the Backup Account name in the Backup Account Setup Wizard must be automatically populated with the computer name, user name, user domain, or any combination of the standard parameters, e.g. %UserDomain%-%UserName%. You can also specify the variable for the default Backup Account name. The Deployment Wizard supports all variables that can be found by typing "set" in the Command Prompt.*

3. If necessary, specify proxy settings in the boxes provided.
4. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 3 of 11: Configure backup scheduling



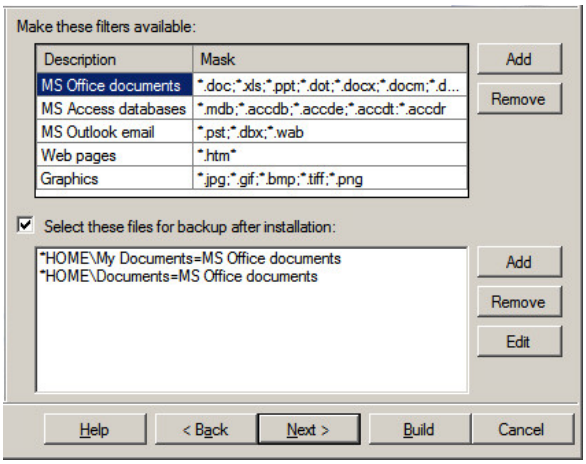
1. Specify a time for the daily automated backup. The default backup time is 19h00.

   ***Warning**: Automatic backups can be disabled, but the end-user will then have to manually initiate backups which is not recommended.*

2. Desktop & Laptop Edition Backup Clients can warn the user if backups were skipped by displaying a popup message whenever a network connection is detected. Select what action the Backup Client should take if a backup is skipped. Warn the user after 4 days when online is the default selection, to accommodate offline periods that typically occur during weekends.

3. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 4 of 11: Define default selection filters



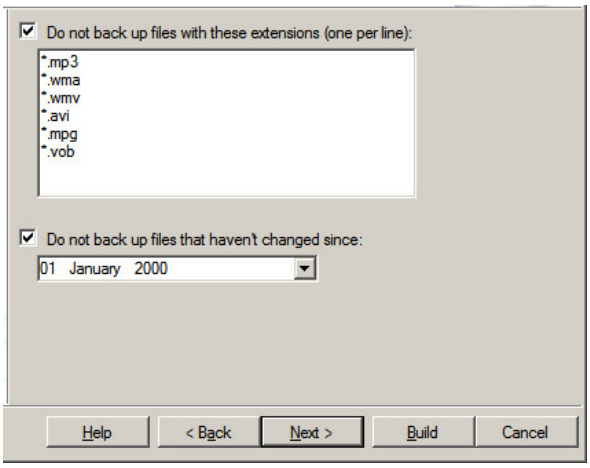
1. Use the **Add** and **Remove** buttons to specify the default selection filters that will be available in the Backup Client.

2. Enable the **Select these files for backup after installation** check box to apply some of the abovementioned filters when the Backup Client is opened for the first time. Use the **Add**, **Remove** and **Edit** buttons to configure the filter types that you want to include in the Backup Client's initial backup selection.

   ***Note**: *HOME\ refers to the logged in user's home folder.*

3. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 5 of 11: Specify exclusions



1. If you wish to stop certain file types from being backed up, select the **Do not backup files with these extensions (one per line)** check box and type the file extensions to be excluded in the box provided.

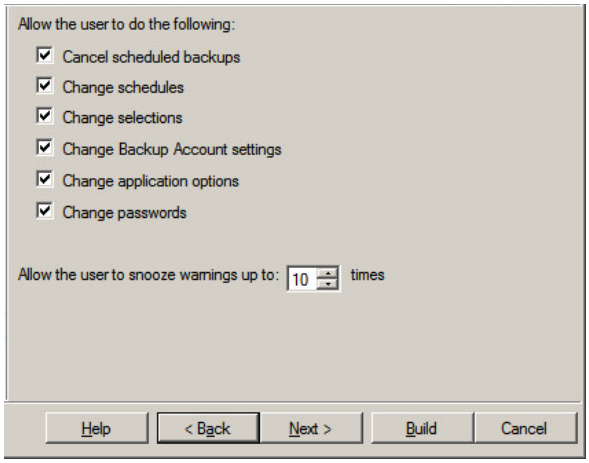
   ***Note**: Type each extension on a new line in the format: *.file.*

2. To prevent the backup of files that have not been modified recently, select the **Do not backup files that haven't changed since** check box, and then select a date.
3. Click **Next** to continue to the next step, or **Build** to start the build process.

   ***Note**: The exclusions specified above are marked in the Backup Client as **Excluded by Administrator** and take priority over the backup selection made by the end-user.*

Step 6 of 11: Specify restrictions (DL advanced option)

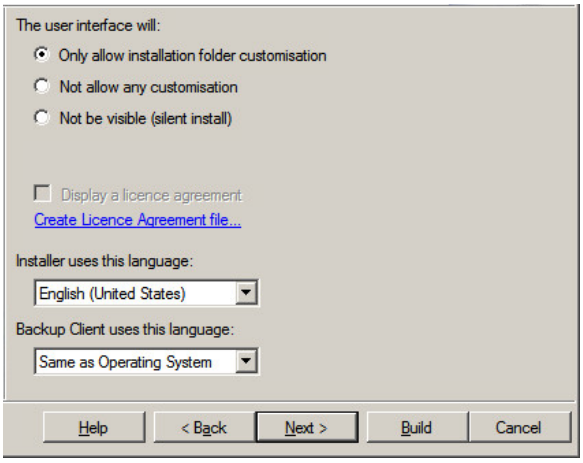
***Note**: This step is only available when deploying a DL Backup Client.*



1. Modify users' ability to cancel or change scheduled backups, change backup selections, change Backup Account settings, change application options and/or change passwords by selecting or deselecting the respective check boxes.
2. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 7 of 11: Specify restrictions (Advanced option)

1. Modify the behaviour of the MSI installer by selecting the level of customisation that the end-user will be allowed to perform during the install process.



> ***Note**: If you select **Not be visible**, you must have administrator privileges when running the installer or the installation will fail. This option causes the installation to run in the background. (See "Step 9 of 11: Configure custom Backup Client settings" for instructions on configuring the MSI properties so that the Backup Account name, password and encryption key are installed without user input.)*

2. Click **Create Licence Agreement file...** to create a licence agreement. After you have created a licence agreement, you can choose to display it in the installer wizard by selecting the **Display a licence agreement** check box.

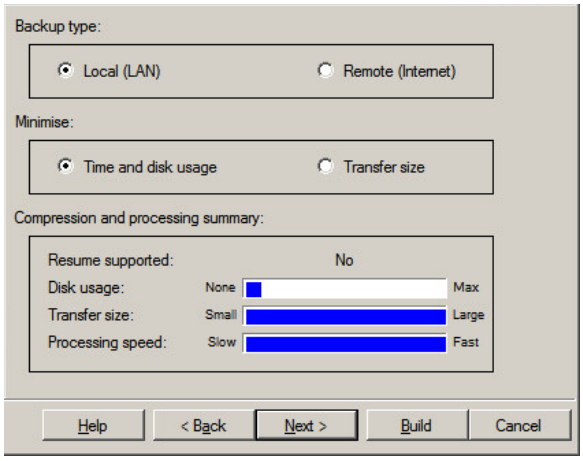
> ***Note**: If the Deployment Wizard detects a Licence.rtf file in C:\Users\{User}\AppData\Roaming\Deployment, the **Create Licence Agreement file...** link changes to **Edit Licence Agreement file...**.*

3. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 8 of 11: Set environment optimisation (SE advanced option)

***Note**: This step is only available when deploying a SE Backup Client.*

1. Select **Local (LAN)** or **Remote (Internet)** as the backup type. The default is Local (LAN). This option determines whether the Backup Client will be optimised to use Streaming Backup.
2. You can choose to minimise backup time and disk usage, or transfer size. The default is Time and disk usage.
3. Click **Next** to continue to the next step, or **Build** to start the build process.



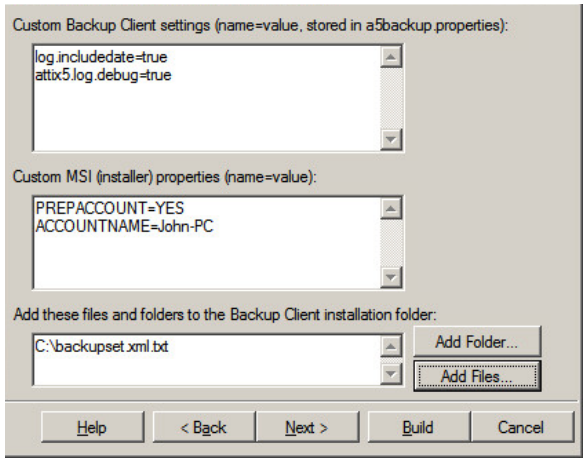
***Note**: The compression and processing summary displays the outcome of the choices you have made, with regards to support for resuming interrupted backups, disk usage, transfer size and processing time. The default selections optimise the Backup Client for backing up over a local network with network traffic not being an issue.*

Step 9 of 11: Configure custom Backup Client settings (Advanced option)

***Warning**: This step contains advanced features that could corrupt the functioning of the Backup Client. Please consult your Backup Administrator before configuring these settings.*

1. Specify any custom Backup Client settings that should be stored in the **a5backup.properties** file.

   ***Note**: Settings specified here will not override existing settings if you manually update the Backup Client using this deployment. The settings will only take effect if you perform a clean install or if the setting is new to the version being deployed.*



   ***Example**: To pre-configure the Backup Client so that backup and restore logs include the date, and the service log includes debug messages, type the following in the **Custom Backup Client settings...** box:*

   log.includedate=true

   attix5.log.debug=true

2. In the **Custom MSI (installer) properties...** box, if you wish to add properties to the MSI file, type each property on a new line.

***Note**: The encryption key must be 8 characters or more.*

***Example**: To pre-configure the MSI properties so that the Backup Client installs with the AccountServer IP: "192.168.20.215", the Backup Account name: "John-PC", the Backup Account password: "password", the Backup Group create key: "pas", the encryption key: "password" and the Backup Group: "A-SP OWNER\RESELLER A\BACKUP ACCOUNTS", type the following in the **Add these properties...** box:*

PREPACCOUNT=YES

SERVERIP=192.168.20.215

ACCOUNTNAME=John-PC

ACCOUNTPASSWORD=password

CREATEKEY=pas

ACCOUNTKEY=password

GROUP=A-SP OWNER\RESELLER A\BACKUP ACCOUNTS

3. To specify additional folders or files to be added to the MSI file when built, e.g. the **backupset.xml** file with a default selection, click the **Add Folder** or **Add Files** button, navigate to and select the items to add, and then click **Open**.

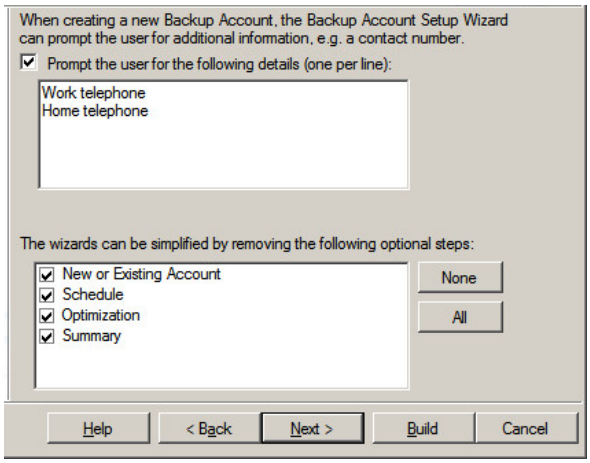
***Warning**: Files and folders added in this step will overwrite any existing files found in the installer. Please be careful when using this feature as you may corrupt the Backup Client when replacing files.*

***Note**:*

- *To add a folder to the Backup Client you must include its parent folder in this step.*
- *The contents of the selected folders are added to the installer.*

4. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 10 of 11: Configure Backup Client wizards (Advanced option)

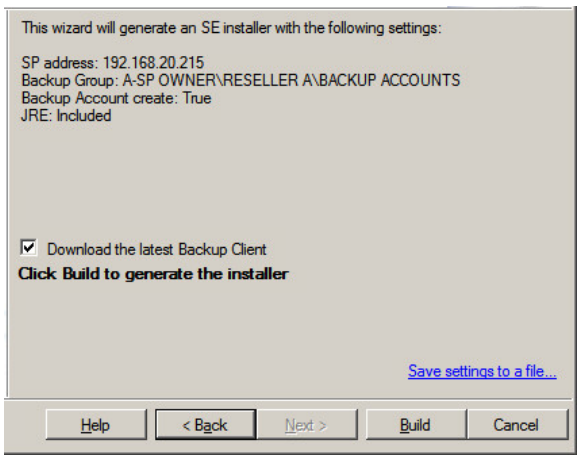


1. If you wish to specify any mandatory custom fields in a separate step in the Backup Account Setup Wizard, select the **Prompt the user for the following details (one per line)** check box and then type the names of the fields in the box provided, listing them on separate lines.

   ***Note**: The supplied values are stored in the AccountServer database and can be viewed in the SP Console.*

2. To simplify the Backup Client wizards for the end user, you can remove optional steps from them.
3. Click **Next** to continue to the next step, or **Build** to start the build process.

Step 11 of 11: Build



1. Select whether to download the latest Backup Client from the Storage Platform.

   ***Note**: If this check box is not selected, the Deployment Wizard will use the Backup Client that it currently has. If it does not have a Backup Client, the wizard will download it from the Storage Platform regardless of the check box selection.*

2. Confirm all the settings and then click **Build** to start the build process.
3. The Deployment Wizard will prompt you for the folder where the created MSI file must be stored. Your Desktop is the default location.
4. Once the MSI has been built, you can choose to open the Deployment folder on exit from the Deployment Wizard.
5. Click **Close**. The Deployment Wizard will save the current deployment settings before closing. The next time you open the Deployment Wizard, your settings will be automatically populated.

MSI Installer

The BackupVault MSI installer enables you to remotely deploy Server Edition and Desktop & Laptop Edition Backup Clients using your preferred desktop management solution, e.g. Microsoft SMS. Use the Deployment Wizard to include the AccountServer and Group settings in the MSI. With these settings populated, you can specify that the Backup Account must be created automatically during the install process.

***Warning**: You are advised to install a Group Certificate to the specific Groups as the encryption keys are random. Without this certificate you will not be able to connect to a Backup Account to restore any data, should the computer crash. The password can be changed in the Storage Platform Console.*

Use the following command to run the installer (ensure that you have administrator privileges):

./BackupClientFileName.msi PREPACCOUNT=Yes

If you do not wish to use the preconfigured AccountServer and Backup Group details, you can use additional parameters to override the default settings configured:

- **SERVERIP** – IP address of the AccountServer
- **ACCOUNTNAME** – Backup Account name

  ***Note**: BackupVault will use the Windows Computer Name as the Backup Account name by default.*

- **ACCOUNTPASSWORD** – Backup Account password.

  ***Note**: If you do not specify an Account password, a random one will be used.*

- **CREATEKEY** – Backup Group Create Key
- **ACCOUNTKEY** – Backup Account encryption key.

  ***Note**: If you do not specify an encryption key, a random one will be used.*

- **GROUP** – Backup Group name

***Tip**: You can use Environment Variables to supply the parameters listed above.*

- *Type "set" in the command prompt to view a list of variables you can use.*
- *You can use these properties as fixed values or use templates based on the variables, for example:*

  ./BackupClientFileName.msi PREPACCOUNT=Yes ACCOUNTPASSWORD=%USERDOMAIN%

- *You can also use a combination of variables, for example:*

  ./BackupClientFileName.msi PREPACCOUNT=Yes ACCOUNTPASSWORD=%USERDOMAIN%\%USERNAME%

The standard MSI parameters are also available. A few examples are:

- /help – Help information
- /quiet – Quiet mode, no user interaction

- /passive – Unattended mode, progress bar only

***Example**: To deploy the Server Edition Backup Client, run the following with administrator privileges:*

*...\A5BPSE5.0.msi **PREPACCOUNT**=YES **SERVERIP**=SERVERNAME **GROUP**=COLLECTION01\GROUP01 **CREATEKEY**=KEY021 /passive /quiet*

7: Reports

Reports view

In the Reports view, you can administer the following:

- Enterprise Reports
- Standard Reports

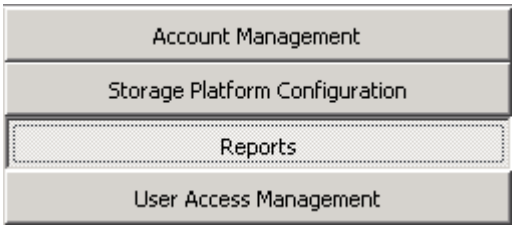
You can manually run reports at any point in time or schedule that they be emailed automatically.

***Note**:*

- *Enterprise Reports are installed by default and can be used by any Admin user.*
- *If you do not see the Standard section in the left-hand pane, it is not installed and/or activated. Please contact your Service Provider for additional information.*
- *Report logging is displayed in the Storage Platform Diagnostics area.*

To access the Reports view:

1. Open the SP Console and connect to the Storage Platform. [See Chapter 5, “Graphical User Interface (GUI)”.]
2. In the view selector on the left of the SP Console, click the **Reports** button.



Reports view icon legend

Icon	Location	Description
	Reports tree	Enterprise Reports node
	Reports tree	Standard Reports node
	Reports tree – Enterprise node	Enterprise report
	Reports tree – Standard node	Enabled report
	Reports tree – Standard node	Disabled report

Enterprise Reports

The Enterprise ReportServer collects information from the AccountServer at predefined intervals and populates it into an ODBC-enabled database. This database can be queried using the Enterprise Reports.

***Note**:*

- *The Enterprise Reports feature will only be available in the SP Console once it has been licenced. To acquire a licence, please contact your software provider.*
- *This User Manual describes how to work with existing SP Console reports. For information on creating new reports and advanced report editing, please refer to the BackupVault Enterprise Reports User Manual.*
- *Normal database management needs to occur to ensure correct report functionality.*

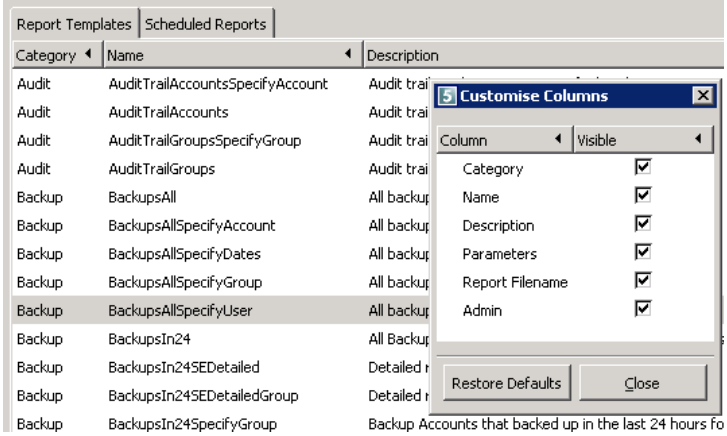
An extensive range of report templates are available in the SP Console and displayed on the **Report Templates** tab in the work area when the **Enterprise** node is selected. These templates are grouped into nodes in the Reports tree, according to their functionality:

- **Audit** – Various audit trail reports to track user access and Storage Platform changes at Group and Account level.
- **Backup** – Backup reports include all backups for a specified period/Group/Account, detailed Server Edition (SE and ESE included) reports and the ability to highlight backups that did not backup in the last 24 hours.
- **HSM** – Reports include the Account name, roll-up date and the size and number of files.
- **Licence** – Information on Storage Platform, Backup Groups and Backup Accounts level.
- **Mirror** – Reports include Mirror due, all mirrors done for the previous month, all mirrors due for the current month, and mirroring information for the current month.
- **Other** – Includes a range of reports from the Backup Account and group summaries to capacity, roll-ups and success reports.
- **Restore** – Provides information about all restores for the current and previous month.

***Tip**: For information on creating new categories and reports, please refer to the BackupVault Enterprise Reports User Manual.*

Modifying the display settings

When either the **Enterprise** node or a sub-category is selected, the **Report Templates** tab displays a list of reports and their properties. You can select the property columns you wish to display/hide using the **Customise Columns** dialog box.



To show/hide property columns in the work area:

1. Click the **Customise Columns** button on the toolbar.
2. In the **Customise Columns** dialog box that appears, specify which columns you wish to display by selecting the check boxes next to the column names.
3. Clear the check boxes next to the names of any columns you wish to hide.
4. Click **Close**.

***Tip**: Click the **Refresh** button on the main toolbar option to refresh the Reports view.*

ReportServer properties

In some circumstances, you may wish to change the SP Console's ReportServer URL reference.

***Example**:*

- *If your AccountServer (which includes your ReportServer) is behind a firewall and the IP address is translated from public to private (NAT), you would need to configure the SP Console to use the public IP address or host name.*
- *You may wish to view your reports over a secure connection. To do this, you would need to change the SP Console's ReportServer IP address reference to begin with "https://" instead of "http://". Please note that to do this, you need to install the Root Certificates in your browser to prevent it warning you about the SP certificate every time you try to view a report.*

To change the ReportServer URL reference:

1. Click the **Enterprise** node in the Reports tree and then click the **Configure** button on the toolbar. Alternatively, double-click the **Enterprise** node.
2. In the **ReportServer properties** dialog box that appears, modify the ReportServer URL field as required.
3. Click **OK** to save the changes or **Cancel** to exit the window.

In cases where you wish to view your reports over a secure connection, you should install Root Certificates in your browser to prevent it warning you about the SP certificate every time you try to view a report. The certificates are added to your computer's trusted root certificates.

To install Root Certificates:

1. In the **ReportServer properties** dialog box, click the **Install Root Certificates** button.
2. In the **Security Warning** dialog box that appears, click **Yes**.

Another modifiable ReportServer property is the report retention period. You can specify how long the ReportServer will keep reports before deleting them.

To modify the report retention period:

1. Click the **Enterprise** node in the Reports tree and then click the **Configure** button on the toolbar. Alternatively, double-click the **Enterprise** node.
2. In the **ReportServer properties** dialog box that appears, specify how long the ReportServer should store reports before deleting them (the retention period is enabled by default and set to 60 days.) Modify the settings as required.
3. Click **OK** to save the changes or **Cancel** to exit the window.

Running vs. scheduling reports

In the Reports view, you can run a report manually at any time or schedule reports to run at particular times.

To run a report manually:

1. In the Reports tree, click the report template type.
2. In the work area, right-click the report name and then click **Show report**. Alternatively, double-click the report name.

The report will open in your default Internet browser. You can also schedule reports to be emailed automatically. See below.

To create a scheduled report:

1. Click the **Schedule Report** button on the toolbar.
2. The wizard will prompt for the report category and report template to be used, if you did not select a particular report before clicking the **Schedule Report** toolbar button.
3. Provide a name and description for this report, and then click **Next**.
4. Specify the delivery schedule.
5. Specify the delivery options. Use the **Add** button to specify the email addresses to which the reports must be emailed. Multiple email addresses must be separated with a semicolon.

***Tip**: Scheduled reports are displayed in the **Scheduled Reports** tab in the work area. The schedule of existing reports may be modified by clicking the **Configure** button on the main toolbar and can be removed by clicking the **Delete** button*

Standard Reports

The following reports can be emailed to one or more specified email addresses automatically, notifying the recipient(s) of certain activities on the Storage Platform:

- **Overview Report** – This report enables you to receive an overview of all activities on the Storage Platform. Information includes Account Information, Backup Status, Mirror Status and Usage Status. Any Backup Account issues will also be highlighted in the report.
- **Licence Report** – This CSV file reports on all licences allocated in the Storage Platform, sorted by Group.
- **StorageServer Disk Space Report** – This report will give you an indication of how much hard disk space is used and available on the StorageServer.
- **Mirror Report** – This is a notification message that will be sent to you after mirroring was completed successfully. Information includes the mirror duration, the number of Backup Accounts mirrored and the amount of data that was transferred.
- **Storage Platform Expiry Report** – You can configure this to notify you a certain number of days before the Storage Platform expires.
- **Group Expiry Report** – This is a notification message that will be sent to you before any of the Storage Platform Groups expire.
- **StorageServer Down Report** – This is a notification message that will be sent to you when the AccountServer cannot communicate with the StorageServer.

Before you can enable these reports, you must supply valid SMTP settings that will be used when the reports are emailed.

To configure SMTP settings:

1. Click the **Standard** node in the left-hand pane and then click the **Configure** button on the toolbar. Alternatively, right-click the node and then click **Configure** on the shortcut menu that appears.
2. Type the host and port numbers in the boxes provided.
3. Select **Use secure connection (STARTTLS)** to establish a secure connection to an online mail service like Gmail.
4. If the server requires authentication, select the **Server requires authentication** check box and then type the username and password details in the boxes provided.
5. Click the **Test SMTP** button to ensure that the details are correct.
6. If successful, click **OK**.

To enable a report:

1. Select the report name in the left-hand pane and then click the **Configure** button in the toolbar. You can also double-click the report entry.
2. Select the **Enable this report** check box.
3. Supply the required Report Configuration settings. You can enter multiple email addresses in the **To** box by separating them with commas.

***Note**: The **BillingReport.csv** file is automatically attached to the Licence Report and includes the Storage Platform licence information, specified per group.*

4. In the Report SyncSchedule area, specify when you would like to email the reports by entering a date in the box provided or by selecting a particular email frequency.
5. Use the **Email this report now** button to send the report manually (you may wish to do this to verify that all settings are correct or if you only want to run the report once).

***Tip**: The Storage Platform Console Diagnostics area will display the necessary logging information.*