



The SyncBack Management System

An Introduction to the SyncBack Management System

The purpose of the [SyncBack Management System](#) is designed to manage and monitor multiple remote installations of SyncBackPro V8. The SBMS allows you to:

- Limit what users can do with SyncBackPro, e.g. stop users from creating their own profiles.
- Track which profiles are being run, their results and their run history.
- Remotely manage SyncBackPro profiles.

The SyncBack Management Service is installed as a Windows Service, runs in the background, and provides services to remote clients.

The SBM Console is for administrators to configure the SBM Service, e.g. adding users, checking the profiles results, etc.

Communication with the SBM Service is via HTTP, TCP/IP, so it can be used over the Internet or via a Local Area Network. All communication is encrypted and access is restricted by using usernames and passwords.

There are two client applications: the SyncBack Management Console (installed on one machine used by the manager) and SyncBackPro (installed on many machines).

Working together, the SBM Service (installed on the server), SBM Console, and SyncBackPro complete the SyncBack Management System.

An Overview of How the SyncBack Management System Works

In order to manage and monitor remote installations of SyncBackPro using SyncBack Management System, you will need to install three software programs (or software that installs as a service):

- SyncBack Management Service (SBM Service)
- SyncBack Management Console (SBM Console)
- SyncBackPro backup and synchronization software

Note that the first two (SBM Service + SBM Console) makes up SBM System.

First, install SBM Service on a Windows server in your network. This could be any server that is accessible/connectable by all desktop clients in your office network (or through VPN, etc).

Next, install the SyncBack Management Console (SBM Console) so that you can configure and manage the SBM Service. It should be noted that during the initial SBM System setup, you need to install the SBM Console on the same computer/server as the SBM Service in order for SBM Console to connect with SBM Service through localhost; the SBM Service will not accept external connections other than the local computer. This is for security reasons. You can choose to install SBM Console on another computer only after you have configured the IP addresses/hostnames as described in **Step 2C**.

The SBM Console is used by the System Administrator in charge of managing the office backups through the SBM System, thus it is recommended that the SBM Console be installed on a machine that the administrator will have access to (**after Step 2C configuration**). The SBM Console can either be installed in the same server where the SBM Service is located, or it can be installed on any Windows computer system that is connectable to the SBM Service via the network (for example, the Administrator's PC for easier administration).

If you have not already done so, a copy of SyncBackPro software have to be installed on each of the Windows PC/laptop systems that you want monitored/managed using SBM System.

Lastly, configuration and setup on the SBM Console is required. This is detailed in the steps outlined below in this document. Once the SBM Console is configured, you will need to set up SyncBackPro so that it can connect with the SBM Service over the network and so that you can upload/update SyncBackPro profiles as well as uploading histories of past profiles run by all managed SyncBackPro clients to the central location.

Operating System Requirements

All three applications in the SyncBack Management System (the SBM Service, the SBM Console, and SyncBackPro) require either Windows Vista, 7, 8, 10 or newer or Windows Server 2003, 2008, 2012, 2016 or newer.

Both 32-bit and 64-bit versions of Windows are supported.



The SyncBack Management System: A Case Study

To ensure the security of data all communication in the SBM System is encrypted.

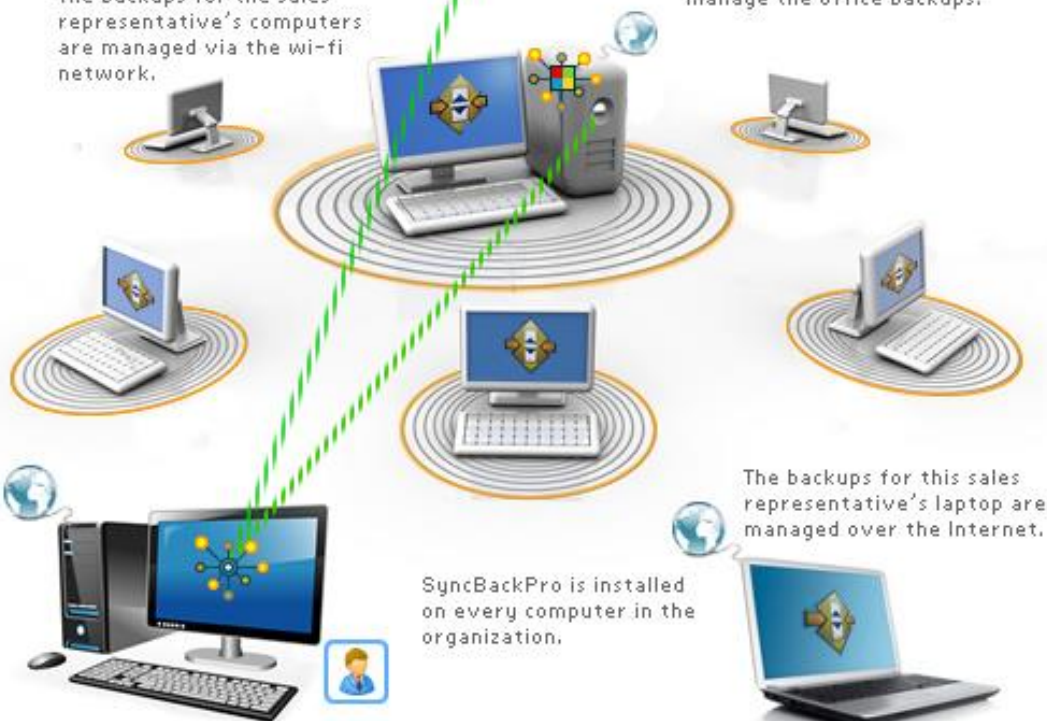
Office Network

The office computers are managed via a cable network.



Sales Network

The backups for the sales representative's computers are managed via the wi-fi network.



The Office System Administrator uses the SBM Console to connect to the office SBM Service to manage the office backups.

The backups for this sales representative's laptop are managed over the Internet.

SyncBackPro is installed on every computer in the organization.

In this example the Chief System Administrator is connected to the Internet and uses the SBM Console from a different location to manage both the office and sales backups.



SyncBackPro



SBM Service



SBM Console



Administrator



Cable Network



Wi Fi Network



Internet Connection

The SBMS Setup Guide

Follow the step by step guide below to prepare the SyncBack Management System for deployment.

Step 1 – Install the SyncBack Management Service (SBM Service)

The SBM Service will be installed as a Windows service. You can download and install the latest version of SBM Service here:

http://www.2brightsparks.com/assets/software/SBMService_Setup.exe

Install the SBM Service on a server within your network environment. This server must be accessible by all SyncBackPro client machines in your network.

Step 2 – Install SyncBack Management Console (SBM Console)

Download the latest version of SyncBack Management Console here:

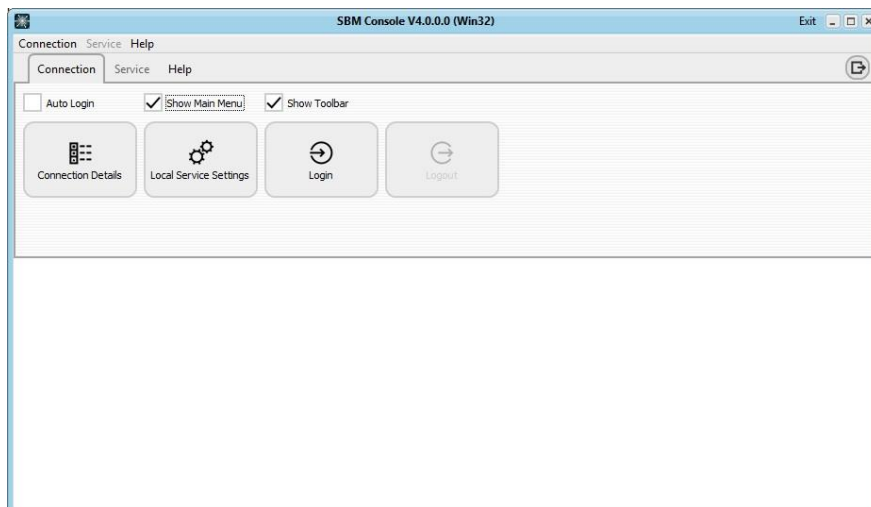
http://www.2brightsparks.com/assets/software/SBMConsole_Setup.exe

For the initial SBMS setup, install the SBM Console on the same machine that the SBM Service is located (for security reasons). The administrator can choose to install SBM Console on another machine after configuring **Step 2C**.

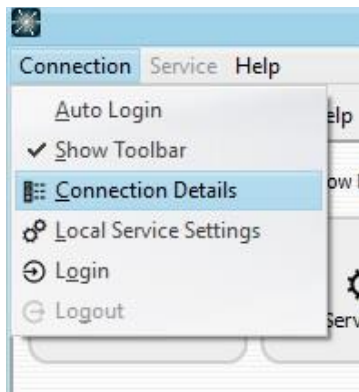
Please note that you must first install the SBM Service first before launching the SBM Console.

Step 2a - Setup and Configuring the SBM Console (First Steps)

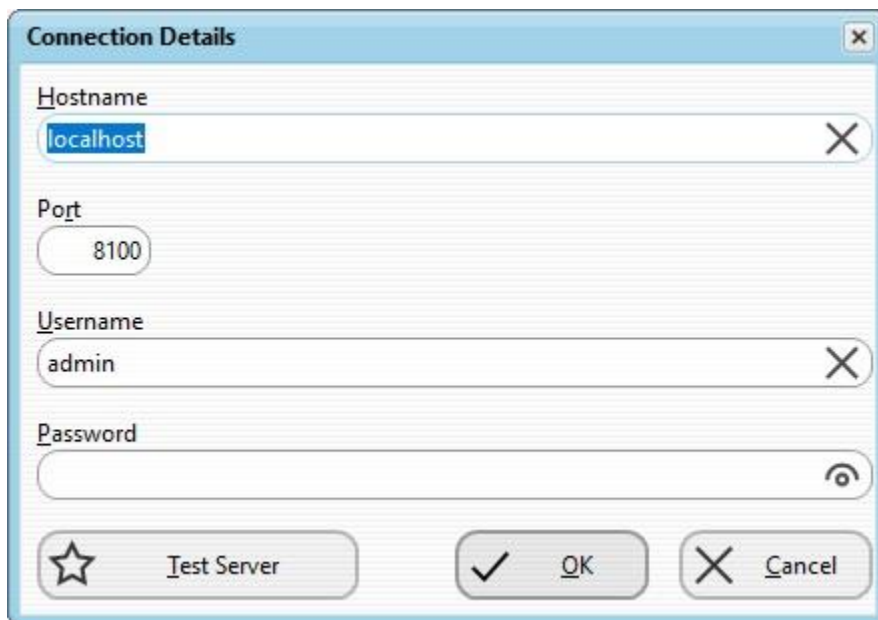
Launch the SBM Console (after installing the SBM Service).



Select the **Connection** menu and click on **Connection Details**:



The **Connection Details** window will appear:



Change the following fields as shown (by default they should already be set to these values):

Hostname – localhost

Port – 8100

Username – admin

Password - Leave this blank

Click on **Test Server** and you will hopefully see the **Success** message:



Click the **OK** button to save these settings.

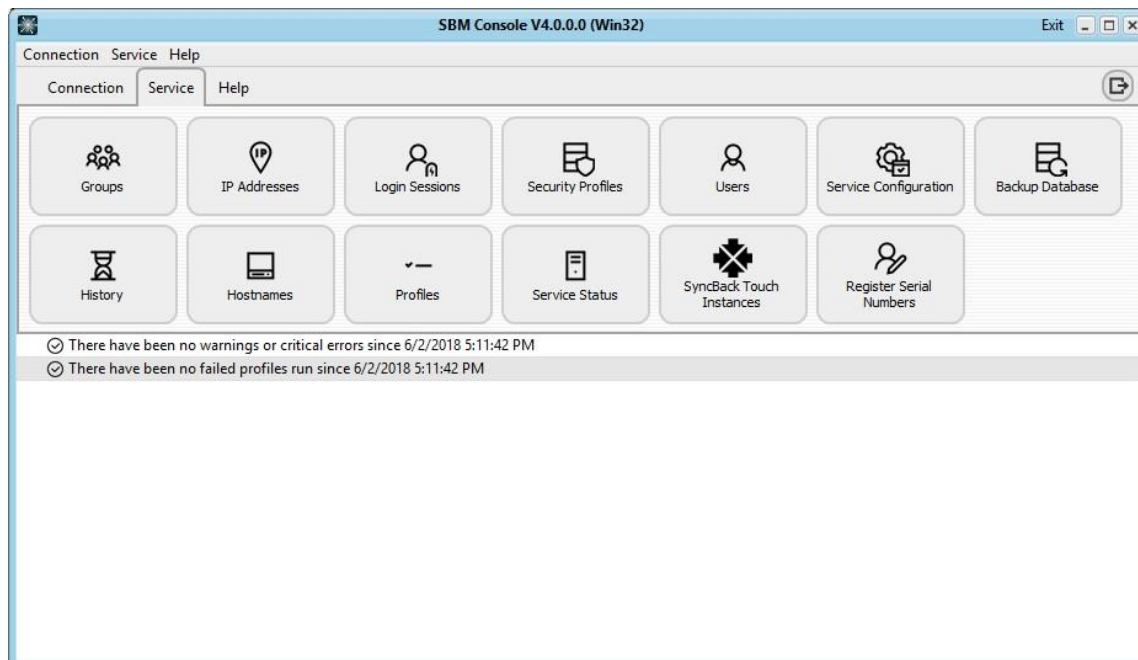
If the test connection failed, double-check to make sure the SBM Service is running. If so, double-check the connection details to make sure there are no typos.

If the connection details are correct then go to the Local Service Settings window to make sure that the connection settings on the server are as expected. You can also use any web browser to see the status of the service. Simply navigate to <http://localhost:8100/STATUS> where localhost is the hostname or IP address of the server running the SBM Service (if you're using the browser on the same computer then you can use localhost) and 8100 is the port number you've set (8100 is the default).

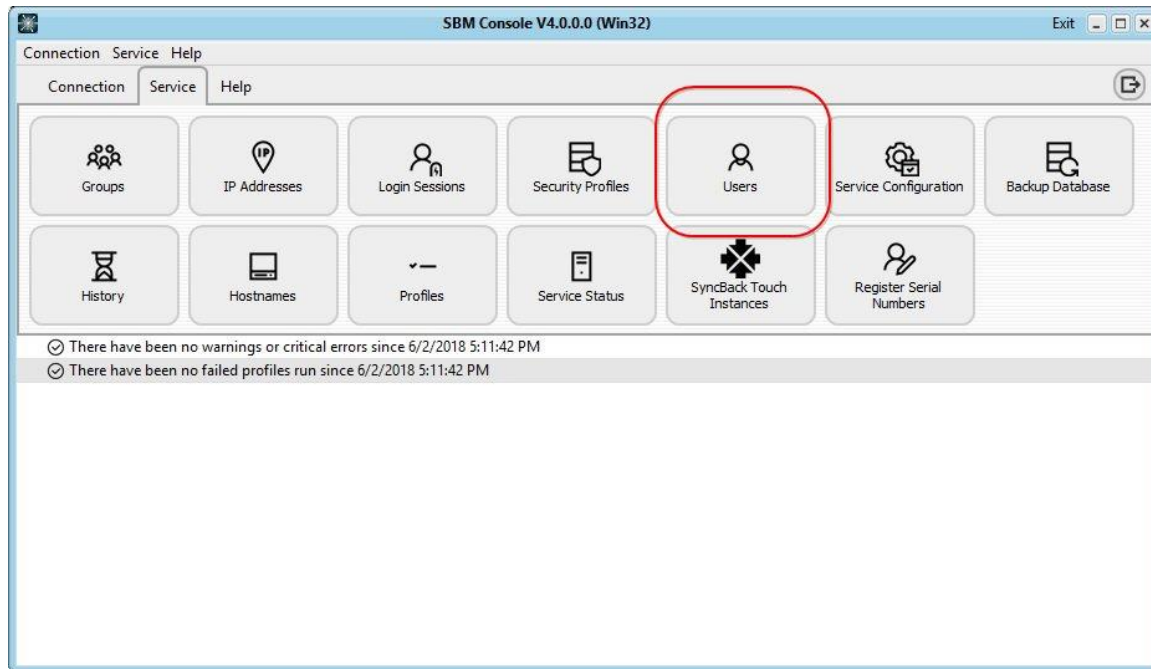
For more information on the Connection Details window, please refer to

SBM Console Help File > Using the SBM Console > Connection > Connection Details

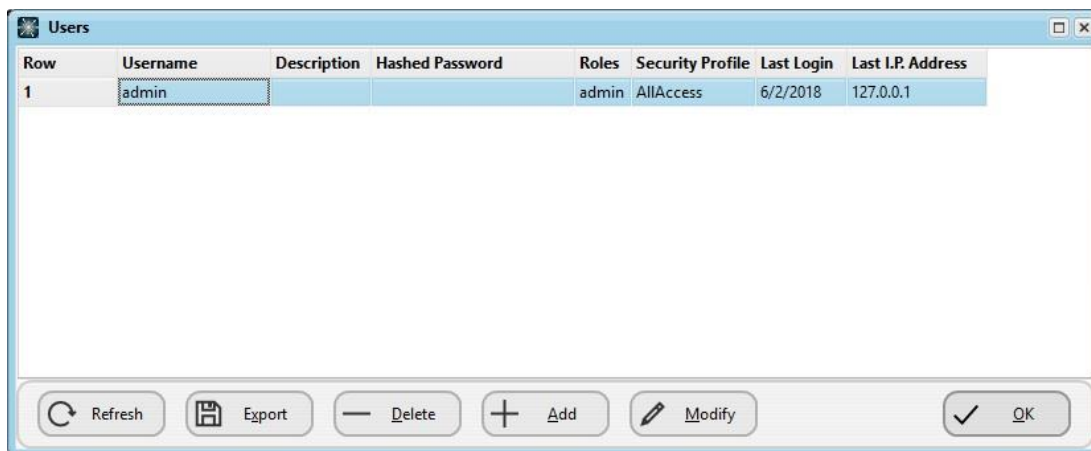
From the **Connection** tab in the SBM Console select **Login**. The console will display messages similar to the following:



Before continuing you should change the default user admin's password by selecting the **Users** option from the **Service** tab:

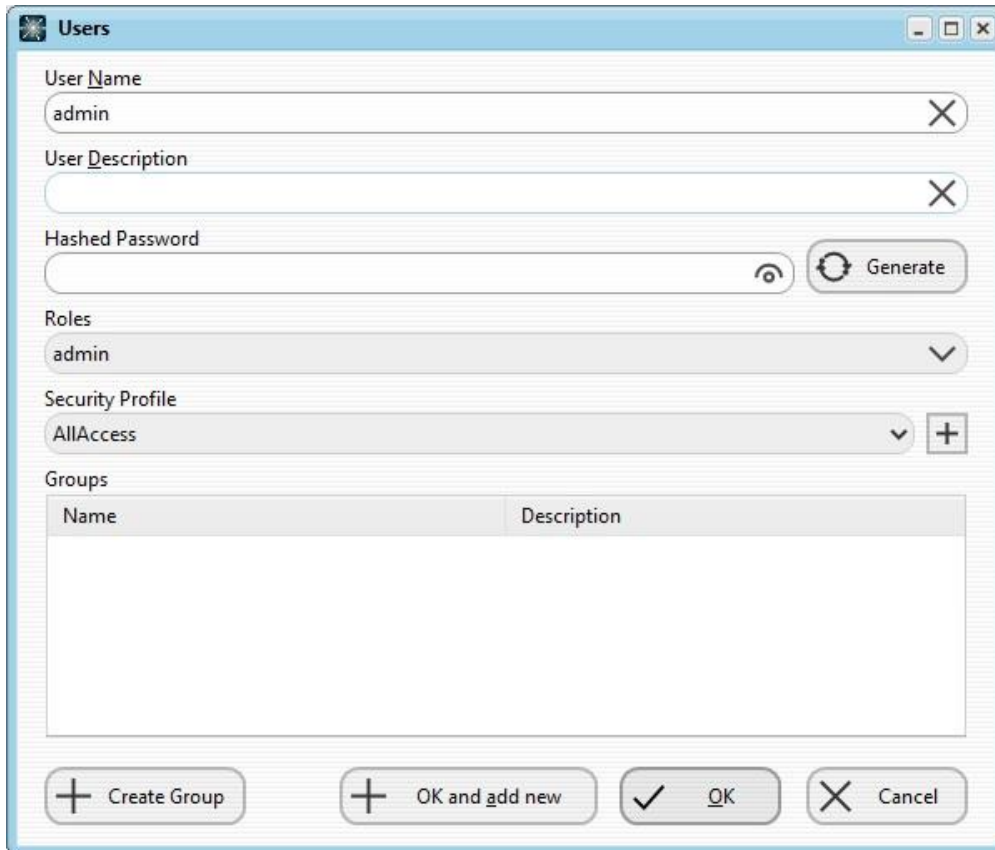


The following User's window will open:



Note that the default user above is defined as **admin** and has no password.

Click on the **Modify** button to add a password to the admin user:



The screenshot shows a 'Users' dialog box with the following fields and controls:

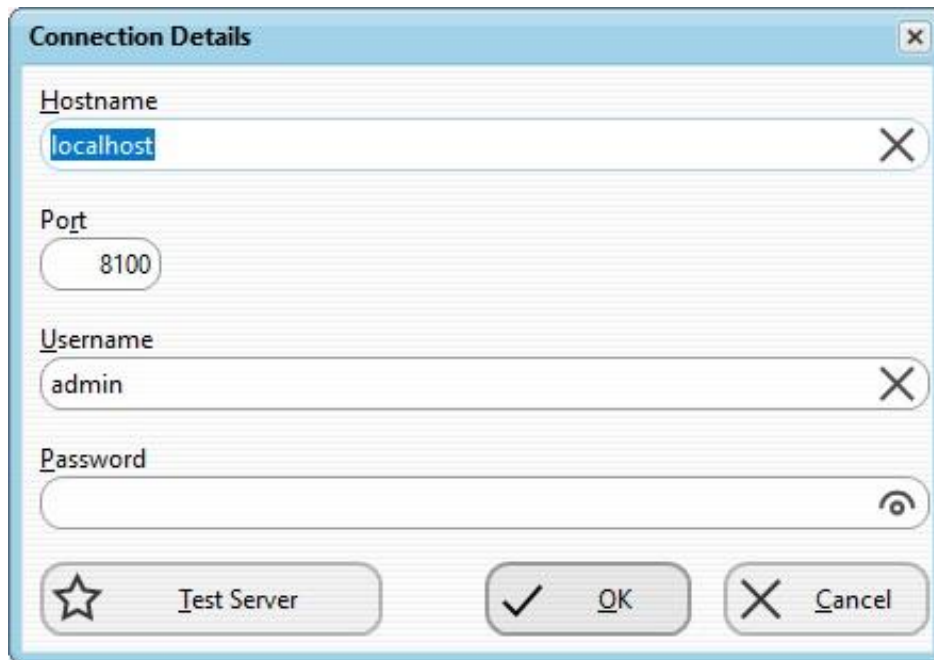
- User Name:** Text field containing 'admin'.
- User Description:** Text field.
- Hashed Password:** Text field with a 'Generate' button and a toggle icon.
- Roles:** Dropdown menu showing 'admin'.
- Security Profile:** Dropdown menu showing 'AllAccess'.
- Groups:** A table with columns 'Name' and 'Description'.
- Buttons:** '+ Create Group', '+ OK and add new', '✓ OK', and '✗ Cancel'.

Edit the password field and enter a password.

Important: Ensure you make a record of your password and keep it somewhere secure. If you are saving the password to disk ensure it is encrypted. If you forget your administration password you will need to reinstall the SBM Console all over again!

Once you have decided on a password and are able to recall it easily click the **OK** button.

Now reset the connection details by opening the **Connection Details** form:



The screenshot shows a 'Connection Details' dialog box with the following fields and controls:

- Hostname:** A text field containing 'localhost' with a blue highlight and a close button (X) on the right.
- Port:** A text field containing '8100'.
- Username:** A text field containing 'admin' with a close button (X) on the right.
- Password:** An empty text field with a visibility toggle icon (an eye) on the right.
- Buttons:** At the bottom, there are three buttons: 'Test Server' (with a star icon), 'OK' (with a checkmark icon), and 'Cancel' (with an X icon).

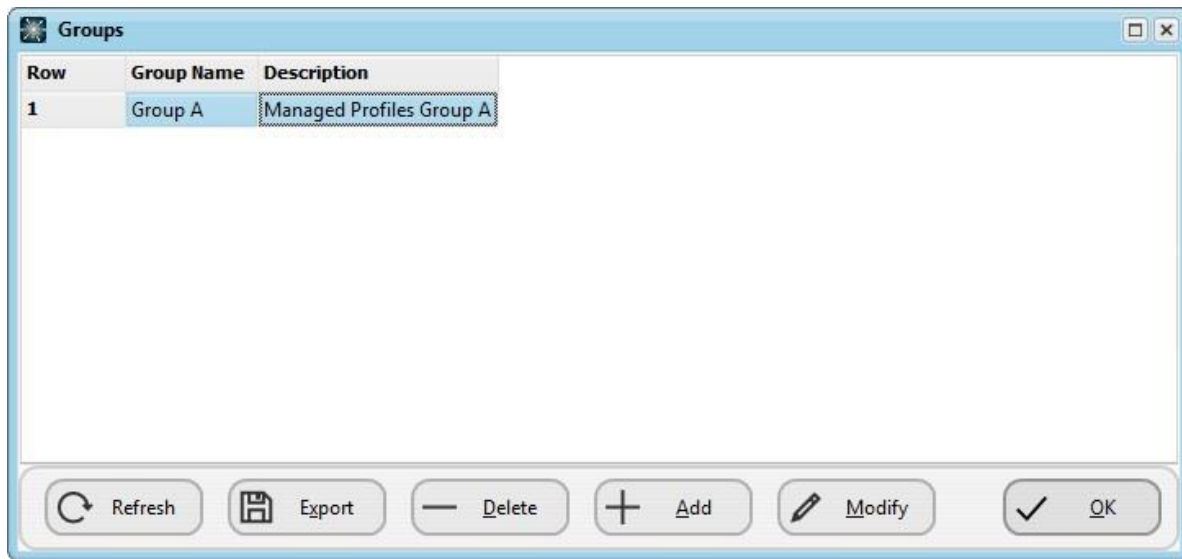
In the **Password** field enter the password you added earlier to the admin user, and before saving the change, select the **Test Server** button to confirm that you can login with the new password.

Click the **OK** button.

Logout by selecting **Logout** on the **Connection** menu and then log back in again via the **Login** menu option in the Connection menu.

The SBM Console is now ready for use. However, it will only allow local connections, i.e. connections from the same computer that the SBM Service is installed on. To change this see the **IP addresses/Hostnames** section.

Step 2b – Configuring Groups in the SBM Console (Service tab > Groups)



Defining group membership within the SBM Console allows the administrator to determine which users are able to access certain profiles.

For example, you can create a Group called Finance. Users allocated to this Finance Group would be able to access profiles with a custom configuration (to backup only the “Financial” database for example).

A second example: If you want all the client’s machine in the organization to start a backup every morning, and only the staff in the Sales department to have incremental backups. You can do that by assigning the corresponding user accounts and profiles to the respective Groups.

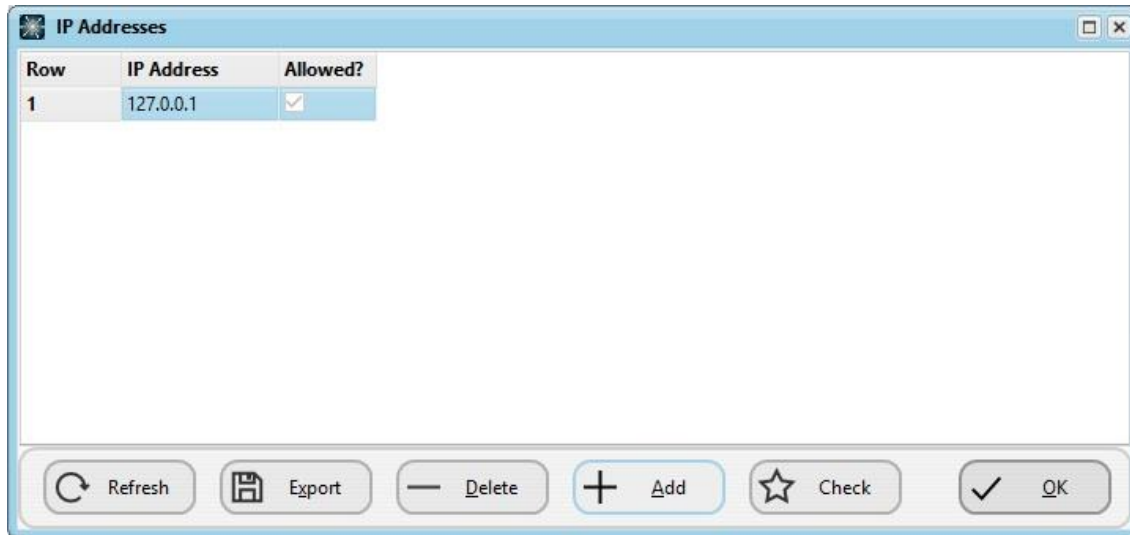
In order to allow users access to run a specific managed profile, you will need to

- Create a Group
- Add users to this Group so that they are a member
- Add profiles to this Group so that they are a member of the same group

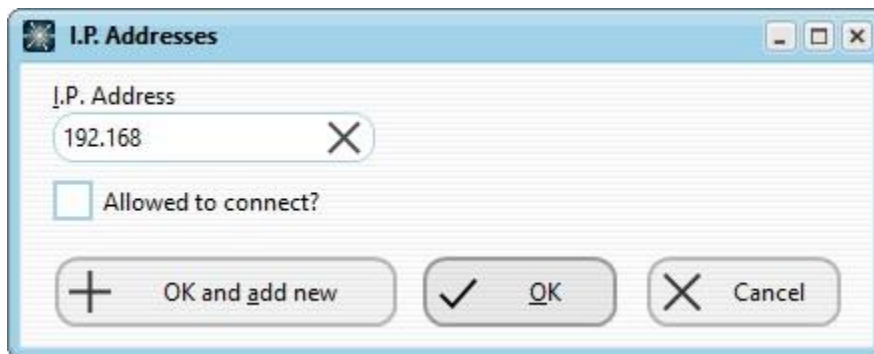
For more information on configuring Groups, please refer to the Groups section in the SBM Console Help file.

Step 2c – Configuring IP Addresses or Hostnames in SBM Console (Service tab > IP Addresses/Hostnames)

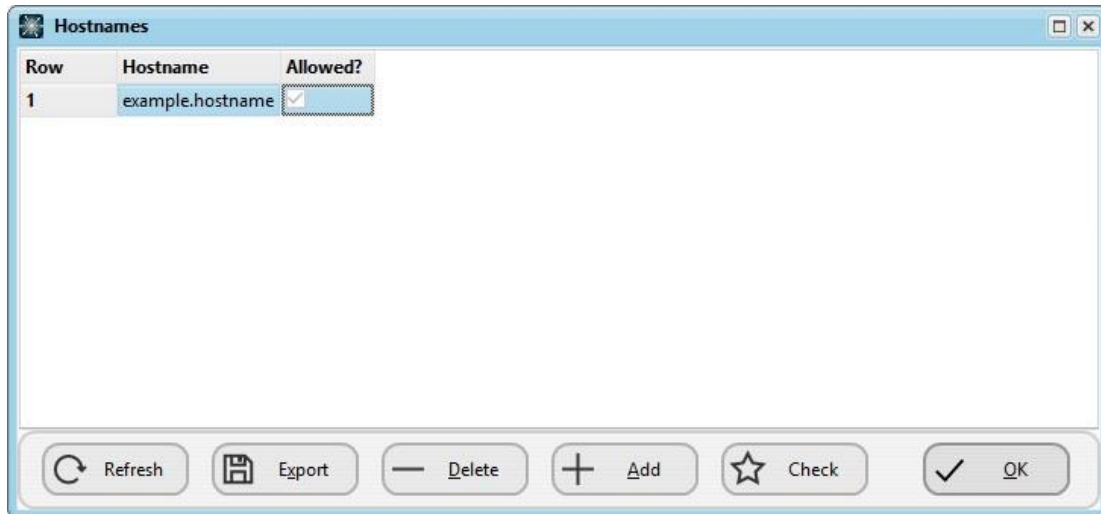
In the SBM Console, you will need to specify either the **IP Address** or the **Hostnames** of machines within these sections in order for such machines to be connectable to the server. By default, there is only one record in IP Address/Hostname table, which is the localhost or current machine.



IP Address: - You can add a portion of the IP address, for example – entering *192.168* will allow all IP addresses starting with *192.168* to connect to the server. You can also use an asterisk (*) to allow all IP addresses to connect.

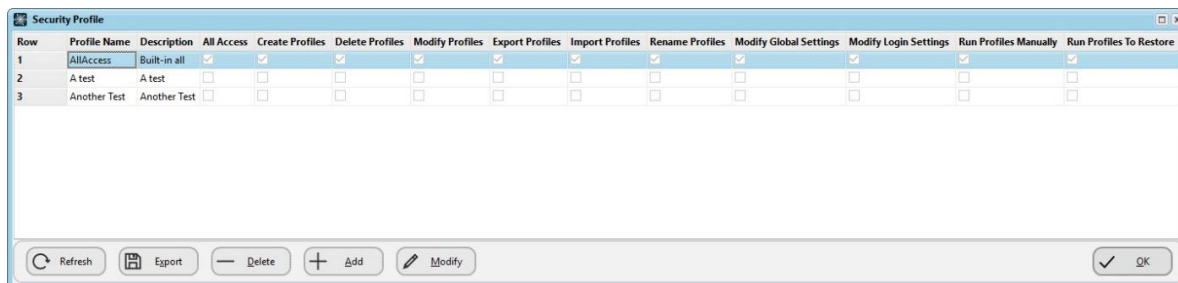


Hostnames: - In common with IP addresses, you can enter a portion of the Hostname, for example - instead of entering myserver.com, you can enter *mys* so that any hostname starting with *mys* will be allowed to connect. You can also use asterisk (*) to allow all IP addresses to connect.



For more information on configuring IP Addresses and/or Hostnames, please refer to the respective section in the SBM Console Help file.

Step 2d – Configuring Security Profiles (Service tab > Security Profiles)



Every user should have a Security Profile. The Security Profile defines what the SyncBackPro user can do. For example, you can assign All Access security profiles to administrator accounts, and assign the security profile rights to manually run profiles on end-user accounts so that they can only run the profiles, etc.

Security Profiles

Name: AllAccess

Description: Built-in all access security profile

- ☒ All access?
- ☒ Can create profiles?
- ☒ Can delete profiles?
- ☒ Can modify profiles?
- ☒ Can export profiles?
- ☒ Can import profiles?
- ☒ Can rename profiles?
- ☒ Can modify global settings?
- ☒ Can modify login settings?
- ☒ Can run profiles manually?
- ☒ Can run profiles to restore?

Buttons: + OK and add new, ✓ OK, ✗ Cancel

For more information on configuring Security Profiles, please refer to the Security Profiles section in the SBM Console Help file.

Step 2e – Configuring Users in the SBM Console (Service tab > Users)

Row	Username	Description	Hashed Password	Roles	Security Profile	Last Login	Last I.P. Address
1	admin			admin	AllAccess	6/2/2018	127.0.0.1

Buttons: Refresh, Export, Delete, Add, Modify, ✓ OK

It is compulsory to create an entry in this section for each user who requires login rights to the system.

Please note that these user accounts are independent from the Users in Active Directory - **they are not the same**. User accounts created here are only meant to be used in the SBMS environment.

Roles refer to the security roles used by the system. At present only one role is defined: admin. Some functions, e.g. to delete history, a user must be a member of that role otherwise they will not be able to perform the associated function.

The screenshot shows the 'Users' configuration window. It includes fields for 'User Name' (Desmond), 'User Description', and 'Password'. There is a 'Generate' button for the password. Below these are dropdowns for 'Roles' and 'Security Profile'. A 'Groups' table is at the bottom, listing 'Group A' with the description 'Managed Profiles Group A'. At the bottom of the window are buttons for 'Create Group', 'OK and add new', 'OK', and 'Cancel'.

Name	Description
<input type="checkbox"/> Group A	Managed Profiles Group A

For more information on configuring Users, please refer to the Users section in the SBM Console Help file.

Step 3 – Install SyncBackPro on each client machine / Setup and Configure Profiles

If you have not already done so, install SyncBackPro on each of your office end-user's machines that you want backed up and monitored.

Download the latest version of SyncBackPro here:

(32-bit) http://www.2brightsparks.com/assets/software/SyncBackProV8_Setup.exe

(64-bit) http://www.2brightsparks.com/assets/software/SyncBackProV864_Setup.exe

Note - The administrator can create installation executables using command line parameters to distribute the program silently to client machines within the organization. It is also possible to create custom command line strings to configure the SBMS settings during installation using this model. Details are available here:

<http://support.2brightsparks.com/knowledgebase/articles/213973-install-syncbackfree-se-pro-no-prompts>

Please note that we only provide the instructions to compose the command line string. It is your administrator's responsibility to create scripts/batch files of any appropriate commands, before they distribute them to the various departments/groups and/or end-user machines.

Next, nominate/designate one of the client's machines (for example, it can be the administrator's PC) as the 'Master' where you will then create and configure 'master' copies of profiles that will eventually be uploaded to the SBM Service at a later stage. These managed profiles will be downloaded by other installations of SyncBackPro in your network, provided they are in the correct group (more details are provided about this in **Step 5** below).

Further instructions on configuring the various settings in SyncBackPro are available in the Help file of the program. Access SyncBackPro's Help file by pressing F1 when using the program's main interface opened. You can also refer to the online tutorial here:

<http://www.2brightsparks.com/syncback/help/index.html#welcome.htm>

Step 4 – Connecting to SBM Service using SyncBackPro

To connect to the SBM Service, it is required to set up the connection details on each SyncBackPro program that is installed on every end-user's machine.

Note – You can skip this step if you have already configured these SBMS settings during the deployment of SyncBackPro via silent installs as per **Step 3**.

From SyncBackPro, select the **Preferences** menu > **Management Service Settings**

Hostname: - This is the hostname of the SBM Service that you want to connect to. Simply enter the hostname or IP address, e.g. **myserver.com**

Port: - The port number of the SBM Service (Default port number is 8100)

Username: - The login username for the SBM Service. You must have a username to login to the SBM Service. User accounts have to be first created from SBM Console (**Service menu > Users**)

Password: - The login password of this user account for the SBM Service.

To test the settings click the **Test Server** button. SyncBackPro will then attempt to connect and login to the SBM Service.

Once these settings have been set (and validated) you will need to use an account with administrative rights to change them. If not then the settings will be read-only. To change the settings click the **Modify** button and enter the administrator's username and password.

Step 5 – Uploading a Profile to the SBM Service using SyncBackPro

In order for the SBM Service to start distributing profiles to all SyncBackPro installations, you will first need to upload a 'master' copy of a profile from a designated machine.

To upload profiles to the SBM Service, first select the profile to upload in SyncBackPro, then select **Profiles > Upload Profile to SBM Service**. Optionally right-click on the profile and select **Upload Profile to SBM Service** from the pop-up menu.

You can only upload profiles if you are an administrator. You must enter a description for the profile and then specify if the schedule for the profile should also be exported.

After the profile has been uploaded a message will be displayed giving the unique GUID for the profile. This is for information purposes only so that when you edit the profile's details using the SBM Console you can check to make sure that the profile is the same one you uploaded. Every profile has a universally unique GUID.

Important: Once a profile has been uploaded you must use the **SBM Console** to assign the profile to one or more groups so that this 'master' profile can be distributed to the rest of the accounts within those groups. If you are updating an existing profile then the profile will still be in the same groups as it was before the update – in other words, there is no need to re-assign the updated profile to those groups again.

Managed Profiles

Every hour a check is made to see if there are any new or updated managed profiles. The system also checks to see if any managed profiles should be deleted. If so they are downloaded from the SBM Service and installed, or deleted as necessary. This is only done when online. You can do an immediate check by pressing **Ctrl-F5**.

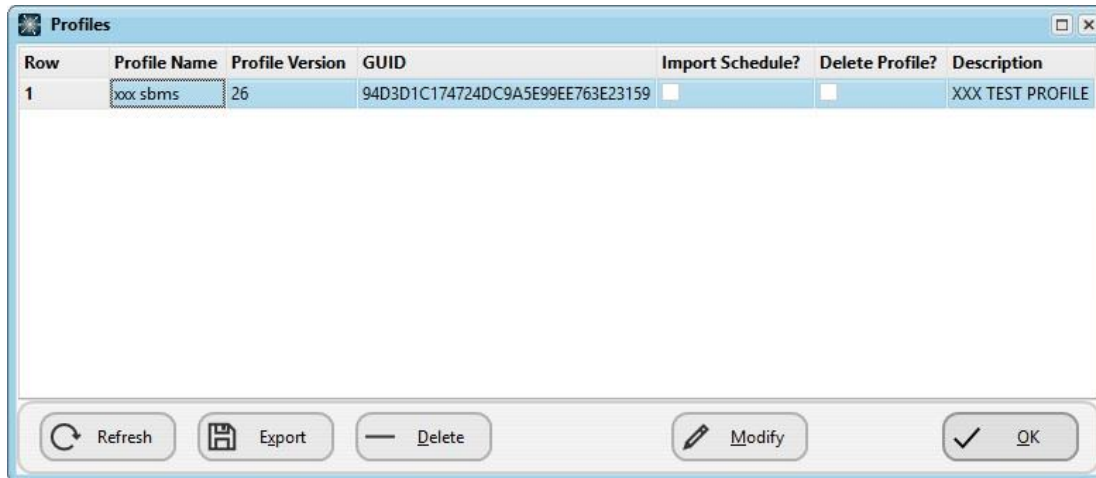
Offline

If SyncBackPro cannot connect to the SBM Service, e.g. there is no network connection, then it will proceed in offline mode. The window caption for SyncBackPro will show in offline mode. When in offline mode it will use the cached security settings (retrieved during the last online login) so that the user will still be restricted in what they can or cannot do. Any profile history created while in offline mode will be automatically and silently uploaded once SyncBackPro can connect to the SBM Service and it has been an hour or more since it last uploaded cached history. You can do an immediate upload by pressing **Ctrl-F5**.

Step 6 – Assigning Profiles to Groups from SBM Console (Service menu > Profiles)

Managed profiles are profiles created by and uploaded from SyncBackPro V8 and greater. They are neither created nor added to the database from the SBM Console.

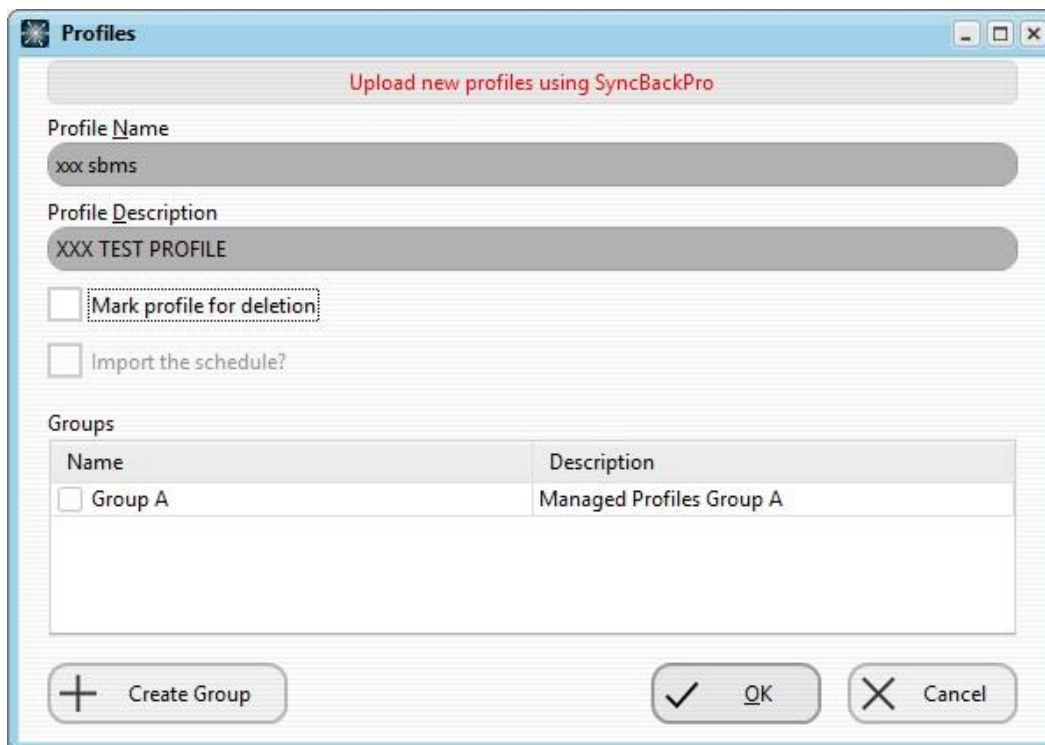
The profile window displays the profiles that have been uploaded to the SBM Service from SyncBackPro.



The screenshot shows a window titled "Profiles" with a table containing one row of profile data. The table has columns for Row, Profile Name, Profile Version, GUID, Import Schedule?, Delete Profile?, and Description. Below the table are buttons for Refresh, Export, Delete, Modify, and OK.

Row	Profile Name	Profile Version	GUID	Import Schedule?	Delete Profile?	Description
1	xxx sbms	26	94D3D1C174724DC9A5E99EE763E23159	<input type="checkbox"/>	<input type="checkbox"/>	XXX TEST PROFILE

Use the **Modify** button to Mark a profile for deletion or add the profile to a group.



The screenshot shows the "Profiles" window in a "Modify" mode. It features a red banner at the top that says "Upload new profiles using SyncBackPro". Below this are input fields for "Profile Name" (containing "xxx sbms") and "Profile Description" (containing "XXX TEST PROFILE"). There are two checkboxes: "Mark profile for deletion" and "Import the schedule?". Below these is a "Groups" section with a table showing a group named "Group A" with the description "Managed Profiles Group A". At the bottom, there is a "Create Group" button with a plus icon, and "OK" and "Cancel" buttons.

Upload new profiles using SyncBackPro

Profile Name: xxx sbms

Profile Description: XXX TEST PROFILE

☐ Mark profile for deletion

☐ Import the schedule?

Groups

Name	Description
<input type="checkbox"/> Group A	Managed Profiles Group A

+ Create Group ✓ OK ✗ Cancel

Note that it is not possible to modify the Profile Name and Profile Description.

Clicking on the **Create Group** button allows the creation of a new group without closing this screen while opening the Group form.

Click **OK** to accept the modifications or **Cancel** to discard them.

You can get more information by referring to the Profiles section in the SBM Console Help file.

Step 7 – Managing and Monitoring profiles History from SBM Console (Service menu > History)

When a profile is run the results are sent to the SBM Service. This allows administrators to keep track of which users are making backups and if they are failing.

SyncBackPro caches the history information locally in case a connection cannot be made to the remote SBM Service. Once a connection can be made it uploads the history.

New records are created and uploaded by SyncBackPro as and when profiles are run. The SBM Console can delete records but cannot modify them.

Row	Login Username	Profile	Profile Version	Part of Group?	Computer Name	Username	Thread Start Time	Profile Start Time	Group Start Time	Restore?	Profile Type
1	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	23/6/2017 4:16:30	23/6/2017 4:16:30		<input type="checkbox"/>	Backup
2	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	23/6/2017 4:16:01	23/6/2017 4:16:01		<input type="checkbox"/>	Backup
3	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 3:25:54	20/6/2017 3:25:54		<input type="checkbox"/>	Backup
4	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 3:25:08	20/6/2017 3:25:08		<input type="checkbox"/>	Backup
5	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 3:12:48	20/6/2017 3:12:48		<input type="checkbox"/>	Backup
6	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 3:00:37	20/6/2017 3:00:37		<input type="checkbox"/>	Backup
7	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 3:00:08	20/6/2017 3:00:08		<input type="checkbox"/>	Backup
8	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:51:44	20/6/2017 2:51:44		<input type="checkbox"/>	Backup
9	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:50:09	20/6/2017 2:50:09		<input type="checkbox"/>	Backup
10	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:47:37	20/6/2017 2:47:37		<input type="checkbox"/>	Backup
11	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:46:44	20/6/2017 2:46:44		<input type="checkbox"/>	Backup
12	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:44:50	20/6/2017 2:44:50		<input type="checkbox"/>	Backup
13	admin	amazon cloud drive	26		MICKSTOWER	MICKSTOW	20/6/2017 2:43:54	20/6/2017 2:43:55		<input type="checkbox"/>	Backup

For more information on configuring History, please refer to the History section in the SBM Console Help file.

Additional Questions Regarding the SBMS

If you require further assistance with setting up the SBMS, please check our Knowledge Base:

<http://support.2brightsparks.com/knowledgebase>

Our Knowledge Base contains hundreds of technical articles that are updated regularly, and you may also **Contact Support** using the online form so you may write to us about your issue. The Contact Support links to our ticketing system.

Please review this article for the information to include when submitting a Support Ticket.

<http://support.2brightsparks.com/knowledgebase/articles/230027-information-to-include-for-technical-support>

Support Policy

Please review our support policy which is available online:

<http://support.2brightsparks.com/knowledgebase/articles/196920-support-policy>

Each operating system and network are set up differently with a range of security protocols, privileges and access requirements that are specific to your organization's needs.

We qualify the scope of our support as there are, very occasionally, single licensees who require an unreasonable level of support that crosses the boundary into consultancy. We try our very best to be prompt with our responses, however our support is limited to ensuring our products perform appropriately, rather than advising on FTP servers, server infrastructure etc.

We do not offer phone or remote session support. Phone support and remote sessions tend by their nature to pressure people (us) into making snap decisions, whereas emails can be considered, mulled over and tweaked till we are sure what we do say is the best answer we can give. Sometimes 2BrightSparks will need to refer issues between the team to ensure accuracy and clarity. Direct email support gives all parties a handy written reference as to who said what.