

ABS Enterprise[®]

Installation Guide - StorageCraft

June 2014



Contents

Preamble	3
Installing the Backup Agent on Clients	4
Configuration of Windows Firewall on Clients	8
Accessing ABS Appliance®	12
Dropbox Folder Configuration	13
Configuring Clients on Appliance	15
Configure Image Manager	23
Offsite Replication Setup	28

Preamble

Operating Systems

- Windows 2012
- Windows 2008 R2
- Windows 2008 SP2
- Windows 2003 R2
- Windows 2003 SP2
- Windows 2000 SP4
- Windows SBS 2011/2008/2003
- Windows 8/7/Vista/XP SP3

Notes

- 1Gb network strongly recommended
- ReFS Partitions are not supported
- A reboot is required after agent installation
- Storage Spaces are not supported

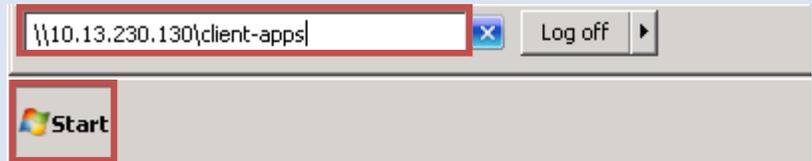
Definitions/Abbreviations:

- **AD** = Active Directory Users and Computers
- **OU** = Organizational Unit
- **Appliance** = ABS onsite device
- **Agent** = Computer being protected (i.e. server/workstation)

Installing the Backup Agent on Clients

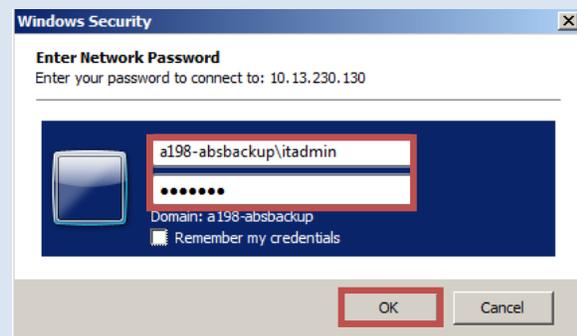
1. Access the Agent

- From the client, click the **Start** button
- Enter in the share path in the search field



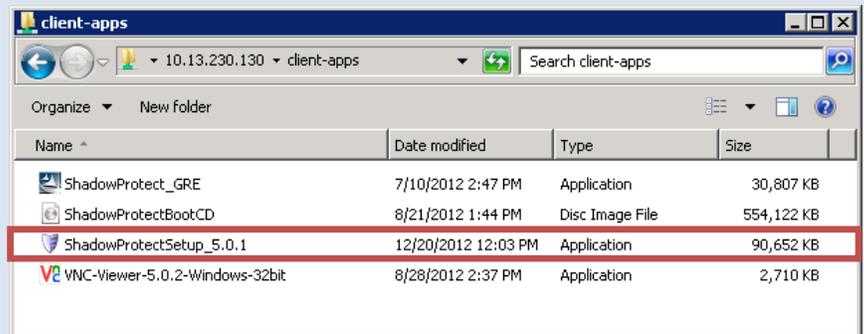
i Share path example:
\\10.13.230.130\client-apps
Substitute example IP address with the IP address that was set on the appliance

- Enter in the **itadmin** account credentials (refer to your **Activation Letter** for the password)



i When authenticating against the appliance, make sure to add the appliance name before the username. Example:
a198-absbackup\itadmin

- It is recommended to copy **ShadowProtectSetup_.exe** to a local directory on the client, but is not required



2. Install the Agent

- Double Click the agent installer:
ShadowProtect_.exe
- Click **Run**



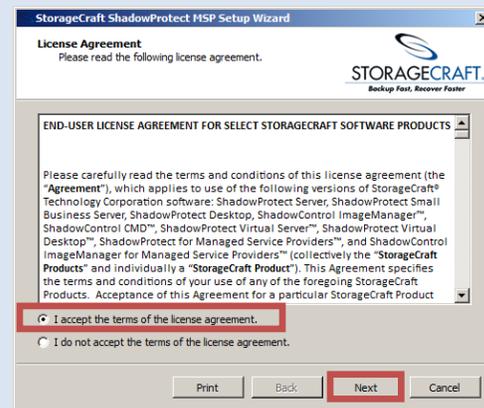
c. Select **English**, click **Next**



d. Click **Next**



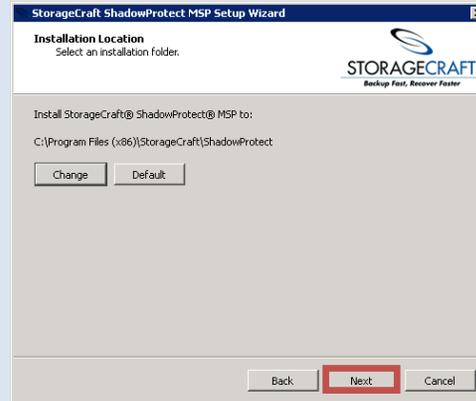
e. Accept the agreement, click **Next**



f. Select **Custom**, click **Next**

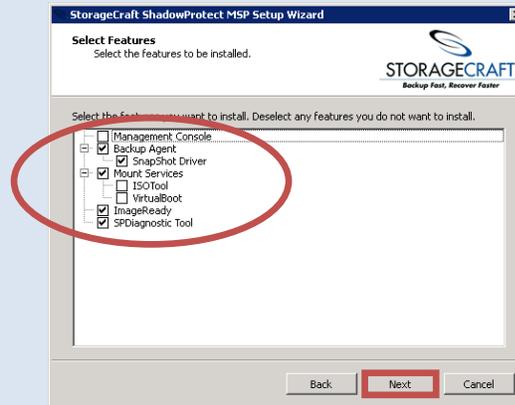


g. Click **Next** to accept the default install directory

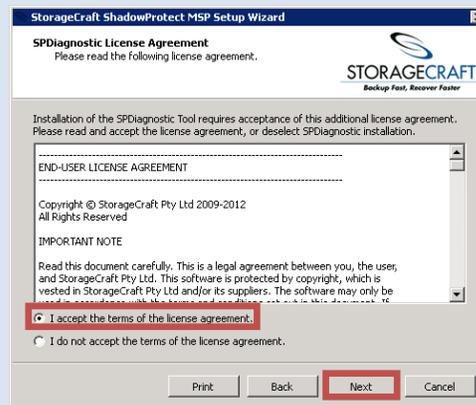


h. Select only the following:

- **Backup Agent**
- **SnapShot Driver**
- **Mount Services**
- **ImageReady**
- **SPDiagnostic Tool**



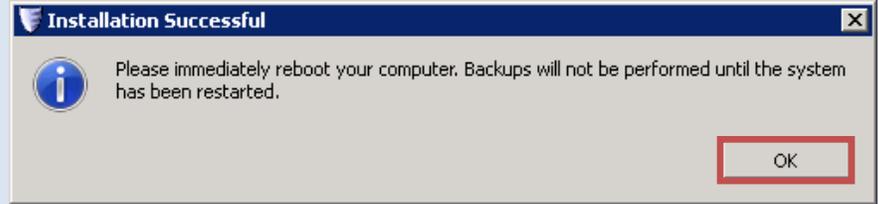
i. Click **Next**



j. Click **Install**

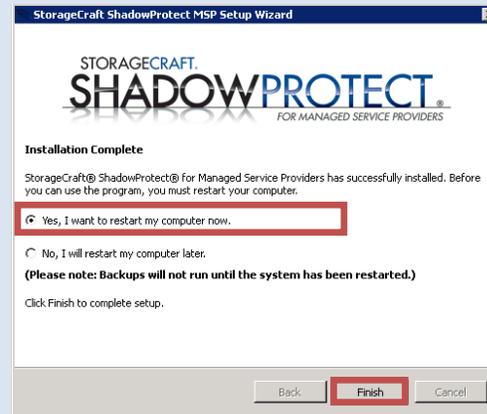


k. Click **OK**



l. Select "Yes, I want to restart my computer now," click **Finish**

After the reboot has completed, the ShadowProtect agent installation is **Complete**.



Configuration of Windows Firewall on Clients

1. Create Firewall Rule

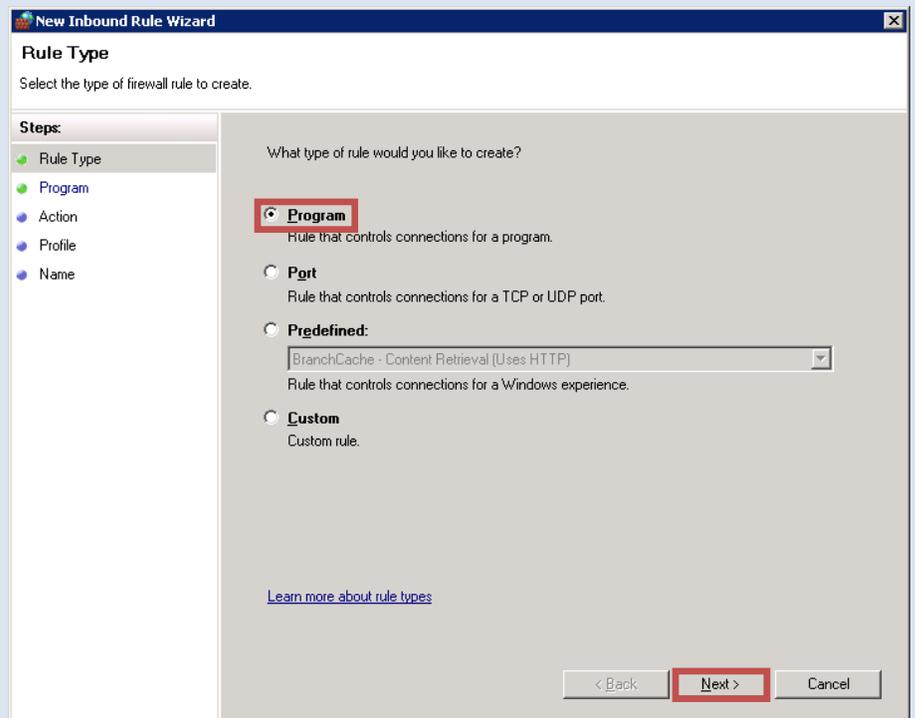
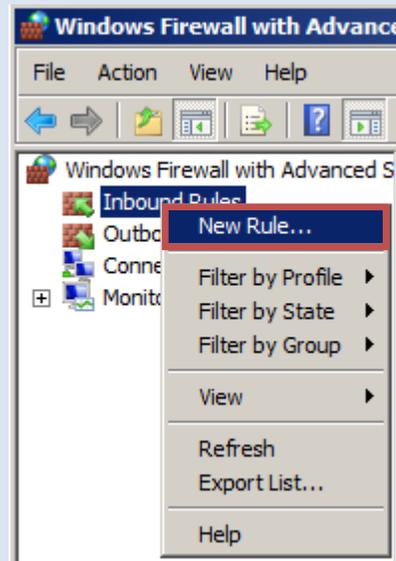
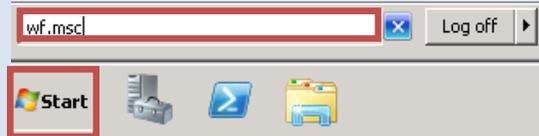
a. Log into the machine where you have the ShadowProtect Agent installed

b. Click **Start**

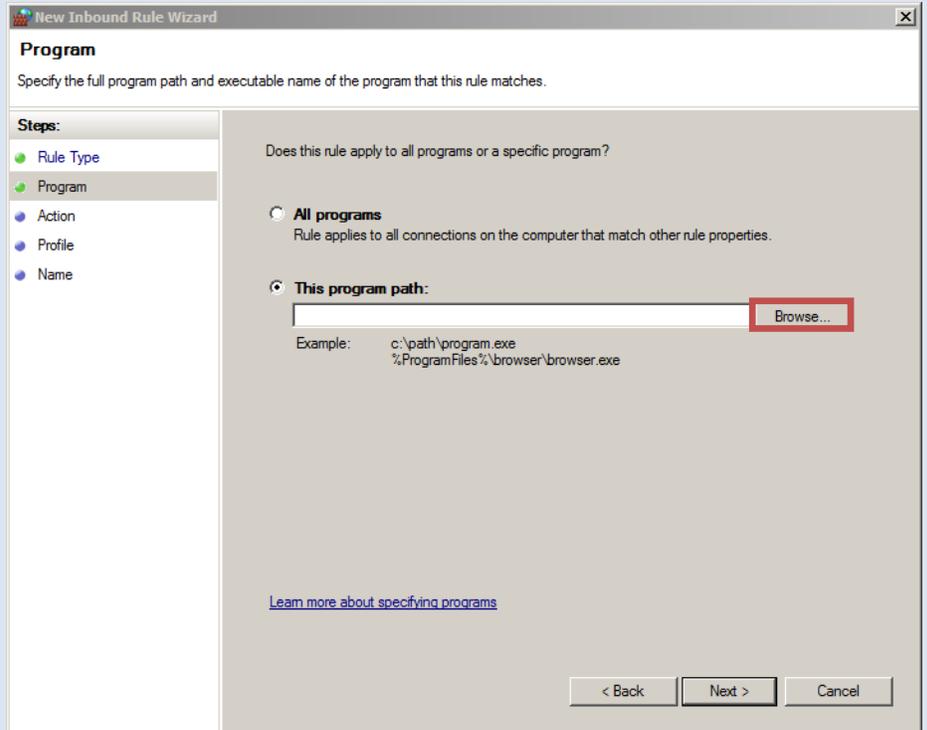
c. Type in **wf.msc**, hit **Enter**

d. Select **Inbound Rules**, right click, select **New Rule**

e. Select **Program**, click **Next**



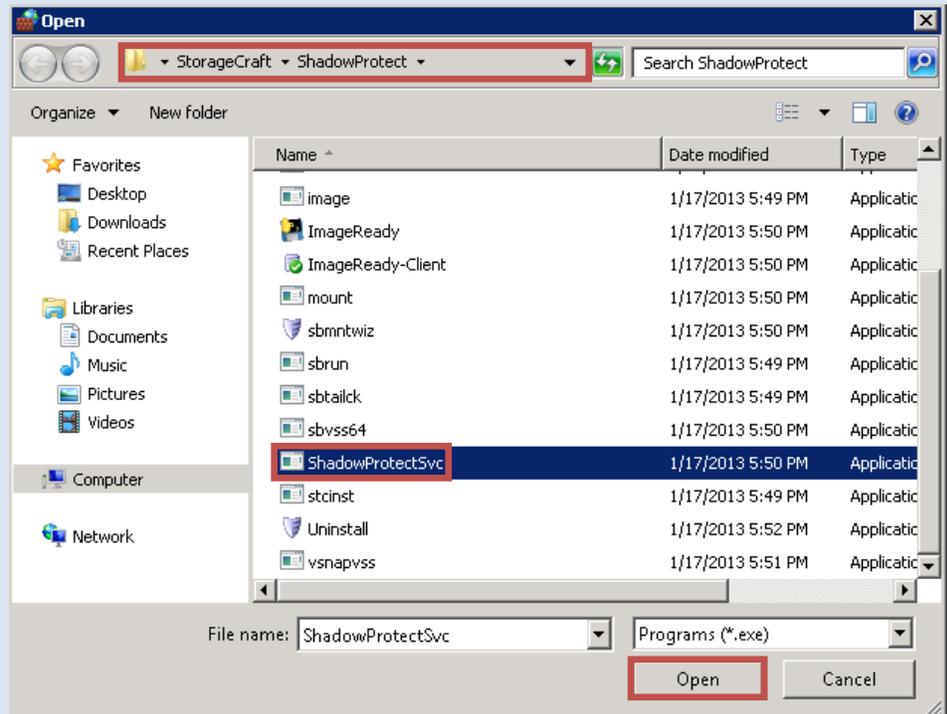
f. Select **Browse**



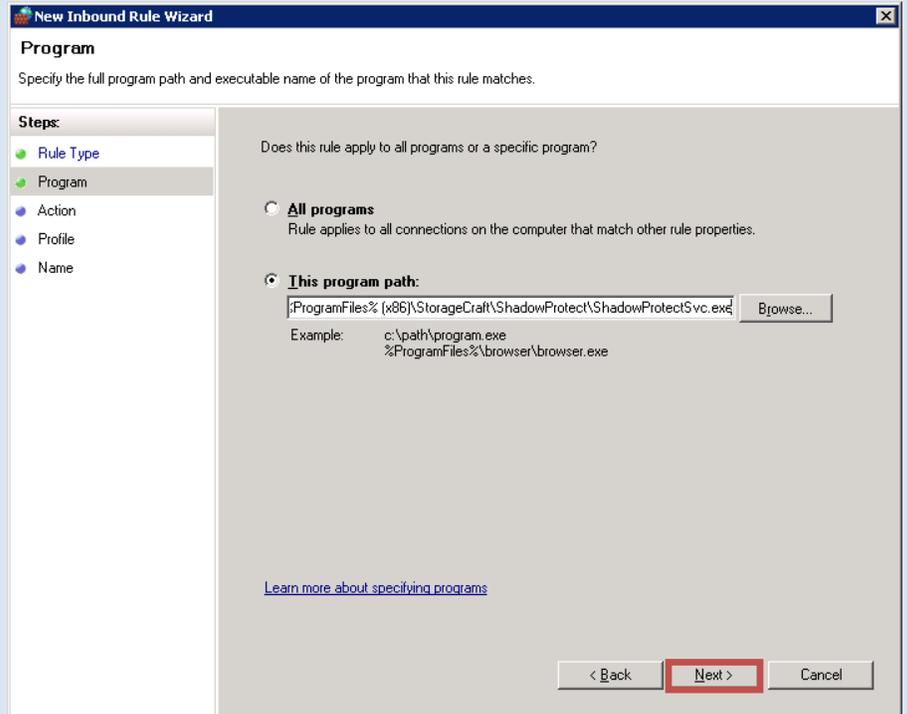
Go to: **C:\ProgramFiles (x86)\StorageCraft\ShadowProtect**

Select: **ShadowProtectSvc**

g. Click **Open**

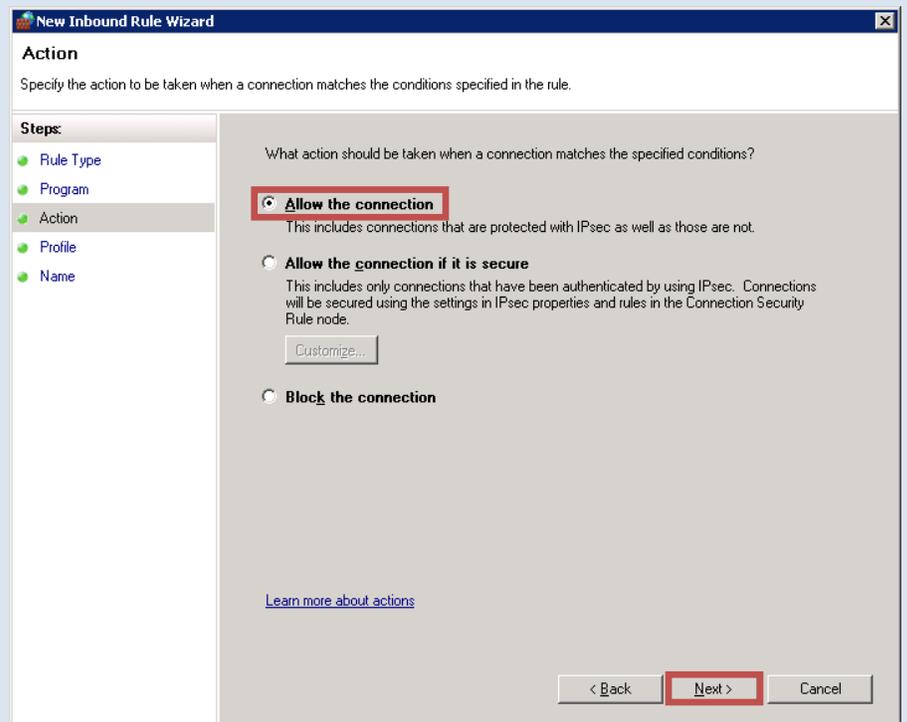


h. Click **Next**



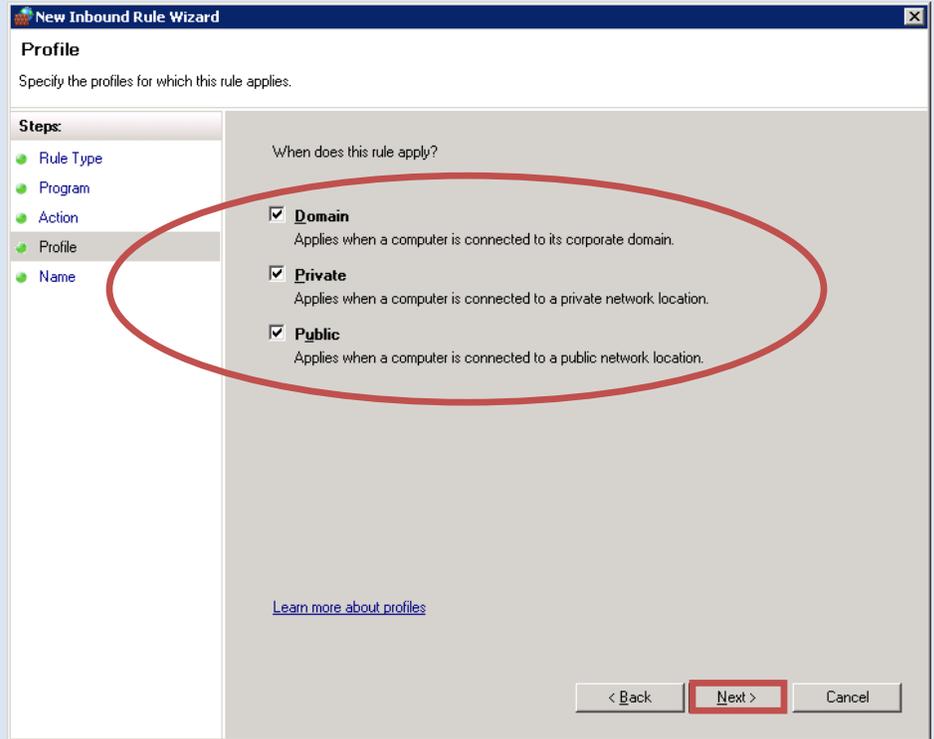
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Program' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Program'. Below it, the instruction says 'Specify the full program path and executable name of the program that this rule matches.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name', with 'Program' selected. The main area asks 'Does this rule apply to all programs or a specific program?' with two radio button options: 'All programs' (unselected) and 'This program path:' (selected). Under 'This program path:', there is a text box containing the path '|ProgramFiles% (x86)\StorageCraft\ShadowProtect\ShadowProtectSvc.exe|' and a 'Browse...' button. Below the text box, an 'Example:' shows 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. A blue link 'Learn more about specifying programs' is at the bottom. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

i. Select **Allow the connection**, click **Next**



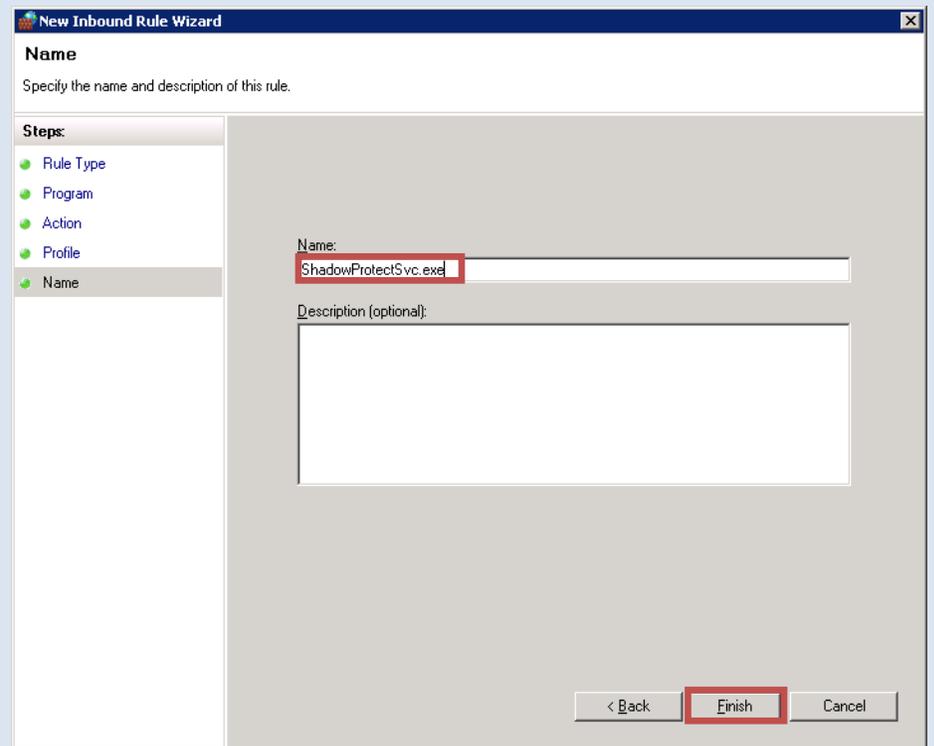
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Action' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Action'. Below it, the instruction says 'Specify the action to be taken when a connection matches the conditions specified in the rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name', with 'Action' selected. The main area asks 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (selected and highlighted with a red box), 'Allow the connection if it is secure' (unselected), and 'Block the connection' (unselected). Under 'Allow the connection', there is a description: 'This includes connections that are protected with IPsec as well as those are not.' Under 'Allow the connection if it is secure', there is a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' and a 'Customize...' button. Under 'Block the connection', there is a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' A blue link 'Learn more about actions' is at the bottom. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

- j. Ensure that **Domain**, **Private** and **Public** are selected, click **Next**



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. Below the title bar, the text says 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name', with 'Profile' selected. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location.), and 'Public' (Applies when a computer is connected to a public network location.). A red oval highlights these three options. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

- k. For name type: **ShadowProtectSvc.exe**, click **Finish**



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. Below the title bar, the text says 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Action', 'Profile', and 'Name', with 'Name' selected. The main area has a 'Name:' label followed by a text box containing 'ShadowProtectSvc.exe', which is highlighted with a red box. Below that is a 'Description (optional):' label followed by a large empty text area. At the bottom right, there are three buttons: '< Back', 'Finish', and 'Cancel'. The 'Finish' button is highlighted with a red box.

Windows firewall configuration is now **Complete**

Accessing ABS Appliance®

1. Remote Desktop

i The following steps must be performed on a computer that is connected to the **same network** as the ABS Appliance

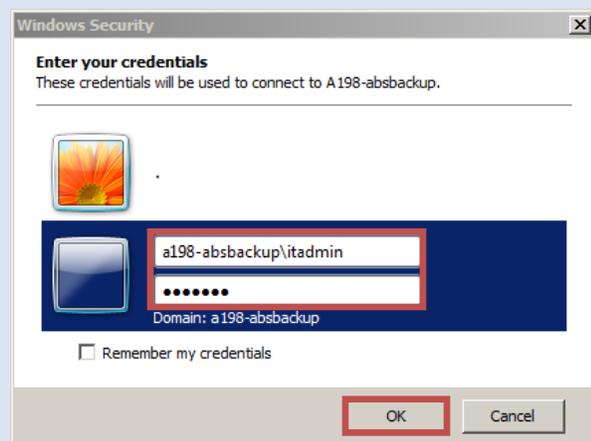
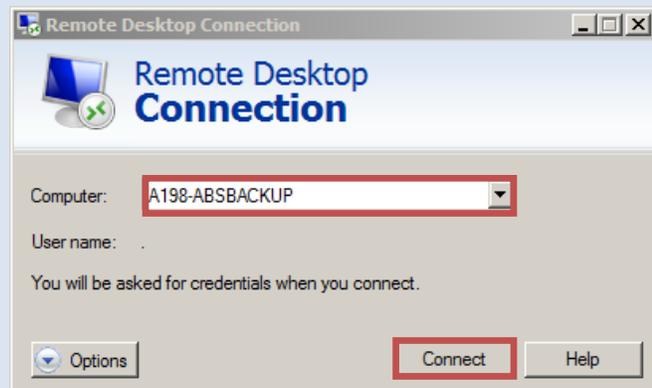
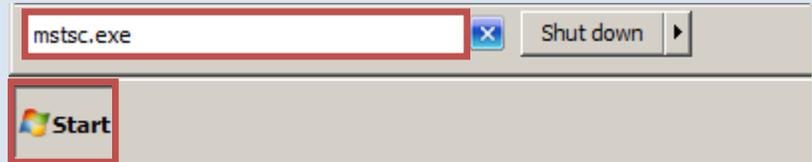
- Click the **Start Menu**
- In the search box, type **mstsc.exe**, hit **Enter**

i You can also access Remote Desktop by going to:
Start>All Programs>Accessories>Remote Desktop Connection

- In the **Computer** section, type in the name of the ABS Appliance or the static IP you assigned to the appliance, click **Connect**

i If you do not know the name of the ABS Appliance, refer to your **Activation Letter**

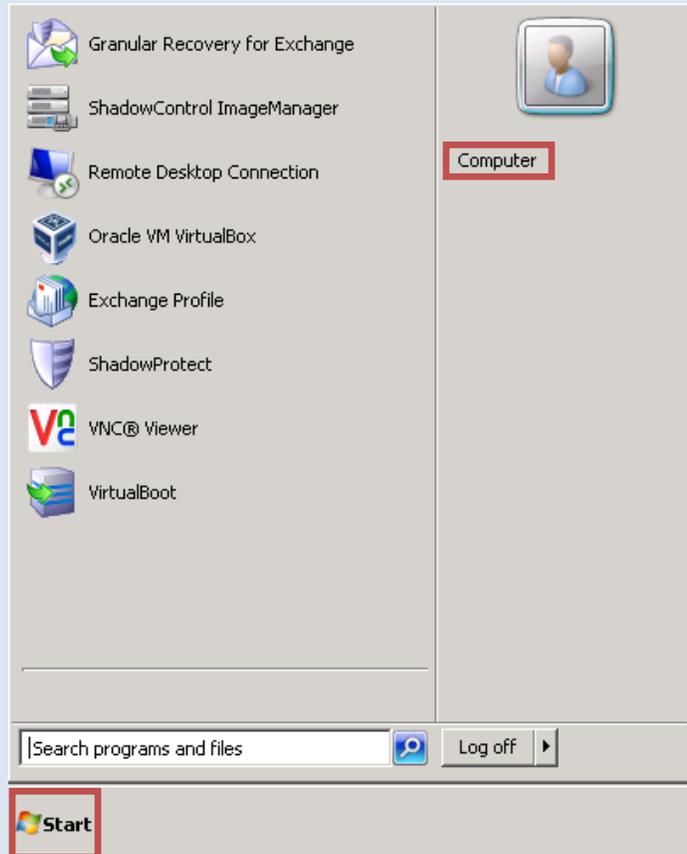
- Select **Use Another Account**
- Use the following username to log in:
axxx-absbackup\itadmin
(replace "xxx" with the appliance number)
- Use the password provided in the **Activation Letter**
- Click **OK**



Dropbox Folder Configuration

1. Create Folder

- a. Click the **Start Button**
- b. Click **Computer**

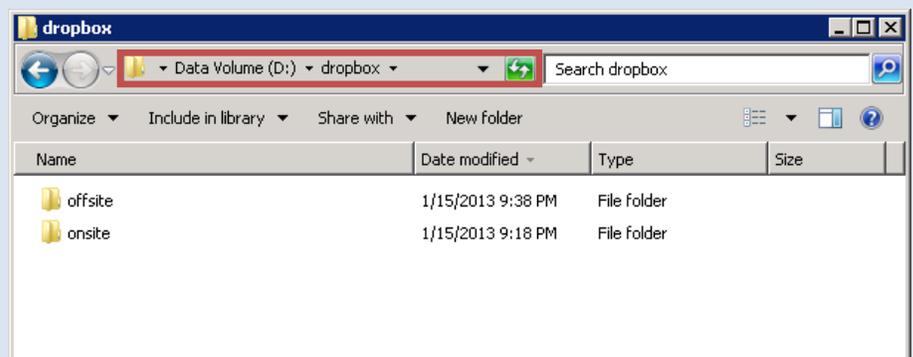


- c. Navigate to **D:\dropbox**
- d. Double click on the appropriate storage folder

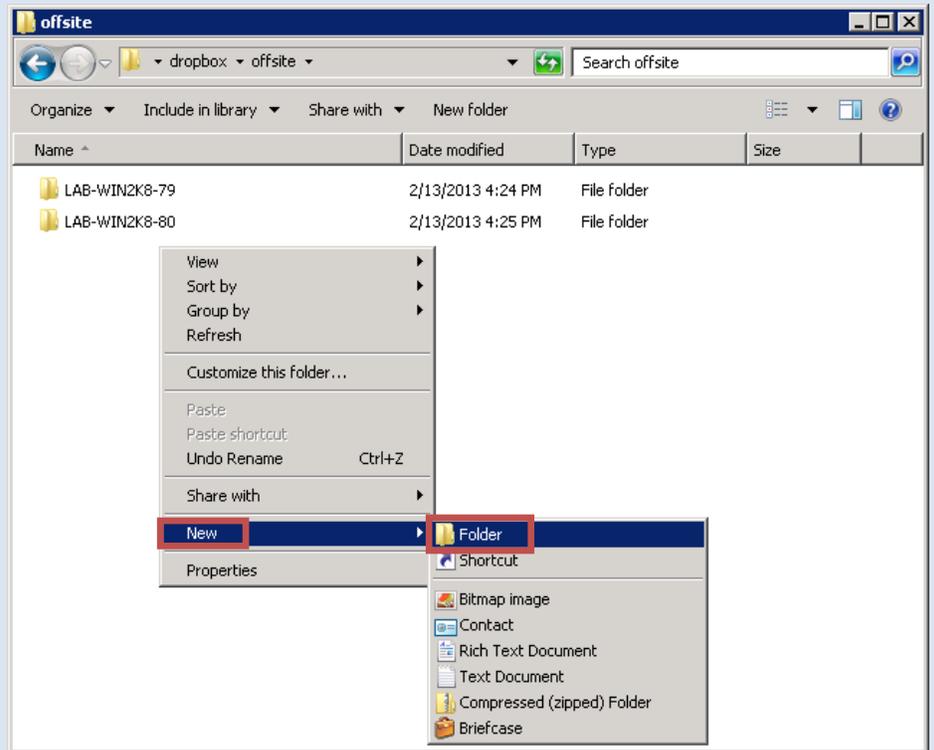
i You will find an **offsite** and an **onsite** folder under **dropbox**

Use **offsite** folder for storing snapshots that are being replicated to the **ABS Cloud**

Use **onsite** folder for storing snapshots locally on the appliance (not replicated to the **ABS Cloud**)



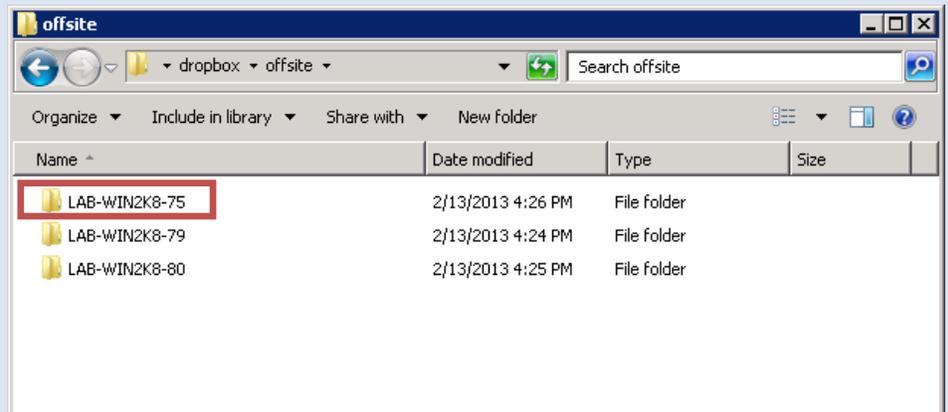
- e. Right click the blank area
- f. Select **New**
- g. Click on **Folder**



- h. Name the folder

i For easy identification, use the name of the client machine. In this case we are protecting a machine named **LAB-WIN2K8-75**

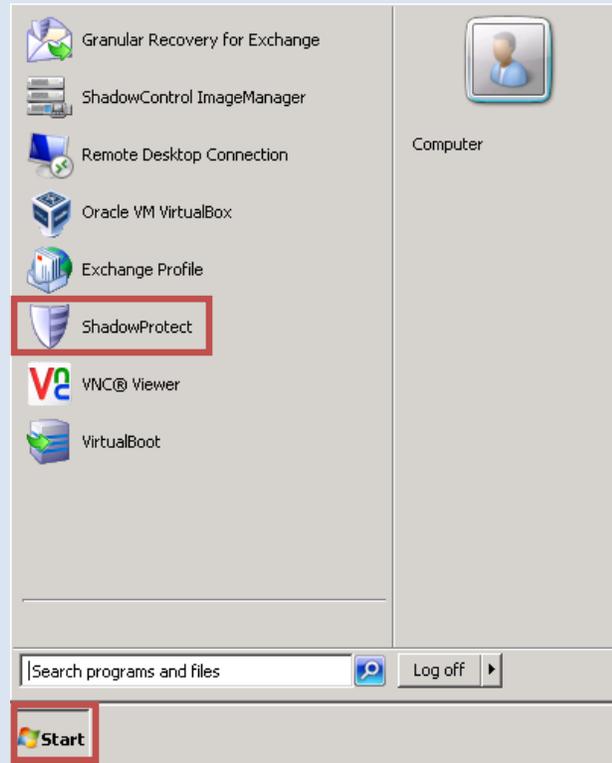
Dropbox folder configuration is now **Complete**



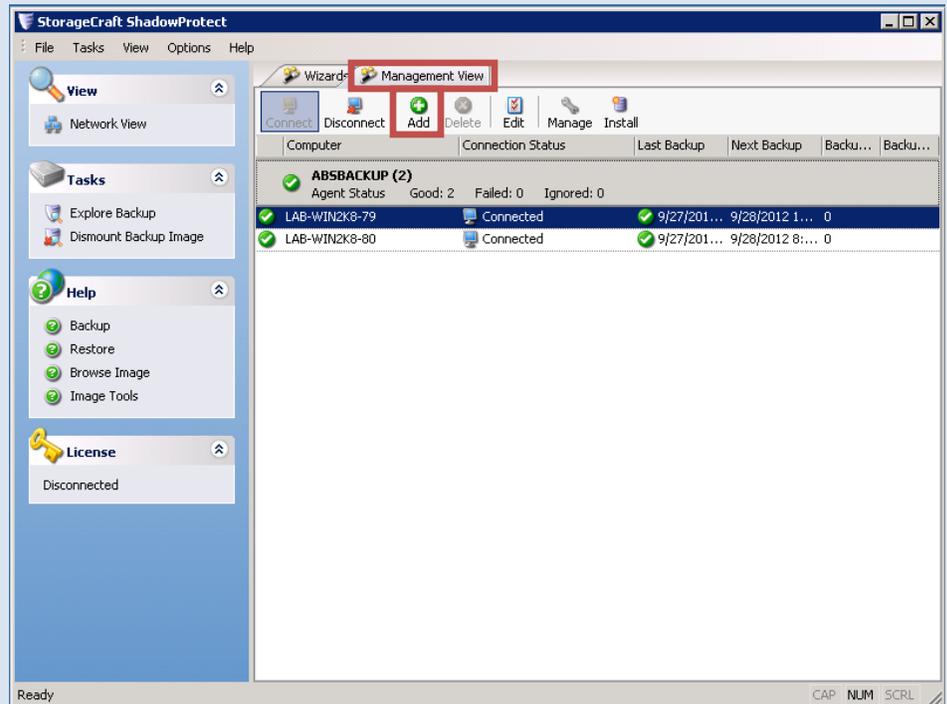
Configuring Clients on Appliance

1. Connecting the Client

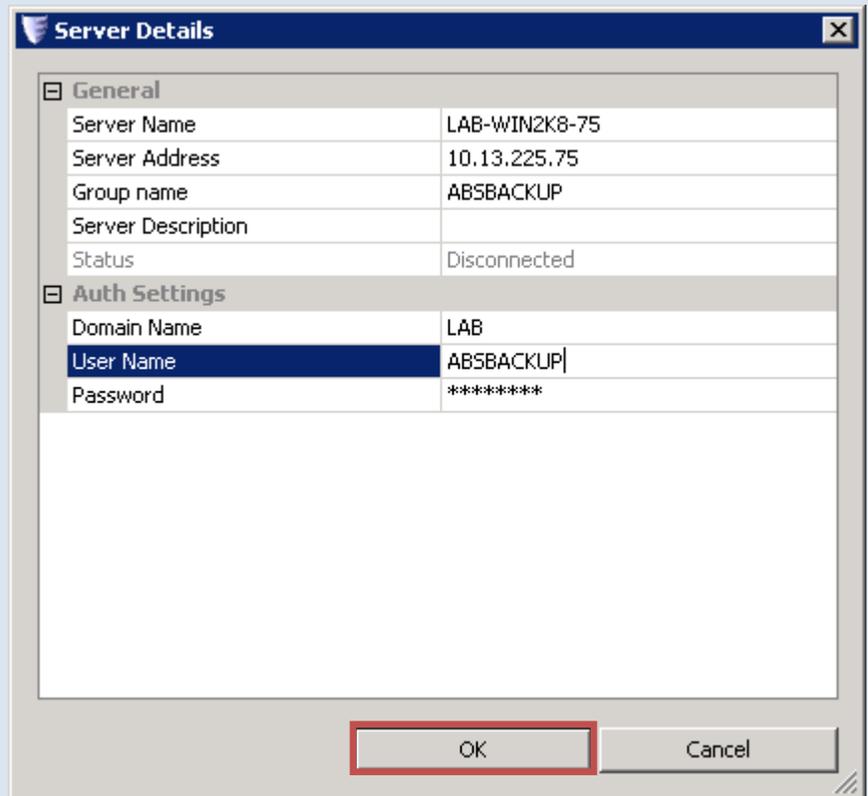
- a. Click **Start**
- b. Click **ShadowProtect**



- c. Click the **Management View** tab
- d. Click **Add**



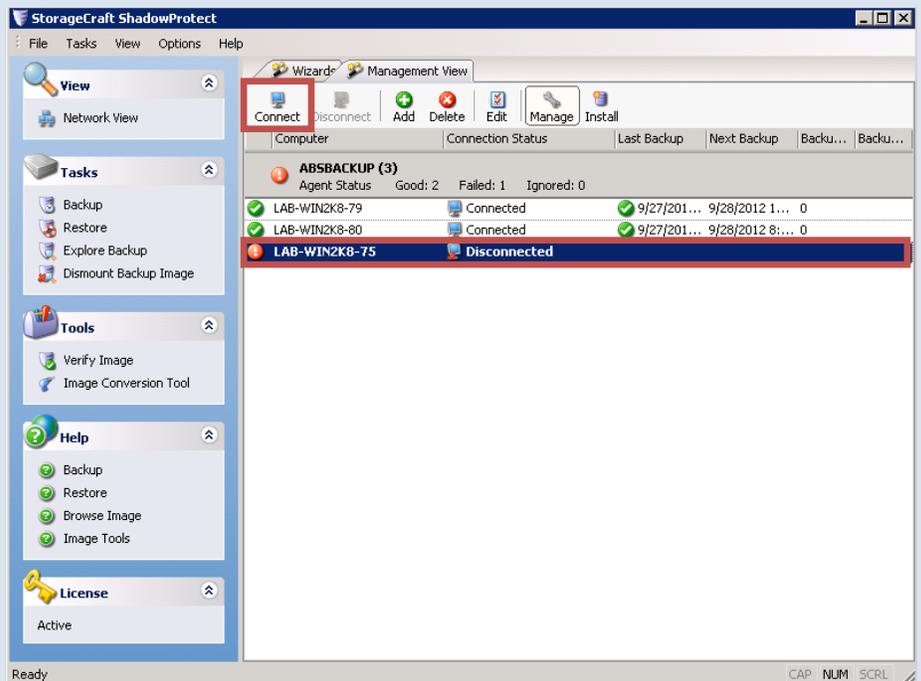
- e. Type in the **Name** and **IP** address of the client machine
- f. Type in **ABSBACKUP** for Group name
- g. Type in the **company domain**
- h. Type in the username and password for the **absbackup** domain admin account that was created during the pre-installation process
- i. Click **OK**



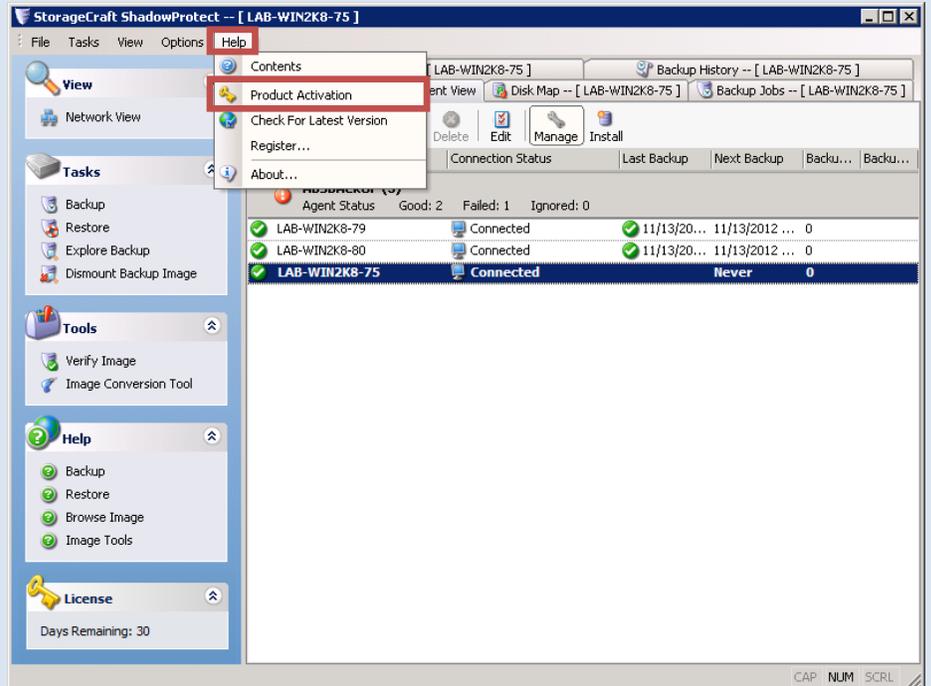
- j. **Double click** the client that was just configured
- k. Click **Connect**

! If you are presented with a failure to connect, verify the information you have entered under **Server Details** by clicking **Edit**

i When there are multiple machines configured with ShadowProtect, select machines by double clicking on them. The machine in **Bold** is the one selected.



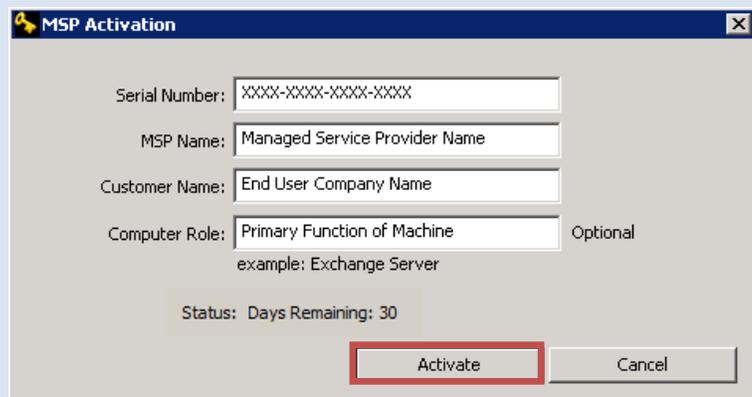
- l. Click **Help**
- m. Click **Product Activation**



- n. Populate all fields with the required information

i Refer to the **Activation Letter** for the **Serial Number**

- o. Click **Activate**

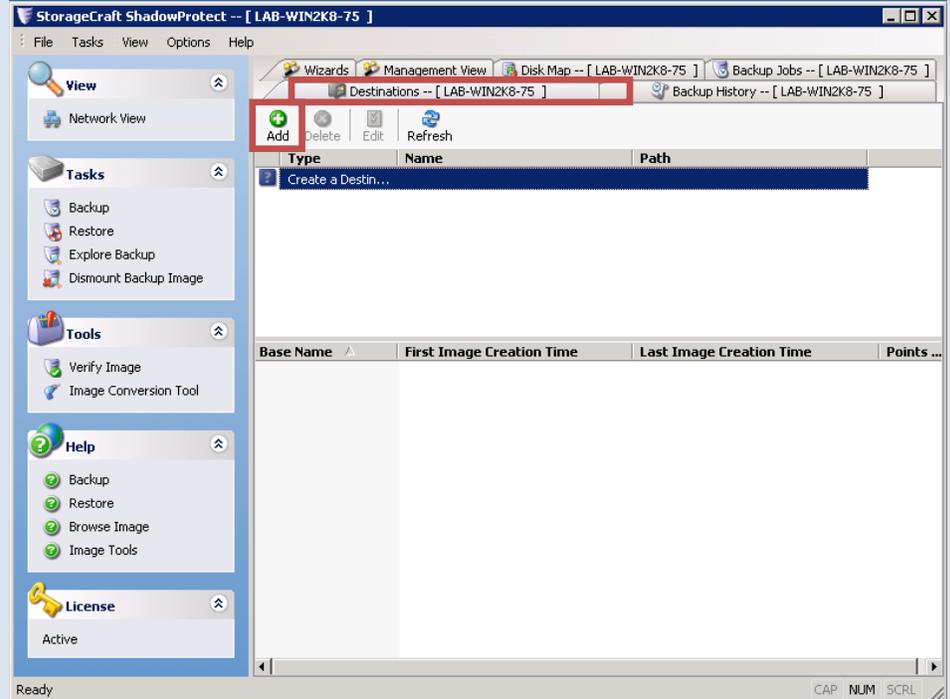


- p. Click **OK**



2. Configuring Destinations

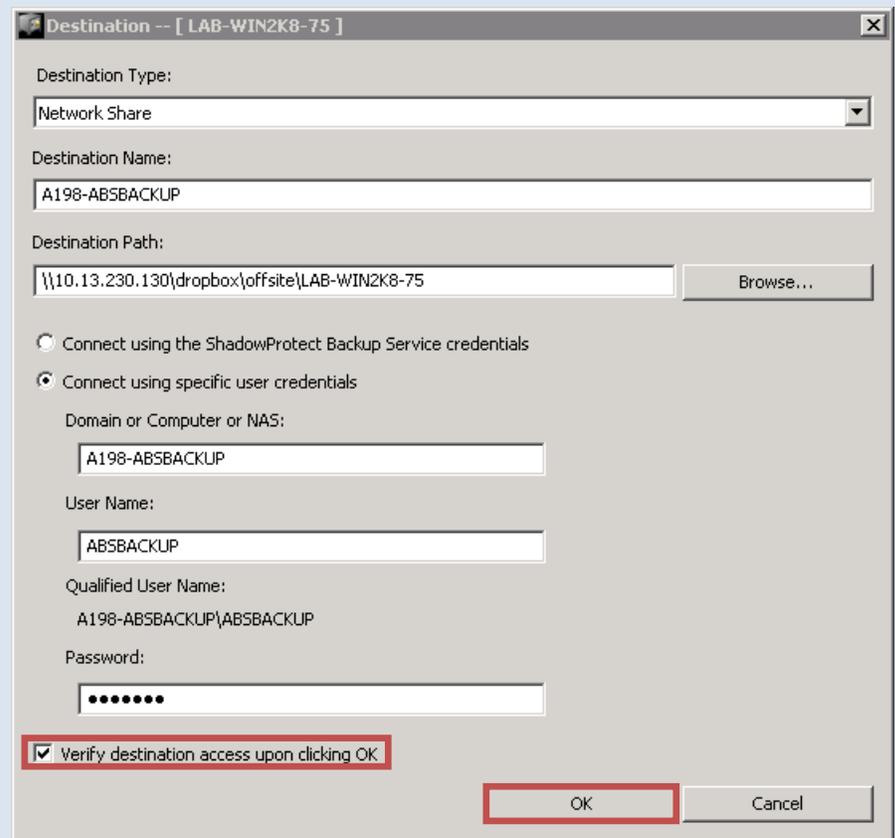
- a. Click the **Destinations Tab**
- b. Click **Add**



- c. For Destination Type, select **Network Share**
- d. For Destination Name, type in the **name of the appliance**
- e. For Destination Path, type in the path using the following format:

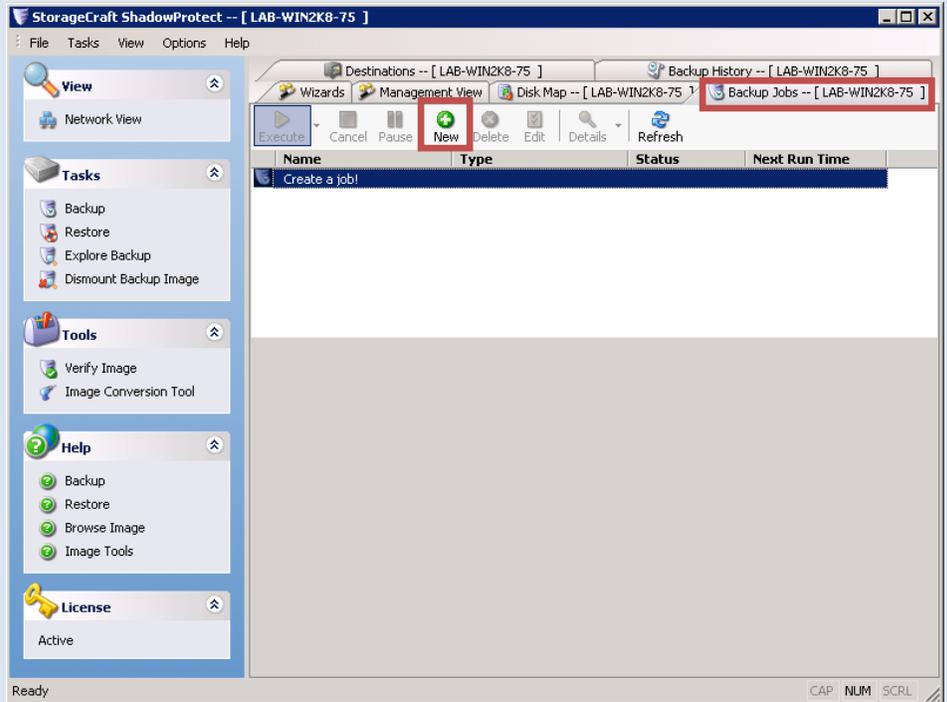
**\\appliance IP address
\\dropbox\offsite or
onsite\client-machine name**

- f. Select **Connect using specific user credentials**
- g. For the Domain, type in the **appliance name**
- h. For the username, type in **ABSBACKUP**
- i. Use the password provided in the **Activation Letter**
- j. Select **Verify destination access... check box**
- k. Click **OK**

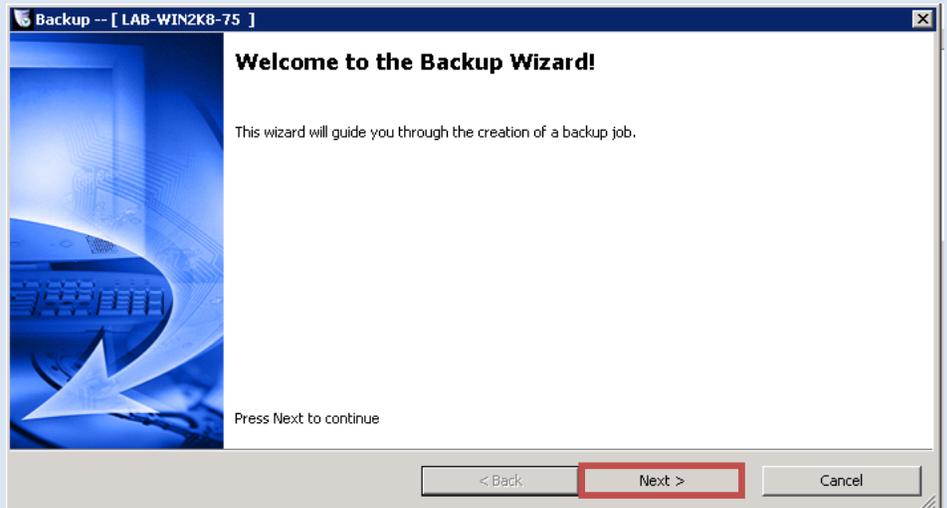


3. Configuring Backup Jobs

- a. Click the **Backup Jobs** tab
- b. Click **New**

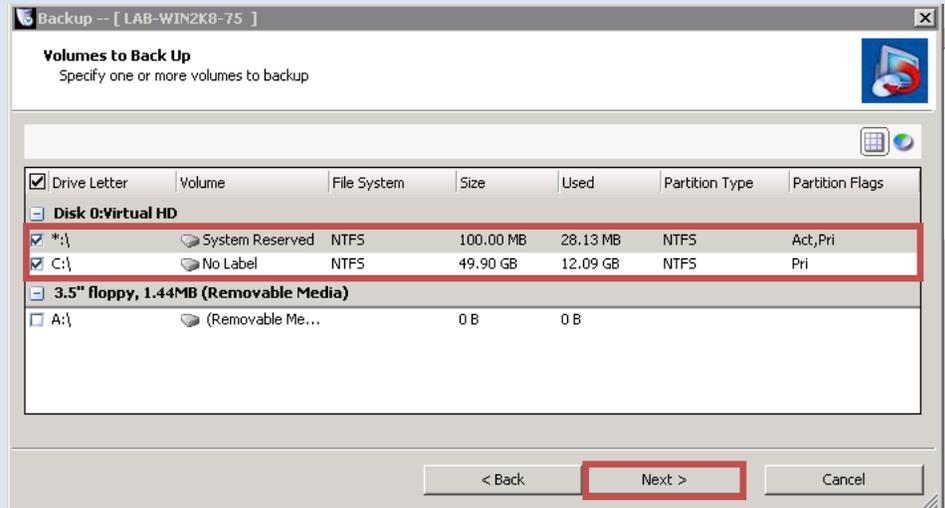


- c. Click **Next**

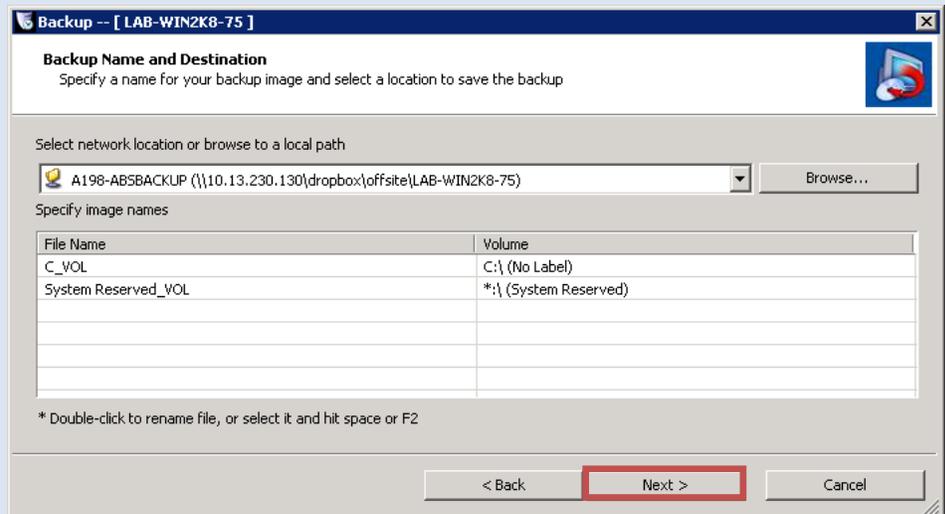


d. Select all the disks to be protected

e. Click **Next**



f. Click **Next**

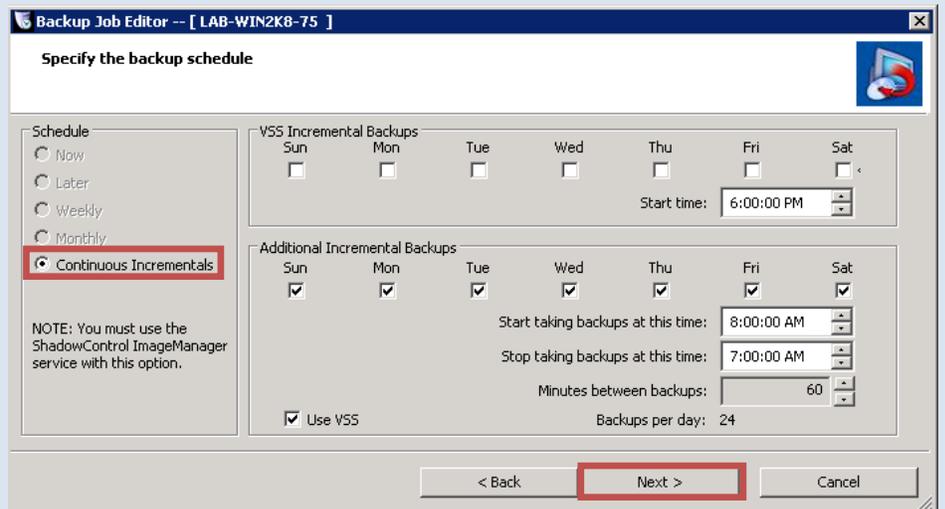


g. Under schedule, select **Continuous Incrementals**

h. Select Additional Incremental Backups to run **Sun-Sat, 8:00AM-7:00AM** with **60 minutes** in between backups

i. Ensure that **Use VSS** is selected

j. Click **Next**



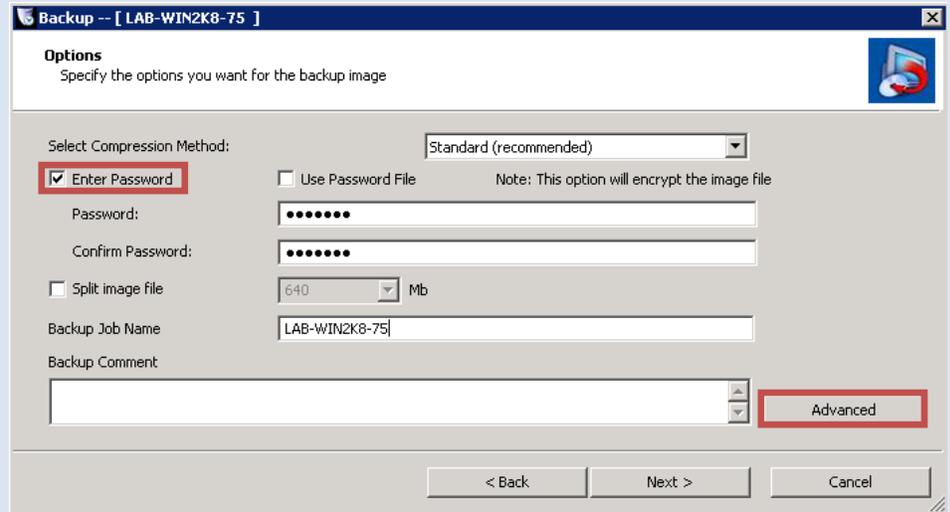
 For best performance, stagger backup jobs between machines by at least 10 minutes

- k. Check off **Enter Password**
- l. Type in the **Encryption Password** as it appears in the **Activation Letter**
- m. Under **Backup Job Name**, type in the name of the client machine
- n. Click **Advanced**

i If the client does not wish to use the ABS provided **Encryption Password**, feel free to use a unique one. Remember to store the password in a safe place.

- o. Select the **Encryption** tab
- p. Under Encryption Algorithm, Select **AES 256 bit**
- q. Click **OK**

- r. Click **Next**



Backup -- [LAB-WIN2K8-75]

Options
Specify the options you want for the backup image

Select Compression Method: Standard (recommended)

Enter Password Use Password File Note: This option will encrypt the image file

Password:

Confirm Password:

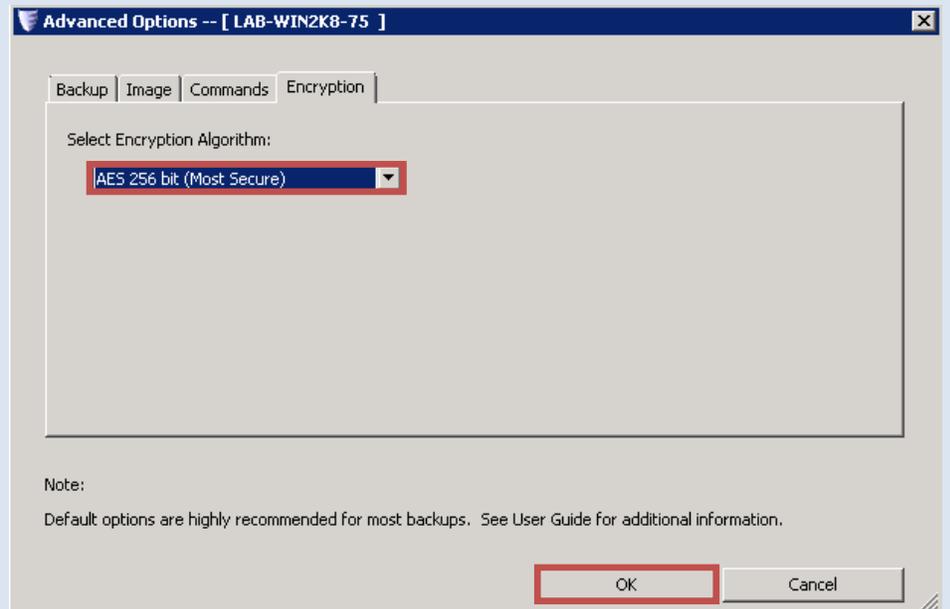
Split image file 640 Mb

Backup Job Name LAB-WIN2K8-75

Backup Comment

Advanced

< Back Next > Cancel



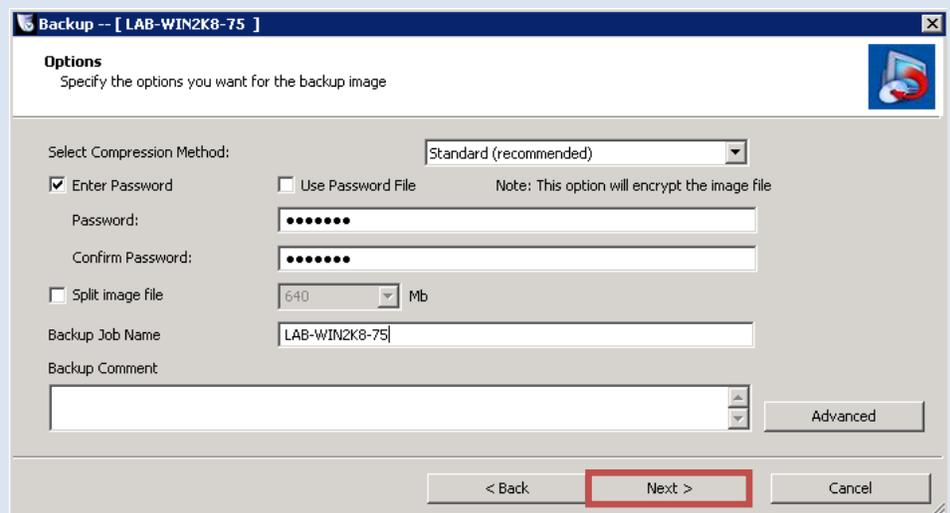
Advanced Options -- [LAB-WIN2K8-75]

Backup Image Commands Encryption

Select Encryption Algorithm:
AES 256 bit (Most Secure)

Note:
Default options are highly recommended for most backups. See User Guide for additional information.

OK Cancel



Backup -- [LAB-WIN2K8-75]

Options
Specify the options you want for the backup image

Select Compression Method: Standard (recommended)

Enter Password Use Password File Note: This option will encrypt the image file

Password:

Confirm Password:

Split image file 640 Mb

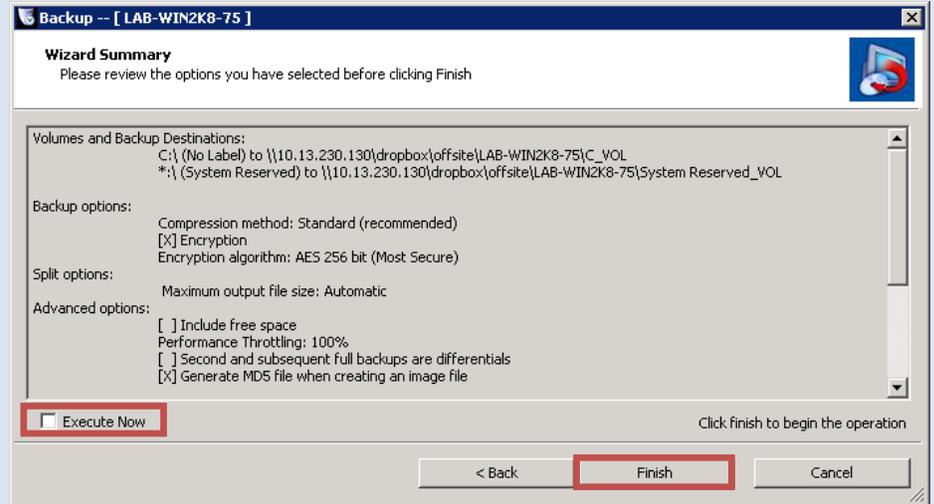
Backup Job Name LAB-WIN2K8-75

Backup Comment

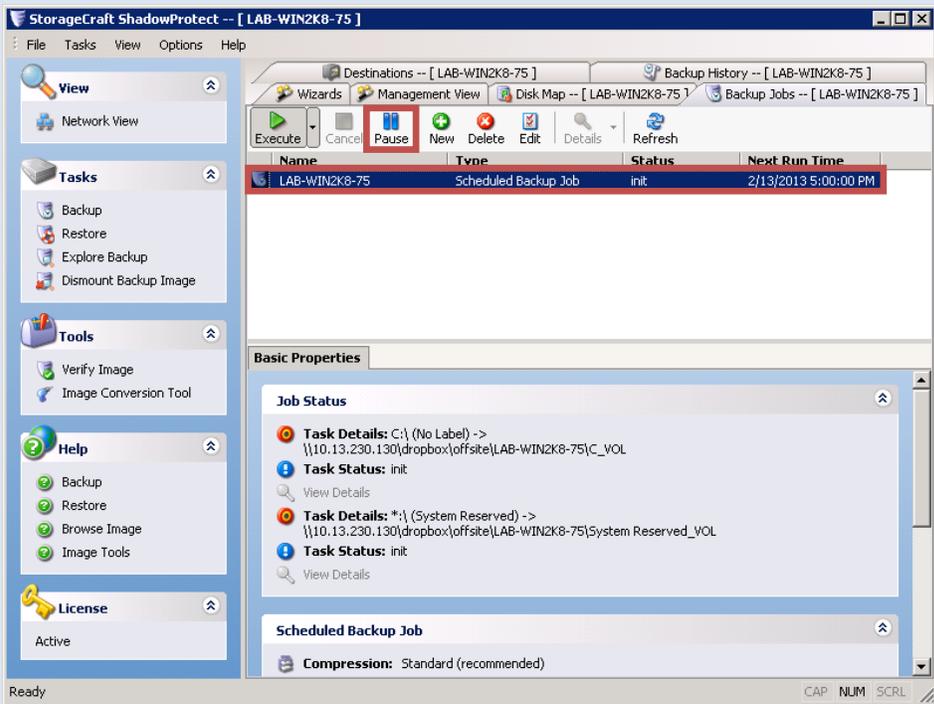
Advanced

< Back Next > Cancel

- s. Uncheck **Execute Now**
- t. Click **Finish**



- u. Click the newly created backup job
- v. Click **Pause**



! Initial base image jobs may impact network performance. Resume the backup job when most convenient.

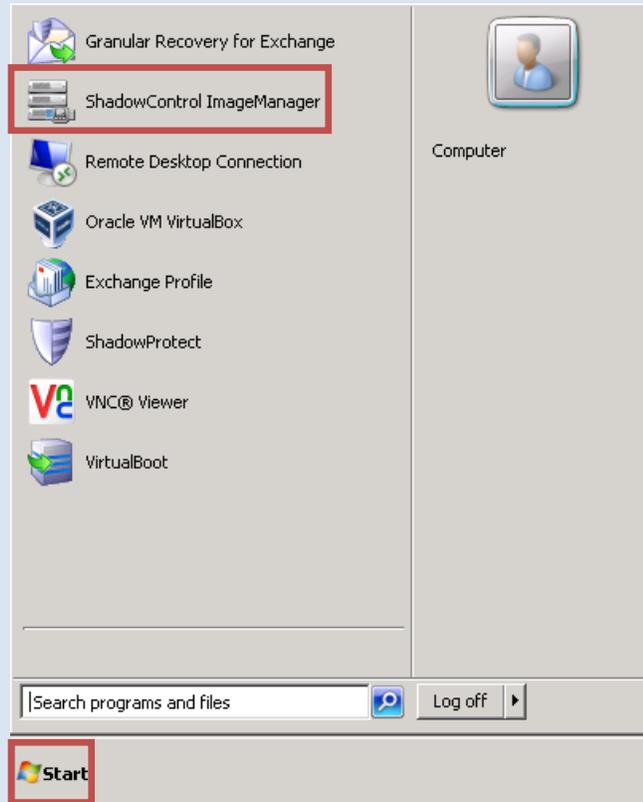
i Daily incremental snapshots barely impact network performance.

Backup job configuration is now **Complete**

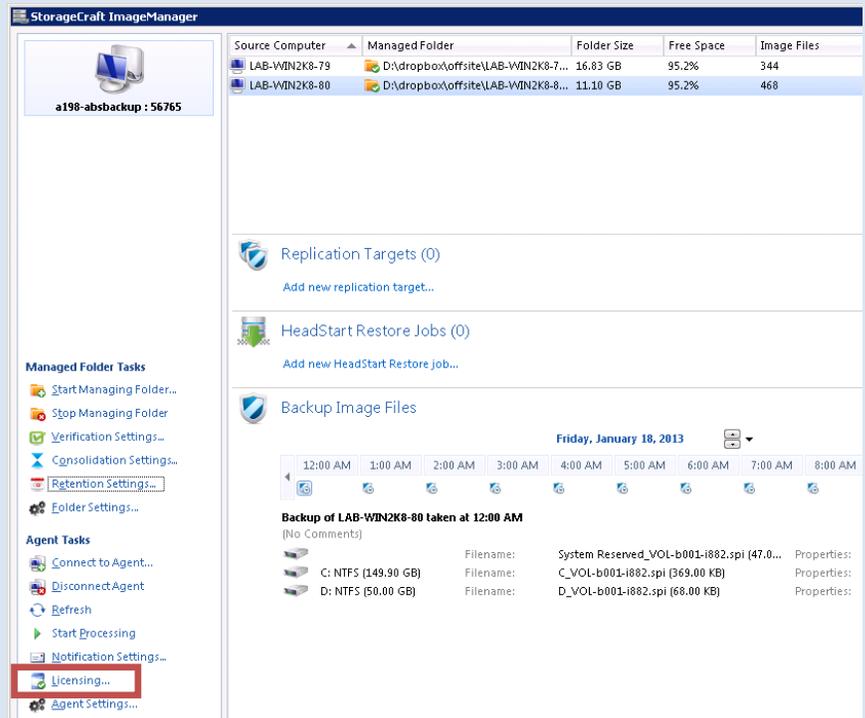
Configure Image Manager

1. Activate License

- a. Click **Start**
- b. Click **ShadowControl ImageManager**



- c. Under Managed Folder Tasks, Click **Licensing...**



d. Populate the fields with **MSP Name** and **End User Name**

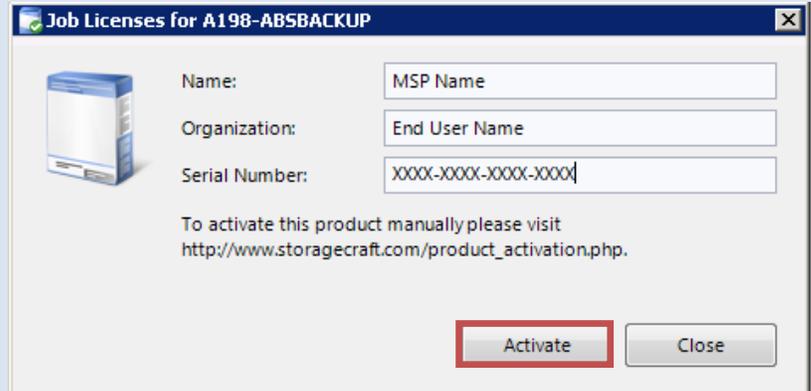
i Refer to the **Activation Letter** for the **Serial Number**

e. Click **Activate**

f. Click **OK**

g. Click the **up arrows** to assign all available licenses to agent

h. Click **Update**



Job Licenses for A198-ABSBACKUP

Name:

Organization:

Serial Number:

To activate this product manually please visit
http://www.storagecraft.com/product_activation.php.

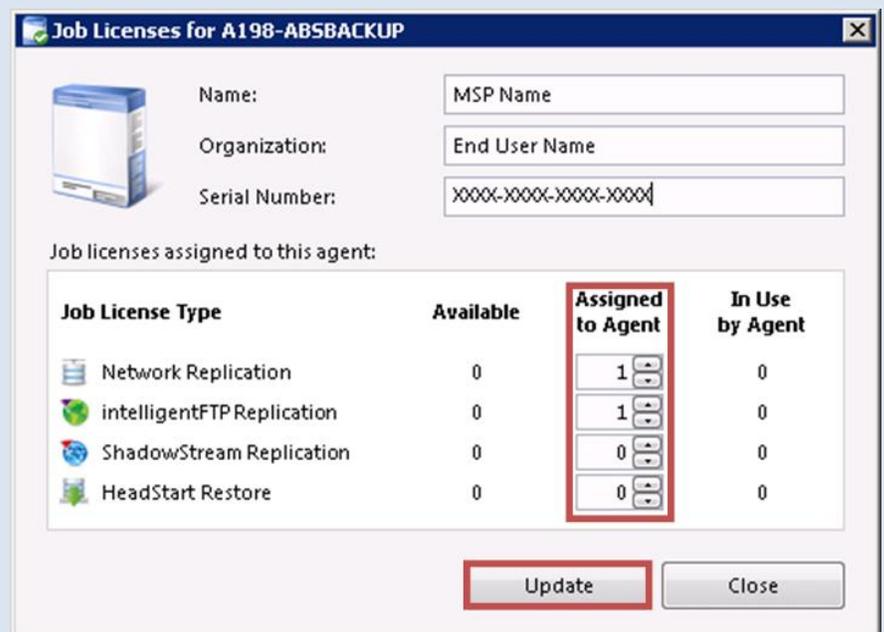
Activate



Activation Succeeded

i The StorageCraft ImageManager agent on A198-ABSBACKUP is now activated. Before you can create replication or HeadStart Restore jobs, however, you must first assign job licenses to this agent.

OK



Job Licenses for A198-ABSBACKUP

Name:

Organization:

Serial Number:

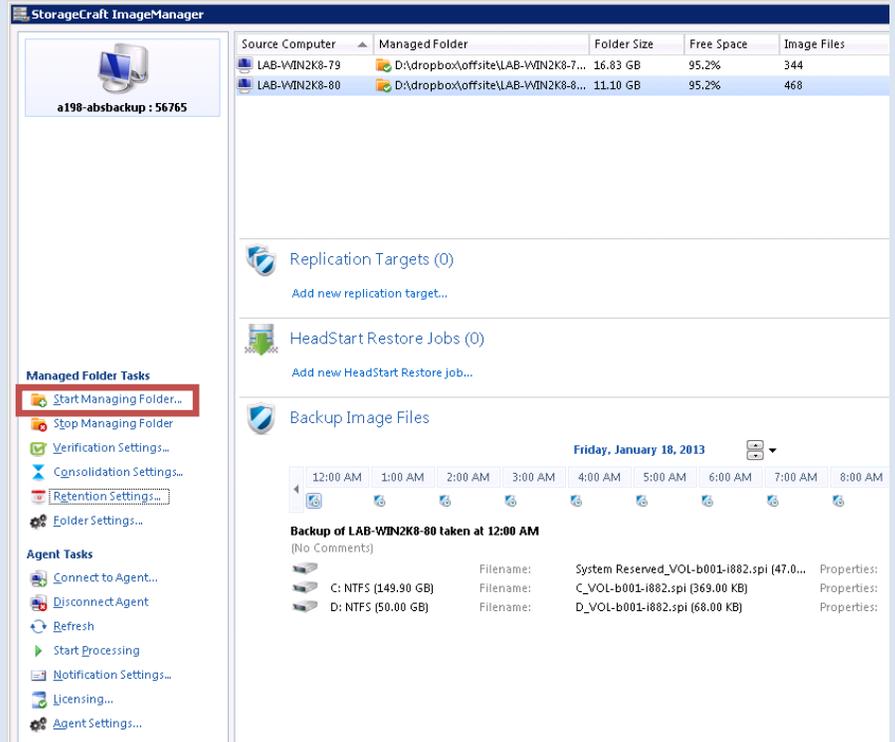
Job licenses assigned to this agent:

Job License Type	Available	Assigned to Agent	In Use by Agent
 Network Replication	0	1	0
 intelligentFTP Replication	0	1	0
 ShadowStream Replication	0	0	0
 HeadStart Restore	0	0	0

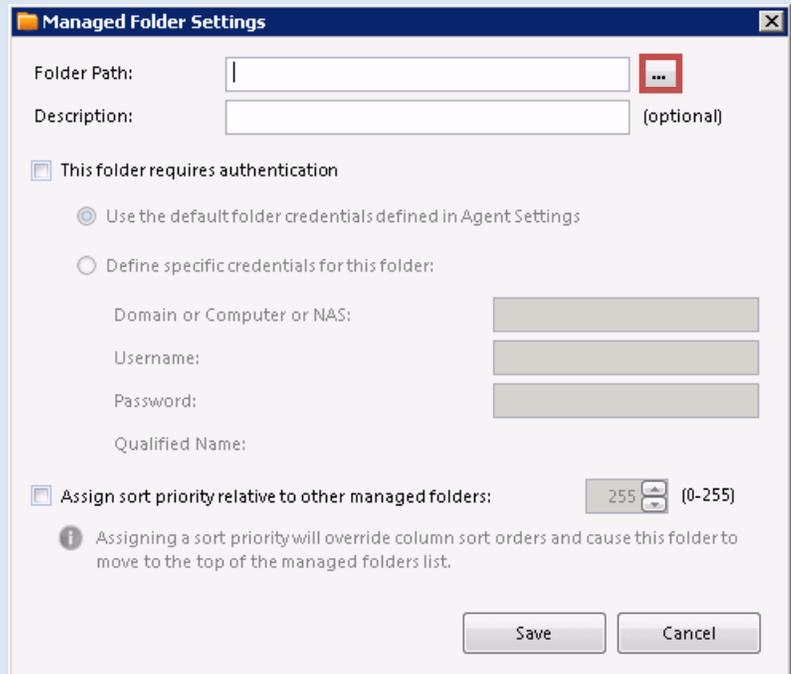
Update

2. Add Managed Folder

a. Under **Managed Folder Tasks**, click **Start Managing Folder**



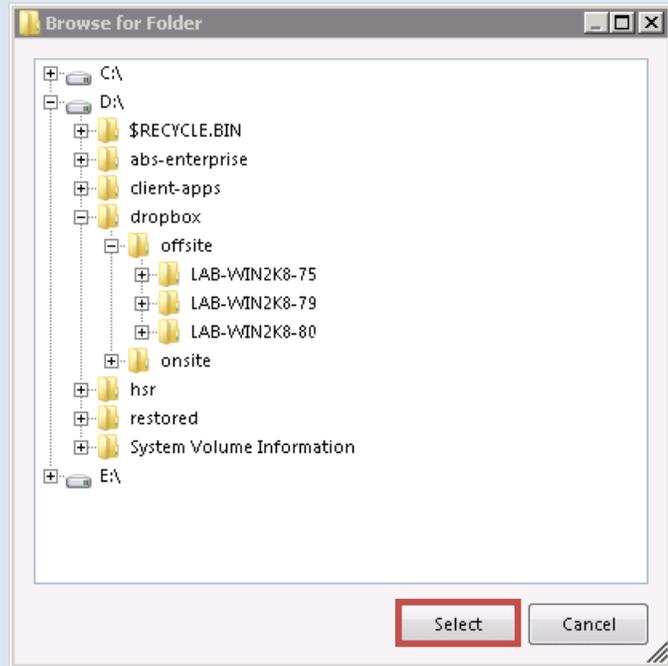
b. Click the **Browse** button to the right of the **Folder Path** field



c. Navigate to:
D:\dropbox\xxx\client-name

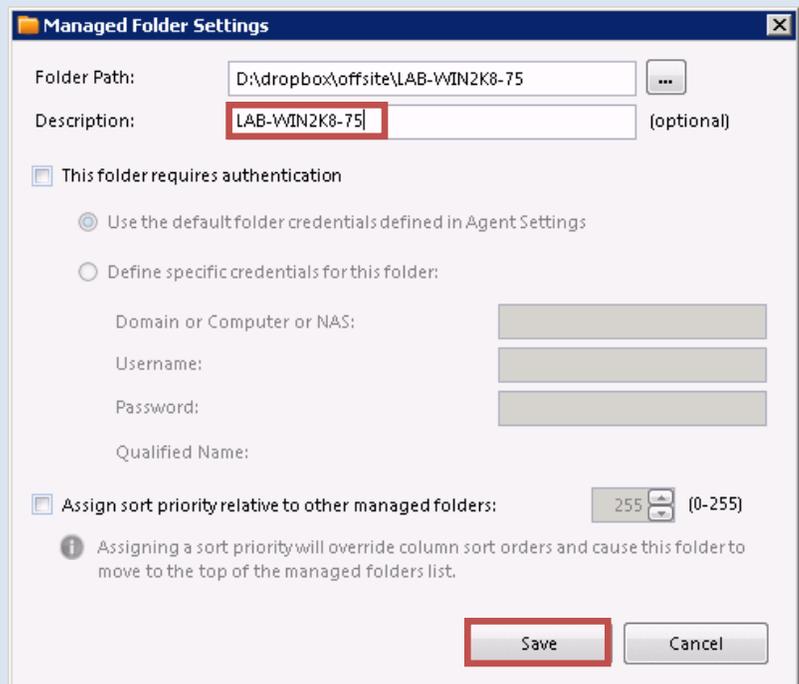
i Replace **xxx** with **offsite** or **onsite** depending on the storage location of the protected machine

d. Click **Select**



e. Type in the description (use name of client machine being added for protection)

f. Click **Save**



3. Retention Policy

- a. Click the **Managed Folder**
- b. Under **Managed Folder Tasks**, click **Retention Settings**

- c. Configure the retention policy

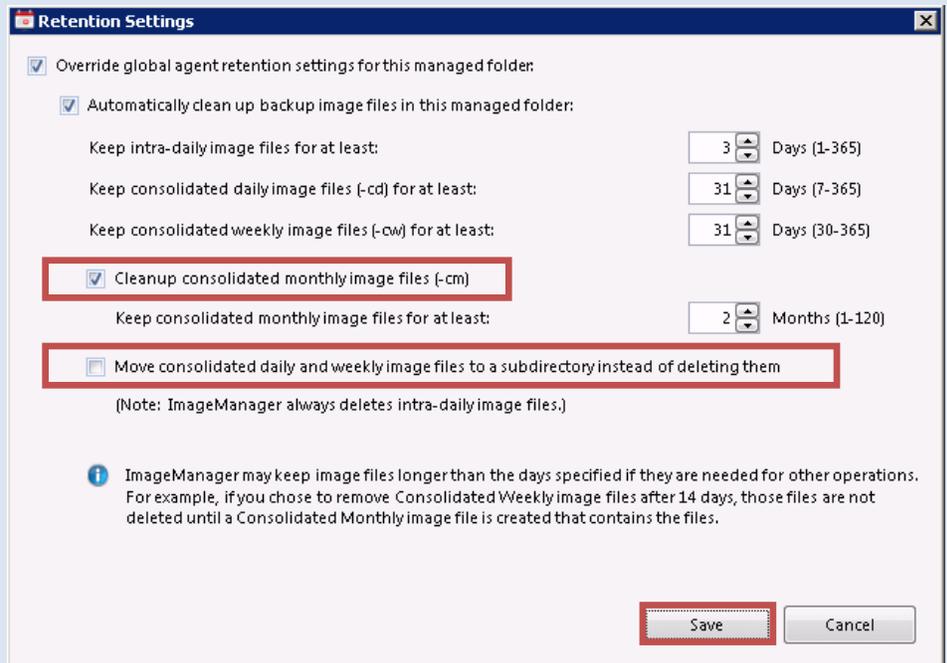
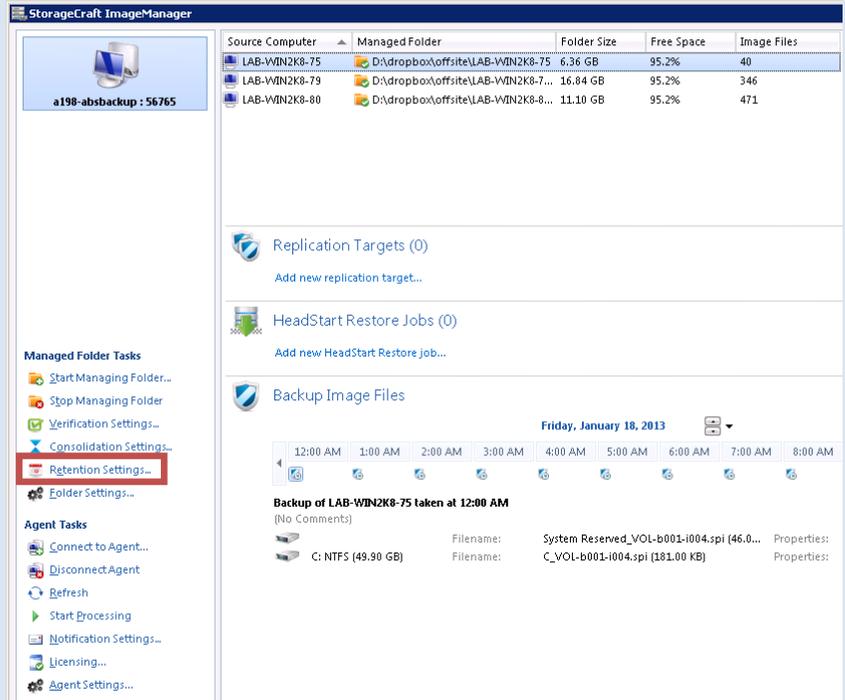
ABS Recommended Settings:

- **Intra-Daily(Hourly) - 3**
- **Consolidated Daily - 31**
- **Consolidated Weekly - 31**

- d. Select **Cleanup consolidated monthly...** , set it to **2 Months**
- e. Uncheck the **Move consolidated daily and weekly image files...** checkbox
- f. Click **Save**

i The retention policy can be modified to meet the client's requirements, keep in mind, a longer retention policy will consume more disk space.

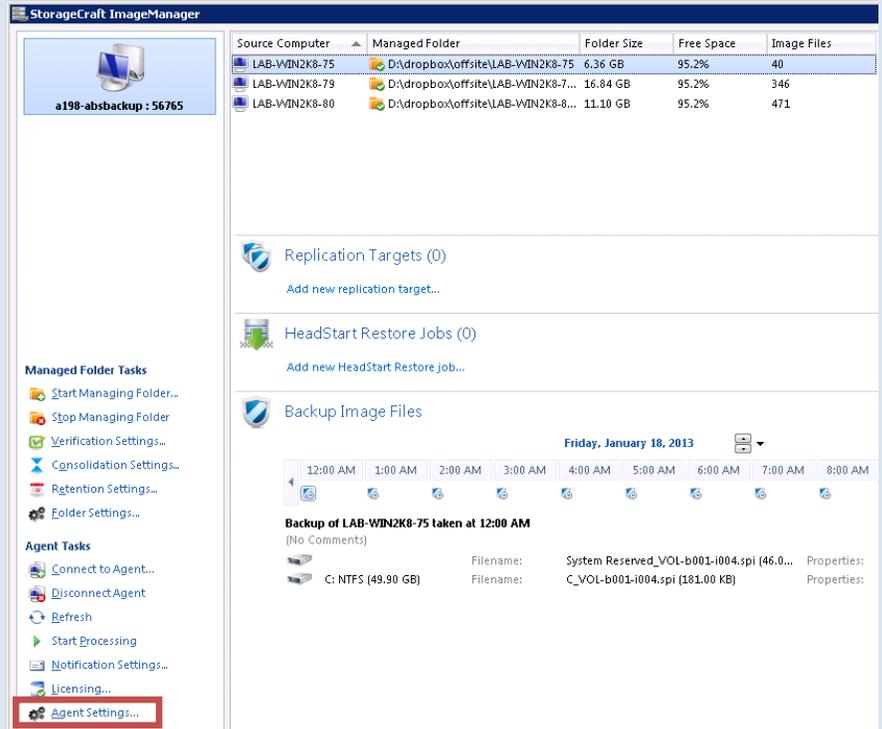
Retention configuration is now **Complete**



Offsite Replication Setup

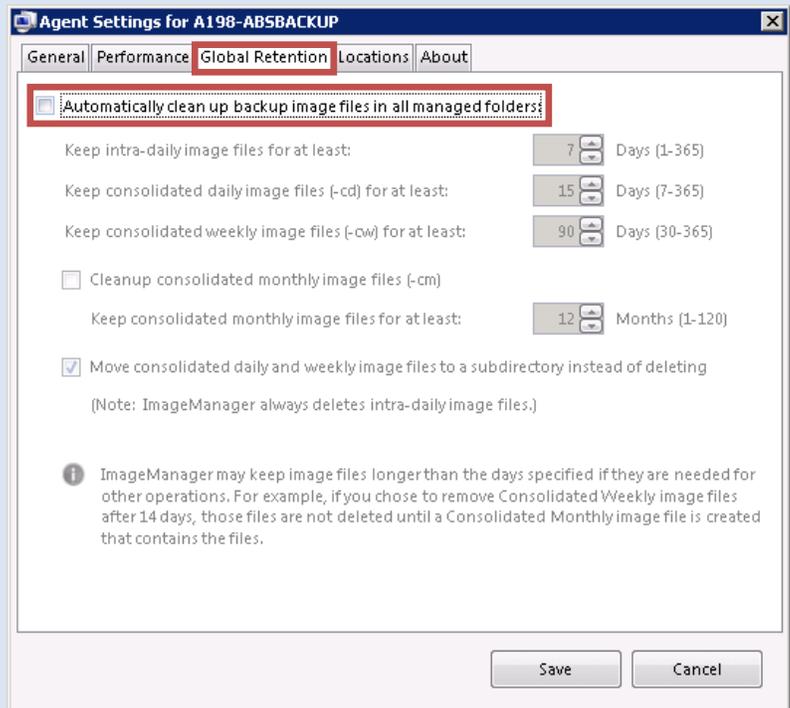
1. Add Locations

a. In ImageManager, click **Agent Settings**



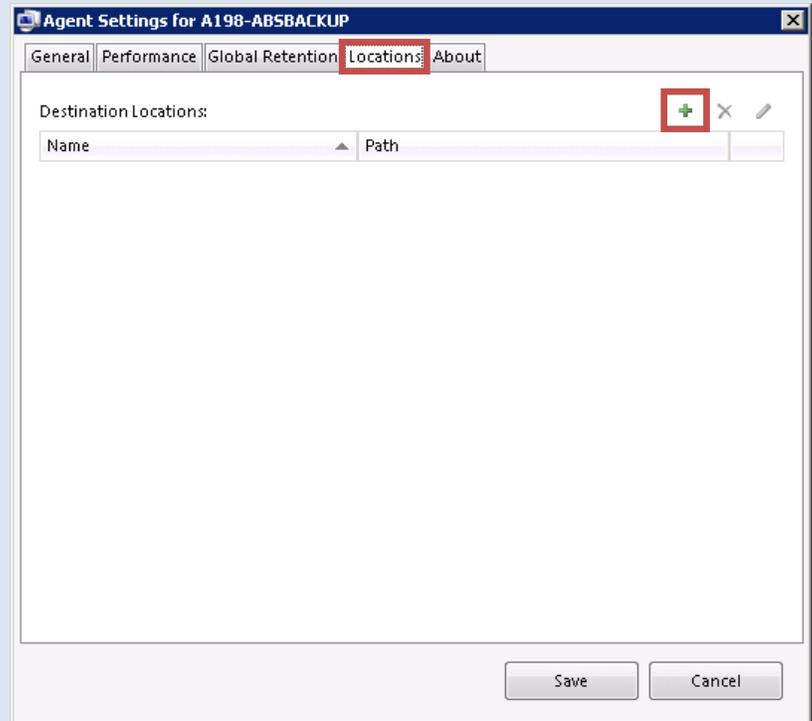
b. Click **Global Retention** tab

c. Uncheck **Automatically clean up backup....**



i Running global retention is not necessary when retention is configured individually for agents. This allows greater customization of retention settings.

- d. Select the **Locations Tab**, click the **"plus" icon**



- e. Setup the **Location Settings** using the information below

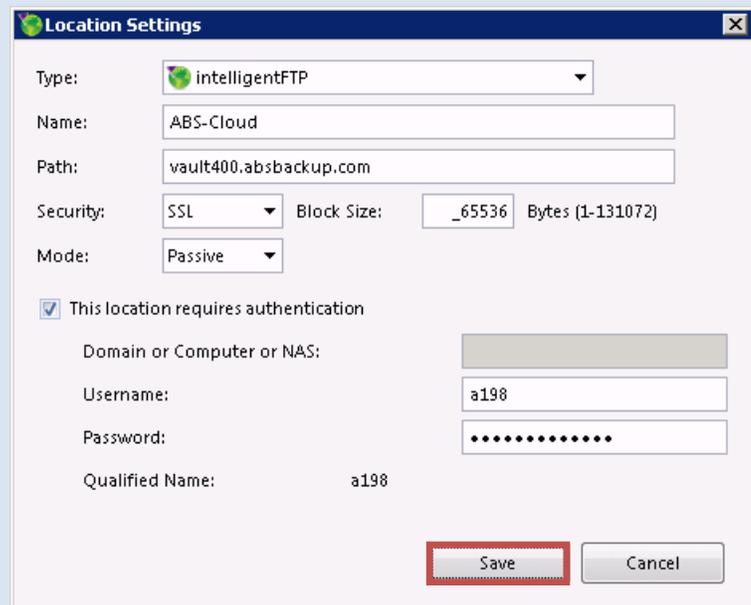
Type: **intelligentFTP**
Name: **ABS-Cloud**
Path: **ABS Vault Name**
Security: **SSL**
Block Size: **Default** (65536)
Mode: **Passive**

- f. Select **This location requires authentication**

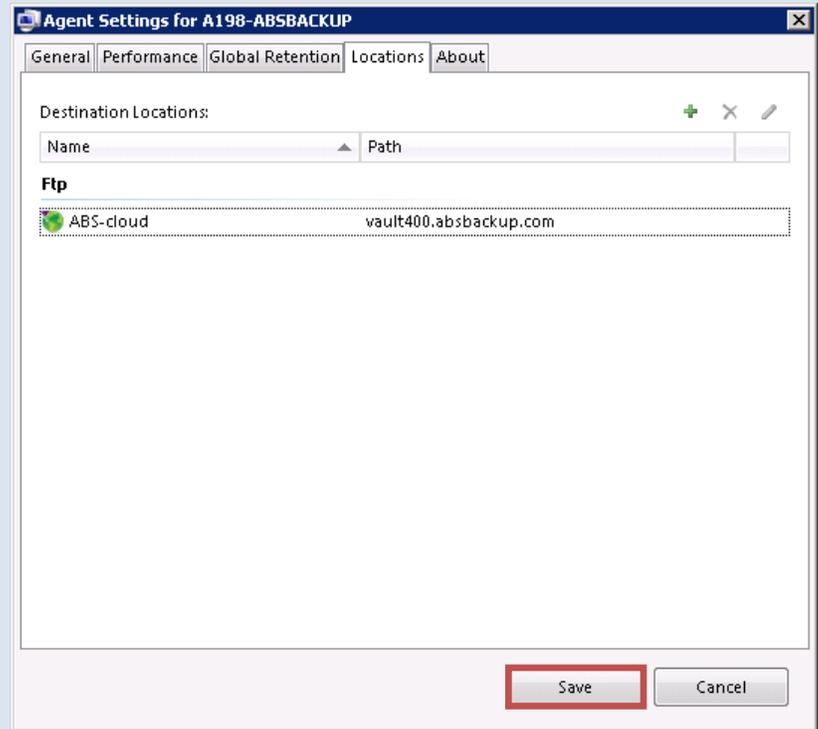
- g. Type in the Username and Password

 For the **ABS Vault Name**, **Username** and **Password**, refer to the **Activation Letter**

- h. Click **Save**

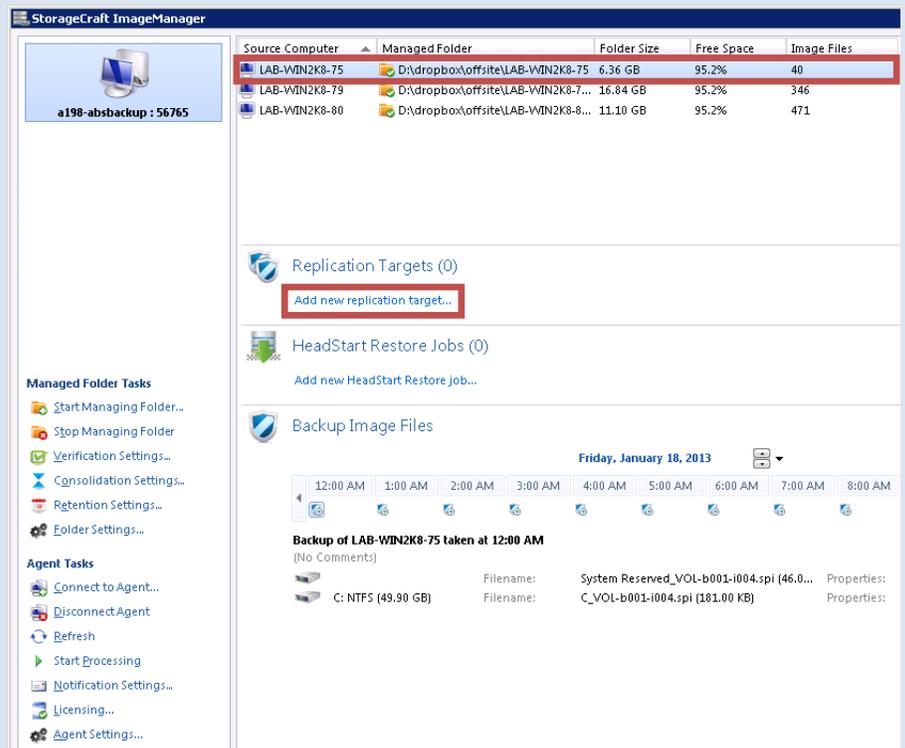


i. Click **Save**



2. Replication Targets

- Select the name of the machine being added for replication
- Click **Add new replication target...**



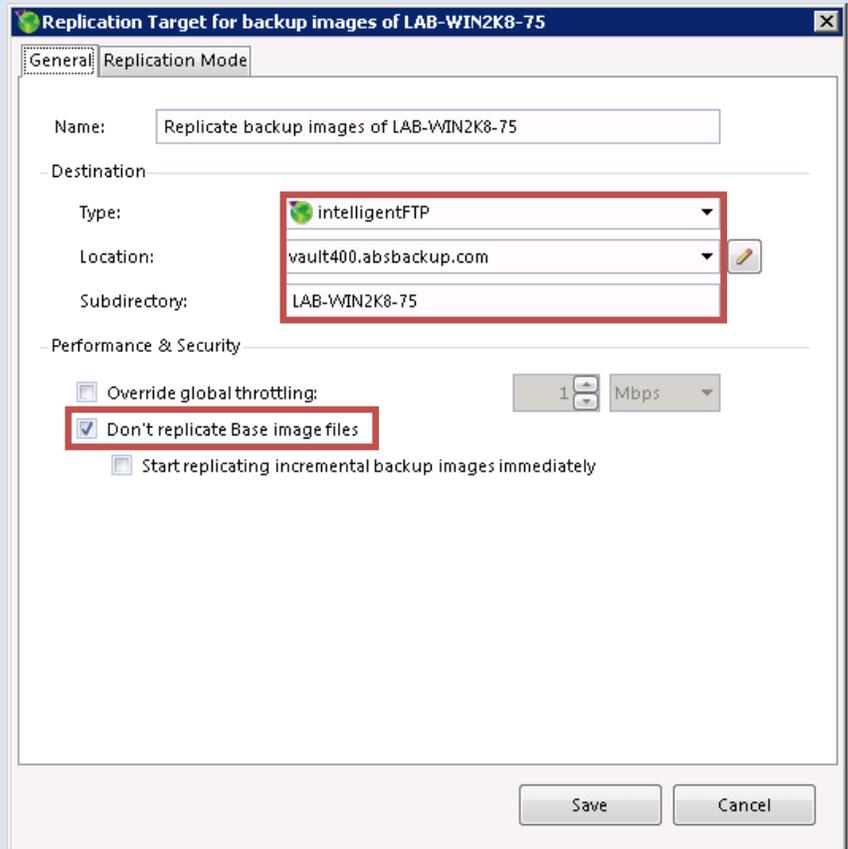
- c. For **type**, click the drop down, select **intelligentFTP**
- d. For **location**, click the drop down, select **vault name**
- e. For subdirectory, type in the **client computer name**
- f. Make sure **Don't replicate Base image files** is selected

! If you are not performing an initial seedload and would prefer to replicate entirely over the network, uncheck **Don't replicate Base image files**

- g. Click the **Replication Mode** Tab
- h. Make sure that **Yes - Replicate only... daily image files** is selected
- i. Click **Save**

Replication configuration is now **Complete**.

Please email us at support@absbackup.com to inform the support team that the appliance configuration is now complete.



Replication Target for backup images of LAB-WIN2K8-75

General | Replication Mode

Name: Replicate backup images of LAB-WIN2K8-75

Destination

Type: intelligentFTP

Location: vault400.absbackup.com

Subdirectory: LAB-WIN2K8-75

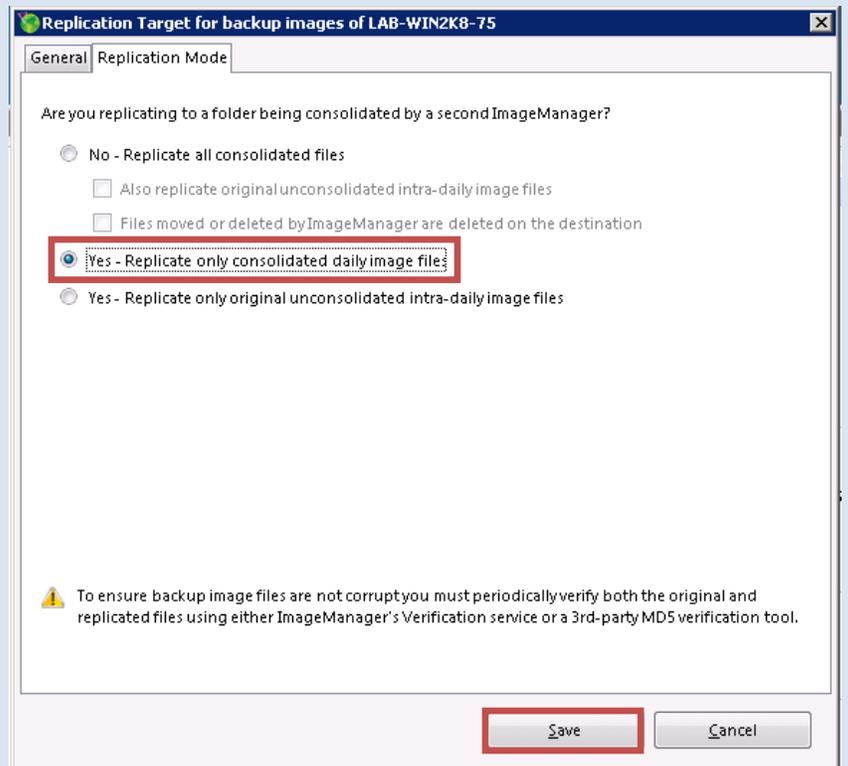
Performance & Security

Override global throttling: 1 Mbps

Don't replicate Base image files

Start replicating incremental backup images immediately

Save Cancel



Replication Target for backup images of LAB-WIN2K8-75

General | Replication Mode

Are you replicating to a folder being consolidated by a second ImageManager?

No - Replicate all consolidated files

Also replicate original unconsolidated intra-daily image files

Files moved or deleted by ImageManager are deleted on the destination

Yes - Replicate only consolidated daily image files

Yes - Replicate only original unconsolidated intra-daily image files

! To ensure backup image files are not corrupt you must periodically verify both the original and replicated files using either ImageManager's Verification service or a 3rd-party MD5 verification tool.

Save Cancel