StorageCraft ImageManager User Guide

Table of Content

StorageCraft ImageManager User Guide

Welcome to the StorageCraft® *ImageManager™ User Guide*. This guide describes how to use ImageManager to manage backup image files created with StorageCraft ShadowProtect®.

The guide includes the following major sections:

Additional Information

For new or additional details, see:

- ImageManager FAQ and Most Recent Version Updates lists a localized subset of the English ReadMe.
- ImageManager `English ReadMe` links you to the full ReadMe which contains enhancements, fixed issues and known issues.
- StorageCraft technical support lists important support information.
- StorageCraft glossary lists definitions for all StorageCraft products.
- StorageCraft *ShadowProtect User Guide* contains detailed ShadowProtect product information.

Documentation Conventions

⚠ This symbol designates a **Note** or **Warning** which contains critical information about ImageManager.

ImageManager User Guide document version 6.6.

December 10, 2014

1 ImageManager Overview

StorageCraft ImageManager helps you maintain and manage backup image files and storage space used by those files. Based on a policy that you create, ImageManager automatically consolidates incremental backup image files into daily, weekly, and monthly incremental images. ImageManager also provides ongoing verification and replication services for your backup images.

ImageManager consists of these components:

ImageManager Service: A Windows service that performs the backup file management for policies you define.

ImageManager Client: The UI that lets you create and manage retention policies for your ShadowProtect environment.

This section includes these topics:

⚠ **Note:** ImageManager policies only apply when you are using the continuous incrementals backup schedule defined in ShadowProtect. Standard weekly and monthly backup schedules do not use ImageManager and have separate retention policies. For more information, see "Creating Backup Image Files" in the *ShadowProtect User Guide*.

1.1 FAQ and Most Recent Version Updates

This page gives you a localized subset of the English ImageManager ReadMe. It contains the most recent and important information about ImageManager (version 6.6.0 as of December 2014). It is provided because the full ReadMe file is published only in English. If there is a discrepancy between this page and the English ReadMe, the English ReadMe is the controlling document.

ImageManager 6.6.0 (December 2014)

Enhancements

- Verbose logging switches added: ImageManager has a registry setting to enable verbose logging. You can set this level between 1-4 or 6. The values 1 through 4 simply increase the amount of detail written to the logs. Level 6 includes more logging information from the new ShadowStream.
- ImageManager now includes additional error messages that notify the user when an HSR Job encounters a problem updating the related VM file (VMDK, VHD, VHDX).

  Stop the errors by:

  - Stopping the HSR Job
  - Collecting the related log files
  - Submitting the log files to StorageCraft support

  Support will review the log files. If the VM file has encountered a critical update issue you will need to recreate the HSR Job.

  Note: Additional code was added in this ImageManager 6.6.0 release to help mitigate the chance of this error occurring.
- ImageManager now supports both legacy ShadowStream and the new ShadowStream options.
- ImageManager now includes improved localized string support for Polish and other languages.
- ImageManager now shows a warning pop-up message if you try to access or test an HSR ESXi location running ESXi 4.1 Update 3, or earlier. These older versions of ESXi are not supported.
- ImageManager now uses the following terms in the logs to differentiate between legacy ShadowStream and new ShadowStream log entries:

  - SST - Original ShadowStream
  - SST2 - New ShadowStream

Fixed Issues

- ShadowStream replication job logs now specify throttling numbers in bits per second (bps).
- Fixed an issue where global throttling couldn't be disabled for FTP and ShadowStream jobs.
- Fixed a licensing issue for the Brazilian Portuguese ImageManager. The Brazilian Portuguese key now works correctly.
- Fixed an issue where ImageManager wouldn't delete ShadowStream jobs if the destination server was not available.
- Fixed ImageManager so that it can now replicate using ShadowStream from a network share.
- Fixed the issue where in some rare cases, a replication job failed to replicate files immediately when using the new ShadowStream option. This occured if multiple ShadowStream replication jobs were created one after the other and the user selected one of the two replication options:
  - (1) Replicate only consolidated daily image files
  - (2) Replicate only original unconsolidated intra-daily image files

  The error message seen by the user is:

  - Error sending
    "Sync error: RemoteInfoFile not present after successful send"
- Fixed the issue where in some situations if an FTP connection was temporarily dropped the newly replicated files were written to the root folder, rather than the correct sub-folder.
- Fixed an issue where Concurrent Processing settings were not being immediately applied.
- Fixed ImageManager so that it no longer generates a verification exception in the Windows Event Manager when managing a large number of folders (300+).
- Fixed the username and password functionality so that entries are no longer removed when the Notification Settings are saved and re-opened.
- Fixed the issue where under rare situations ImageManager might indicate that a Replication job is in a "Ready" status when files are queued for replication, but not actually being replicated. This might happen for any replication type.

  This condition is more likely to be triggered in situations where the target server (or ShadowStream Service) is being restarted. ImageManager should automatically begin replicating within a maximum of 15 minutes. To troubleshoot these conditions, you can enable ImageManager DetailedLogging.

  Some ImageManager logs would also include the following harmless "SyncFiles error" message when replicating files (see example below). This has also been fixed in this release.

  Example:

  - 07-Oct-2014 12:25:24 SyncFiles error(s):
    Specified cast is not valid.
- Fixed ImageManager so that it now includes improved support for unicode characters for ShadowStream job usernames, passwords and paths.
- Fixed ImageManager so that the User Interface no longer hangs if a ShadowStream job is paused and restarted in rapid succession.
- Fixed the issue where creating a new Replication Job in ImageManager could cause a .remote file to not be written to the correct shared folder on the remote server. This didn't affect Replication at all but generated an error in the logs. This issue is now fixed in this release.
- Fixed the issue where if a user mounted a backup file as writeable and then chose the "Shrink" option when dismounting the backup file, the resulting file may not have been correctly verified by ImageManager. The file was fine but ImageManager may have incorrectly marked it as bad. The errors generated might include the following error messages:
  - sbrest 503 Fatal I/O error on (-1392 Invalid data format.)
  - (loader) 504 Final error (-1392 Invalid data format.)

  Unfortunately, this could result in ShadowProtect reporting a false verification warning when it next creates a backup for that chain. The warning relates to the backup that the user manually "shrunk".

  In this release ImageManager correctly identifies and verifies a backup "shrunk" by the user. This also prevents ShadowProtect from listing a verification warning for the file.

- Fixed an issue so that users are now able to enter a value of zero (0) as a peak hour throttling entry.
- Fixed the issue where on some Windows OS versions, ImageManager attempted to check if there was a valid .Net 3.5 framework installed. If it was missing, the installer normally showed a pop-up window to warn the user. This installer pop-up window is now localized.
- Fixed ImageManager so it is now possible to delete an FTP Replication job without first pausing the job. Previously this caused the ImageManager user interface to hang.
- Fixed an issue where In some rare situations the ImageManager user interface didn't report when there was a problem replicating a file.

Known Issues

- In some situations it is possible that ImageManager can successfully write the contents of a new incremental backup to the VMDK file but then fail to update the related .HSR file information. This can occur when another process has a lock on the .HSR file. To avoid this, make sure there is no AV product, or similar, that might lock the .HSR files.

  Note: This release of ImageManager 6.6.0 includes additional error handling to limit the chance of this error occurring. If this situation occurs ImageManager displays an error in the User Interface.

- Japanese passwords in HSR jobs aren't being accepted.
- HSR jobs that create VHD files are unable to select all volumes in the managed folder.
- HSR jobs to a VMDK disk on an ESXi server are failing with the error: "Missing arguments" in HSR job.
- Some of the Polish strings are missing in this release.
- If you create an HSR job and then later increase the size of the Source Volume the HSR Job fails. Increasing the Source Volume used for an HSR Job is not currently supported. If you increase the size of the Source Volume you need to delete the HSR Job, start a new backup chain, and then start a new HSR job with the new backup chain.
- HSR to VCenter/ESXi returns Access Denied error when processing starts.
- Replication fails on files that have previously been sent and won't continue until files are removed from destination.
- An "Unknown error encountered" message is displayed if you attempt to upgrade from ImageManager version 6.5.1 to version 6.5.4 if the "My Documents" folder is missing.

1.2 ImageManager Features

ImageManager has the following basic features:

- **Verify:** Based on a frequency that you define, ImageManager automatically verifies, and re-verifies, the integrity of backup image files. This is similar to manual verification when using the Verify Wizard in ShadowProtect.
- **Consolidate:** Based on a policy that you define, ImageManager automatically consolidates incremental backup image files. This limits the risk of having large backup image file chains where one bad file can render a whole backup image useless.
- **Retain:** Based on a policy you define, ImageManager automatically deletes and/or retains image files after a selected period of time. These policies apply to intra-daily, daily, and weekly image files. You can also define how long to keep consolidated monthly images (-cm) (1 to 120 months) before cleaning them up. This creates a rolling consolidated image file (-cr) that consists of the number of specified -cm image files.
- **Replicate (Local):** Based on a profile that you define, ImageManager automatically creates redundant copies of backup image files to locally-attached hard drives. Smart replication technology evaluates the consolidation policy to avoid transferring unnecessary or obsolete backup image files.

Beyond these basic features, ImageManager offers other premium features available with the purchase of a job license or StorageCraft Cloud service level agreement:

- **Replicate (Cloud Services):** Based on a profile that you define, ImageManager automatically replicates encrypted backup image files to the StorageCraft Cloud.
- **Replicate (Network):** Based on a profile that you define, ImageManager automatically creates redundant copies of backup image files to a network share.
- **Replicate (Off-site):** Based on a profile that you define, ImageManager automatically creates and sends copies of backup image files to a remote server. ImageManager provides both high-speed ShadowStream replication and intelligentFTP replication options for off-site replication.
- **HeadStart Restore:** HeadStart Restore (HSR) is the ability to restore a backup image while ShadowProtect continues to add Incremental backup images to the same backup image chain. For information about using HeadStart Restore, see HeadStart Restore Scenarios.

For more information about licensing ImageManager or its premium features, see Licensing.

1.3 HeadStart Restore Scenarios

With StorageCraft HeadStart Restore (HSR), you can start a system restoration before a disaster hits. These scenarios illustrate some of the ways to benefit from HSR.

Virtual Server Migration

Problem: You need to migrate a database server with 2TB of data to a new virtual machine environment, but you cannot afford to have the server offline for three days to migrate the data.

ImageManager Solution: Keep the old server running, and generating incremental backups, while you begin a HeadStart Restore of the same backup image chain into a virtual machine file (VMDK, ESX Server, VHD). Over time, the HSR catches up to the most current incremental from the database server, at which point you can take the old server down in off hours, apply the final incremental backup to the new server, and bring the new system online very quickly. You can even migrate the operating system volume by doing a Hardware Independent Restore (HIR) to make sure the migrated OS boots properly on the new server hardware.

Hardware Failure

Problem: You have a database server and the 20TB disk array crashes. You need to get the system back online and replace the disk subsystem.

ImageManager Solution: Use ShadowProtect's VirtualBoot feature to boot the latest backup image of your database server and configure the VM to continue adding incremental backups to your original backup image chain. Users can then continue to use the VM database server as if the original is still online.

Once the VM is running, start an HSR to the database server's new disk subsystem. When HSR catches up to the most current incremental, you can finalize the HSR installation on the new disk subsystem, take the VM down, then bring the original database server back online.

Virtual Standby Server

Problem: You want to have a stand-by server that can take over if your primary server fails, but you can't afford the high-priced server mirroring technology.

ImageManager Solution: Your production server generates continuous incremental backups. Configure an HSR solution to automatically restore those incremental backup images into a virtual machine file (VMDK, ESX Server, or VHD). If your production server fails for any reason, finalize the HSR, then use the Recovery Environment to apply any remaining incremental images to the virtual machine (a matter of minutes), then bring it online as a replacement for the failed production server.

2 Install ImageManager

This section covers:

2.1 System Requirements

Hardware Requirements

ImageManager has the following hardware requirements:

- At least 1 GB physical RAM (4 GB recommended).
- At least 75 MB of free hard disk space for installation files.
- Must meet the minimum operating system support requirements listed in the following section.

Operating System Support

ImageManager runs on:

Windows OS	Version
Windows Server 2012 R2 (Requires .NET 3.5)	(64-bit x64)

Windows Server 2012 (Requires .NET 3.5)	(64-bit x64)
Windows Small Business Server 2011	(64-bit x64)
Windows Server 2008 R2 Foundation	(64-bit x64)
Windows Server 2008 R2	(32-bit x86 and 64-bit x64)
Windows Server 2008	(32-bit x86 and 64-bit x64)
Windows Small Business Server 2008	(32-bit x86 and 64-bit x64)
Windows EBS Server 2008	(32-bit x86 and 64-bit x64)
Windows Server 2003	(32-bit x86 and 64-bit x64)
Windows Small Business Server 2003 Standard	(32-bit x86 and 64-bit x64)
Windows Small Business Server 2003 Premium	(32-bit x86 and 64-bit x64)
Windows 8.1 (Requires .NET 3.5)	(32-bit x86 and 64-bit x64)
Windows 8 (Requires .NET 3.5)	(32-bit x86 and 64-bit x64)
Windows 7	(32-bit x86 and 64-bit x64)
Windows Vista Home Basic	(32-bit x86 and 64-bit x64)
Windows Vista Home Premium	(32-bit x86 and 64-bit x64)
Windows Vista Ultimate	(32-bit x86 and 64-bit x64)
Windows Vista Enterprise	(32-bit x86 and 64-bit x64)
Windows Vista Business	(32-bit x86 and 64-bit x64)
Windows XP Media Center	(32-bit x86 and 64-bit x64)
Windows XP Professional (SP2 or above)	(32-bit x86 and 64-bit x64)
Windows XP Home	(SP2 or above) (32-bit x86 and 64-bit x64)

Note: ImageManager runs on most Windows operating systems but StorageCraft recommends using a Windows Server operating system such as Windows Server 2008 R2 or Windows Server 2012.

Other Requirements

Microsoft .NET version 3.5 Required

ImageManager requires Microsoft .NET version 3.5 Service Pack 1 (for some operating systems) or higher (for other operating systems). You must ensure that the right version of .NET is installed before installing ImageManager 6. The information below will help you decide which versions of .NET are needed for your operating system.

- Windows Server 2012 normally has .NET4.5 installed by default. You also must install .NET 3.5 manually. The installer for .NET 3.5 is under the "Turn Windows Features on or off" option.
- Windows 8 normally has .NET 4.5 installed by default. You also must install .NET 3.5 manually. The installer for .NET 3.5 is under the "Turn Windows Features on or off" option.
- Windows Server 2008 R2 does not come with .NET Framework pre-installed. The installer for .NET 3.5 is under the "Turn Windows Features on or off" option and must be installed manually.
- *Windows Server 2008 does not come with the .NET Framework pre-installed. The installer for .NET 3.0 is under the "Turn Windows Features on or off" option. However, ImageManager requires version 3.5 or 4.0. The ImageManager installer attempts to download and install .NET 3.5 or higher. If that fails, you can download and install the Framework manually.
- *Windows Server 2003 R2 requires a manual installation of .NET 3.5 (in some cases) before you can install ImageManager 6.
- *Windows Vista normally has .NET 3.0 installed by default. The ImageManager installer attempts to download and install .NET 3.5 or higher. If that fails, you can download and install the Framework manually.

- Windows 7 normally has .NET 3.5 installed by default.

* The Microsoft .NET Framework 3.5 Service Pack 1 can be downloaded here.

ImageManager Activation

- Automatic activation requires an Internet connection.
- Manual Activation requires you to complete the form on the StorageCraft Product Activation page.

2.2 Upgrade from ImageManager 4.x or 5.x

If you upgrade ImageManager from v4.x, or v5.x you don't need to uninstall the earlier version. Close the ImageManager Console (if it is running) prior to doing the install. The installer preserves your existing configuration and job settings.

Warning: Run the installation as a Windows administrator to prevent losing settings from previous installations. Right click on the ImageManagerSetup.exe file then select **Run as administrator**.

Premium Services

If you purchased a job license for intelligentFTP, HeadStart Restore, or Network Replication with ImageManager 4.x or 5.x, these convert to one license for intelligentFTP (includes one license for network replication) and one license for HeadStart Restore.

2.3 Installation

To install ImageManager:

1. Launch the ImageManager installer (`ImageManagerSetup.exe`).
   You can find the ImageManager installer in the following locations:
   - **ShadowProtect Recovery CD**: `Installers\ImageManagerSetup.exe`
   - **Online**: On the STC Trial Downloads page (http://www.storagecraft.com/trial_downloads.php).

     Warning: Run the installation as a Windows administrator to prevent losing settings from previous installations. Right click on the ImageManagerSetup.exe file then select **Run as administrator**
2. Select the language then click **OK**.
3. Click **Next** on the ImageManager Wizard Welcome page.
4. Follow the steps in the Installation Wizard to install the ImageManager software.
5. Click **Finish** when the installation is finished.
6. Reboot the computer to ensure all drivers load properly.
7. Click **Start** > **Programs** > **StorageCraft** > **StorageCraft ImageManager** to start ImageManager.

Modifying the Configuration File

The ImageManager agent loads automatically after installing ImageManager. A configuration file (`ImageManager.exe.config`) is used to set the agent parameters. You can change the port used by the ImageManager agent in the configuration file, if necessary.

2.4 Activate Premium Features

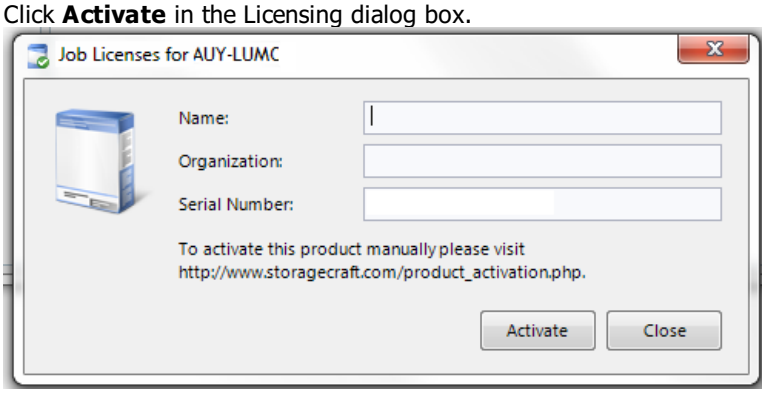
You need to use ImageManager's activation function if you purchased one or more premium ImageManager features (HeadStart Restore, ShadowStream or intelligentFTP).

Note: ImageManager standard functions such as consolidation, retention, verification, or local replication are available without activation. Replicating to the StorageCraft Cloud does not require activation but does require a cloud account and a service level agreement.

You need an Internet connection for automatic activation.

To activate one or more ImageManager premium features:

1. Click **Licensing** in the configuration pane of the ImageManager console.
2. Click **Activate** in the Licensing dialog box.



3. In the job licenses dialog box, provide the requested information, then click **Activate**.
   - **Customer Name:** (Optional) Specify the name of the product purchaser.
   - **Organization:** (Optional) Specify the name of the company.
   - **Serial Number:** Enter the Product Key received with ImageManager.

   ImageManager communicates with the StorageCraft Licensing server.
4. If the activation is successful, click **OK**.
   If the activation was not successful, review the message to determine why it failed. To correct the problem:
   1. Review the information accuracy in the Product Activation dialog box. Correct any errors, then click **Activate** to resubmit the activation request.
   2. If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again. If you continue to have problems activating these features, contact Product Support.

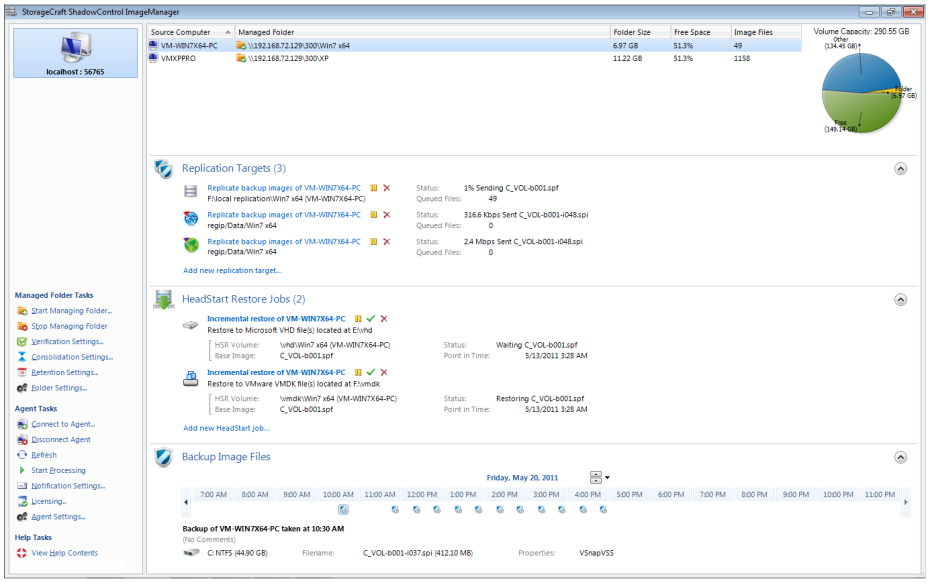
ImageManager can be configured to use premium features after they are activated.

You can also activate manually by going to the StorageCraft Product Activation page if automatic activation can't be done.

3 User Interface Overview

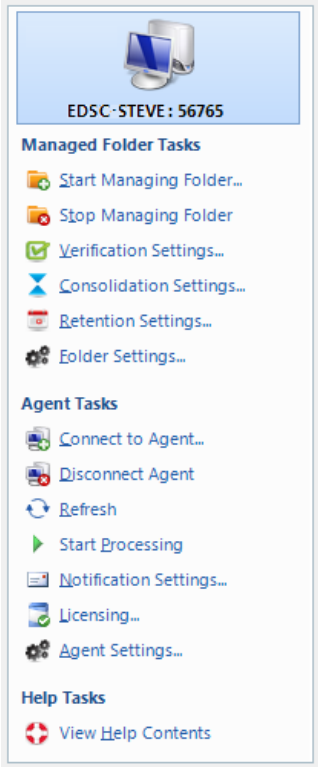
The ImageManager user interface consists of the:

- ImageManager Navigation Pane
- ImageManager Managed Folder Pane
- ImageManager Services



3.1 ImageManager Navigation Pane

The left-side Navigation pane displays a list of connected ImageManager agents. ImageManager displays the information for the selected agent.



The Navigation pane also provides links to ImageManager features and functionality:

Managed Folder Tasks

Link	Function / Description
Start Managing Folder	Select the storage locations for backup image files and start managing them with ImageManager. (See Create a Managed Folder).
Stop Managing Folder	Stop managing the selected folder and remove it from the Managed Folder window.
Verification Settings	Configure the automated verification service. (see Verifying Backup Image Files).
Consolidation Settings	Configure ImageManager's consolidation service. (see Consolidating Backup Image Files).
Retention Settings	Configure which image files ImageManager retains, and how long they are kept. (see Consolidating Backup Image Files).
Folder Settings	Modify the settings for the selected managed folder (see Create a Managed Folder).

Agent Tasks

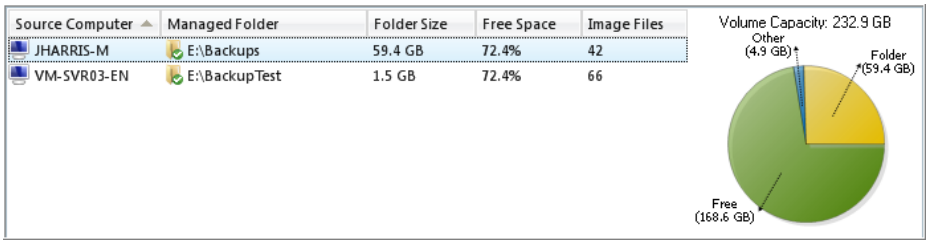
Button or Link	Function or Description
Connect to Agent	Connect to an ImageManager agent on another system. (see Connecting to an ImageManager Agent).
Disconnect Agent	Disconnect the ImageManager Console from the selected ImageManager agent.
Refresh	Display available ImageManager agents after running a new system query.
Start Processing	Perform the operations defined in the verification and consolidation schedules.
Notification Settings	Select default or custom settings for ImageManager email events and notifications. (see Configuring ImageManager Notifications).
Licensing	Select and configure ImageManager agent licensing options (see Configuring an ImageManager Agent).
Agent Settings	Select ImageManager agent options and configure the settings. (see Configuring an ImageManager Agent).

Help Tasks

Button or Link	Function or Description
View Help Contents	StorageCraft ImageManager user guide

3.2 Managed Folder Pane

The managed folder pane (top-center) displays information about the connected ImageManager agent. Select a managed folder in the list to see the usage pie chart. Selecting a managed folder also puts focus on it for operations in the navigation and services panes.



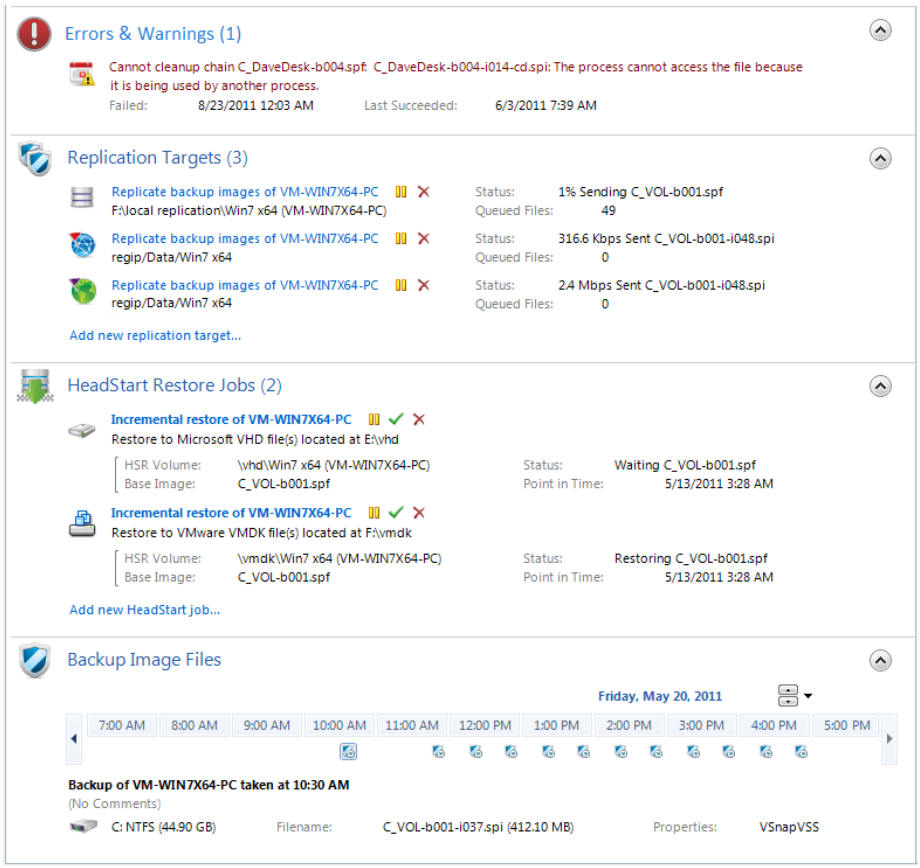
The managed folder pane provides the following information about each managed folder:

Link	Description
Source Computer	The name of the computer where ShadowProtect creates and stores (i.e. where the managed folder resides) the backup image files managed by ImageManager.
Managed Folder	The path to the managed folder where the backup image files (managed files) are stored.
Folder Size	The amount of storage space used by backup image files in the managed folder.
Free Space	The amount of available free storage on the source computer where the managed folder resides.
Image Files	The number of backup image files contained in the managed folder.
Volume Capacity	The graphical view of volume usage (in GB) for the managed folder.

3.3 ImageManager Services

The ImageManager services pane gives you access to, and control over your backup images. It contains the following main categories:

- Errors & warnings
- Replication targets
- Headstart restore jobs
- Backup image files



Each service displays in its own pane that you can expand and collapse as needed. Within each pane you can see information about that service and perform tasks related to it.

UI Component	Description
Errors and Warnings	Displays error or warning information about ImageManager's automated Verification and Consolidation services for backup image files. **Note:** This pane only displays if ImageManager encounters verification or consolidation errors.

Replication Targets

Displays information about ImageManager's automated backup image replication service (see Replicating Backup Image Files).

From the *Replication Targets* pane you can:

Add New Replication Target: Opens the Replication Target dialog box where you can configure a target location to use with the replication service.
Edit a Replication Target: Click the replication target name to modify the settings of an existing replication target.

Delete Replication Target: Deletes a replication target.

Pause Replication Target: Stops replicating to the associated target.

Enable Replication Target: Resumes replication for a previously paused replication target.

The Replication Target list icons represent the type of destination connection/drive:

- Locally-attached drive
- intelligentFTP-connected drive
- ShadowStream-connected drive

HeadStart Restore Jobs

Displays information about ImageManager's HeadStart Restore (HSR) service (see Using HeadStart Restore).

From the *Head Start Restore* pane you can:

Add New HeadStart Job: Opens the HeadStart Job dialog box where you can configure a new HSR job.

Edit a HeadStart Job: Click the HeadStart job name to modify the settings of an existing replication target.

Delete HeadStart Job: Deletes a HeadStart job.

Pause HeadStart Job: Stops a HeadStart job.

Enable HeadStart Job: Resumes a previously paused HeadStart job.

Finalize HeadStart Job: Opens the Finalize dialog box, where you can prepare the selected HSR target for use once the restoration process is complete (see Finalizing a HeadStart Job).

The HeadStart Restore list icons represent the type of destination drive for that job:

- Microsoft VHD virtual disk drive
- VMware VMDK virtual drive

Backup Image Files

Displays information about the backup image files in the selected managed folder. You can also browse to a particular day using the selector to see the backup image files created on that day (see Browsing Backup Image Files).

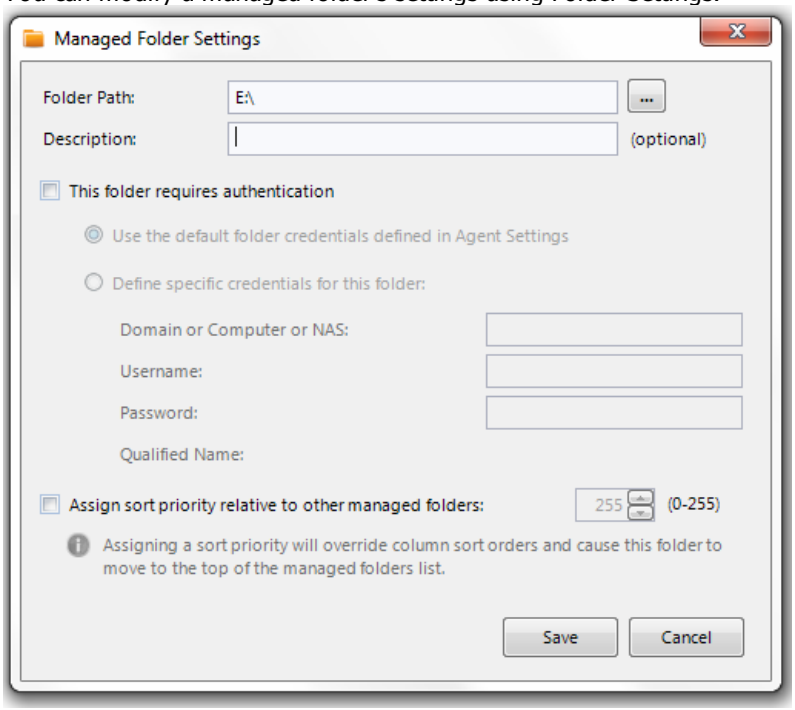
4 Configure ImageManager

Before using any of the ImageManager services, you must configure the ImageManager console to access the system you want to manage. These configuration tasks follow a logical order:

- Connect to an ImageManager Agent
- Configure an ImageManager Agent
- Create a Managed Folder
- Configure ImageManager Notifications

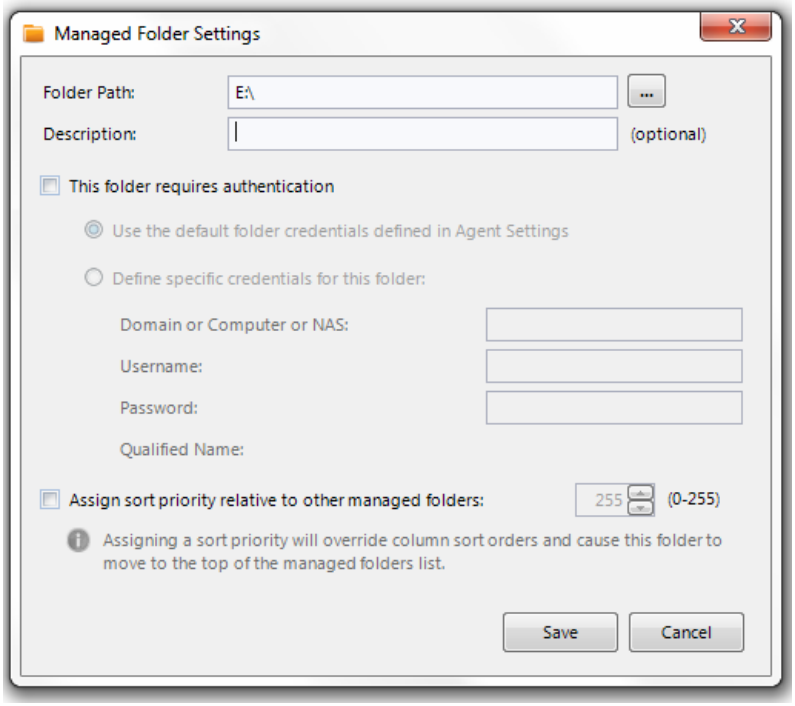
4.1 Manage Folder Settings

You can modify a managed folder's settings using Folder Settings.



To modify the settings of a managed folder

You can modify a managed folder's settings using Folder Settings.



To modify the settings of a managed folder

1. In the ImageManager console, select the ImageManager agent that you want to configure.
2. In the Navigation pane, click **Folder Settings**.
3. In the Managed Folder Settings dialog box, provide the required information, then click **Save**.

Description	(Optional) A description of the managed folder.
Authentication	(Conditional) The managed folder's authentication credentials. You can either use the default credentials specified in the ImageManager agent settings (see Configuring an ImageManager Agent), or specify authentication credentials specific to this managed folder.
Assign sort priority	(Default: Disabled) When enabled, ImageManager sorts the managed folders in the Managed Folder pane in ascending order based on the specified sort value (0 - 255). ImageManager will then run these jobs in this order.

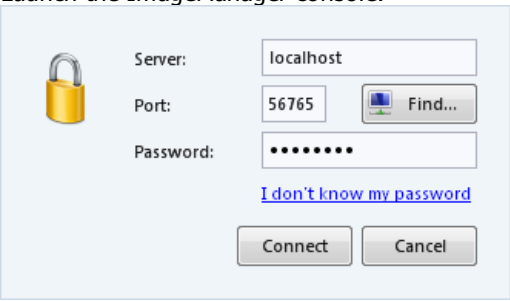
Note: You cannot modify the path of the managed folder. If you need to change the path, Stop Managing Folder to delete it, then use Start Managing Folder to specify the new path, then reconfigure the folder path.

4.2 Connect ImageManager Agents

Connect the ImageManager console to one or more ImageManager agents to manage the backup image files.

To connect to an ImageManager agent:

1. Launch the ImageManager console.



2. In the Connect dialog box, provide the required information, then click connect.

Server	The name or IP address of the system running the ImageManager agent. You can use the *localhost* server name to connect to an ImageManager agent running on the same system as the ImageManager console. Click **Find** to browse the network by computer name for a system you want to connect to.
Port	The TCP port used to communicate with the ImageManager agent. The default ImageManager agent port is 56765. You can change the port used by ImageManager in the ImageManager\ImageManager.exe.config file. **Note:** You might need to modify your firewall settings to make the ImageManager agent port accessible.
Password	The ImageManager agent password. The default password, when connecting to an ImageManager agent for the first time, is "*password*". ImageManager prompts you to change the password after connecting for the first time. Click **I don't know my password** to get instructions about how to reset a forgotten password. See Resetting the Agent Password.

ImageManager connects to the specified agent and displays its icon in the navigation pane.

Connecting to Multiple ImageManager Agents

To connect to multiple ImageManager agents simultaneously

1. Click **Connect to Agent** in the navigation pane. ImageManager opens the Connect dialog box.
2. Specify the details for the additional ImageManager agent.
3. Click **Connect**.

ImageManager connects to this additional agent and adds the agent's icon to the navigation pane.

Note: ImageManager opens port 8080 when it starts up. This can cause problems with web servers and other applications that might already be using that port. You can avoid this conflict by changing the ImageManager configuration file to use a different port.

1. Open the ImageManager config file: `C:\Program Files (x86)\StorageCraft\ImageManager\ImageManager.exe.config`
2. Change the "wcfPort" from the default value of 8080 to one of the available dynamic ports on your computer (the range is 49152 through 65535). Be sure to select a port that isn't already in use by another application or service. For example: Do not use the default ImageManager port number 56765.
3. Restart the ImageManager service with services.msc.

4.3 Select Agent Passwords

Connect to ImageManager Agents the first time with the default password of `password`. You must then select a new (your own) agent password while connected.

If you forget your selected password, use the StorageCraft password reset utility to change it back to the default.

To reset the agent password

1. Make sure the ImageManager console is closed.
2. Download (save) the Password Reset utility to a location of your choice.
3. Browse to the location where you saved the utility.
4. Run (as administrator) the Password Reset utility (right-click on ImageManager.ResetPassword.exe, then select Run as Administrator).
5. Restart ImageManager.
6. Connect to the ImageManager agent using the default password of `password`.
7. When prompted, select a new agent password of your choice.

4.4 Authenticate Agents

The ImageManager console needs to authenticate to the agent through a secure TCP connection.

Same Domain Authentication

If the console and agent are installed on the same computer, or on computers in the same Windows domain, the authentication happens automatically in the background.

Different Domain or Workgroup Authentication

However, if the console and agent are installed on computers in different domains, or in a Windows workgroup, you must create a user account on the agent computer for the console to use. This account must use the same credentials (username and password) as the user (logged-in) that started the console.

An example for the MSHOME workgroup:

On the Console Computer

- In the MSHOME workgroup
- Logged in as JDoe
- ImageManager Console running

On the Agent Computer

- In the MSHOME workgroup
- Not logged in
- User account JDoe must exist
- Password for JDoe must be the same as user JDoe on the console computer.
- ImageManager Agent running (under the context of LocalSystem)

Important: In this scenario the agent computer must have an account named "JDoe". The password for the "JDoe" user account on the agent computer must be the same as the password for the "JDoe" user account on the console computer. This allows the ImageManager console to successfully authenticate to the ImageManager agent.

4.5 Configure Agents

There are two ImageManager Agent configuration options:

- Agent Settings
- Licensing

Agent Settings

Select **Agent Settings** to modify ImageManager agent settings. The Agent Settings dialog includes the following tabs:

- General
- Performance
- Global Retention
- Locations
- About

Licensing

StorageCraft licenses premium features on a per-job basis. Each job license grants one job to a single ImageManager agent. (You can later reassign a license to a different job or to a different agent as needed.) Each license supports one of the following operations:

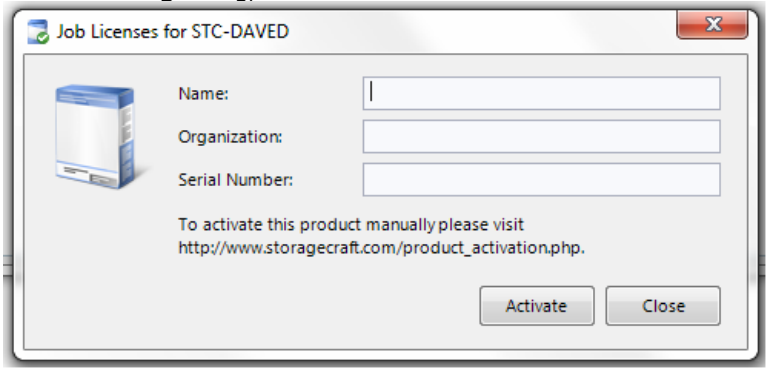
- Each intelligentFTP license supports one Network Replication or one off-site replication job using intelligentFTP.
- Each ShadowStream license supports one Remote Replication (Off-site) job using ShadowStream. (See ShadowStream for details.)
- Each HeadStart Restore license supports one device restoration.

For more information about each of these operations, see ImageManager Features

Note: You can purchase as many premium feature job licenses as needed, but each license is activated for only a single ImageManager console. You cannot purchase a premium license and then move its job operations among multiple ImageManager consoles. For more information about ImageManager licensing, see ImageManager License Scenarios.

To activate ImageManager premium features

1. In the Configuration pane of the ImageManager console, click **Licensing**.
2. In the **Licensing** dialog, click **Activate**.



3. In the Activate StorageCraft ImageManager dialog box, provide the requested information, then click **Activate**:
   - **Customer Name:** (Optional) Specify the name of the product purchaser.
   - **Organization:** (Optional) Specify the name of the company.
   - **Serial Number:** Enter the Product Key that you received when purchasing ImageManager or premium feature licenses.
4. If the activation is successful, click **OK**.

If the activation was not successful, review the message to determine why the activation was unsuccessful. To correct the problem, do one of the following:

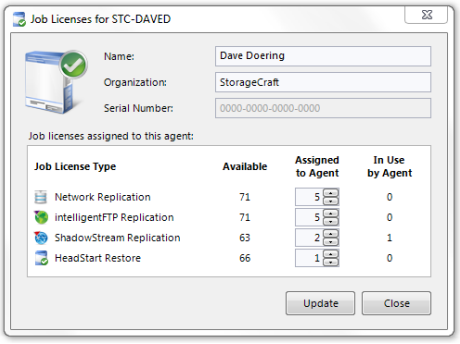
1. Review the information in the Product Activation dialog box for accuracy. Correct any errors, then click **Activate** to resubmit the activation request.
2. If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again. If you continue to have problems activating these features, contact Product Support.

Assigning Licenses

The Licensing dialog box also controls the assignment of job licenses to this agent. These features include:

- Network Replication
- intelligentFTP Replication
- ShadowStream Replication
- HeadStart Restore

ImageManager licenses these premium features on a per-job basis and lists them in the dialog box after they are installed:

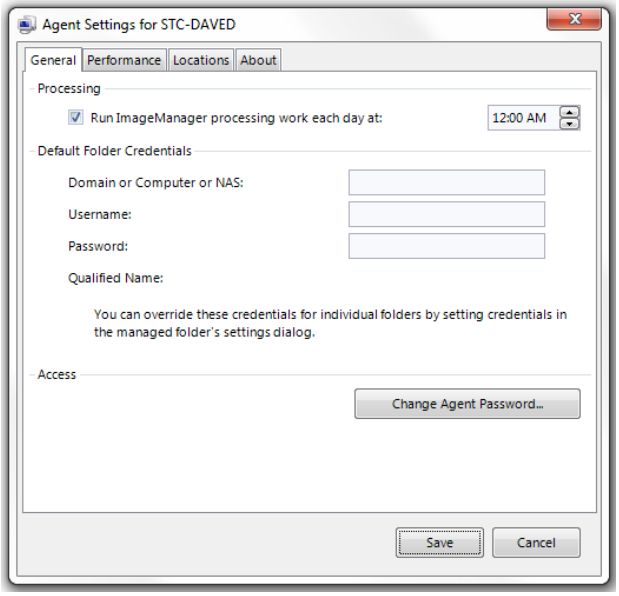


Each job license type shows its usage. The Network Replication and intelligentFTP Replication represent the same licenses. Assigning a Network or an intelligentFTP replication license will therefore decrement both of these licenses.

Field	Description
Available	Shows the total number of purchased job licenses for this feature. This pool is available to all ImageManager agents.
Assigned to Agent	Shows the number of the purchased job licenses assigned to the selected agent. Use the *Assigned to Agent* column to dynamically assign licenses or modify their assignments. Use the selector to specify or modify the assignment. Click **Update** to reflect the new assignment. **Note:** You cannot reduce the number assigned to this agent to less than the number already in use by jobs for this agent. If you need to do so, you must delete those job(s) first in order to reduce this number.
In Use by Agent	Shows the number of licenses actually in use by a ImageManager job for this selected agent.

General

The settings on the General tab let you configure or modify the ImageManager agent properties.



To configure ImageManager agent properties:

1. In the ImageManager console, select the ImageManager agent that you want to configure.
2. In the Configuration pane, click **Agent Settings**.
3. In the **General** tab of the Agent Settings dialog box, provide the required information, then click **Save**.

Control	(Default: Enabled at 12:00 AM) Lets you specify a time of day when the ImageManager agent performs its daily validation and consolidation operations. Disabling this setting suspends the ImageManager agent's automated re-verification and consolidation services. However, you can manually start the agent processing of a single job, multiple jobs, or all jobs by clicking **Start Processing** in the Configuration pane (see Navigation Pane).
Default Folder Credentials	The default authentication credentials used by the ImageManager agent to access managed folders. You can override these credentials for a specific managed folder, if necessary (see Create a Managed Folder).
Access	Click **Change Agent Password** to update the password used to access the ImageManager agent.

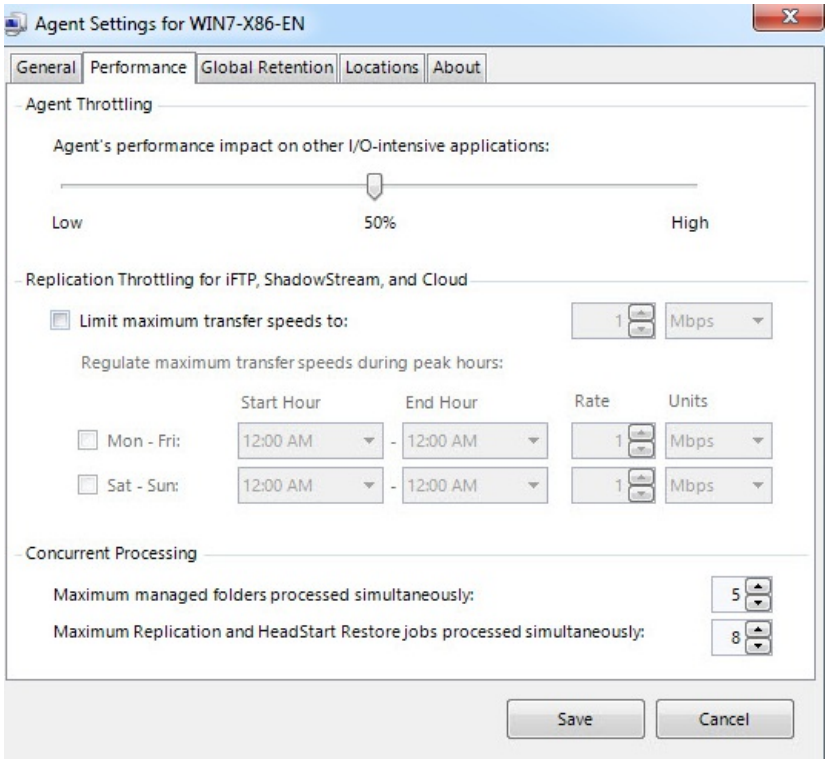
Note: To modify the ImageManager agent port setting, edit the ImageManager configuration file: `ImageManager\ImageManager.exe.config`.

Performance

The settings on the **Performance** tab let you configure or modify how the ImageManager agent uses system resources.

The Performance tab has these settings:

- Agent Throttling
- Replication Throttling
- Concurrent Processing



Agent Throttling

Use the Agent Throttling setting to increase or decrease the CPU cycles available for processing ImageManager operations. This setting lets you prioritize ImageManager against other CPU-intensive application tasks. The default setting is 50%, which means that ImageManager can use up to 50% of CPU processing time to complete its work. The adjustable range is from 1% to 100%.

To modify the setting, click on and move the arrow to the left or right of the scale. As the arrow moves, the percentage value changes to reflect the new setting.

Replication Throttling for iFTP, ShadowStream, and Cloud

This optional setting lets you manage the network bandwidth used by ImageManager by limiting transfer speeds. Replication throttling allows you to modify how fast ImageManager can upload data to a remote site. When "Limit maximum transfer speeds" is enabled, the default throttling setting is 1 Mbps, with a range from 1Kbps to 999 Gbps. This setting applies if you have purchased and installed one or both of the add-on transfer tools: intelligentFTP or ShadowStream, or if you are using the StorageCraft Cloud. The download speed (the transfer rate from the remote site back to the agent) is fixed at 15Mbps maximum.

Note Throttling applies to each job instead of all jobs which means network usage increases as jobs are added. For example network usage will double when two jobs are running instead of just one. However, replication throttling is a global setting for all jobs unless you override global throttling when you configure a job.

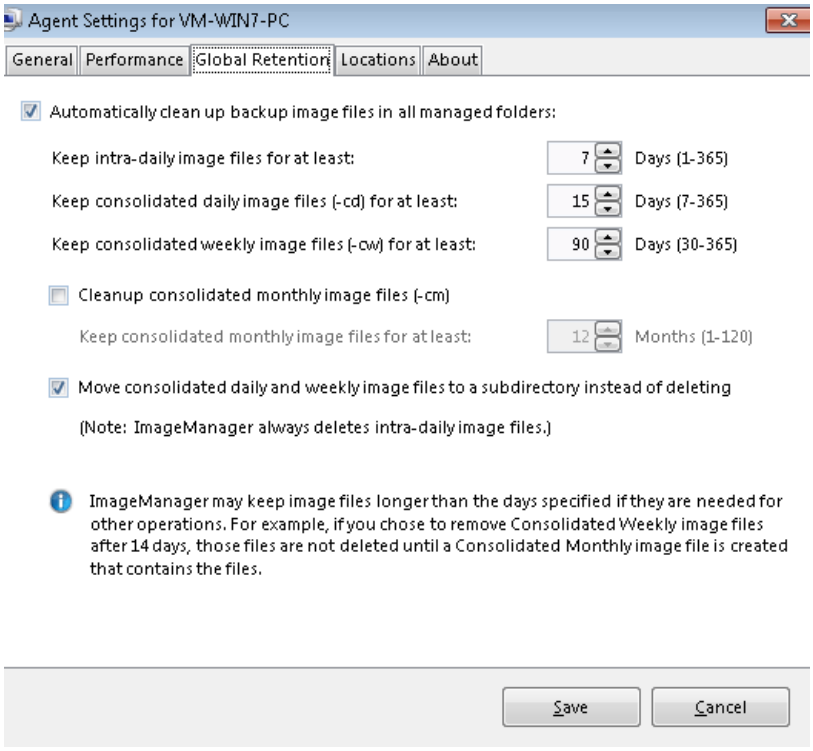
Concurrent Processing

Use this setting to control the maximum number of folders to be processed simultaneously and the maximum number of jobs processed simultaneously for replication and HeadStart Restore. These settings give you more granular control over the number of jobs and folders ImageManager works on at the same time.

Note: Concurrent jobs apply to the replication type, NOT all replication jobs.

Global Retention

Global Retention allows you to manage automatic cleanup settings for all managed folders. ImageManager deletes the files after the number of days specified (unless they are required for other operations).



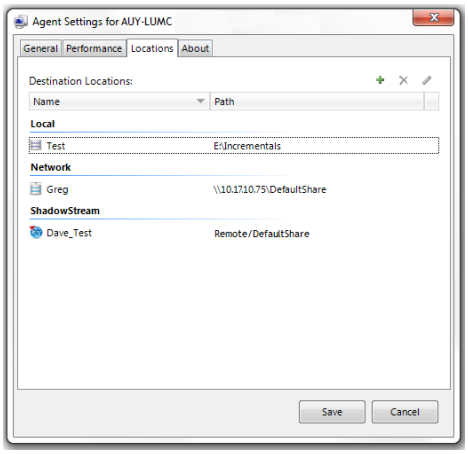
You can reduce the amount of storage space used by managing, consolidating and deleting image files that aren't needed.

Automatically clean up backup image files in all managed folders	Checking this box enables you to: • Keep intra-daily files for at least: 7 days (default). You can select between 1 and 365 days. • Keep consolidated daily image files for at least: 15 days (default). You can select between 7 and 365 days. • Keep consolidated weekly image files for at least: 90 days (default). You can select between 30 and 365 days.
Cleanup Consolidated Monthly image files	You can reduce the amount of storage space used by deleting consolidated monthly files after the amount of time specified in the setting. The default minimum time is 12 months.
Move Consolidated daily and weekly image files	Consolidated daily and weekly images can be moved into a subdirectory if you choose not to delete them.

Note: These settings can be used in conjunction with the Override global agent retention settings options. These options are found in the Retention Settings dialog box under Managed Folder Tasks in the ImageManager user interface.

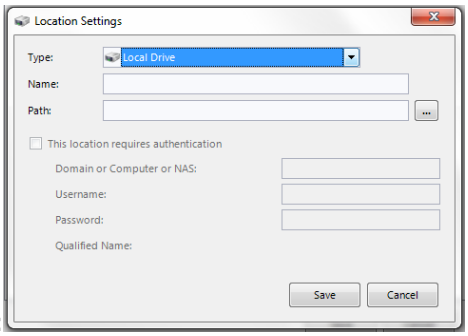
Locations

The **Locations** tab simplifies the task of maintaining the destinations for your ImageManager jobs. By defining resource paths in the Locations tab, you can use these resources as you define ImageManager jobs. You can also globally modify the specific types, paths, or credentials used to access these resources (as they may change over time) without having to modify each ImageManager job that uses these destinations.



The list shows each resource by *Type*, *Name*, and *Path*.

To Add a new Location



1. In the Locations tab, click the + icon to display the Location Settings dialog:

2. In the Location Settings dialog, enter the required information then click **Save**.

Location types and settings are:

Field	Description
Type	**Local drive**: Replicate to any locally attached device. **Network drive**: Replicate to a network resource such as a server, NAS, or BDR. **intelligentFTP**: Replicate remotely using iFTP. **StorageCraft ShadowStream server**: Replicate remotely using ShadowStream. **StorageCraft Cloud Services**: Replicate remotely to StorageCraft Cloud Services. **VMware ESX/ESXi Server**: Replicate to a VMware server.
Name	(Optional) Enter a descriptive name for the location.
Path	Enter the path for the location.
Authentication	Enter the credentials (if needed) to access the location.

To Delete a Location

Note: ImageManager can't delete a Location that is in use by a replication job. You must first modify or delete that job before deleting the Location.

1. Click on the location you want to remove.
2. Click on the × icon at the upper-right of the dialog.

   ImageManager removes the selected destination location from this agent's list.

To Modify a Location

1. Select the location you want to modify.
2. Click the Edit icon .
3. In the Location Settings dialog, modify the location's path or credentials.
4. Click **Save** to save your changes.

The agent job is now configured to use the new settings for this Location.

Drive Settings

Location settings can be for local or network drives.

Local Drive Settings

For a Local Drive, ImageManager only asks for a path to the resource. Click on the Browse button to select the path. (Browse only displays locally-attached drives.) For example, a local drive path might be: `E:\Replicate`.

Network Drive Settings

For a Network Drive, ImageManager requires:

Server	You can use UNC, IP address, or server name.
Share	Specify which Windows share on the server you wish to use for this location.
Authentication	(Default: Disabled)--Provide ImageManager with the authentication credentials needed to log into the server or network resource (Domain/Computer/NAS name, Username, and Password).

ShadowStream Server Settings

StorageCraft ShadowStream Server Settings

For a remote replication using the StorageCraft ShadowStream tool, ImageManager requires:

Server	You can use UNC, IP address, or server name to specify the server running ShadowStream.
Port	(Default: 4365)--Identify the port number this job will use to transfer data to ShadowStream. (Use the Port Number defined in the ShadowStream server's administrator console.)
Share	Specify which ShadowStream Share on the destination server you wish to use for this Location.
Authentication	(Default: Enabled)--Provide ImageManager with the required authentication credentials needed to log into the ShadowStream service (ShadowStream username and password).

Note: ShadowStream maintains its own list of users, passwords and shares as defined using the Administrator Console. These are independent of Windows users and shares and should not be confused with them.

StorageCraft Cloud Services Settings

For StorageCraft Cloud Services, ImageManager requires:

Name	You can give the cloud location any name you choose.

Security	This option can't be changed. SSH is displayed to indicate that it is a secure location.
Block size	You can select a block size between 1 and 131072 bytes. The default size is 65536.
Create/Manage StorageCraft Cloud Services account	If you have an MSP account you can click on this link and create a cloud services account.
Location requires authentication	Location requires authentication is selected by default and can't be changed. Enter a user name and password. **Note:** This is the same cloud services username and password that was used when the StorageCraft Cloud services account was created.

VMware ESX/ESXi Server Settings

For a network replication to a VMware destination, ImageManager requires:

Server

You can use UNC, IP address, or server name to specify the VMware server.

Note: You can click the **Test ESX server connection** icon next to the Server field to confirm you have an active connection to the server as a target.

Authentication (Default: Disabled)--Provide ImageManager with the authentication credentials needed to log into the server or network resource (Domain/Computer/NAS name, Username, and Password).

Note: You can click the **Test ESX server connection** icon next to the Server field to confirm you have an active connection to the server as a target.

intelligentFTP Settings

intelligentFTP Settings

For a remote replication using the intelligentFTP tool, ImageManager requires:

Path Path to the FTP server

Note: You need a functioning FTP server and link between the local and the remote site for intelligentFTP to use. Unlike a manual FTP transfer, the intelligentFTP tool automates the process to ensure that the image chain replicated at the remote site is restorable.

Security ImageManager can encrypt the FTP link using either SSL or SSH based on how the Destination FTP server is configured. You can choose *None*, *SSL* or *SSH*.

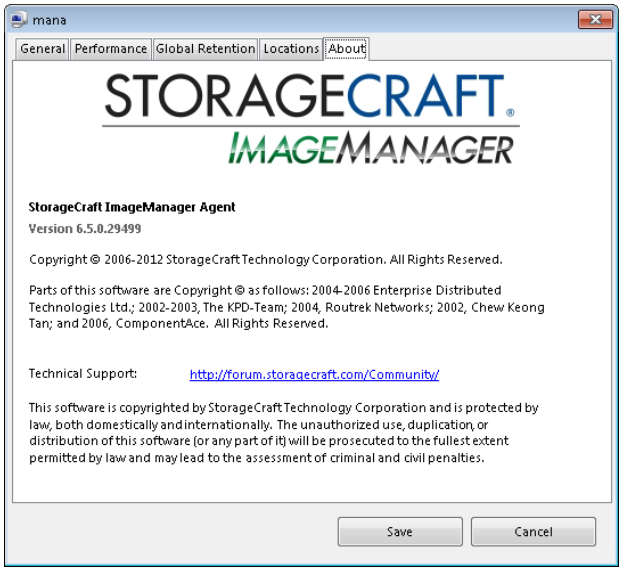
Block Size (Default: 65536 bytes)--The size range is from 1-131072 bytes.

Mode You can select *Active* or *Passive* based on the destination's firewall configuration. (An FTP connection made in Active Mode may appear to the destination firewall that the sender is trying to initiate a connection directly to one of its internal clients. Typically, firewalls will block this type of connection. Making an FTP connection in Passive mode can avoid this problem.)

Authentication (Default: Disabled)--Provide ImageManager with the authentication credentials needed to log into the FTP server or network resource (Domain/Computer/NAS name, Username, and Password).

About

The About tab displays ImageManager agent version information:



Click **Cancel** to close the dialog.

Licensing

StorageCraft licenses premium features on a per-job basis. Each job license grants one job to a single ImageManager agent. (You can later reassign a license to a different job or to a different agent as needed.) Each license supports one of the following operations:

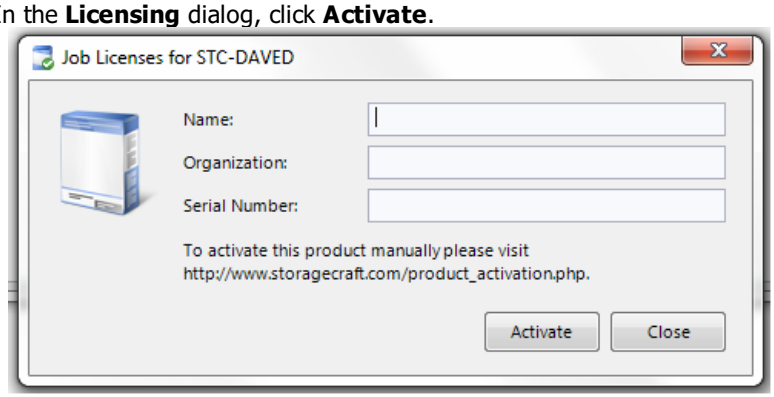
- Each intelligentFTP license supports one Network Replication or one off-site replication job using intelligentFTP.
- Each ShadowStream license supports one Remote Replication (Off-site) job using ShadowStream. (See ShadowStream for details.)
- Each HeadStart Restore license supports one device restoration.

For more information about each of these operations, see ImageManager Features

Note: You can purchase as many premium feature job licenses as needed, but each license is activated for only a single ImageManager console. You cannot purchase a premium license and then move its job operations among multiple ImageManager consoles. For more information about ImageManager licensing, see ImageManager License Scenarios.

To activate ImageManager premium features

1. In the Configuration pane of the ImageManager console, click **Licensing**.
2. In the **Licensing** dialog, click **Activate**.



3. In the Activate ShadowProtect ImageManager dialog box, provide the requested information, then click **Activate**:
   - **Customer Name:** (Optional) Specify the name of the product purchaser.
   - **Organization:** (Optional) Specify the name of the company.
   - **Serial Number:** Enter the Product Key that you received when purchasing ImageManager or premium feature licenses.
4. If the activation is successful, click **OK**.
   If the activation was not successful, review the message to determine why the activation was unsuccessful. To correct the problem, do one of the following:
   1. Review the information in the Product Activation dialog box for accuracy. Correct any errors, then click **Activate** to

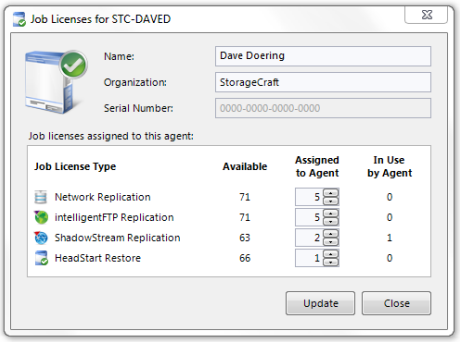
resubmit the activation request.
2. If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again. If you continue to have problems activating these features, contact Product Support.

Assigning Licenses

The Licensing dialog box also controls the assignment of job licenses to this agent. These features include:

- Network Replication
- intelligentFTP Replication
- ShadowStream Replication
- HeadStart Restore

ImageManager licenses these premium features on a per-job basis and lists them in the dialog box after they are installed:



Each job license type shows its usage. The Network Replication and intelligentFTP Replication represent the same licenses. Assigning a Network or an intelligentFTP replication license will therefore decrement both of these licenses.

Field	Description
Available	Shows the total number of purchased job licenses for this feature. This pool is available to all ImageManager agents.
Assigned to Agent	Shows the number of the purchased job licenses assigned to the selected agent. Use the *Assigned to Agent* column to dynamically assign licenses or modify their assignments. Use the selector to specify or modify the assignment. Click **Update** to reflect the new assignment. **Note:** You cannot reduce the number assigned to this agent to less than the number already in use by jobs for this agent. If you need to do so, you must delete those job(s) first in order to reduce this number.
In Use by Agent	Shows the number of licenses actually in use by a ImageManager job for this selected agent.

ImageManager License Scenarios

The following licensing scenarios demonstrate the use of ImageManager premium feature licenses. If you have additional questions, please contact a StorageCraft Sales Representative.

Example 1

Environment: You have backup image sets from five servers and want to manage them from a single ImageManager console. You need to replicate each of the servers locally and off-site, and you want to start using HeadStart Restore.

Licensing Solution: Purchase one ImageManager license with an intelligentFTP or ShadowStream 5-jobs license. (A license to replicate each server to a directly-attached storage device to that server is included with the ImageManager license.) Purchase 5 HeadStart Restore licenses, one for each of the servers you want to use with HSR.

Example 2

Environment: You have three servers, two of which are being backed up to one physical location, and one to a separate physical location. You need to replicate each of the servers locally on the network and off-site, and want to start using HeadStart Restore.

Licensing Solution: Purchase three intelligentFTP licenses for the local and off-site replication. (You have the option to purchase three ShadowStream licenses to do the remote off-site replication with improved throughput using this tool.) Purchase three HeadStart Restore licenses, one for each server.

Example 3

Environment: You have four servers (A, B, C, and D) managed by a single ImageManager console. You want to replicate server A and B backups off-site, server C backups locally, and server D to use HeadStart Restore.

Licensing Solution: Purchase two intelligentFTP or ShadowStream licenses for servers A and B. ImageManager includes support for server C to backup to a locally-attached device, so no additional license is needed. Purchase one HeadStart Restore operation for server D.

Example 4

Environment: You have three servers at one location and another at a remote site that you want to manage using ImageManager. You want to replicate the three local server backups using intelligentFTP to an offsite location and perform consolidation at that site along with backups from the fourth server. You want to protect all servers at both locations with HeadStart Restore.

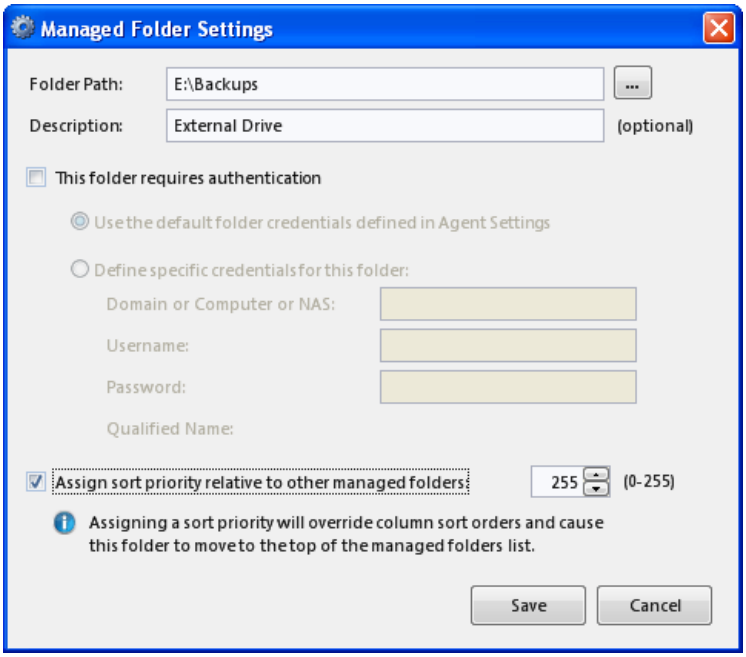
Licensing Solution: Install ImageManager at the local and remote sites. Purchase 3 intelligentFTP licenses for remote replication and assign all three to the local ImageManager agent. Purchase 7 HeadStart Restore license, assign three licenses for the local and three for the remote site--plus one at the remote site for the remote server .

4.6 Managed Folders

You must select one or more folders that contain backup image files to be managed by ImageManager.

To create a new managed folder

1. In the ImageManager console, select which ImageManager agent you want to configure.
2. In the Configuration pane, click **Start Managing Folder**. This displays the Managed Folder Settings dialog box.



3. In the Managed Folder Settings dialog box, provide the required information, then click **Save**.

Folder Path	The path to the new managed folder. You can type in the name and path or browse to the desired folder by clicking on the Browse button.
Description	(Optional) A description of the managed folder.
Authentication	(Conditional) The authentication credentials needed to access the managed folder. You can either use the default credentials specified in the ImageManager agent settings (see Configuring an ImageManager Agent), or specify authentication credentials specific to this managed folder.
Assign sort priority	(Default: Disabled) When enabled, ImageManager sorts the managed folders in the Managed Folder pane in ascending order based on the specified sort value (0 - 255). ImageManager runs these jobs in this order.

4.7 Configure Notifications

ImageManager can automatically send email notifications when specific events occur.

To modify the notification settings

1. In the ImageManager console, select the ImageManager agent that you want to configure.
2. In the Configuration pane, click **Notification Settings**.
3. In the Notification Settings dialog box, select the Conditions tab.
4. In the Conditions tab select the events to generate email notifications.

Failures	Send an email when an ImageManager operation fails.
Warnings	Send an email when ImageManager needs attention to prevent a failure.
Inactivity	Send an email when the ImageManager agent is inactive for the specified number of days.
Low Free Space	Send an email when the space available in the managed folder drops below the specified threshold.
All Daily Activity	Send a daily email with a summary of the ImageManager operations.

5. Select the Email Setup tab in the Notification Settings dialog box.
6. Specify the name of the email account to receive email notifications.

SMTP Server Name	The SMTP server name and port that ImageManager uses to send the email notification. If necessary, provide valid authentication credentials for the SMTP server. Select **SSL** to send the email via secure connection.
Email Template	The email configuration. Provide the email recipients and, if desired, a Sender name and Subject line for the notification emails.
Send Test Email	Sends an email whenever the ImageManager notification settings change.

7. Click **Send test email** to verify that the settings work correctly.
8. Click **Save**.

5 Verify Backup Images

The ImageManager verification service periodically tests the integrity of your backup image files. This process is similar to the manual process provided by ShadowProtect in the Verify Wizard (see Verifying Backup Image Files in the *ShadowProtect User Guide*). While the Verification service is enabled by default, you can configure specific verification behavior for each managed folder.

To configure the verification service

The ImageManager verification service can periodically test the integrity of your backup image files. This verification of file integrity is similar to the manual process provided by ShadowProtect in the Verify Wizard (see Verifying Backup Image Files in the *ShadowProtect User Guide*). While the Verification service is enabled by default, you can configure specific verification behavior for each managed folder.

To configure the verification service:

1. In the ImageManager console, select the ImageManager agent and managed folder.
2. In the Configuration pane, select **Verification Settings** .

3. In the Verification Settings dialog box, provide the desired information, then click **Save**.

Immediately verify newly created image files	(Default: Enabled) Instructs ImageManager to verify each backup image file immediately following its creation.
Periodically re-verify existing image files	(Default: Reverify every seven days) Instructs ImageManager to re-verify backup image files in the managed folder on a regular basis. You can re-verify the backup image files every 1 - 30 days, as specified in the Days field.
Override default performance impact for image file verification	(Default: Disabled) Lets you manage how the ImageManager agent uses processing resources during the verification process. More processing resources result in faster verification, but can impact other system operations. When this setting is disabled, the agent uses the throttling setting in Agent Settings to manage I/O usage by ImageManager (see the General tab in Agent Settings).

6 Consolidating Backup Image Files

The ImageManager consolidation service lets you periodically merge incremental backup image files into a consolidated file. Doing this reduces the time to restore and lets you reduce the size of the file chain necessary to restore a system. Fewer files means fewer opportunities for file failure.

ImageManager provides the following types of consolidated files:

- **Daily Consolidated Files:** At the end of each day, ImageManager rolls up all incremental backup image files created during that day into a single point-in-time incremental image file. Daily consolidated files include a `-cd` in the file name. For example:

  `D_VOL-b001-i005-cd.spi`

- **Weekly Consolidated Files:** At the end of each week, ImageManager can roll-up all Daily Consolidated files created during that week into a single point-in-time incremental image file. Weekly consolidated files include a `-cw` in the file name. For example:

  `D_VOL-b001-i026-cw.spi`

- **Monthly Consolidated Files:** At the end of each month, ImageManager rolls up all Weekly Consolidated files created during that month into a single point-in-time incremental image file. Monthly consolidated files include a `-cm` in the file name. For example:

  `D_VOL-b001-i097-cm.spi`

- **Rolling Consolidated Files:** ImageManager rolls up multiple monthly consolidated files to further reduce the amount of storage space used. This creates a rolling consolidated monthly image file that consists of the specified number of `-cm` image files. Rolling consolidated files include a `-cr` in the file name. For example:

  `D_VOL-b001-i097-cd-cm-cr.spi`

  Note: To use rolling consolidation you must use ImageManager 6 and ShadowProtect 5. You are NOT required to create a new backup chain. The rolling consolidation feature of ShadowProtect 5 works with ShadowProtect 4 image chains.

Configure Consolidation Settings

Note: The policies configured with ImageManager are different from the policies set in ShadowProtect. The policies defined in ShadowProtect apply only to weekly and monthly backup jobs. They don't apply to continuous incremental jobs. ImageManager handles the policies for the continuous incremental job types. Policies for StorageCraft Cloud services are also different than those in ImageManager or ShadowProtect. See the StorageCraft Cloud Services user guide for more information.

To configure the consolidation service

1. In the ImageManager console, select the ImageManager agent and managed folder.
2. In the Configuration pane, select **Consolidation Settings.**
3. Select **Enable image file consolidation for this managed folder.**
   This option is selected by default. This means that once you add a managed folder to ImageManager, the Consolidation service automatically begins to monitor the folder.
4. Configure the consolidation schedule, then click **Save**.

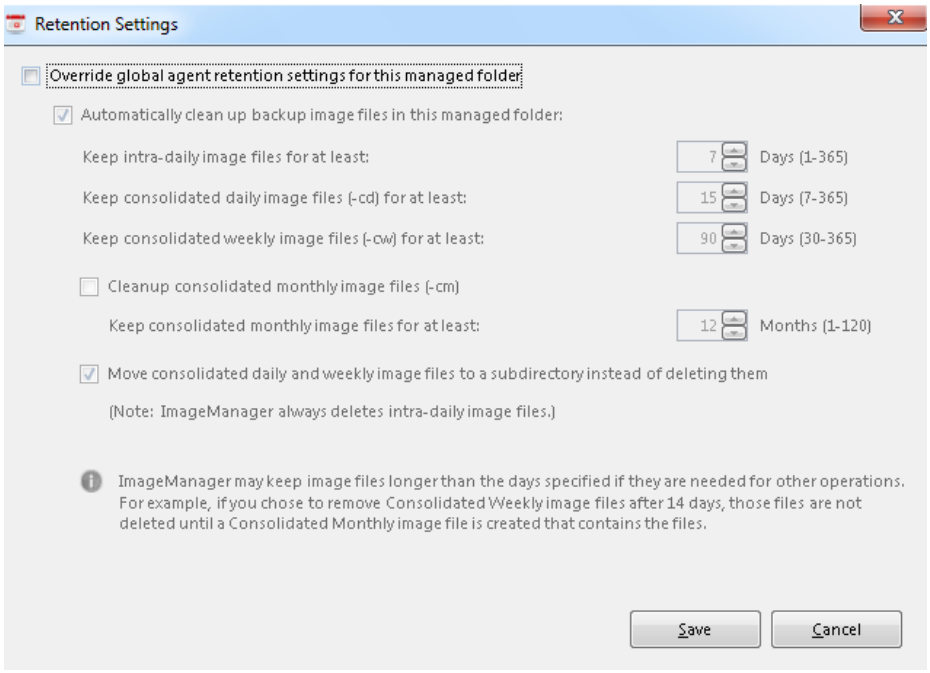
Weekly Consolidation	(Default: Saturday) Specifies the effective end of the week for the purpose of creating a Consolidated Weekly backup image file.
Monthly Consolidation	(Default: the 31st day of the month) Specifies the effective end of the month for the purpose of creating a Consolidated Monthly backup image file. You can select a specific date, or a relative day of the week in the month (for example, the last Friday, or the fourth Monday).

ImageManager saves your consolidation settings. You can now configure your retention policy settings.

7 Retention Settings

ImageManager Retention Settings

ImageManager lets you to override global agent retention settings for selected managed folders. The files are retained at least as long as specified in the settings. In some cases the files are kept longer if they are needed for other operations.



Retention of Dependent Image Files

It's important to understand how ImageManager file retention works before configuring your retention policy.

Important: In some cases ImageManager may keep backup image files longer than the amount of time specified in the retention settings if those files are needed for other operations.

Dependent image file retention schedule

C_VOL-b001-i026-cw.spi 6th June 2014 (First -cw file created)
C_VOL-b001-i052-cw.spi 13th June 2014 (Second -cw file created)
C_VOL-b001-i078-cw.spi 20th June 2014 (Third -cw file created)
C_VOL-b001-i104-cw.spi 27th June 2014 (Last -cw file created)

C_VOL-b001-i104-cm.spi 30th June 2014 (Consolidated file created)

All dependent -cw files are kept until 30 days after the last -cw file was created.

This means the following dependent files would be deleted on 27th July, which is 30 days after the last -cw file was created (27th June 2014).

C_VOL-b001-i026-cw.spi 6th June 2014
C_VOL-b001-i052-cw.spi 13th June 2014
C_VOL-b001-i078-cw.spi 20th June 2014

To configure the retention policy:

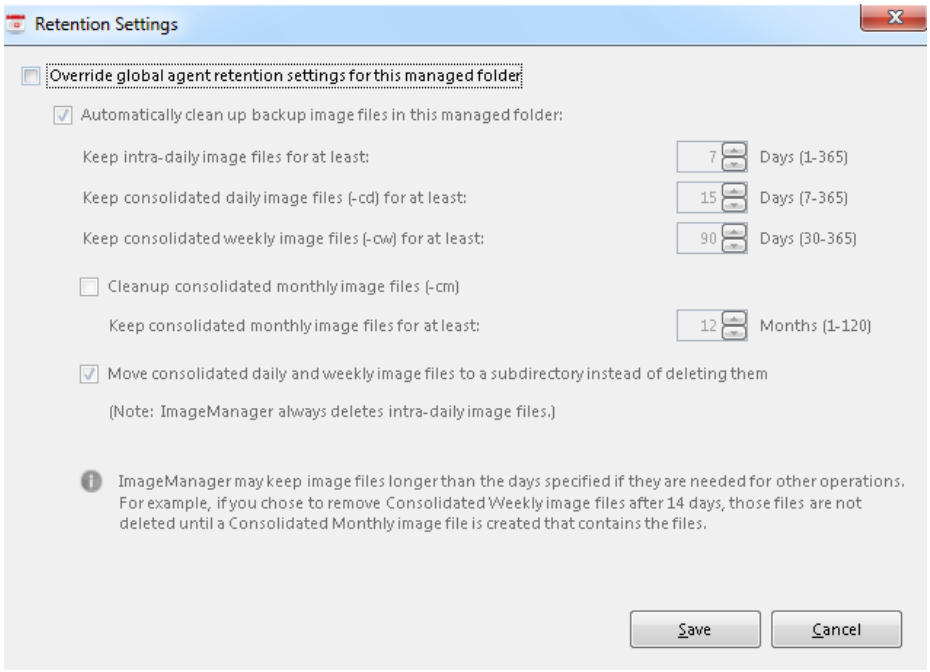
1. In the ImageManager navigation pane click **Retention Settings.**
2. Select **Override global agent retention settings for this managed folder**.
3. Select **Automatically clean up backup image files in this managed folder**.
4. Select the retention settings for this managed folder:

   Note: If the retention settings for this managed folder change, but the **Override global agent retention setttings for this managed folder** box is not checked, the global settings still apply.

Keep Intra-daily image files	(Default: 7 days) The minimum number of days ImageManager keeps intra-daily incremental backup image files after they have been rolled up into a daily consolidation. If the files are not required for another operation ImageManager deletes them after the specified number of days. To keep the backup images, implement a replication procedure to save them to another system.
Keep consolidated daily image files (-cd)	(Default: 15 days) The minimum number of days ImageManager keeps daily consolidated backup image files, plus the time required for weekly consolidation files to be created (if they are dependent on consolidated weekly files). If the files are not required for another operation ImageManager deletes the source image files unless you choose to keep them. (See "Move Consolidated Image Files to a Subdirectory" later in this section.)

Keep consolidated weekly image files (-cw)	(Default: 90 days) The minimum number of days ImageManager keeps weekly consolidated backup image files, plus the time required for monthly consolidation files to be created (if they are dependent on the monthly files). If the files are not required for another operation, ImageManager deletes in the daily files as defined in the "Move Consolidated daily and weekly image files" setting.
Cleanup consolidated monthly image files (-cm)	(Default: not selected) This setting lets you clean up consolidated monthly image files after a specified period of time to further save storage space.
Keep consolidated monthly image files	(Default: 12 months) This is the minimum number of months ImageManager keeps monthly consolidated backup image files. This is the retention setting for rolling consolidation.
Move consolidated daily and weekly image files to a subdirectory	(Default: Disabled) Following consolidation, ImageManager can move the source backup image files into the incrementals subdirectory (inside the managed folder) instead of deleting them. This requires more storage space because ImageManager keeps both the consolidated and the source incremental files. Images moved into the incrementals folder become orphans and are no longer associated the associated full image or chain.

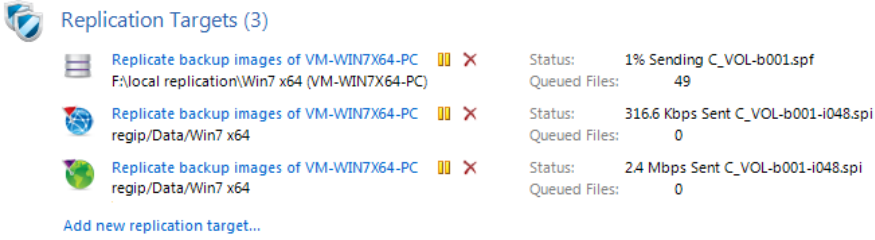
Warning: Do not attempt to restore files from the incrementals folder.



Important: In some cases ImageManager may keep backup image files longer than the amount of time specified in the retention settings IF those files are needed for other operations. See the retention exception example below.

8 Replicate Backup Images

The ImageManager replication service lets you automatically copy backup image files to a secondary location.



Note: ImageManager uses multiple operating system connections during replication. In rare cases, on Windows desktop operating systems older than Windows 8, all available connections can be used when many small incremental files are being replicated. If this happens, replication stops temporarily until connections become available.

To avoid this problem use a Windows Server or Windows 8 desktop for sending and receiving replication jobs.

To configure a replication job

1. In the ImageManager console, select the ImageManager agent and managed folder whose files you want to replicate.
2. In the Replication Targets pane, click **Add new replication target**.
3. In the Replication Target dialog box, select the **General** tab.
4. Specify the appropriate settings in the General tab dialog:

   Name (Optional) Enter a descriptive name for the replication target.

Type (Default: Local Drive) Identifies the type of replication target. Supported options include:
Local Drive: The replication target is attached directly to the local system (for example, an external hard drive).
Network Drive: The replication target is accessible via the local network (LAN).
intelligentFTP: The replication target is accessible via FTP (File Transfer Protocol) using intelligentFTP. (See Licensing for details.)
StorageCraft Cloud Services: The replication target is accessible via the cloud. (See Creating a cloud target for details.

> **Warning:** StorageCraft Cloud Services does not support image files from UEFI + GPT disk systems. ImageManager allows configuring this for cloud replication, but the job fails when it runs. For UEFI + GPT systems, only use intelligentFTP or ShadowStream for replication.

StorageCraft ShadowStream Server: The replication target is accessible via ShadowStream. (See ShadowStream for details.)

> **Note:** Network and FTP remote replication targets require intelligentFTP. However, ShadowStream high-performance replication requires ShadowStream. (See Licensing for details.) ImageManager tests the connection to ShadowStream when you save this replication job. If it cannot confirm the ShadowStream connection, ImageManager does not save the job.

Location Specifies that this job use either an existing globally-defined location for the replication target or a new destination that you specify here. (For details, see Locations under Agent Settings.)

Performance and Security **Override global throttling** (Conditional): Available only when Type = intelligentFTP or ShadowStream Server. Lets you modify the maximum bitrate for sending data to the remote site for this job from the global value set for either intelligentFTP or ShadowStream. Range is from 1 Kbps. to 999 Gbps.
Don't replicate Base image files: Instructs ImageManager to not send the large `.spf` base (Full) image files to preserve bandwidth and reduce transfer time. (These files could be sent manually instead.)
Compress data stream (Default = disabled): Available only when Type = ShadowStream Server. Enables compression on the data sent using ShadowStream. Do not compress the data stream if you already have ShadowProtect compress your image files. Doing so reduces system performance.
Encrypt data stream (Default = disabled): Available only when Type = ShadowStream Server. Enables encryption on the data sent using ShadowStream. Do not encrypt the data stream if you already have ShadowProtect encrypt your image files. Doing so reduces system performance.

5. Select the **Replication Mode** tab.
6. Select the settings for replicating to a folder being consolidated by a second ImageManager at the target.

> **Note:** ImageManager can be installed on more than one system to distribute the consolidation process. Images from one system's managed folder can be replicated to another system's managed folder. One system performs the daily consolidations and the other performs the weekly and monthly consolidations. The Replication Mode tab lets you configure replication services to perform distributed consolidation.

No--Replicate all consolidated files (Default: Enabled) Select this option when the replication target is not managed by ImageManager. You can choose the following options when replicating in this way:
Also replicate original unconsolidated intra-daily image files (Default: Disabled) Sends both the consolidated and the original incremental files to the secondary site. This requires the most bandwidth and storage space.
Files moved or deleted by ImageManager are deleted on the destination. (Default: Enabled) Deletes a backup image file at the primary site, it will also remove the file from the replication target.

Yes--Replicate only consolidated daily image files (Default: Disabled) Specifies that the replication target is also an ImageManager-managed folder that performs the weekly and monthly consolidation.

Yes--Replicate only original unconsolidated intra-daily image files (Default: Disabled) Specifies that you want to perform all file consolidation at the replication target, rather than at the source.

7. Click **Save** to close the Replication Target Settings dialog box.

9 Install ShadowStream

StorageCraft ShadowStream is a high-performance transfer tool that lets you send backup image files to a destination system much faster than using traditional FTP. This tool greatly reduces the time needed to replicate data over noisy or high latency (>150-200ms) networks even when replicating full backup images. It is also simpler to configure and maintain than conventional FTP.

ShadowStream has two parts:

- ShadowStream service
- Administrator console

After configuring ShadowStream you can use ImageManager to create ShadowStream replication jobs. (See configuring Locations under Agent Settings for details.) Multiple ImageManager agents can use the same ShadowStream service.

System Requirements

The ShadowStream service and administrator console run on:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows XP SP3
- Windows Vista SP1
- Windows 7
- Windows 8

Ports

ShadowStream uses these ports by default:

Port	Purpose
4363	Data connection control port
4364	Admin connection port
4365	Data transfer port
54363 to 55263	Used for parallel connections

Confirm access to these ports through your firewalls to run ShadowStream.

Installing the ShadowStream Service

To install the ShadowStream service (or both if you haven't installed ImageManager on this system):

1. Run the ShadowStreamSetup6.exe file.
   The installation file can be found on the StorageCraft Updates page. You select default installation options, or select custom options.

   Custom installation options

Console Application	This is the ShadowStream administration tool. At a minimum, the system running the ShadowStream service needs a console to enable remote access. Additional consoles can run on any workstation with access to the ShadowStream Service system.
ShadowStream Service	The file transfer service.
Install Path	The default is program files (x86)\StorageCraft\Shdowstream. Click **Change** to choose another location.

2. Click **Finish** when the Install Wizard completes.
3. Click **Start**/**StorageCraft**/**ShadowStream Admin Console**.
   This displays the ShadowStream administrator console.
4. Click **Admin Connect** at the upper-left.

5. Click **OK** to log in using the default "Admin" account with a password of "*password*".
   Note: Earlier versions of ShadowStream used a default password of "shadowstream".

You can now configure ShadowStream for use with ImageManager.

Remote ShadowStream Console Installation

The ShadowStream administrator console is automatically installed when ImageManager is installed. Enable remote management on the system where the ShadowStream service is running to use the remote console.

10 Configure ShadowStream

After you install ShadowStream:

- Change the administrator password
- Add a ShadowStream user to execute replication jobs
- Create a ShadowStream share as the destination file folder
- Configure the port settings for access through the firewall
- Raise the maximum concurrent file transfer connections

10.1 ShadowStream User Roles

ShadowStream users can have multiple of roles. You can be exclusively a User, exclusively an Administrator, or you can have rights to perform both roles. The Administrator (exclusive) can only administer the ShadowStream service (i.e. there are no rights to process replication jobs). The User role has the rights so ImageManager can process replication jobs. See **Add a New User** for information on adding a new user or changing the role for an existing user.

To Change the Administrator Password

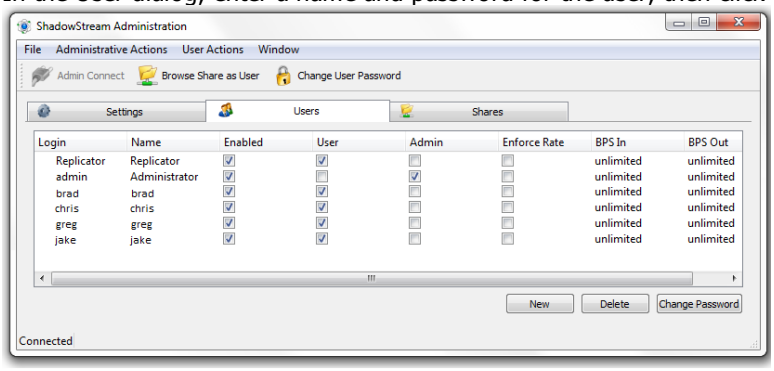
As a safety precaution you need to change the default Administrator password for the ShadowStream server.

1. Log in to the ShadowStream administrator console.
2. Click the **Users** tab.
3. Click **Change Password**.
4. Enter a new password for the Administrator, then click **OK**.

10.2 Add a New User

To add a new user to ShadowStream:

1. Click the **Users** tab.
2. Click **New.**
3. In the User dialog, enter a name and password for the user, then click **OK**.



Configure Users

You can change settings for new or existing users:

Setting	Description
Enabled	(Default: Enabled). Enables the ShadowStream user.
User	The user is not a ShadowStream administrator.
Admin	The user is a ShadowStream administrator.
Enforce Rate	Enforces the bandwidth limit for this user.
BPS In	Specifies the maximum bitrate (in Mbps) available to this user for downloads. The range is from 1 to 1000Mbps or unlimited.
BPS Out	Specifies the maximum bitrate (in Mbps) available to this user for uploads. The range is from 1 to 1000Mbps or unlimited.

ShadowStream automatically updates the list on the Users tab after you make the changes.

10.3 Configure Settings

The ShadowStream Settings tab configures:

- File Transfer
- Administration

Configuration Port Options

Setting	Value
Control Port	Default: 4363. Use the default unless your firewall policy requires a different port.
Transfer Port	Default: 4365. Use the default unless your firewall policy requires a different port.
Maximum Concurrent Connections	Default: 5. Limits the number of user and ImageManager connections to the ShadowStream server.

Maximum Concurrent Connections

Maximum Concurrent Connections limits both user and replication connections. A user consumes one connection to open the console and browse a share. Each additional share the user views consume another connection. ShadowStream does not release these connections until the user closes the console.

ImageManager also uses a ShadowStream connection for each active ShadowStream replication job. If Maximum Concurrent Connections is set too low, ShadowStream might not have enough connections available to run the replication job. ImageManager makes three attempts to open a ShadowStream connection for a replication job. If it fails, ImageManager stops the attempt and issues an error message. The replication job is not yet complete. ImageManager retries again after ShadowProtect creates a new incremental backup image. The new incremental causes ImageManager complete its consolidation and replication jobs. Setting the Maximum Current Connections higher than the total number of replication jobs and users allows the replication job to continue without interruption.

Administration

You can allow administrators remote access to the ShadowStream console by checking **Allow Remote Administration**. In the interest of security, remote administration is not enabled by default.

If you enable remote administration, you can configure:

Setting	Value
Administration Port	Default: 4364. The port that the ShadowStream server uses for the administrative connection. Leave this at the default unless your firewall policy requires a different port.
Maximum Concurrent Connections	Default: 1. The number of simultaneous administrator connections on the server. StorageCraft recommends using the default value to enhance security.

10.4 Create a ShadowStream Share

With ShadowStream installed, ImageManager can replicate data to a shared ShadowStream folder. ShadowStream creates a default folder:

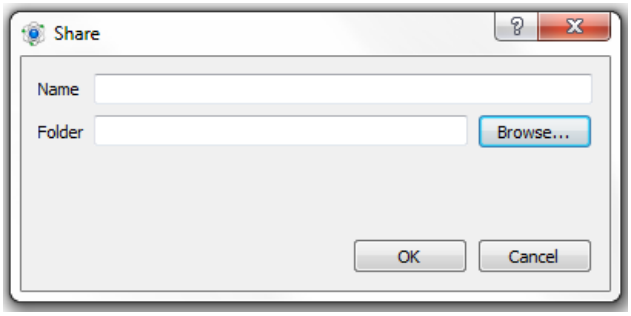
- **Name:** DefaultShare
- **Location:** `program files (x86)/StorageCraft/ShadowStream/DefaultShare`
- **Permissions:** Share (all)

ImageManager can use this `DefaultShare` folder as its target, but you may want to add one or more shares in order to:

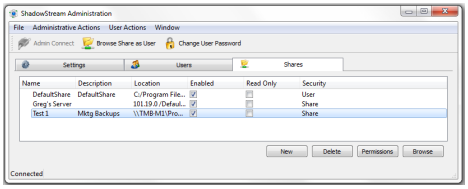
- Better differentiate between jobs.
- Restrict users to a specific share rather than to the general DefaultShare folder.

To add a share

1. Create the destination folder(s) on the target ShadowStream server.
2. In the ShadowStream console, click the **Shares** tab.
3. Click **New**.



4. In the Share dialog specify the share information, then click **OK**.
5. Click **Browse** to locate the destination folder for this share.
6. Click on the folder to highlight it.
7. Click **Select Folder**.



ShadowStream adds this new share to the list:

Share Settings

These options can be used to configure settings for the new share:

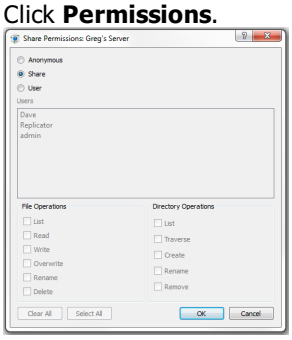
Setting	Description
Name	Double-click on the name to modify it. Keep in mind that ImageManager might use this name in a replication job. Changing the name when it is in use by a job causes the job to fail.
Description	Double-click on the Description to enter descriptive information about the share.
Location	Displays the path selected for this share. Modifying this lets you to change the destination folder for this share. If you change the location move the contents of the previous destination folder to the new path. ImageManager replication jobs are not be affected by the change and will run normally. This prevents ImageManager from re-sending all the contents intended for the folder instead of only the updates.
Enabled	(Default: Enabled) Temporarily disables a share. (Click **Delete** to permanently remove a ShadowStream share.)
Read Only	Makes a share read-only.

Security	Anonymous, Share, and User. (Click **Permissions** to modify the setting.)

Configuring Share Permissions

To modify the Share permissions for the highlighted share:

1. Click **Permissions**.



2. In the Share Permissions dialog, select the desired permission setting, then click **OK**.

Permission	Description
Anonymous	Grants all permissions to any user, not just ShadowStream users. For security reasons, StorageCraft recommends that you don't use anonymous.
Share	This is the default setting. Grants all rights to the Share to ShadowStream users. (This does not include the right to change folder permissions. Only administrators can change folder permissions.)
User	Choose User to grant specific ShadowStream users permissions to this share. These permissions are listed below the Users field.

ShadowStream automatically updates the Shares tab to reflect changes in permissions.

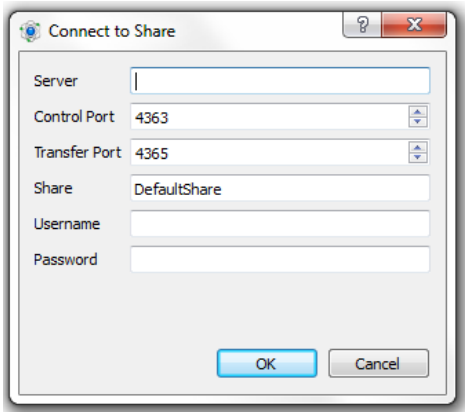
11 ShadowStream Console

The primary purpose of ShadowStream is to perform ImageManager replication jobs. The ShadowStream administrator console can also be used to:

- Confirm that remote site backup image replications have completed
- Download image files from remote sites to the workstation.
- Change user passwords.

Accessing the console

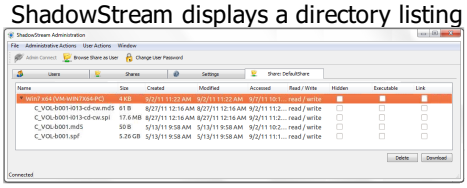
1. Click **Start>StorageCraft>ShadowStream Admin Console**.
2. Click **Browse Share as User**



3. In the User login dialog, enter the connection information, then click **OK**.

Note: ShadowStream maintains its own database of users and shares. These users and shares are unique to ShadowStream and are not the same as a Windows user or Share (even if there are existing Windows shares on the target server).

4. ShadowStream displays a directory listing for the selected ShadowStream share:



Folder and File Actions

You can perform various actions on the files or folders based on user permissions set by the administrator.

Note: By default, all ShadowStream users have the full permission to the ShadowStream shares. They do not, however, have permission to change permissions.

Action	Result
Double-click a folder	Opens the folder and displays a list of its contents.
Click **Delete**	Deletes the highlighted files/folders.
Click **Download**	Opens a local directory dialog so you can select where you want to download the selected files to.
Click **Refresh**	Refreshes the listing to show the changes you've made.

Password Management

To change the ShadowStream console password

1. Click **Change User Password**.
2. Enter these details, then click **OK**.

Field	Comment
Server	Enter the name of the local ShadowStream server.
Control Port	Default: 4363. Leave this default unless your administrator specifically changed it.
Username	Enter your ShadowStream username.
Password	Enter your current password.
New Password	Enter the new password.
Confirm New Password	Repeat the new password.

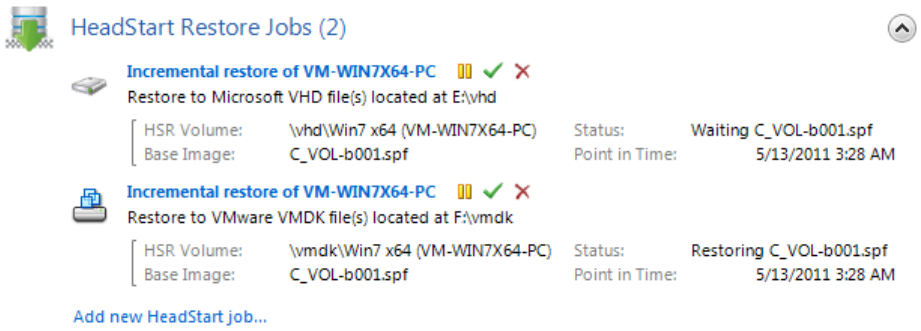
ShadowStream asks for the new password the next time you log into the administrator console.

12 HeadStart Restore

ImageManager HeadStart Restore (HSR) lets you start a restore operation on a new system while the original production server continues to run. ShadowProtect continues adding incremental backup images to the image chain on the original server. This greatly reduces downtime associated with various failover operations, particularly for systems with very large storage systems (ie: multi-Terabyte).

See HeadStart Restore Scenarios to learn about HSR use cases.

Run HSR from the ImageManager HeadStart Restore Jobs pane:



Note: Don't delete an HSR job while the job is still running. Cancel the HSR job first and then delete it to prevent the ImageManager user interface from becoming unresponsive.

The HSR process consists of:

- Create a HeadStart Job
- Finalize a HeadStart Job

12.1 Create HSR Job

Use the **Add new HeadStart job** option on the HeadStart Restore (HSR) pane to configure a specific restore operation.

Important: HSR can't create GPT volumes. Use the Recovery Environment to do a normal restore for GPT volumes.

VMware Considerations

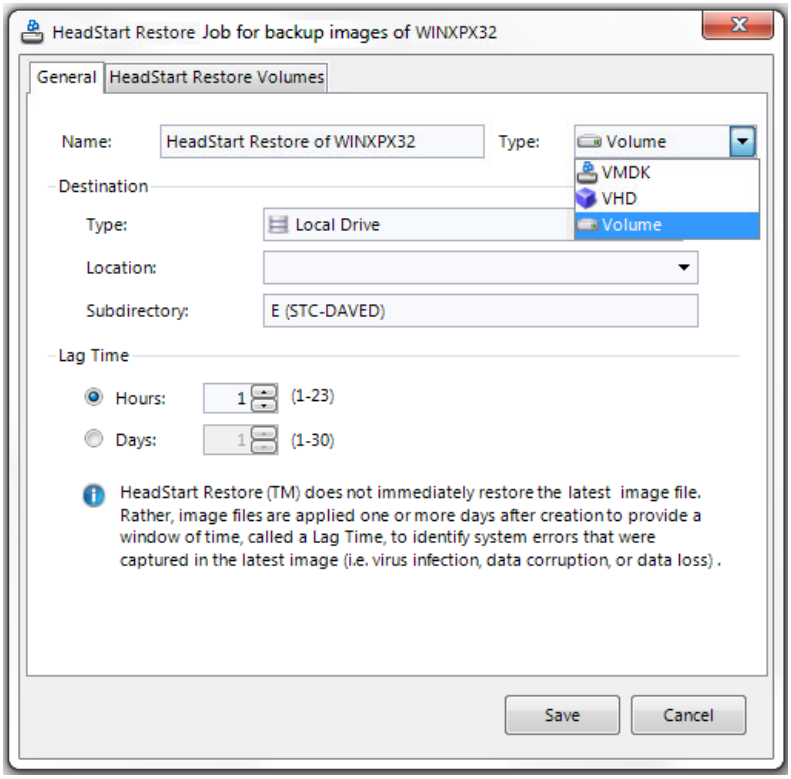
HeadStart Restore can use VMware targets with these considerations:

- Close all instances of VMware VSphere client before attempting to contact an ESX server with ImageManager.
- When creating an ESX job type, the Domain or Share fields don't appear when you select the ESX/ESXi target type for HSR. See ESX Server Permissions for information about the minimum permissions ImageManager needs to use an ESX server target.
- ImageManager doesn't support the free (limited functionality) version of ESXi.
- To restore to a VCenter Cluster, set the correct permissions on the datacenter's root VM folder.

Note: ImageManager doesn't show folders (on the Folder tab) for an ESXi target when creating a minimal virtual machine. This is because the datastores folder is different than the datacenters virtual machine folders. Learn more about the ESXi folder hierarchy in the Folders section of the vSphere Managed Inventory Objects page.

To Create a new HeadStart Restore Job

1. In the ImageManager console, select the ImageManager agent and then the managed folder you want to use for this HeadStart job.
2. In the *HeadStart Restore Jobs* pane, click **Add new HeadStart Job**



Note: An HSR license is required to create automated HSR jobs.

3. In the HeadStart Restore job dialog **General** tab, select or specify the applicable settings:

Name (Optional) Enter a descriptive name for the HSR job.

Volume **Type**
The type of volume you want HeadStart Restore to create. The supported types are:

- **VMware VMDK:** Create a Virtual Machine Disk (VMDK) file compatible with VMWare virtual environments.
- **Microsoft VHD:** Create a Virtual Hard Disk (VHD) file compatible with Microsoft Hyper-V and Oracle VirtualBox virtual environments.
- **Volume:** Create a physical volume on a local physical disk.

Destination ***Type***
The destination type for your HSR. The supported destination types are:

- Local Drive (locally-attached device)
- Network Drive
- VMware ESX/ESXi Server (Only available for VMDK targets.)

Location
The list of pre-defined destination locations based on destination type. You can use your pre-defined locations or create new ones with **Add new location**. ImageManager asks for:

- **Type** The Location type defaults to the most recently used type.
- **Name** (Optional) The Location name should make it easy to identify the location.
- **Server** The destination server name can be UNC (for VHD targets), or an IP address.

  Note: For VMDK targets, click **Test ESX server connection** to confirm the connection is active with the destination server.
- **Share** The Windows Share on the server to use for this operation. (Only available for VHD targets.)
- **Authentication** (Default: Disabled) The credentials ImageManager needs (Domain/Computer/NAS name, Username, and Password) to log into the server or network resource.

Subdirectory
The default subdirectory created by ImageManager on the destination where HSR files are stored. The name can be changed if necessary.

Lag Time The delay between the creation and application of incremental backup images. ShadowProtect creates backup image files and HSR applies the backup images to the HSR volume. Lag time gives you a chance to identify problems (system errors, image corruption, virus, etc.) in the images before they are applied.

Lag time is settable:

- 1-23 hours
- 1-30 days

Add HeadStart Volumes

ImageManager lets you create one or more new HSR volumes from existing base images in the backup chain.

To create the volumes

1. Click the **HeadStart Volumes** tab.
2. Click **Add new HeadStart volumes.**
3. In the Base Backup Images dialog, select the base image file to use, then click **OK**.
4. (By default, ImageManager lists all the .spf files in the managed folder.)
5. Provide the the password for encrypted backup image files, then click **Save** to create the new HeadStart job.

To create a raw (unformatted) local physical volume

Warning: Configuring an HSR job to locally-attached physical storage requires a raw (unformatted) drive. When you configure an HSR for a physical volume, the volume must be created first. If the volume has been formatted you need to use Windows Disk Manager, or another similar tool, to delete the volume and then create it again WITHOUT formatting it.

1. Go to the Windows "Run" menu or command prompt and run **diskmgmnt.msc**.
2. **Create a new volume** (which automatically creates a raw volume).
3. **Set the volume size** as needed. The volume size must be bigger than the volume being backed up.
4. **Select a drive letter**.
5. In the Format Partition window select **Do not format this volume**.
6. Finish the volume creation by clicking **Next**.

You should now be able to configure an HSR job for the new local physical volume.

To create a VMware ESX/ESXi Server HSR job (Conditional)

1. Locate the target VMDK by clicking on **Click to Browse for Volume**.

2. Select the VMDK, then click **Select**.

ImageManager displays the ESX Inventory dialog box.
This dialog lets you:

- Browse an ESX server for an existing VMDK.
  When creating a target VMDK without using ImageManager (for example with the vSphere client), add 18 MB to the minimum size shown in ImageManager to compensate for worst-case sector alignment in the file system structure.
- Create a new VMDK in an existing VM.
  To do this, right-click an existing VM, then select **Create New Virtual Disk**.
- Create a new VM in an existing Resource Pool.
  To do this, right-click an existing Resource Pool, then select **Create New Virtual Machine**.
  After it is created, you can add a virtual disk to the new VM.

Note: After the job is configured and saved, the only thing you can change is the image file password. If you need to modify any other settings, or change volume sizes, you need to delete the job and create a new one.

ImageManager enables the HeadStart Restore job and displays it in the HeadStart Restore Jobs list.

Warning: Do not click **Delete** on an HSR job once it begins creating a new virtual disk. This may cause ImageManager to freeze. If it is necessary to delete a job, click **Pause** first. When the job pauses, click **Delete**.

12.2 ESX Permissions

HeadStart Restore requires the following minimum permissions on the ESX server resource pool where you plan to create virtual machines and virtual disks for HeadStart Restore. If you are not using resource pools, you must set these permissions on the host, datacenter, or cluster. StorageCraft recommends that you create an HSR role on the ESX server that contains at least these permissions, then assign the user accounts used by HSR jobs to the HSR role.

Category	Permissions
Datastore	Allocate space Browse datastore Low-level file operations
Global	Capacity planning Licenses Manage Custom attributes Script action
Network	Assign network
Resource	Assign virtual machine to resource pool
Virtual Machine > **Configuration**	Add new disk Add or remove device
Virtual Machine > **Inventory**	Create new
Virtual Machine > **Provisioning**	Allow disk access

If you restore to a vCenter cluster, HeadStart Restore also requires the following permissions on the root of the cluster:

Category	Permissions
Global	Licenses

12.3 Finalize HSR Job

Once created and enabled, an HSR job begins the process of restoring a volume from its backup image files to a virtual disk file. However, the restored volume remains unusable until it is finalized. (This prevents users from inadvertently accessing the volume before the restore operation is complete.)

To finalize a HeadStart job

1. In the ImageManager console, select the ImageManager agent and managed folder for the HSR job you want to finalize.
2. In the *HeadStart Restore Jobs* pane, click **Finalize** next to the HSR job you want to finalize.
3. In the Finalize dialog box, provide the required information, then click Finalize.

HeadStart Volumes	Select one or more HeadStart volumes to finalize.
Finalize to	For each HeadStart volume that you want to finalize, specify the specific point-in-time that you want to finalize it to. Once finalized, the restored volume reflects its state at this selected point-in-time.

4. Click **Finalize**.

Note: The StorageCraft Recovery Environment (RE) can be used to finalize an incomplete HSR job. For example: If you configure an HSR job using ImageManager, then the ImageManager system fails, it can leave an orphaned HSR. The orphaned HSR job can't apply any unapplied (currently existing or future) incrementals and can't be finalized. StorageCraft RE can help you recover from this scenario.

To prepare the HSR volume for use in a VM

Once finalized, do the following to prepare the HSR volume for use in a VM:

- Add the virtual disk file to a virtual machine. (The specifics of this process vary depending on your virtual machine software. Consult your virtual machine documentation for more information.)

  Note: This step is already done for you if you are finalizing an HSR job of type ESX/ESXi Server.

- If this is a bootable volume, do the following:

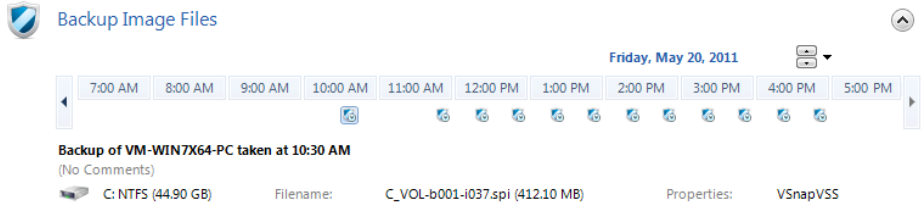
Category	Permissions
HSR of a Physical Machine	1. Edit the Virtual Machine settings and set the appropriate guest operating system. 2. Load the StorageCraft Recovery Environment. 3. Run Hardware Independent Restore (HIR) to setup the hardware configuration in the virtual disk file to match the settings in the virtual machine. (For more information about the Recovery Environment and HIR, see the StorageCraft Recovery Environment User Guide.) **Note:** To run Recovery Environment on an ESX server, upload the Recovery Environment ISO to a datastore on the ESX host. Set the VM's CD-ROM settings to boot from the Recovery Environment ISO. When booting the VM, confirm that the BIOS boot sequence has the CD-ROM as the first boot device. 4. Reboot the VM and let the operating system load from the VMDK.
HSR of a Virtual Machine	1. Edit Virtual Machine settings and set the appropriate guest operating system. 2. Start the VM and let the operating system load from the VMDK.

After the Restoration

There is no need to keep a finalized job enabled. You can reuse the license by disabling or deleting the finalized job.

13 Browse Backup Images

The ImageManager Backup Images service lets you view a historical record of your backup image file creation.

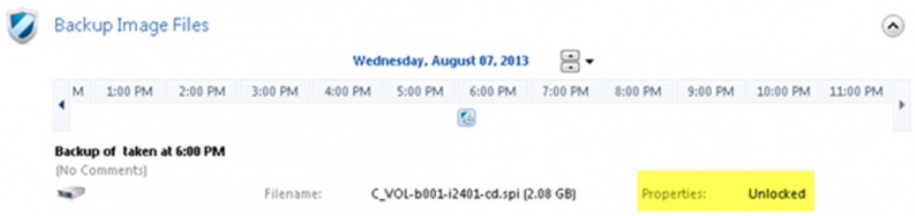


The Backup Image Files pane lets you view information about the backup image files created on a given day.

You can also:

- Use the calendar controls to browse to a specific date. By default, the Backup Image Files pane displays the current date.
- Use the left-arrow and right-arrow icons to move along the daily timeline.
- Select a file icon to see general information about that backup image file. (ImageManager displays a file icon at each point on the timeline where ShadowProtect created a backup image in the selected managed folder.)

Note: In rare situations ImageManager may report a backup file property as "Unlocked". This can occur for a variety of reasons but is benign and can be ignored. An example is shown below.



Unlocked Image