



ImageManager User Guide

1. ImageManager User Guide	3
1.1 ImageManager Overview	4
1.1.1 ImageManager Features	5
1.1.2 What's New	6
1.1.3 HeadStart Restore Scenarios	7
1.1.4 Installing ImageManager	8
1.2 Understanding the ImageManager UI	10
1.2.1 Configuration Pane	11
1.2.2 Managed Folder Pane	13
1.2.3 Services	14
1.3 Configuring ImageManager	16
1.3.1 Connecting to an ImageManager Agent	17
1.3.1.1 Resetting the Agent Password	18
1.3.1.2 Authentication Restrictions	19
1.3.2 Configuring an ImageManager Agent	20
1.3.2.1 Agent Settings	21
1.3.2.1.1 General	22
1.3.2.1.2 Locations	23
1.3.2.1.3 Performance	26
1.3.2.1.4 About	27
1.3.2.2 Licensing	28
1.3.2.2.1 ImageManager License Scenarios	30
1.3.3 Create a Managed Folder	31
1.3.4 Configuring ImageManager Notifications	32
1.4 Verifying Backup Image Files	33
1.5 Consolidating Backup Image Files	34
1.6 Replicating Backup Image Files	36
1.7 Using ShadowStream	38
1.7.1 Configuring ShadowStream	40
1.7.1.1 Changing the Administrator Password	41
1.7.1.2 Add a New User	42
1.7.1.3 Configure Settings	43
1.7.1.4 Create a ShadowStream Share	44
1.7.2 Users and ShadowStream	46
1.8 Using HeadStart Restore	48
1.8.1 Creating a HeadStart Job	49
1.8.1.1 ESX Server Permissions	52
1.8.2 Finalizing a HeadStart Job	53
1.9 Browsing Backup Image Files	54
1.10 Product Support	55
1.11 Glossary	56

ImageManager User Guide

Welcome to the StorageCraft® ShadowControl™ ImageManager™ User Guide. This Guide describes the purpose of ShadowControl ImageManager, the ImageManager technology, and how to use it to manage backup images.

This Guide includes the following major sections:

- ImageManager Overview
- Understanding the ImageManager UI
- Configuring ImageManager
- Verifying Backup Image Files
- Consolidating Backup Image Files
- Replicating Backup Image Files
- Using HeadStart Restore
- Browsing Backup Image Files

Additionally, this Guide includes these general information sections:

- Product Support
- Glossary

Additional Information

- For emerging issues and other resources, see:
 - The `readme.txt` file included with the ImageManager product files.
 - The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- For more information about using ShadowProtect, see the StorageCraft ShadowProtect User Guide.

Documentation Conventions



This symbol designates Note or **Warning** text that highlights critical information about the configuration and/or use of ImageManager.

ImageManager Overview

ShadowProtect ImageManager lets you maintain Incremental backup images and the storage space consumed by your backup image files. Based on a policy that you create, ImageManager automatically consolidates Incremental backup image files into daily, weekly and monthly Incremental images. Additionally, ImageManager provides ongoing verification and replication services for the files that comprise your backup images.

ImageManager consists of these components:

ImageManager Service: A Windows service that performs the backup file management as defined by your policy.

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

This section includes these topics:

- [ImageManager Features](#)
- [HeadStart Restore Scenarios](#)
- [Installing ImageManager](#)



Note: ImageManager policies only apply when you are using the Continuous Incrementals backup schedule as 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.

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. The verification process is similar to that available manually 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.
- **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 these premium features available with the purchase of a job license:

- **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 an 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. In a world of multi-Terabyte storage HSR lets you short-circuit the restore process, greatly limiting the down-time associated with a hardware or software failure. For information about using HeadStart Restore, see [HeadStart Restore Scenarios](#).

For more information about licensing ImageManager or its premium features, see [Licensing](#).

What's New

ImageManager 5.0 provides these new features and updates:

- Dramatically increased remote replication speeds using ShadowStream
- Enhanced user interface to improve usability.
- Simplified licensing with dedicated interface for assigning and tracking licenses.
- Improved FTP performance for remote replication using intelligentFTP.
- Full support for VMware ESX clusters (when sufficiently licensed) as either replication destinations or as HeadStart Restore targets.

(For a complete version history of product updates, see the `Readme.rtf`, located in the `\StorageCraft\ImageManager` folder of your ShadowProtect installation.)

HeadStart Restore Scenarios

The concept of a HeadStart Restore (HSR) is extremely powerful, particularly for today's business environments where multi-Terabyte servers are becoming the norm. HSR lets you take advantage of your ShadowProtect backup images in ways that were previously not possible, as illustrated by the following usage scenarios.

Virtual Server Migration

Problem: You need to migrate a database server with 20TB of data to a new Virtual Machine environment, but you cannot afford to have the server offline for three days it takes 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 on-line 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 on-line 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 on-line.

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 on-line. Using ImageManager with VirtualBoot reduces downtime from several days to only minutes.

Virtual Standby Server

Problem: You want to have a stand-by server that can take over should your primary server fail, 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 on-line as a replacement for the failed production server.

Installing ImageManager

ShadowProtect includes the ImageManager software, but does not install it by default. Before installing ImageManager, make sure your system meets the following requirements:

- ImageManager requires Microsoft .NET version 2. The 32-bit ImageManager installer will add .NET automatically if it does not detect it. However, the 64-bit installer does not. If your system needs this .NET version, you must manually install it before installing ImageManager.
- If you choose to install the ShadowStream remote replication tool, you will need a dual-core processor as a minimum for each system running ShadowStream.
- ImageManager automatic activation requires an Internet connection. (If this system does not have Internet access, you can manually activate ImageManager using the procedure on the StorageCraft website.)

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 StorageCraft Trial Downloads page (<http://www.storagecraft.com/backupsupport.php>).
2. Select the install 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. When the installation completes, click Finish.

You can launch ImageManager in Windows by selecting Start > Programs > ShadowProtect > ShadowProtect ImageManager.



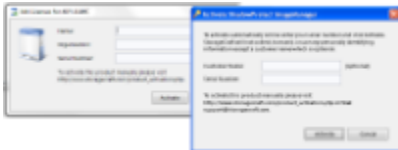
Note: The ImageManager agent loads automatically once you install ImageManager. When it loads, it uses a configuration file (`ImageManager.exe.config`) to set the agent parameters. You can modify the configuration file to change the port that the ImageManager agent uses, if desired.

Activating ImageManager

Once installed, you will need to activate ImageManager before configuring jobs. As mentioned, you will need an Internet connection for the automatic activation process to communicate with the StorageCraft Licensing server. If this system does not have Internet access, you can use the Manual Activation procedure on the StorageCraft website.

To activate ImageManager:

1. In the Configuration pane of the ImageManager console, click Licensing.
2. In the Licensing dialog, click Activate. The Activate dialog box appears:



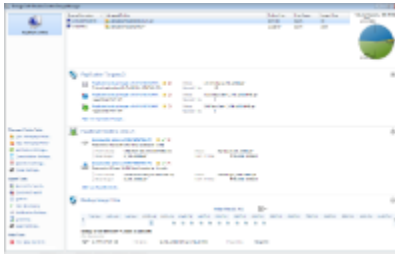
3. In the Activate ShadowProtect ImageManager dialog box, provide the requested information:
 - Customer Name: (Optional) Specify the name of the product purchaser, either person or organization.
 - Serial Number: Enter the Product Key that you received when purchasing ImageManager.
4. Click Activate. ImageManager will communicate with the StorageCraft Licensing server.
5. 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:

- a. Review the information in the Product Activation dialog box for accuracy. Correct any errors, then click Activate to resubmit the activation request.
- b. 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 [StorageCraft Support](#).

Once you activate ImageManager, you can configure it to manage backup folders.

Understanding the ImageManager UI

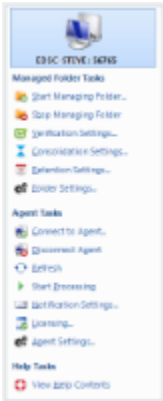


The ImageManager UI consists of these components:

- Configuration Pane
- Managed Folder Pane
- Services Pane







Configuration Pane

The left-side Configuration pane displays a list of currently-connected ImageManager agents. Select an agent in the list to have ImageManager display information from that agent in the ImageManager UI.









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

Managed Folder Tasks


Link	Description
 Start Managing Folder	Opens the Managed Folder Settings dialog box, where you specify the storage locations for backup image files that you want ImageManager to manage (See Creating a Managed Folder).
 Stop Managing Folder	Removes the currently selected managed folder (in the Managed Folder pane).
 Verification Settings	Opens the Verification Settings dialog box, where you can configure the automated verification service (see Verifying Backup Image Files).
 Consolidation Settings	Opens the Consolidation Settings dialog box, where you can configure ImageManager's consolidation service (see Consolidating Backup Image Files).
 Retention Settings	Opens the Retention Settings dialog box, where you can configure what ImageManager keeps and for how long (see Consolidating Backup Image Files).
 Folder Settings	Opens the Managed Folder Settings dialog box, where you can modify the settings for the currently selected managed folder (see Create a Managed Folder).

Agent Tasks

Link	Description
 Connect to Agent	Opens the Connection pane so you can connect to a system's ImageManager agent (see Connecting to an ImageManager Agent).
 Disconnect Agent	Disconnects the ImageManager Console from the currently connected ImageManager agent.
 Refresh	Instructs the ImageManager agent to re-query the system and update the data displayed in ImageManager Console.

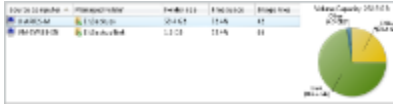
 Start Processing	The ImageManager agent examines its verification and consolidation schedule, and starts any operations scheduled to run at this time.
 Notification Settings	Opens the Notification Settings dialog box, where you can configure the Email notification parameters for ImageManager events (see Configuring ImageManager Notifications).
 Licensing	Opens the Job Licensing dialog box, where you can configure ImageManager agent licensing (see Configuring an ImageManager Agent).
Agent Settings	Opens the Agent Settings dialog box, where you can configure ImageManager agent behavior (see Configuring an ImageManager Agent).

Help Tasks

 View Help Contents	Opens the ImageManager help system.
--	-------------------------------------

Managed Folder Pane

The top-center Managed Folder pane displays information about the managed folders associated with the currently connected ImageManager agent. Select a managed folder in the list to see a graphical representation of the folder usage. 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 system from where ShadowProtect created the backup image files found in the managed folder.
Managed Folder	The path to the managed folder
Folder Size	The size of the managed folder
Free Space	The amount of free space available on the storage device where the managed folder resides. The Managed Folder pane also displays a graphical view of the storage space in the managed folder's volume.
Image Files	The number of backup image files contained in the managed folder.









Services

ImageManager Services dialog appears in the bottom-center portion of the ImageManager UI.



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	<p>Displays error or warning information about ImageManager's automated Verification and Consolidation services for backup image files.</p> <div style="background-color: #ffffcc; padding: 5px; margin-top: 10px;">  Note: This pane only displays if ImageManager encounters verification or consolidation errors. </div>
 Replication Targets	<p>Displays information about ImageManager's automated backup image replication service (see Replicating Backup Image Files).</p> <p>From the Replication Targets pane you can:</p> <p>Add New Replication Target: Opens the Replication Target dialog box where you can configure a target location to use with the replication service.</p> <p>Edit a Replication Target: Click the replication target name to modify the settings of an existing replication target.</p> <p> Delete Replication Target: Deletes a replication target.</p> <p> Pause Replication Target: Stops replicating to the associated target.</p> <p> Enable Replication Target: Resumes replication for a previously paused replication target.</p> <p>The Replication Target list icons represent the type of destination connection/drive:</p> <ul style="list-style-type: none">  Locally-attached drive  intelligentFTP-connected drive  ShadowStream-connected drive

 <p>HeadStart Restore Jobs</p>	<p>Displays information about ImageManager's HeadStart Restore (HSR) service (see Using HeadStart Restore).</p> <p>From the Head Start Restore pane you can:</p> <p>Add New HeadStart Job: Opens the HeadStart Job dialog box where you can configure a new HSR job.</p> <p>Edit a HeadStart Job: Click the HeadStart job name to modify the settings of an existing replication target.</p> <p> Delete HeadStart Job: Deletes a HeadStart job.</p> <p> Pause HeadStart Job: Stops a HeadStart job.</p> <p> Enable HeadStart Job: Resumes a previously paused HeadStart job.</p> <p> 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).</p> <p>The HeadStart Restore list icons represent the type of destination drive for that job:</p> <ul style="list-style-type: none"> •  Microsoft VHD virtual disk drive •  VMware VMDK virtual drive
 <p>Backup Image Files</p>	<p>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).</p>

Configuring ImageManager

Before using any of the ImageManager services, you must do some basic configuration so that ImageManager console can access the system you want to manage. These configuration tasks follow a logical order:

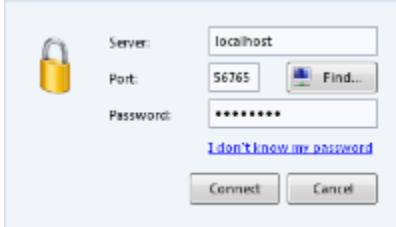
- [Connecting to an ImageManager Agent](#)
- [Configuring an ImageManager Agent](#)
- [Create a Managed Folder](#)
- [Configuring ImageManager Notifications](#)

Connecting to an ImageManager Agent


You must connect the ImageManager console to one or more ImageManager agents in order to manage an agent's backup image files.

To connect to an ImageManager agent:

1. Launch the ImageManager console. Upon startup, ImageManager displays a Connect dialog box:



2. In the Connect dialog box, provide the required information:

Server	The name or IP address of the system running the ImageManager agent. You can use the keyword localhost to connect to an ImageManager agent running on the same system as the ImageManager console.
Find	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 agent in the ImageManager\ImageManager.exe.config file. <div style="background-color: #ffffcc; padding: 5px; border: 1px solid #ccc;">  Note: You might have to modify your firewall settings to make the ImageManager agent port accessible. </div>
Password	The ImageManager agent password. The default password, when connecting to an ImageManager agent for the first time, is "password". Following your first connection, ImageManager prompts you to change the password. If you forget the ImageManager agent password, click I don't know my password to get instructions about how to reset your password (see Resetting the Agent Password).

3. Click Connect. ImageManager will connect to the specified agent and display its icon on the left-hand side of the ImageManager UI.

Connecting to Multiple ImageManager Agents

You can connect to multiple ImageManager agents simultaneously. To do this:

1. In the Configuration pane, click Connect to Agent. ImageManager reopens the Connect dialog box.
2. Specify the details for this other ImageManager agent.
3. Click Connect. ImageManager will now connect with this additional agent and display the agent's icon on the left-hand side of the ImageManager UI.

Resetting the Agent Password

When first installed, each ImageManager agent has a default password of "password". Use this when connecting to the ImageManager Agent for the first time. After connecting for the first time, you must change the Agent password. Once you have changed the password, if you forget it StorageCraft provides a password reset utility so you can reset the Agent password.

To reset the agent password

1. Download the Password Reset utility from <http://www.storagecraft.com/downloads/ImageManager.ResetPassword.exe> to a location of your choice.
2. Open a Windows command line shell (`cmd.exe`).
On Windows Vista / 7 / 2008 / 2008R2 systems, run the Password Reset utility from an administrative command prompt (right-click on the Command Prompt shortcut, then select Run as Administrator).
3. Browse to the directory where you downloaded the password reset utility, then execute `ImageManager.ResetPassword.exe`.
You can close Command Prompt after running the password reset utility.
4. Start ImageManager, then connect to the ImageManager Agent using the default password of "password".
5. When prompted, reset the agent password to a value of your choosing.

Authentication Restrictions

Because the ImageManager Console and ImageManager Agent communicate through a secure TCP connection, the Console must be able to authenticate to the Agent. If you install the Console and Agent on the same computer, or on computers in the same Windows domain, this happens automatically in the background.

However, if you install the Console and Agent on computers in different domains, or in a Windows workgroup, you must create a user account for the Console to use on the computer where the Agent is running. This account must have the same credentials (username and password) as the logged-in account used to start the Console. For example:

Console Computer	<ul style="list-style-type: none">• In workgroup MSHOME• Logged in as JDoe• ImageManager Console running
Agent Computer	<ul style="list-style-type: none">• In workgroup MSHOME• Not logged in• ImageManager Agent running (under the context of LocalSystem)



Note: In order for ImageManager Console to successfully authenticate to ImageManager Agent, the Agent computer must have a "JDoe" user account with the same password as the "JDoe" user account on the Console computer.

Configuring an ImageManager Agent

In the Configuration pane, you have two options that configure the ImageManager Agent:

- [Agent Settings](#)
- [Licensing](#)

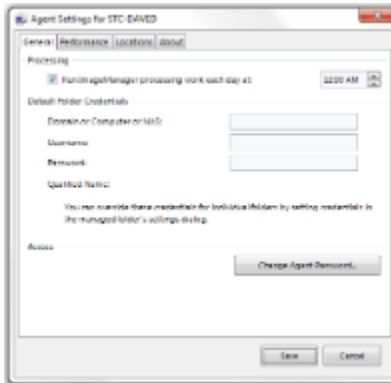
Agent Settings

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

- General
- Performance
- Locations
- About

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.

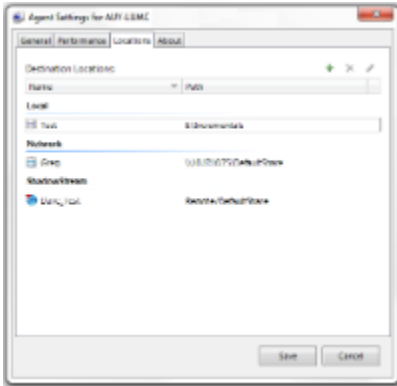
Control	(Default: Enabled at 12:00 AM) Lets you specify a time of day when the ImageManager agent performs its daily validation and consolidation operations. Disabling this setting suspends the ImageManager agent's automated re-verification and consolidation services. However, you can manually start the ImageManager agent processing of all jobs by clicking Start Processing in the Configuration pane (see Configuration 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.

Locations


The settings on the Locations tab let you configure or modify access to the Destination network resources or servers used by ImageManager. When you click on the tab, ImageManager displays a list of your currently configured destination locations (if you have not defined any, the list is blank):

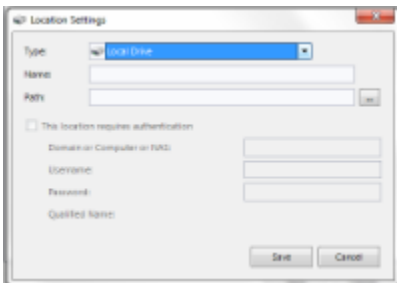


The list shows each resource by Type, Name, and Path.

This 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 agent 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 individual ImageManager job that uses these destinations.

Add a new Location

To add a new location for use with an ImageManager job, click on the  icon at the upper-right of the dialog. ImageManager displays the Location Settings dialog:



Here you can specify the settings for this new location:

- Type--You can choose a variety of types based on where the resource is located or by its connection:
 - Local Drive (locally-attached device)
 - Network Drive (server, NAS, BRD device, or other network resource)
 - intelligentFTP (for remote replication)
 - ShadowStream (for remote replication)
 - VMware ESX/ESXi Server (for network replication to a VMware server)
- Name (Optional)--Enter a descriptive name for this location to help identify it.

Based on which Type you just selected, ImageManager will only show the settings fields used by that resource type:

Local Drive Settings

For a Local Drive, ImageManager will only ask 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 will ask you to specify:

- 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).

intelligentFTP Settings

For a remote replication using the intelligentFTP tool, ImageManager will ask for:

- Path--Provide the path to the server running intelligentFTP.
- 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 server or network resource (Domain/Computer/NAS name, Username, and Password).

StorageCraft ShadowStream Server Settings



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.

For a remote replication using the StorageCraft ShadowStream tool, ImageManager will ask for:

- 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: Disabled)--Provide ImageManager with the authentication credentials needed to log into the server or network resource (Domain/Computer/NAS name, ShadowStream username and password).

VMware ESX/ESXi Server Settings

For a network replication to a VMware destination, ImageManager will ask for:

- 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).

Click Save to add your new Location to the global destination list.


Delete a Location



Note: ImageManager will not delete a Location that is in use by one or more jobs. You will need to go through and modify or delete those jobs in order to delete the selected Location.


To delete a location once you have modified or deleted all jobs using this Location:

1. Click on the location you want to remove.

2. Click on the  icon at the upper-right of the dialog.
ImageManager will remove the selected Destination Location from this agent's list.

Modify a Location

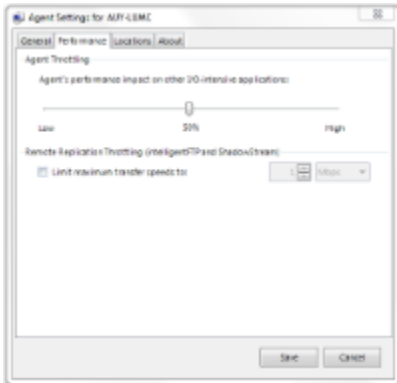
You can modify the settings for any of the defined Destination Locations. To do so:

1. Click on the location you want to change settings for.
2. Click on the  at the upper-right of the dialog.
ImageManager will display the location's Settings dialog. You can then modify the location's path or credentials as needed.
3. Click Save to save your changes.

All agent jobs now will use the new settings for this Location.

Performance

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



The Performance tab has two settings:

- Agent Throttling
- Remote Replication Throttling

Agent Throttling

Use the Agent Throttling setting to increase or decrease the amount of CPU utilization available for processing ImageManager operations. This setting lets you prioritize ImageManager or other CPU-intensive application tasks. The default setting is 50%, which means that at most ImageManager can use 50% of CPU processing time to complete its work. The 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 will change to reflect the new setting.

Remote Replication Throttling

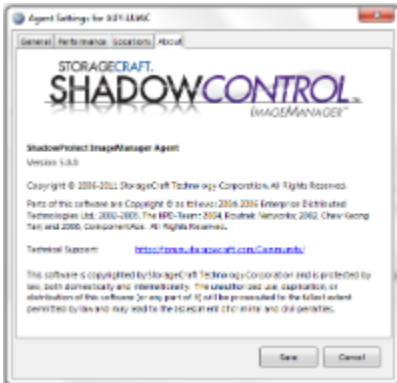
This optional setting modifies how fast ImageManager can send data to a remote site. (The download speed, that is, the transfer rate from the remote site back to this agent, is fixed at 15Mbps maximum.) The default is 1Mbps, with a range from 1Kbps to 999 Gbps. This setting only applies if you have purchased and installed one or both of the add-on transfer tools: intelligentFTP or ShadowStream.



This replication throttling setting is a global setting for all jobs assign to this ImageManager agent. You can modify this transfer rate setting for a particular job when you configure it.

About

The About tab displays version information about the ImageManager agent:



Click Save or Cancel to exit the About dialog.

Licensing

The Licensing menu option lets you activate ImageManager premium features:

- HeadStart Restore
- intelligentFTP
- ShadowStream

StorageCraft licenses each of these features on a per-job basis. You assign each job license to one agent for one job. (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.
- Each HeadStart Restore license supports one device restoration.

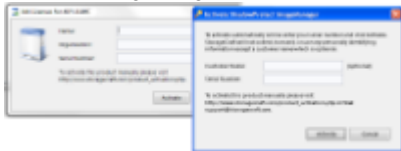
For more information about each of these operations, see [ImageManager Features](#).



Note: While you can purchase as many premium feature job licenses as needed, 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. The Activate dialog box appears:



3. In the Activate ShadowProtect ImageManager dialog box, provide the requested information:
 - Customer Name: (Optional) Specify the name of the product purchaser, either person or organization.
 - Serial Number: Enter the Product Key that you received when purchasing ImageManager or premium feature licenses.
4. Click Activate.
5. 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:

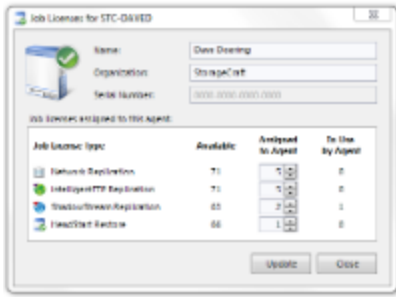
- a. Review the information in the Product Activation dialog box for accuracy. Correct any errors, then click Activate to resubmit the activation request.
- b. If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again.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

Assigning Licenses


The Licensing tab also controls the assignment of premium feature licenses to this agent. These features include:

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


Each of these add-on features is licensed per-job and, once installed, will appear listed in the dialog:



Each job license type shows its usage:

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. <div style="background-color: #ffffcc; padding: 5px; border: 1px solid #ccc;"> <p> Note: 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.</p> </div>
In Use by Agent	Shows the number of licenses actually in use by a ImageManager job for this selected agent.

You can 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 will need to delete those job(s) first in order to reduce this number.

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: I have Backup Image Sets from five servers that I want to manage from a single ImageManager console. I need to replicate each of the servers locally and off-site, and I would like to start using HeadStart Restore as well.

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 wish to use with HSR.

Example 2

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

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: I have four servers (A, B, C, and D) managed by a single ImageManager installation. I 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.

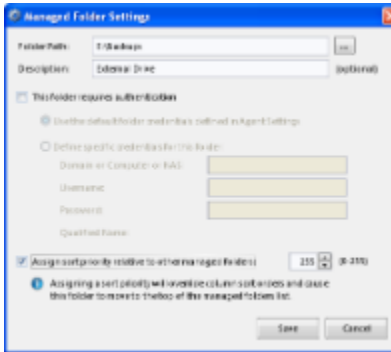
Example 4

Environment: I have three servers at one location and another at a remote site that I want to manage using ImageManager. I 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. I want to protect them all using HeadStart Restore at either location.

Licensing Solution: Install ImageManager at the local and the remote site. 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 .

Create a Managed Folder

You must assign ImageManager to one or more folders in order to manage backup image files.



To create a new managed folder

1. In the ImageManager console, select the ImageManager agent that you want to configure.
2. In the Configuration pane, click Start Managing Folder.
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 will then run these jobs in this order.

Configuring ImageManager 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, then select the events that you want to generate Email notifications.

| Failures

| Send an Email when an ImageManager operation fails. |

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.

4. In the Notification Settings dialog box, select the Email Setup tab to configure the Email account where you want to send the Email notifications.

| SMTP Server

| 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.

5. Click Save.

Verifying Backup Image Files

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).

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 can roll-up all Incremental backup image files created during that day into a single point-in-time Incremental image file that contains all updates made to the system that day. 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 that contains all updates made to the system that week. 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 can roll-up all Weekly Consolidated files created during that month into a single point-in-time Incremental image file that contains all updates made to the system that month. Monthly consolidated files include a `-cm` in the file name. For example: `D_VOL-b001-i097-cm spi`.



ImageManager retains the Monthly Consolidated files permanently as part of the backup chain.

Configure Consolidation Settings



The retention policies you configure using ImageManager are different from the retention policies set in ShadowProtect. The policies set in ShadowProtect apply only to weekly or monthly backup jobs, not to continuous incremental jobs. While you define both types of jobs in ShadowProtect, ImageManager handles the retention policies for the continuous incremental ones.

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. Next, configure the consolidation schedule:

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).

5. Click Save.

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

Configure Retention Settings

To configure your retention policy:

1. In the Configuration pane, click Retention Settings.
2. Specify the settings for this folder's file retention policy:

Keep Intra-daily image files	(Default: 7 days) The minimum number of days to keep Incremental backup image files that ImageManager has rolled into a daily consolidation.
------------------------------	--

Keep consolidated daily image files (-cd)	(Default: 15 days) The minimum number of days to keep daily consolidated backup image files that ImageManager has rolled into a weekly consolidation.
Keep consolidated weekly image files (-cw)	(Default: 90 days) The minimum number of days to keep weekly consolidated backup image files that ImageManager has rolled into a monthly consolidation.
Move consolidated image files to a subdirectory	(Default: Disabled) Following consolidation, ImageManager can move the source backup image files into a subdirectory (called Incrementals) of the managed folder, rather than delete the backup image files once consolidated.



Warning: The Incremental files in the Incrementals folder are "orphans" since they are no longer stored with their associated Full image. Do not attempt to restore these files from the Incrementals folder.

Replicating Backup Image Files


The ImageManager Replication service lets you automatically copy backup image files to a secondary location. You can configure this service using the ImageManager Replication Targets pane:



During processing, the ImageManager replication service considers your retention policy and other ShadowProtect settings so that it duplicates only those backup image files necessary to ensure a full disaster recovery.

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	<p>(Default: Local Drive) Identifies the type of replication target. Supported options include:</p> <p>Local Drive: The replication target is attached directly to the local system (for example, an external hard drive).</p> <p>Network Drive: The replication target is accessible via the local network (LAN).</p> <p>intelligentFTP: The replication target is accessible via FTP (File Transfer Protocol).</p> <p>StorageCraft ShadowStream Server: The replication target is accessible via ShadowStream.</p> <div style="background-color: #ffffcc; padding: 10px; margin-top: 10px;"> <p> Note: Network and FTP replication targets require intelligentFTP installed, while the ShadowStream high-performance replication tool requires ShadowStream. Both of which are available for purchase separately. ImageManager will test the connection to ShadowStream when you save this replication job. If it cannot confirm the ShadowStream connection, ImageManager will not save the job.</p> </div>
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 & Security	<p>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 to 999 Kbps, Mbps, or Gbps.</p> <p>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.)</p> <p>Compress data stream (Default = disabled): Available only when Type = ShadowStream Server. Enables compression on the data sent using ShadowStream. You do not need to compress the data stream if you already have ShadowProtect compress your image files. Doing so reduces system performance.</p> <p>Encrypt data stream (Default = disabled): Available only when Type = ShadowStream Server. Enables encryption on the data sent using ShadowStream. You do not need to encrypt the data stream if you already have ShadowProtect encrypt your image files. Doing so reduces system performance.</p>

5. Select the Replication Mode tab.
6. Specify the appropriate settings for this replication in answer to the question: "Are you replicating to a folder being consolidated by a second ImageManager at the target?"

You can distribute the effort of consolidating backup image files by replicating from one managed folder to another managed folder on a different system that also runs ImageManager. By doing this, you can have one system perform the daily consolidations while another performs the weekly and monthly consolidations. The Replication Mode tab lets you configure your replication service to support your use of the ImageManager consolidation service.

No--Replicate all consolidated files	<p>(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:</p> <p>Also replicate the original Incremental backup image files (Default: Disabled) Enabling this option sends both the consolidated and the original incremental files to the secondary site. This requires the most bandwidth and storage space.</p> <p>Files moved or deleted by ImageManager are also removed on the destination. (Default: Enabled) This means that if ImageManager deletes a backup image file at the primary site, it will also remove the file from the replication target.</p>
Yes--Replicate only consolidated daily image files	<p>(Default: Disabled) Enabling this option means that the replication target is also an ImageManager-managed folder which will perform the weekly and monthly consolidation.</p>
Yes--Replicate only original unconsolidated intra-daily image files	<p>(Default: Disabled) Enabling this option means that you plan on performing all file consolidation at the replication target, rather than at the source-managed folder.</p>

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

Using ShadowStream

The StorageCraft ShadowStream high-performance transfer tool 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 sending full backup images to the remote site. It is also simpler to configure and maintain than conventional FTP.

ShadowStream has two parts run on a server: the ShadowStream service itself and an Administration interface. Once the service runs, you can use ImageManager to configure replication jobs to use ShadowStream. (See configuring [Locations](#) under Agent Settings for details.) Multiple ImageManager agents can access the ShadowStream transfer service to perform these replication services.

Ports

ShadowStream uses these ports by default:

- Port 4363 is the data connection control port
- Port 4364 is the admin connection port
- Port 4365 is the data transfer port
- Ports 54363 to 55263 are used for parallel connections

Confirm that these ports are accessible through your firewalls for ShadowStream to run.

Installing ShadowStream

The ShadowStream service and administrator console run on:

Operating System

- Windows 2000 Server and Professional
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows XP SP3
- Windows Vista SP1
- Windows 7

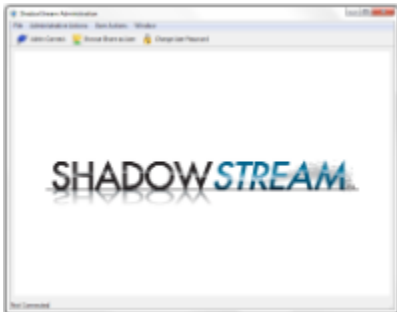
Hardware

You will also need a dual-core or better processor to run ShadowStream.

To install ShadowStream:

1. Run the ShadowStream Setup file.
2. Click Finish when the Install Wizard completes.
3. Click on Start/StorageCraft/ShadowStream Admin Console.

The ShadowStream administrator console displays:



4. Click Admin Connect at the upper-left.
5. Click OK to log in using the default Admin account and password.

You can now configure ShadowStream for use with ImageManager.

Configuring ShadowStream

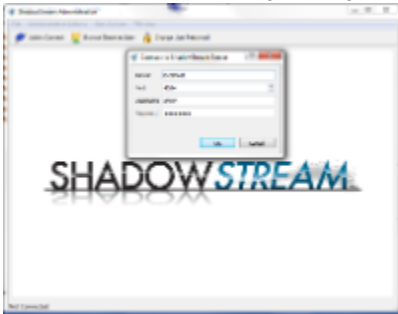
Once you install ShadowStream, at a minimum you should configure:

- A new administrator password
- At least one ShadowStream user for executing replication jobs
- A share as the destination file folder
- Settings to raise the maximum concurrent file transfer connections

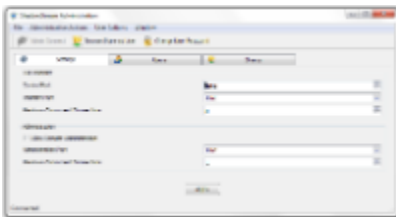
The default port settings should only be changed if necessary.

To configure ShadowStream:

1. Launch the ShadowStream administrator console.
2. Click Admin Connect and log in using the default Admin account and password:



3. The console displays the Settings tab:



4. The system installs with these defaults:

- A single share called "DefaultShare" is created in the same location as the server. It has Share (all) permissions.
- An administrative user is created named "admin" with the password "shadowstream"
- Port 4363 is the data connection control port
- Port 4364 is the admin connection port
- Port 4365 is the data transfer port

Changing the Administrator Password

You will need to change the default Administrator password for the ShadowStream server.

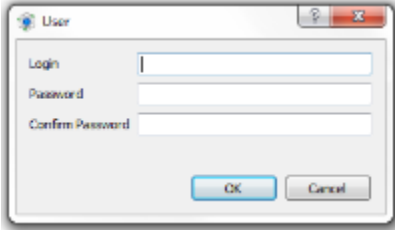
1. If you haven't done so, log in to the ShadowStream administrator console.
2. Click the Users tab.
3. Click Change Password in the lower-right corner of the dialog.
4. Enter a new password for the Administrator.
5. Click OK to change the administrator password.

The Admin user only has rights to administer the ShadowStream service, you will now need to [add a new user](#) so ImageManager can process replication jobs.

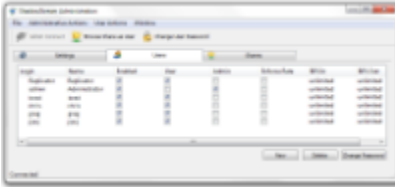
Add a New User

To add a new user to ShadowStream:

1. Click on the Users tab.
2. Click New in the lower-right corner of the dialog. ShadowStream displays the New User dialog:



3. Enter a name and password for the user.
4. Click OK to save the new user. ShadowStream now shows the new user in the Users tab:



Configuring Users

You can change settings for new or existing users:

Setting	Description
Enabled	Default is Enabled. Uncheck this box to disable this ShadowStream user.
User	This is the default. A user can be either or both a ShadowStream user and a ShadowStream administrator.
Admin	Mark this box if you want this user to be a ShadowStream administrator.
Enforce Rate	Check this box to enforce the limit to the bandwidth available to 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. (ShadowStream limits downloads to a maximum of 15Mbps.)
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 once you make the changes.

Configure Settings

The ShadowStream Settings tab configures:

- File Transfer
- Administration

The one setting that will need adjusting is the File Transfer Maximum Concurrent Connections.

File Transfer

You can configure:

Setting	Value
Control Port	Default is 4363. Leave this default unless your firewall policy requires a specific change.
Transfer Port	Default is 4365. Again, leave this default unless your policy requires a change.
Maximum Concurrent Connections	Default is 1. This limits the number of user, administrator, and ImageManager connections to the ShadowStream server.



Note: A Best Practice is to set the Maximum Concurrent Connections setting at least 2 higher than the number of users and administrators on the ShadowStream server. This setting can be critical if there are no available connections for an ImageManager agent to perform a replication job. Users consume connections while doing a Browse Share listing. These connections stay active until the user closes the console. It is possible then for all connections to be in use before an ImageManager agent attempts to run a replication job. If all connections are consumed, ImageManager will only make three attempts then stops the replication job and reports an error. Setting the number of connections higher prevents this from occurring.

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 is 4364. This specifies which port on 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 is 1. This limits the number of administrator connections on the server. If you do allow remote administration, you should leave the default to enhance security.

Click Apply when you complete your settings.

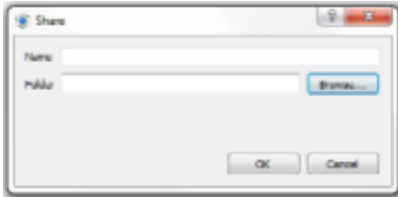
Create a ShadowStream Share

ShadowStream creates a DefaultShare folder under the StorageCraft/ShadowStream install folder on the destination server with Share (all) permissions. You can configure ImageManager to use this DefaultShare folder as the target for replication jobs. However, you may want to add one or more shares in order to:

- Better differentiate between jobs and where ShadowStream stores their content.
- Grant users permissions to only a specific share rather than to the general DefaultShare.

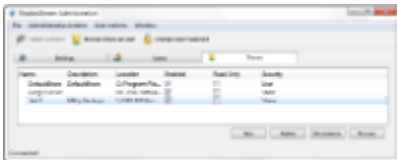
To add a share:

1. Create the destination folder(s) on the target ShadowStream server using that system's operating system tool.
2. In the ShadowStream console, click the Shares tab.
3. Click New. ShadowStream displays the Share dialog:



4. Enter a descriptive name for this share.
5. Click Browse to locate the destination folder for this share.
6. Click on the folder to highlight it.
7. Click Select Folder.
8. Click OK.

ShadowStream adds this new share to the list:



Configuring Share Settings

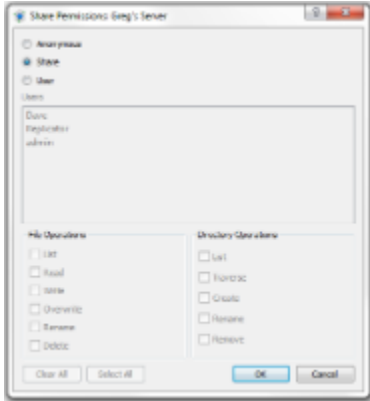
You can also change settings for this new share:

Setting	Description
Name	Double-click on the name to modify it. Keep in mind that ImageManager may be using this name in a replication job. Changing the name once it is in use by a job will cause the job to fail.
Description	Double-click on the Description to enter a phrase about the share.
Location	Displays the path selected for this share. Modifying this allows you to change the destination folder for this share. If you move also move the contents of the previous destination folder to the new path, ImageManager replication jobs will not be affected by the change and will run normally. (Otherwise, ImageManager will re-send all the contents intended for the folder instead of only the updates.)
Enabled	(Default is Enabled) Use this setting to temporarily disable a share. (Use the Delete button to permanently remove a ShadowStream share.)
Read Only	Use this setting to make a share read-only.
Security	Displays the Permissions setting for this share. The settings are Anonymous, Share, and User. (Click the Permissions button to modify this.)

Configuring Share Permissions

You can modify the Share permissions for the highlighted share:

1. Click the Permissions button. ShadowStream displays the Share Permissions dialog:



2. You can select:

Permission	Description
Anonymous	Grants all permissions to any user, not just ShadowStream users. For security reasons, we strongly suggest not selecting Anonymous.
Share	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.

3. Click OK to accept the permissions settings.

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

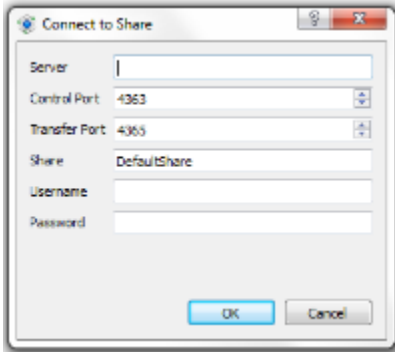
Users and ShadowStream

The primary use of ShadowStream is to perform ImageManager replication jobs. However, users can also access the ShadowStream administrator console to:

- Confirm their backup image files have replicated at the remote site
- Download image files from the remote site to their workstation.
- Change their password.

Users can access the console by:

1. Click Start/StorageCraft/ShadowStream Admin Console.
2. Click Browse Share as User at the top. ShadowStream displays the User Login dialog:

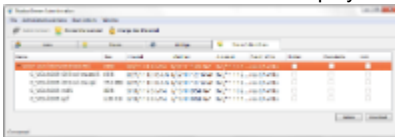


3. Enter the destination Server name, ShadowStream Share then the username/password.



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, for example, existing Windows shares on the target server).

4. Click OK. ShadowStream will display a directory listing for the selected ShadowStream share:



Folder and File Actions

You can perform various actions on the files or folders based on your 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.

Change Your Password

To change your password for accessing the ShadowStream console:

1. Click Change User Password.
2. Enter these details:

Field	Comment
Server	Enter the name of the local ShadowStream server.
Control Port	The default is 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.

3. Click OK to change your password.

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

Using HeadStart Restore

The ImageManager HeadStart Restore (HSR) service lets you start a restore operation at a destination system even while the original production server continues to run and ShadowProtect continues to add Incremental backup image files to the image chain from that server. This greatly reduces downtime associated with certain failover operations, particularly for systems that have very large storage systems (ie: multi-Terabyte). For information about HSR use cases, see [HeadStart Restore Scenarios](#).

You can access the HeadStart Restore service in the ImageManager HeadStart Restore pane:



An HSR operation involves the following tasks:

- Creating a HeadStart Job
- Finalizing a HeadStart Job

Creating a HeadStart Job

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

VMware Considerations

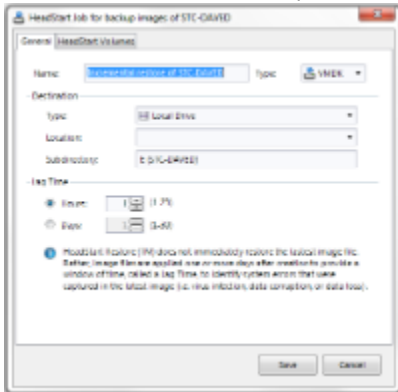
HeadStart Restore can use VMware targets with these considerations:

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

Create a new HeadStart Restore Job


To create a 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. The HeadStart Job dialog appears:



3. In the General tab, specify the appropriate settings:

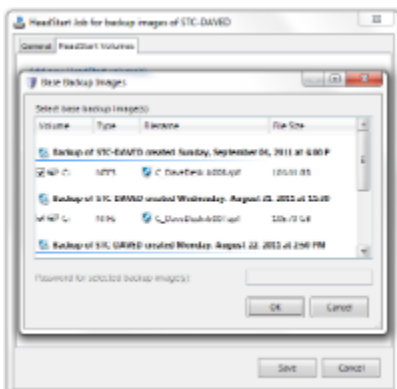
Name	(Optional) Enter a descriptive name for the HeadStart job.
Type	Indicates the type of Virtual Machine file that you want HeadStart Restore to create. The supported types are: <ul style="list-style-type: none"> • VMware VMDK: Create a Virtual Machine Disk (VMDK) file compatible with VMWare virtual environments. • Microsoft VHD: Create a Virtual Hard Disk (VHD) file compatible with Microsoft Hyper-V and Oracle VirtualBox virtual environments.

Destination	<p>The HSR target. You can specify:</p> <ul style="list-style-type: none"> • Type • Location • Subdirectory <p>Type</p> <p>You can choose a:</p> <ul style="list-style-type: none"> • Local Drive (locally-attached device) • Network Drive • VMware ESX/ESXi Server (Only available for VMDK targets.) <p>Location</p> <p>You can select from the dropdown list of your pre-defined locations to use for this HeadStart Restore operation. If you haven't defined any locations, you can specify a new one by clicking on Add new location. ImageManager will ask you for:</p> <ul style="list-style-type: none"> • Type--ImageManager will default to the same type you chose earlier. • Name (Optional)--Enter a descriptive name for this location to identify it. • Server--You can use UNC (for VHD targets), IP address, or server name. <div style="background-color: #ffffcc; padding: 10px; margin: 10px 0;"> <p> Note: For VHDK targets, 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.</p> </div> <ul style="list-style-type: none"> • Share--Specify which Windows Share on the server you wish to use for this operation. (Only available for VHD targets.) • Authentication (Default: Disabled)--You can provide ImageManager with the authentication credentials needed to log into the server or network resource (Domain/Computer/NAS name, Username, and Password). <p>Subdirectory</p> <p>ImageManager will provide a default name for the subdirectory to store the HeadStart Restore files on the target. You can modify this name as needed.</p>
Lag Time	<p>The lag time associated with a HeadStart job. You can set the lag time in hours (1 - 23) or days (1 - 30).</p> <p>Lag time defines the delay between when ShadowProtect creates an Incremental backup and when HeadStart Restore applies that backup to the HeadStart volume. The lag time protects you by giving you time to identify problems (system error, corruption, virus, etc.) with the Incremental backup(s) before applying it to the HeadStart volume.</p>

Add HeadStart Volumes

Next, you need to create one or more HeadStart volumes for this job. ImageManager creates these volumes from your existing base images in your backup chain. To create these volumes:

1. Click the HeadStart Volumes tab.
2. Click Add new HeadStart volumes. The Base Backup Images dialog appears:



1. In the Base Backup Images dialog box, checkmark the base image file you want to use for the HSR job from the list. (By default,

ImageManager marks all of the .spf files it finds in the managed folder.)

2. Click OK.
3. If you encrypted the file, provide the necessary password for accessing the image file.
4. (Conditional) When creating an HSR job of type VMware ESX/ESXi Server:
 - a. Click Click to Browse for Volume to locate the target VMDK.
 - b. Select the appropriate VMDK.
 - c. 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 outside of ImageManager (using the vSphere client, for example), add 18 MB to the minimum size shown in ImageManager to accommodate worst-case sector alignment in file system structures. ImageManager accounts for this automatically when creating a VMDK.
 - 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. Once created, you can add a virtual disk to the new VM.
5. Click Save to create the new HeadStart job.



Note: Once saved, the only supported modification to the job is to update the image file password. If you need to modify any other setting, you will need to delete this one and create a new HSR job.

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

ESX Server Permissions

HeadStart Restore requires the following minimum permissions on the ESX 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 creating an HSR role on the ESX server that contains at least these permissions, then assigning 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 are restoring to a vCenter cluster, HeadStart Restore also requires the following permissions on the root of the cluster:

Category	Permissions
Global	Licenses

Finalizing a HeadStart 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 whose 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:

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.


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	<ol style="list-style-type: none"> 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.) <div style="background-color: #ffffcc; padding: 10px; margin: 10px 0;">  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. </div> <ol style="list-style-type: none"> 4. Reboot the VM and let the operating system load from the VMDK.
HSR of a Virtual Machine	<ol style="list-style-type: none"> 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




Once you perform a HeadStart Restore on a system, you can keep the existing HSR job as defined in ImageManager for that system. You may also want to consider disabling this job, creating a new HSR job for a different system, and assigning the HSR job license to this new job.

Browsing Backup Image Files

The ImageManager Backup Images service lets you view a historical record of your backup image file creation. You can access the Backup Image service in the ImageManager Backup Images pane:



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

- 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.)

Product Support

Technical support for StorageCraft products is available beginning with the release of the product and ending six months after the release of the next major version of the product or after StorageCraft discontinues the product line.

Complimentary Technical Support

StorageCraft complimentary technical support consists of self-help support tools, available at <http://forum.storagecraft.com/Community> (in English only), and a powerful knowledge base that helps you find answers to most frequently asked product questions, as well as “how-to” procedures and technical information about all StorageCraft products.

Email Support

To obtain email technical support for specific technical questions or issues, fill out the form at <http://forum.storagecraft.com/Community/web2case/>. Please provide as much detail as possible to help the technical support engineers understand and diagnose the issue.

In order to ensure efficient service, please provide at a minimum the following information:

- Product name and version number
- Detailed problem description, error code, log file description, etc.
- Hardware and software configuration, operating system version, service pack number, etc.

Telephone Support

StorageCraft offers telephone support for customers. For details, see our support guide at:

http://www.storagecraft.com/documents/StorageCraft_Technical_Support_Guide.pdf

Our online support information site is at: <http://www.storagecraft.com/support.html>.

Glossary

Backup: The process of copying files, volumes, and databases to preserve them in case of equipment failure or other catastrophe. Backup is a critical part of a disaster recovery strategy, but it is often neglected, particularly by personal computer users.

Backup Image File: A file that holds the contents of a backup activity. Backup Image Files let you restore the data of a computer system to a specific point-in-time.

Bare Metal Recovery: The complete restoration of computer data after a catastrophic failure (including the operating system, file system, partitions, volumes and data) from a complete backup image.

Base Image File: A backup file that contains a copy of all used sectors on a disk drive. This image file contains all data on the computer, including the operating system, applications, and user data.

Basic Disk: A physical disk drive that MS-DOS and all Windows operating systems can access. In Windows, basic disks can contain up to four primary partitions, or three primary partitions and an extended partition with multiple logical drives.

Cold Backup: A backup taken from the Recovery Environment, rather than when the computer's operating system is running.

Continuous Incrementals: A backup scheduling model for ShadowProtect that lets you create a base backup file, then create additional incremental backup files that include only changes that occurred since the last backup.

Compression: A technology that reduces the size of a file while preserving the original content. Compression lets you save time, bandwidth and storage space.

Differential Image File: Backup files containing the hard drive sectors that have changed since the Base Image File was created. Differential image files take about the same time to create as Base Image Files, but they are smaller. When restoring a drive (or files and folders), you must use the Base Image File with the appropriate Differential Image File to restore the computer to a specific point-in-time.

Disaster Recovery: The ability to recover from the complete loss of a computer, whether due to natural disaster or malicious intent. Typical disaster recovery strategies include replication and backup/restore.

Disk Device: A locally-accessible disk drive, including locally-attached USB or FireWire disk drives, and network drives such as SAN, NAS, iSCSI, SCSI, USB or FireWire.

Driver: A program that interacts with a particular device or software. The driver provides a common interface to the device, or software, that makes it accessible to other computer systems and the user.

Drive Letter: See Mount as Drive Letter.

Dynamic Disk: A physical disk that provides features that basic disks do not (see Basic Disk), such as support for volumes spanning multiple disks. Dynamic disks use a hidden database to track information about dynamic volumes on the disk and other dynamic disks in the computer.

Encryption: A procedure that renders the contents of a file unintelligible to anyone that cannot present the appropriate decryption key.

ExactState™ Imaging: The ability to create a backup image at a point where the computer is in the best state for creating a backup (for example, no open files).

Full Image File: See Base Image File.

Hard Drive: An electromagnetic storage device, also referred to as a "disk drive," "hard drive," or "hard disk drive" that stores and provides access to data on a computer.

Head Start Restore (HSR): The ability to begin the restoration of a large backup image chain while ShadowProtect continues to add Incremental backup image files to the same image chain. This reduces the time necessary to restore a large volume from days or weeks, to minutes or just a few hours.

Hot Backup: A backup image taken when ShadowProtect is loaded on the computer's standard operating system. A hot backup requires the use of a snapshot filter driver (see Snapshot).

Hot Restore: The restoration of a backup image while the computer or server remains up and running. You cannot perform a hot restore of a system volume.

Image or Image File: See Backup Image File.

Image Set: The combination of a Full image and all additional Incremental images necessary to restore a computer to a given point-in-time.

Incremental Image File: Backup files containing the sectors that have changed since the last Incremental backup was taken. Incremental Images are fast to create and smaller than either Base Image Files or Differential Image Files. When restoring a drive (or files and folders), you must use the Base Image File and the appropriate Incremental Image Files necessary to restore the computer to a specific point-in-time.

intelligentFTP: An optional tool available for ImageManager that improves transfer performance and usability over standard FTP for performing remote replication of backup files.

Lock Volume: A software request to gain exclusive access to a particular drive. Locking the volume prevents other software programs from changing the file system or opening files during the process of writing the image file.

Microsoft VolSnap: The proprietary Microsoft snapshot technology.

Microsoft Volume Shadow Copy Service (VSS): The backup infrastructure for Microsoft Windows XP and Microsoft Windows Server 2003 and later operating systems, as well as a mechanism for creating consistent point-in-time copies of data. VSS produces consistent snapshots by coordinating between business applications, file-system services, backup applications, fast-recovery solutions, and storage hardware.

Mount as Drive Letter: The process of assigning volumes (active primary partitions and logical partitions) to specific letter designators in the root namespace of a Microsoft operating system. Unlike mount points (see Mount Point), drive letter assignment permits only letters in the namespace, and they solely represent volumes. In other words, it is a process of naming the roots of the "forest" that represents the file system (with each volume being an independent tree in the "forest").

Mount Point: A directory on a volume that an application can use to "mount" (set up for use) a different volume. Mount points overcome the limitation of drive letters (see Mount as Drive Letter) and allow for a more logical organization of files and folders.

Mounted Volume: The ability to see and use a backup image that is physically located somewhere else on the network. When mounted, the backup image appears as a volume and behaves as if it were a part of the local computer system. Mounted volumes are read/write capable so users can update existing image files, scan for viruses or other malware, and repair the image file.

Operating System: Software that, after being loaded into the computer by a boot program, manages all other programs on a computer. These other programs are called applications or application programs.

Partition: The portion of a physical disk that functions as though it were a physically separate disk. Once created, a partition must be formatted and assigned a drive letter before data can be stored on it. On basic disks, partitions can contain basic volumes, which include primary partitions and logical drives. On dynamic disks, partitions are known as dynamic volumes and come in the following types: simple, striped, spanned, mirrored, and RAID--5 (striped with parity) volumes.

Point-In-Time Backup: A backup routine that lets you restore a file, folder, or the entire system to a specific point-in-time. Point-in-time backups are often used to roll-back a computer to a point prior to a computer problem.

Protected Volumes: Volumes that users have selected for backup by ShadowProtect.

RAID: Redundant Array of Independent Disks. A collection of disk drives that together offer increased performance and fault tolerance. There are a number of different RAID levels. The three most commonly used are 0, 1, and 5:

- Level 0: striping without parity (spreading out blocks of each file across multiple disks).
- Level 1: disk mirroring or duplexing.
- Level 5: block-level striping with distributed parity.

Real-Time: A level of computer responsiveness that a user perceives as essentially immediate, or that enables the computer to keep up with some external process such as backing up.

Recovery Environment: See StorageCraft Recovery Environment.

Remote Computer (Node): A computer that is physically located somewhere else on a network but is accessible from a local computer.

Restoring: The activity of retrieving computer data from a previously-saved backup image file.

Service: A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

Scheduled Job: A job created in the ShadowProtect interface. Scheduled jobs let ShadowProtect backup events to occur automatically.

ShadowStream: An optional high-performance transfer tool for remote replication of backup files using ImageManager. ShadowStream significantly improves transfer rates over traditional FTP.

Snapshot: A type of backup that provides a point-in-time view of a volume. When you perform a backup or scheduled backup, ShadowProtect uses either the StorageCraft Volume Snapshot Manager (VSM) or the Microsoft Volume Shadow Copy Service (VSS) to take a snapshot of the volume. Any changes that occur to the volume after the snapshot is taken are not included in the backup.

.spf: A file extension representing a ShadowProtect full or base image file.

.spi: A file extension representing a ShadowProtect incremental or differential image file.

.sp(number): A file extension representing a ShadowProtect image file that spans multiple files. The number following .sp is the sequence of the file in the spanned image file group.

Spanned Image Set: A Backup Image File that is divided into multiple smaller files for easier management or storage. This lets you save the Backup Image File to removable media such as a CD or DVD.

StorageCraft Recovery Environment: A secondary boot environment (or operating system) that gives a user the functionality necessary to access and restore Backup Image Files on a network. This environment is typically used when a drive cannot be restored from within Windows or when the computer has suffered a catastrophic failure and the entire hard drive must be restored.

System downtime: The amount of time a server or PC is offline and inaccessible to users. This is commonly known as having the system out of production.

System Volume: The volume that stores the boot files necessary to load an operating system. Typically, this is the C: volume.

Tray Icon: A graphical representation of a computer program or application. For example, ShadowProtect uses a tray icon for the user to gain information about the program. Tray icons reside in the Windows system tray.

UNC (Universal Naming Convention): A method used to identify folders, files and programs on a network computer. A UNC path begins with two backslashes followed by the server name, share name, directory and filename. For example, \\server_name\share_name\backup_name.spi.

Unprotected Volumes: Volumes not protected by ShadowProtect.

User Interface (UI): The portions of a computer system with which a user interacts (display, keyboard, mouse, etc.) and the portion of a software program that accepts and responds to user interaction.

Virtual Private Network (VPN): A private data network that makes use of the public telecommunication infrastructure. VPNs maintain privacy through the use of tunneling protocols, encryption, and other security procedures.

VirtualBoot: ShadowProtect's ability to create a Virtual Machine based on an existing backup image chain. Once started using VirtualBoot, the VM provides complete access to data, applications, and services provided by the original system, in a state corresponding with the last Incremental image included in the VM.

Virtual Volume: A locally-referenced volume that does not physically exist on the system. ShadowProtect uses virtual volumes for the benefit of protecting computer systems.

Volume: An area of storage on a hard disk. A volume is formatted using a file system, such as file allocation table (FAT) or NTFS, and typically has a drive letter assigned to it. A single hard disk can have multiple volumes, and volumes can also span multiple disks.

VSS-Aware: An application designed to work with the Microsoft Volume Shadow Copy Services (VSS) framework to ensure consistent data backup.