



# BDR for ShadowProtect User Guide

Updated September 2015



## Introduction to the BDR

Thank you for your purchase or evaluation of this product. If you have any questions or would like assistance, please contact technical support and it will be our pleasure to assist you.

The Backup and Disaster Recovery (BDR) appliance has three primary purposes:

1. Backup every single bit of data on other servers and desktops.
2. Ensure continuity of business operations in the event of a hardware failure or disaster.
3. Optionally backup data to the cloud or replicate to another BDR appliance

The BDR is installed in the same network as the servers and desktops it is protecting, data is backed up to the appliance on the local network, and then optionally that data is additionally replicated to other BDRs or to a storage cloud, for safekeeping and quick disaster recovery.

If you are a first-time user we recommend reviewing the [Getting Started](#) guide. We highly recommend that all users rely on the [configuration checklist](#) at the end of this document.

The BDR provides the following functionality:

- **Bare-metal backups.** Bare-metal backups of the customer's computers are streamed to the BDR appliance as often as every 15 minutes.
- **Fast virtualization.** If a customer has a server crash or equipment failure, the server can be instantly virtualized and run on top of the BDR appliance, restoring service in less than 5 minutes.
- **Transparent continuity.** Once the failed server has been virtualized on the BDR, users are unaware of the original server failure.
- **Cross-site and off-site replication.** Data on the BDR can be efficiently and securely replicated across a VPN or the public Internet to another BDR appliance. The target BDR appliance acts as a geographically diverse hot standby. If there is a major site-wide disaster that affects both that site's server(s) and their associated BDRs, the servers can be quickly virtualized on the standby BDR unit.
- **Off-site backup.** Data on the BDR can be backed up to a storage cloud dedicated to BDR data, where it is protected by unique silent data corruption protection technology and an unparalleled level of data redundancy.
- **Exchange granular recovery.** Individual mailboxes and messages can be copied out of raw Exchange databases inside of bare-metal backup images. Quickly find and restore individual messages and mailboxes, and also ease migration between Exchange servers.
- **NAS device.** The BDR also acts as a high-powered NAS device, for storing file-based customer data.

## Getting Started Guide

This getting started guide will review the basic steps required to physically install the appliance, and then configure the desired services. First-time users should review all steps in detail to ensure proper operation of the appliance and its services. The getting started guide will walk you through the following steps:

1. **Physical Configuration:** Mounting and cabling.
2. **Windows Configuration:** License agreements, computer name, and initial password.
3. **Configuring Credentials:** Ensuring you have the credentials needed for setup.
4. **Update Appliance Software:** Allow the appliance to download software updates.
5. **Setup Bare-metal Backups:** Setup other computers on the network to be backed up to the BDR.
6. **Setup Off-site Monitoring and Backups:** Connect the BDR appliance to an online backup account. This is required even if you will not be backing up data off-site.
7. **Setup Cross-site Replication** (*Optional*): Configure the BDR as a replication source or target.
8. **Setup Exchange Archiving** (*Optional*): Setup long-term retention of Exchange data. This is not required in order to use the Exchange granular recovery feature.
9. **Setup Notifications** (*Recommended*): Ensure end-users and resellers are notified of warnings or errors, as desired.
10. **Test Virtualization** (*Highly Recommended*): Ensure that your servers are able to be virtualized without difficulty, so you can have confidence things will go smoothly in a time of crisis.

Use the **Configuration Checklist** (on the desktop on the BDR, or at the end of this documentation) to review and make sure everything is configured properly.

## Physical Configuration

When you unpack the appliance, check that it came with the following additional parts:

- **Power cord(s).** If your appliance also has a redundant power supply, it should also come with a second power cord.
- **Mounting rails** (rack-mounted appliances only). These rails are designed for mounting of the equipment in standard 19" racks.

Follow these steps to begin configuring the appliance:

1. **Mounting.** Secure the appliance in its desired location. The location should have an environment suitable for computing equipment, including environmental controls for temperature and humidity, and filtering of the air to remove dust and other particulate material. Hardware sensors and monitoring software on the appliance will help you measure environmental quality over time.
2. **Power.** Connect the power cord(s) to a filtered power source, such as a UPS or surge protector, to avoid damage to the appliance.
3. **Networking.** Use Cat5e or Cat6 cables to connect one or more of the Gigabit Ethernet ports on the back of the appliance to the appropriate network switch(es) or router(s). Each appliance comes with one or more Gigabit Ethernet ports (in addition to the dedicated management port, if any) and supports a variety of network configurations. Each port can be configured with separate IP addresses (on the same or different subnets), or two or more ports can be "teamed" together to support automatic failover and 802.3ad link aggregation. At this point, you will need to connect at least one of the network ports to a network, so that you will be able to remote desktop into the appliance once it is past the initial out-of-box setup.
4. **Lights-out Management Port.** If you have a model with Lights-out Management (IPMI) and wish to use it, connect a Cat5e or Cat6 cable to the dedicated management port on the back on the appliance. The management port is located separate and apart from the other non-management network ports and is clearly labeled as a management port. If the management port is connected to the same network as the non-management ports (which is not required, you can use a dedicated management network), the management port will acquire a different IP address than the non-management ports.
5. **Get Access to the Console.** Turn on the appliance. If you have a model with Lights-out Management, you can use the remote console feature to access the console (virtual monitor/keyboard) of the appliance across the management network. Without Lights-out Management, you will need to temporarily connect a monitor, keyboard, and mouse to perform the initial configuration steps until you reach a point where you can use remote desktop to access the appliance.

If you are using Lights-Out Management, the management processor will automatically obtain an IP address through DHCP as soon as the management port is connected to a network. To learn the IP address that was acquired, consult your DHCP server (router or network server), or connect a monitor and use the screens in the BIOS to view the current IP address. Once you know the IP address, open <http://ipaddress/> in your browser. The default username is ADMIN and the default password is ADMIN (case sensitive). Once logged in, make sure to change the default ADMIN password, and then use the menus to start the remote console (requires Java).

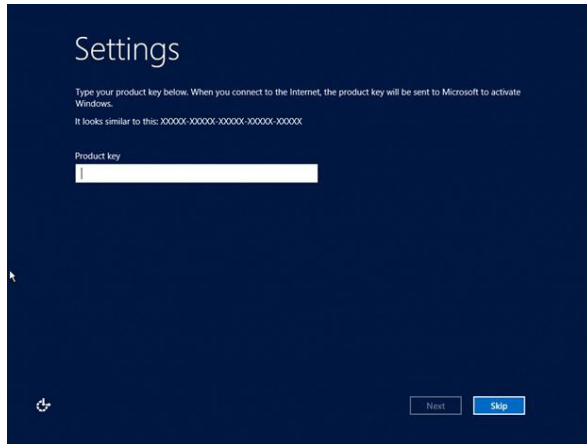
At this point, the appliance should be powered on and connected to the network, and you should have access to the console via a monitor and keyboard or via the Lights-out Management remote console feature.

## Windows Configuration

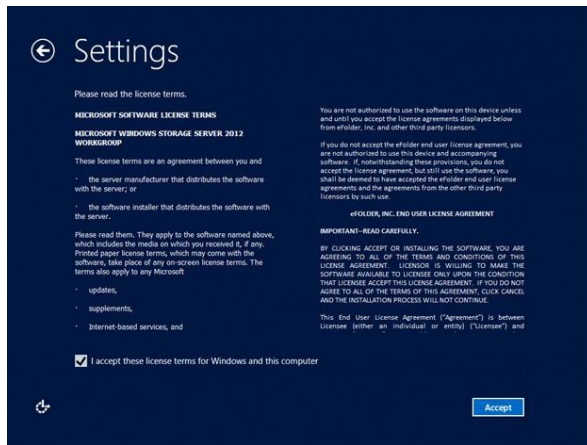
When the appliance first boots, you will be presented with the Windows Storage Server first-run setup wizard. You will be unable to login to windows or use remote desktop until this setup wizard is completed.

The wizard takes you through the following steps:

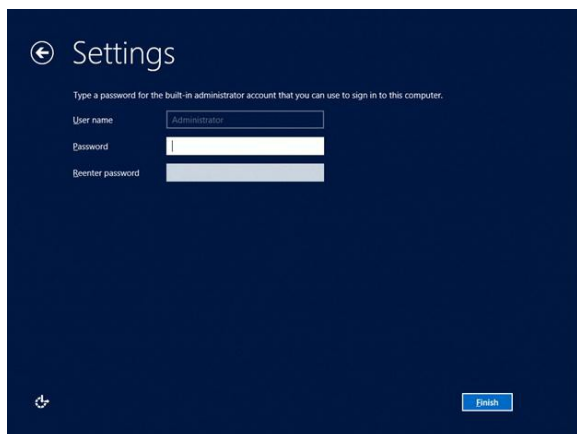
1. **Activate windows.** Enter the activation key on the label that is attached to the BDR.



2. **License agreement.** Read, review, and decide whether or not to accept the license terms presented on the screen. Use of the equipment and its bundled software is subject to acceptance of the presented license terms. If you choose not to accept the terms, the appliance will turn off.



**Administrator password.** The wizard will prompt you to set a password for the *Administrator* Windows user. Choose a password of sufficient length and complexity to meet your security requirements. For maximum security, we recommend setting a password that is at least 15 characters in length or longer. The Administrator password authorizes logging in to the server, as well as accessing the network data shares hosted by the appliance.



Once you have finished the wizard, you will be prompted to login to Windows. Login as the Administrator with the password that you set above.

Once logged in to Windows, you may want to perform one or more of the following additional configuration tasks:

- **Configure networking.** For example, you may want to set static IP addresses, configure link failover or link aggregation, etc.
- **Install additional management software.** You may want to install additional software to help manage the appliance, such as an IT monitoring agent, an end-point security agent (anti-virus, etc.), etc. If you just need basic virus scanning to meet compliance needs, [ClamWin](#) is a free and open-source anti-virus engine that is easy to install, updates automatically, and should meet your compliance requirements.
- **Join the appliance to a domain.** You may optionally join the appliance to a Windows domain, to gain the benefits of active directory integration and to apply group policies.

**Important Tip:** If you do join the BDR to the domain, we highly recommend creating a local administrative windows user on the BDR so that you can still easily login if the domain controller is down and you are trying to virtualize the domain controller on the BDR.

Windows comes configured with two data volumes:

1. **C:\ (Operating system).** Typically 80 GB with space reserved for a recovery partition. This contains the operating system and the bundled software. Do not create writable network shares or otherwise allow user data to be stored on this volume. The documentation and other important files are all stored within subdirectories of C:\Appliance. This partition may be larger for certain models that come with a large amount of RAM, to ensure that there is enough room for the virtual memory swap file.
2. **X:\ (Data files).** This volume is given the rest of the disk space. It is used to store all user data (including bare-metal backup images). This volume can be dynamically expanded without rebooting through the purchase of storage add-on packs and a short configuration process (see instructions for expanding storage).

These volumes are stored on top of a hardware RAID1 (or RAID10) volume, managed by either an Intel or an LSI controller.

## Configuring Credentials

Now that Windows is up and running, and networking is fully configured, the next step is to configure the off-site and bare-metal backups. First, make sure that you have the following credentials readily available:

1. **Online backup account credentials.** Even if you are not sending backed up data off-site, the online backup account credentials will be used to connect the appliance with the centralized Web Portal for monitoring and reporting purposes.

If you have purchased the appliance, you will receive a username and temporary password in an email.

If you are evaluating the appliance, use the partner Web Portal to create a new BDR free trial account. If you do not have access to the partner Web Portal, please contact your reseller or sales representative to receive a free trial account.

2. **Encryption pass phrase.** A pass phrase is a textual phrase (letters, numbers, characters, symbols, etc.) that will be converted into a 256-bit encryption key and used to encrypt your data on-disk. If you are sending your data off-site, you must create a pass phrase if you will be sending data off-site. If you are only doing local backups or cross-site replication, use of on-disk encryption and therefore creating a pass phrase is optional but recommended.

The pass phrase cannot be changed once configured, so choose the pass phrase carefully and document it. A strong pass phrase is longer than a password. One possible strategy for creating a strong pass phrase is to combine several known passwords or phrases, separating them with various letters, numbers, and symbols.

**VERY IMPORTANT:** It is extremely important that the pass phrase is documented in multiple places, so that you will be able to decrypt and restore your data when needed. Appropriate places to document the pass phrase depend on your individual security and compliance requirements. For example, possible places include PSA automation software, asset tracking software, a secure password wallet, with your reseller, and/or a safety deposit box.

**Credentials to computers that will be backed up.** A Windows login with administrative credentials for each server or desktop that needs to be backed up. This could either be a domain administrator or a local account with administrative privileges on each of the machines.

## Update Appliance Software

The software that runs the appliance is continually being updated and enhanced. All BDRs require a maintenance and support subscription that ensures you always have access to the most recent version of all BDR software.

To ensure that your BDR is running the latest version of all BDR software before it is configured, the software update process should be manually initiated. Note that the BDR will also automatically install software updates every evening at a random time between 6pm and 11pm.



To install software updates, double click the **Update Software Appliance** icon on the desktop: The software update process will run. Depending on the size of the updates, this may take some time to finish. It will display the progress of any downloads on the console as the software update process runs.

## Setup Bare-metal Backups

One of the primary functions of the BDR is to manage and receive data for [bare-metal backups](#) for other computers in your local network (or across a VPN that allows the SMB file-sharing protocol). The bare-metal backups are powered by StorageCraft ShadowProtect. The setup process involves four main steps for each computer (server or desktop) you want to backup:

1. Perform [Preparatory Work](#) on each server or workstation that will be backed up.
2. [Install ShadowProtect](#) This does require a reboot of the computer (not the BDR), which can be scheduled as part of the install. (Note that you **can** configure the backup jobs without rebooting. You will just not be able to start the initial backup until the computer has rebooted.)
3. [Configure a Continuous-Incremental Backup Job](#) to backup to a directory on the BDR that is unique to this computer. If you plan to backup the data off-site, you must place the ShadowProtect backup images in a subdirectory of X:\VolumelImages. If you do not want the backup images to be taken off-site, you should place the backup images in a subdirectory of X:\LocalVolumelImages.
4. [Configure the ShadowProtect ImageManager](#) (running on the BDR) to monitor the directory that contains the bare-metal backup images. This monitors the integrity of the backups, and also collapses incremental files to save storage space (both on the BDR and off-site).

## Setup Off-site Monitoring and Backups

Next, we will configure your online backup account. Even if you will not be sending data off-site, you still must configure the online backup account so that licensing, monitoring, and reporting continue to operate correctly.

If you need additional detailed instructions or help configuring the online backup account, refer to the getting started guide that will appear when you first start the backup manager. Our technical support team is also available and will be pleased to assist you.

The backup manager comes preconfigured to backup any bare-metal backup images (in X:\VolumelImages). It also is preconfigured to monitor (but not upload data) for bare metal backup images in X:\LocalVolumelImages. The bare-metal backups generate a base image file and thereafter generate incremental files (for example, one every 15 minutes). Once per day, the ShadowProtect Image Manager consolidates these incremental files into a single daily incremental, consolidates daily incrementals into weekly incrementals, consolidates weekly incrementals into monthly incrementals, and consolidates monthly incrementals into a single rolling incremental. Online backup comes preconfigured to back up the base image, the daily incrementals, the monthly incrementals, and the rolling incremental.



## Account Configuration

Each BDR must be connected to the Web Portal via an online backup account, even if you do not plan on sending data off-site. This account provides integration with the Web Portal, and supports the notification, reporting, and licensing features of the BDR.

In short, the backup manager should be used to enter the online backup user name and password, create the pass phrase, choose a backup schedule, and set bandwidth throttling options. Refer to the detailed [online backup configuration instructions](#) for more information.

## Initial Backup Overview

If you plan to backup the data on the BDR off-site, then the initial base image must be uploaded. The data can either be uploaded over the network, or a [preload \(seed\) drive](#) can be used to encrypt and copy the data, which is then mailed to our data center for processing. Unless you have a fast connection (> 5 Mbit/sec), performing a preload is recommended if you have more than 50 GB of data.

## Initial Backup via Internet Upload

No extra configuration is needed to upload the data over the Internet. The initial upload may take hours, days, or even weeks depending on the amount of data and the speed of your connection. To estimate how much data will be sent, open the backup manager, go to the *Folders* page, click the *Visualize* button, and wait for the total disk usage to be tallied and displayed at the bottom of the *Visualize* dialog.

## Initial Backup via Preload (Seed) Drive

The process consists of putting the account into maintenance mode, requesting a preload (seed) disk from eFolder, initiating the preload operation, shipping us the drive, and waiting for it to be processed. Please review the detailed [preload instructions](#) for important information.

## Setup Cross-site Replication

[Cross-site replication](#) is optional. Skip this step if you will not be using cross-site replication (Note: off-site backup is not replication; if you are only using [off-site backups](#) then skip this section.)

## Setup Notifications

The BDR is configured by default to monitor the health of all services, including bare-metal backups, off-site backups, cross-site replication, RAID status, system health, and hardware health.

End-users can configure email notifications by changing the notification settings in the online backup manager (Options page, Notifications tab). The online backup manager is the software responsible for monitoring *all* other services on the BDR as well as the hardware.

Resellers can configure notifications by logging in to the partner Web Portal and choosing the *My Partnership -> Notifications* menu action. On this page, you can configure generic notification rules that apply to all of your customers' systems. For example, you can setup an email alert such that on any warning or error condition an email will be sent to your support address.

Alerting is also integrated with certain ticketing and PSA systems, such as ConnectWise PSA.

Resellers can also monitor the status and health of all systems through the dash panel report in the partner Web Portal.

**Tip:** If you are a reseller or MSP, we highly recommend installing a remote monitoring and management (RMM) agent onto the BDR and also the servers being backed up so that you can be alerted in real-time of backup failures and other important events.

## Test Virtualization

We strongly recommend that once you have completed your initial backup of each server, you do a test virtualization for each of the computers you plan to be able to virtualize later, to ensure that your systems are fully compatible with our technology.

**It is also advisable that you do regular scheduled testing to ensure that your backups stay viable and useable.**

Do not be caught by surprise when you are in the middle of an emergency. **Test now to ensure everything works properly when you really need it most!**

To do this, follow the instructions to [virtualize a server in test mode](#).

## Bare-metal Backup and Restore

Bare-metal backups and restores are powered by the latest version of [StorageCraft ShadowProtect](#). ShadowProtect provides both the user interface and backup engine for backing up the servers and desktops in the local network on to the BDR.

**Tip:** *Bare-metal backup* denotes a type of backup where data is backed up at the volume level (rather than at the individual file level), and where an entire computer can be restored without having to first reinstall the operating system. Thus, you can take a computer that is just "bare-metal" (without an OS) and directly restore all of the data.

When used in combination with the BDR, backups are always configured in the *Continuous Incremental* mode, allowing incremental snapshots to be taken every few minutes.

If configured properly, the BDR monitors the ShadowProtect backups to ensure that:

- The bare-metal backups are happening as scheduled.
- The files containing the bare-metal backup images are not corrupted (verified periodically and also as the data is replicated or uploaded).
- The chain of incrementals (from the base image to the current point in time) is unbroken and intact.
- The incremental files are being consolidated properly.

If there are any warnings or errors from the above processes, the BDR will take the appropriate notification actions (see [Monitoring and Reporting](#)).

Notable features of ShadowProtect include:

- **Fast, fully compressed, and optionally encrypted volume-level backups.**
- **Efficient and lightweight incremental snapshots**, allowing incremental backups to be taken every few minutes. Such backups do not scan the entire disk, but rather track which blocks change in real-time, and then when a backup begins only those changed blocks need to be read and packaged into an incremental.
- **Multi-tiered data aging schedule.** Intra-daily deltas are automatically consolidated into daily deltas. Daily deltas are consolidated into weekly deltas. Weekly deltas are consolidated into monthly deltas. Monthly deltas are consolidated into a single rolling delta. You can choose to retain an arbitrary number of daily and weekly and monthly deltas, to tradeoff between the granularity of recovery points and the required storage.
- **Easy restore of individual files.** Bare-metal backup images can be mounted as a drive letter, allowing individual files to be restored from a bare-metal backup through Windows Explorer. A restore wizard is also provided.
- **Hardware independent restore (HIR).** Volume-level data can be restored to a server or desktop, even if the hardware is different (e.g., motherboard, CPU, memory, storage devices, volume sizes, etc.). Note that HIR is not available on trial licenses.
- **Instant virtualization.** ShadowProtect is integrated with Oracle VirtualBox, allowing for the instant virtualization of servers or desktops in just seconds. Your BDR comes bundled with the open source edition of Oracle VirtualBox, it's preinstalled and ready to go.

- **Conversion to VMDK and VHD.** A wizard is provided so that ShadowProtect bare-metal backup image files can be converted to VMDK (VMware) or VHD (HyperV) virtual hard disk files.
- **P2V / V2V / V2P:** The combination of the above features allows you to easily perform P2V or V2V (via conversion to VMDK or VHD) or V2P (through bare-metal restore)

ShadowProtect is normally licensed through a monthly subscription (per computer per month). A ShadowProtect activation key should have been provided when you purchased the BDR that should be used when activating a ShadowProtect backup agent that will be backing up to the BDR. If you already own your own ShadowProtect licenses, you may use these with the BDR (to do this, do not use the activation key that came with the BDR; rather, use the activation key you obtained when you purchased your own license of ShadowProtect).

**Tip:** There are two different versions of the ShadowProtect installer that you can use -- one for each kind of license. If you have bought a perpetual license, you must use the perpetual installer. Otherwise, you should use the MSP installer.

**Tip:** The MSP edition of ShadowProtect requires that a separate license key be used to activate each agent (server or desktop) that you are backing up. You can use the partner Web Portal to instantly provision a MSP license keys to use to activate your servers.

If you are just evaluating the BDR, during install of the agents simply do not enter a license key, and you will have 15 days to evaluate the software.

**Tip:** ShadowProtect can only backup data to a Windows share on the network through the Windows file sharing protocol (SMB). This means that the BDR will need to be on the local network, or a VPN tunnel with sufficient bandwidth and reliability will need to exist between the computers that are backing up and the BDR. In many cases we recommend using one BDR per physical site to ensure best performance and reliability. Contact technical support for more detailed guidance.

## Instant Virtualization

The BDR allows a server or desktop that has been backed up to the BDR (as a bare-metal backup image) to be virtualized in just a few seconds or minutes. Virtualization is powered by [Oracle VirtualBox](#). Your BDR comes with the open source edition of VirtualBox, which is preinstalled and preconfigured on the BDR appliance.

**IMPORTANT:** Many applications on the BDR are integrated with the specific version of VirtualBox that comes preinstalled. **Do not upgrade or downgrade VirtualBox without explicit instructions from technical support.**

The virtualization works through a tool called *VirtualBoot*. Running this tool displays a wizard that walk you through selecting the bare-metal backup image file(s) that contain the server or desktop you want to virtualize, configuring the appropriate amount of RAM to dedicate, performing the driver conversion process, and booting the virtual machine.

Servers or desktops can be virtualized in either [Test Mode](#) or [Production Mode](#):

- **Test Mode:** In this mode, the virtual server is either not connected to the network, or is connected to the network in NAT mode. In NAT mode the virtual server will be able to initiate outbound network connections, but will not be able to receive inbound connections.
- **Production Mode:** In this mode, the virtual server will appear on the same physical network that the original server was connected to. End-users will be able to connect to and use the server or desktop just like they normally would. The BDR must be connected to all appropriate subnets. If you have more than one sub-net, either use VLANs or dedicate a different network port on the BDR to each production subnet.

## Off-site Backups

The bare-metal backup images and other file data can be backed up off-site to our private storage cloud, offering unique benefits for BDR data vs public clouds or pure replication:

- **Silent data corruption protection:** Our private storage cloud has been built from the ground up for end-to-end silent data corruption identification and automatic repair. Strong and redundant checksums guard each data block from the moment it leaves the BDR, as it goes across the network and is received into our cloud, on-disk in our storage cloud, and as it comes back during a restore. Our level of data redundancy is unparalleled, providing nearly the equivalent of a triple mirror protecting the data.
- **Extremely fast restores:** When restoring data, the restore client will open 15 network connections to our storage cloud and download data in parallel. This overcomes *bandwidth-delay product* limitations, allowing you to fully utilize line speeds over 100 Mbit/sec.

For example, if you are restoring from our private cloud to a public cloud (such as the Terremark vCloud), you should be able to restore data very quickly (e.g., 45 GB/hour).

- **Strong on-disk and over-the-network encryption:** Your data is encrypted on disk with the AES-256-bit algorithm in CTR mode. The AES-256-bit algorithm is the best international standard available, and has been approved by the U.S. government for the encryption of TOP SECRET data.

Our strong encryption means you will remain compliant with HIPAA, NASD, and other regulations governing data and privacy for your backed up data.

- **Data integrity assurance:** Each 2kb data block is digitally signed with your 256-bit encryption key, providing cryptographic assurance that the data has not been accidentally or maliciously tampered with. Enjoy strong compliance with regulations that require evidence of the non-modification and integrity of backed up data.
- **Pass phrase recovery:** Our unique two-party pass phrase recovery system provides both ultimate privacy and peace-of-mind that data will always be recoverable.

Off-site backups are typically scheduled to happen once per day ~~in the early evening hours~~ after all of the previous days intra-daily incremental files have been collapsed into a single daily delta. The integrity of these local delta files are verified as they are backed up to our private storage cloud. Once in our private storage cloud, our unique silent data corruption protection technologies ensure your data will remain intact and free from corruption for as long as it's stored there.

### Cross-site Replication

Cross-site and off-site *replication* allows the data on one BDR to be replicated to another BDR, or another Windows server that is running the local backup server software (which could be located in the cloud or at a different site). The local backup server can easily be installed onto a server in the cloud (e.g., a Terremark server instance), so you can replicate into the cloud.

See the [configuration instructions](#).

**Note: Replication is not backup.** There are advantages and disadvantages of replication vs backup. It is important to understand the differences and what each is best suited for. Replication and backup **can** be used at the same time for maximum data protection.

**Backup** is best suited for long-term data retention, pristine data integrity, and for retaining of historical versions and deleted data for file-level data.

**Replication** is best suited for quick access to data on the target device, including instant virtualization of servers.

The following table summarizes the major differences between replication and backup:

|   | <b>Replication</b>   | <b>Backup</b>  |
|---|--|--|
| <b>Format of data on target device (BDR or local backup server)</b> | The data is stored in the same format on the replication target as it exists on the replication source. If the data is not encrypted on the source BDR, it will not be encrypted on the target BDR.  | The data is stored in a proprietary, compressed, and encrypted format.   |
| <b>Accessing data</b>   | Replicated data can be accessed immediately without having to perform a restore operation.   | Data must first be restored using the file manager tool before it can be accessed. (The file manager decrypts and decompresses the data from the backup storage.)                    |
| <b>Quick virtualization</b>   | Bare-metal backups can be instantly virtualized.   | Bare-metal backup images must first be restored using the file manager before they can be virtualized.   |
| <b>Historical data</b>  | Replication does not store historical versions of files. However, since the bare-metal backups store each point in time as a separate file, it is possible to restore historical data located in a bare-metal backup image on the target BDR.  | Backups support storing as many historical versions of a file as are desired.  |
| <b>Data corruption</b>  | <p>If data is corrupted on the source BDR and is not detected, the corrupted data will be replicated to the target BDR.</p> <p>Bare-metal backup images are always checked for corruption before they are replicated, mitigating the risk.</p> | Backups can store historical versions of a file, allowing the restoration of a previous (uncorrupted) version of a file if there is undetected silent data corruption on the source. |

### Cross-site Backups

Cross-site backups allow data to be backed up to another BDR or another Windows computer running the local backup server software, across any IP network (LAN, VPN, Internet). See the [configuration instructions](#).

For synchronizing data between sites, typically it is better to use [Cross-site Replication](#) rather than cross-site backups. A typical configuration will perform off-site backups (to our private storage cloud), or cross-site replication, or both [use of cross-site *backups* is much more rare].

### Exchange Granular Recovery

The BDR appliance comes bundled with software that allows you to open raw Exchange information store files and copy individual emails or mailboxes back into Exchange or into PST files, in just seconds. This allows an administrator to use the BDR to:

- Restore an important email that was deleted several months ago back into its original mailbox.
- Restore a mailbox that was permanently deleted back into a live Exchange information store.
- Easily migrate data to a new Exchange server (even different versions). This works by backing up the old Exchange server, starting the Kroll Ontrack PowerControls program on the BDR, opening the backup image, connecting to the *new* Exchange server, and dragging and dropping all of the mailboxes from the backup store to the new Exchange information store. The program will take care of creating all of the new mailboxes and restoring all of the mailbox data into the new Exchange information store.

The license for the Kroll Ontrack PowerControls software is tied to the BDR appliance hardware and cannot be transferred to another computer. As a result, you must run the Kroll Ontrack PowerControls software on the BDR appliance.

**To use the software you must first request an activation key.** Each unit is entitled to a license for a certain number of mailboxes for no charge, and additional mailboxes beyond this limit are available for subscription. For details, please contact your sales representative.

**IMPORTANT:** In order to use the Kroll software you must install Microsoft Outlook onto the BDR so that the Outlook version of MAPI is available to the GRE software-



## Monitoring and Reporting

IT without monitoring and reporting is chaos. The BDR monitors the activities of all key services running on the BDR, as well as hardware health, and provides mechanisms to issue notifications of failures and other events of interest.

The appliance monitors the following features and services:

- **Hardware health:** The appliance has many sensors embedded in its circuitry to monitor both the health of the electronic components (e.g., voltages, fan speeds) as well as the quality of the surrounding environment (e.g., ambient temperature). A full history of these metrics over the last day, week, month, and year is available in the system health report.
- **System health:** Performance problems, lockups, and other such problems can be frustrating to diagnose. The appliance is continually monitoring CPU usage, interrupt counts, memory usage, IO performance, file system usage, RAID health, network usage, and other system health metrics. Graphs of these metrics are available for viewing, just as with the hardware health metrics. Warnings or errors are triggered when the metrics indicate that the appliance needs some attention (for example, the file system is almost completely full).
- **Windows event log:** Any abnormal or unexpected errors in the Windows event log will be reported.
- **Bare-metal backups:** The appliance is monitoring the StorageCraft ShadowProtect backups to ensure that they are backing up every day, that the backed up data has not become corrupted, that the chain of incrementals is complete and intact, and that the deltas are being collapsed properly.
- **Off-site backups, cross-site backups, and replication:** Any and all errors needing attention with these services are monitored and reported at the end of any off-site backup, cross-site backup, or replication job. The services attempt to avoid introducing errors due to temporary problems that were resolved during the backup. For example, if the Internet connection went down for 30 minutes during the backup and it was able to resume once the Internet came back up, it will not trigger an error condition in this case.

Monitoring is performed primarily through two key mechanisms:

1. **System health report:** This report is generated locally every 5 minutes. When triggered, metrics are collected from the appropriate sensors and performance counters; warnings and errors are identified based on the data; a report and corresponding graphs are then generated. An up to date (within 5 minutes) report is available on the BDR by clicking the *Hardware Health* icon on the desktop.

A snapshot of this report is also available in the Web Portal for viewing from anywhere. This report snapshot is updated whenever the BDR contacts the Web Portal, typically once per day, according to the schedule set within the backup manager user interface.

2. **Web Portal reporting:** The BDR is configured to contact the Web Portal on at least a daily basis to upload reports and notify the Web Portal of any new warnings or error conditions. The Web Portal then creates summarized reports showing the status of services for all BDRs (e.g., via the *Dash Panel*/report). The Web Portal also allows detailed reports for individual BDRs to be viewed online as well. The Web Portal will also propagate any information via email (or other configured methods) according to the notification rules, as configured in the Web Portal.

When the BDR connects to the Web Portal, it analyzes the system and any configured services (such as bare-metal backups, email-archiving, off-site backups, etc.) to determine if there are warnings or errors to report.

Notifications are available to cover events triggered by all of the above monitored features, as follows:

#### Notifications for End-users:

- Emails sent at the end of backup or replication jobs: The backup manager can be configured to send an email at the end of a job (in the backup manager, go to the *Options* page, *Notifications* tab). The destination email address should normally be configured by editing the contact record associated with the account in the Web Portal.
- Email sent if there an appliance hasn't "checked in" and/or backed up within a certain interval of time (default is 3 days). This is configured in the Web Portal. (*My Account* -> *Notifications*).
- Email sent if disk usage has increased too rapidly or is above a certain level. This is also configured in the Web Portal. (*My Account* -> *Notifications*).

#### Notifications for Resellers:

- As a reseller, you can setup reseller-wide notification rules that apply to all accounts within your stewardship. These notifications are configured in the Web Portal (*My Partnership* -> *Partner Notifications*).

These notification rules are quite flexible and can match events based on a number of different constraints (event type, severity, etc.).

Supported notification actions currently include sending an email and notification actions with supported 3rd-party systems (e.g., opening a ticket in your helpdesk). For more information, review the reseller Web Portal documentation or contact technical support.

Additionally, backup and replication jobs can be configured to send an additional detailed email at the end of each job. We recommend that end-users interested in notifications configure the appliance to send them emails directly at the end of jobs, and that reseller partners rely instead on the *Partner Notifications* feature in the Web Portal for notification of failures.

## NAS / File Sharing

The BDR appliance runs the powerful Windows Storage Server 2012 operating system, and comes configured with an unusually powerful CPU and amount of RAM for a NAS device (due to the requirements for virtualization). You can take advantage of this by also using the BDR as a NAS appliance.

Because the BDR runs Windows, you can directly join it to a Windows domain, integrate seamlessly with active directory, and use the Windows server management tools to create network shares on the device. Simply RDP into the appliance and proceed as you would with any other Windows server.

Windows Storage Server 2012 is a specially optimized operating system for high-performance and reliable file sharing.

## Hardware RAID

The BDR is a key component of a business continuity solution, and must be highly reliable. All BDR models thus come configured with the OS and data stored redundantly over multiple hard drives, in a RAID 1 (mirroring) or RAID 10 (striped mirror) configuration, providing protection from drives failures.

RAID 1 or 10 provides superior virtualization performance and data redundancy compared to a RAID 5 or RAID 6 solution. Virtualization frequently exhibits random I/O read requests. The mirroring of RAID 1 and RAID 10 allow random read requests to be serviced 2 (or more) times as quickly as RAID 5 or RAID 6, due to the independent copies of the data on each side of the mirror.

RAID is implemented through quality controllers from either Intel or LSI.

The BDR comes with a [user interface](#), available in either the BIOS or as a Windows program (when the OS is running) to monitor and manage hardware RAID.

Additionally, all BDRs come with hot-swappable drive carriers. If a drive fails, RMA the drive with us and swap it out, then use the user interface on the BDR to integrate the new drive back into the RAID array.

Due to the hardware RAID design, the hot-swappable drive carriers, and the advanced Windows Storage Server 2012 OS, the data storage volume (X:\) can be expanded without having to bring the BDR offline and without having to reboot! (See [instructions for adding more storage](#).)

## Automatic Software Updates

The software that runs the appliance is continually being updated and enhanced. All BDRs require a maintenance and support subscription that ensures you always have access to the most recent version of all BDR software.

The BDR comes with a secure automatic software updater that receives software updates from our datacenter network. The software updater will run automatically every day at a random time between 6pm and 11pm. If you wish to disable automatic software updates, use the windows task scheduler to disable the *Update Appliance Software* task.

You can also initiate the software update process at any time by using the *Update Software Appliance* icon on the desktop:



When you start this program, the software update process will run. Depending on the size of the updates, this may take some time to finish. It will display the progress of any downloads on the console as the software update process runs.

## Bare-metal Backup and Restore Overview

This section describes procedures to install, configure, and manage bare-metal backups, as well as how to perform restores of entire volumes or individual files from bare-metal backups. See also [the overview](#) of this feature. It's also very important to perform [preparatory work](#) on the computers that will be backed up.

Additional detailed instructions are available in the ShadowProtect documentation, which is available in the C:\Appliance\Documentation\StorageCraft\directory on the appliance.

## Overview of Installing ShadowProtect Agents

ShadowProtect requires that a software "agent" be installed onto each server or desktop that will be using bare-metal backups. The agent should be installed with the user interface. The agents can be configured and monitored through a centralized management console that runs on the BDR.

Before installing the agents, we highly recommend performing [preparatory work](#) on each computer that is going to be backed up, to ensure optimal performance and to minimize the size of incremental backups.

Alternatively, the BDR comes preconfigured with a Windows share called *SetupPrograms*, which you can use to manually run and install the agent on each computer that needs to be backed up.

**VERY IMPORTANT: Reboot required:** After installing ShadowProtect (or after a major version update), the computer must be rebooted so that the new (or updated) file system monitoring driver can become active. Bare-metal backups will not be able to begin until the system has been rebooted.

## Preparatory Work before Installing ShadowProtect Agents

Before installing the ShadowProtect backup agents on each server or workstation, it is important to prepare each computer properly. ShadowProtect provides volume-level backups, which means that it scans for changed data at the volume-level instead at an individual file level. To ensure that incrementals are as small as possible, it is helpful to perform preparatory work before starting the initial ShadowProtect backup. These steps include:

- **Ensure volumes are NOT dynamic volumes.** ShadowProtect does not support restoring dynamic volumes, only basic volumes. (ShadowProtect will backup dynamic volumes, but will then restore them as basic volumes, and your system will not boot properly.) You should check and make sure that the volumes on the server are basic volumes and not dynamic volumes. Note that hardware RAID is fully supported. Due to hardware RAID or motherboard RAID, use of dynamic volumes is rare, but possible. You should always check.
- **Windows licensing and activation issues.** If you plan on being able to virtualize a down server on the BDR, you need to make sure that the Windows license of the servers being backed up will allow this. Certain OEM manufacturers use a custom Windows license that is specifically tied to their hardware's BIOS and will not allow booting or activation of windows unless their own BIOS is detected. In these circumstances, the Windows license may need to be upgraded to a Microsoft Open license or other volume-license. Contact your OEM server manufacturer for details on how to upgrade your Windows server license, if applicable.

- **Defragmenting any heavily fragmented drives.** Fragmentation can slow both backup and restore times, as well as reduce performance if the computer becomes virtualized on the BDR appliance.

Additionally, if a heavily fragmented volume is defragmented after the initial ShadowProtect backup, the incremental on the next backup will be relatively large, because of all of the moved data blocks at the volume level.

Thus, we recommend for optimal performance that if any volumes are heavily fragmented that they be defragmented before starting bare-metal ShadowProtect backups.

- **Documenting and Synchronizing the Directory Services Restore Mode password.** In order for you to be able to virtualize a domain controller (including SBS servers) you must know the directory services restore mode (DSRM) password. The first time you virtualize a domain controller, you must start the server in directory services restore mode (using F8 during boot), and then you must use the DSRM password to logon as the local Administrator user. This allows you to logon and set the IP address for the new virtual network adapters. For information on how to synchronize the DSRM password, see [http://technet.microsoft.com/en-us/library/ee808906\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee808906(WS.10).aspx)
- **Identifying legacy backup jobs and ensuring they backup to separate partitions that will not be backed up by ShadowProtect.** A common reason for very large incremental ShadowProtect backups is when legacy backup jobs are backing up data on the server to one of the volumes on the server that is also being backed up by ShadowProtect.

For example, we have seen cases where ShadowProtect was configured to backup the C: (OS) and D: (Exchange information store) volumes, but then there was also a task scheduler task to run an ntbak job to perform a full backup of the Exchange database every day and store it to D:\ExchangeBackup. So every day, a new file was being written by ntbak to D:\ExchangeBackup that was approximately the size of the Exchange store, and ShadowProtect was seeing this new file as all new data, and so the incremental was tens of GBs every day.

Another common example is where full SQL backups (e.g., SQL dumps) are scheduled to run and are placing the .bak files (SQL dump files) on one of the volumes that is being backed up by ShadowProtect. The solution in these cases is to either disable the legacy backup jobs, or to modify the legacy backup jobs so that they are storing the backed up data to a dedicated backup partition that is not also backed up by ShadowProtect.

Additionally, if legacy backup jobs attempt to run at the same time as a ShadowProtect backup, conflicts can occur because of Microsoft VSS. We recommend that you schedule legacy backups so that they do not attempt to run during the period of time when the volumes are being backed up by ShadowProtect.

- **Fully Documenting OS version and Networking Settings.** If you virtualize a down server on the BDR, you will need to know the OS type (e.g., Server 2008 64-bit) and correct IP address and DNS information for that server. You should make sure this information is documented and readily accessible so that in the event of a disaster, the information will be quickly at hand, and you will not have to guess at what the server IP address should be. This is especially important for domain controllers.
- **32 bit servers: Check IRPStackSize registry parameter.** Heavily loaded 32-bit Windows servers may need to adjust the IRPStackSize parameter to ensure backups are reliable. Please see [StorageCraft KB article 54](#).

## Configuring ShadowProtect Bare-metal Backups

Now that ShadowProtect is installed on each server or workstation, a continuous incremental backup job needs to be configured on each of the machines you want to backup. This can be performed without having to login to each machine through the use of the ShadowProtect management console that is installed on the BDR.

Follow these steps for each computer that you need to configure:

1. Login to the BDR, and open the ShadowProtect management console and go to the *Management View* tab.
2. If the management console indicates that it has not yet connected to that computer, click the *Connect* button to attempt to connect:



3. Once connected, you can click the *Manage* button to activate the management user interface for that particular computer:



4. The management console should now show several additional tabs across the top of the screen:

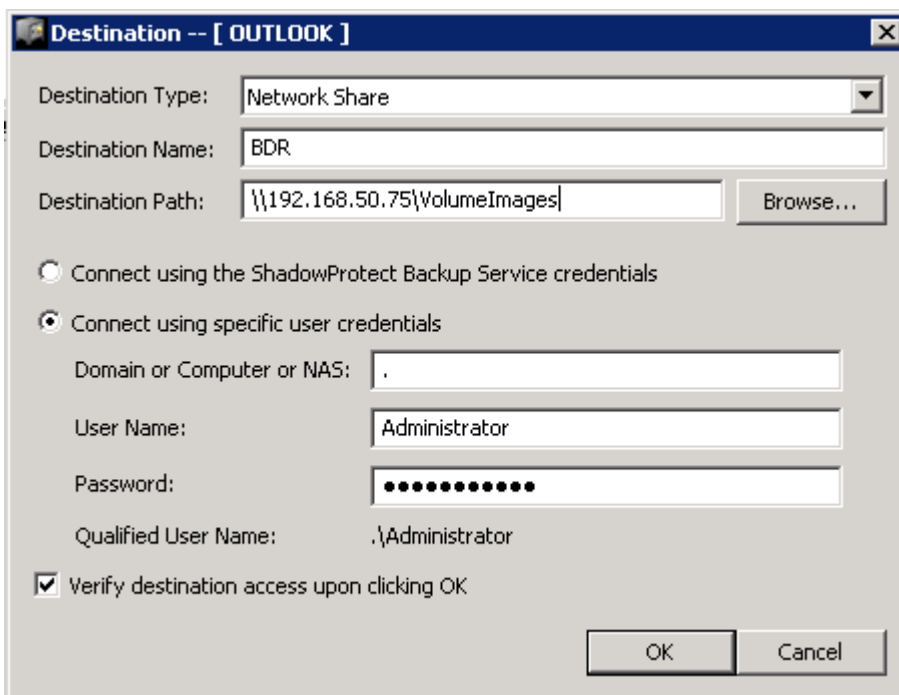


5. On the BDR, open Windows Explorer and create a new empty directory on the X: that will hold the bare-metal backup data for this specific computer (there should be a different directory for each computer you are backing up).

**IMPORTANT:** If you plan to backup the bare-metal backup images off-site, then make sure to create the new directory as a sub-directory of X:\VolumelImages. (e.g., X:\VolumelImages\ExchangeServer). If you do **not** plan to backup the bare-metal images offsite, create a new subdirectory of X:\LocalVolumelImages (e.g., X:\LocalVolumelImages\ExchangeServer).

6. With the new empty directory created, go back to the ShadowProtect management console, and click the *Destinations* tab. Then click the *Add* button. In the dialog that appears, enter the UNC path of the appropriate share (VolumelImages or NotBackedUp-LocalVolumelImages) of the BDR.

Also enter the credentials to access the share **on the BDR** (these are not necessarily the same as the credentials to access the machine you are backing up). If the BDR is not joined to a domain, use a period (.) for the Domain name and *Administrator* for the user name. When you are done, click *OK*. For example:



Destination -- [ OUTLOOK ]

Destination Type: Network Share

Destination Name: BDR

Destination Path: \\192.168.50.75\VolumeImages Browse...

Connect using the ShadowProtect Backup Service credentials

Connect using specific user credentials

Domain or Computer or NAS: .

User Name: Administrator

Password: .....

Qualified User Name: .\Administrator

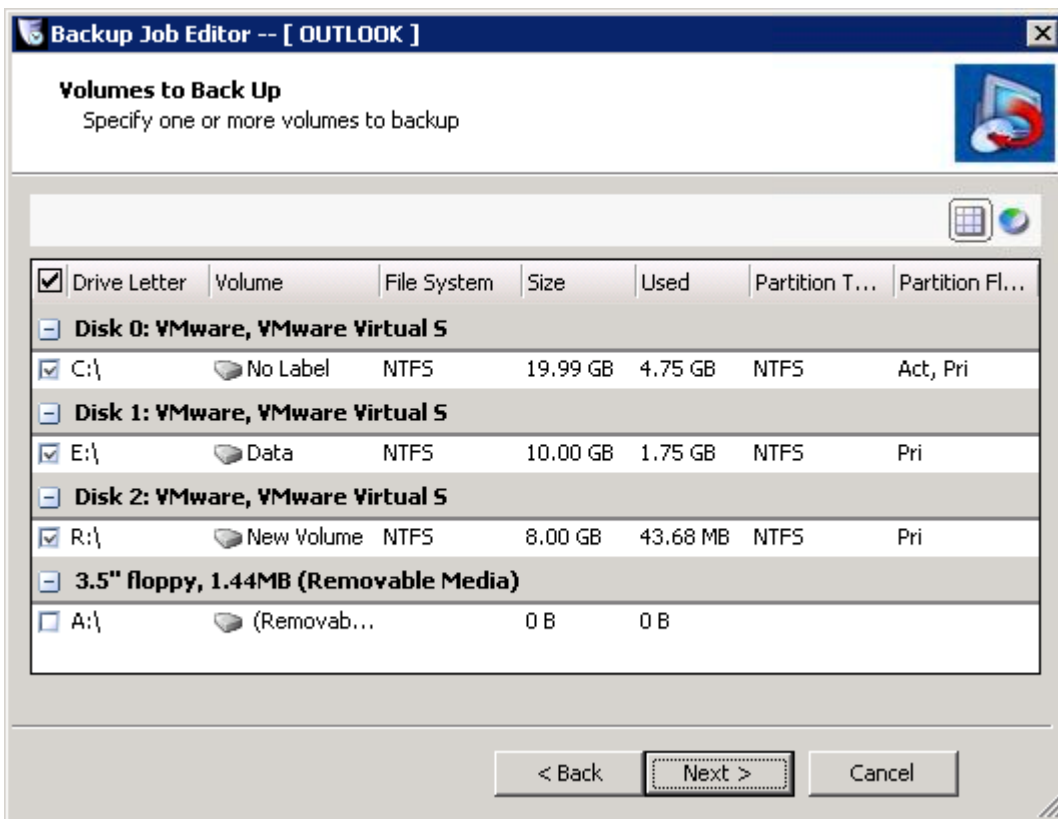
Verify destination access upon clicking OK

OK Cancel

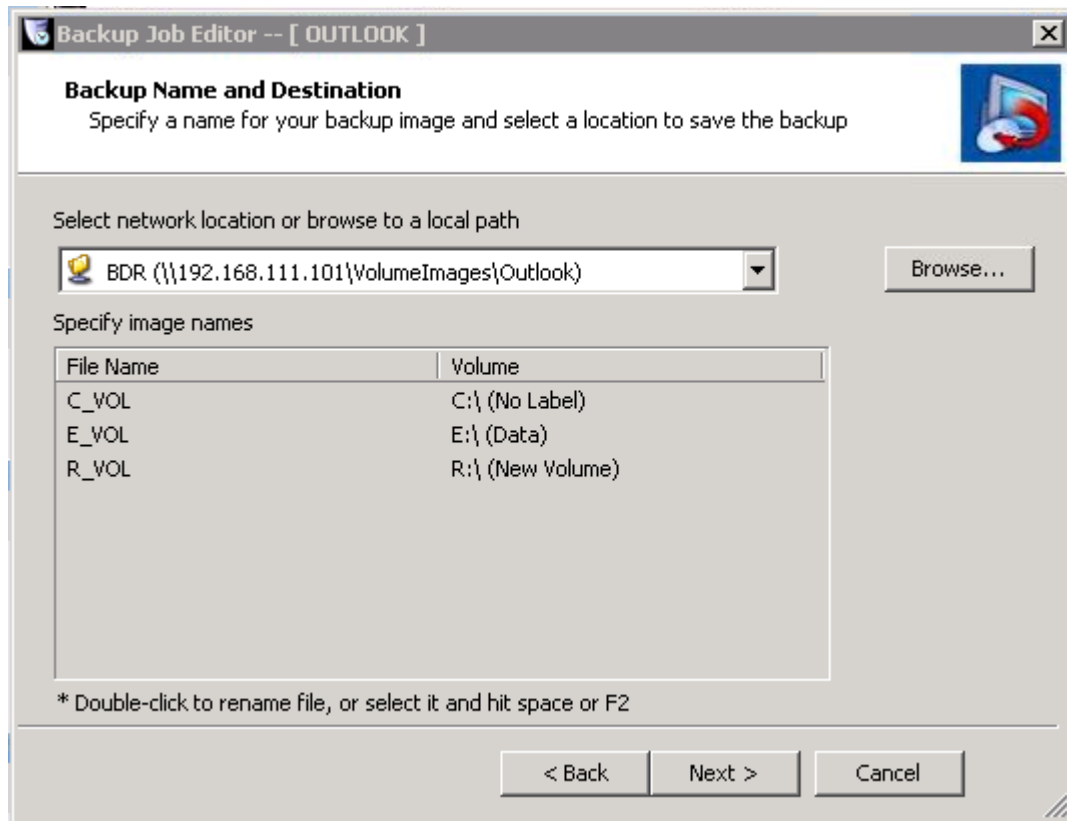


- Next go to the *Backup Jobs* tab and click the *Add* button to start the wizard. Click *Next* to get to the volume selection page. We recommend selecting **all** lettered volumes. If you are backing up SQL or Exchange databases, you must have both the database and log volumes on the same job, in order to truncate the logs.

For example:



7. On the next page, select the Network Destination that you created in step 7:



- On the next page, configure the backup schedule. **Make sure to select *Continuous Incremental mode***. Choose the backup window and the frequency (as often as every 15 minutes). If you want it to always backup, set the end of the backup window to one minute before the start of the backup window, it is smart enough to wrap around.

The screenshot shows the 'Backup Job Editor -- [ OUTLOOK ]' dialog box. The title bar includes a close button. The main heading is 'Specify the backup schedule'. On the left, under 'Schedule', there are radio buttons for 'Now', 'Later', 'Weekly', 'Monthly', and 'Continuous Incrementals', with the last one selected and highlighted in yellow. Below this is a note: 'NOTE: You must use the ShadowProtect ImageManager service with this option.' To the right, there are two sections: 'VSS Incremental Backups' and 'Additional Incremental Backups'. The 'VSS Incremental Backups' section has a row of checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat), with 'Sun' checked. Below it is a 'Start time' field set to '6:00:00 PM'. The 'Additional Incremental Backups' section has a similar row of checkboxes, with 'Mon', 'Tue', 'Wed', 'Thu', and 'Fri' checked. Below this are three time fields: 'Start taking backups at this time' (8:00:00 AM), 'Stop taking backups at this time' (7:00:00 AM), and 'Minutes between backups' (60, highlighted in yellow). At the bottom of this section, there is a checked 'Use VSS' checkbox and a 'Backups per day' field set to '24'. At the very bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'.

9. On the next page, set the compression mode to *High*. Optionally, set a password to use to encrypt the data.

**Tip:** if you use off-site backup, the data will **always** be encrypted regardless of whether you set a password here. The password here will be used to encrypt the bare-metal backup data stored on the BDR itself. As a best practice, we recommend that you do enable encryption on the StorageCraft backups.

**Tip:** If you are replicating data, you should strongly consider encrypting the bare-metal backup images, especially if the target replication device is not in a secure location.

**Tip:** If you decide you want to encrypt the ShadowProtect backup data, then we highly recommend using the same password here as you use for the online backup account pass phrase. This keeps things consistent and allows you to use the secure pass phrase recovery mechanism of your online backup account.

**WARNING:** If you encrypt the data using a password, you must know the password in order to restore your data. Keep the password well documented in several places that will be available even during a disaster, so you can be sure you will be able to restore your data. **StorageCraft does NOT have any means of recovering your encryption password.**

**Backup Job Editor -- [ OUTLOOK ]**

**Options**  
Specify the options you want for the backup image

Select Compression Method: **High**

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

Password:

Confirm Password:

Split image file **640** Mb

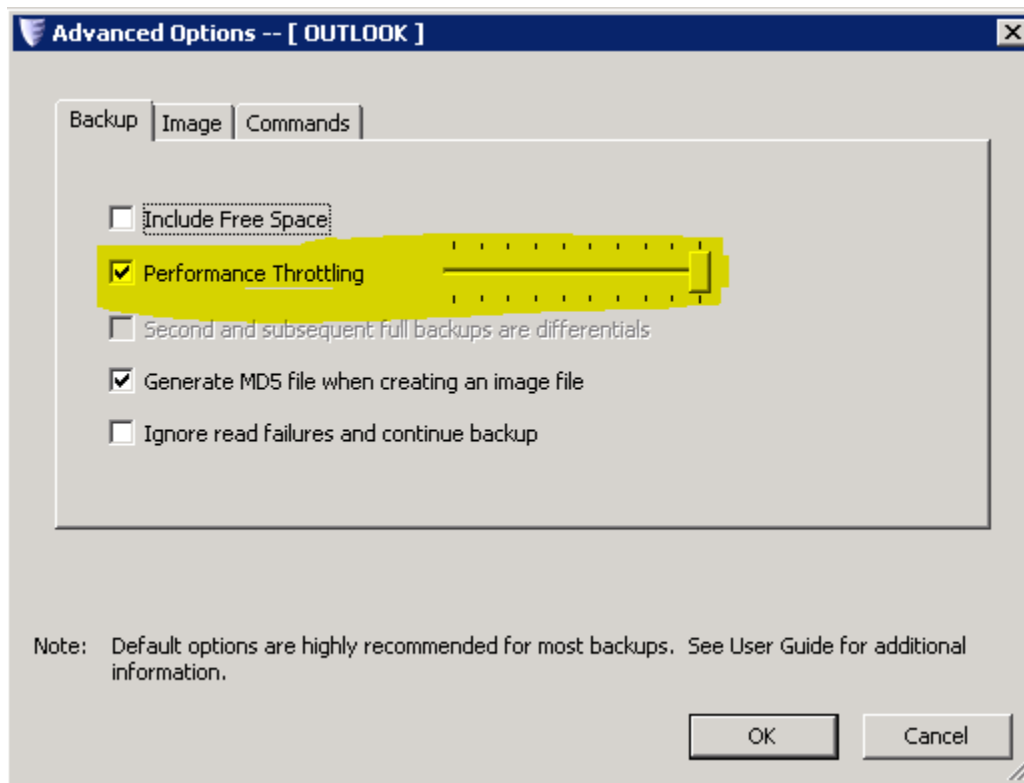
Backup Job Name

Backup Comment

**Advanced**

< Back **Next >** Cancel

Typically you do not need to change any of the advanced settings. The one setting you may want to change is the performance throttling if you are backing up a very busy server:



10. Click through to finish the steps in the wizard. You can use the *Execute* button to start the initial backup. The initial backup may take some time depending on how much data you have. Typically data rates are between 10 MB/sec and 80 MB/sec, depending upon your network, processor speed, and whether data encryption is enabled.

You now need to use the ShadowProtect ImageManager program on the BDR to tell it to start monitoring the folder that contains the bare-metal backups for this computer you are backing up. This is crucial to monitor the integrity of the data and to collapse deltas.

Follow these instructions to configure the ImageManager.

**Tip: Use of the ImageManager is required for continuous incremental backup jobs.**

## Configuring ShadowProtect ImageManager

The ShadowProtect ImageManager runs on the BDR and performs two critical functions:

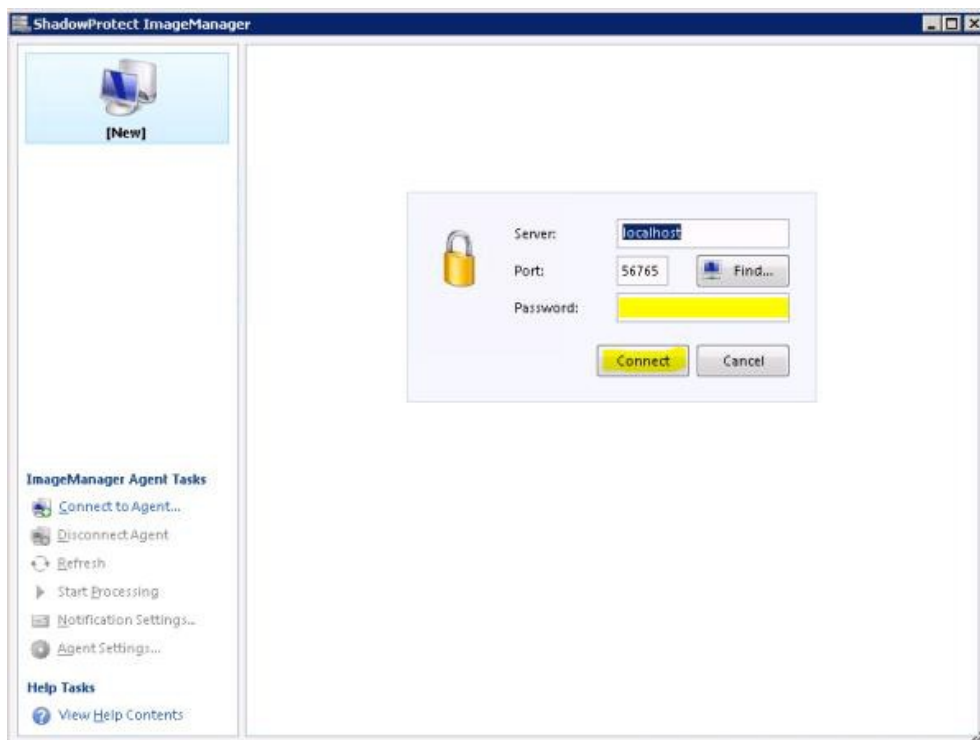
1. **Delta Consolidation.** It consolidates the incremental backup deltas on a daily basis, consolidating intra-daily deltas into daily deltas, daily deltas into weekly deltas, weekly deltas into monthly deltas, and monthly deltas into a rolling delta. The base image, the last 35 days of daily deltas, plus all of the monthly deltas and the rolling delta must be retained until a new base image is taken.
2. **Image Verification.** The integrity of the data stored locally on the BDR is periodically verified. Any errors will be reported in the management Web Portal and through any configured email and partner notifications (as configured in the online backup manager and in the partner Web Portal).

First, follow these instructions to configure the ImageManager global settings:

1. Start the ImageManager (double click the icon on the desktop or start menu):



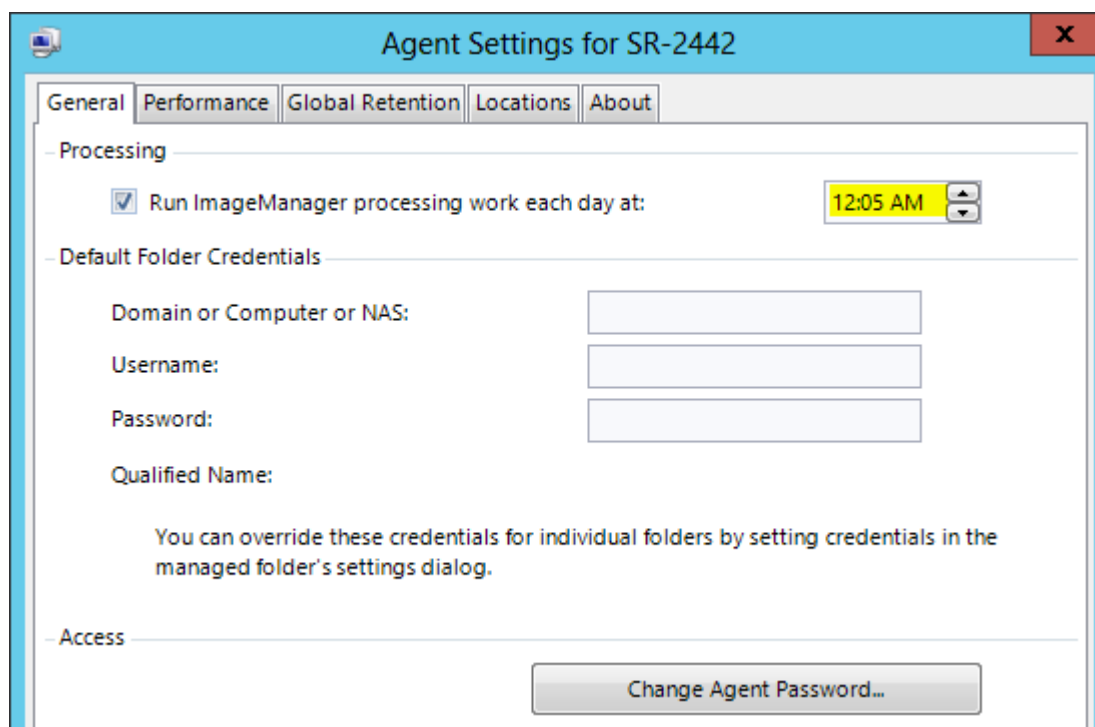
2. The ImageManager will ask you to login. The default password for the ImageManager is 'imagemanager' (without the quotes).



3. Choose a time when ImageManager should collapse the deltas. To do this, click the *Agent Settings* button on the left-hand side:

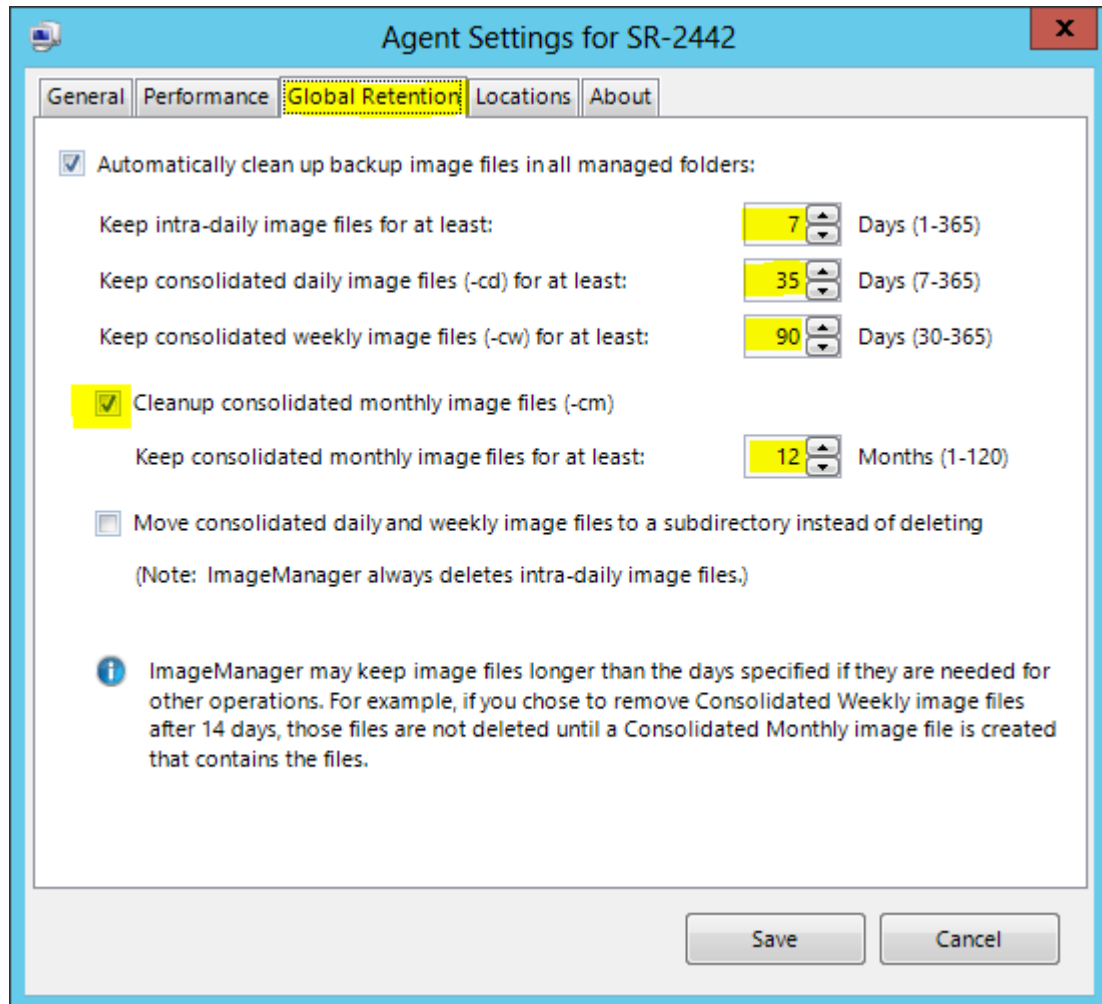


4. Then choose the time when processing should occur:



**Important Tip:** You should always choose a time after midnight (12:01am). If you choose an earlier time, your off-site backups will always be at least 24 hours behind. You should set the online backup manager to start its processing about one hour after the image manager performs its work (longer for really large sites). This will allow the ImageManager to complete its work before the off-site backups and replication start.

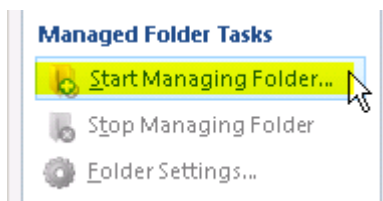
5. You can also configure your default data retention policy in the agent settings. The BDR comes pre-configured with a retention policy that is suitable for most customers. However, you can customize this to your needs:



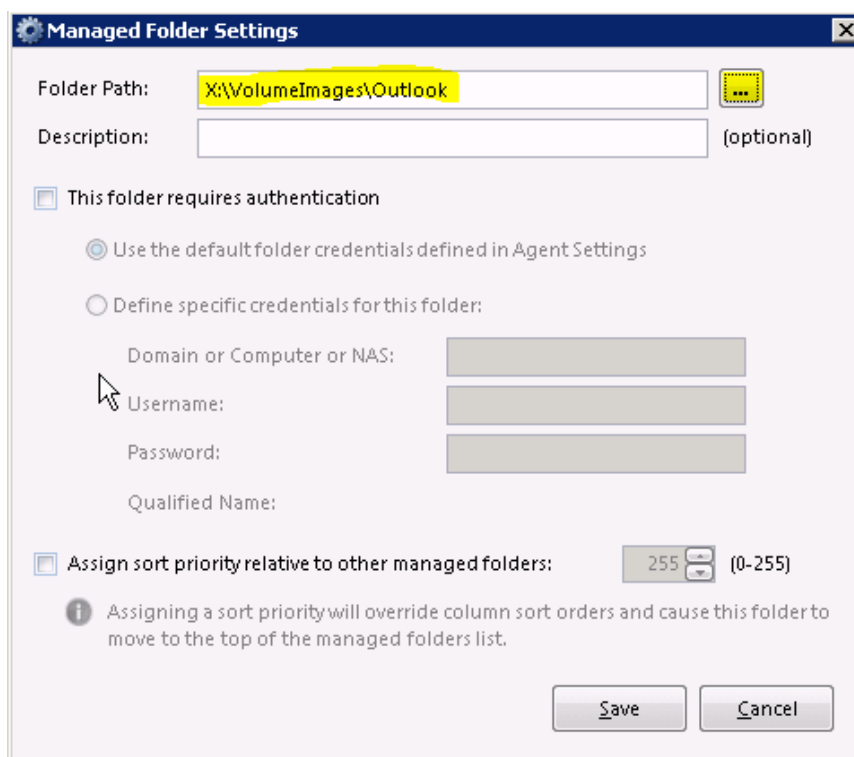
**EXTREMELY IMPORTANT:** If you are performing off-site backups, you must set the number of days to keep consolidated daily image files (-cd) to at least 35. You must keep at least 35 days of daily image files to maintain your chain. This is because weekly image files are not backed up offsite (only the base image, daily files, monthly files, and the rolling delta file).



6. Next, the ImageManager must be told about each directory that contains bare-metal backup image files. For each server or workstation that you are backing up, perform the following steps:
  - a) While still logged in to the ImageManager user interface, on the left hand side, click the
    - a. *Start Managing Folder* button:



- b) Click the ... button to browse for the folder that contains the bare-metal backup images. Typically, the folder you want to select will be a subdirectory of X:\VolumeImages or X:\LocalVolumeImages. Note that you should select a subdirectory of X:\VolumeImages (or X:\LocalVolumeImages), not X:\VolumeImages itself. You can leave the other options at their default settings.



**VERY IMPORTANT:** You must add the folder that directly contains the .spf and .spi files. (You cannot add just the parent directory). For example, if you have three servers backing up to the BDR, you will have three separate directories that contain the bare-metal backup image files, and you will use the Start Managing Folder button three times to add each of the three folders separately to the ImageManager.

- c) **Optionally, you may configure agent-specific retention policies.** If you need to override the global data retention policy for a specific agent, select the agent and then click **Retention Settings** on the left side.

This will bring up the retention settings dialog, where you can customize how long you want to retain each type of image file.

**EXTREMELY IMPORTANT:** If you are performing off-site backups, you must set the number of days to keep consolidated daily image files (-cd) to at least 35. You must keep at least 35 days of daily image files to maintain your chain. This is because weekly image files are not backed up offsite (only the base image, daily files, and monthly files).

Now that ImageManager has been configured to monitor and manage each folder for each protected agent, we can proceed to the next steps.

## Managing ShadowProtect Backups

The ShadowProtect management console on the BDR allows you to connect to and manage all of the ShadowProtect installations on your local network, without having to login separately to each computer. The *Management View* tab in the ShadowProtect console is what allows you to do this. In the Management View you can start managing one of the computers in the list by double clicking on the desired computer or clicking the *Manage* button. (You may also need to click the *Connect* button if it has not yet connected to that agent.)

Once you have selected a computer to manage, the other tabs will allow you to configure and control bare-metal backups on that computer.

For more detailed information, please refer to the ShadowProtect documentation on the BDR in the C:\Appliance\Documentation\StorageCraft directory.

## Bare-metal Restores

Bare-metal restores allow you to restore an entire computer without having to first reinstall the operating system, even to different hardware.

This page describes how to restore an entire system from bare-metal backups. If you just want to restore an individual file, follow [these other instructions](#).

To restore an entire system from bare-metal, follow these steps:

1. You will need to create the Recovery Environment CD or DVD following the instructions in this link: <https://www.storagecraft.com/support/book/storagecraft-recovery-environment-user-guide/starting-recovery-environment/creating-recovery-en>
2. Follow the on-screen instructions to restore the volume images from the BDR onto the bare-metal. You will need to tell it to connect to the network and map a network drive to the `VolumImages` (or `LocalVolumImages`) share on the BDR. This can be done after it boots from the recovery CD by going to the Tools menu and selecting the *Network Configuration Utility* command.

**IMPORTANT:** If you are restoring a domain controller, the first time the server boots, when the Windows boot menu appears, you should immediately press F8 and choose *Active Directory Restore Mode* or *Directory Services Restore Mode*. Once the server comes up, edit the settings for the network adapter to reset the static IP and the DNS server address. For SBS servers, the DNS server address will be the same as the static IP.

**Tip:** If you are restoring to dissimilar hardware, please see [StorageCraft KB article 72](#).

**Tip:** The trial version of ShadowProtect does not allow restoring to dissimilar hardware. If you need to test this functionality and do not have a ShadowProtect license key, please contact your sales representative.

**Tip:** You can configure the recovery environment to start a VNC server and then use the UltraVNC software on the BDR to remotely connect to the bare-metal recovery environment console (it is located in the C:\Appliance\Software\UltraVNC directory).

**IMPORTANT:** After the restore has completed successfully, you should take a new base image.

You should make sure to archive the old backups for the restored image to a location not in the original folder. This will provide you with a backup history of the system, prior to the restore

More detailed documentation, including a walkthrough with screenshots, is available by opening the ShadowProtect Recovery Environment.pdf file in the C:\Appliance\Documentation\StorageCraft directory on the BDR appliance.

## Restoring Individual Files

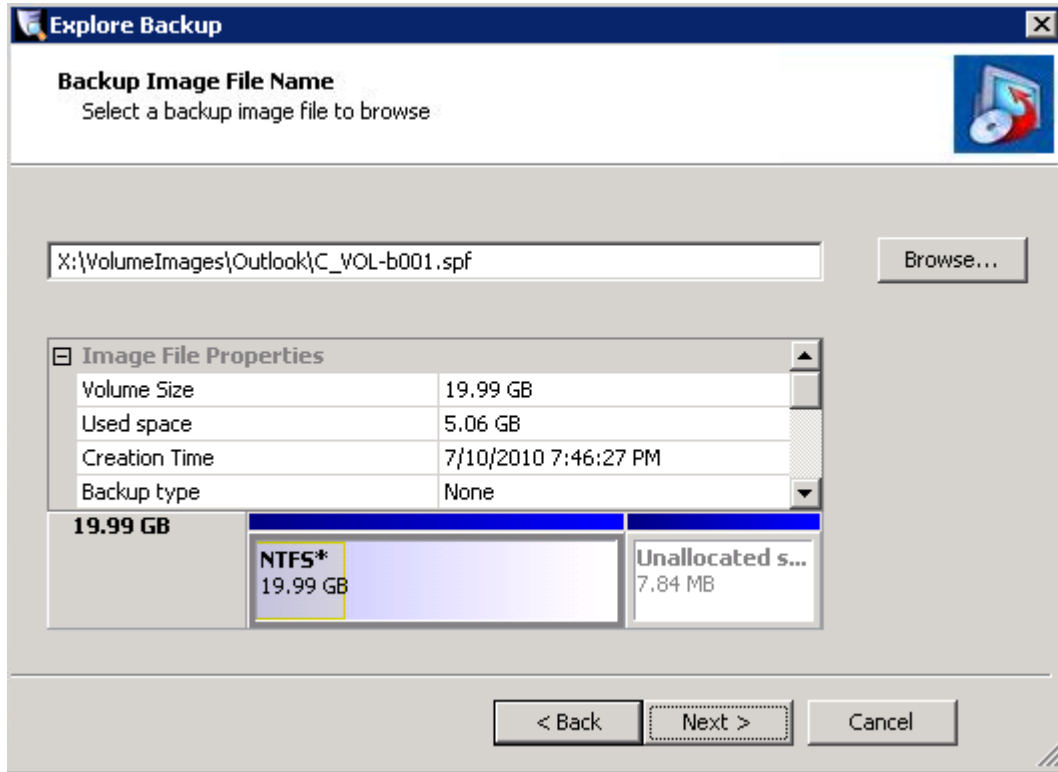
Even though bare-metal backups are backing up entire file system volumes, you are still able to restore individual files or directories easily. If you want to restore an entire system from bare-metal, follow these [other instructions](#) instead.

Follow these steps to restore one or more individual files:

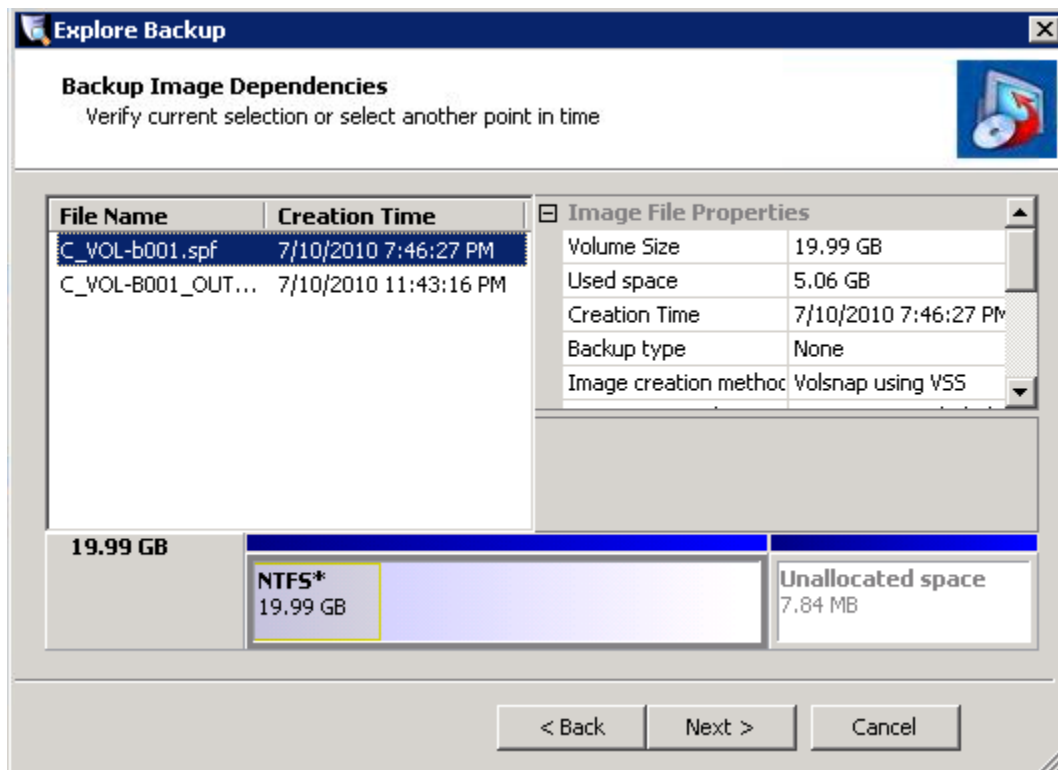
1. Start the ShadowProtect management console (either on the BDR, or if you installed the user interface on the computer itself then you could also do this on the computer).
2. In the Management View use the *Connect* and *Manage* buttons to connect to the appropriate computer.
3. In the pane on the left, click the *Explore Backup* command:



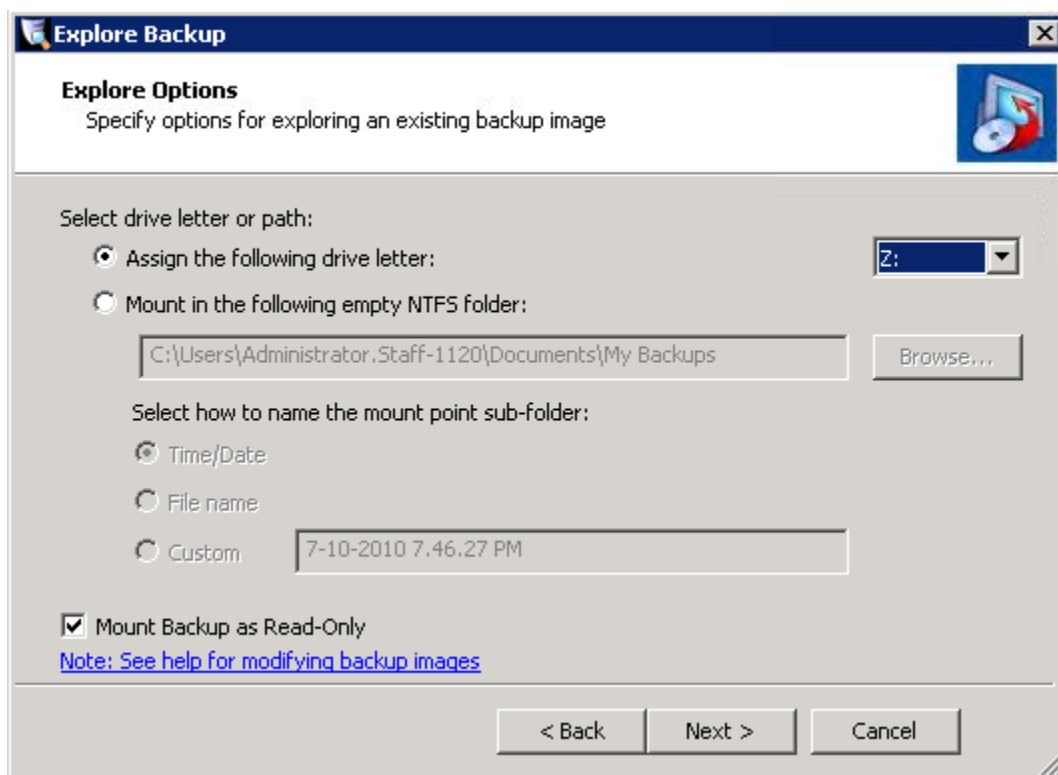
4. Follow the steps of the wizard to select the appropriate ShadowProtect image file (\*.spf) that contains the backup data for the volume that has the file you want to restore:



5. The next step of the wizard allow you to select the desired point in time:



- In the next step, tell it where to mount the backup image (for example, Z:\):



- Finish the wizard. Windows explorer will popup showing the data on the drive. Now copy the desired data to the desired location.
- When finished, in explorer right click the mounted drive (e.g., Z:\) and choose *Dismount*.

Alternatively, on the BDR you can also use Windows Explorer to browse to the .spf or .spi file that contains the data for the volume with the file you want to restore, right click it, and choose *Mount* and it will mount the backup image as the Z:\ -- you can then use Windows Explorer to copy the data to the desired location.

## Overview of Virtualization

This section describes how to quickly virtualize and run servers or desktops from bare-metal backup images stored on the BDR. Bare-metal backup images can be virtualized in just seconds through the VirtualBoot tool (does not require the data to be copied or converted, very fast).

Virtualizations on the BDR can be done in [test mode](#), where the virtualized server will not communicate with other computers on the network, or in [production mode](#), where it will be visible on the network.

Alternatively, you can use the [image conversion tool](#) to convert the bare-metal backup images into VMDK (VMware) or VHD (HyperV) virtual disk images, which can be booted within your existing infrastructure (e.g., if you are running VMware ESXi or HyperV on other servers in your network) after running the HIR tool on them.

This section also describes how to restore back to a physical (or virtual) server after you have virtualized a server on the BDR with VirtualBoot.

[An overview](#) of this feature is also available.

Additional details are also available in the ShadowProtect VirtualBoot documentation.

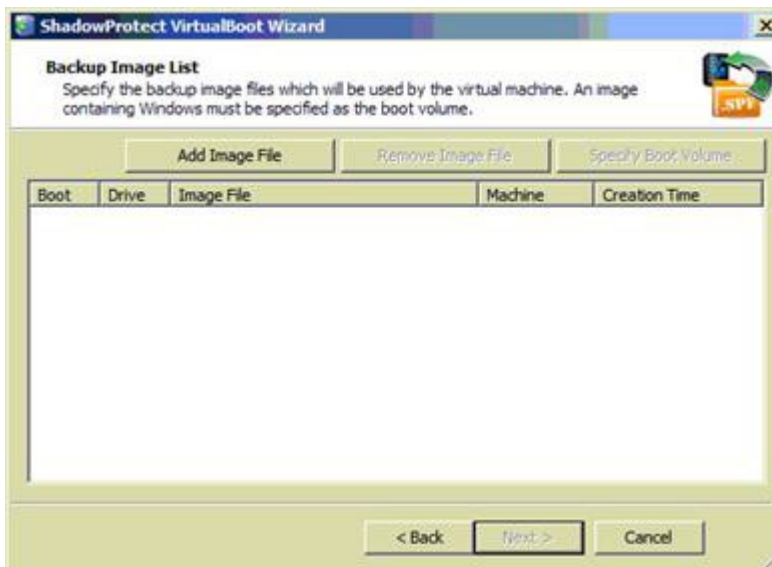
## Virtualizing in Test Mode

You can virtualize a backed up computer in a test environment by:

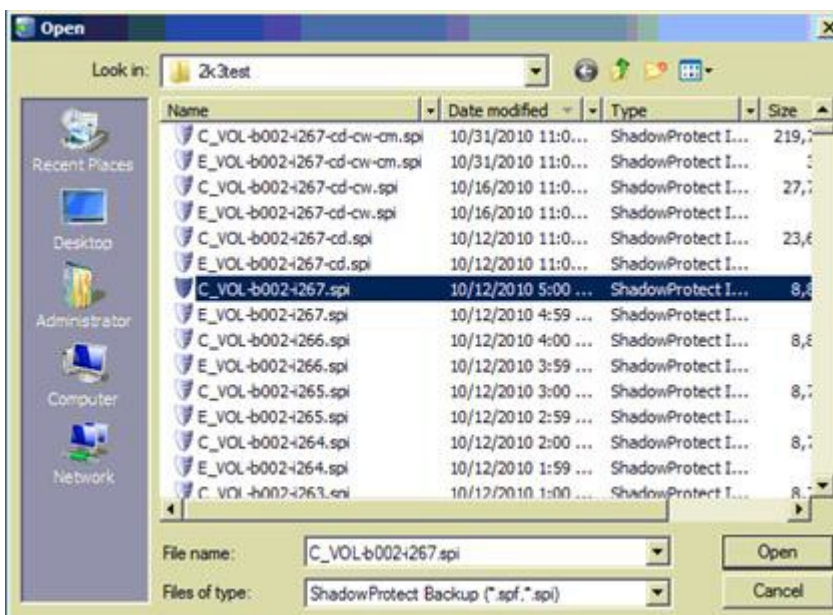
1. Start the *VirtualBoot* wizard on the BDR



2. Click Next



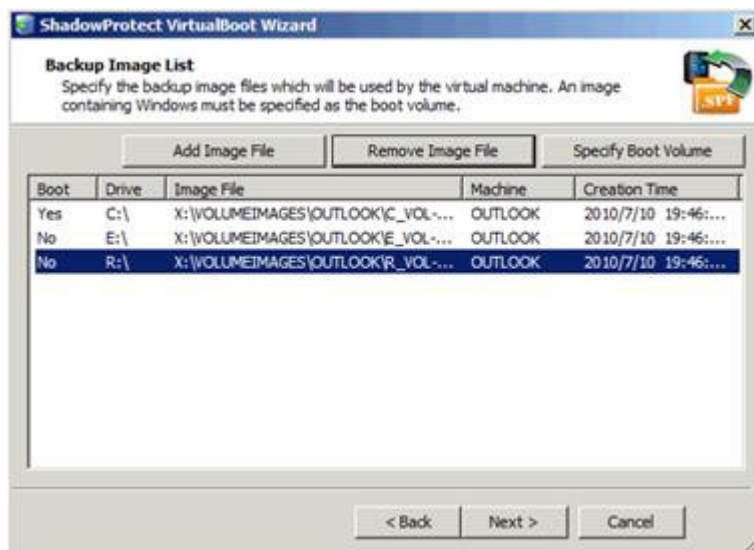
3. Click the *Add Image File* button. Select the .spf or .spi file containing the point-in-time backup for the computer you want to virtualize.



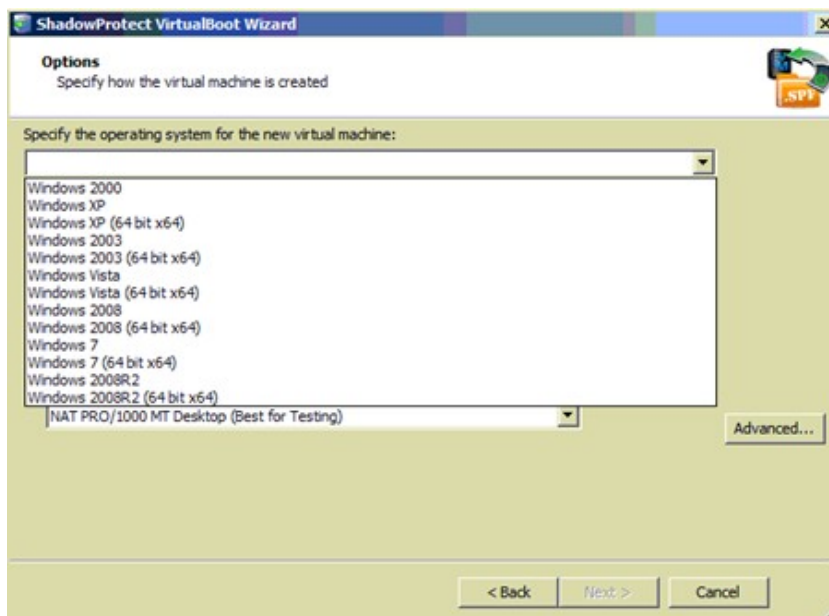
**Tip:** When selecting which backup image to virtualize, do not select a consolidated image file (a file whose name ends in -cd.spi, -cw.spi, or -cm.spi).

4. Once you have selected a backup image, it will automatically select the point-in-time backup image for any other volumes that depend upon the volume you selected. For example:



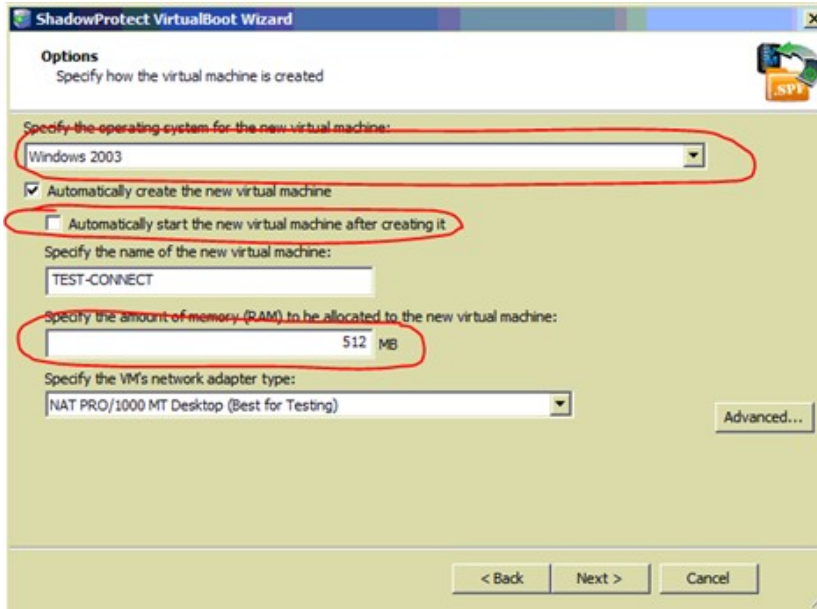


5. Check that the boot volume it selected is correct. If it isn't, use the *Specify Boot Volume* button to indicate which volume is the boot volume. Click *Next* when everything looks correct.
6. You will need to select the appropriate operating system version from the drop down menu. You must select the correct operating system version, or the virtual machine will not boot correctly.

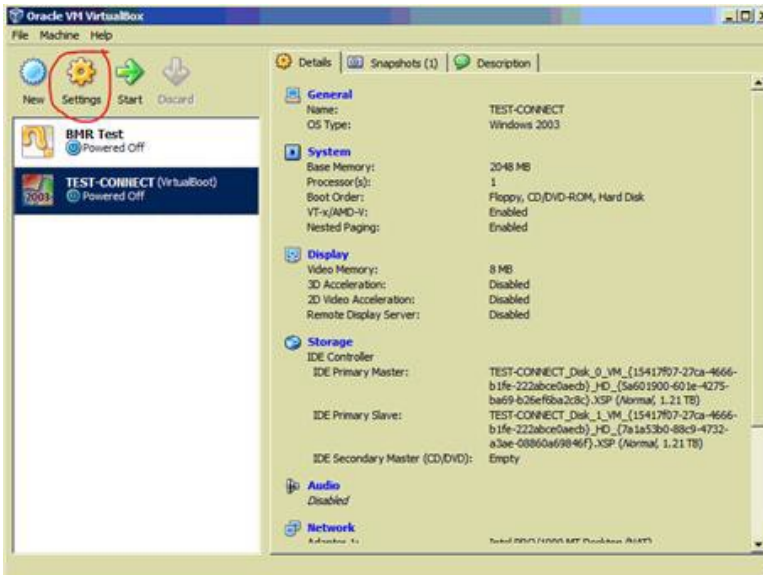


7. Choose *not* to start the virtual machine automatically (you will want to adjust networking settings before starting it). Choose the amount of RAM to dedicate to the virtual machine. You should leave at least 1GB free for the BDR itself to use (recommended leaving at least 2GB free -- e.g., if you have 8GB of RAM, we recommend using no more than 6GB).

**IMPORTANT:** SBS Servers require at least 6GB of RAM to function properly.



8. Click Next when finished, review that everything looks correct, and click the *Finish* button.
9. It will show a progress dialog while it prepares the virtual machine. Normally this process only takes about 60 seconds, but it may take up to several minutes under rare circumstances. Please be patient while it prepares the virtual machine.
10. Once it's finished, it will show a dialog box confirming the creation of the virtual machine.
11. Once the VirtualBoot wizard has finished, start *Oracle VirtualBox* on the BDR and edit the settings for the newly created virtual machine.



12. In the Network settings section, make sure Adapter 1 is enabled. Select the appropriate network type:

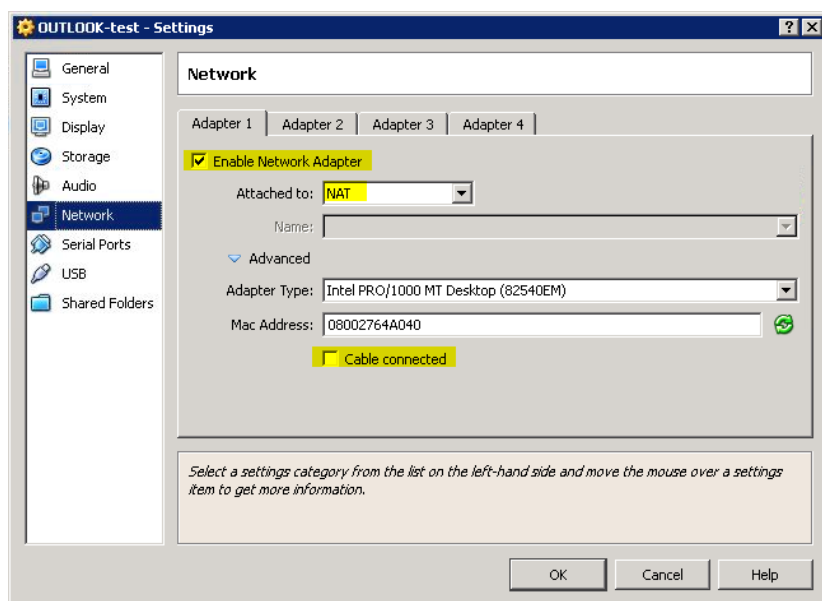
**Internal Network:** This puts the VM in a completely isolated, virtual network. It will not be able to communicate with the BDR or the networks that the BDR is attached to, but it will be able to communicate with other VMs running that are attached to the same internal network.

**IMPORTANT:** If you are virtualizing an SBS server or domain controller, the server must have a valid DNS server IP address, which requires a connected network adapter. You should therefore use the Internal Network and make sure that the virtual network adapter network cable stays connected. The first time you boot you also have to use the *Directory Services Recovery Mode* to assign an IP address and DNS server address (see below).

**Host-only Adapter:** This is similar to Internal Network, except that the host (BDR) can also be a participant of the network. Usually you do not need to use this option.

**NAT:** This puts the VM in a virtual network behind a virtual firewall that will perform NAT translation from the virtual network onto the primary physical network of the BDR. Use NAT if you want the test VM to have access to the Internet or if it needs a DHCP server and you do not want it present on the physical network attached to the BDR.

**IMPORTANT:** If the test VM doesn't need Internet access, you should expand the *Advanced* settings, and making sure that the *Cable connected* option is **unchecked**:



- When ready, use the VirtualBox interface to start the virtual machine.  
**Do not log out of windows while the virtual machine is running.**

**Tip:** You can disconnect from a remote desktop session and the virtual machine will continue to run. Just do not log out.

**IMPORTANT:** If you are virtualizing an SBS server or domain controller, the first time the server boots (when the Windows boot menu appears), immediately press F8 and choose *Active Directory Restore Mode* or *Directory Services Restore Mode*. Once the server comes up, login as the local Administrator (.\Administrator) using the Directory Services Restore Mode password, then edit the settings for the network adapter to reset the static IP and the DNS server address. For SBS servers, the DNS server address will be the same as the static IP (or 127.0.0.1).

14. When you are finished testing, stop the virtual machine, and follow the directions to [delete the virtual machine](#).

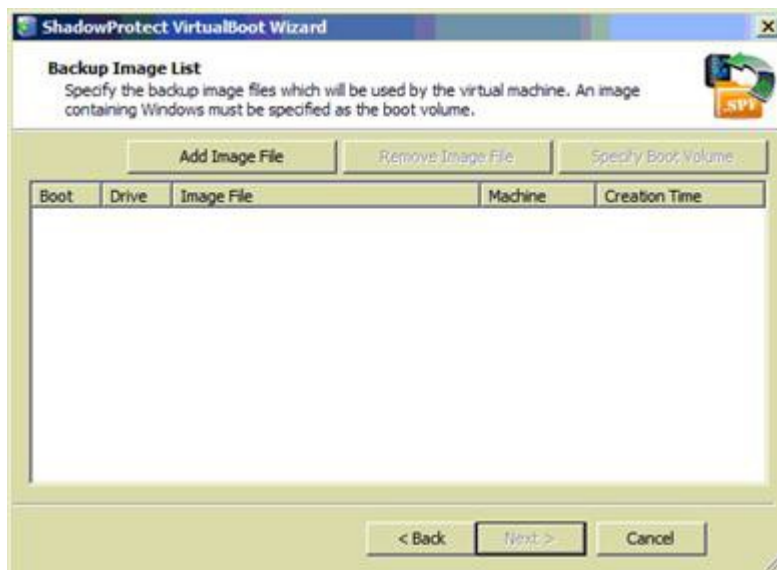
## Virtualizing in Production Mode

If you have experienced a computer failure and need to virtualize the server or desktop on the BDR, follow these steps:

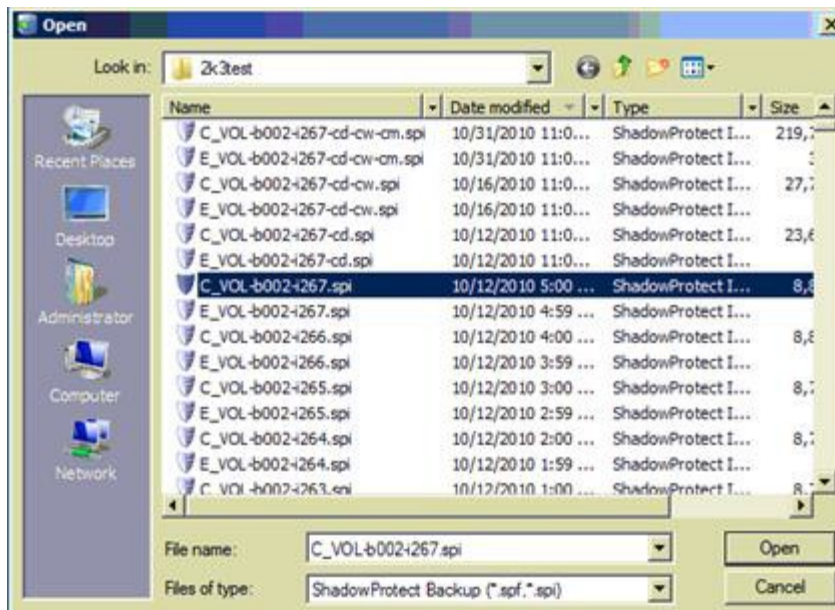
1. Start the *VirtualBoot* wizard on the BDR



2. Click Next

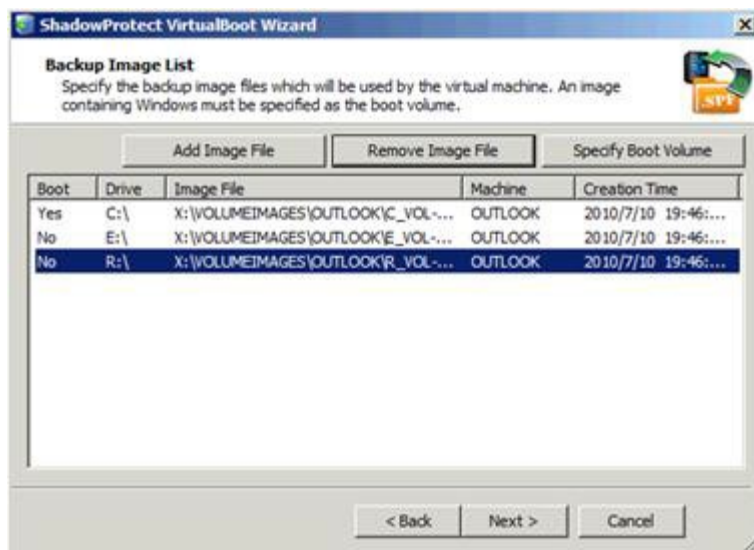


- Click the *Add Image File* button. Select the .spf or .spi file containing the point-in-time backup for the computer you want to virtualize.



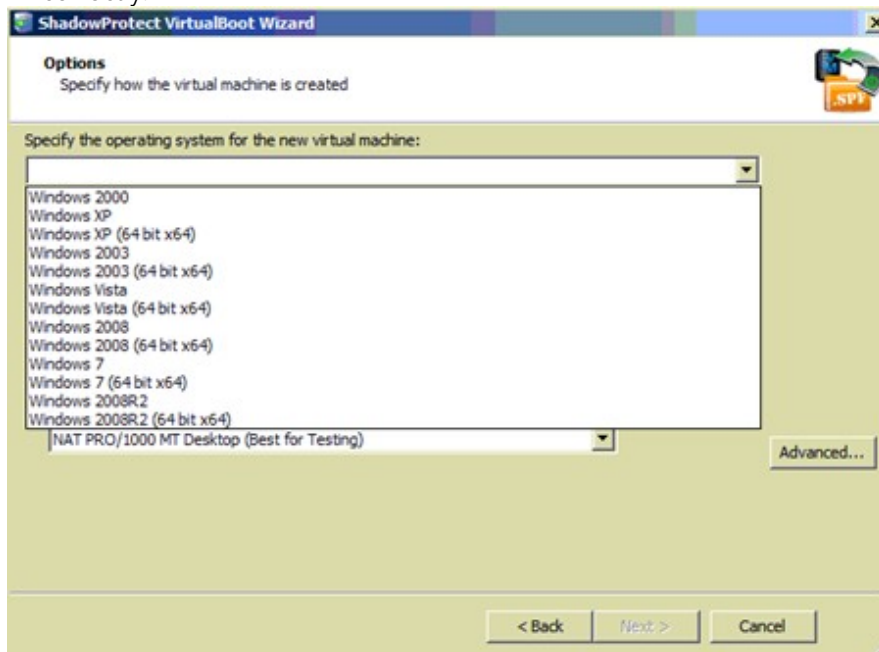
**Tip:** When selecting which backup image to virtualize, do **not** select a consolidated image file. (Do not choose a file whose name ends in -cd.spi, -cw.spi, or -cm.spi).

- Once you have selected a backup image, it will automatically select the point-in-time backup image for any other volumes that depend upon the volume you selected. For example:



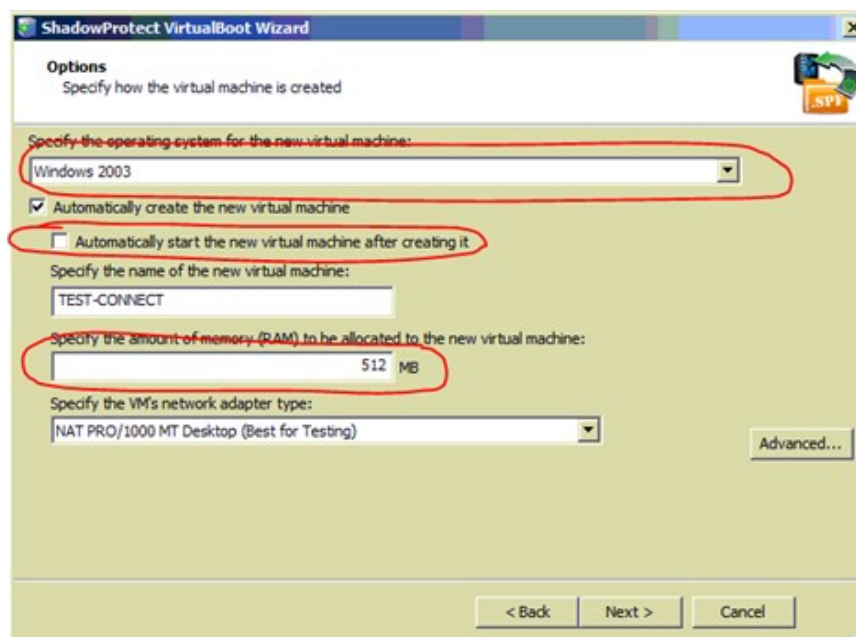
- Check that the boot volume it selected is correct. If isn't, use the *Specify Boot Volume* button to indicate which volume is the boot volume. Click *Next* when everything looks correct.

6. Select the appropriate operating system version from the drop down menu. You must select the correct operating system version, or the virtual machine will not boot correctly.



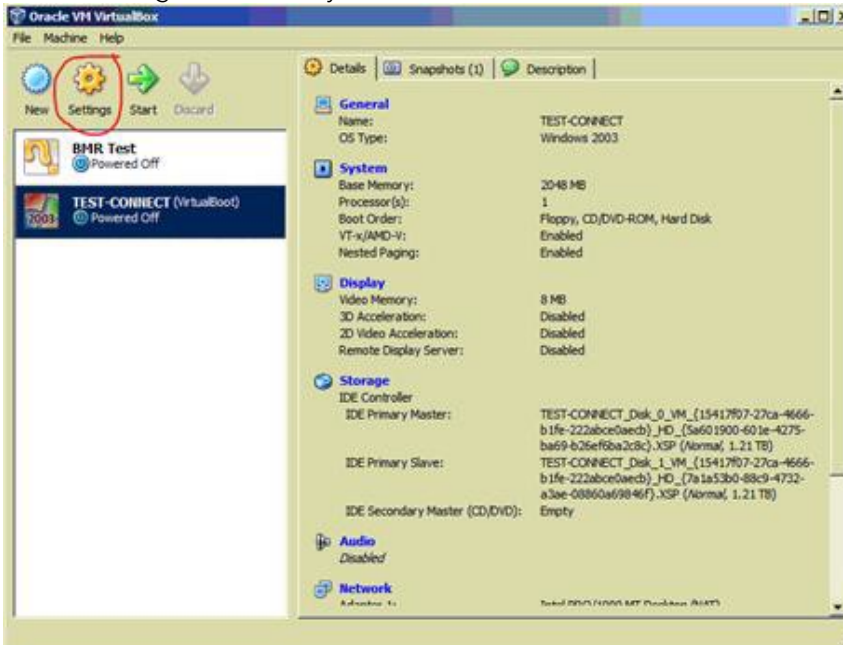
7. Choose **not** to start the virtual machine automatically. (You will want to adjust networking settings before starting it). Choose the amount of RAM to dedicate to the virtual machine. Leave at least 1GB free for the BDR itself to use (We recommend leaving at least 2GB free. For example, if you have 8GB of RAM, we recommend using no more than 6GB).

**IMPORTANT:** SBS Servers require at least 6GB of RAM to function properly.

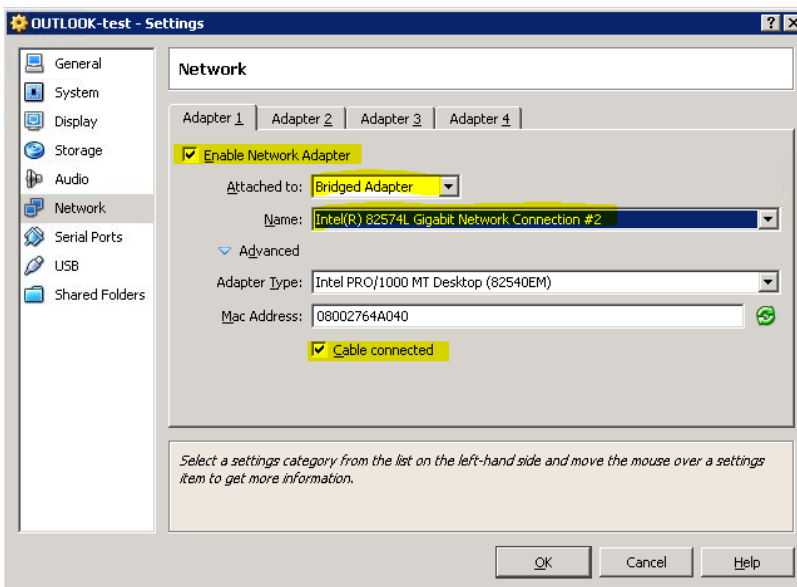


8. Click **Next** when finished, review that everything looks correct, and click the *Finish* button.

9. It will show a progress dialog while it prepares the virtual machine. Normally this process only takes about 60 seconds, but it may take up to several minutes under rare circumstances. Please be patient while it prepares the virtual machine.
10. Once it's finished, it will show a dialog box confirming the creation of the virtual machine.
11. Once the VirtualBoot wizard has finished, start *Oracle VirtualBox* on the BDR and edit the settings for the newly created virtual machine.



12. In the Network settings section, make sure Adapter 1 is enabled. Then attach to the *Bridged Adapter*, choose the appropriate physical adapter to bridge to, expand the *Advanced* settings, and make sure that the *Cable connected* option is **checked**.



**IMPORTANT:** If you are virtualizing Windows 2000, expand the Advanced network settings, and change the Adapter Type to be PCnet-FAST III.

- When ready, use the VirtualBox interface to start the virtual machine. Do not log out of windows while the virtual machine is running.

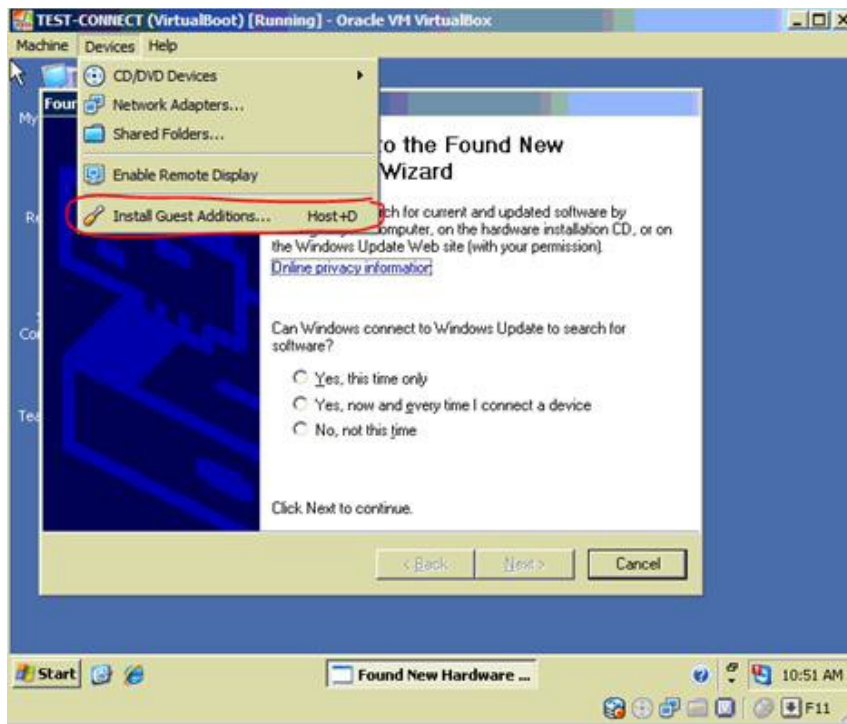
**IMPORTANT:** You can disconnect from a remote desktop session and the virtual machine will continue to run. Just do not log out.

**IMPORTANT:** If you are virtualizing an SBS server or domain controller, the first time the server boots, when the Windows boot menu appears, you should immediately press F8 and choose *Active Directory Restore Mode* or *Directory Services Restore Mode*. Once the server comes up, login as the local Administrator (.\Administrator) using the Directory Services Restore Mode password, then edit the settings for the network adapter to reset the static IP and the DNS server address. For SBS servers, the DNS server address will be the same as the static IP (or 127.0.0.1).

- Once the virtual machine boots in production mode, you may have to reactivate Windows. There is no way to circumvent windows activation restrictions. If you have to reactivate Windows, it will attempt to do it online, or it may have you call Microsoft.

**Tip:** Typically computers do not have to be activated if you are booting an image that was backed up within the last 3 days, or if you are using volume-based licensing.

- It is recommended that you install the Guest additions inside of the virtual machine once it has booted into Windows. Doing this can boost performance. To do this, once the VM is running, click the Devices menu in the VirtualBox window, choose *Install Guest Additions*, and follow the instructions. (If setup does not start, browse to the setup executable on the CDROM drive in the VM).



**VERY IMPORTANT:** To continue incremental backups, open the ShadowProtect management console on the BDR, connect to the server, and make sure ShadowProtect backups are enabled.



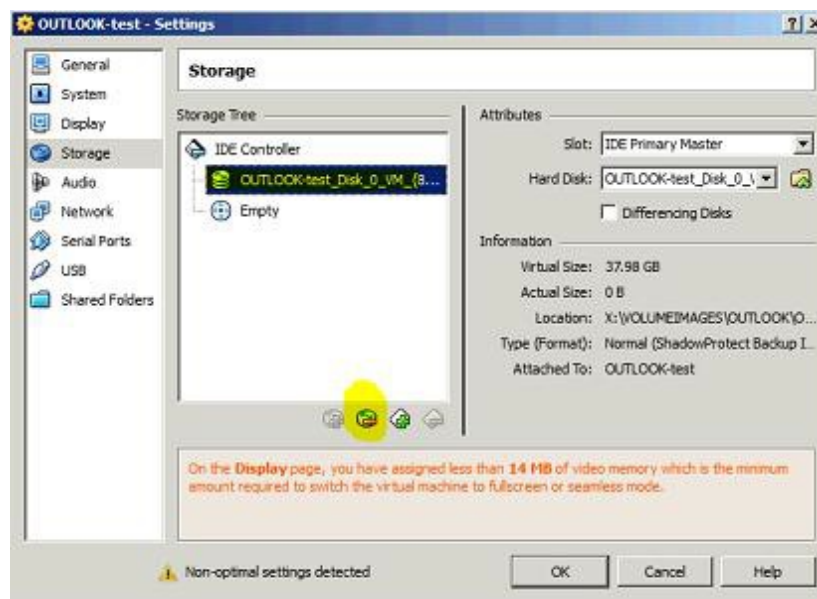
**NOTE:** ImageManager will be unable to remove collapsed incremental files and will throw an error. This is meant to be a short term solution, until such time that a full restore can happen.

16. When you are ready to restore back to the original server, you will take a final backup inside the virtual machine, shut down the virtual machine, and use the bare-metal restore process to complete the restore. You will probably have to take a new base image once the machine has been restored back to bare-metal. See [these instructions](#) for more details.

### Deleting a Virtualized Server

Once you have finished using a server or desktop you have virtualized on the BDR, delete the VM and cleanup any related files. Follow these steps to do this:

1. Right click on the Virtual Machine and click remove, it will ask you if you wish to remove ALL files or just the VM itself.
2. Select Remove All Files



Congratulations, you made it through the process! All files should be cleaned up now.

## Restoring After Virtualization

To restore a server or desktop after you have virtualize it, follow these instructions:

1. **Perform one last incremental backup.** Make sure that the VM has completed a recent ShadowProtect backup to the BDR. To do this, open the ShadowProtect management console, connect to the server like normal, and check on the backup job. We recommend kicking off one last incremental backup (it should be quite fast).
2. **Shut down the VM.** Once you gotten your one last incremental backup, immediately shut down the VM.
3. **Perform the bare-metal restore.** Follow the [bare-metal restore instructions](#) to restore the latest backup image back to a physical server or the new production virtual machine.
4. **Check on backup status.** After finishing the bare-metal restore, ShadowProtect may decide to take a new full backup. Check if there are any new base images on the BDR after it completes the first backup after the bare-metal restore.

If ShadowProtect did decide to take a new full backup, we recommend creating a new directory on the BDR and starting over with this new empty directory (just like you were configuring a new server).

5. **Delete the VM on the BDR.** Once the server is back in production and stable, follow the directions to [delete the virtualized server on the BDR](#).

Please contact technical support with any questions.

## Converting to Virtual Hard Disks

The ShadowProtect Management Console can be used to convert a bare-metal backup image to VMware VMDK or Hyper-V VHD virtual hard disk files, which can then easily be turned into a runnable virtual machine.

The process involves the following steps:

1. Using the Image Conversion tool inside the ShadowProtect Management Console to convert one or more backup images to VMDK or VHD files.
2. Moving the VMDK/VHD files to the hypervisor server that will host the new VM(s).
3. Creating the virtual machine in your hypervisor.
4. Mounting the bare-metal recovery CD .iso file inside the VM and booting from the virtual CD to perform "HIR" (the .iso is located on the appliance in C:\Appliance\Software\ShadowProtect).

Detailed documentation of this process is available [here](#).

## Overview of Off-site Backups

This section gives an overview of the procedures to perform off-site backups. Note that even if you do not want to upload your data off-site, you should still configure the online backup manager using these instructions, so that the Web Portal will provide monitoring of the local backups and also of the BDR.

More detailed instructions are available in the online help for the backup manager (start the backup manager, and choose *Help menu, Contents*). See also the [overview of this feature](#).

### Configuration of Off-site Backups and Monitoring Software Branding

If you are a reseller and wish to change the branding of the online backup software, please install your custom brand and then use the brand conversion wizard located in the C:\Appliance\Software directory. Running the wizard is very important because it converts many of the backup policies that come preconfigured for the BDR.

## Account Configuration

All BDR services (monitoring, notifications, licensing) require that the appliance be connected to an online backup account. To configure the account, follow these steps:

1. Open the desktop, click the *Online Backup* icon to start the backup manager.
2. On the *My Account* page, enter your online backup credentials and click the *Test Connection* button. If you have a temporary password, it will help you change it to a permanent password.

**Tip:** Your password is not your pass phrase. The password of an account can be changed or reset; however, **the pass phrase cannot be changed once it is configured.**

3. Click the *Create Pass Phrase* button and follow the prompts to setup your pass phrase.
4. If you do not plan to send data off-site, go to the *Folders* page in the backup manager, and uncheck the online backup destination column (earth icon) for the Volumelimages folder. Note that by default the LocalVolumelimages folder will be monitored but not backed up offsite, and you should leave this folder checked.

**Tip:** The backup manager is preconfigured to backup all data in the X:\Volumelimages folder, and is configured with a special policy to properly backup ShadowProtect data. If you add additional folders to the backup that contain ShadowProtect data, make sure that you set it to use the same backup policy. This is also true for data that you do not want to backup offsite but that you do want to monitor.

5. On the *Schedule* page, set the frequency to daily (once per day) and choose a time. We recommend choosing a time that is one hour after the time you chose for the collapsing of incrementals, with ImageManager.
6. On the *Options* page, *Bandwidth* tab, optionally adjust bandwidth constraints as desired.

Note that if you want to receive email notifications for just this account, you should typically leave the *Email Address* setting on the Options page set to *(auto)* and instead change the email address for your account in the Web Portal.

**Tip:** If you are a reseller and want to setup standard notification rules, we recommend using the *Partner Notifications* feature of the reseller Web Portal instead of setting up individual notifications for accounts. Or if your end-users want to be notified, configure the backup manager with the end-user's email address, and rely on the *Partner Notifications* feature in the Web Portal for your own notifications.

**Tip:** The BDR service plan only allows bare-metal backups to be backed up off-site. If you wish to backup other kinds of file-level data that is on the BDR, you will need to create an additional settings profile and configure an additional online backup account (Basic or Select). In summary, to create an additional settings profile, in the backup manager, do *File* menu, *Switch Profile*, and click the plus (+) button to add a new profile. Refer to the backup manager documentation, partner training, and technical support for additional information.

## Initial Backup

You can choose to perform the initial backup over the network or via a [preload \(seed\) drive](#). How long an initial backup will take over the network depends on the speed of the network connection and the amount of data to upload. You can estimate how much data needs to be uploaded by clicking the *Visualize* button on the Folders page, and looking at the line of text in the bottom left of the window that starts with *Amount to backup in all folders*.

**Tip:** During the initial backup make sure that automatic installs of windows security updates are disabled, so that the BDR does not reboot in the middle of uploading a large file.

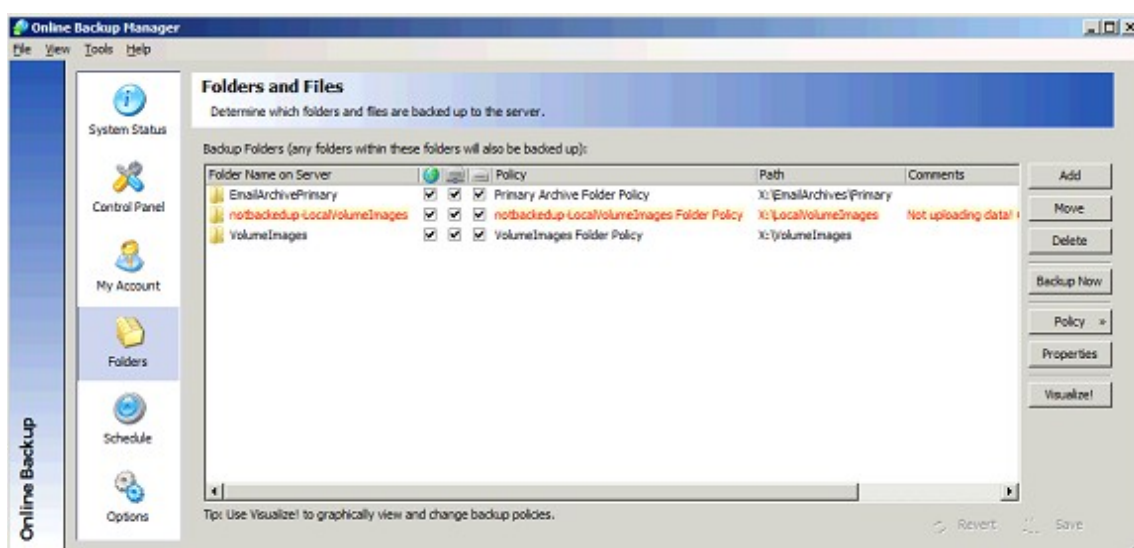
## Configuring Backups of Bare-metal Images

The appliance comes preconfigured to backup all bare-metal backup images stored in subdirectories underneath the X:\VolumelImages directory. The appliance is also preconfigured to monitor (but not backup) bare-metal backup images in the X:\LocalVolumelImages directory.

The bare-metal images for each server or desktop that you want to backup off-site should be stored in separate subdirectories of X:\VolumelImages (one subdirectory for each computer being backed up), or X:\LocalVolumelImages if you just want to monitor the local backups.

**VERY IMPORTANT:** The VolumelImages and LocalVolumelImages folders are configured with a special policy to properly monitor and backup the ShadowProtect bare-metal images. You must store all ShadowProtect data that you want to backup in a sub-directory of VolumelImages or LocalVolumelImages. Otherwise the data may not be properly backed up and preserve a full chain of incrementals. If you do add an additional folder to the backup set that contains ShadowProtect data, be sure to set it to use the *Backup ShadowProtect Images* policy, to ensure that the proper data is backed up and monitored.

If you do **not** want to back up the bare-metal images for a particular server or desktop, store the bare-metal backup images in a subdirectory of X:\LocalVolumelImages. This directory is still monitored for backup frequency and integrity but the data itself will not be backed up offsite.



## Preload (Seed) Drive for Off-site Backup - Overview:

Preload (seed) drives are useful when the total amount of data to backup is too large to quickly backup over the network. **We recommend using a preload (seed) drive any time you are backing up more than 100GB of data on a standard Internet connection.**

eFolder offers a round-trip preloading (seeding) service, which includes everything required for you to properly preload (seed) your account. The hard drives are 4TB and can be interfaced via USB 2.0/3.0 or SATA.

- The initial backup is sent via a preload (seed) hard disk. Once the data from the preload is implemented, only the incremental changes (which are much smaller) need to be sent over the network.
- Preloads can be performed on a new or existing account.
- When a preload is performed on an existing account, all previous data for that account will be replaced with the contents of the new preload.
- We recommend that you allow backups to run locally for at least a few days before performing a preload. This will allow you to determine if there are change rate issues that need to be diagnosed before you send the data off-site.

**IMPORTANT:** When creating a preload (seed) drive, the desired account must first be put into Maintenance Mode from the eFolder [Web Portal](#). When an account is in Maintenance Mode, online backups are not allowed to proceed. This is important, because until eFolder receives the disk and loads the data onto your storage server, **that account should not try to upload incremental changes to your data.** The account must remain in maintenance mode until the preload has been processed, at which point the maintenance flag will be removed by eFolder.

**IMPORTANT:** Do not take the account out of maintenance mode. This will be performed by one of our technicians when the preload has been fully processed. Incremental backups will *not* be sent to the off-site data center until the preload has been processed.

Once the preload has been processed, we will take the account out of maintenance mode and send you an email. If you have already scheduled off-site backups using the backup manager, incremental backups will automatically begin during the next scheduled time when the backup is to begin. The first incremental backup after the preload will take more time than normal, as it has to upload a few days' worth of data instead of the incrementals for just one day.

### How to request and create a ShadowProtect preload (seed) drive

The below instructions are intended for resellers. If you are an end-user, please coordinate the preload operation with your reseller.

[How to request a preload \(seed\) drive](#)

[How to create a ShadowProtect preload \(seed\) drive](#)

## Restoring Data from Off-site Backups Overview

Usually you will want to restore data using the bare-metal backup images stored on the BDR appliance itself. Restoring data from off-site backups is applicable when the local backup data is unavailable. Example scenarios would include: (1) the local data has experienced silent data corruption, (2) there was a disaster and the local data was lost or destroyed, (3) the data is being restored after a RAID failure on the BDR device, or (4) the data is being restored to a cloud server (such as a Terremark vCloud windows node).

Restoring data from off-site backups is performed using the **File Manager** tool, which can be started from the **Control Panel** page in the backup manager.

In summary: You will login, select the data you want to restore, indicate where to restore it to and choose the point in time. **Note:** There are important additional steps if you are restoring the data back to a BDR appliance after a BDR appliance has experienced a RAID failure.

### Restore Instructions

1. Start the online backup **File Manager** tool.
2. Login with your account credentials.
3. Choose to **Restore** using the button.
4. Select the data you want to restore by checking off one or more folders or files. If you want to restore only a single file, right click that file and choose **Versions...** to see a dialog where you can browse for restored individual versions of that file.
5. On the next page in the wizard, indicate where the data should be restored to, and which point in time to use. (This is usually the current point in time.)
6. Click **Next** to download the list of file versions about to be restored. Once the download is finished, a report summarizing what it is about to do will appear.
7. If the report looks correct, choose to proceed and it will start restoring data. If you are restoring data on a computer other than the BDR, it will ask you for the encryption pass phrase at this point.

### Additional Instructions If Restoring After a RAID Failure

There are a few additional steps if you are restoring data back to the BDR because the RAID volume on the BDR has failed, *and* you intend to continue off-site backups from the machine you are restoring the data to. This includes any circumstance where the X:\ has failed or the online backup program files directory has been lost or destroyed.

In this case, first perform the restore as you did before, but then also download the configuration settings profile (@@SoftwareSettings folder), and import the configuration into the backup manager.

**IMPORTANT:** Do not reschedule backups until you have finished the steps below.

Finally, start the file manager, choose to restore all of the data, as you did before, but this time on the **Options** page, **check** the **Rebuild incremental backup cache (advanced)** option. Proceed through the rest of the wizard. You will not actually restore the data this time, but will only rebuild the incremental backup cache.

See the *Restoring after a System Crash* article in the backup manager documentation for even more detailed instructions.



## Overview of Cross-site Backups

This section summarizes how to configure cross-site backups between a pair of BDRs or between a BDR and a Windows computer running the local backup server software. A [feature overview](#) is also available.

## Configuration of Cross-site Backups

On the BDR that will be *receiving* the data, follow these steps:

1. Open the online backup manager. Go to **Tools** menu, **Local Backup Server**. This will open the Local Backup Server manager.
2. On the **Configure** page, enter the credentials assigned to that BDR. Click **Save**.
3. On the **Server Status** page, verify that the service is now running.
4. Configure your firewall to route TCP traffic on port 5470 from an external IP to the internal IP of the BDR receiving the data.

On the BDR that will be sending the data, follow these steps:

1. Open the online backup manager.
2. On the **My Account** page, in the **Local Server** field, enter the network hostname or IP address that is routing TCP traffic (port 5470) to the BDR receiving the data. **Save** changes.
3. On the **Schedule** page, **Local Server** tab, set the desired schedule. (We recommend starting one hour after ImageManager performs its processing).
4. If you do *not* want to perform off-site backups in addition to cross-site backups to the other BDR, then on the **Folders** page, uncheck the checkboxes in the column with the earth icon. Then go to the **Schedule** page, **Remote** tab, and set the Schedule to **manual**.

If you have questions or need assistance, please contact Technical Support.

## Overview of Cross-site Replication

This section summarizes how to configure cross-site replication between a pair of BDRs or between a BDR and a Windows computer running the network backup server software.

To configure replication, follow these steps:

- [Configure the replication target](#) to receive replicated data.
- [Configure each replication source](#). (There may be more than one.)
- For each replication source, [configure the ImageManager on the replication target](#).
- [Configure data monitoring on the replication target](#). (This can also be used to backup data on the replication target to the cloud)

If there is a large amount of data to replicate, then you may also want to do a [preload for replicated data](#).

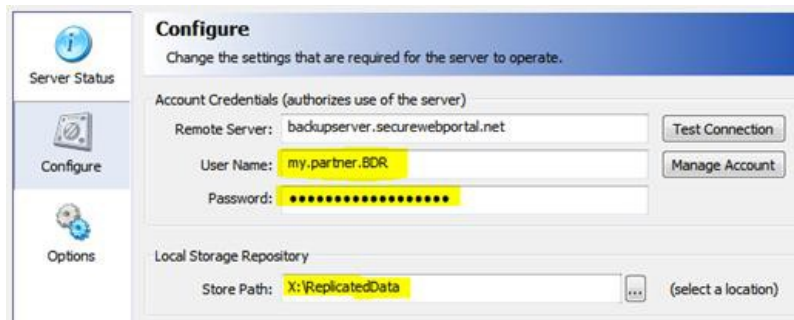
Once data has been replicated to the target BDR, you can follow the normal processes to virtualize the server on the target BDR. You can also [restore data from the replication target](#).

## Replication Target Configuration

First, make sure that the online backup manager is at least version 3.8.5 (Use the **Software Updates** tab on the **System Status** page in the backup manager to check).

On the Windows computer that will act as the replication target, install the backup client software. Once installed, start the backup manager, and from the **Tools** menu, run the network backup server (or local backup server) command.

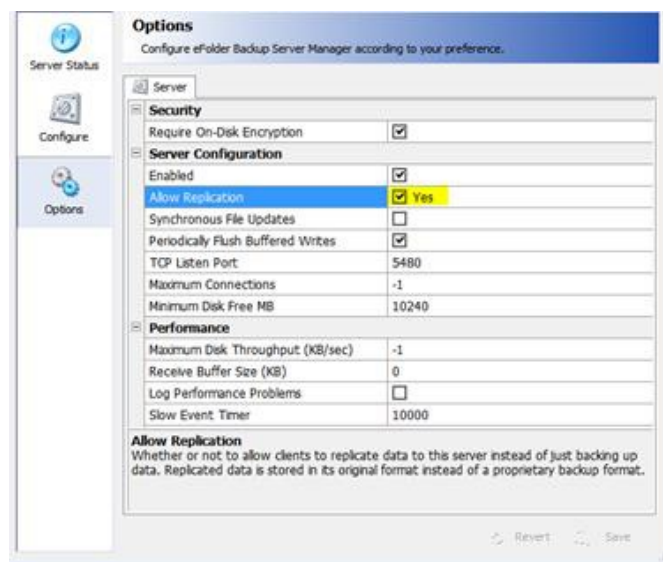
On the **Configure** page, choose where the replicated data should be stored, and also enter in your credentials for an appropriate online backup account:



**IMPORTANT:** If the replication target is a BDR, then you should use the account credentials you received specifically for that BDR unit (and not the credentials for one of the replication source computers). If the replication target is not a BDR, create a new account in the Web Portal.

**IMPORTANT:** The account used for the network backup server must belong to the same end-user customer (in our Web Portal) as the accounts for all of the replication sources. If you are doing many-to-one replication for multiple end-user customers, please contact your account representative to ensure that many-to-one replication has been enabled for your account.

In the Options page in the network backup server manager, make sure that the Allow Replication setting is set to Yes:



Finally, configure your network (routers/firewalls) so that any clients that will send the server data will be able to do so over a TCP/IP network on port 5470.

## Replication Source Configuration

On the BDR that will act as the replication source, start the online backup manager. Follow the instructions to [configure the online backup account](#) (In this case, it will only be used for authentication and monitoring). Go to the **My Account** page. Enter in the account credentials assigned to that computer. (These should be different than the account credentials you used on the replication target). In the **Network Server** (or **Local Server**) field, enter in the IP address or network hostname of the Network Backup Server:

Destination for Data

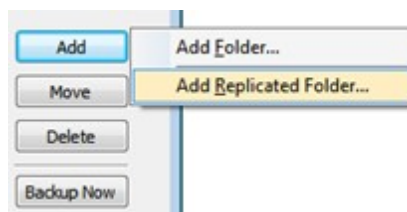
Remote Server: backupserver.securewebportal.net

Local Server: 192.168.50.120

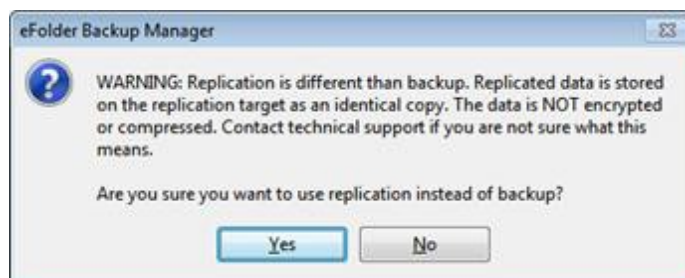
Local Disk: [...]

Test Connection

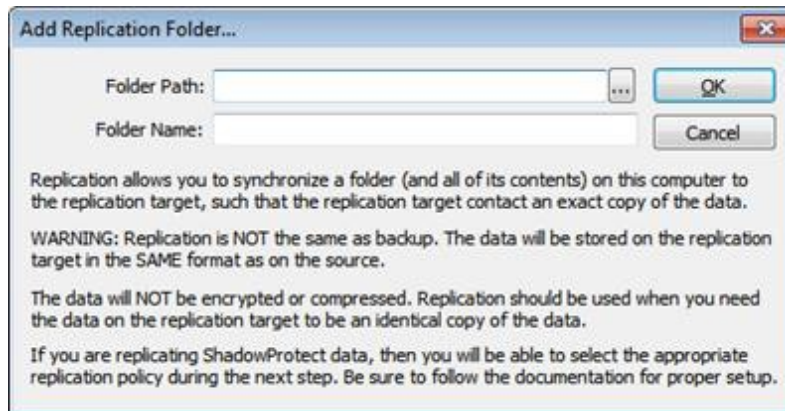
Next, go to the folders page, click the **Add** button, and choose **Add Replicated Folder**:



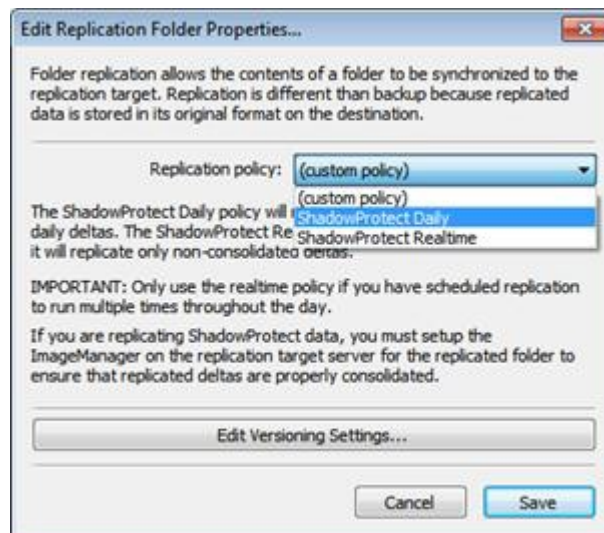
The program will warn you of the differences between replication and backup. If you are sure that you want to use replication instead of backup, then click **Yes** to proceed.



Next, select the folder that should be replicated (for example, X:\VolumeImages).



Finally, choose a replication policy:



Replication policy affects which files will be replicated to the target. Your choices are:

- **ShadowProtect Daily:** This will replicate ShadowProtect base image files (\*.spf files) and ShadowProtect daily image files (\*-cd.spi). It will not replicate weekly (\*-cw.spi) or monthly (\*-cm.spi) image files. (Weekly and monthly files will be created by the consolidation process on the replication target).
- **ShadowProtect Realtime:** This will replicate ShadowProtect base image files (\*.spf files) and any non-consolidated image files (such as hourly image files). This option requires more bandwidth, as all changes recorded by ShadowProtect throughout the day will be uploaded. If you choose this policy, we highly recommend setting the schedule (see below) so that replication is performed multiple times per day.
- **(custom policy):** Choose this if you are not replicating ShadowProtect data. By default it will replicate everything.

**IMPORTANT:** If you are configuring replication on a source computer that has already been consolidating the ShadowProtect backup chain for a while, it is possible that some of the daily image files (\*-cd.spi) will have already been consolidated. **If this is the case, you will need to temporarily add an 'include \*-cm.spi' policy rule to the bottom of your replication policy.**

Once the initial replication has completed, you can then remove this policy rule. This extra step is normally not needed, but it becomes necessary if the source computer has been consolidating the backup chain for long enough for some of the daily image files to be deleted.

**EXTREMELY IMPORTANT:** If you are replicating ShadowProtect data, you must configure the ImageManager on **both** the replication source **and** the replication target to consolidate the backup images. If you do not, your backups will not be verified, you will run out of disk space, and your backups may eventually have a backup chain that is too long to be usable. **Setting up the ImageManager is not optional and must be configured to ensure proper data protection.**

Note that the ImageManager must be configured to individually add each folder that contains ShadowProtect data. It is not sufficient to add the parent directory: You have to add each subdirectory individually. See below for more detailed instructions.

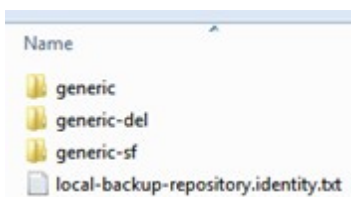
Finally, use the **Schedule** page in the backup manager to set the network server backup schedule. If you are using the ShadowProtect Daily policy, replication should begin 1 hour after the ImageManager processing is configured to begin. Otherwise, choose an appropriate schedule. Usually once per day is sufficient, unless you are performing real-time replication.

## Configure ImageManager on the Replication Target

If you are replicating ShadowProtect backup data, then you **must** set up ImageManager to consolidate the replicated backup images on the replication target. This must be configured for each computer that you are backing up with ShadowProtect.

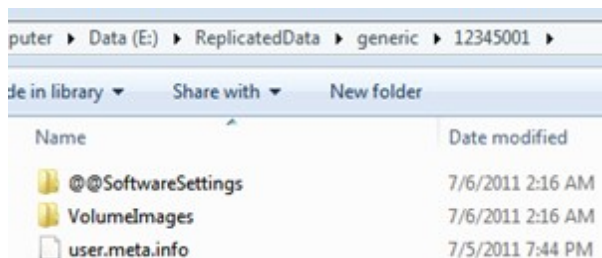
To configure, login to the replication target server, and use the network backup manager program to check the top-level folder where you are storing replicated data. In the example in this document, the location is X:\ReplicatedData. We will use Explorer to find the location(s) of the folder(s) that need to be added to the ImageManager program.

The top-level folder will contain 3 folders (each named after your brand ID). For example:

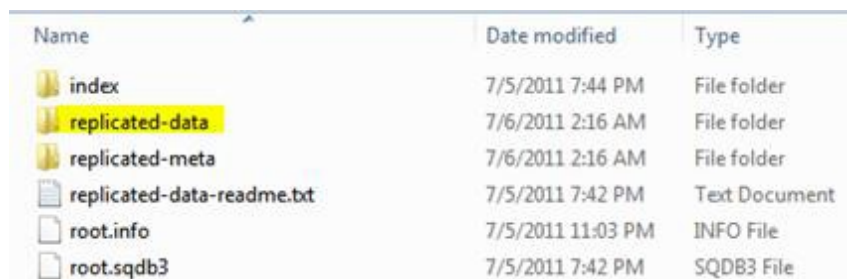


You should ignore the folders that end in '-del' and '-sf'. The replicated data will be contained within the folder that is named after your brand ID (in this case, 'generic').

In the brand ID folder, there will be one subdirectory for each replication source storing data on this replication target. (The directory names are the account numbers of each replication source). If you drill down into one of these account directories, you'll see:



There will be one subdirectory for each top-level folder in your folders list. In this case, VolumelImages is the folder that contains the ShadowProtect data. Inside, you'll see:



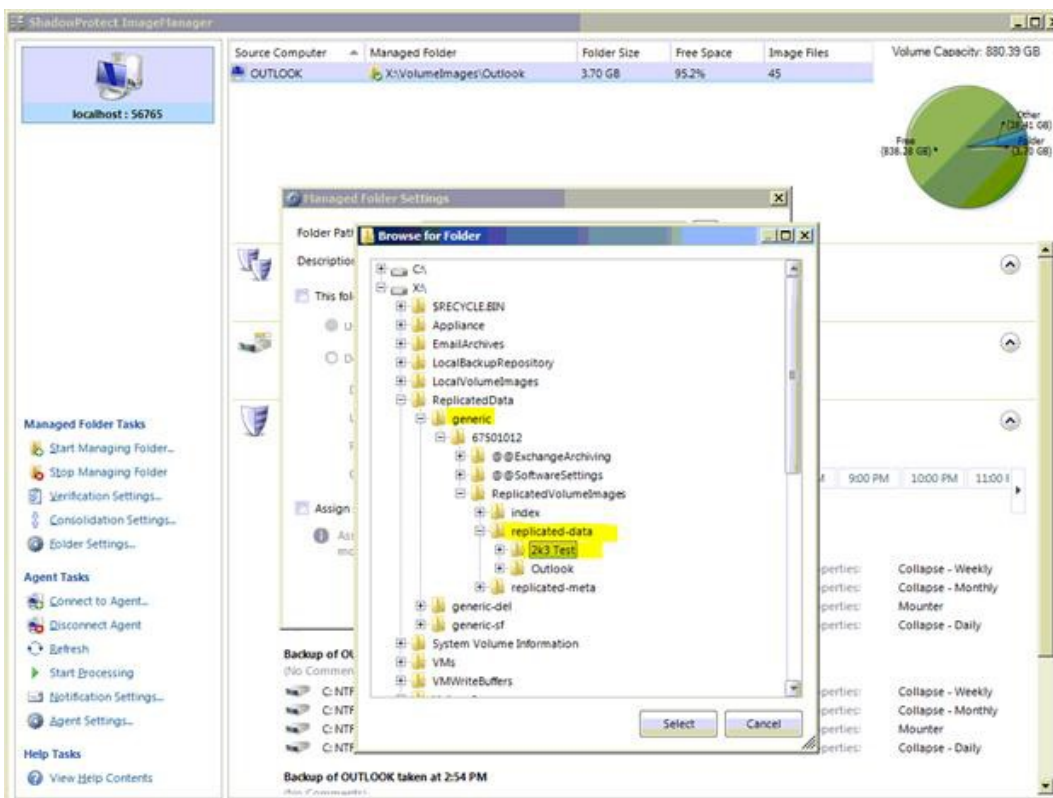
Most of the folders contain metadata needed to efficiently replicate the data. The folder we want contains the actual replicated data and is within the **replicated-data** folder. Inside of the replicated-data folder will be the actual replicated data from the replication source. In this case, we are replicating ShadowProtect backup images for 3 servers, so we see:

| Name                    | Date modified    |
|-------------------------|------------------|
| ExchangeServer          | 7/6/2011 2:30 AM |
| PrimaryDomainController | 7/6/2011 2:30 AM |
| SQLServer               | 7/6/2011 2:30 AM |

These are the folders that we need to add to the ImageManager as managed folders. In our example, we would add the following folders:

- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\ExchangeServer
- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\PrimaryDomainController
- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\SQLServer

For example, here is a screenshot on the replication target adding a folder for a replicated server inside of ImageManager:



You are free to use whatever ImageManager retention policy settings that you want on both the replication source and the replication target. This is unlike cross-site and online backup of ShadowProtect data, where you are required to keep at least 35 days of daily delta files.

Notwithstanding, we still highly recommend keeping at least 35 days of daily delta files even when you are using replication. (Default is 90 days).

## Backing up or Monitoring Replicated Data Stored on the Replication Target

In certain scenarios, you may want to backup replicated data stored on the replication target server to an online backup storage cloud, to another site using site-to-site backup, or to use the local disk feature to make an additional backup to a USB disk (or NAS).

Even if you do not wish to backup the replicated data further, if you are replicating ShadowProtect backup data, then we highly recommend configuring eFolder to monitor the replicated ShadowProtect backups so that you will be alerted if the consolidation process on the replication target server has problems.

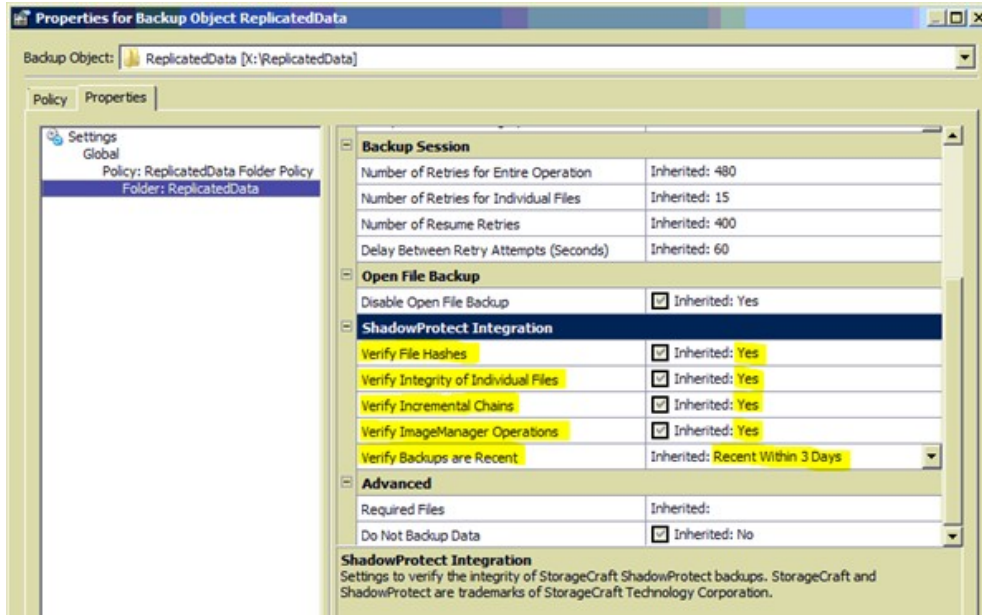
To configure the backup or monitoring of the data, open the backup manager on the replication target server. Configure the **My Account** page with the same credentials that you used in the network backup server manager program. (These credentials should be unique to this replication target server).

Next, in the backup manager, go to the **Folders** page and add the folder that is configured as the top-level data folder in the network backup server manager. In our example, this is X:\ReplicatedData.

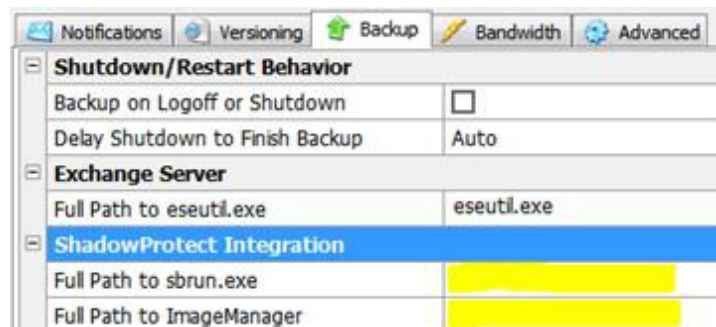
Next, configure remote backups, site-to-site backups, or local disk backups as you normally would for other backups. This may include setting up an encryption pass phrase and setting the relevant backup schedules. If you are only setting up monitoring and not backup, then configure the backup manager to perform remote backups. (We'll discuss a step later used to indicate that the data should only be monitored, but not actually backed up).

If the replication target contains ShadowProtect data, make sure that ShadowProtect monitoring is turned on by right clicking on the folder on the **Folders** page and choosing **properties**. Make sure that all of the ShadowProtect Integration settings are enabled:





If you don't see these folder options, check to make sure that the ShadowProtect management console is installed on the replication target server. If it is installed in a non-default location, you may have to manually tell the backup manager where to find certain ShadowProtect files. To do this, go to the **Backup** tab of the **Options** page, and change the **Full Path to sbrun.exe** and the **Full Path to ImageManager** settings:



Finally, if you only want to monitor the replicated data but do not want to back it up, on the **Folders** page in the backup manager (on the replication target), right click the folder and choose **Properties**. Under the **Advanced** section, set the **Do Not Backup Data** option to **Yes**.



## Preloads of Replicated Data

Performing a preload (initial replication to disk) for replicated data is quite similar to the process of performing a preload for online backups. First, you configure the account, but instead of starting the initial replication, you do the following:

1. Use the Web Portal to put the account into maintenance mode.
2. In the backup manager on the replication source, go to the file menu and choose **Preload Remote Backup** (Choose this even though we will be preloading replication).
3. In the dialog, choose a path to the external preload disk and click **OK**.
4. It will ask which backup destination you want to do a preload for. Choose the network server location (or it might be called the local server). If it does not ask, make sure that you have properly configured the Network Server (or Local Server) field on the My Account page in the backup manager.
5. It will start the initial replication job. Wait for it to finish.
6. When finished, physically transport the preload disk and attach it to the replication target.
7. On the replication target, in Explorer, open the preload disk and navigate to the top-level directory that contains the preload data. Then, navigate into the brandID subdirectory (for example, *generic*). There should be a single subdirectory that has the same name as the account number of the account you preloaded. Use Explorer to copy this directory to the replication target underneath the NetworkServerStoragePath\brandID directory. (For example, copy E:\mypreload\generic\12345001 to X:\ReplicatedData\generic).
8. Finally, use the Web Portal to take the account out of maintenance mode.

**IMPORTANT:** Do not take the account out of maintenance mode until you have completed all of these steps. If you clear the maintenance flag early and the replication source attempts to replicate data, you will have to do the preload all over again.

Note that you can put multiple preloads onto the same preload disk. To do this, use a different top-level directory on the preload disk for each account that you preload. When you are finished preloading multiple accounts, on the replication target there should be multiple subdirectories of the NetworkServerStoragePath\brandID subdirectory, one for each account that was preloaded. For example, X:\ReplicatedData\generic could contain the subdirectories 12345001, 12345002, 12345003.

### How to request and create a ShadowProtect preload (seed) drive

The below instructions are intended for resellers. If you are an end-user, please coordinate the preload operation with your reseller.

[How to request a preload \(seed\) drive](#)

[How to create a ShadowProtect preload \(seed\) drive](#)

## Restoring Replicated Data

You can "restore" (or download) data stored on the replication target back to the replication source by using the File Manager tool, just like you would with a normal backup.

Please note that data that is changed on the replication target will not be automatically downloaded to the replication source. (Automatic replication is one-way only). If data has changed on the replication target, the File Manager tool can be used to download the changed data back to the replication source.

This can be useful, for example, if you virtualized an end-user's server off-site on the replication target and you need to download the updated bare-metal backup image back to the end-user's primary site. There is an option in the file manager that allows you to skip files that already exist on the client that are the same or more recent, so you can easily and quickly download only those files that need to be downloaded to bring the replication source up to date.

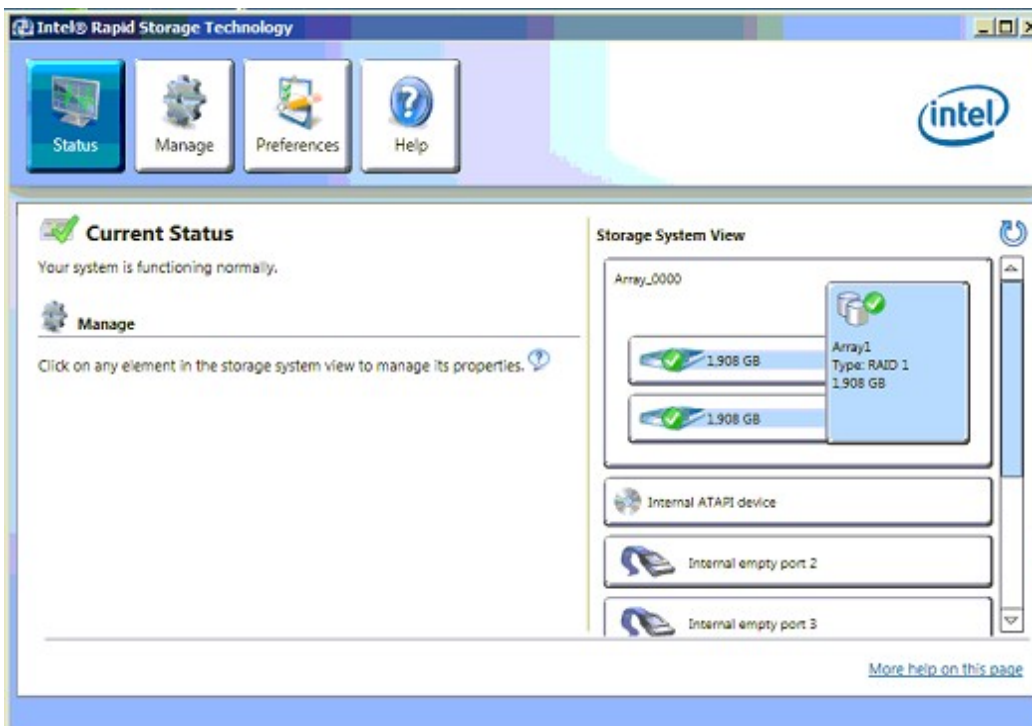
## Overview of Hardware RAID

This section discusses basic management of the RAID volumes, including viewing and monitoring the health of RAID volumes, replacing failed drives, and adding additional storage (without rebooting or taking the system offline). An [overview of the RAID feature](#) is also available.

## Viewing Status of Hardware RAID

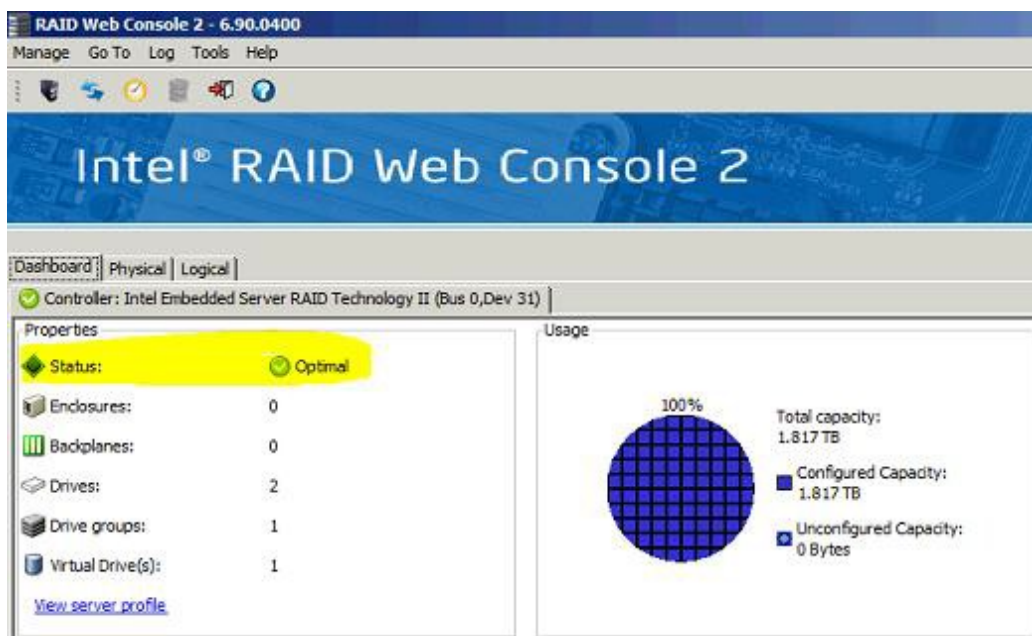
On the desktop, double click the *RAID Management* icon. For LSI RAID systems, click the localhost system, click **Login**, and then enter a *Windows* username and password for an administrator of the BDR.

Intel-based RAID systems will see something similar to:



Make sure that current status shows that the system is functioning normally.

LSI-based RAID systems will show something like:



The **Physical** and **Logical** tabs can be used to obtain more detailed information.

### Replacing Failed Drives

All BDR models come with hot-swappable drive carriers. When you receive the replacement drive, simply remove the drive carrier with the failed drive, unscrew the failed drive, screw in the replacement drive, and re-insert the drive carrier. You do not need to power down the BDR.

Then, you should start the RAID management console ([see instructions](#)) to check if the RAID controller sees the new drive, and to tell it to start rebuilding the RAID volume.

In many cases after you re-insert a new drive, the RAID controller will automatically start rebuilding the RAID array using the new disk. You should be able to use the RAID status screen in the RAID management console to check.

If it does not show that the RAID array is rebuilding, use the RAID management interface to tell it to use the new drive to rebuild the RAID array. In LSI RAID system, go to the **Logical** tab, find the new drive, right click it, and choose **Rebuild**. The progress of the rebuild can then be monitored on the **Dashboard** tab.

### Adding Storage Overview

The BDR employs hot-swappable drive carriers and RAID controllers capable of adding drives to a live system. Additionally, the advanced operating system of Windows Storage Server 2012 allows file system volumes to be expanded without having to take any services offline or reboot.

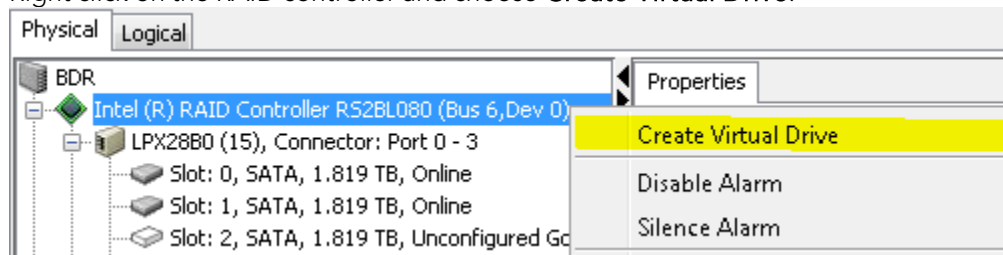
Due to the use of RAID1 or RAID10, drives are always added in pairs.

The X:\ volume is the data volume, and it is the volume that should be expanded. We recommend expanding the X:\ volume onto the new pair(s) of drives, rather than creating a separate partition for the new storage.

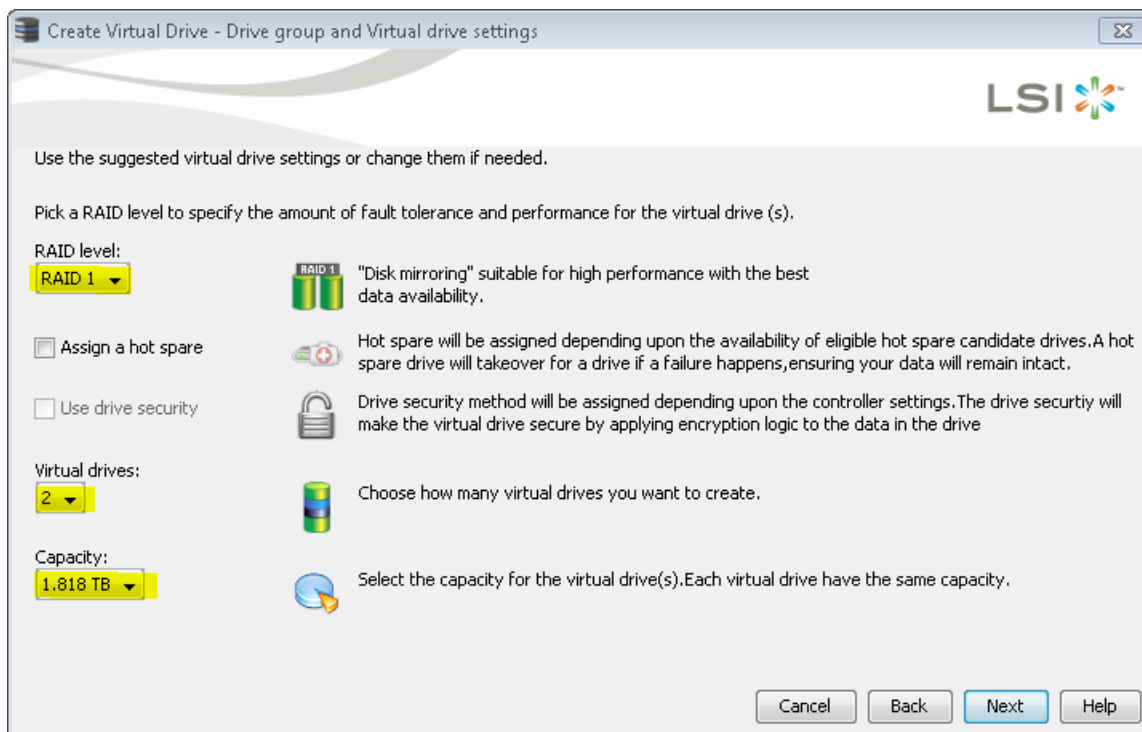
NOTE: The screenshots on this page are for LSI-based RAID controller, but the procedures are nearly identical for Intel-based RAID controllers.

### Instructions to Add Storage without Rebooting

1. Physically insert the new pair of drives in the next available slots. For tower models, drive slots are numbered top to bottom. For rack mounted servers, drive slots are numbered bottom to top, then left to right (The first drive is in lower-left, last drive is in top-right).
2. Start the **RAID Manager** using the desktop icon. Login using a valid Windows username and password.
3. Right click on the RAID controller and choose **Create Virtual Drive**:



4. Choose **Simple mode** and click **Next**.
5. **Choose RAID level of RAID 1**. Click the 'Virtual drives' drop down and select the number of virtual drives (normally you will want to choose the largest number available). For capacity, you normally want to choose the smallest capacity available. Click **Next** when finished. Here is an example where we are adding two pairs of drives:

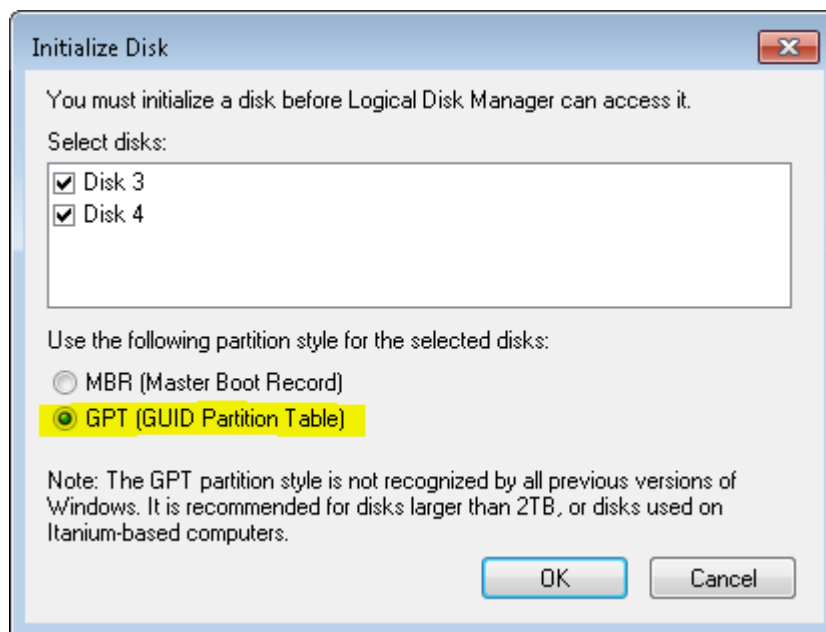


6. Review the information on the Create Drive summary page, and if correct, click **Finish**. It takes about 10 seconds per pair of drives to become active. Click the Logical View tab at the top to verify that all new logical drives are present and correct.
7. **IMPORTANT:** The write cache policy of the new virtual drives must be changed in order to ensure maximum data integrity. In the **Logical View** tab, for each new virtual drive, right click the virtual drive and choose **Set Virtual Drive Properties**. Change the settings so that they are:

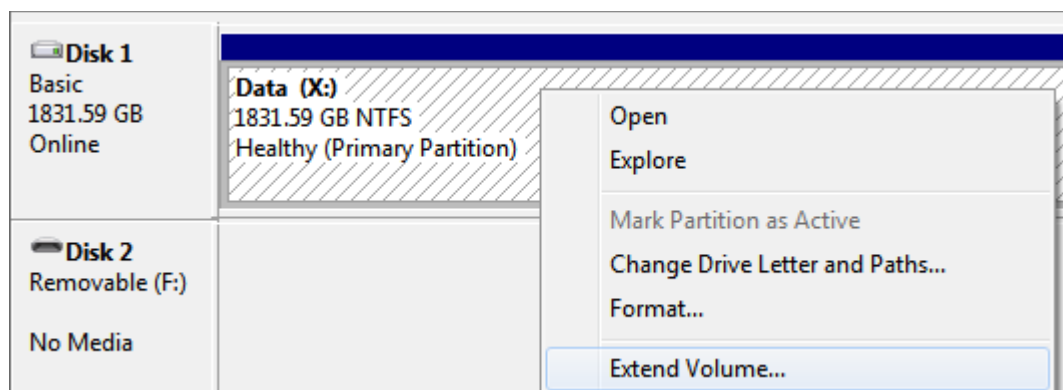
Read Policy: No Read Ahead  
 Write Policy: Write Back with BBU  
 IO Policy: Direct IO  
 Access Policy: Read Write Disk  
 Cache Policy: Disabled  
 Background Initialization: Enabled

Click **OK** and confirm to save changes. Repeat this for each new virtual drive.

- Open the *Server Manager* program from the Windows task bar, and then expand the *Storage* category and open *Disk Management*. It should prompt you to initialize the new disk(s). Choose to use a **GPT-style partition table**, and click **OK**:



- Find X: in the volume list, right click, and choose **Extend Volume**:



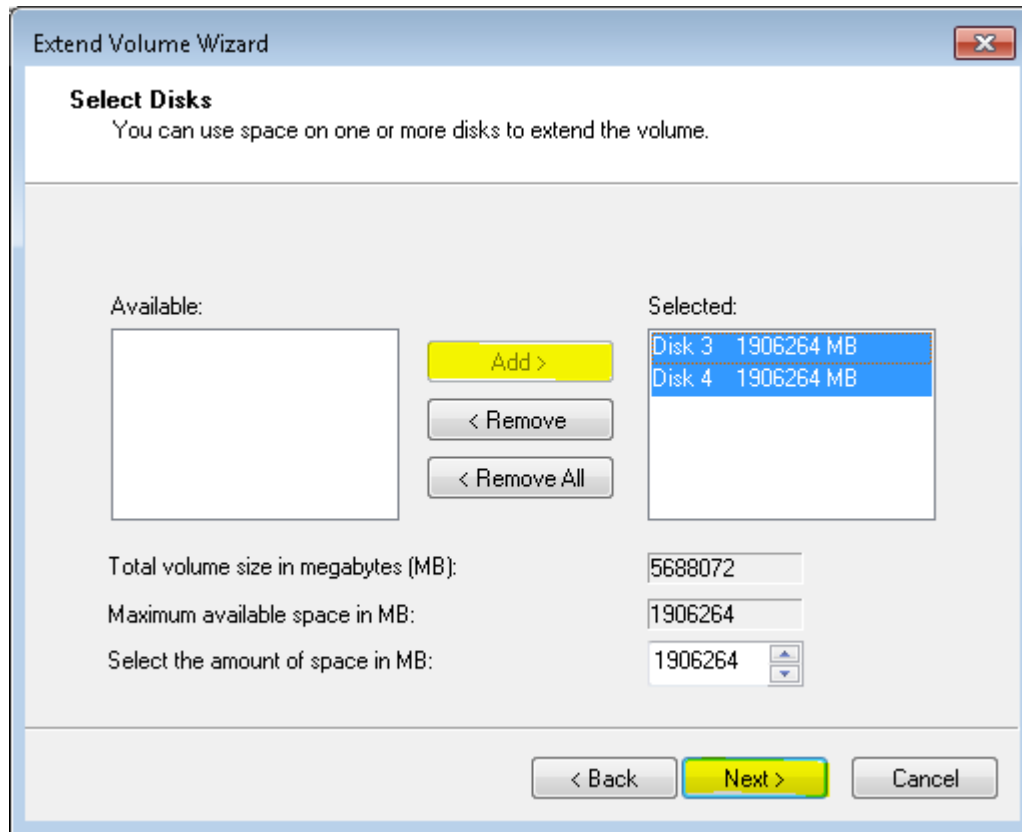
**Tip:** You may have to first right click on *Disk 1* (or whichever disk contains the X:) and choose *Convert to dynamic* before it will allow you to use the **Extend Volume** command.

**IMPORTANT:** Make sure you convert only the volume that contains the X: to a dynamic disk and not to any other volume.



10. The Extend Volume Wizard will open. Click **Next** to start the wizard. Choose the disk(s) that you want to add to the volume. Select the one or more disks you are adding (they should be listed as having 1906264 MB free per disk) and click **Add** and then **Next**.

**CAUTION:** This operation may be hard to undo. Only proceed once you are sure!



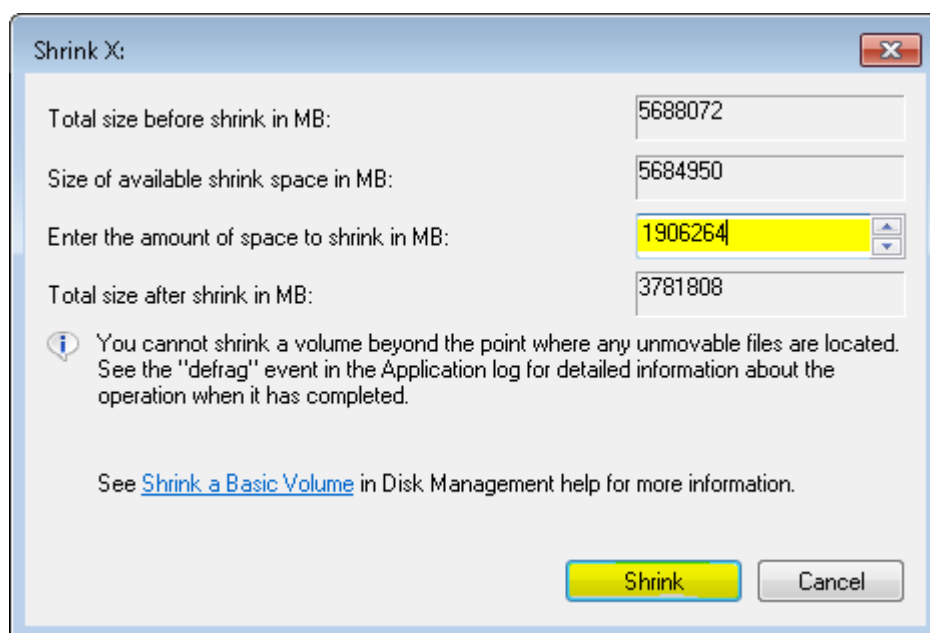
11. If it asks you if you are sure you want to convert a Basic volume to a Dynamic volume, then choose **Yes** to continue.
12. It should only take a few seconds for the expansion operation to complete.

### Shrinking Storage without Rebooting (Advanced Users Only!)

If you wish to remove pairs of drives, this is possible as long as enough free space is available on the volume. You may have to defragment the drive before it will allow you to shrink the volume and remove the drives. Note that you cannot control which pair of drives will be freed. Even if you have just added a pair of drives, following this procedure may not allow you to remove this pair of drives (although it is quite likely).

**WARNING: Proceed at your own risk:** Improperly following this procedure (and/or unexpected configurations) may result in the complete failure of your data volume (X:\) and/or OS volume (C:\). Follow the instructions very carefully. We will be unable to provide an easy solution if the data volume is marked as failed because the wrong virtual disk is deleted in the RAID manager.

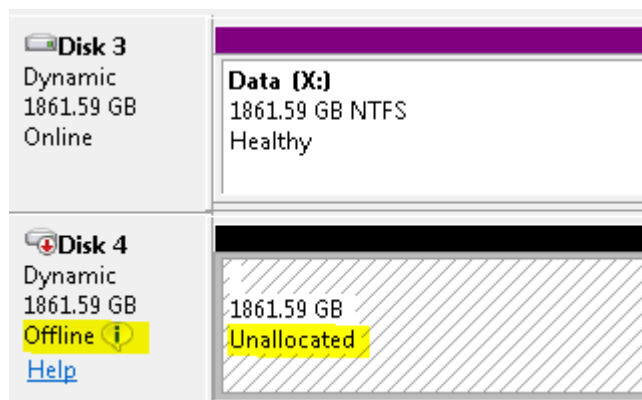
1. Open the *Server Manager* program from the Windows task bar, and then expand the *Storage* category and open *Disk Management*.
2. Right click the X: volume in the list and choose *Shrink Volume*.
3. Each pair of drives normally provides 1906264 MB of space, so to remove one pair of drives, choose to shrink the volume by 1906264 MB.



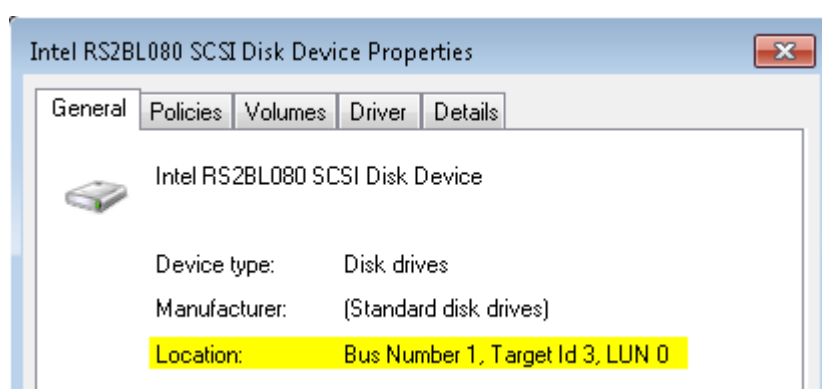
4. After the shrink operation has completed, one or more of the disks should show up as **Unallocated**.

**Tip:** If part of the disk is still in use, hovering your mouse over the allocated region should show you the amount still in use. You can do another **Shrink** operation by that amount to completely unallocate the space used on that disk.

5. Once the disk shows up as unallocated, right click that disk (right click the left-hand side) and choose **Offline**. The disk should now show up as Offline, similar to:



6. Right click the disk again and choose **Properties**. Look at the location information:



7. Use the desktop icon to start the RAID manager. Click the **Logical** view. The target ID in the location information found in the previous step indicates which 'virtual disk' number in the RAID manager should be deleted. (In the above screen shot, the virtual disk we want to delete would be virtual disk #3.)

Before we actually delete the virtual drive in the RAID manager, it is extremely important that we determine that we are about to delete the correct virtual drive.

To determine if the correct virtual drive is about to be deleted, right click the virtual drive in the RAID manager and choose **Set Virtual Drive Properties**. Change the **Access Policy** to **blocked** and click **OK**, confirming changes. Then switch back to disk management and choose *Action menu -> Rescan Disks*. If you have chosen the wrong virtual drive to delete, the data volume (X:) will now be marked as **failed**. If this happens, do not panic. Go back to the RAID manager, edit the virtual drive properties, and change the **Access Policy** back to **Read/Write**. Then go back to disk management and rescan the disks again. Now the X: should show up as healthy again. Now carefully recheck the target ID and identify the correct virtual drive that should be deleted.

Repeat this procedure (changing the write policy to blocked and rescanning in disk management) to see if you are about to delete the correct virtual drive. If you have identified the correct virtual drive, then once you change the **Access Policy** of that virtual drive to **Blocked** and rescan disks, the Data volume (X:) should still show up as healthy and available.

8. Once you have identified the correct virtual drive to be deleted using the above step, right click the drive in the RAID manager and choose *Delete Virtual Drive*. Confirm changes. Go back to disk management and ensure the Data volume (X:) is still healthy and available. It may show the disk that you just removed as a dynamic disk is unavailable. You may right click this disk and choose *Remove*.

**WARNING:** If you delete the wrong virtual drive in the RAID manager it cannot be undone, and the data volume will be marked as failed. You will have to format the data volume and start over. Make sure you follow the previous step precisely to ensure that you have selected the correct virtual drive to delete.

For each physical drive you want to remove (which should be showing up as **unallocated** now), left click the drive in the RAID manager to view the slot information. If you are in doubt which physical location corresponds to that slot number, right click the physical drive and choose *Start Locating Drive*. Once you know where the drive is, right click and choose *Stop Locating Drive*. Then right click the drive, and choose *Prepare to Remove*. Once this is complete for all drives you want to remove, you may remove the physical drive(s) from the appliance.

## Network Interfaces Overview

This section discusses advanced setup for the network interfaces on the appliance, including [NIC teaming](#) (link aggregation) and [VLANs](#). In many networks you will not need these advanced features.

NOTE: Prior to any Network changes it is advised that you ensure that the drivers for your particular NIC are up to date. This is NOT done with the software updater.

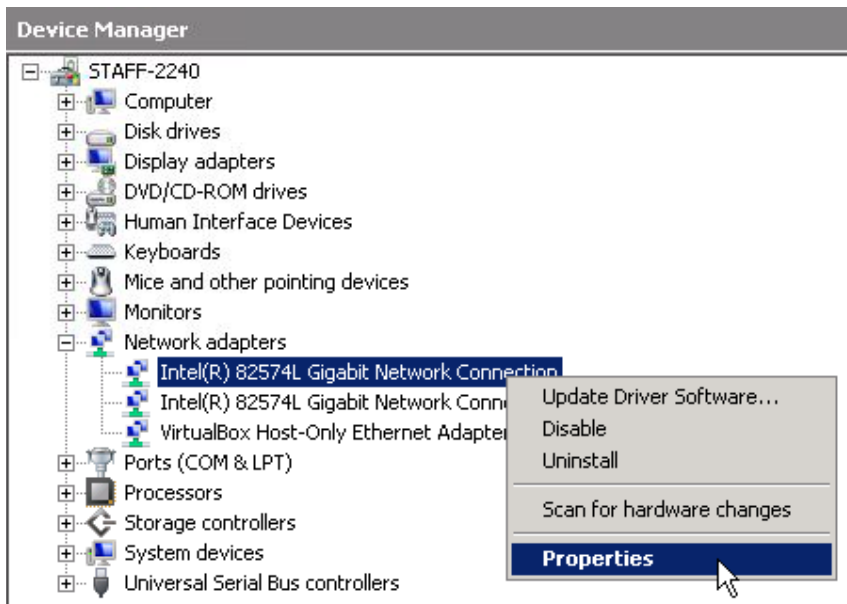
## NIC Teaming Setup

NIC teaming allows you to "team" two or more Ethernet ports together on the server to form a single more fault-tolerant virtual Ethernet port. Intel NIC teaming supports several different types of teams, to accommodate different switching standards and network topologies. This includes:

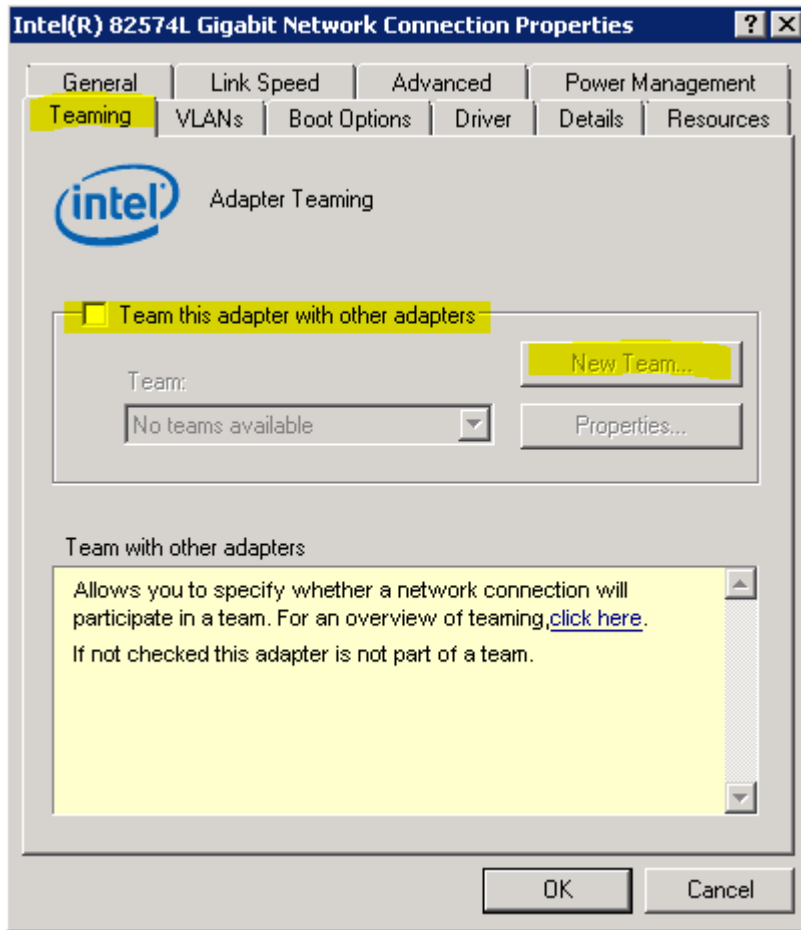
- **Adapter Fault Tolerance:** All NICs in the team should be connected to the same switch. If one of the NICs fails, another NIC in the team will take over the MAC address of the failed NIC.
- **Adaptive Load Balancing:** The same as Adapter Fault Tolerance, except that in addition to failover, outgoing traffic is distributed more evenly across all of the NICs in the team.
- **Switch Fault Tolerance:** The two NICs in the team should each be connected to a separate switch. The switches must be running a spanning tree protocol (such as STP). This ensures continued connectivity even if a single switch fails.
- **Static and Dynamic Link Aggregation:** Allows multiple NICs to be aggregated together to form one faster link. Your switch must support and be configured for 802.3ad.

For more information, please consult the Intel documentation and KB articles about NIC teaming, especially their [how-to guide](#).

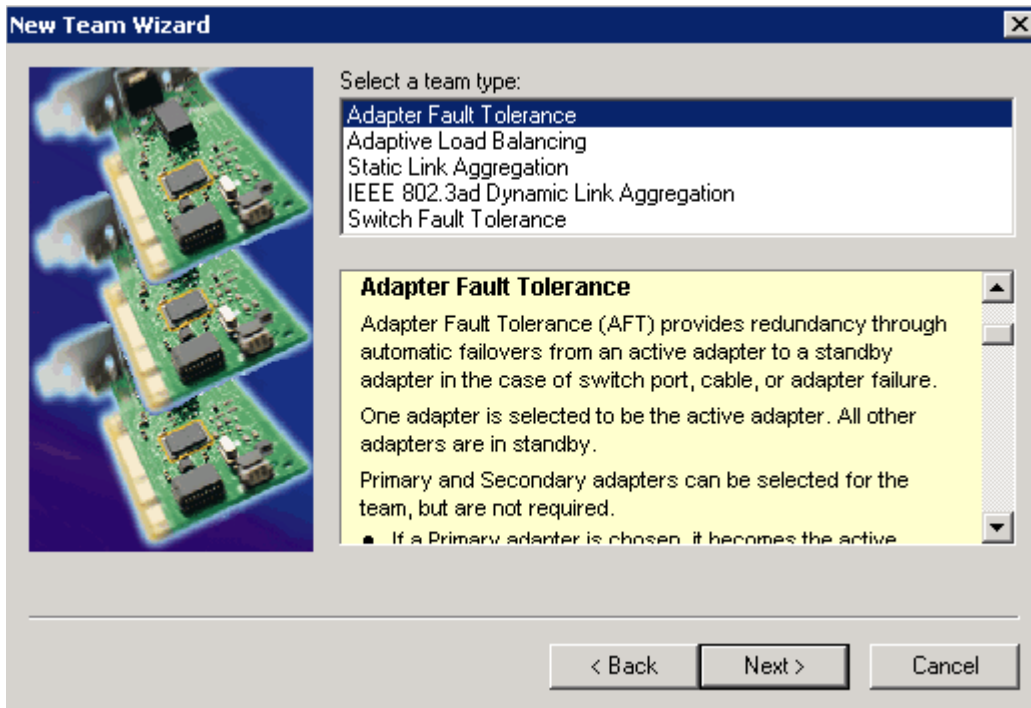
To configure NIC teaming, first open device manager, find one of the Intel network adapters in the list, right click and choose **Properties**:



In the properties window, find and click the **Teaming** tab. Check the *Team this adapter with other adapters* checkbox, and click the **New Team...** button to start the team creation wizard:



The team creation wizard will guide you through the process of selecting the type of NIC team and fully configuring the NIC team. For example, this step in the wizard allows you to select the team type:



Follow the instructions in the wizard to finish setting up the NIC team. Please consult the Intel documentation on NIC teaming for additional detailed instructions if needed.

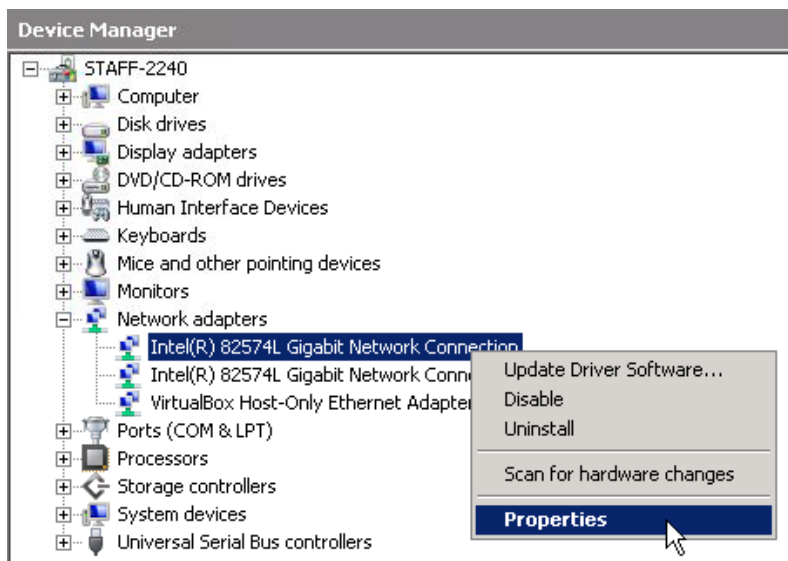
### NIC VLAN Setup

VLANs provide a standard to create several virtual networks on top of one physical network. Each virtual network is completely isolated from any other (for example, broadcast packets on one VLAN do not propagate to another VLAN). If you plan to use VLANs, your network switch and/or router must first be configured with the VLAN IDs expected on each port.

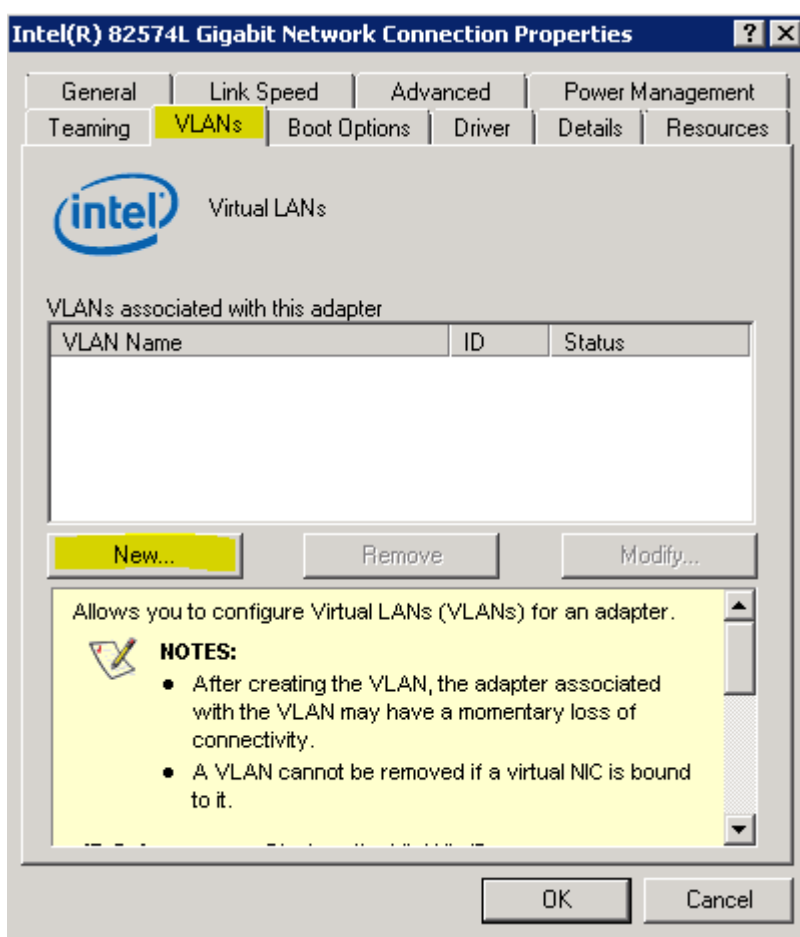
VLANs are implemented either by (1) using **untagged** ports (dedicating certain ports on a switch to a specific VLAN), or (2) by using **tagged** ports (ports that prepend a header on all network packets with the VLAN ID and other relevant information).

No special steps are required to connect the Ethernet ports to an untagged VLAN port on a switch.

The BDR also supports connecting to a tagged port, in which case the Ethernet adapter(s) must be specifically configured with the correct VLAN ID(s). To do this, open device manager, find the network adapter, right click, and choose properties:



Click the **VLANs** tab. Use the **New** button to create one or more VLANs:



Follow the wizard to finish setting up the VLAN(s) you want to configure.

At this point, additional network adapters will appear, and you can use the Windows control panel network connections screen to set IP addresses and other relevant information for the virtual adapters joined to the virtual networks.

For more information, please see the [Intel VLAN Set Up instructions](#).



## BDR Configuration Checklist (Summary Version)

 Setup Lights-out Management (iLOM)

- Connect management Ethernet port to switch.
- Assign IP address (Default is DHCP. Use BIOS to set static IP)
- Login to <https://ipaddress/> (username ADMIN password ADMIN) and change ADMIN password

 Setup Windows and Update Appliance Software

- Accept license.
- Set computer name.
- Set Administrator password.
- Configure networking.
- Run *Update Appliance Software* link on the desktop and let it finish.

 Setup ShadowProtect

- For servers being backed up, defragment volumes if needed. Make sure any legacy backup jobs (such as SQL dumps, ntbackup, etc.) are **not** backing up to partitions that will be backed up by ShadowProtect.
- For domain controllers, document the Directory Services Recovery Mode (DSRM) password. (see [http://technet.microsoft.com/en-us/library/ee808906\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee808906(WS.10).aspx))
- Create a subfolder in X:\Volumelimages or X:\LocalVolumelimages for each server you are backing up. (Use this location if you do **not** want to upload the data offsite.)
- Install ShadowProtect agents.
- Reboot servers.
- Setup ShadowProtect **Continuous Incremental** Backup Jobs using **maximum compression**.
- **IMPORTANT:** Make sure volumes being backed up are basic volumes, and are **not dynamic volumes**.
- Activate ShadowProtect agent licenses (purchased BDRs only).

 Setup ImageManager

- Add a folder for each server in ImageManager.
- Optionally, customize retention settings for each folder.
  - **IMPORTANT:** You must keep daily image files (-cd) for **at least 35 days**.  
(The retention settings for each folder must not be less than 35 days.)

 Virtualization

- Test virtualization using the VirtualBoot wizard. (Use NAT networking mode) Delete VMs when done testing.

 Configure the Backup Manager Account (required for proper monitoring, even if you are not sending data offsite)

- Enter account information and test the connection.
- Setup encryption passphrase.
- Configure remote backup schedule. (Set to one hour after ImageManager does it's processing. You must do this even if you are only backing up locally.)

#### ❑ Preload (optional)

**Tip:** You may want to run incremental backups for a few days to ensure deltas are reasonably sized.

- Put account into maintenance mode using Web Portal.
- Request preload drive from eFolder by filling out the form here:  
<https://backup.securewebportal.net/admin-console/drive-request/>
- Receive preload drive from eFolder
- Attach preload +drive to BDR.
- Run preload (backup manager, file menu, preload remote backup).
- Ship the preload drive back to eFolder using return label provided.

#### ❑ Configure Notifications

- Configure partner-wide notifications in **My Partnership**, under **Notifications** in the Web Portal [This configuration choice is only available for branded partners.]
- Optionally, configure your email address in the **Online Backup Manager** program.

## Additional Questions?

- Submit all eFolder questions to [support@efolder.net](mailto:support@efolder.net).
- Call us at 800-352-0248.
- Browse our [Knowledgebase](#)



The People Behind Your Cloud