# *Install and Configure an eFolder BDR for ShadowProtect* Video Script

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Introduction and overview**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Welcome to this overview of how to install and configure an eFolder BDR for ShadowProtect.

A Backup and Disaster Recovery (or BDR) appliance is a computer dedicated to backup and disaster recovery that typically backs up images of servers and desktops and can provide fast virtualization of failed servers on the BDR itself. An *eFolder* BDR appliance can:

* Backup and restore individual files, mailboxes, messages, or entire machine images;
* Virtualize a server or a desktop to provide business continuity in the event of a failure or disaster; and
* Optionally, backup your BDR data to the eFolder storage cloud, replicate the data to another BDR appliance, and/or virtualize the server in the cloud or on another BDR in case of local site disaster.

In short, an eFolder BDR offers peace of mind through data protection and disaster recovery.

When you deploy an eFolder BDR, you must make a couple of decisions:

* First, you must decide whether to backup the data on the BDR to the cloud, replicate it to another BDR, or just keep it stored locally on the BDR.
* Second, you must decide whether or not you will use optional file-level backups to protect selected files on your end-user’s machines, such as laptops or desktops.

Normally, the BDR backs up entire images of servers and workstations, but you can also backup individual files to the BDR (or to the cloud) from machines of your choosing, if you also have signed up to use the optional eFolder Backup for Files service.

Getting your BDR up and running involves nine steps, two of which are optional. Let’s overview these steps and then walk through each step in detail:

Step 1, set up the physical configuration, involves mounting and cabling the BDR.

Step 2, configure Windows, includes reading license agreements, setting your computer name, and choosing an initial administrator password.

Step 3, verify administrator/service account configuration credentials, ensures you have the account credentials you need for setting up the BDR.

Step 4, update appliance software, consists of downloading and installing any new appliance monitoring software updates that are available.

Step 5, setup bare-metal backups, involves setting up other computers on the network that will be imaged and backed up to the BDR.

Step 6, setup off-site monitoring and backups, consists of connecting the BDR appliance to an online backup account. This is required even if you will not be backing up data off-site.

Step 7, setup cross-site replication, is optional and involves configuring the BDR as a replication source or target for cross-site replication.

Step 8, setup notifications, ensures that end-users and resellers are notified of warnings or errors, as desired.

Step 9, test file restores and virtualization, is optional but highly recommended and ensures that you can recover files or virtualize your servers without difficulty, so you can have confidence things will go smoothly in a time of crisis.

Use the Configuration Checklist, found in the **Resources** tab of this training video, to keep track of these steps as you go through them.

Now let’s look at each step in detail.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 1. Set up the physical configuration**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The first step in installing and configuring an eFolder BDR for ShadowProtect is setting up the physical configuration. This involves mounting and cabling the BDR appliance.

First, unpack the appliance and check that it came with the following additional parts:

* A bare-metal recovery CD. This CD can be used to boot a computer and restore data from a bare-metal backup without having to reinstall the operating system first.
* One or more power cords. If your appliance has a redundant power supply, it should also come with a second power cord.
* For rack-mounted appliances, mounting rails. These rails are designed for the mounting of equipment in a standard 19" rack.

Next, mount the appliance and secure the appliance in an appropriate location. This location should have an environment suitable for computing equipment, including environmental controls for temperature and humidity and the filtering of the air to remove dust and other particulate material. Hardware sensors and monitoring software on the appliance will help you measure and monitor environmental quality over time.

Now, connect the power cords to a filtered power source, such as a UPS or surge protector, to avoid damage to the appliance.

The next step is connecting the appliance to the network. 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 switches or routers. 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. Connect at least one of the network ports to a network so that you can remote desktop into the appliance after the initial out-of-box setup.

If you have a BDR model with a Lights-out Management port, referred to as IPMI (or Intelligent Platform Management Interface), and you wish to use it, connect a Cat5e or Cat6 cable to the dedicated management port on the back on the appliance. The IPMI is a physically separate computing board that is installed into the computer that runs independently from the computer. It allows for complete remote management of the physical box. Even if the machine is turned off, you can still connect to the IPMI port to power on the machine, edit the bios settings, configure RAID or host bus adapters, and even see the desktop after the machine boots. Lights-out Management is sometimes called by different names, depending on the vendor that makes it. For example, HP calls theirs ILO, which stands for integrated lights out, while Dell calls theirs DRAC, which stands for Dell Remote Access Controller.

This management port is located separate and apart from the other non-management network ports and is clearly labeled as a management port, except on BDR model 1122, where it is unlabeled. If the management port is connected to the same network as the non-management ports, the management port will acquire a different IP address than the non-management ports. Of course, if you want, you can connect the management port to a dedicated management network. Either way, you should assign a static IP address to the IPMI port.

You are now ready to power up the appliance. Turn on the appliance. If you have a model with IPMI and know the assigned IP address, you can use the remote console feature to access the console using the web browser on another computer that has access to the same network. You can then use the virtual monitor and keyboard that is in the IPMI web console. If you have a BDR model *without* IPMI, 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 the remote desktop to access the appliance.

If you are using a BDR model with IPMI and you would like to use it to do the initial configuring, you must determine the IP address assigned to the Lights Out Management port. 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, which is either a router or network server, or connect a monitor to the BDR and go into the BIOS of the IPMI to view the current IP address assigned to the IPMI port. Note that while you are there would be a good opportunity to assign a static IP address.

After you know the IP address, open a browser and go to *http://ipaddress/* where *ipaddress* is the IP address assigned to the IPMI port. The default username is ADMIN in all caps and the default password is ADMIN in all caps, which are both case sensitive. After you are logged in, be sure you change the default ADMIN password, and then use the menus to start the remote console, which requires Java.

At this point, the appliance should be powered on and physically connected to the network, and you should have access to the console using a monitor and keyboard or using the IPMI remote console feature.

This completes step 1 of installing and configuring the BDR, which was setting up the physical configuration.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 2. Perform Windows configuration**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 2 is configuring Windows so that you can get the BDR appliance on the network. When the appliance first boots, you will be presented with the Windows Storage Server first-run setup wizard. You will be unable to log in to windows or use remote desktop until this setup wizard is completed. Follow the prompts in the wizard.

First, enter your activation key, which can be found on the label that is attached to the BDR, and click **Next**.

Read, review, and decide whether or not to accept the license terms presented on the screen. Note that the 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. To accept the license terms, check the checkbox and click **Accept**.

The wizard now prompts you to set an *Administrator* Windows password. Choose a password of sufficient length and complexity to meet your security requirements. For better security, the National Institute of Standards and Technology (or NIST) recommends that administrator passwords be at least 15 characters in length or longer. The Administrator password authorizes you to log in to the BDR appliance, as well as access the network data shares hosted by the appliance. Type in your password twice and click **Finish**.

You are now prompted to log in to Windows. Log in as the Administrator with the password that you just set.

After you have 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, and so forth.
* Consider renaming the server to match your standard naming convention.
* 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, such as an anti-virus, and so forth. 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, to apply group policies, and to be able to give domain accounts permissions to the folder shares on the BDR. Note that the Granular Recovery for Exchange program from eFolder does *not* require the BDR being joined to a domain.

Note that if you are backing up a SBS server or an environment with non-redundant domain controllers, we recommend that you do *not* join the BDR to the domain to avoid delays when you try to log in to the BDR when the domain controller is down. Also, if you do join the BDR to the domain, we strongly recommend that you create a local administrative Windows user on the BDR so that you can still easily log in if the domain controller is down and you are trying to virtualize the domain controller on the BDR.

Windows will come configured with two data volumes on the BDR:

* C:\ . This is typically 80 GB in size. This data volume hosts the operating system and the bundled software. Do *not* create writable network shares or otherwise allow user data to be stored on this volume. 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. Note that the documentation and other important files are all stored within subdirectories of C:\Appliance.
* X:\. This volume is given the rest of the disk space. It is used to store all of the user data, including bare-metal backup images and replicated data. This volume can be dynamically expanded without rebooting by purchasing additional storage add-on packs and performing a short configuration process.

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

This completes step 2 of installing and configuring the BDR, which was getting Windows up and running and configuring the network.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 3. Verify configuration credentials**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 3 is verifying configuration credentials, which is making sure you have all the credentials you will need to install and configure your BDR.

This step consists of verifying that you have the following three sets of credentials readily available:

The first set of credentials you will need is your online eFolder *backup account credentials*. Even if you are *not* sending backed up data off-site from the BDR, the online backup account credentials will be used to connect the appliance to the centralized eFolder Web Portal for monitoring and reporting purposes. Use the eFolder Web Portal to create a new account with a ShadowProtect BDR or Trial (ShadowProtect) service plan. If you need help on creating accounts, refer to the video “Create an account using the New Account Wizard” in the Learning Center of the Partner Center that is accessed by hovering over the **Support** button in the main menu of the eFolder Web Portal.

The second credential you might need is your encryption *pass phrase*. A pass phrase is a textual phrase consisting of about 30 letters, numbers, characters, symbols, and so forth that will be converted into a 256-bit encryption key and used to encrypt your data when it is stored. If you are sending your data off-site to the eFolder storage cloud, you *must* create a pass phrase. If you are only doing local backups or cross-site replication, the use of on-disk encryption is optional; therefore, creating a pass phrase is also optional.

This pass phrase is required to restore any data that is backed up and encrypted with this password. If you later change the pass phrase after the original pass phrase has been used in backing up data, then both pass phrases would be required to restore your data: the old pass phrase for files backed up previously, and the new pass phrase to restore data backed up after the pass phrase was changed. To avoid this, many partners perform a new full backup or preload after changing the pass phrase so that all files can be restored with the new pass phrase. Each of your customers should have a unique pass phrase.

It is extremely important that you document the pass phrase in multiple places, so that you will be able to decrypt and restore your data when needed. Appropriate places to document your 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, your reseller, and a safety deposit box.

The third set of credentials you will need are the credentials for the computers that will be backed up, meaning a Windows login with administrative privileges for *each* server or desktop that needs to be backed up. This could either be a domain administrator, a service account, or a local account with administrative privileges on each of the machines.

This completes step 3 of installing and configuring the BDR, which was verifying your configuration credentials.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 4. Update the appliance software**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 4 in installing and configuring an eFolder BDR for ShadowProtect is updating the appliance software. This involves downloading and installing any BDR appliance monitoring software updates. Note that updating the eFolder backup software, which is different from the monitoring software, will be covered in Step 5.

The software that monitors the appliance is continually being updated and enhanced. Each BDR requires a maintenance and support subscription that ensures you always have access to the most recent version of all BDR software. Although the BDR is set to automatically install software updates every evening at a random time between 6pm and 11pm, you should manually initiate the software update process when you are first setting up the BDR to ensure that your appliance is running the latest version of all BDR software before you configure that software.

To install any available monitoring software updates, verify internet connectivity and then double click the **Update Software Appliance** icon on the desktop of the BDR. The software update process will run. Depending on the size of the updates, this may take some time to finish. The update program will display the progress of any downloads in a PowerShell window as the software update process runs. When it completes, you are prompted to *Press any key to continue…* to close the window and complete the process.

This completes step 4 of installing and configuring the BDR, which was downloading and installing any Appliance Monitoring software updates.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 5. Setup bare-metal backups** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 5 is setup bare-metal backups, which is setting up other computers on the network to be backed up to the BDR.

One of the primary functions of a BDR is to manage and receive data for bare-metal backups from 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. To setup bare metal backups, you will need to perform four steps on *each* server or desktop you want to backup. We’ll list the four steps here and then discuss each one in detail.

The first step is to perform preparatory work on each server or workstation that will be backed up.

The second step is to install the ShadowProtect agent on each computer to be backed up. This requires a reboot of each computer on which the agent was installed.

The third step is to configure a continuous-incremental backup job to backup to a directory on the BDR that is unique to this computer.

And the fourth step is to configure the ShadowProtect ImageManager that is running on the BDR to monitor the directory that contains the bare-metal backup images for the computers you are backing up.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing preparatory work on machines to be backed up** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now let’s look at each of these steps in detail. The first step in setting up bare-metal backups is to perform preparatory work on each server or workstation that will be backed up to ensure optimal performance and to minimize the size of incremental backups. 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, perform the following preparatory work on each server or workstation to be imaged and backed up:

* 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.
* Be aware of Windows licensing and activation issues. If you plan on being able to virtualize a down server on the BDR, 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.
* Defragment 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 that you defragment any volumes that are heavily fragmented before starting bare-metal ShadowProtect backups. You should also disable any scheduled defragmentations.
* Document and synchronize the Directory Services Restore Mode password. For you to be able to virtualize a domain controller, including SBS servers, you must know the directory services restore mode (or 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 log in as the local Administrator user. This allows you to log in 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>.
* Identify legacy backup jobs and ensure they backup to separate partitions that will not be backed up by ShadowProtect. A common reason that very large incremental ShadowProtect backups occur 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, suppose ShadowProtect is configured to backup the C: (the OS) and D: (the Exchange information store) volumes. Also suppose that there was a task scheduler task scheduled to run an *ntbackup* job to perform a full backup of the Exchange database every day and store it to *D:\ExchangeBackup*. In this case, every day, a new file is being written by *ntbackup* to *D:\ExchangeBackup* that was approximately the size of the Exchange store. ShadowProtect sees this new file as all-new data, which can create incremental ShadowProtect backups of tens of gigabytes every day. Another common example is where full SQL backups (for example, SQL dumps) are scheduled to run and are placing the *.bak* files (the SQL dump files) on one of the volumes that is being backed up by ShadowProtect. The solution in both of 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 being 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 Document the operating system (or OS) version and Networking Settings. If you virtualize a down server on the BDR, you will need to know the OS type (such as Server 2008 64-bit) and the 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.
* For 32-bit servers, check the *IRPStackSize* registry parameter. Heavily loaded 32-bit Windows servers may need to adjust the *IRPStackSize* parameter to ensure backups are reliable. See the StorageCraft Knowledgebase articles at <http://www.storagecraft.com/support/kb/article/14> and <http://www.storagecraft.com/support/kb/article/241>.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Installing the ShadowProtect Agent on each machine** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now that you have completed the preparatory work on each of the machines that will be imaged with a bare-metal backup, the second step in setting up bare-metal backups is to install the ShadowProtect agent on each computer to be backed up, either using a push install from the BDR or a manual install on the computer itself.

Before installing ShadowProtect on each of the machines, you need to determine what type of license the customer will be using: a monthly *MSP license* or a *Perpetual license*. Then you need to download the current version of the corresponding installer.

The MSP version of the installer can be downloaded from <https://msp.storagecraft.com/msp/login.jsp> by clicking **Download Product Installers** on the top left and then clicking **ShadowProtect for Managed Service Providers.** Note thatyou do *not* have to log in to download the software. Save the MSP download to *C:\Appliance\SetupPrograms\ShadowProtect\.*

If you are using a perpetual license, download the Legacy version of the installer from the *ShadowProtect Installers* section of the web page <http://www.storagecraft.com/software_update.php>. Save the Legacy version of the installer to *C:\Appliance\SetupPrograms\ShadowProtect\.*

For the push install, download all of the files in the *ShadowProtect Push Installer ISS Files* section of <http://www.storagecraft.com/software_update.php> and save them in the folder, *C:\Appliance\SetupPrograms\ShadowProtect*. Unzip the file to create a folder similar in name to *C:\Appliance\SetupPrograms\ShadowProtect\ShadowProtect\_ISS\_5.2.0.*

You should also download the current version of ImageManager to the folder, *C:\Appliance\SetupPrograms\ShadowProtect*.

On the BDR, install the new ShadowProtect and ImageManager versions you have downloaded, if they are newer than the currently installed versions. Remember to reboot the BDR after installing the new versions.

Now let’s overview how to install the ShadowProtect Agent on each machine to be backed up. After the overview, we will then provide detailed instructions.

This procedure requires a reboot of the computer that will be backed up, which can be scheduled as part of the install. Note that you can configure the backup jobs without rebooting, but you will *not* be able to start the initial backup until after the computer reboot has occurred.

For a small deployment (say, one to four agents) or for non-domain environments, the manual installation method is typically less work. For larger deployments, we recommend first using the push install method and then using the manual installation method if this fails.

The push install can be accessed on the **Management** tab of the ShadowProtect console. The agent can be installed with or without a user interface. Each agent can be configured and monitored through the **Management** tab in the ShadowProtect console on the BDR.

Alternatively, for manual installs, eFolder BDRs come preconfigured with a Windows share called SetupPrograms, located at [*\\BDR*](file:///\\BDR) *name or IP address\SetupPrograms*. This share is directed to the folder, *C:\Appliance\SetupPrograms\,* where you can manually run and install the agent on each computer that needs to be backed up.

With this high-level overview, let’s look at the specific actions you need to take to perform a push or manual install. First we’ll discuss how to do a *push* install of the ShadowProtect agent. Then we will discuss how to do a *manual* install.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing a “push” install of the ShadowProtect client**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The ShadowProtect Centralized Management Console that runs on the BDR can be used to connect to and install (or upgrade) ShadowProtect on computers throughout your network. This is called a "push install." There are two different versions of the ShadowProtect installer that you can use—one for each kind of license, either MSP or perpetual. If you bought a perpetual ShadowProtect license, you must use the legacy (non-MSP) installer. Otherwise, you should use the MSP installer.

Note that the MSP edition of ShadowProtect requires that a separate license key be used to activate each agent on each server or desktop that you are backing up. You can use the eFolder Web Portal to instantly request MSP license keys that you can use to activate your servers.

To perform a push install, follow these steps to install the agent onto one or more computers on your network:

First, make sure you have downloaded the current version of the ShadowProtect software and the Push Installer ISS Files as described in the previous section.

You may choose to install either the agent that does *not* include the user interface on the server being backed up (located in the *Agent* subfolder) or the Full client that *does* include the user interface (located in the *Full* subfolder). Whether or not the user interface will be installed depends on the ISS file that you copy into the folder, *C:\Appliance\SetupPrograms\ShadowProtect*. If you want to install the Agent-only version, copy the ISS file from the folder, *C:\Appliance\SetupPrograms\ShadowProtect\ShadowProtect\_ISS-5.2.0\Agent*, to the folder, C:\Appliance\SetupPrograms\ShadowProtect\, where you downloaded the file, *ShadowProtectSetup\_5.2.0.exe*. If you want to install the Full client, then copy the ISS file from the folder, *C:\Appliance\SetupPrograms\ShadowProtect\ShadowProtect\_ISS-5.2.0\Full.*

Next, click the **ShadowProtect** icon on the desktop of the BDR to start this program.

Then click the **Management View** tab, click the **Install** button, and click **Next**.

On the next screen, click the **Browse** button and browse to the directory, *C:\Appliance\SetupPrograms\ShadowProtect*, and select the executable file; for example, *ShadowProtectSetup\_5.2.0.exe*, and click **Open**. Then click **Next**.

You can now search for the computers on which to install the client either by the name of the computer in the domain or by hostname. If you are *not* joined to a domain, you must choose to search by hostname or IP address. If you are searching by domain and are logged in as a domain administrator, you do *not* need to enter credentials for the target machine. Otherwise, specify a Windows username and password that is valid on the target machine.

Check the **Discover services** box if you want the installer to attempt to log in to each machine to see if the ShadowProtect agent is already installed on that machine. Then click **Next**.

If you are searching by domain, the installer will display all computers on the domain. If you are searching by host name, it will only display one computer, if it is found. If you checked **Discover services**, it will attempt to log in to each machine. Note that if a version of ShadowProtect that is older than 4.0 is installed on the client computer, then upgrading is not an option. In this case, you must deactivate the current license, then manually uninstall the older version, reboot, and then perform the push install again or perform a manual install.

If you get the error message "The RPC server is unavailable," this typically means that a firewall on the client computer is blocking incoming connections to the ShadowProtectSvc.exe process. Configure the firewall on the client to unblock this process. If you are using the Windows advanced firewall on that machine, also make sure that the Windows Management Instrumentation (DCOM-In) rule is allowing connections. If you continue to have trouble, we recommend that you configure the firewall to accept all inbound connections from the BDR's IP address.

If you get an *access denied* error and the target computer is *Server 2008* or later or *Windows Vista* or later and if the target computer is part of a workgroup and *not* part of a domain and if UAC is enabled on the target machine, then a registry value *must* be changed on the target machine before you can do a push install or remotely manage the machine. This is a restriction of the Windows security model and *not* a restriction caused by ShadowProtect. To fix this, on the target machine, open *regedit*, navigate to the folder, *HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System*, create a new *DWORD* value called *LocalAccountTokenFilterPolicy*, and set this value to *1*. You must then reboot the computer. To avoid rebooting the computer twice—once after setting this registry value and again after installing ShadowProtect—manually install ShadowProtect after setting this registry key value so you can perform a single reboot to activate both.

Select the check box to the left of the computer names or IP addresses for the computers in the displayed list for which you want to install the ShadowProtect agent, then click **Next**.

The next page will optionally allow you to choose to automatically activate the ShadowProtect agents with a particular license key. ShadowProtect *MSP* license keys can be obtained from the Web Portal. ShadowProtect *Perpetual* License Keys can be obtained from the eFolder licensing team and can be purchased for multiple computers. Note that the *license key username* that you will enter during the push procedure is any descriptive name you want to use that can help ShadowProtect lookup your license key if needed. We recommend using your eFolder *online backup username* for the BDR here.

It is important to note that the MSP edition of ShadowProtect requires a separate license key for each activated server. If you are doing a large push install, choose *not* to activate the agents at this time, and then go back later in the ShadowProtect Console and individually activate each agent with a different license key.

Also note that if you are evaluating the BDR and have *not* yet purchased it, uncheck *Automatically activate installed agents*. You will have 15 days to evaluate the bare-metal backup process. Do *not* enter a license key.

Finally, this page allows you to immediately reboot the target machines after install or schedule a reboot to happen later.

Click **Next** to continue. The installer displays a summary of what it is about to do. Click **Next** again to begin the installation process. You will see the progress of the installation displayed for each agent.

At the end, the installer will tell you whether or not it could install the agent onto each computer that was selected. Those agents that were successfully installed or upgraded will automatically be added to the *Management* view in the ShadowProtect console.

After the agents have been installed, you can use the *Management View* to connect to and manage each agent from the BDR.

This completes the push install process. Next, we’ll discuss the manual install process.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing a manual install of the client** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you have trouble with the push install process, we recommend that you remote desktop into the desktop or server and manually install ShadowProtect.

There are two different versions of the ShadowProtect installer that you can use—one for each kind of license (MSP or perpetual). If you have bought a perpetual license, you must use the perpetual installer. Otherwise, you should use the MSP installer.

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 eFolder Web Portal to instantly provision MSP license keys to use to activate your servers.

To manually install the ShadowProtect client on a machine, first log in to the target machine.

Next, open the *SetupPrograms* Windows share on the BDR in Windows Explorer. For example, open *\\BDR name or IP address\SetupPrograms\ShadowProtect* and navigate to the desired install file that represents the type of license you have. Then run the *ShadowProtectSetup* executable.

Follow the steps that are presented to install the software. You must reboot the computer sometime after the install and before the initial backup. If you plan to reboot the server at a later time, you can still configure the backup, then pause the job until after you reboot the server, and then unpause the job to run the initial backup.

Next, on the BDR, open ShadowProtect, click the **Management View** tab, click the **Add** button, and enter the Server name, IP address, and Windows credentials that are needed to access the computer being backed up.

Highlight the server that you want to manage and click **Connect**. If you receive an “access denied” or a “The RPC server is unavailable” error message, follow the troubleshooting instructions in the previously discussed *push install* section of this video to configure your firewall to allow the management console to communicate with the agents.

This completes the manual install process.

It is very important to note that after installing the ShadowProtect agent or after a major version update, the computer *must* be rebooted so that the new or updated *filesystem monitoring driver* can become active. If you use the push install method, then the reboot can optionally be initiated manually at this time; alternately, it can be scheduled to automatically occur at a later time. Bare-metal backups will *not* be able to begin until the system has been rebooted.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring a continuous-incremental backup** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Now that you have installed the ShadowProtect agent on each machine to be backed up to the BDR, the third step in setting up bare-metal backups is to configure a continuous-incremental backup job to backup data from the source computers to a directory on the BDR that is unique to each computer. If you plan to backup the data off-site to eFolder cloud or a remote server, we recommend that you place the ShadowProtect backup images in a subdirectory of *X:\VolumeImages* (the *VolumeImages* share on the BDR). If you have backup images that you do *not* want to be taken off-site, we recommend that you place the backup images in a subdirectory of *X:\LocalVolumeImages,* which is the *NotBackedUp-LocalVolumeImages* share on the BDR.

Follow these steps for each computer that you need to configure. First, log in to the BDR, open the *ShadowProtect Management Console*, and click on the **Management View** tab.

Next, select the appropriate computer from the list of configured computers by left-clicking on the computer. If you do *not* see the computer, please follow the push install process or manual install process to add it to the Management Console.

Next, if the Management Console indicates that it has not yet connected to that computer, click the **Connect** button to connect. After you are connected, click the **Manage** button to activate the management user interface for that particular computer. The Management Console will now show several additional tabs across the top of the screen. The name of the machine that you are managing is shown in each of the new tabs and in the ShadowProtect title bar.

Next, on the BDR, open Windows Explorer and create a new empty directory on the *X:* drive that will hold the bare-metal backup data for this specific computer. Note that you should create a different directory for each computer you are backing up.

If you plan to backup the bare-metal backup images off-site, then be sure to create the new directory as a sub-directory of *X:\VolumeImages*—for example, *X:\VolumeImages\ExchangeServer*. If you do *not* plan to backup the bare-metal images offsite, create a new subdirectory of *X:\LocalVolumeImages*—for example, *X:\LocalVolumeImages\ExchangeServer*.

Next, with the new empty directory created, return to the ShadowProtect Management Console and click the **Destinations** tab. Then click the **Add** button. In the dialog box that appears, enter the UNC path of the folder in the appropriate share of the BDR: *VolumeImages* or *NotBackedUp-LocalVolumeImages*. For example, you might enter [*\\BDR\VolumeImages\ExchangeServer*](file:///\\BDR\VolumeImages\ExchangeServer). Also enter the credentials to access the share on the BDR; these are *not* necessarily the same as the credentials that are required 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. Ensure that the checkbox labelled *Verify destination access upon clicking OK* is checked. When you are done, click **OK**. You will be notified if you have entered the UNC path and credentials incorrectly.

Next, click the **Backup Jobs** tab and click the **New** button to start the wizard. Click **Next** to go to the *Volume Selection* page. We recommend that you select all volumes, including any unlabeled volumes that are common with Server 2008 and later, unless you are absolutely sure that something does *not* need to be backed up. Then click **Next**.

On the next page, select the *network destination* that you created previously in the **Destinations** tab; then click **Next**.

On the next page, configure the backup schedule. Select **Continuous Incrementals** in the *Schedule* section and choose the backup schedule and the frequency, which can be as often as every 15 minutes. If you want it to backup around the clock, set the stop time in the *Stop taking backups at this time* field to one minute before the start time in the *Start taking backups at this time* field. It will then wrap around. Then click **Next**. Note that if *Continuous Incrementals* is grayed out, there is probably another job already defined on the computer. You might need to edit or delete the existing job.

On the next page, set the compression mode to *High*. High gives you a 50% compression, while *Standard* gives you a 40% compression. Optionally, set a password to use to encrypt the image files. As a best practice, we recommend that you enter a password to encrypt the ShadowProtect image files so that they are protected while they are stored on the BDR and if they are ever archived to a USB drive. Note that this password can only be set when the job is first created. Note also that the image files will always be encrypted by the eFolder software when the files are backed up to the eFolder Cloud regardless of whether you set a password here.

Also, if you are replicating data to another BDR or server, you should strongly consider encrypting the bare-metal backup images, especially if the target replication device is *not* in a secure location. If you decide to encrypt your ShadowProtect images, then we highly recommend using the same password here that you set for your eFolder Backup Manager pass phrase. This keeps things consistent and allows you to use the secure pass phrase recovery mechanism of your online backup account. Be forewarned, though, that if you encrypt the data using a password, you *must* know the encryption password to restore your data. Keep the password well documented in several places where it will be available in the event of a disaster so you can restore your data.

On this same options screen, you can also name the backup job. We recommend that you enter a name if you will have more than one job.

There are two settings to consider when clicking the **Advanced** button. On the **Backup** tab, you might want to change the performance throttling if you are backing up a very busy server. On the **Image** tab, we recommend that you enable the **Enable Write Caching** to create a buffer between the computer and the data destination.

You can click the **Execute Now** button before completing the wizard or you can click the **Execute** button on the **Backup Jobs** tab to start the initial backup. Note that for the backups to run successfully, the computer must have been rebooted prior to clicking either the **Execute** or **Execute Now** button. The initial backup may take some time depending on how much data you have. Typically, data throughput rates are between 10 megabytes per second and 80 megabytes per second, depending upon your network, processor speed, and whether data encryption is enabled.

You will now need to configure the ShadowProtect ImageManager on the BDR. The use of the ImageManager is required for continuous incremental backup jobs. We will discuss how to do this next.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the ShadowProtect ImageManager program** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The fourth step in setting up bare-metal backups is to configure the *ShadowProtect ImageManager* that is running on the BDR to monitor the directory that contains the bare-metal backup images for the computer you are backing up. This is crucial to monitor the integrity of the backups and to collapse incremental files to save storage space, both on the BDR and off-site.

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

The first function is *delta consolidation*. It consolidates the incremental backup deltas on a daily basis by 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 full recovery chain, consisting of 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. We recommend taking a new base image every two to three years.

The second function of the ShadowProtect ImageManager is image verification. The integrity of the data stored locally on the BDR is periodically verified. Any errors will be reported in the *System Status* screen in the eFolder Backup Manager software, in the eFolder Web Portal, and through any configured email and partner notifications, as configured in the Backup Manager and in the eFolder Web Portal.

To configure the ImageManager global settings, start the ImageManager by double clicking the **ImageManager** icon on the desktop or selecting it in the *Start* menu. The login dialog box appears. The default password for ImageManager is *password* and is frequently set to *imagemanager*.

After logging in, choose a time when ImageManager should collapse the deltas by clicking the **Agent Settings** button on the left side. Then choose the time when processing should occur.

Note that you should always choose a time after midnight, such as 12:05 a.m. ImageManager is hard-coded to consolidate files from the previous calendar day. If you choose a time before midnight, such as 7 p.m., the consolidated daily file will be for the day that ended 19 hours previous. This causes your off-site backups to be at least 24 hours behind. Note also that you should configure the eFolder Backup Manager to start *its* processing about one hour *after* the ImageManager starts to consolidate the files (or even later when ImageManager is managing five or more servers). This will allow the ImageManager to complete its work *before* the off-site backups and replication start.

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

It is also extremely important to note that, if you are performing off-site backups, you must set the number of days to keep consolidated daily image files (the ones that have –cd in their filenames) 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 are backed up offsite. The minimum settings are 7 days of intra-daily files, 35 days of daily files, and 35 days of weekly files. You can set them to a longer retention if you have enough drive space.

The next option is *Cleanup consolidated monthly image files (-cm)*. This enables the *Consolidated Rolling* feature that consolidates monthly files older than the value that you have set and combines them into a single Consolidated Rolling file (-cr). This allows you to control the amount of space used by the images by limiting the number of monthly files maintained. The advantage of this feature is that it controls the space on the local drive and the Cloud backup.

The next option is *Move all consolidated image files to a subdirectory instead of deleting them*. With this option, instead of deleting the daily and weekly files, ImageManager moves them to the incremental folder where they can eventually fill up the hard drive. We recommend that you clear this option.

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.

While still logged into ImageManager, on the left side, top option, click the **Start Managing Folder** button. Next, click the “***...”*** (or ellipsis) 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 the *X:\VolumeImages* directory itself. You can leave the other options at their default settings.

It is very important to note that 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. You will use the **Start Managing Folder** button three times to add each of the three folders separately to ImageManager.

Next, optionally configure agent-specific retention policies. If you need to override the global data retention policy for a specific folder, select the folder and then click the **Retention Settings** button on the left side. The *Retention Settings* dialog box appears, where you can customize how long you want to retain each type of image file. Again, if you are performing off-site backups, you *must* set the number of days to keep consolidated daily image files—the ones that have *–cd* in their filenames—to at least 35 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 are backed up offsite.

ImageManager has now been configured to monitor and manage each folder for each protected agent.

This completes step 5 of installing and configuring the BDR, which was setting up other computers on the network to be backed up to the BDR with bare-metal backups.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 6.** **Setup off-site monitoring and backups** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 6 in installing and configuring an eFolder BDR for ShadowProtect is setting up the eFolder Backup Manager for backups and off-site monitoring, which is establishing a connection between the BDR appliance and an online backup account in the eFolder Web Portal. This is done by configuring the Backup Manager on the BDR with the appropriate backup account credentials that you verified in Step 3. Note that *each* BDR must be connected to the Web Portal using a separate online backup account. This account provides integration with the Web Portal and is required even if you will *not* be backing up data to the eFolder Cloud so that licensing, monitoring, notification, and reporting continue to operate correctly. For additional training on how to create an account in the eFolder Web Portal, see the “Create Account Wizard” section of the related video in this series entitled, *Overview of the Web Portal*.

The Backup Manager that was preinstalled on the BDR comes preconfigured to backup the bare-metal backup images in *X:\VolumeImages*. It is also preconfigured to monitor—but not upload data—for bare metal backup images in *X:\LocalVolumeImages*.

On the eFolder BDR, both the *VolumeImages* and *LocalVolumeImages* folders are preconfigured with a special *policy,* called *Backup ShadowProtect Images*, to properly monitor and backup the ShadowProtect bare-metal images. You must store all ShadowProtect data that you want to backup to the eFolder Cloud in a sub-directory of *VolumeImages*. Otherwise the data may *not* be properly backed up and may *not* preserve a full chain of incrementals. If you add another folder in addition to the *X:*\*VolumeImages* folder to the backup set that contains ShadowProtect data, be sure to add the folder in the **Folders** tab, assign it to use the *Backup ShadowProtect Images* policy, and configure the properties in the **Properties** tab, to ensure that the proper data is backed up and monitored.

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

The bare-metal backups generate a base image file and thereafter generate incremental files—for example, an incremental file every 15 minutes. Once per day, the ShadowProtect ImageManager consolidates these incremental files into a single daily incremental. Each week, ImageManager consolidates daily incrementals into weekly incrementals. Each month, ImageManager consolidates weekly and daily incrementals into monthly incrementals, and optionally consolidates monthly incrementals into a single rolling incremental. The Backup Manager comes preconfigured on the eFolder BDR to backup the base image, the daily incrementals, the monthly incrementals, and the rolling incremental.

Each BDR must establish a connection with an online backup account in the Web Portal, 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 account credentials, create the pass phrase, choose a backup schedule, adjust the retention of deleted files in the eFolder Cloud, and set bandwidth throttling options.

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-Converter-Wizard-x64.exe* located in the *C:\Appliance\Software* directory of your BDR. Running the wizard is very important because it ensures that the backup policies that come preconfigured on the BDR are transferred to the newly branded version of the Backup Manager.

All BDR services (monitoring, notifications, licensing) require that the appliance be associated with an online backup account. To do this, follow these steps: First, click the **Backup Manager** icon on the desktop of the BDR to start the Backup Manager. Click the **My Account** button on the left side, enter your online backup account credentials, and click the **Test Connection** button. If you have a temporary password, you will be prompted to change it to a permanent password. Note that your *password* is not the same as your *pass phrase*. The password of an account can be changed or reset; however, the pass phrase should not be changed once it is configured unless you are ready to create a new preload drive.

Next, click the **Create Pass Phrase** button and follow the prompts to setup your pass phrase. Note that it is *not* required that you create a pass phrase if you are *not* backing up data to the eFolder Cloud. However, you *must* set up a local-disk or local-server backup job in the Backup Manager for reporting data to be sent to the eFolder Web Portal on the status of the BDR and the integrity of the *LocalVolumeImages* files. This is because certain reporting data is sent to the eFolder Cloud only when a backup job is completed.

The next step in setting up off-site monitoring and backups is to configure the **Properties** tab in the **Folders** page of the Backup Manager. To navigate to the **Properties** tab, highlight the *VolumeImages* folder in the folder list in the **Folders** page and click the **Properties** button on the right. The **Properties** tab appears in a new window.

In the **Properties** tab, verify that the *Number of Days to Keep Historical Versions* and *Number of Days to Keep Deleted Files* fields are both set to seven days. The deleted files will be retained in the eFolder Cloud for seven days after ImageManager deletes them. Click the *Disable Open File Backup* checkbox one or more times until *Yes* is displayed. Then click **Save** to close the *Properties* window.

Next, click the **Schedule** button on the left side, click the **Daily** option, make sure that all seven days of the week are checked, and select a starting time for the backup. We recommend choosing 1:00 a.m. which is about one hour after the time you configured ImageManager to consolidate the incrementals backups. Then click **Save**.

Next, click the **Options** button on the left side, click the **Bandwidth** tab, and optionally adjust bandwidth constraints as desired. Adjust the *Business hours* starting time to an hour *before* and the ending time to an hour *after* the employees are in the office. Set the *Usage Mode During Business Hours* field to the desired bandwidth level—Max, High, Medium, or Low. Adjust the corresponding bandwidth to about 20 to 25 percent of the site’s upload speed. Then set the *Usage Mode During Off Hours* field to *Max* if the customer will *not* be using the Internet for VPN after hours. If they need the Internet after hours, then set the mode to *High* and adjust the *High Bandwidth Usage* field to 75% of their upload speed. Note that you should test the Internet bandwidth with a tool like *speedtest.net* to confirm the upload speed. Often a 20 megabit pipe will only have a 2 megabit upload speed.

Next, you can optionally adjust email notifications as desired. To do this, click the **Notifications** tab in the *Options* page. If you want to receive email notifications for this BDR, leave the *Email Address* field set to *(auto)*, which sends email notifications to the configured email address for the BDR account in the eFolder Web Portal. Then ensure that the account is configured with *your* email address or any other email address to where you want the notifications to be sent.

If you are a reseller and want to setup standard notification rules, we recommend using the *Partner Notifications* feature of the reseller’s 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 by adding a semi-colon and their email address after the *(auto)* in the *Email address* field on the *Options* page and rely on the Partner Notifications feature in the Web Portal for your own notifications.

Note that the BDR service plan only allows bare-metal backups and Email Archiving data to be backed up off-site. If you want to backup other kinds of file-level data that is on the BDR, you must create an *additional* settings profile in the Backup Manager and configure an *additional* online backup account (either *Basic* or *Select*). To create an additional settings profile, in the Backup Manager, select *Switch Profile* in the **File** menu at the top of the screen. Then click the **plus (+)** button to add a new profile. Refer to the Backup Manager *Help* and user documentation for additional information.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing the initial backup** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next, you perform the initial backup. If you plan to backup the data on the BDR to the eFolder Cloud, then the initial base image of the individual servers must each be uploaded to the cloud. The data can either be uploaded over the Internet, or a USB preload can be used to encrypt and copy the data onto a USB disk which is then mailed to our data center for processing. Unless you have a fast connection (say, greater than 5 megabits per second), performing a USB preload is recommended if you have more than 50 gigabytes of data. The process consists of putting the account into maintenance mode, preparing the USB disk, initiating the preload operation, shipping us the drive, and waiting for it to be processed. For further information on how to perform a USB preload, see the section of this video entitled, *Performing a USB preload*, or contact eFolder Technical Support.

If you are uploading the initial base image over the Internet, no extra configuration is needed. 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, after the initial full backups have completed, 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* screen on the line that starts with *Amount to backup in all folders.* 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.

Finally, for additional training on installing and configuring the Backup Manager, see the video entitled, *Installing and Configuring the Backup Manager* or refer to the *Getting Started Guide* in the **Help** menu of the Backup Manager.

Next, we’ll go through the steps for performing a USB preload.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing a USB preload for off-site backups to the cloud** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

USB preloads are useful when the total amount of data to backup is too large to quickly backup over the Internet, such as when you have over 50 gigabytes of data to back up over a 2 megabit upload speed Internet connection. Instead, the initial backup can be sent on a USB disk. After the preload is completed, only the much smaller incremental changes need to be sent over the Internet.

USB preloads can be performed on a brand new account or on an existing account. If it is performed on an existing account, all previous data for that account will be replaced with the contents of the new USB preload.

We recommend that you allow image backups to run locally for at least a few days before performing a USB preload. This will allow you to determine if the consolidated daily files are larger than expected. You can address this issue and create a new base image before creating the preload.

The following instructions are intended for partners and resellers. If you are an end-user, please coordinate the USB preload operation with your IT provider.

First, as soon as you have finished configuring the account credentials and setting up your pass phrase in the Backup Manager, log in to the eFolder Web Portal and put the account into *maintenance mode* by right clicking on the account and selecting **Put into Maintenance Mode** in the *Account Status* option. It is very important that you do this step as soon as you have finished configuring the Backup Manager to prevent it from sending the initial backup over the Internet. It is also important to note that, after the account is in maintenance mode and the USB disk is on its way for processing, you must *not* take the account out of maintenance mode. If you do, you will have to redo the USB preload.

Next, wait for all of the bare-metal backups to finish locally, meaning wait until all initial bare-metal backups have stored their data onto the BDR.

Next, prepare the USB drive. Buy an external USB drive that is large enough to contain all of the base images. Any external USB drive will do, as long as it can be connected using USB. Please note that eSATA is *not* supported. We recommend and support USB drive docks that allow a bare 3.5 inch SATA drive to be connected via USB. You can then ship us just the 3.5 inch bare drive for processing. However, make sure you format the USB drive with the NTFS file system. Many external drives come formatted with FAT32 out of the box. If this is the case, perform a quick format on the drive for NTFS or you will experience problems. Plug the USB drive into the BDR appliance. Windows should recognize the drive and show an additional drive letter for the external device.

Next, perform the initial backup to the USB disk. To do this, open the Backup Manager. Click **File** on the menu bar and select *Preload Remote Backup*. Then specify a new empty directory on the external USB disk. When you are ready, click the **Start** button. It will begin what looks like a remote backup, but in reality the data is being encrypted and backed up to the USB disk. Note that if you have already backed up some of the data over the Internet, it will warn you that you are about to start over and take a full backup. All previously uploaded data, including historical versions of files, will be replaced with the new full backup image on the USB preload disk. Note also that you can use the same USB disk to preload data for multiple accounts and multiple BDRs. For best results, make sure you use a separate top-level directory on the external USB disk for each account.

Wait for the USB preload job to finish. Depending on the type of USB drive, data is typically sent to the USB drive between 5 megabytes to 15 megabytes per second, which is 18 gigabytes to 54 gigabytes per hour. You can run the preload again, if you are not able to stay until the initial preload has completed. You can restart it again later, and it will copy new and additional files that were not copied previously.

The next step is to open a ticket with Technical Support to track the preload drive as it is processed. Include the *username* or, more preferably, the *account number* of the eFolder account of the BDR with the new ticket request. You will receive a reply with the mailing address and shipping instructions for the USB preload. Each new preload drive must be tracked with a new ticket, as this is this method that our data center engineers use to track the process all the way through returning the drive. In the shipping box, include the external drive and all cables needed to operate the drive, especially the power adapter. Also be sure to label the drive and include a prepaid return shipping label so we can return the drive back to you. After you have shipped the drive, reply to the email of your support ticket and include the tracking number.

Note that throughout all of this process, failure to confirm the mailing address, include the appropriate USB or power cable, include a return shipping label, or email the tracking number will result in processing delays. Please be sure to follow all instructions carefully so we can better assist you. Remember also to *not* take the account out of maintenance mode. This will be done 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. For this reason, we have measures in place to make sure that preloads are processed quickly.

Next, wait for the USB preload to be received and processed. Our technicians use the tracking number that you emailed to Technical Support to receive the drive and process it in a timely fashion. Failure to send a tracking number will result in a delay. Depending on how much data is on the drive, the preload should be processed within one to two business days of its receipt. After loading the data, the data center technician will erase the preload drive and ship it back to you as quickly as possible using your prepaid shipping label. After the preload has been processed, Technical Support will take the account out of maintenance mode and update the ticket, which will 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 start time. 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.

This completes step 6 of installing and configuring the BDR, which was setting up off-site monitoring and backups.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 7. (Optional) Setup cross-site replication** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 7 in installing and configuring an eFolder BDR for ShadowProtect, which is optional, is setting up cross-site replication. If you are only using Cloud or Local Disk backups, then skip this step and go directly to step 8 by clicking **Step 8** in the *Contents* section of this training video on the left side of the course window.

This optional step involves configuring the BDR as a replication source or target for cross-site replication. This allows the data on one computer to be replicated to another computer that is running the *Local Backup Server* software that is included with the Backup Manager. The target server could also be a Windows server in a non-eFolder cloud, such as a Terremark server instance. In other words, you can replicate data to a non-eFolder cloud, to your office, to your data center, or to the client’s remote office.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**A comparison of replication versus backup** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next, let’s compare replication versus backup. There are advantages and disadvantages of replication and of backup. It is important to understand the differences and what each is best suited to do, although replication and backup can both be used at the same time for maximum data protection.

Backup is best suited for long-term data retention of file-level data, pristine data integrity, and the retention of historical versions and deleted data. Replication is best suited for quick access to data on the target device, including fast virtualization of servers.

Let’s summarize some of the differences between replication and backup.

Regarding the format of data on the target device, which could be a BDR or local backup server, with replication, 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 with a ShadowProtect encryption password on the source BDR, it will *not* be encrypted on the target BDR. Whereas with backup, the data is stored in a proprietary, compressed, and optionally encrypted format.

Regarding assessing the data, with replication, replicated data can be accessed immediately without having to perform a restore operation. With backup, data must first be restored using the *File Manager* tool in the Backup Manager before it can be accessed. The File Manager decrypts and decompresses the data from the backup storage.

Regarding the speed of virtualization, with replication, bare-metal backups can be instantly virtualized. With backup, bare-metal backup images must first be restored to a computer using the File Manager tool in the Backup Manager before they can be virtualized.

Regarding historical data, it is important to note that 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. With backup, backup supports storing as many historical versions of a file as are desired.

Regarding data corruption, with replication, if data is corrupted on the source BDR and is *not* detected, the corrupted data will be replicated to the target BDR. Bare-metal backup images are always checked for corruption before they are replicated, mitigating the risk. With backup, 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.

Click the **Resources** tab of this training program to download the document entitled *A Comparison of Replication and Backup* that summarizes these differences.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the BDR for replication** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To configure a BDR for replication, you will need to configure both the replication target and each replication source. The replication *target* is the machine you are replicating data to, such as a server in your office or a data center or at your client’s remote office. The replication *source* is the machine you are replicating data from, such as a BDR.

Configuring cross-site replication involves four main steps. The first step is configuring the replication target to receive replicated data. The second step is configuring each replication source, as there may be more than one. The third step is configuring the ImageManager on the replication target for each replication source. The fourth step is configuring data monitoring on the replication target, which can also be used to backup data on the replication target to the cloud and report the integrity of the image files. Let’s walk through each of these four steps in detail.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the replication target to receive replicated data** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

On the Windows computer that will act as the replication *target*, install the Backup Manager software if it is not yet installed. Then start the Backup Manager and verify that you have the most current version of Backup Manager by clicking the **Software Updates** tab on the ***System Status*** page.

As you configure each of the *source* computers, verify that the version of Online Backup Manager is at least version 3.7.8 by clicking the **Software Updates** tab on the ***System Status*** page of the Backup Manager. It is recommended that you upgrade all the servers to the same version, preferably the current version.

To configure the replication target, select *Local Backup Server* on the **Tools** menu in the Backup Manager. Note that, for future ease of access, you can create an icon for the Local Backup Server application by opening Windows Explorer, browsing to the folder where the Backup Manager is installed, right clicking the branded *LocalServerManager* file, creating a shortcut, and then dragging the new shortcut to the desktop.

In the Local Backup Server software, on the **Configure** page, enter the target location where the replicated data will be stored in the *Local Storage Repository Store Path* field and then enter the appropriate account credentials in the *User Name* and *Password* fields for the replication target machine. If the replication target is a BDR, then you should use the account credentials you created specifically for that BDR unit, not the credentials that you are using for the replication source computers. If the replication target does *not* yet have an eFolder backup account, then create a new account in the eFolder Web Portal and use those new account credentials. Click the **Test Connection** button at the top right corner of the *Configure* window. The message, *Connection Verified,* will appear. If instead an error message appears, contact eFolder Technical Support to resolve the issue before proceeding.

Note that if the target Local Backup Server will only be used by a single *customer,* as eFolder defines *customer*, then the account must belong to the same *customer* in the eFolder Web Portal as all of the other accounts being used for replication sources to that BDR. If the target *Local Backup Server* will be the target server for multiple customers, please verify that the account is assigned the *Multitenant Network Server* service plan.

Next, click the **Options** button on the left side and make sure that the *Allow Replication* checkbox has been checked and displays *Yes*.

Finally, configure your network, including your routers and 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the replication source machine** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step two, configure the replication source machine, is a two-part process. You will first configure the Backup Manager on the source machine so that it will *monitor* the replication process. Then you will configure the Backup Manager on the source machine so that it is setup for the actual *replication*.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the Backup Manager to monitor replication** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Begin by installing the Backup Manager on the source machines if in has not been previously installed. Note that the Backup Manager *must* be installed and configured on each replication source machine; it will be used for authentication, replicating the data, and monitoring the success of the replications. The Backup Manager on each source machine can also be used to send data to the eFolder cloud and/or to a local disk.

To configure the Backup Manager to monitor the replication process on each source machine, complete the following six steps.

First, on the desktop, click the **Backup Manager** icon to start the Backup Manager.

Second, click the **My Account** page. If the account credentials have not been previously configured, enter the account credentials for this machine’s backup account and click the **Test Connection** button. If you have a temporary password, you will be prompted to change it to a permanent password. Note that your *password* is *not* your *pass phrase*. The password for an account *can* be changed or reset; however, if you later change the pass phrase after the original pass phrase has been used in backing up data, then both pass phrases would be required to restore your data: the old pass phrase for files backed up previously, and the new pass phrase to restore data backed up after the pass phrase was changed. To avoid this, many partners perform a new full backup or preload after changing the pass phrase so that all files can be restored with the new pass phrase. Each of your customers should have a unique pass phrase.

Third, if you have already created a pass phrase and the **Change Pass Phrase** button appears on the right side, you do not need to alter the pass phrase. However, if you have *not* created a pass phrase and the **Create Pass Phrase** button appears, then click the button and follow the prompts to setup your pass phrase.

Fourth, if you do *not* plan to send data off-site to the eFolder cloud, click the **Folders** page and *uncheck* the online backup destination column, which is in the column with the **earth** icon, for the *VolumeImages* folder. Note that by default the *LocalVolumeImages* folder will be monitored but *not* backed up offsite, and you should leave this folder checked if you are storing images in the *LocalVolumeImages* folder. If the *LocalVolumeImages* folder is being replicated to the target server, you can clear the checkbox in the middle column (the one with the icon of the computer and network cable underneath it) for the *LocalVolumeImages* folder.

Fifth, click the **Schedule** page, set the frequency to daily, or once per day, and choose a time. We recommend choosing a time in the early morning that is one hour after the time you have set in ImageManager to consolidate the incrementals.

Sixth, click the **Options** page; then click the **Bandwidth** tab and adjust bandwidth constraints as desired.

Finally, note that the BDR service plan only allows bare-metal backups and Email Archiving data to be backed up to a destination other than the eFolder Cloud. If you wish to backup or replicate other kinds of file-level data that is on the BDR, such as individual files or Exchange files, you will need to create an *additional* settings profile and create and configure an *additional* online backup account with either the *Basic* or *Select* service plan. After you have created the additional account, to create an additional settings profile, start the Backup Manager on the source machine and select *Switch Profile* on the **File** menu. Then click the plus **(+)** icon to add a new profile, then highlight the new profile and click **Switch**. Finally, configure the new profile for the files you want to backup with the new service plan.

This completes configuring the Backup Manager on the source machine so that it can monitor the replication process. Repeat this procedure on each source machine.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring the Backup Manager for replication** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Next, configure the Backup Manager on each source machine so that it is setup for the actual replication.

To begin, open the Backup Manager on the source machine, click the **My Account** page, and verify that the account credentials are properly configured, or, if they have *not* yet been entered, enter the account credentials assigned to the source computer. The account credentials you use for this machine should be different than the account credentials you are using on the replication target.

Next, if you are replicating or backing up to a target *server* outside of the eFolder Cloud, enter the IP address or DNS name of the target server in the *Local Server* field.

Next, click the **Folders** page, click the **Add** button, and select *Add Replicated Folder*. The Backup Manager 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*—and click **OK**.

Finally, choose a replication policy. The replication policy affects which files will be replicated to the target. You have three choices.

The first choice is *ShadowProtect Daily*. Selecting this choice will replicate ShadowProtect base image files (or *\*.spf* files) and ShadowProtect daily image files (or *\*-cd.spi* files). It will *not* replicate weekly (or *\*-cw.spi* files) or monthly (or *\*-cm.spi*) image files that are created by the consolidation process on the replication target.

The second choice is *ShadowProtect Realtime*. This will replicate ShadowProtect base image files (or *\*.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 in the Backup Manager so that replication is performed multiple times per day.

The third option is *(custom policy)*. Choose this option if you are *not* replicating ShadowProtect data. By default, this option replicates everything.

Note that 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 (or *\*-cd.spi* files) 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. If you plan to use the Real Time Replication policy, then you would also need to temporarily add an *include \*-cd.spi* policy rule. After the initial replication has completed, you can then remove this policy rule. This extra step is normally not needed. It is only necessary if the source computer has been consolidating the backup chain for a while, meaning long enough for some of the daily image files to have been deleted.

Also note that if you are replicating ShadowProtect data, you *must* configure the ShadowProtect ImageManager software on both the replication source and the replication target to consolidate the backup images. We strongly recommend that the retention settings be identical on both the source and target servers. If you do *not* configure ImageManager on both servers, your backups will *not* be verified, you will run out of disk space, and your backups will have an increased risk of becoming damaged and unusable. Setting up the ImageManager is *not* optional and *must* be configured to ensure proper data protection.

Note that each folder that contains ShadowProtect images must be added individually to ImageManager on both the source and target servers, to consolidate and verify the image chains. It is *not* sufficient to add the parent directory. You must add each subdirectory individually. We will discuss how this is done shortly.

Next, on the **Folders** page, select the middle column (the one with the icon of the computer and network cable underneath it) for the folder that you will be replicating.

Finally, use the **Local Network Backup** tab on the **Schedule** page in the Backup Manager to set the local server backup schedule. If you are using the ShadowProtect Daily policy, replication should begin about one hour after the ImageManager processing is configured to begin. If you are preforming real-time replication, you may want to schedule replication for several times per day so the target is as current as possible. Otherwise, choose an appropriate schedule. Usually once per day is sufficient.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring ImageManager on the replication target** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The third step in configuring the replication target is to configure ImageManager on the replication target server. If you are replicating ShadowProtect backup data, then you *must* setup the ImageManager on the replication target to manage each folder that contains replicated backup images.

To perform this configuration, log in to the replication target server, open the *Backup Server Manager* program, open the *Configure* page, and check the *Store Path* field to confirm that it shows the top-level folder where you will store replicated data. For example, the location might be *X:\ReplicatedData.* Use Windows Explorer to browse to this folder and identify the folder path(s) that need to be added to the ImageManager program. Here’s how.

The top-level folder (in this example, *X:\ReplicatedData*) will contain three folders that are each named after your brand ID. For example, if your brand ID is DataProtection, then your top-level folder will contain three folders beginning with DataProtection. You can ignore the two folders that end in *–del* and *-sf.* The replicated data will be contained within the folder that is named after your brand ID, which, in this case, is *X:\ReplicatedData\DataProtection*.

In your brand’s folder, there will be one subdirectory for *each* replication source that is storing data on this replication target. The subdirectory names are the account numbers of each replication source, such as *X:\ReplicatedData\DataProtection\12345001*. What do these source replication subdirectories contain? They contain, among other things, one subdirectory for each top-level folder that is displayed in your folders list in the **Folders** tab of the Backup Manager on the source server. For replication, *VolumeImages* is the folder that contains the ShadowProtect data.

Most of the folders inside *VolumeImages* contain metadata needed to efficiently replicate the data. The folder that contains the actual replicated data is the *replicated-data* folder.

For example, if we are replicating ShadowProtect backup images for three servers with the names ExchangeServer, PrimaryDomainController, and SQLServer, we will see three folders, one for each server.

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

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

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* backup of ShadowProtect data to the eFolder Cloud, where you are required to keep at least 35 days of daily delta files.

Notwithstanding, we highly recommend keeping at least 35 days of daily delta files even when you are using replication. The default for ImageManager is 14 days. **We *strongly* recommend that you set the *same* ImageManager settings on both the source and target servers.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuring data monitoring on the replication target** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The fourth step in configuring the replication target is to configure *data* *monitoring* on the replication target. Note that in addition to monitoring the data on the replication target, you can also backup the data on the replication target to the eFolder Cloud, to another target local server, or to a local disk.

Even if you do *not* want to backup the replicated data further, if the target server has *replicated* ShadowProtect data, then we highly recommend that you configure the Backup Manager to monitor the integrity of the replicated ShadowProtect backups.

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 Local Backup Server Manager program. These credentials should be unique to this replication target server.

Next, in the Backup Manager, click the **Folders** button on the left side and add the folder that is configured as the *Store Path* on the *Configure* page of the Backup *Server* Manager. As this can seem a little confusing, let’s demonstrate how this is done. Returning to our previous example, where the location of the store path on the target server is *X:\ReplicatedData*, the first step is to log in to the replication target server, open the *Backup Server Manager* program, open the *Configure* page, and note the folder in the *Store Path* field. In this example, the location is *X:\ReplicatedData.* At this point, you are finished using the Backup Server Manager, and it can be closed.

Next, configure remote backups, site-to-site backups, or local disk backups like you normally would for other backups in the Backup Manager. This might include setting up an encryption pass phrase and setting the relevant backup schedules. Note that when you are using the Backup Server Manager program and the Backup Manager on the same server, we recommend that you use the same *user name* for the eFolder account in each program.

As part of this configuration of the Backup Manager, to add the replicated data to the list of folders to backup or monitor in the Backup Manager on the target server, click the **Folders** button in the Backup Manager on the replication target, click **Add** in the upper right and select *Add Folder*. Drill down the directory structure on the left to the *X:\ReplicatedData* folder*.* Click on the folder to select it, then click the green arrow button to move it to the right side to the list of folders and files to be backed up. Finally, click **Save**. The folder should now show up in the list of folders on the *Folders* page.

Click on the folder to highlight it and then click the **Properties** button on the right side. Scroll down to the *Advanced* section and click the *Do Not Backup Data* field until it is set to *Yes*. Because the replication target contains ShadowProtect data, make sure that all of the ShadowProtect integration settings are enabled in the *ShadowProtect Integration* section of the Properties window.

If you do *not* see these folder options, then 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, click the **Backup** tab of the **Options** page, click on the blank field to the right of the *Full Path to sbrun.exe*field label to bring up the file browser dialog box, browse to the directory that contains the *sbrun.exe* file and select the file. The default location for this file is *C:\Program Files (x86)\StorageCraft\ShadowProtect.* With the folder selected, click **Open**. The name of the file is now displayed in the *Full Path to sbrun.exe* field.

Repeat these steps for the *Full Path to the ImageManager* field. Note that the default location for the *ImageManager.exe* file is *C:\Program Files (x86)\StorageCraft\ImageManager*.

This completes configuring the data monitoring on the target server.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Performing a USB preload for replicated data** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

You can optionally perform USB preloads for replicated data. This means that the initial replication is made to a USB drive, which is then physically transported to the replication target and loaded on the target, rather than performing the initial replication over the network.

Performing a USB preload for replicated data is quite similar to the process of performing a preload for online backups. First, you configure the account in the Backup Manager (see the section, *Step 6: Setup off-site monitoring and backups,* in this video), but instead of starting the initial replication, perform the following steps.

First, use the eFolder Web Portal to put the account into maintenance mode by right-clicking on the desired account and selecting *Put into Maintenance Mode* in the **Account Status** menu option.

Next, in the Backup Manager on the replication source, click **File** in the menu bar at the top and select *Preload Remote Backup*, even though we will be preloading a replication, not a cloud backup. Enter the path to the external USB disk and click **Start**.

Next, you should be prompted to select the backup destination for your preload. Click the **Local Server** button, if that is what is displayed. Then click **Start**. If you are *not* prompted to select the backup destination, make sure that you have properly configured the *Local* *Server* field on the *My Account* page in the Backup Manager and clicked the middle column (the one with the icon of the computer and network cable at the top) for the folder in the *Folders* page. Then click **Start**.

The initial replication begins and the data is written to the USB disk. Wait for the job to finish. Note that you can perform the preload more than once, if you are not able to transport the USB drive to the target server on the same day as the first preload. Whenever you perform the preload again, it will only copy files that are newer that did not exist when you ran the preload the previous time. You can use the same USB drive to run the preload for several servers, if the drive has sufficient capacity.

After the preload is finished, physically transport the USB drive and attach it to the replication target. Stop the Local Server Manager service by opening the Backup *Server* Manager, clicking the **Server Status** tab on the left, and click the **Stop** button to stop the Backup Server Manager service. Open the USB disk directory and navigate to the top-level directory that contains the preload data. Then navigate to the subdirectory with the name of your brandID or the word generic (for example, *E:\Preload\BrandID\*), where you should find a single subdirectory that has the same name as the account number of the account you preloaded. Copy this directory to the replication target under the *NetworkServerStoragePath\brandID* directory. For example, copy *E:\Preload\BrandID\12345001* to *X:\ReplicatedData\BrandID\12345001*. After the copy is completed, open the Backup Server Manager again and select the *Server Status* page. Click **Start** to start the service again.

The final step in performing a USB preload for replicated data is to take the account out of maintenance mode in the Web Portal by right clicking the account and selecting *Take out of Maintenance Mode* in the Account Status menu option. Note, however, that you should *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 perform the preload all over again.

Note also that you can put multiple preloads onto the same USB disk. To do this, you can use the same top-level directory on the USB disk for each account that you preload or create a unique folder. 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* might contain the subdirectories 12345001, 12345002, and 12345003.

This completes step 7 of installing and configuring the BDR, which was setting up cross-site replication.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 8. (Optional) Setup notifications** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 8 is to setup notifications. This optional but recommended step ensures end-users and resellers are notified of warnings or errors, as desired.

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

To understand notifications, you must understand three things: First, you decide in the *Options* page on the **Notifications** tab of the Backup Manager whether or not to generate balloon and/or email notifications when a backup starts, completes, or completes with errors or warnings. Second, in the eFolder Web Portal, in the *Notifications* page of the **My Account** main menu option, you decide whether or not to generate email notifications for this account when certain disk usage specifications are met in the storage cloud, if backups have not occurred within so many days, or if error free backups have not occurred in so many days. Third, in the Web Portal, in the Partner Notifications page of the **My Partnership** main menu option, you decide whether or not to generate notifications when okay events, warning events, error events, or any events occur for any of the accounts in your partnership.

The Backup Manager is the software responsible for monitoring the backup and all other services on the BDR as well as the hardware.

As a partner, to configure notifications that monitor and are triggered by any of your accounts in your partnership, log in to the eFolder Web Portal and select *Partner Notifications* on the **My Partnership** main menu option. This is where 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 can also be integrated with certain ticketing and PSA systems. The eFolder portal works with Autotask, ConnectWise and Continuum. Instructions for configuring these tools to work with the eFolder portal are available in the Partner Documentation section of the Partner Center in the Support menu option of the eFolder Portal.

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

This completes step 8 of installing and configuring the BDR, which was setting up notifications.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 9. (Optional) Test file restores and virtualization** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 9 is test file restores and virtualization of the servers. This step is optional but a highly recommended step that will verify that your files can be restored and your servers can be virtualized without difficulty so you can have confidence things will go smoothly in a time of crisis. Rather than being caught by surprise when you are in the middle of an emergency, perform testing *now* to ensure that everything works properly when you really need it most!

First, we’ll discuss how to test file and folder restores. The bare-metal backup images on the BDR can be mounted in seconds to allow recovery of individual files and complete folders. To test restoring files, browse to the folder where the ShadowProtect images are stored: for example *X:\VolumeImages\Server*. Locate the desired incremental file (with a *.spi* extension) or the full backup file (with a .spf extension). Right-click on the file and select the *StorageCraft Mount… (M)* or the *StorageCraft Quick Mount (Q)* option.

You are now prompted to enter the *ShadowProtect Image File* password if the ShadowProtect job was configured with an encryption password. Enter the password and click **OK**. The *Quick Mount (Q)* option automatically mounts the drive and assigns it a drive letter. The *Mount (M)* option allows you to assign the drive letter and choose whether to allow writes. If you choose to allow writes by selecting the *Allow writes* option, a file with a .*SPWB* extension is created.

On the mounted drive, browse to the desired folder and copy the file(s) or folder(s) to the desired location.

When you are done testing file restore, right-click on the drive letter that was created and select *StorageCraft Dismount…* or *StorageCraft Quick Dismount*. The *Quick Dismount* closes the mapped drive. The *Dismount* option allows you to select the check box to the left of each of the mounted drives you want to dismount. If the drive was created with the *Allow writes* options, the file with the *.SPWB* extension must be deleted manually.

This completes how to test the restoring of individual files and folders. Next, we’ll discuss how to test the virtualization of servers.

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 StorageCraft VirtualBoot and Oracle VirtualBox. Your BDR comes with the open source edition of VirtualBox, which is preinstalled and preconfigured on the BDR appliance. StorageCraft VirtualBoot is included with ShadowProtect on your BDR.

Many applications on the BDR are integrated with the specific version of VirtualBox that comes preinstalled. It is important that you do *not* upgrade or downgrade VirtualBox without explicit instructions from eFolder Technical Support. When you upgrade ShadowProtect, work with eFolder Technical Support to ensure you install the correct version of Oracle VirtualBox.

As an overview, virtualization works through a tool called *VirtualBoot*. Running this tool displays a wizard that walks 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, configuring the network interface, performing the driver conversion process, and booting the virtual machine.

Servers or desktops can be virtualized in either *Test Mode* or *Production Mode*.

In *Test Mode*, the virtual server is either *not* connected to the network, or is connected to the network in Network Address Translation (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.

In *Production 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.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Virtualizing a computer in Test Mode** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Before creating the Virtual Machine, verify that the correct version of Oracle VirtualBox is installed. The following StorageCraft website will give you details about which version of VirtualBox is supported for the version of ShadowProtect that you are running: <http://www.storagecraft.com/support/book/english-readme/storagecraft-shadowprotect>

Contact eFolder Technical Support to verify that you have correctly identified the right version of VirtualBox for your version of ShadowProtect. Download and install this version of Oracle VirtualBox, if required, before continuing on to the remaining steps in this process.

Next, let’s discuss how to virtualize a backed up computer in a test environment on the BDR. To do so, start the VirtualBoot wizard on the BDR by selecting VirtualBoot from the StorageCraft folder in the Windows *Start Programs*. Click **Next** on the *Welcome* screen and click the **Add Image File** button. Then select the *.spf* or *.spi* file containing the point-in-time image backup for the computer you want to virtualize.

After you have selected a backup image, it will automatically select the corresponding point-in-time backup image(s) for any other volumes that depend upon the volume you selected. Check that the boot volume that the program selected is correct. If it is not correct, use the **Specify Boot Volume** button to indicate which volume is the boot volume. Then click **Next** when everything looks correct.

Make sure that the checkbox labeled **Automatically start the new virtual machine after creating it** is *not* checked so you can adjust networking settings before starting the virtual machine. Choose the amount of RAM to dedicate to the virtual machine in the appropriate field. Leave at least 1 gigabyte for the BDR itself to use, but we recommend leaving at least 2 gigabytes. For example, if you have 8 gigabytes of RAM, we recommend using no more than 6 gigabytes. Also note that SBS Servers require at least 6 gigabytes of RAM to function properly.

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

The first time that you start VirtualBox, a pop-up window might appear with a banner, *VirtualBoot – Automatically Upgrade Plugin*. If you see this pop-up window, click **Yes** to install the *dll* plugin. You might also be prompted to install the latest version of Oracle VirtualBox. If so, be sure to click **No**.

A progress dialog box appears while the virtual machine is being prepared. Normally this process only takes about 60 seconds, but it may take up to several minutes under unusual circumstances. Please be patient while it prepares the virtual machine.

After the creation process is finished, another dialog box appears confirming the creation of the virtual machine. Click **OK** to close the window.

Next, start Oracle VirtualBox on the BDR by clicking on the desktop icon. Click on the virtual machine that you just created in the list of virtual machines on the left side. Then click the **Settings** button. The following steps will show you how to edit these settings:

In the *Network settings* section, make sure *Adapter 1* is enabled and then select the appropriate network type from the following three types:

The first network type is *Internal Network*. This puts the virtual machine (or 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 that are running that are attached to the same internal network. It is important to note that 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 type 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, as will be described shortly.

The second network type is *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.

The third network type is *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.

Next, if the test VM doesn't need Internet access, expand the *Advanced* settings and make sure that the *Cable connected* option is unchecked.

When you are ready, use the VirtualBox interface to start the virtual machine by selecting the virtual machine from the list of virtual machines and clicking the green **Start** button. Note that 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*. After the server comes up, log in as the local Administrator (*.\Administrator*) using the *Directory Services Restore Mode* password and 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*).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Stopping and deleting the virtual machine** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

When you are finished testing the virtual machine, you will need to stop it and perform the following steps to delete it:

First, stop the VM. Do this by using the normal Windows shutdown process, or click the **X** to close the window displaying the VM, or right click on the VM name and select **Close** and **Power Off**. You can easily delete the VM and all the related files by right clicking on the VM and selecting **Remove**. Select the option to *Delete all files* when given the option to *Delete all files* or *Remove only*. This completes the process for deleting the virtual machine. All of the files should now be cleaned up.

If you want to manually remove the files, perform the following steps:

First, detach the XSP virtual hard drives. In the VirtualBox GUI, edit the VM settings by highlighting the VM and selecting the **Settings** button on the menu bar. Click the **Storage** icon on the left side, and notice or write down the full names of the virtual hard disk files. Then select each virtual hard disk and click the "minus" icon to detach the virtual hard disk. Then click **OK** to close the *Settings* window.

Next, in the VirtualBox GUI, click **File** on the top menu bar and select *Virtual Media Manager*. Locate the virtual hard disks whose names correspond exactly to the XSP files that were associated with the VM you are deleting, as you recorded in the previous step. For each XSP file, expand the items to drill down as far as you can. Select each child item (or each of the *\*.vdi* files) and click the **Remove** icon and confirm the action by clicking the **Remove** button on the confirmation pop-up window. When it asks if you want to delete or keep files, choose **Delete**. Then click **Close** to close the *Virtual Media Manager* window. Do not remove any *.xsp* files at this time.

Next, go back to the VirtualBox settings for the VM you are deleting, and delete any snapshots that show up by clicking the **Snapshots** icon in the top right corner of the screen. Right click on the older snapshots and select **Delete Snapshots**. Then confirm the **Delete** choice.

Close the VirtualBox program and wait about 10 seconds. This forces a background process to shutdown and avoids creating problems during the next step, so be sure you wait at least 10 seconds.

Next, open the VirtualBox program by clicking on the **VirtualBox** icon on the BDR Desktop, click **File** on the top menu, and select *Virtual Media Manager*. Locate the virtual hard disks whose names correspond exactly to the XSP files that were associated with the VM you are deleting, as you recorded in the previous step. For each XSP file, choose **Remove**. Choose **Remove** when you are given the option to *Remove* or *Cancel*. When you are asked if you want to delete or keep files, choose **Delete**.

Next, close the Virtual Media Manager. Finally, delete the VM itself by right clicking on the VM and selecting *Remove*. You have the option to *Delete all files* or *Remove only*. Select *Delete all files* if you want to remove the remaining folder and files.

This completes the manual process for deleting the virtual machine. All files should now be cleaned up.

This completes step 9 of installing and configuring the BDR, which was testing virtualization to ensure that your servers can be virtualized without difficulty.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Where to go to find additional information \_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Congratulations! You have now installed and configured your eFolder BDR for ShadowProtect.

To find information on any of the additional topics displayed on this slide, please click the **Documentation** link in the *BDR for ShadowProtect* entry in the *Partner Documentation* section of the Partner Center in the Web Portal. There are additional documents on the BDR, including the *BDR Users Guide* on the desktop of the BDR and in the *Documentation* folder of the BDR.

Thank you for watching this video on installing and configuring an eFolder BDR for ShadowProtect. Please see the other video overviews and how-to videos in this series for additional training on partner-related tasks.

Copyright © 2016 eFolder Inc. All rights reserved. eFolder, Inc. is the sole author of this document; use of the StorageCraft and ShadowProtect trademarks does not imply official endorsement by StorageCraft Technology Corporation. eFolder and the eFolder logo are trademarks of eFolder Inc. StorageCraft, ShadowProtect, and their respective logos are a trademarks of StorageCraft Technology Corporation. eFOLDER AND STORAGECRAFT TECHNOLOGY MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT.