

efolder

# AppAssure v5.4.x Cloud Replication Guide



for AppAssure

Revised January 2016



## Contents

Solution Overview.....	3
Definitions:.....	3
Enabling Encryption.....	3
Adding an Encryption Key:.....	3
To apply this encryption key to an existing agent:.....	5
To apply this encryption key to a new agent during initial protection:.....	6
Replication Setup Instructions.....	9
Centralized Monitoring through Integration with the eFolder Web Portal.....	14
To access this detailed Core information:.....	16
Partner Notifications.....	18
Managing Your Off-site Core.....	19
Setting Up Virtual Standby Jobs.....	19
To set up virtual standby jobs:.....	20
Increasing Your Available Off-site Storage.....	24
eFolder Continuity Cloud.....	24
Additional Assistance.....	25

Copyright © 2016 eFolder Inc. All rights reserved. eFolder, Inc. is the sole author of this document; Use of the AppAssure trademarks does not imply official endorsement by Dell Inc.. eFolder and the eFolder logo are trademarks of eFolder Inc. AppAssure logos are trademarks of Dell, Inc. eFOLDER AND DELL INC. MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT.

## Solution Overview



**Important:** This document applies only to AppAssure v5.4.X

If you are using AppAssure v5.3.X, please refer to the companion document entitled [eFolder AppAssure v5.3.X](#).

Using the eFolder AppAssure cloud, you can replicate AppAssure v5 data to the eFolder Enterprise Storage Cloud, effortlessly scaling from terabytes to petabytes. In addition to providing you with high performing AppAssure v5 Core servers, you also have access to the eFolder Continuity Cloud that provides fast off-site virtualization of your replicated servers and networks.

### Definitions:

- Each local Core that replicates data to the cloud is called a **source Core** or master Core.
- A hosted Core running in the eFolder AppAssure cloud is called the **target Core** or the slave Core.

## Enabling Encryption



**Important:** Before setting up replication, please ensure that encryption is enabled on all agent recovery-point chains.

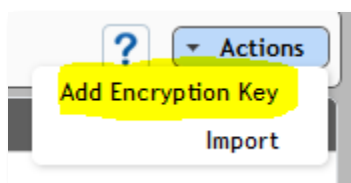
**We will not accept any unencrypted data.**

### Adding an Encryption Key:

1. Navigate to the AppAssure 5 source Core and then click the **Configuration** tab.
2. From the **Manage** option on the Configuration tab, select **Security**.



3. Click **Actions** and then click **Add Encryption Key**.



The Create Encryption Key dialog box appears.

**Create Encryption Key**

Name: BDR1 Encryption Key

Description: Encryption Key for client A

Passphrase: ●●●●●●●●●●●●●●●●●●●●

Confirm Passphrase: ●●●●●●●●●●●●●●●●●●●●

Make sure to store your passphrase in a secure location for future reference. Data recovery will not be possible without the passphrase. AppAssure 5 uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. There are no known methods to compromise this type of encryption.

OK Cancel

4. In the **Name** field, enter a name for the encryption key.
5. In the **Description** field, enter a comment for the encryption key.
6. In the **Passphrase** field, enter a passphrase.
7. In the **Confirm Passphrase** field, re-enter the passphrase.
8. Click **OK**.

**Note:** AppAssure 5 uses AES 256-bit encryption in the Cipher Block Chaining (CBC) mode with 256-bit keys. Using encryption is required for replication of data to eFolder. Store the passphrase in a secure location, as it is critical for data recovery.

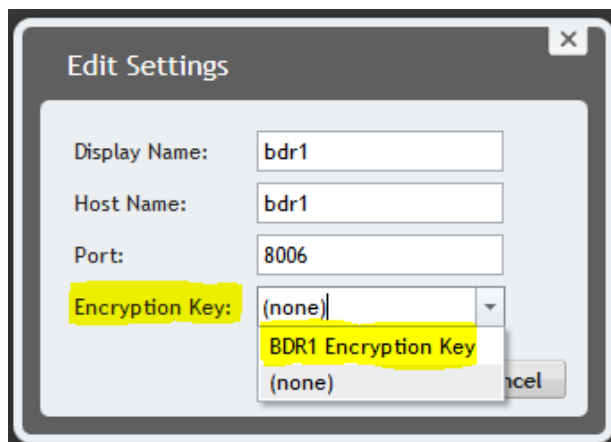
**Without a passphrase, data recovery is not possible.**

To apply this encryption key to an existing agent:

1. Choose an agent which needs to be encrypted from the left pane of the console in the *Protected Agents* section.
2. Click the Configuration tab for the agent and then click **change** in the Settings panel.



The *Edit Settings* dialog box appears.



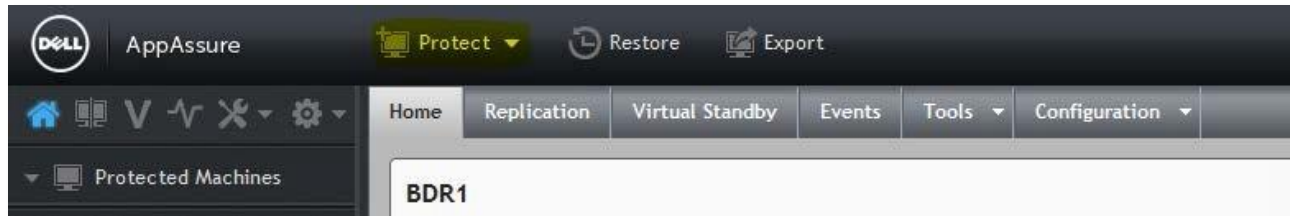
3. In the Encryption Key field, select the appropriate encryption key from the drop-down list.
4. Click OK.

**Note:** Only the subsequent snapshots (and Recovery Points) will be encrypted; earlier snapshots will remain unencrypted.

**Note:** After you apply the encryption key, the next snapshot will be a base image, which will be encrypted.

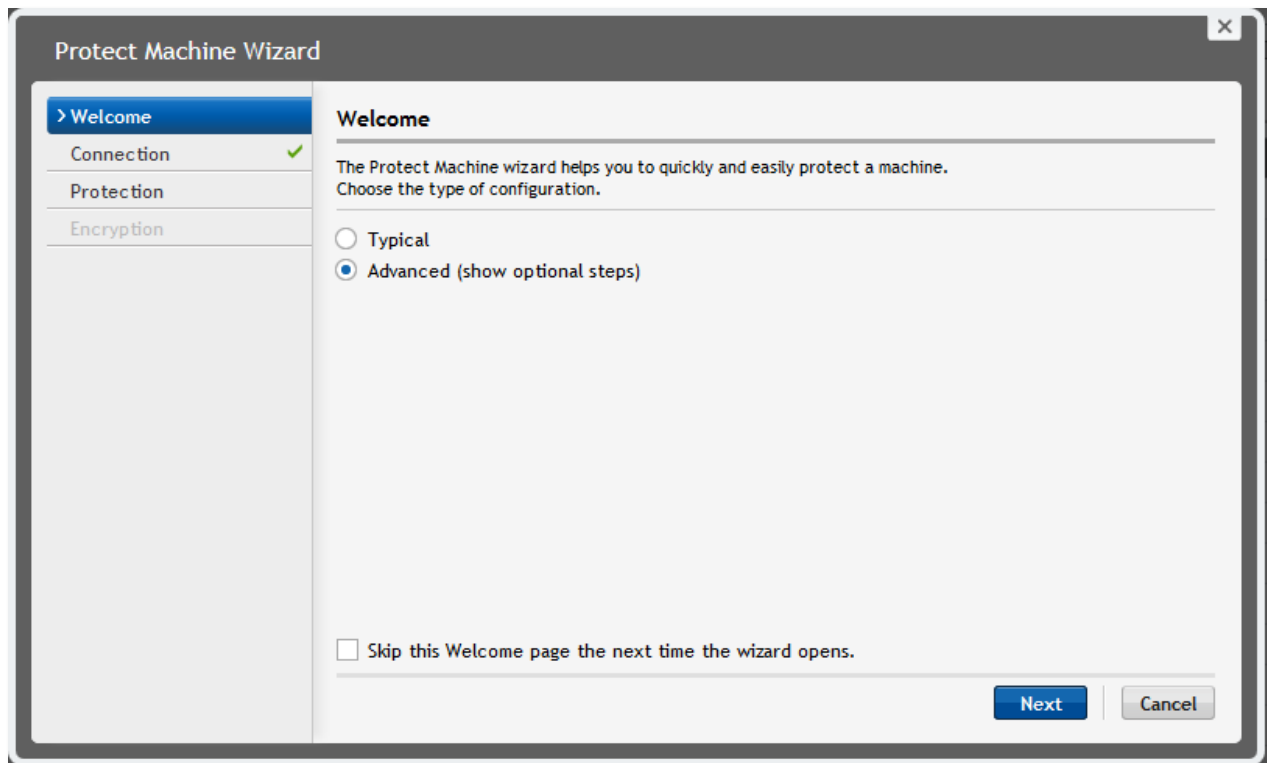
To apply this encryption key to a new agent during initial protection:

1. From the Home screen, click Protect.

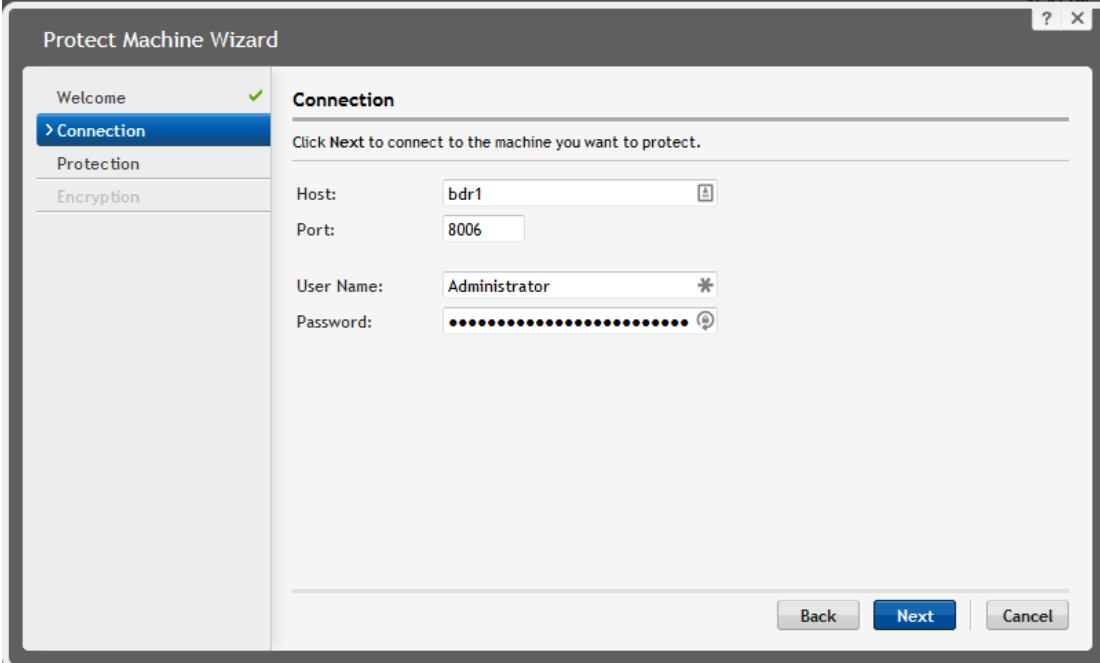


The *Protect Machine Wizard* dialog box appears.

2. Select **Advanced** and click **Next**.



3. On the *Connection* page, enter the Host, User Name, and Password for the machine you want to protect. Leave the default port at 8006. Then click **Next**.

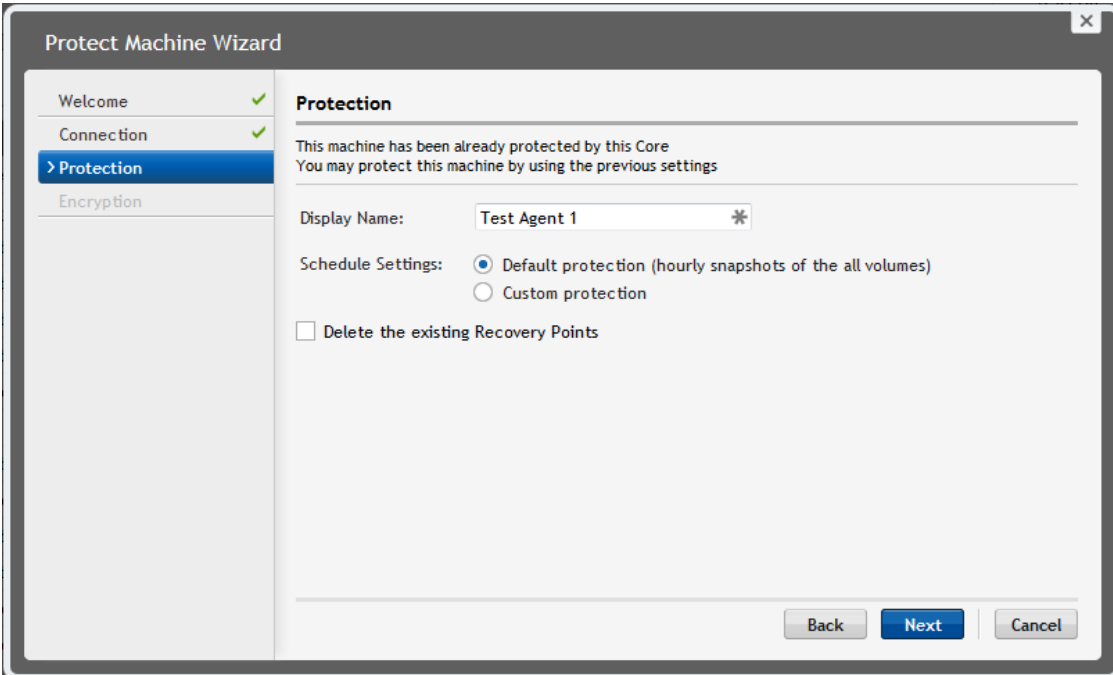


The screenshot shows the 'Protect Machine Wizard' window with the 'Connection' step selected. The 'Welcome' step is marked with a green checkmark. The 'Connection' step is active and contains the following fields:

- Host: bdr1
- Port: 8006
- User Name: Administrator
- Password: [masked]

At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

4. Enter the Display Name for the agent and select the desired option for the Schedule Settings. Then click **Next**.



The screenshot shows the 'Protect Machine Wizard' window with the 'Protection' step selected. The 'Welcome' and 'Connection' steps are marked with green checkmarks. The 'Protection' step is active and contains the following fields:

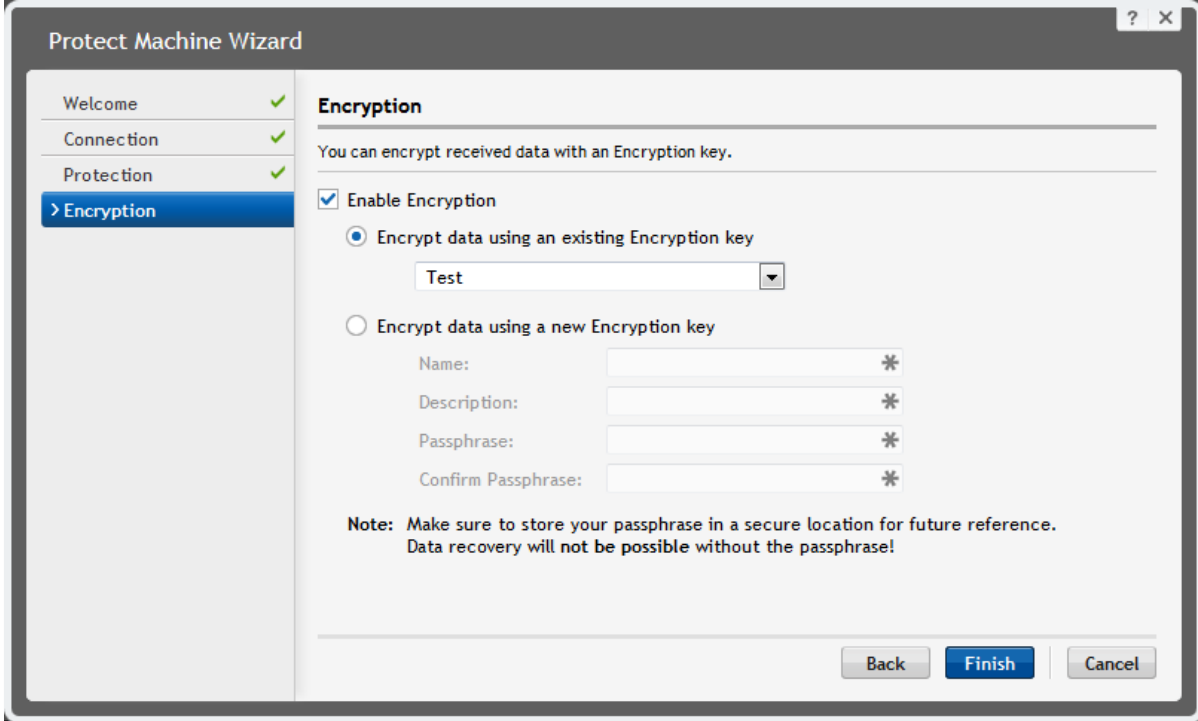
- Display Name: Test Agent 1
- Schedule Settings:  Default protection (hourly snapshots of the all volumes)  Custom protection
- Delete the existing Recovery Points

At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

5. Check the **Enable Encryption** checkbox.

Select your key from the **Encrypt data using an existing Encryption key** drop-down list or create a new encryption key in the **Encrypt data using a new Encryption key** field.

After you have selected or entered your key, click **Finish**.



The screenshot shows the 'Protect Machine Wizard' window, specifically the 'Encryption' step. The left sidebar shows a progress indicator with 'Welcome', 'Connection', 'Protection', and 'Encryption' (highlighted). The main area is titled 'Encryption' and contains the following elements:

- A heading: **Encryption**
- Text: You can encrypt received data with an Encryption key.
- A checked checkbox: **Enable Encryption**
- Two radio button options:
  - Encrypt data using an existing Encryption key**: This option is selected. Below it is a dropdown menu showing 'Test'.
  - Encrypt data using a new Encryption key**: This option is unselected. Below it are four text input fields: 'Name:', 'Description:', 'Passphrase:', and 'Confirm Passphrase:'. Each field has an asterisk (\*) on the right side, indicating it is required.
- A **Note**: *Make sure to store your passphrase in a secure location for future reference. Data recovery will not be possible without the passphrase!*
- At the bottom right, there are three buttons: 'Back', 'Finish' (highlighted in blue), and 'Cancel'.

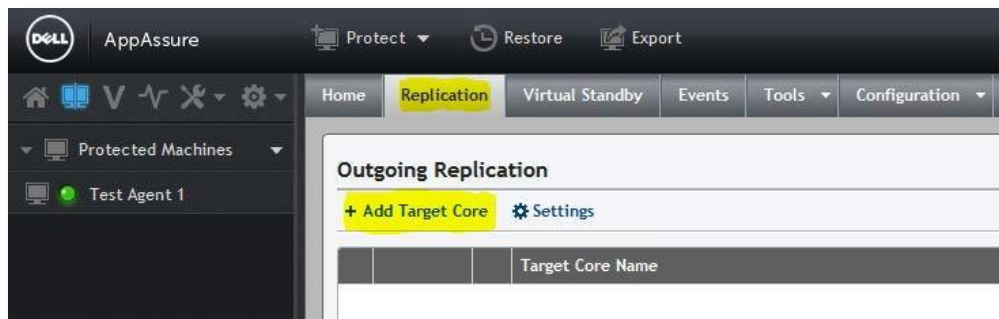


## Replication Setup Instructions

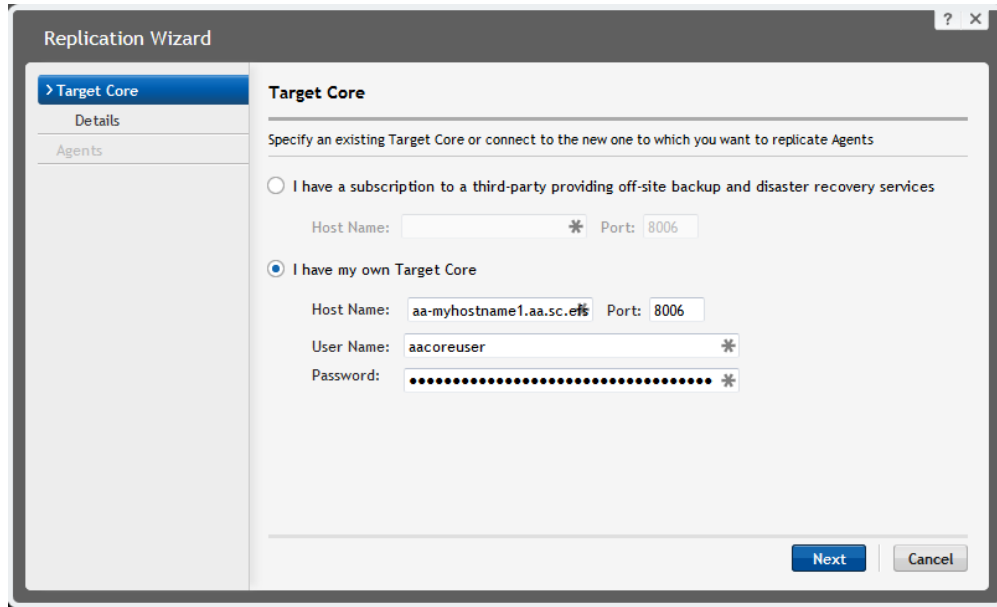
1. For each source Core, make sure that the Core is running a compatible version of AppAssure. **You should be using AppAssure version 5.4.2.228.** This version should be installed on all source Cores that replicate to the eFolder cloud and on all the agents they protect.

**Note:** If the source Core is running a version of AppAssure that is newer than the version running on your target Core, please contact Support and we will upgrade your target Core to a newer version. You can download our recommended version of the AppAssure software from the eFolder Knowledgebase by clicking AppAssure V5 Downloads and License Keys [here](#).

2. Next, configure replication on each source Core. To do this, log in to the source Core's administrative console and click the **Replication** tab.
3. After the Replication tab has loaded, click on **Add Target Core**.



The replication wizard appears. Select the **I have my own Target Core** option.

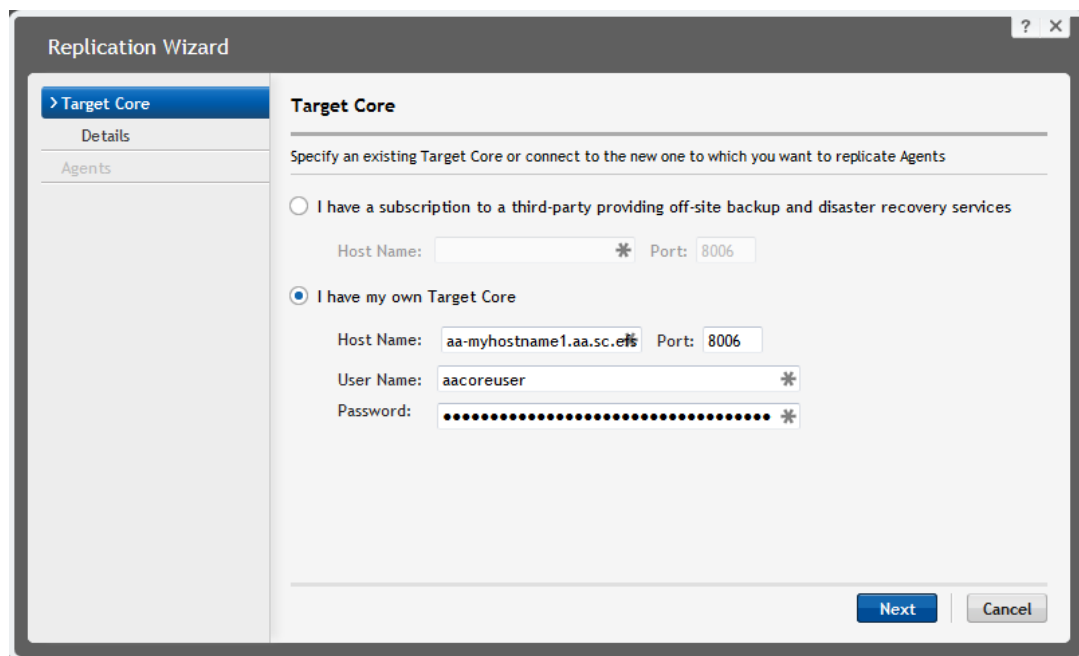


4. Enter the **Host Name** that has been assigned to you as well as your assigned **User Name** and **Password**.

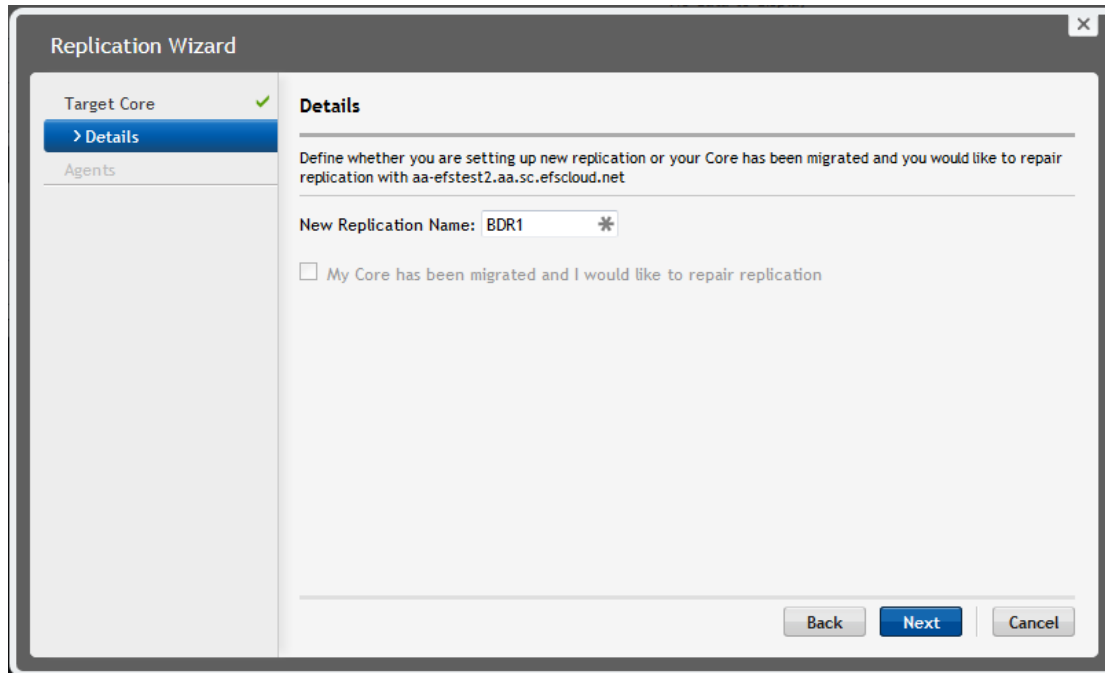
In the example shown, the Host Name is *aa-myhostname1.aa.sc.efsccloud.net*

You should have received your assigned Host Name, User Name and Password when your hosted target Core was provisioned for you.

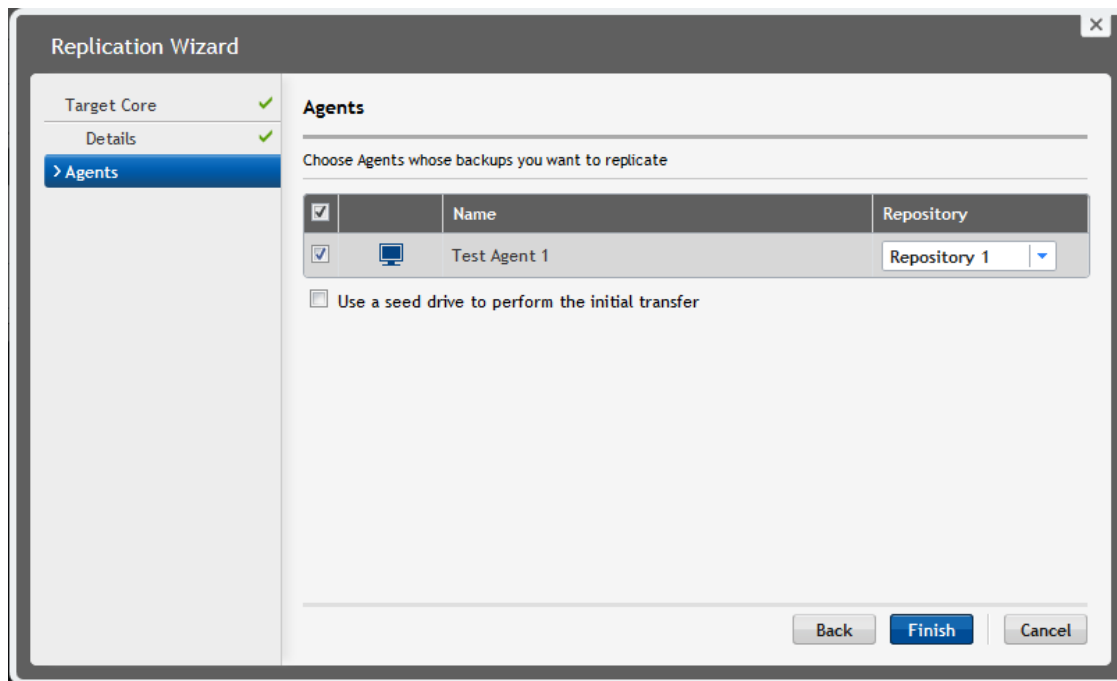
5. Click **Next**



6. Enter the **New Replication Name** for your source Core if the default is not sufficient for identifying the source Core. Then click **Next**.

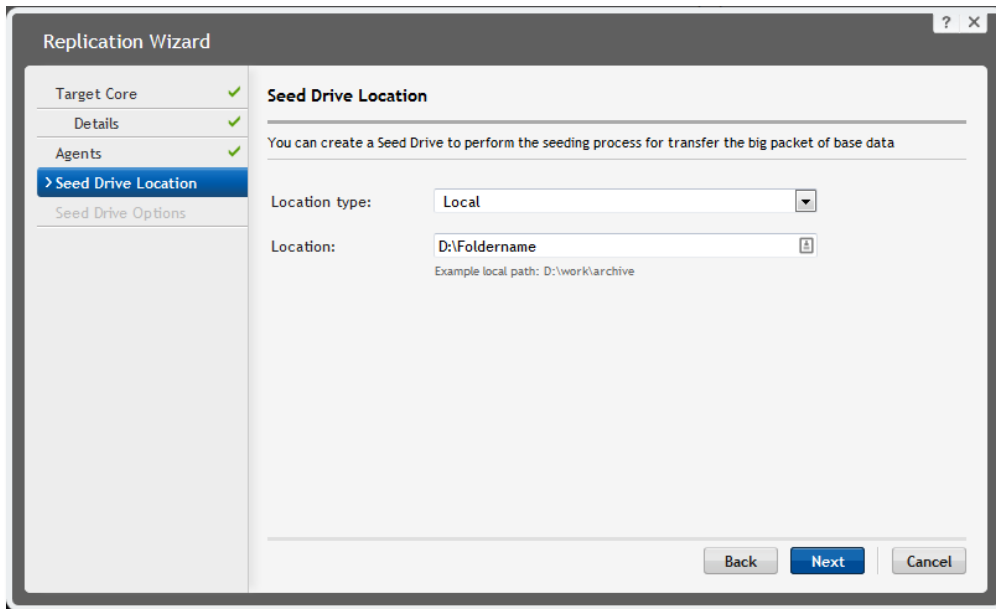


7. In the *Agents* window, select the checkbox next to each agent that you want to replicate to the target Core. Additionally, if you want to ship a local hard disk with the initial set of data, check the **Use a seed drive to perform initial transfer** checkbox. Then click **Finish**.

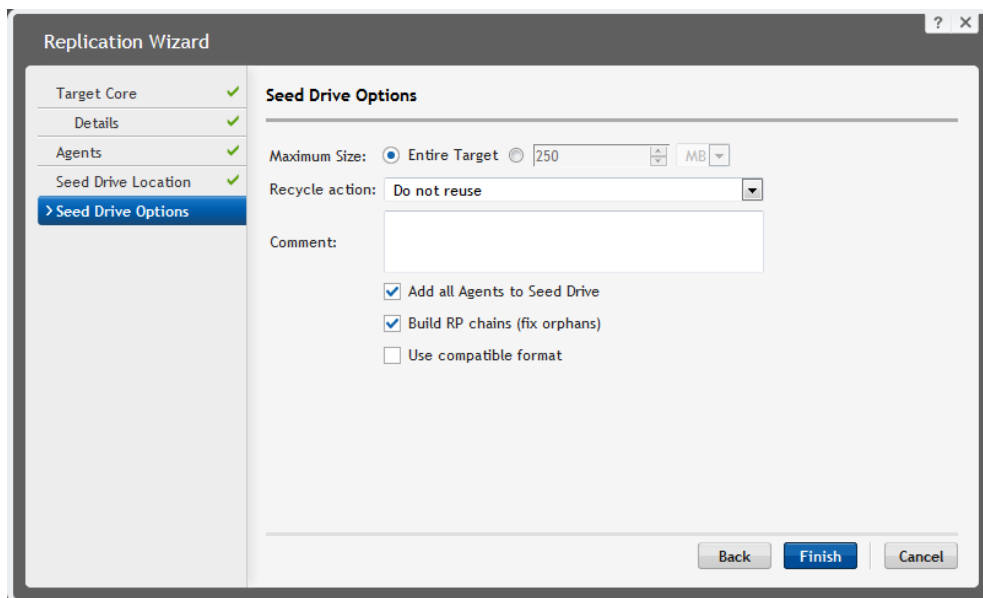


**Note:** If you send an initial “seed” or “preload,” make sure you follow the latest set of instructions for performing an AppAssure preload [here](#).

- If you chose to use a seed drive for the initial data, the *Seed Drive Location* dialog box appears. Select either **Local** or **Network** from the drop-down menu and then enter the location path. If you selected **Network** as the location type, then provide the UNC path and credentials to access the location. Then click **Next**.



- The *Seed Drive Options* window will appear. You do not need to modify anything on this screen. The defaults are correct. Click **Finish**.



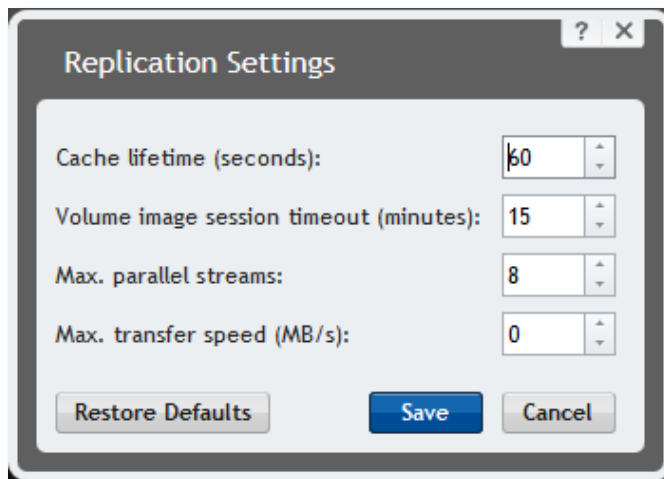
You can monitor the status of the copy (export) operation on the *Events* tab in the console. Also, please be sure to follow all of the directions listed [here](#) when performing a seed operation preload.

When the replication relationship has been established, the information on the *Replication* tab should be similar to this:



**Note:** Replication of the base image (or incrementals, if you are doing a seed) will begin for each agent **after** their next recovery point is received into the source Core.

**Note:** Replication will proceed in parallel for many agents at the same time. The default level of concurrency is normally suitable for most customers. However, it can be customized by changing the settings in the *Actions > Replication Settings* menu:



Set the **Max. parallel streams** to a value that can be handled by the network.

Each replication task opens this number of TCP streams. If the value is set too high, it can cause timeouts. If the value is set too low, then replication is slower than what it could be.

Rule of thumb: For every 1Mb of upload speed, increase Max Parallel Streams by 1.

- 1.5 Mbps Upload: 1 Max Parallel Streams
- 3 Mbps Upload: 2 to 3 Max Parallel Streams

Note that if you increase the **Max. concurrent replication jobs**, you may wish to decrease the number of parallel streams. For example, you may want to use combinations of 2 and 4, or 4 and 2, and so forth. Having replication proceed in parallel to the cloud allows better utilization of WAN bandwidth.

## Centralized Monitoring through Integration with the eFolder Web Portal

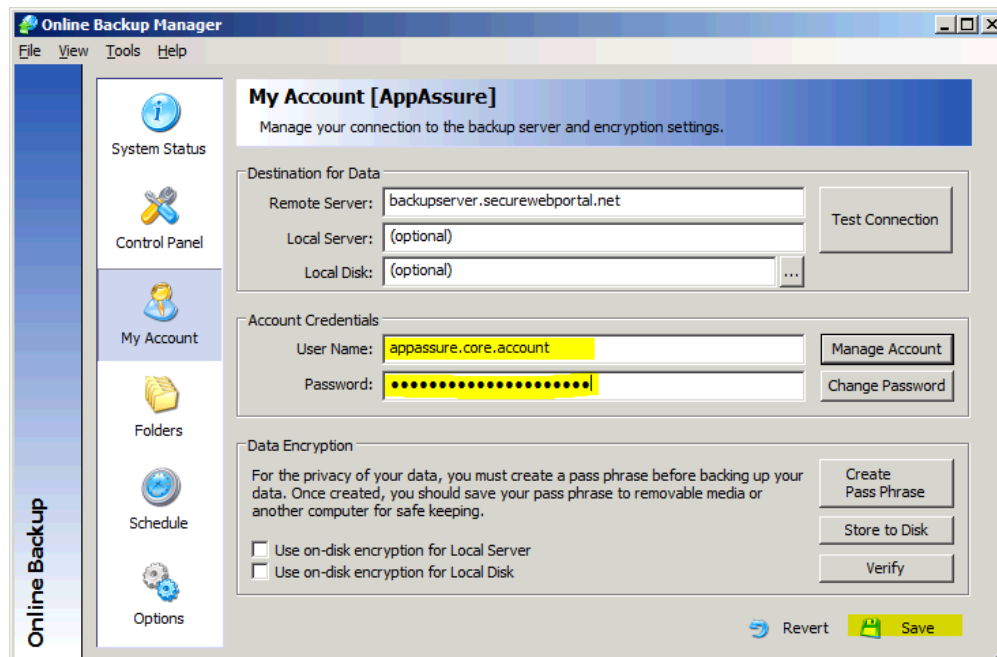
You can optionally use features that integrate data from your source AppAssure Core into the [eFolder Web Portal](#). This allows you to:

1. Centrally monitor the status of all of your Cores from one cloud-based web portal.
2. Set up global alerting rules that generate emails or PSA tickets on warning or error conditions.
3. Set up automated billing integration with supported PSA systems (coming soon).

We highly recommend utilizing the Web Portal integration functionality.

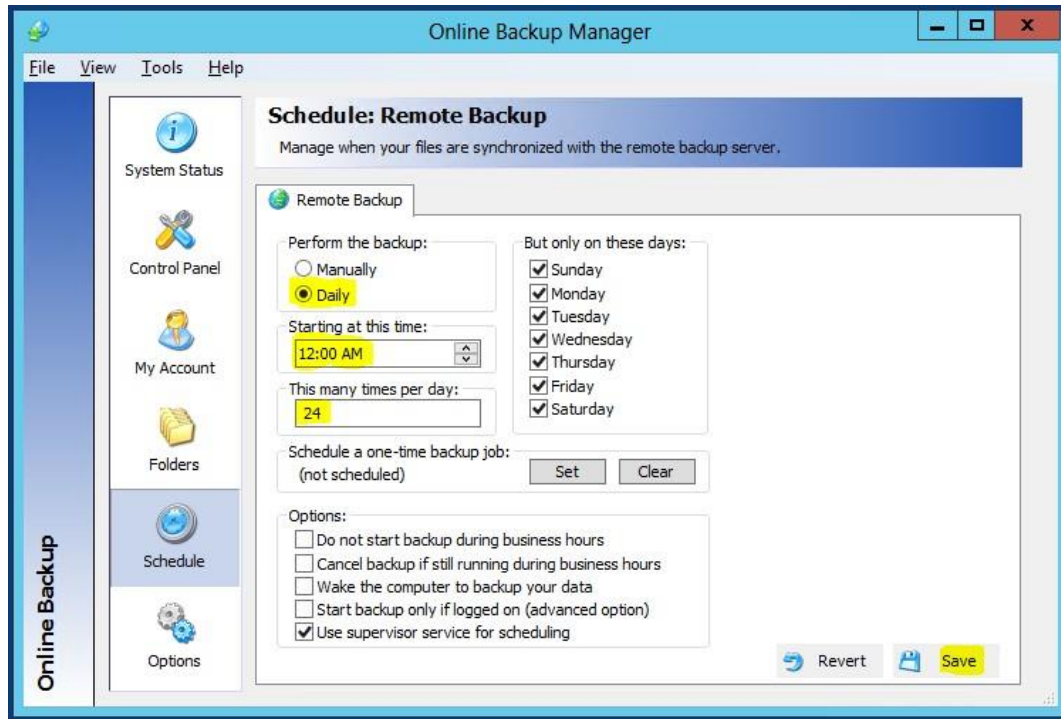
To use this functionality, you will first need a partner account created for you in the eFolder Web Portal. After you have gained access to the [eFolder Web Portal](#), follow these instructions for each source Core:

1. Use the Web Portal to create a new account with the *AppAssure Core* service plan.
2. On the source Core server, download and install the eFolder Backup Manager client program. **Note that you must use version 3.8.5 or later of the Backup Manager client.**
3. In the Backup Manager, on the *My Account* page, configure the Web Portal account **User Name** and **Password** credentials and then click **Save**.



**Note:** You do **not** need to create an encryption pass phrase unless you also plan to use the actual file-level backup features of the account instead of just the AppAssure Core integration features.

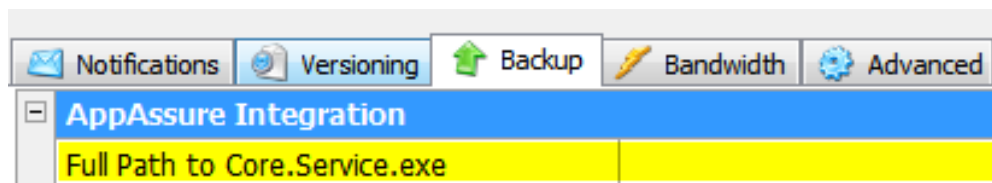
- Configure the settings on the *Schedule* page to back up 24 times per day:



This will cause the Core information to be updated every hour in the Web Portal.  
**We do not recommend or support updating information more frequently than every hour.**

- If you have installed the AppAssure V5 Core in the default location, no further configuration is required.

If you have **not** installed the AppAssure V5 Core in the default location, you must use the Backup tab on the *Options* page to configure the location of the Core program.



After you have finished configuring the integration, the AppAssure Core information in the Web Portal will refresh every hour. The information for the status of each Core and each agent on each Core will appear on the Dash Panel report, allowing you to easily see the last snapshot date or completed replication date for each agent and the status of all backup, replication services, virtual standby services, and repository state and disk usage information.

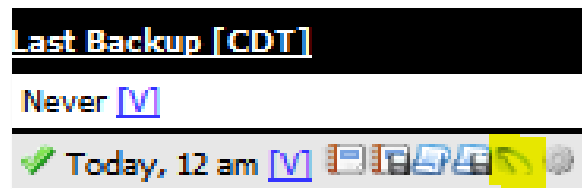
Additional detailed information is available in the Web Portal about each individual Core. You can view repository status, backup status, replication status, the progress of any snapshots, replication jobs, seeds, consumes, or virtual standby jobs, as well as detailed event log history.

**To access this detailed Core information:**

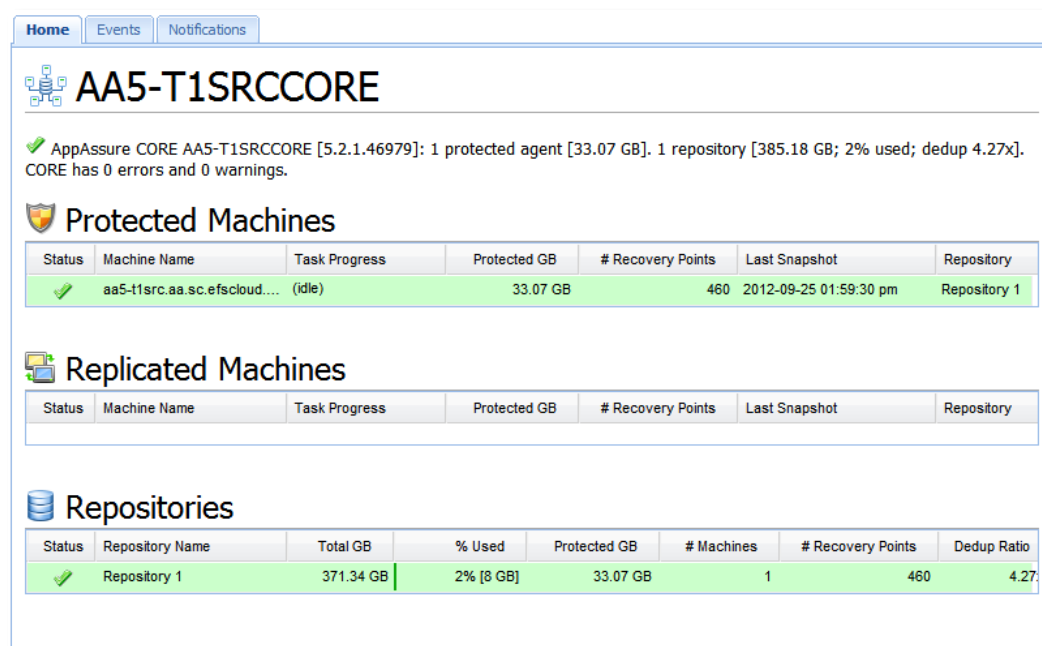
1. Click the **AppAssure** icon in the *Account Summary* tab of the *Account Details* pane in the *Account Center* page.



Alternatively, on the *Account List* page, click the **AppAssure** icon in the last backup column field for the account associated with your target Core.



2. The detailed *Core* dialog appears. The *Home* tab displays the status of protected and replicated machines, and repositories.





The *Events* tab displays the detailed status of backup, replication, or virtual standby jobs, plus the progress of active jobs.

The *Notifications* tab shows a history of the status state changes of this Core server (for example, when error alerts and error resolution alerts were sent, and which of your notification rules were triggered).

The screenshot shows the 'Events' tab in the AppAssure interface. At the top, there are tabs for 'Home', 'Events', and 'Notifications'. Below the tabs is a 'Tasks' section with a table listing various tasks. The first task is expanded to show detailed information.

Task	Status	Start Time	End Time
'Replicating 'aa5-t1src.aa.sc.efsccloud.net' to 'AA5-T1DSTCORE'	OK [0.0 GB]	2012-09-25 02:00:00 pm	2012-09-25 02:00:34 pm
<b>Succeeded: 'Replicating 'aa5-t1src.aa.sc.efsccloud.net' to 'AA5-T1DSTCORE'</b>			
<b>Start Time:</b>	Tue Sep 25, 2012 02:00:00 pm	<b>Rate:</b>	0.11 MB/sec
<b>End Time:</b>	Tue Sep 25, 2012 02:00:34 pm	<b>Progress:</b>	100%: 0.00 GB of 0.00 GB
<b>Elapsed Time:</b>	34 seconds	<b>Total Work:</b>	0.00 GB
<b>Child Tasks</b>			
Task	Status	Rate	Progress
Updating agent metadata	Succeeded	...	Succeeded
Transferring	Succeeded	0.11 MB/sec	OK [0.0 GB]
Updating agent and volume(s) metadata	Succeeded	...	Succeeded
Transfer of volumes [(Volume Labeled 'System Reserved'),C...	OK [0.0 GB]	2012-09-25 01:59:30 pm	2012-09-25 02:00:00 pm
'Replicating 'aa5-t1src.aa.sc.efsccloud.net' to 'AA5-T1DSTCORE'	OK [0.0 GB]	2012-09-25 01:54:58 pm	2012-09-25 01:55:29 pm
Transfer of volumes [(Volume Labeled 'System Reserved'),C...	OK [0.0 GB]	2012-09-25 01:54:29 pm	2012-09-25 01:54:58 pm
'Replicating 'aa5-t1src.aa.sc.efsccloud.net' to 'AA5-T1DSTCORE'	OK [0.0 GB]	2012-09-25 01:49:58 pm	2012-09-25 01:50:28 pm
Transfer of volumes [(Volume Labeled 'System Reserved'),C...	OK [0.0 GB]	2012-09-25 01:49:27 pm	2012-09-25 01:49:58 pm

Below the tasks is an 'Alerts' section with a table of messages:

Date	Message
2012-09-25 03:00:00 am	Nightly attachability job has been skipped. Reason: There are no SQL Server instances configured for attachability check on the Core
2012-09-24 03:00:00 am	Nightly attachability job has been skipped. Reason: There are no SQL Server instances configured for attachability check on the Core
2012-09-23 03:00:00 am	Nightly attachability job has been skipped. Reason: There are no SQL Server instances configured for attachability check on the Core
2012-09-22 05:45:43 am	The Core service on AA5-T1SRCCORE was not shut down cleanly. The system is running checks to ensure data integrity.
2012-09-22 05:45:41 am	The Core service on AA5-T1SRCCORE has started

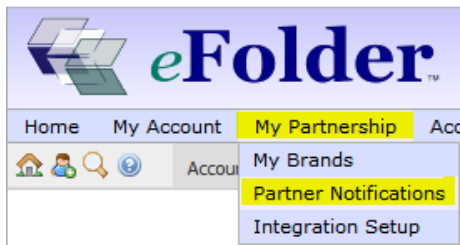
**Note:** If you prefer, eFolder technical support can set up the Web Portal integration for your target Core (if we have not already done so).

Simply submit a ticket with your Web Portal username and the hostname of your target Core, and we will take care of it for you.

## Partner Notifications

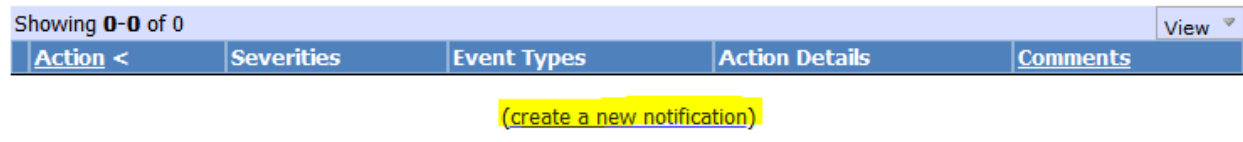
We highly recommend setting up partner notification rules in the Web Portal so that you can be alerted when any of your Cores or agents have error conditions that need attention.

1. In the Web Portal, select Partner Notifications on the *My Partnership* menu.



2. On this page, click the [\(create a new notification\)](#) link.

Use this page to setup notifications for events generated by any account under your management. This simplifies monitoring as you only have to configure notifications once for your partnership, rather than for each account. Notifications are also used to push information to 3rd party systems, such as ConnectWise PSA (requires [integration setup](#)).



3. The *Create Partner Notification* page appears.

Setting	Value	Description
<b>Notification Action</b>	Send an email	What will happen when this notification is triggered.
<b>Email Addresses</b>	support@mymisp.com	Addresses where the email notification should be sent to. Separate multiple addresses with semicolons.
<b>Include Sub-Brands</b>	Yes	Whether or not to include notifications for accounts associated with sub-brands of your brand. Only relevant if you have more than one brand.
<b>Subscribe to OK Events</b>	No	Whether events that represent successful actions should trigger this notification.
<b>Subscribe to Warnings</b>	Yes	Whether events that represent warnings should trigger this notification.
<b>Subscribe to Errors</b>	Yes	Whether events that represent errors should trigger this notification.
<b>Subscribe to All Event Types</b>	Yes	Whether or not to subscribe to all types of events, except for integration failures (note that the restrictions on event severity configured above still apply).
<b>Comments</b>		Any comments you want to make about this notification.

The notification engine is powerful and can be configured to meet complex needs. We show the simplest example above, wherein you can be notified when any warning or error event occurs.

To configure ticketing and billing integration with your PSA system, please refer to the corresponding eFolder integration guide for your PSA system, available in the [Knowledge Base](#) in the eFolder Web Portal.

## Managing Your Off-site Core

- You can manage and monitor the state of your target Core running in the eFolder AppAssure Cloud by pointing your web browser to

<https://aa5-myhostname.aa.sc.efscloud.net:8006/apprecovery/admin/Core>

(where aa5-myhostname is the name of your Core).

- You can also add your target Core to the AppAssure multi-Core management console software and manage it centrally with your other Cores.

## Setting Up Virtual Standby Jobs

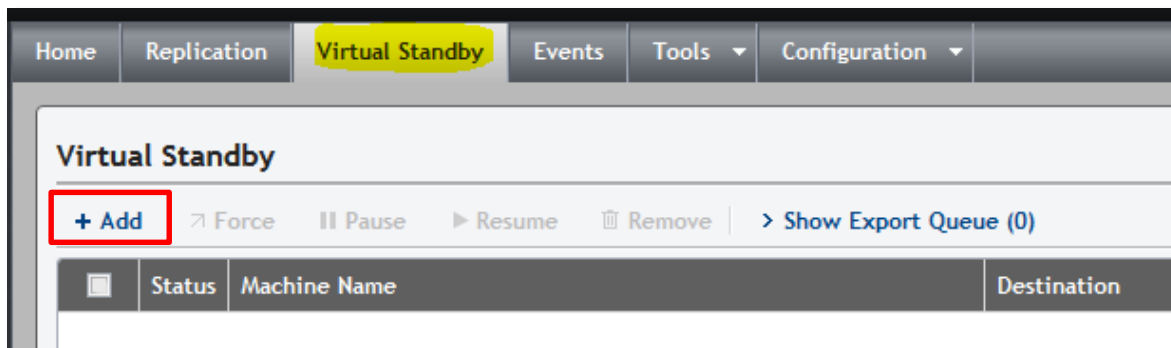
Virtual standby jobs allow you to keep updated Hyper-V or VMware virtual machines (VMs) that represent the latest version of your protected servers. These VMs are thus ready to be started quickly in case the original protected server is no longer available. Please note that virtual standby is only available for protected Windows servers at this time (version 5.3.7.68 or newer of AppAssure).

- **If you are using a BDR appliance locally**, we recommend setting up virtual standby jobs on the source Core so the BDR can nearly instantly virtualize your protected servers locally.
- **If you are using a dedicated eFolder Continuity Cloud node**, you can also set up virtual standby jobs on your hosted target Core. This allows any protected servers to also be virtualized in the cloud nearly instantly.
- **If you are *not* using a dedicated eFolder Continuity Cloud node**, you will only set up virtual standby jobs when you have a need to virtualize a server in the cloud, after you have been assigned your on-demand Continuity Cloud node(s).

Virtual standby VMs are updated after each recovery point is received by a Core and thus are kept continuously up to date. Updates to VMs only need to apply the data blocks changed within the received incremental recovery point; thus, updates to VMs usually complete within a few seconds or minutes. The time required for the initial export depends on the amount of data and other factors and might take several hours.

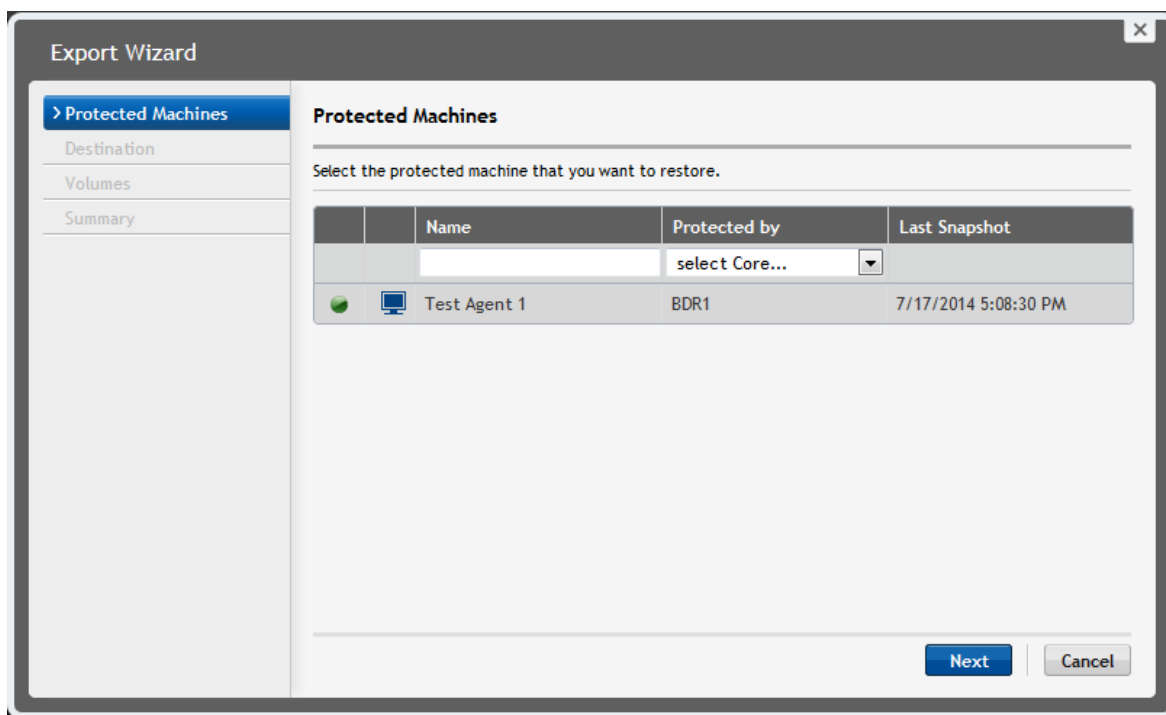
To set up virtual standby jobs:

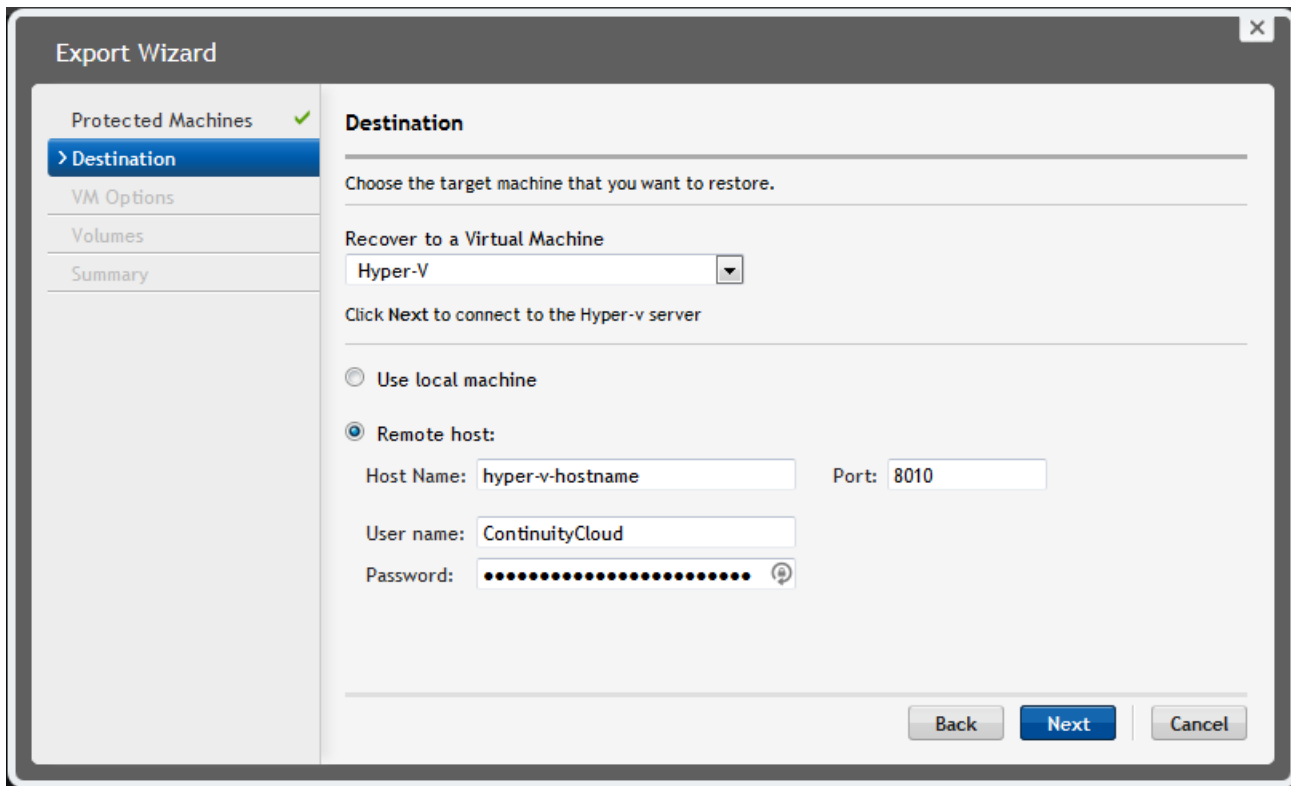
1. Log in to the source or target Core Admin Console and navigate to the *Virtual Standby* tab. Then click **Add**.



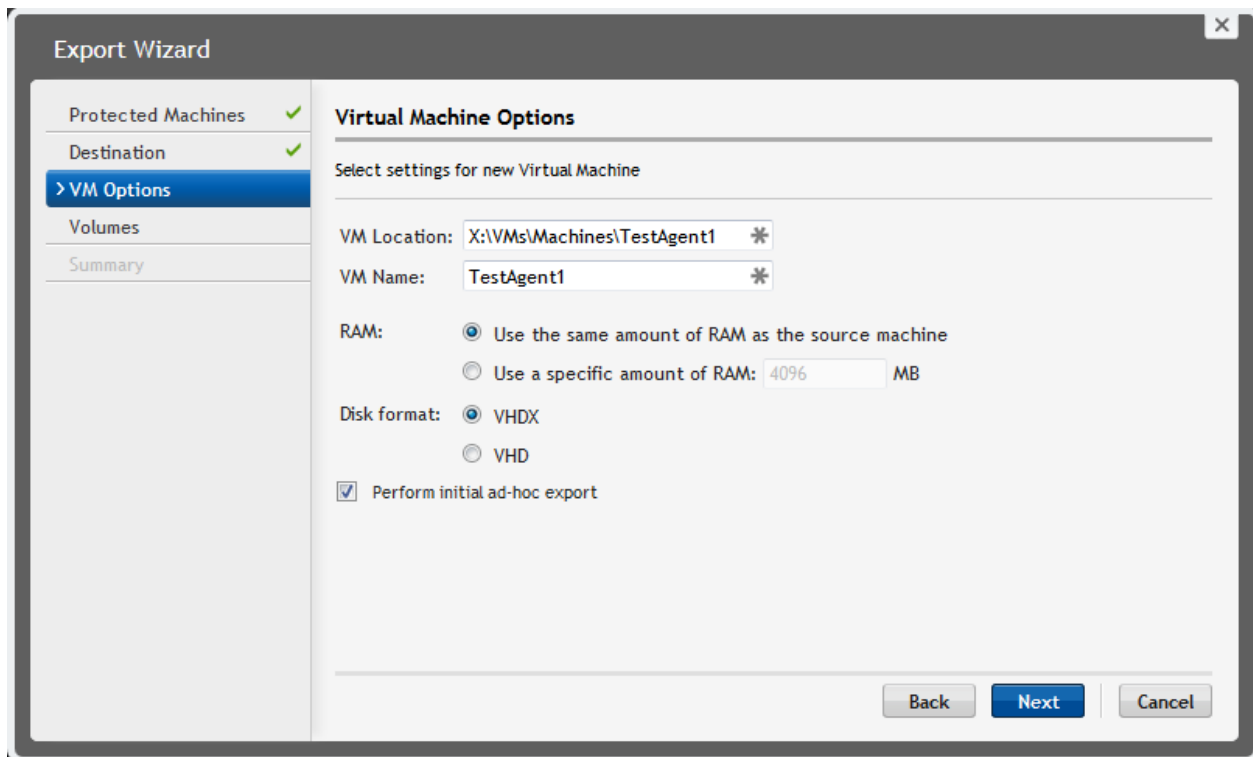
The Export Wizard dialog appear

2. Select the agent for which you want to add a virtual standby job and then click **Next**.





3. Select the target host machine type you want to export the agent to.
4. When configuring the Hyper-V export, for Hyper-V-powered BDR appliances, click **Use local machine**. For the eFolder Continuity Cloud, in the *Hyper-V Host Name* field, enter the AppAssure private IP listed in the *Private-IPs.txt* file on the desktop of your Continuity Cloud node.
5. In the *User name* and *Password* fields, enter the credentials you were assigned for the Continuity Cloud node. Then click **Next**.



6. In the *VM Options* window, in the *VM Location* field, choose a path that is local to the Hyper-V server. Then specify the **VM Location**, enter the **VM Name**, choose the amount of RAM to use, and finally select the disk format.

**Note:** On eFolder Continuity Cloud nodes and eFolder BDR appliances, choose a directory on the "X" volume such as X:\VMs\Machines\agentname.

**Note:** In the VM Name field, spaces are not allowed in the name.

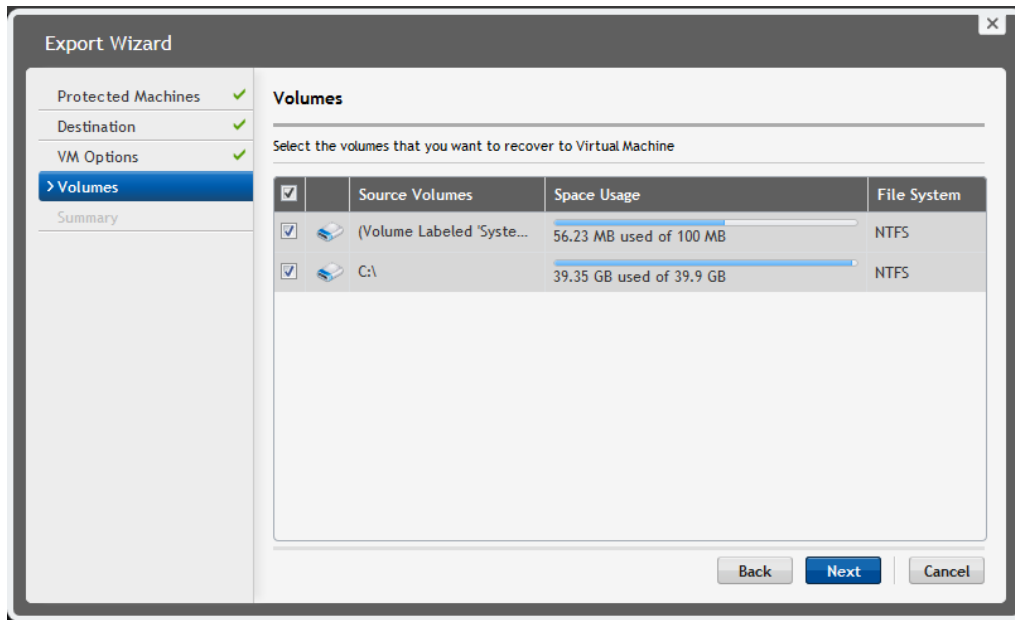
**IMPORTANT!** The directory should be unique to the name of the protected server for which you are configuring the virtual standby job.

Make sure the server name is part of the directory path.

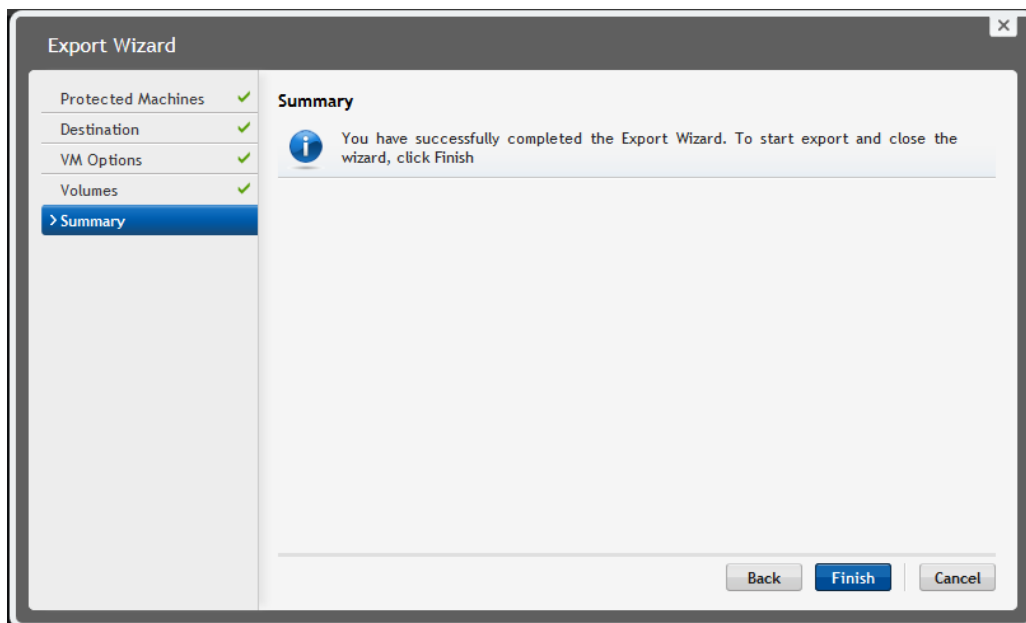
For example, in this case, we are using X:\VMs\Machines\TestAgent1.

7. If you want the virtual standby export to begin immediately, check the **Perform initial ad-hoc export** checkbox; otherwise, the export will begin after the next recovery point is received for this agent. Then Click **Next**.

- In the *Volumes* window, select the volumes you want to export for the Virtual Machine. All volumes are recommended for the VM to operate properly. Then click **Next**.



- The *Summary* window appears. Click **Finish**.



You can monitor the progress of the virtual standby export jobs in the *Events* tab in the management console. **Note:** For replicated agents on the target Core, the initial replication must fully complete (or the initial seed must be fully consumed) before you can configure virtual standby.

## Increasing Your Available Off-site Storage

- To increase the amount of storage available on your hosted target Core, please send a request to [aasupport@efolder.net](mailto:aasupport@efolder.net) and include your assigned Core hostname and how much storage you need.
- Storage is always provisioned in blocks that are multiples of 100 GB.
- Usually, additional storage can be added by our engineering team without needing to reboot your target Core server. Our team will notify you when the additional storage has been added; no additional work is required on your part.
- Please note that eFolder bills partners and end-users based on the total amount of storage that has been provisioned for your target Core.

## eFolder Continuity Cloud

The eFolder Continuity Cloud is provided to partners and end-users and is billed on a per-use, as-needed basis.

To access the Continuity Cloud, send an email to [aasupport@efolder.net](mailto:aasupport@efolder.net) to request access.

If your servers are down and you want after-hours access, be sure to follow the instructions in the ticket autoresponder email to escalate the ticket to the highest priority status.

When you are granted access, you will be given credentials and an IP address that gives you remote desktop access to one or more Continuity Cloud physical nodes. These physical nodes are running Hyper-V and allow you to quickly virtualize your Virtual Standby jobs. You will be assigned public IPs that are pre-routed into a WAN-DMZ network accessible by your Continuity Cloud nodes. You will have access to a virtual router and firewall that will allow you to easily route traffic from the WAN- DMZ to and from a custom virtual LAN.

For detailed instructions on how to use the eFolder Continuity Cloud, please refer to the eFolder article entitled [AppAssure Continuity Cloud Guide](#).



## Additional Assistance

For issues or questions regarding **AppAssure V5 software**:

- If you purchase licenses from AppAssure directly, please contact AppAssure technical support at (703) 480-0100 or [support@appassure.com](mailto:support@appassure.com)
- If you purchase AppAssure V5 licenses through eFolder, please contact eFolder technical support by emailing [support@efolder.net](mailto:support@efolder.net) or calling 800-352-0248

For eFolder Continuity Cloud or to troubleshoot network, replication, or CORE servers:

- Email eFolder Support at [aasupport@efolder.net](mailto:aasupport@efolder.net)
- Call us at 800-352-0248

Additional information is also available:

- [eFolder Partner Portal](#)
- Support Page at <http://www.efolder.net/support/>.

Copyright © 2016 eFolder Inc. All rights reserved. eFolder, Inc. is the sole author of this document; Use of the AppAssure trademarks does not imply official endorsement by Dell Inc.. eFolder and the eFolder logo are trademarks of eFolder Inc. AppAssure logos are trademarks of Dell, Inc. eFOLDER AND DELL INC. MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT.

