



Acronis Backup Advanced 11.5 Solution Guide and Best Practices

Updated May 2015



Table of Contents

Solution Overview	3
Acronis Backup and Recovery Components.....	3
System Requirements.....	4
Supported Operating Systems:	4
Supported File Systems and Storage	5
Deployment Methods	5
Unmanaged deployment.....	5
Managed Deployment.....	6
Provisioning Acronis Keys from the eFolder Web Portal	6
Overview of the types of Acronis Backup Advanced license keys	7
Provisioning Acronis Backup Advanced License Keys	7
Deprovisioning Acronis Licenses	12
Installing and configuring the Management Components	13
Installing the Management Components.....	13
Configuring the Management Components.....	21
Connecting/Configuring the AMS and Storage Node	30
Installing the Acronis Backup Agent: Configuring backup schemes	37
Installing the Acronis backup agent	38
Configuring the Local Backup Plan.....	44
Creating a Remote Backup plan	51
How Acronis performs Full Backups to a Managed Vault with Deduplication.....	52
Remote Backup Plan with Seed Drive.....	52
Remote Backup Plan - Backing up Directly to the eFolder Acronis Vault.....	62
Additional Resources	68
Self Help.....	68
Technical Support.....	68

Solution Overview

The purpose of this how-to guide is to help you become familiar with the different components within the Acronis Backup Advanced 11.5 as well as to help you understand how to install and configure these components and the replication of the Acronis data to the eFolder cloud. We will cover the installation and configuration of the Acronis Backup Advanced 11.5 (Acronis) and the replication of the backed up data to the eFolder cloud from a Backup and Disaster Recovery appliance (BDR). Keep in mind it is not necessary to use a BDR appliance as these technologies can be used in stand-alone environments.

This how-to guide is broken up into the following sections: an overview of the components that are included in the Acronis solution, installation options for those components, deployment and management of the Acronis agent, and the replication of the Acronis data to the eFolder cloud.

Important! The solution that is built around the bundled Acronis Backup Advanced 11.5 and the eFolder BDR/Cloud for Acronis requires Acronis Backup Advanced 11.5. You must upgrade older versions before you can backup to the eFolder cloud.

The installer for the Acronis Backup Advanced can be downloaded from eFolder's Knowledge Base at <https://secure.efoldering.com/support/index.php?efolder/Knowledgebase/Article/View/278/67/acronis-for-efolder-download>

Acronis Backup and Recovery Components

In this section, we list the components that make up the Acronis Backup Advanced 11.5 solution.

- Acronis Console: the console that provides a Graphical User Interface (GUI) and remote connection to the Acronis backup agents and other Acronis technologies like the Acronis Management Server.
- Acronis Storage Node: the storage node that enables administrators to create a highly scalable and flexible storage infrastructure. The storage node contains vaults where the Acronis images are stored. One of the functions of the storage node is the deduplication of backups stored in the vaults.
- Acronis Management Server (AMS): the central server that remotely manages the Acronis Backup Agents that are deployed on the protected machines by centrally managing licenses, creating and managing storage nodes and vaults, and providing a single point for monitoring and reporting functionality.
- Acronis Backup Agent: an agent that is deployed on either a Windows or Linux operating system that provides disk level data protection by backing up a disk or volume. There are also agents that provide the ability to granular restore application data like Microsoft Exchange Server and SQL Server.
- eFolder AMS: to backup your protected machines to the eFolder Acronis Cloud, an eFolder Acronis AMS must be provisioned for you. The eFolder AMS will include a storage node where you can store your cloud backups and will give you the ability to restore those backups to virtual machines in the eFolder cloud in case of a complete site wide disaster.

Important! To obtain your eFolder AMS you must agree to, sign, and return the Acronis Agreement(s). You can obtain the Acronis Agreement(s) from your assigned Account Manager.

System Requirements

Below is the current list of supported operating systems (see Table 1.1).

For file systems and storage media, see Table 1.2.

Supported Operating Systems:

Windows	Linux
<ul style="list-style-type: none"> • Windows XP Professional SP2+ (x86, x64) • Windows 2000 SP4—all editions except for the Datacenter edition • Windows Server 2003, 2003 R2—Standard and Enterprise editions (x86, x64) • Windows Small Business Server 2003/2003 R2 • Windows Vista—all editions except for Vista Home Basic and Vista Home Premium (x86, x64) • Windows Server 2008—Standard, Enterprise, Datacenter, and Web editions (x86, x64) • Windows Small Business Server 2008 • Windows 7—all editions except for the Starter and Home editions (x86, x64) • Windows Server 2008 R2—Standard, Enterprise, Datacenter, Foundation, and Web editions • Windows MultiPoint Server 2010, 2011, and 2012 • Windows Small Business Server 2011—all editions • Windows 8 and 8.1—Pro and Enterprise editions only (x86, x64) • Windows Server 2012 and 2012 R2—all editions • Windows Storage Server 2003, 2008, 2008 R2, 2012, and 2012 R2 	<ul style="list-style-type: none"> • Linux with kernel from 2.4.20 to 3.9 (support for kernel 3.9 starting with build 37975) and glibc 2.3.2 or later. • Various 32-bit (x86) and 64-bit (x86_64) Linux distributions, including: <ul style="list-style-type: none"> ○ Red Hat Enterprise Linux 4.x, 5.x, and 6.x ○ Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, and 13.04 ○ Fedora 11, 12, 13, 14, 15, 16, 17, and 18 ○ SUSE Linux Enterprise Server 10 and 11 ○ Debian 4, 5, and 6 ○ CentOS 5.x and 6.x ○ Oracle Linux 5.x (including UEK) and 6.x (including UEK)

Table 1.1

Supported File Systems and Storage

File Systems	Storage
<ul style="list-style-type: none"> • FAT16 and 32 • NTFS • ReFS * • Ext2, Ext3, and Ext4 • ReiserFS3 * • ReiserFS4 * • XFS * • JFS * • Linux SWAP <p>* Supported with limitations: http://www.acronis.com/en-us/support/documentation/AcronisBackup_1.5/index.html#1456.html</p>	<ul style="list-style-type: none"> • Hard disk drives • Networked storage devices (SMB and FTP) • CD, DVD, HD-DVD, and Blu-Ray • ZIP®, Rev®, and other removable media • P-ATA (IDE), S-ATA, SCSI, iSCSI, IEEE1394 (Firewire), USB 1.1, 2.0, 3.0 drives; and PC card • Tape drives and tape autoloaders • eFolder Cloud Storage

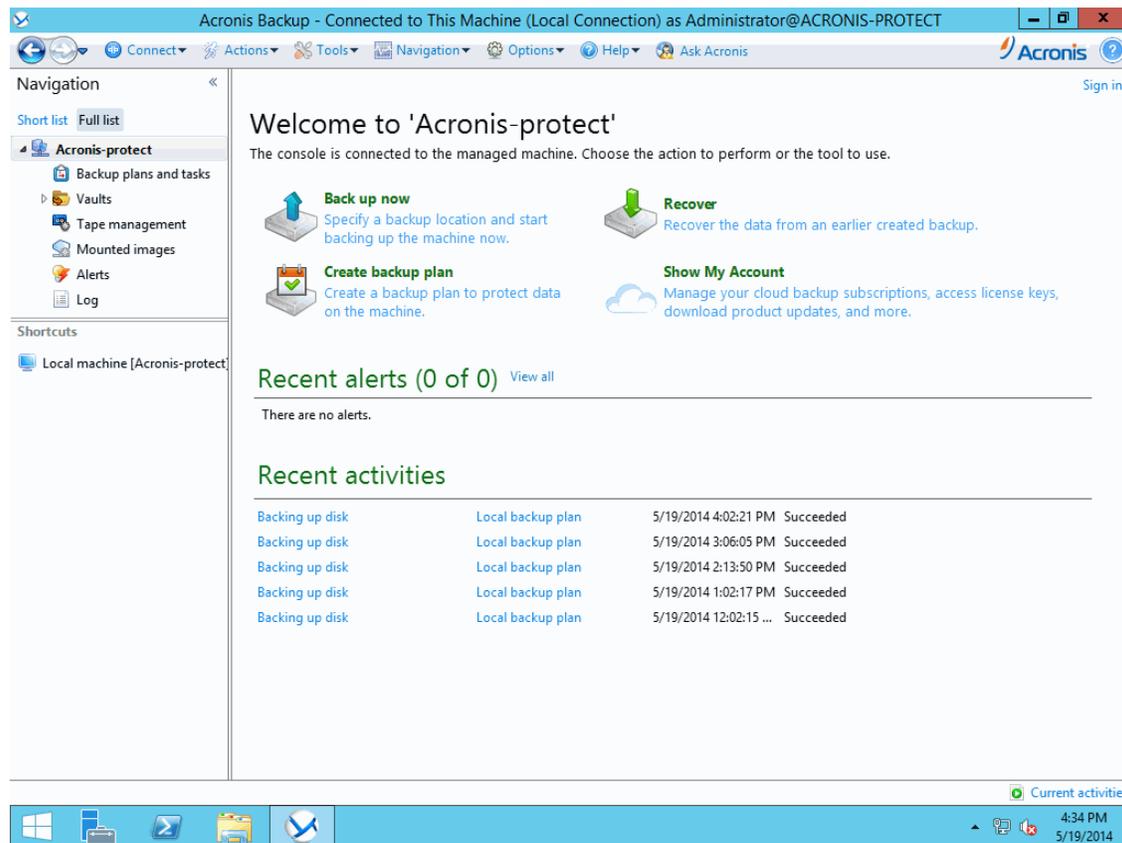
Table 1.2

Deployment Methods

There are two basic ways that the Acronis solution can be deployed: as an agent only/unmanaged backup and as a managed deployment. To take advantage of the offsite disaster recovery that the eFolder BDR/Cloud for Acronis offers, you must use the managed deployment method.

Unmanaged deployment

In an agent only/unmanaged deployment, only two Acronis components are necessary: the Acronis Backup Agent and the Acronis Console. The console is used to connect to the Acronis Backup Agent running on a protected machine; it allows you to configure the backup parameters of the Acronis Backup Agent. See figure 1.1



Managed Deployment

In a managed deployment of the Acronis solution, multiple components are deployed. Based on your architecture, you may choose to deploy all the components onto a device like a BDR appliance, or install the components on a machine that has low resource utilization that could handle the load that the AMS would put on it.

Provisioning Acronis Keys from the eFolder Web Portal

Acronis Backup Advanced license keys can easily be manually provisioned from the eFolder Web Portal.

Note: There is no need to contact Support or your Account Manager to provision an Acronis Backup Advanced license key.

Overview of the types of Acronis Backup Advanced license keys

There are three types of keys that can be provisioned from the eFolder Web Portal:

1. Acronis Backup Advanced Agent – a license that is assigned to a Backup Agent that has been installed onto an operating system.
2. Acronis Add-on Agent – an add-on agent that allows for the granular restore of application data like Microsoft (MS) Exchange, MS SQL Server, MS Active Directory, and MS SharePoint.
 - a. **Note:** Add-on agents are included with the subscription of the Acronis Backup Agent. The Acronis Backup Advanced agent will back up these technologies without the add-on license; however, to restore the granular application data out of the disk backup, the add-on license must be added to your Acronis license server running in the eFolder Cloud and then assigned to the protected machine running the application server.
3. Acronis Hypervisor or Virtual Host Agent – a license key that is assigned to a virtual host like MS Hyper-V or VMware vCenter that allows for the backup of unlimited VMs on that host.

Provisioning Acronis Backup Advanced License Keys

For you to manually deploy Acronis licenses from the eFolder Web Portal, you must agree to, sign, and return the Acronis Agreement(s) to your Account Manager. To obtain the Acronis Agreement(s) please contact your assigned eFolder Account Manager.

Important! eFolder requires a minimum purchase of three Acronis server licenses to begin offering eFolder's Acronis services. After the purchase of three server licenses, additional server licenses may be purchased one server license at a time. eFolder includes 1 TB of storage per Acronis server license per protected server. Additional storage over the included 1 TB per protected server costs \$.20 per GB per month. Storage is aggregated by customer not by partner. All server licenses are automatically activated and billable 15 days after being provisioned.

To manually provision Acronis Backup Advanced license keys, login to the eFolder Web Portal and select **Account Center** from the menu. If this is a new customer, a new account will need to be created and a service plan of *BDR for Acronis* assigned to that new customer. For instructions on how to create new accounts within the Web Portal, see the video in the Learning Center of the web portal entitled *Create an account using the New Account Wizard*. If you are provisioning licenses for an existing customer, create a *New Parent* account for this customer with the service plan of *BDR for Acronis*. After you have created a new account, in the Account Center, left click on the account to select the account and then either right mouse click or click on the Actions menu, mouse over **Service Plan**, and then select **Provision License Keys** from the pop-out menu (see Figure 1.2).

Important! It is recommended that you keep track of which license keys you provision to which customer. It is good practice to always create an account for the customer within the eFolder portal and provision the Acronis license keys under that customer's account. When adding the Acronis license key to the AMS license server installed at your customer's site, always use the licenses keys you provisioned for that customer. If your customer stops using the Acronis solution, you will be responsible to provide the license keys that need to be deprovisioned in order for eFolder to stop the billing of those licenses (see the section entitled Deprovisioning Acronis Licenses for more information). Failure to keep Acronis license keys organized and only installed to the assigned customer could result in additional license fees and penalties.

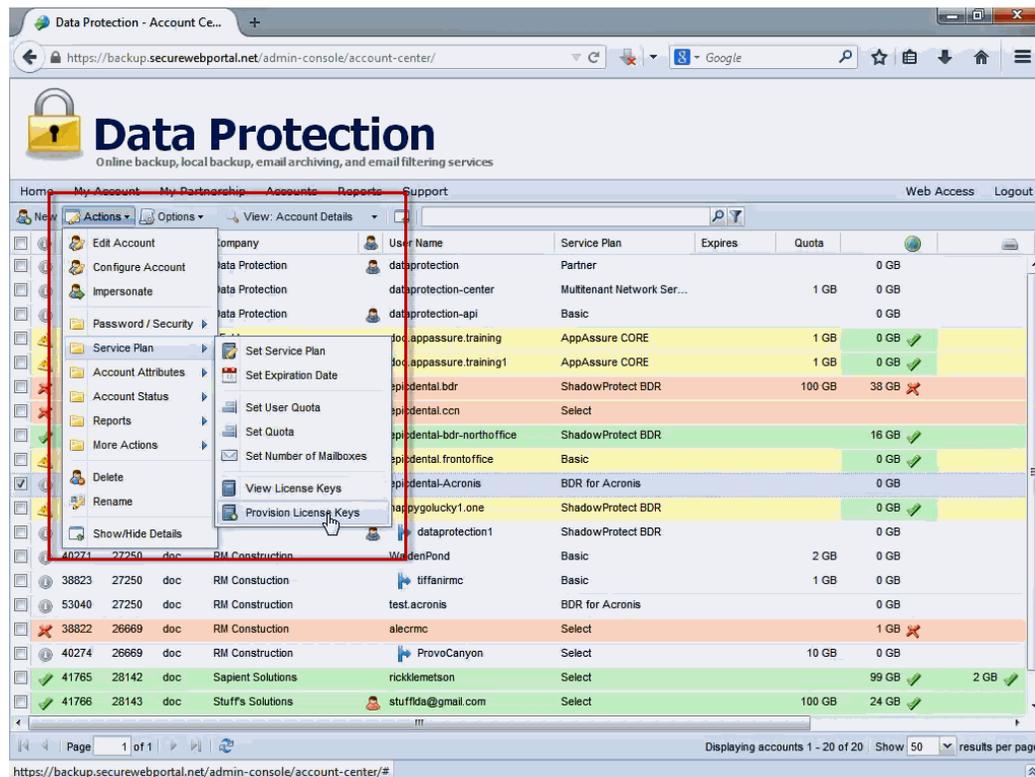


Figure 1.2

The Provision License Keys dialog box opens. In the *# of License Keys:* field enter in the number of licenses you are provisioning, then in the *License Key Type:* drop down, select the type of Acronis Backup Advanced license you need and click **OK** (see Figure 1.3). **Note:** Be sure to provision the correct type of license. For example, the Acronis Backup Advanced for Desktop will not activate on any server-class operating system. Also, you may notice that there is no Desktop option for Linux. Acronis has determined that all Linux Desktop operating systems can fulfill the roll of a server, so they treat a Linux Desktop operating system as a server operating system.

Important! Only provision the number of licenses you plan to deploy immediately. All Acronis licenses will be billable two weeks after they are provisioned regardless of they have been

activated or not. For example, if you provision five Acronis Backup Advanced for Servers today, but only use three of them, you will be billed for all five licenses after two weeks.

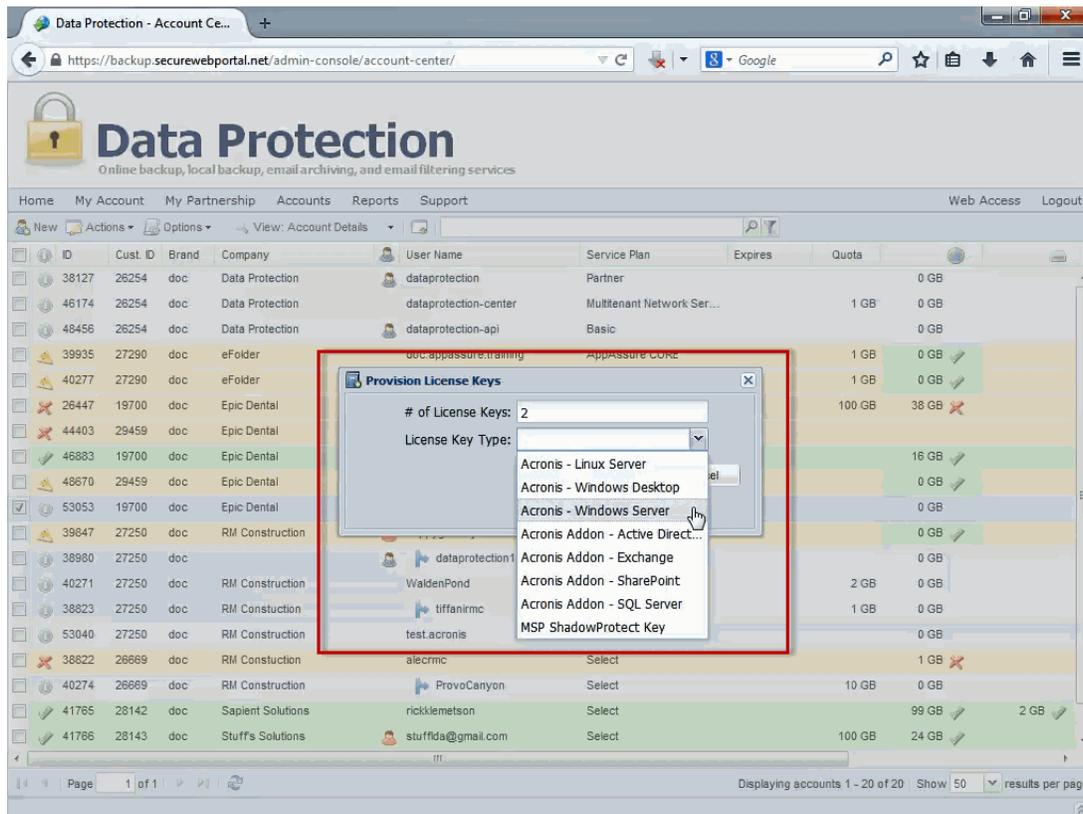


Figure 1.3

Note: If you do not see the listing for the Acronis licenses in the *License Key Type* drop down menu and you only see the option *MSP ShadowProtect Key* (see Figure 1.3.1), then your partner account has not been configured to provision Acronis licenses. For you to manually deploy Acronis licenses from the eFolder Web Portal, you must agree to, sign, and return the Acronis Agreement(s) to your Account Manager. To obtain the Acronis Agreement(s), please contact your assigned eFolder Account Manager. If you have already signed the Acronis Agreement(s), please contact your assigned Account Manager for help resolving this problem. After your account has been configured correctly, you might have to log out of the Web Portal and login again for the change to take effect.



Figure 1.3.1

A dialog box will appear showing you the newly provisioned license keys (see Figure 1.4).

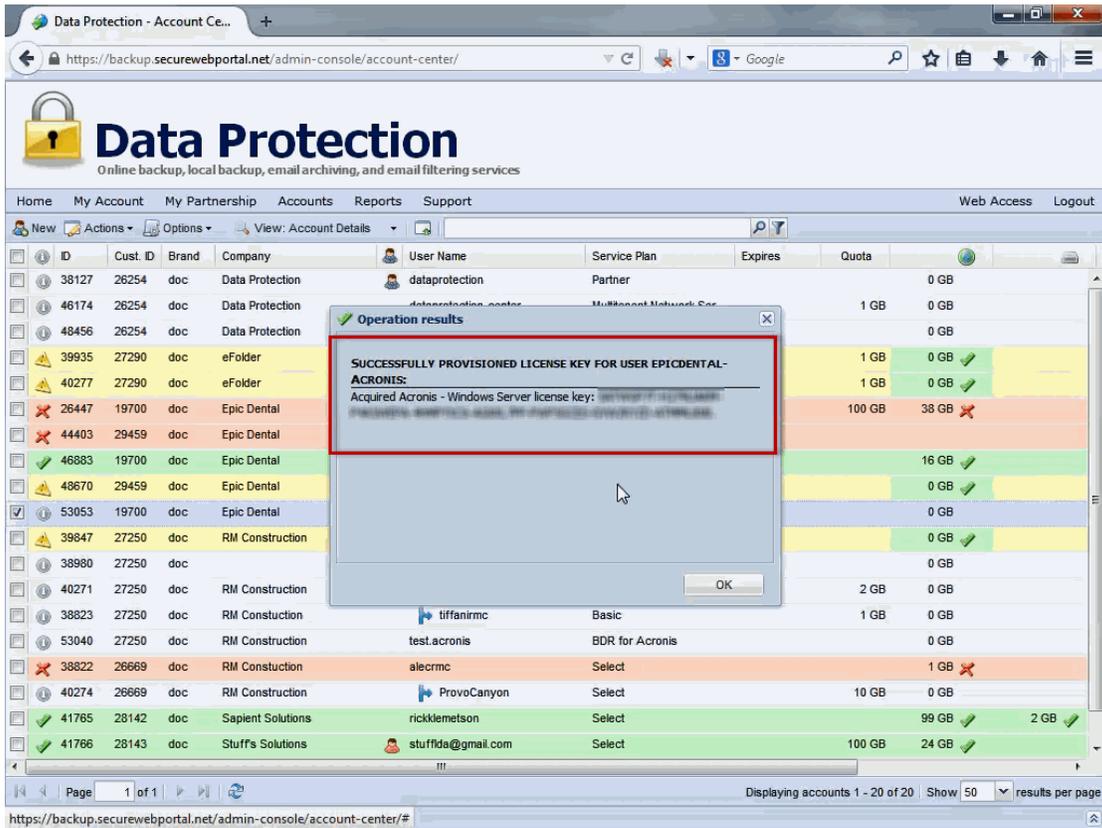


Figure 1.4

To view provisioned license keys in the web portal, in the Account Center, left click on the account that you provisioned the license key to, then either right mouse click or, click on the Actions menu, mouse over **Service Plan** and select **View License Keys** from the pop-out menu (see Figure 1.5).



Figure 1.5

Installing and configuring the Management Components

Although there are many ways of installing the Acronis solution, we will cover the interactive installation method. For instructions on other methods of deployment, please see the Acronis Installation Guide on the Acronis support page.

Download the latest version of the Acronis Backup Advanced 11.5 installer from the eFolder Knowledge Base at:

<https://secure.efoldering.com/support/index.php?/efolder/Knowledgebase/Article/View/278/67/acronis-for-efolder-download>

Note: This file is quite large as it contains all of the installation components necessary to install the management components and the backup agents. At the time of this publication, this file was almost 2 GB in file size, so it might be wise to save the installer onto portal storage for installation rather than downloading it at each site you plan to deploy.

These installation instructions will focus on installing the management components onto a BDR-type device where all the management components are installed onto one device. Note that it is possible to install the storage node onto other devices and then register them with the AMS.

Installing the Management Components

1. Login to the BDR as an Administrator and launch the Acronis Backup Advanced 11.5 setup program. Then select **Install Acronis Backup Advanced 11.5** (see Figure 2.1).

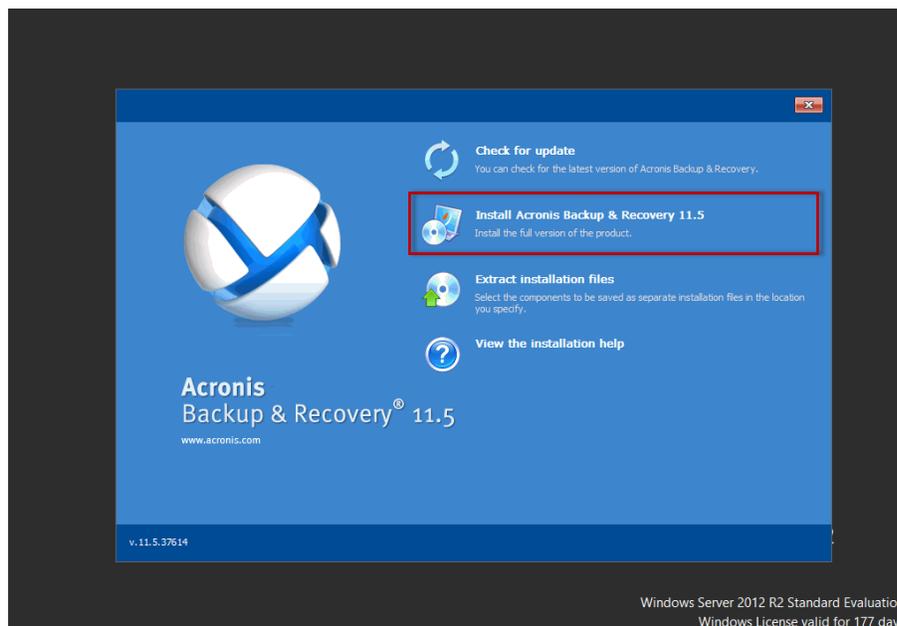


Figure 2.1

Note: The AMS uses TCP port 9876 for local installation and communication between components, and the setup program will automatically open this port through the Windows Firewall. If you are using a third-party firewall, you will need to open this port for both incoming and outgoing communication.

2. Read the Acronis Backup Advanced 11.5 license agreement and click the checkbox labeled I accept the terms of this agreement. Then click the Next button (see Figure 2.2).

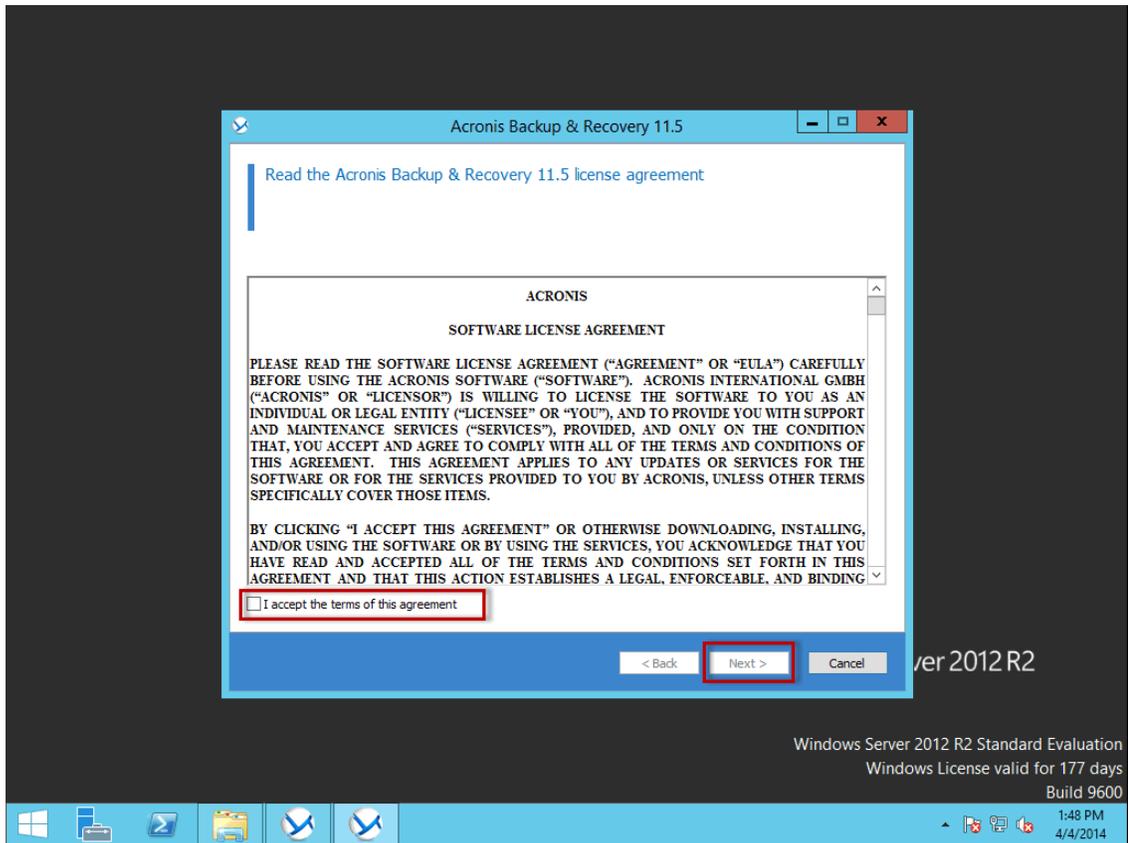


Figure 2.2

- Next, choose the options needed for the management installation. Mark the checkboxes by **Centrally monitor and configure the backing up of physical and virtual machines**, **Store the backups of other machines on this machine**, and **Connect to Remote machines**. Then select the **Next** button. (see Figure 2.3) This will allow for the management of the Acronis solution to be managed from one location.

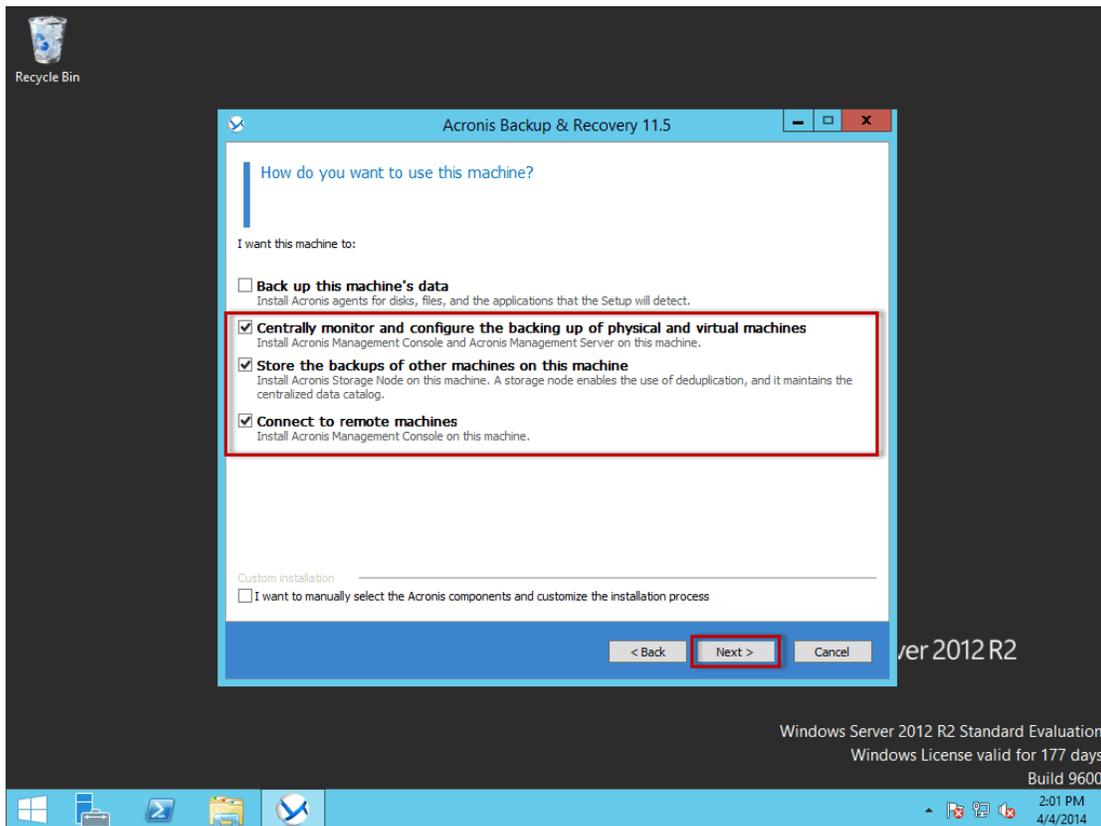


Figure 2.3

- The next screen asks if you would like to add or import any licenses at this time. If you have already provisioned Acronis license key(s) for this customer, you can enter them in at this time. If you skip this step, the licenses can be added to the AMS license server at a later time. Decide if you are going to enter in licenses key(s) at this time by entering them in to the text box or skip this step by clicking **Next** (see Figure 2.4).

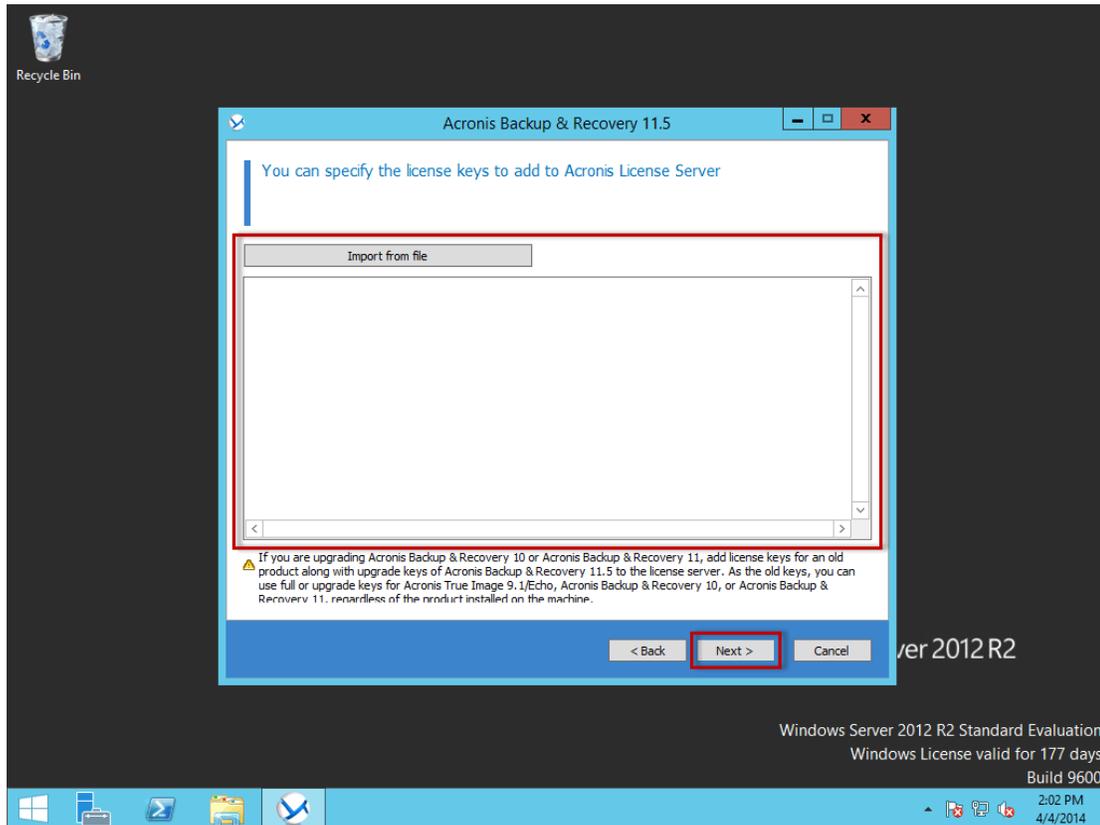


Figure 2.4

- Next, the option is given to either register an Acronis Backup Agent or a storage node. If you plan to store Acronis backups locally or need to use a seed drive to send your backup files to the eFolder cloud, then registering a local storage node is required. However, if you plan to only store Acronis images in the eFolder Cloud and you plan to upload those backup files directly to the eFolder Cloud over the Internet, then this step can be skipped.

For this step, go ahead and register the storage node on this same machine as the AMS. Select the radio button **Register now** and either enter the machine name, IP address, or browse to add this machine. Fill in the username and password with a user that has rights to this machine then click **Next**. (see Figure 2.5) If you choose to register these components later, you can add them in at a later time by using the Acronis Console and connecting to the AMS: select **Storage nodes** from the left side menu, then click **Add storage node** from the main window menu at the top. If you have another machine that you plan to use as a storage node, you must perform a custom install on that machine and then register the storage node on the AMS (see step 12).

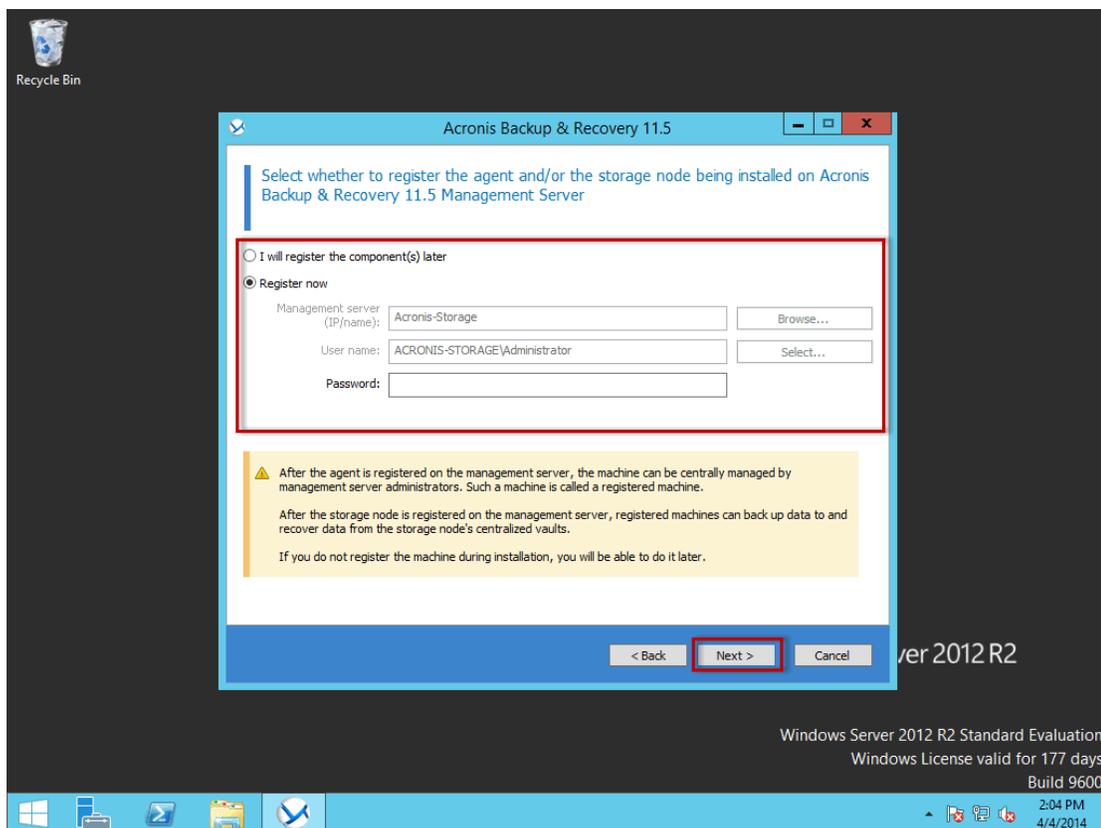


Figure 2.5

- You are now presented the option to participate in the Acronis Customer Experience Program (CEP). Select either the **Yes, I want to participate in the CEP** or the **No, I do not want to participate in the CEP** radio button and then click **Next** (see Figure 2.6).

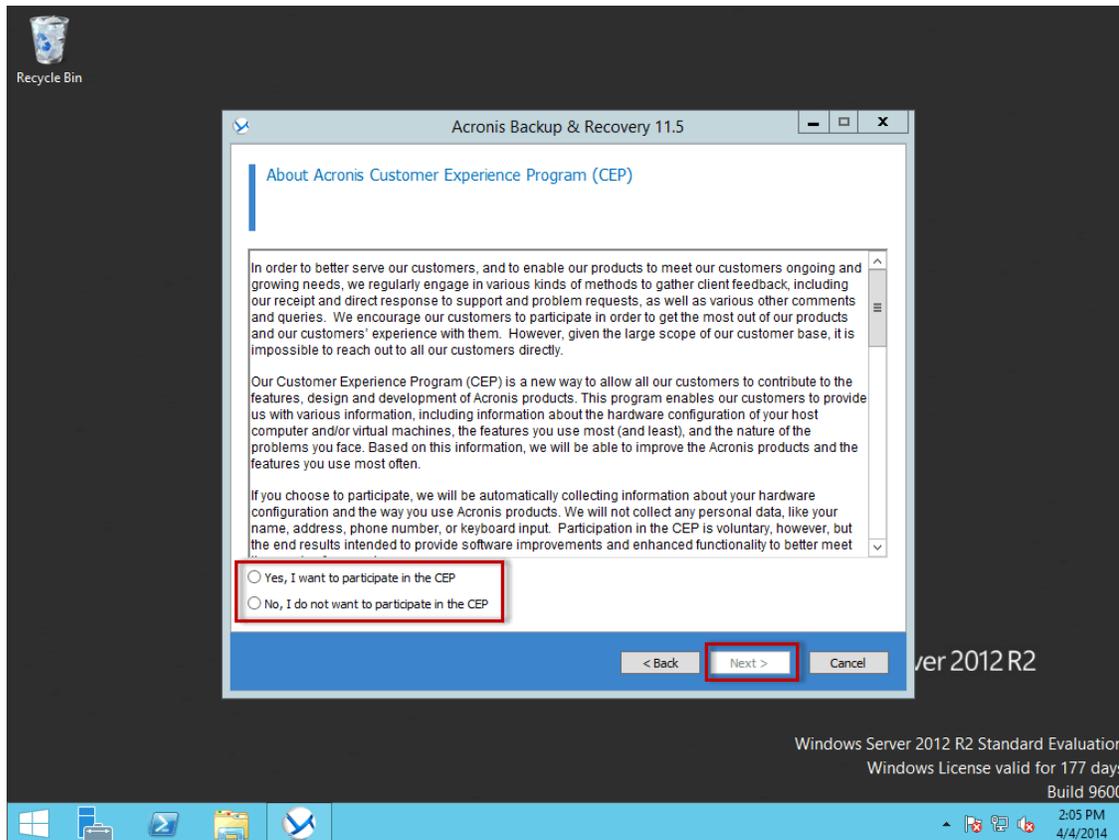


Figure 2.6

7. Now review the summary of the operations to be performed. If you are satisfied with your selections, click **Install**, or click **Back** to review or change your options (see Figure 2.7).

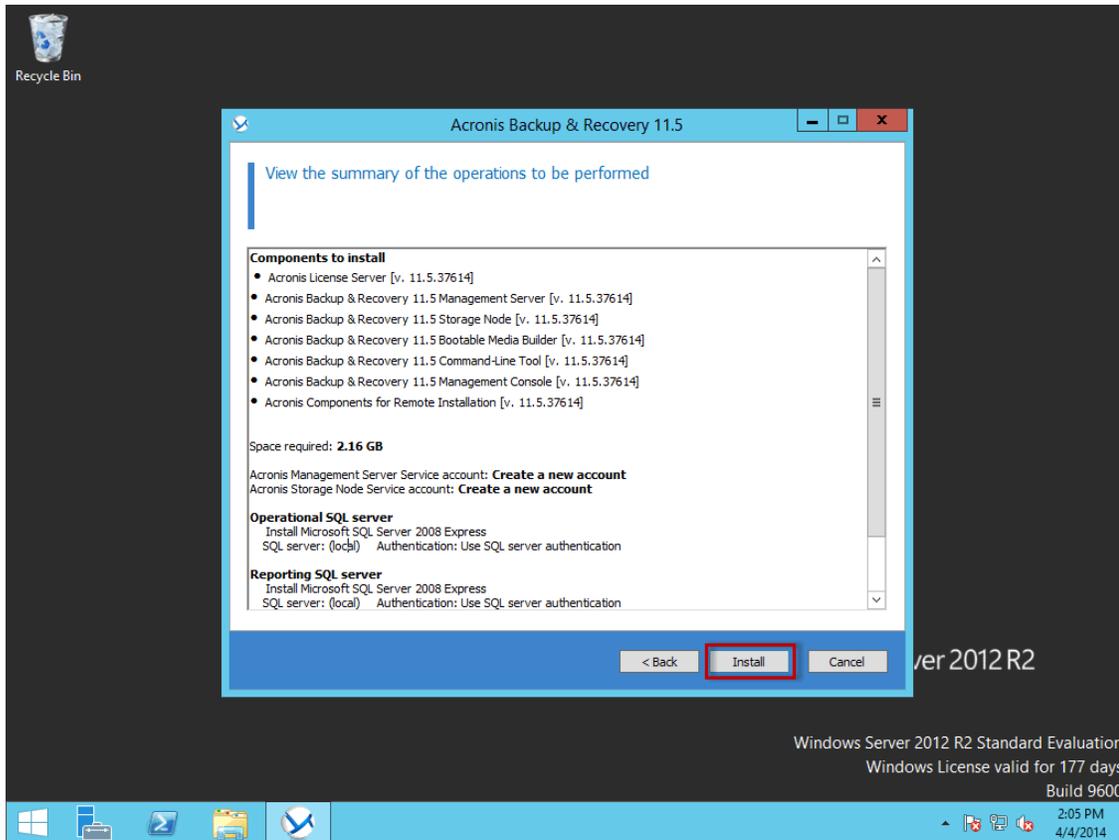


Figure 2.7

8. The Acronis Backup Advanced will now install. After it is completed, the installer will display the message "Installation has completed." Click **Finish** (see Figure 2.8), then exit out of the installer launcher back to the main menu (see Figure 2.1). The management components of the Acronis Backup Advanced are now installed.

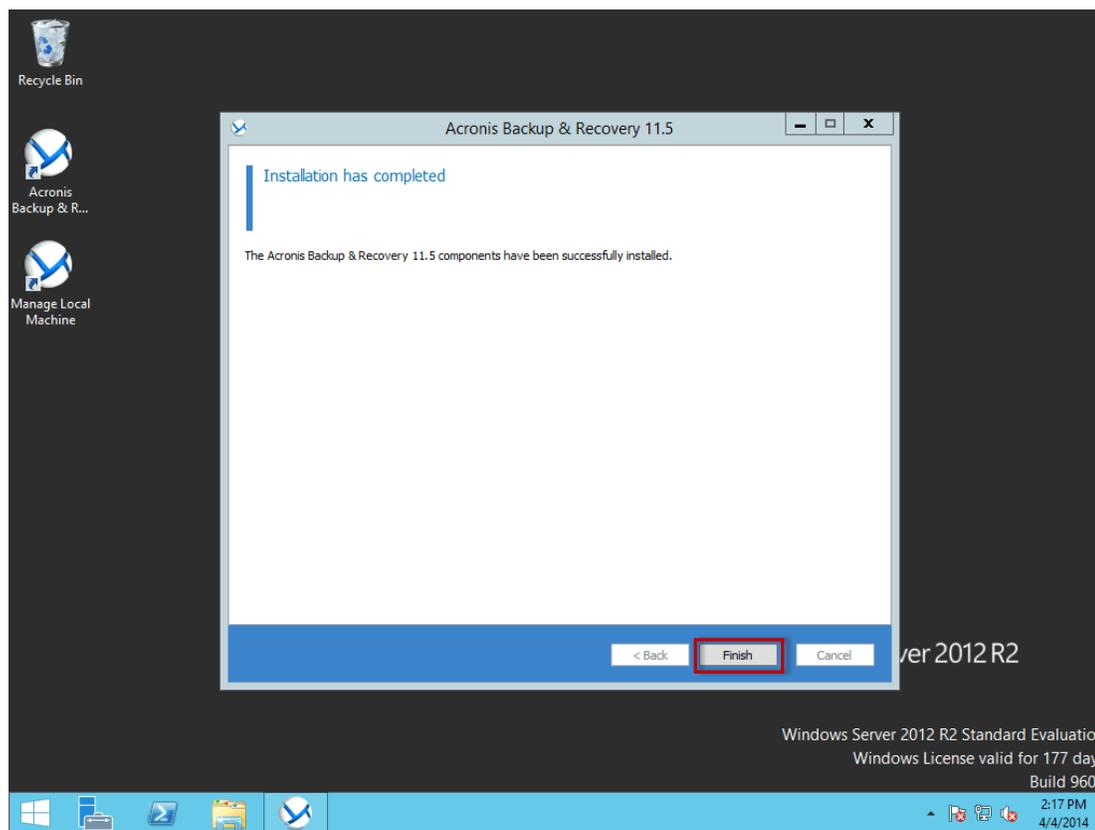


Figure 2.8

Configuring the Management Components

Now that you have successfully installed the management components, you will perform some of the necessary steps to configure the AMS. To begin, you will configure the storage node with a vault where your local Acronis backups will be stored.

9. By default, the installer created desktop icons to launch the Acronis Console that allows you to manage the installed AMS or connect to an Acronis Agent running on a protected machine (see Figure 2.9). Click this icon to launch the program. You can also launch the console from the Windows Start menu.

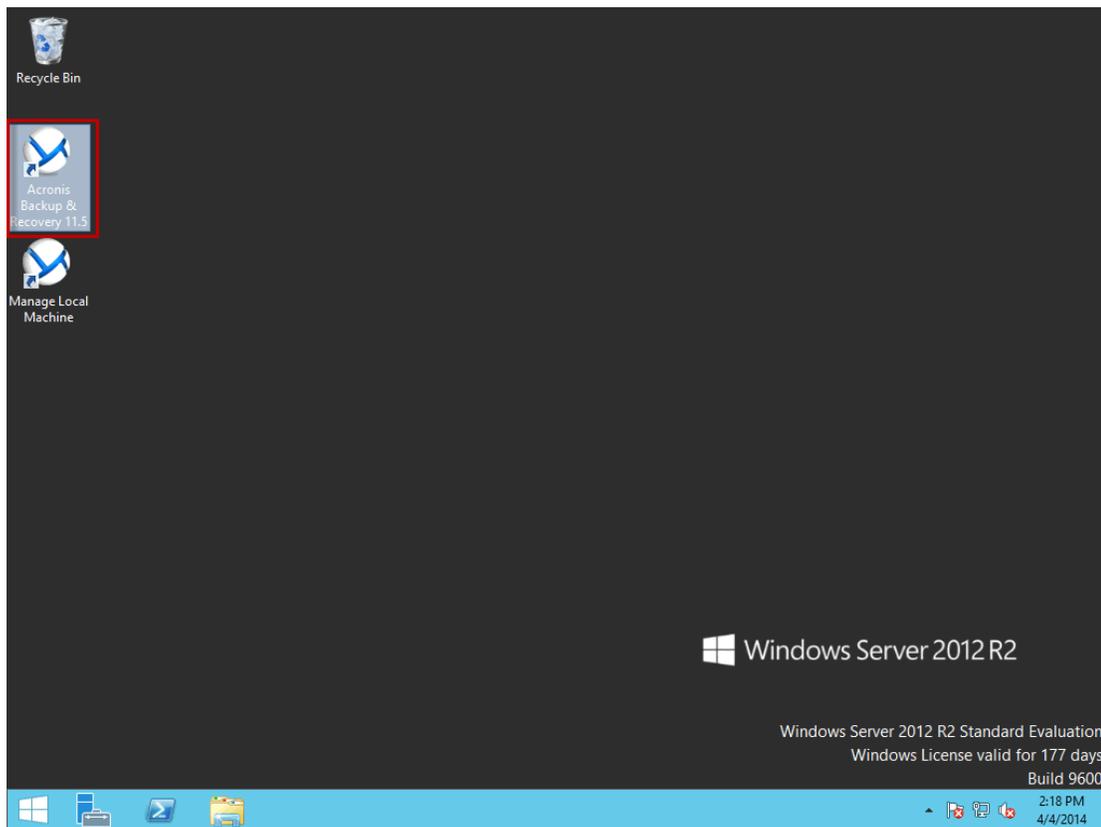


Figure 2.9

10. When the Acronis Console opens, you may be prompted with an available update and the option to create bootable media. For now, click **Close** on both of these prompts.

11. To manage the AMS, you first need to connect to it. Click the **Connect to a management server** menu option in the main window (see Figure 2.10) and then complete the machine information if you are connecting to the AMS from the same machine from which you launched the console.

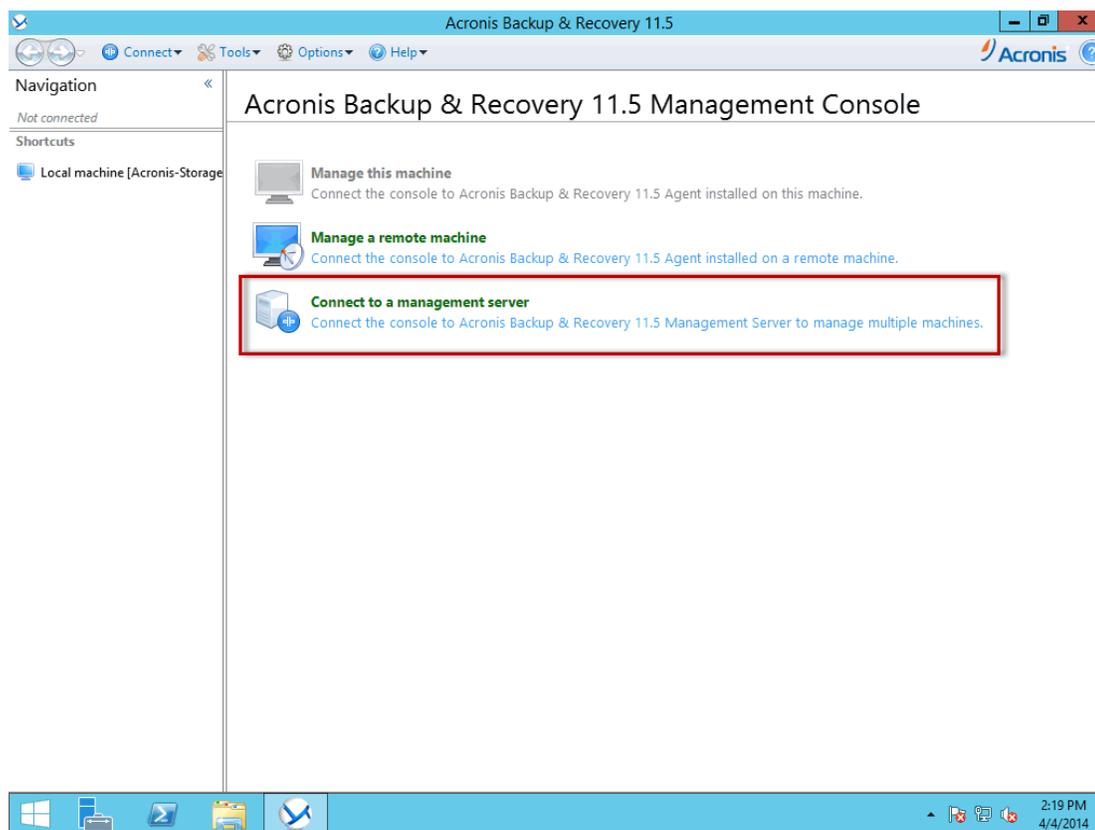


Figure 2.10

12. You are now connected to the AMS. If you followed step 5 from above, you should already have a registered storage node. You can verify this by selecting **Storage nodes** from the left hand menu, after which you should see this machine's storage node listed in the main window. If you did not follow step 5, you will now want to register a storage node by clicking **Add storage node**. After you have verified that you have a registered storage node, create a vault where you will store all of your Acronis backups by clicking **Vaults**, then **Centralized** on the left-side menu. Then click **Create** from the top menu in the main window (see Figure 2.11).

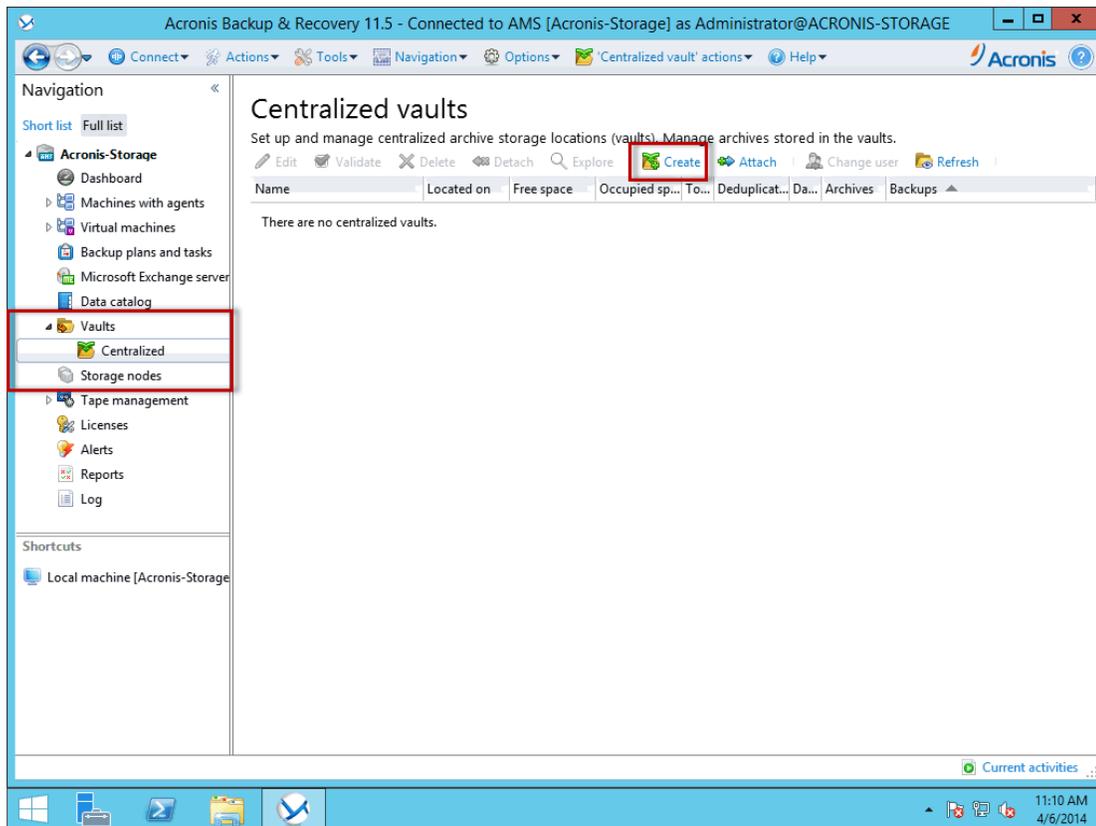


Figure 2.11

13. Fill in the *Create centralized vault* form (see Figure 2.11.1) by completing the following steps:

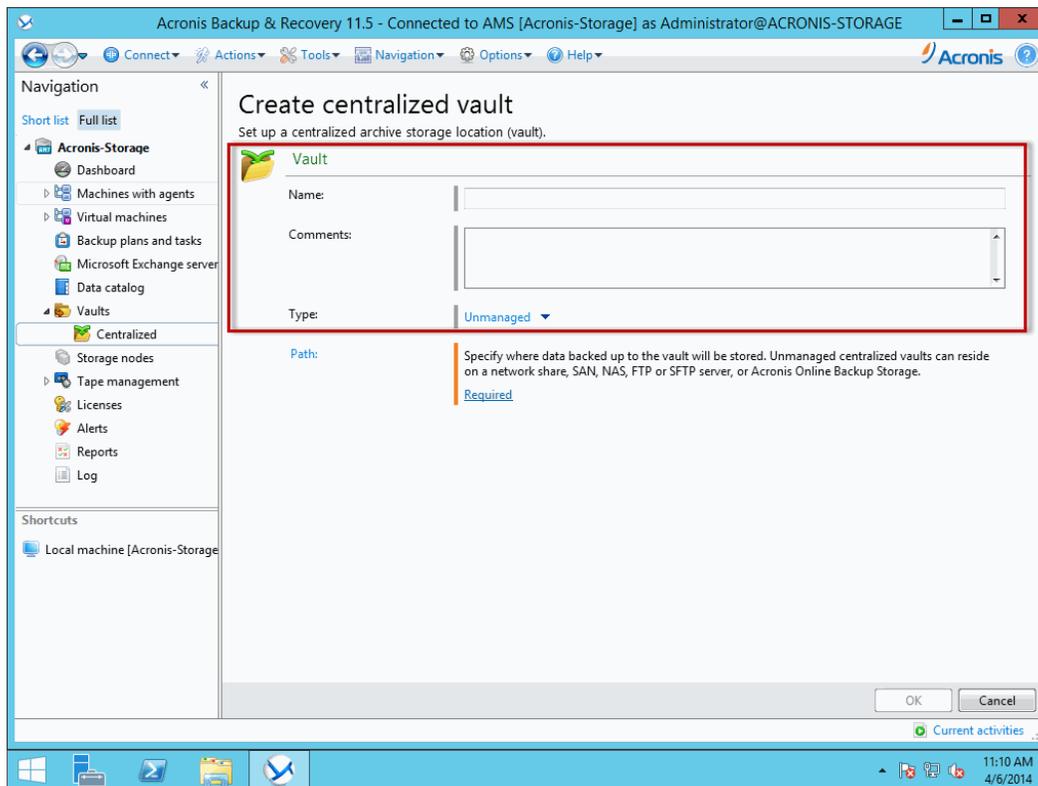


Figure 2.11.1

- Enter a name in the **Name** field. The **Name** field is what your vault will be known by, so create a meaningful name, such as *Acronis-Storage*.
- Enter any desired details about this vault in the **Comments** field.
- The **Type** dropdown menu has two options: Unmanaged or Managed. We recommend that you select **Managed** from the drop down menu. A managed vault provides the ability to duplicate the data that is stored within the vault. This means that identical data will only be backed up to this vault once. This minimizes the network usage during backup and the storage space used by the Acronis backups.

Note: If you plan to store backups locally as well as send them to the eFolder Cloud, there are considerations on using a managed vault locally. First, within a managed vault, all backups are stored within a database-type file structure; therefore, older traditional .TIB files that you may have been used to seeing will not be found. If you are used to working with .TIB files, then you probably mounted a .TIB file as a drive letter on your system for file and folder restore. When backing up to a managed vault, this feature of mounting an image is not available. However, files and folders can still be recovered by performing a Recovery task within AMS.

After you have selected **Managed** as the type of vault you are creating, some additional fields are displayed for you to fill in (see Figure 2.11.2) as explained below.

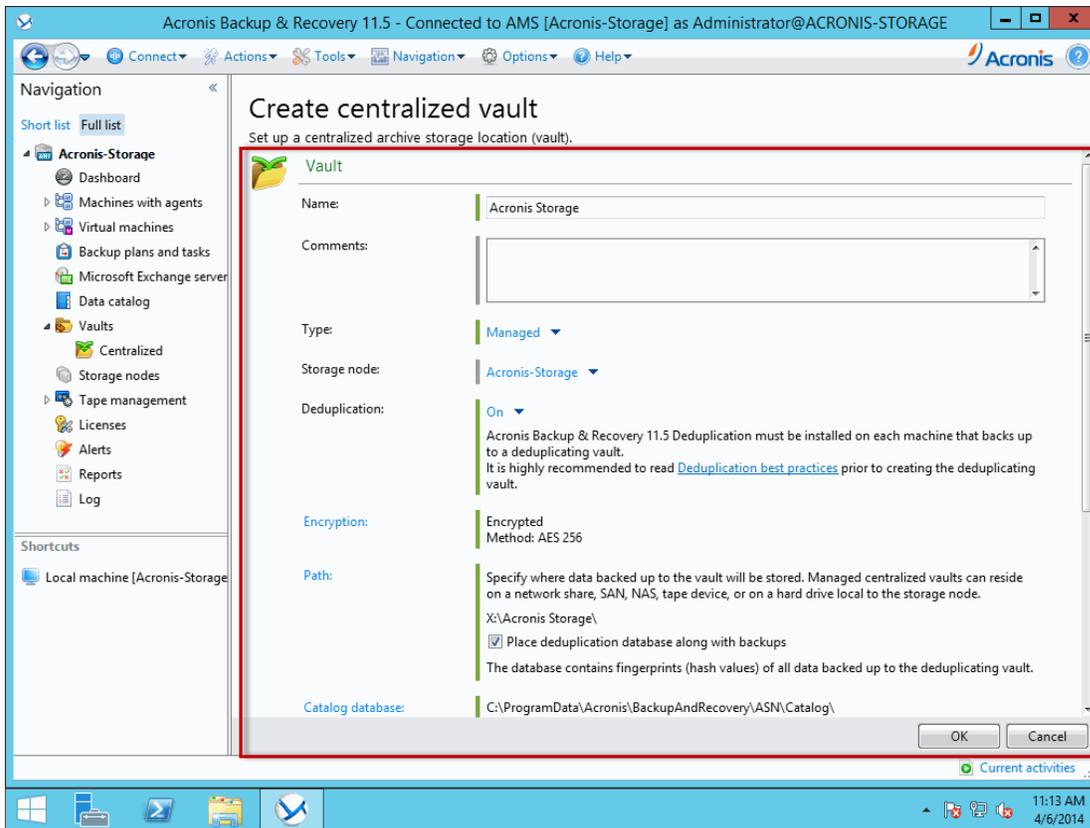


Figure 2.11.2

- d. Select the storage node desired from the **Storage Node** dropdown menu. Select the storage node you registered during the installation process (see Figure 2.11.2).
- e. Next, ensure that Deduplication is set to **Off**.

Note: Enabling deduplication requires more CPU cycles and RAM. If you do enable deduplication, we recommend that you have approximately 8 GB to 20 GB of RAM per TB of deduplicated data.

- f. Enable encryption by clicking the blue **Encryption** link in the main window (see Figure 2.11.2). The vault encryption dialog box appears. In the **Select the encryption algorithm** dropdown list, select the desired AES encryption (AES 128, AES 192, or AES 256.) We recommend that you select the **AES 256** option. Now enter your encryption word or phrase in the **Enter the word** field and re-enter it in the **Confirm** field and then click **OK** (see Figure 2.11.3).

Note: The encryption word or phrase has a 25 character limit.

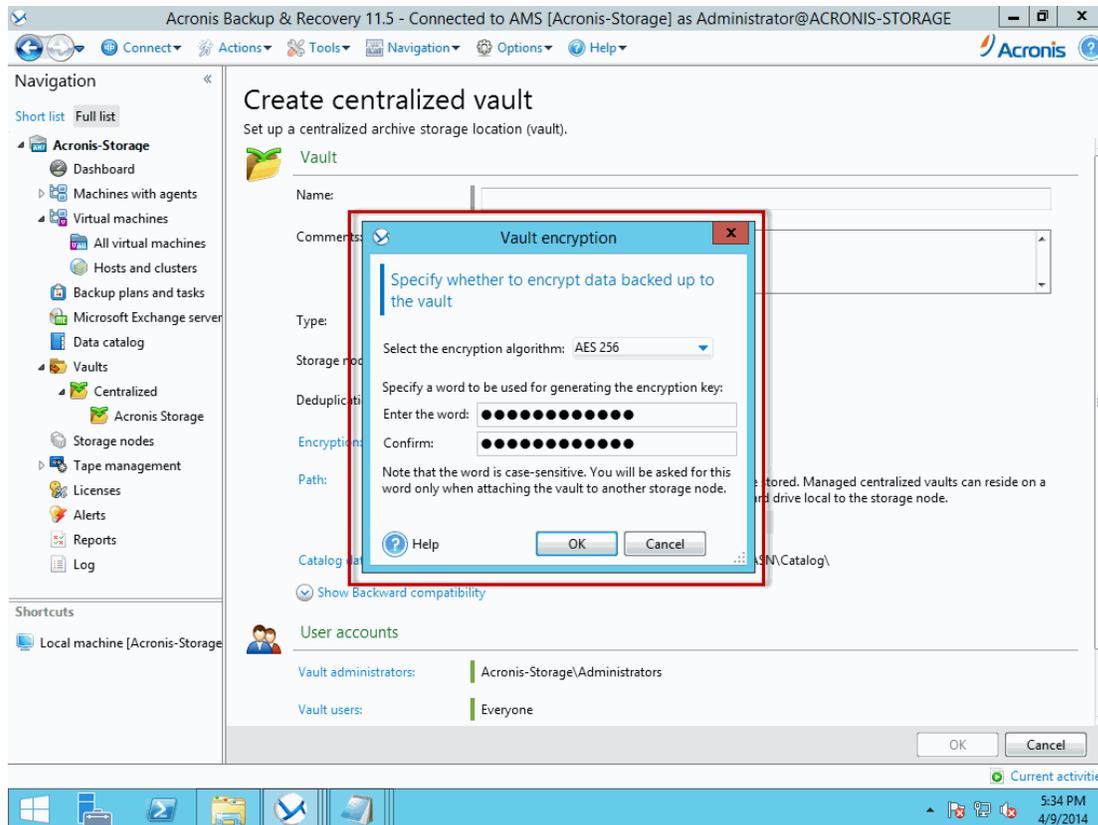


Figure 2.11.2

- g. Next, you will select the path to where your data will be stored. Managed centralized vaults can reside on any network share, SAN, NAS, or on a hard drive local to the storage node. In the example shown in Figure 2.11.2, the data will be stored on a hard drive that is installed on the same machine as the storage node. Click the blue **Required** link in the **Path** field to open the *Vault Path* dialog box. Expand the volume where your data will be stored, then select a folder on the volume (see Figure 2.11.2).

If you have enabled deduplication, you have the option of storing the deduplication database along with the backups. Check the checkbox labeled **Place deduplication database along with backups** to enable this option, if have enabled deduplication.

If you did enable deduplication but did not enable the option above for storing the deduplication database along with the backups, you will need to specify the path to where the deduplication database will be placed (see Figure 2.11.2). If you have deduplication set to off, you can skip this step. To specify the path, click the **Required** link in the Deduplication database: section and the *Vault Database Path* dialog appears (see Figure 2.11.4). Select a folder location on the local machine and click **OK**.

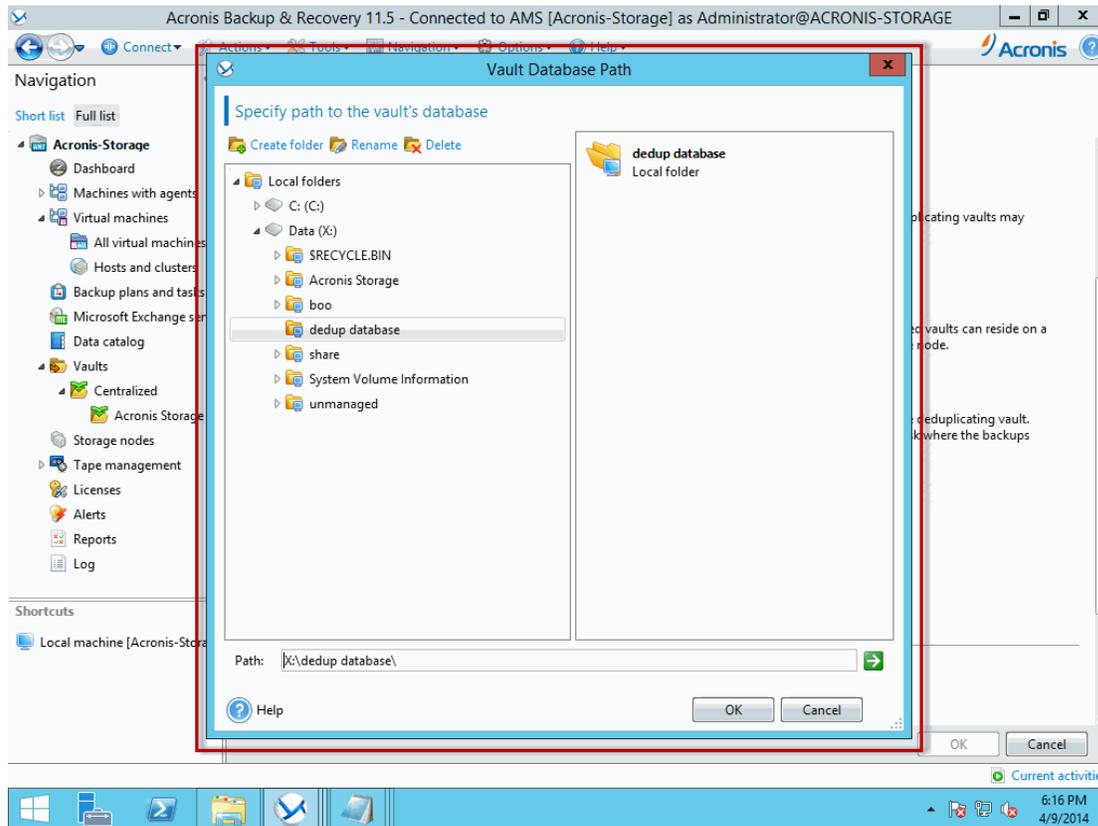


Figure 2.11.4

- h. If you want, you can edit the location of the Catalog database from its default location by clicking the blue **Catalog database:** link in the main window (see Figure 2.11.2).
- i. In the *User Account* section, you can specify vault administrators and vault users. Vault administrators can backup to the vault but also have full control over the vault's content. Vault users can backup to the vault but only manage their own archives.

The process of setting up a managed vault is now complete.

14. All of the Acronis licenses that you obtain from eFolder are managed from within the AMS license server that is installed at each of your customer’s locations. Here, you can enter Acronis license key(s) into the AMS license server and manage the Acronis licenses from one central location at your customer site.
 - a. If you did not add any license keys during the installation, you can add them by clicking **Licenses** in the left *Navigation* window (see Figure 2.13) in the main management window. If you have already added licenses to this deployment, they will appear here.
 - b. To add an Acronis license click the **Add License...** button in the main management window (see Figure 2.13).

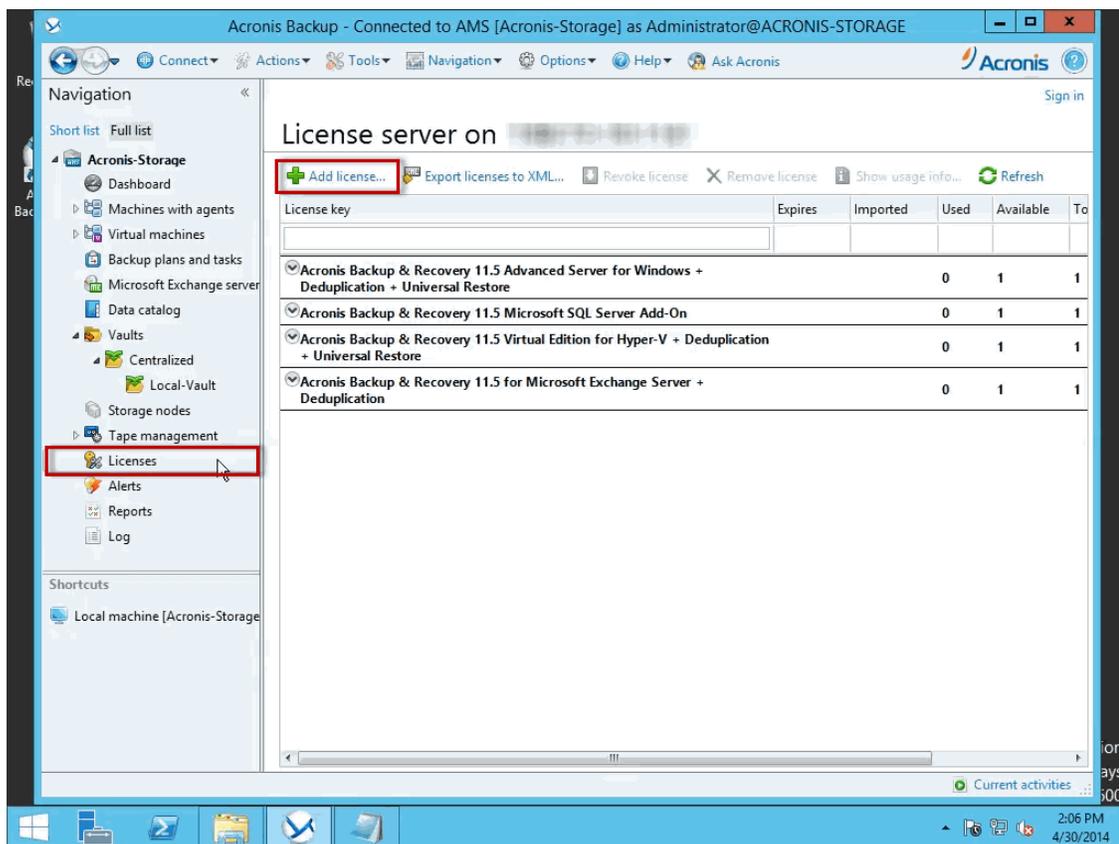


Figure 2.13

- c. The *Add License* window appears, here you can either manually type, paste, or import keys from a file. Enter your license key(s), then click **OK** (see Figure 2.14).

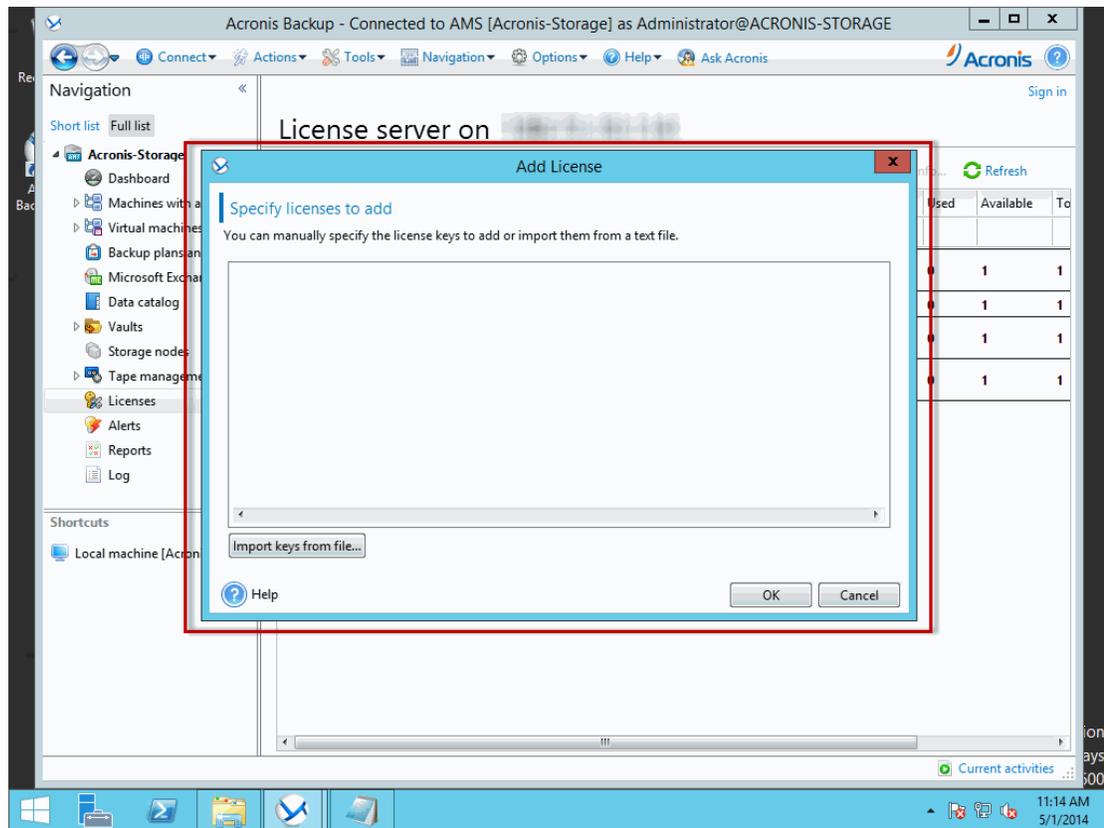


Figure 2.14

Your local AMS license server is now configured to manage the Acronis licenses. In a later section (see *Installing and Configuring the Acronis Backup Agent*), you will be able to register the Acronis backup agent with this AMS license server to assign a license key to the agent being installed.

Connecting/Configuring the AMS and Storage Node

This section will cover the instructions and steps necessary for you to connect to the remote eFolder Acronis Management Server (AMS) and storage node to setup and manage your Acronis Cloud Vault. The Acronis Cloud Vault is where you will store your off-site Acronis backup images for your customers. To maximize your cloud vault, you must set up a managed vault with de-duplication enabled. Also, you will configure the encryption type and an encryption key necessary for your managed vault to store all of your customer's data encrypted in the eFolder cloud.

Important! To obtain your eFolder AMS you must agree to, sign and return the Acronis Agreement(s). You can obtain the Acronis Agreement(s) from your assigned Account Manager.

Important! All data in your Acronis Cloud Vault must be encrypted. It is eFolder's policy that all data stored within the eFolder cloud be encrypted. Encryption is also required for eFolder to maintain its HIPAA compliancy; therefore, when you create a managed vault within the eFolder Acronis cloud, eFolder will run periodic checks to ensure that the vault has encryption enabled. If it is not encrypted, you will be required to work with eFolder to encrypt your Acronis Cloud Vault. Also, you may experience an interruption in service if your Acronis Cloud Vault is found to be unencrypted.

To connect to your eFolder AMS, select **Connect** on the menu bar and **New connection** from the drop down list. Then click **Connect to management server** from the pop-out menu (see Figure 3.1).

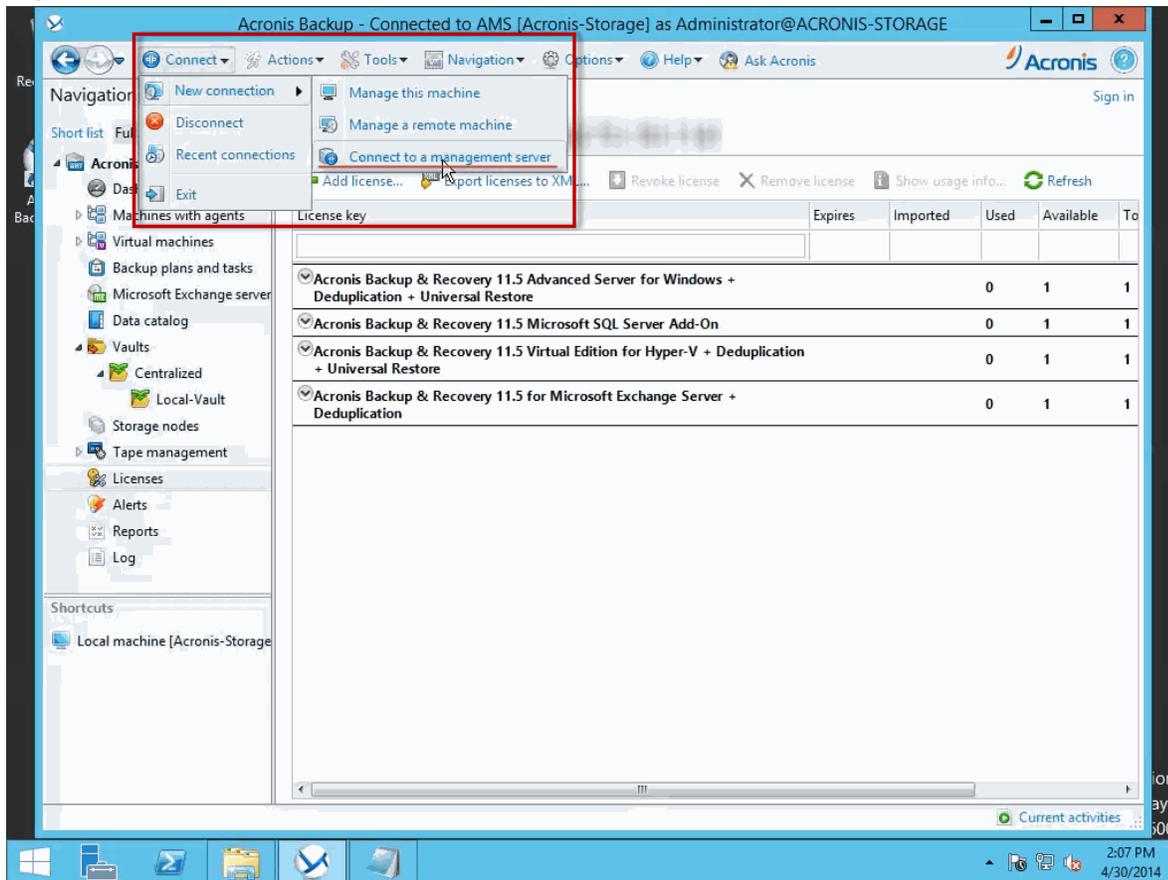


Figure 3.

The *Management Server Connection* dialog box appears. In the **Machine:** field, enter the URL or the IP address of your eFolder Acronis AMS, enter your username and password in the *Logon settings* fields, and click **OK** (see Figure 3.2).

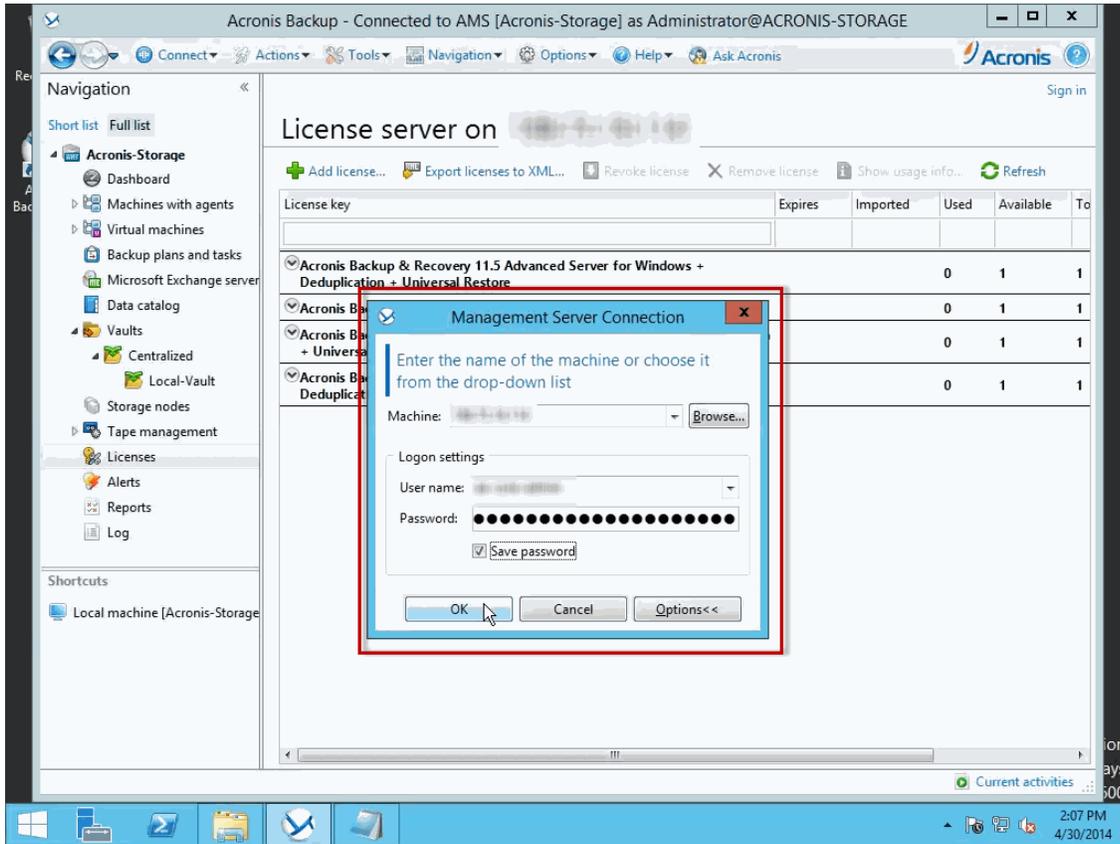


Figure 3.2

- After you are connected to your eFolder AMS, your Acronis console will be directly managing your eFolder Acronis AMS. In the title bar and welcome message, check the name of the server to ensure that you are truly connected to the remote AMS (see Figure 3.3).

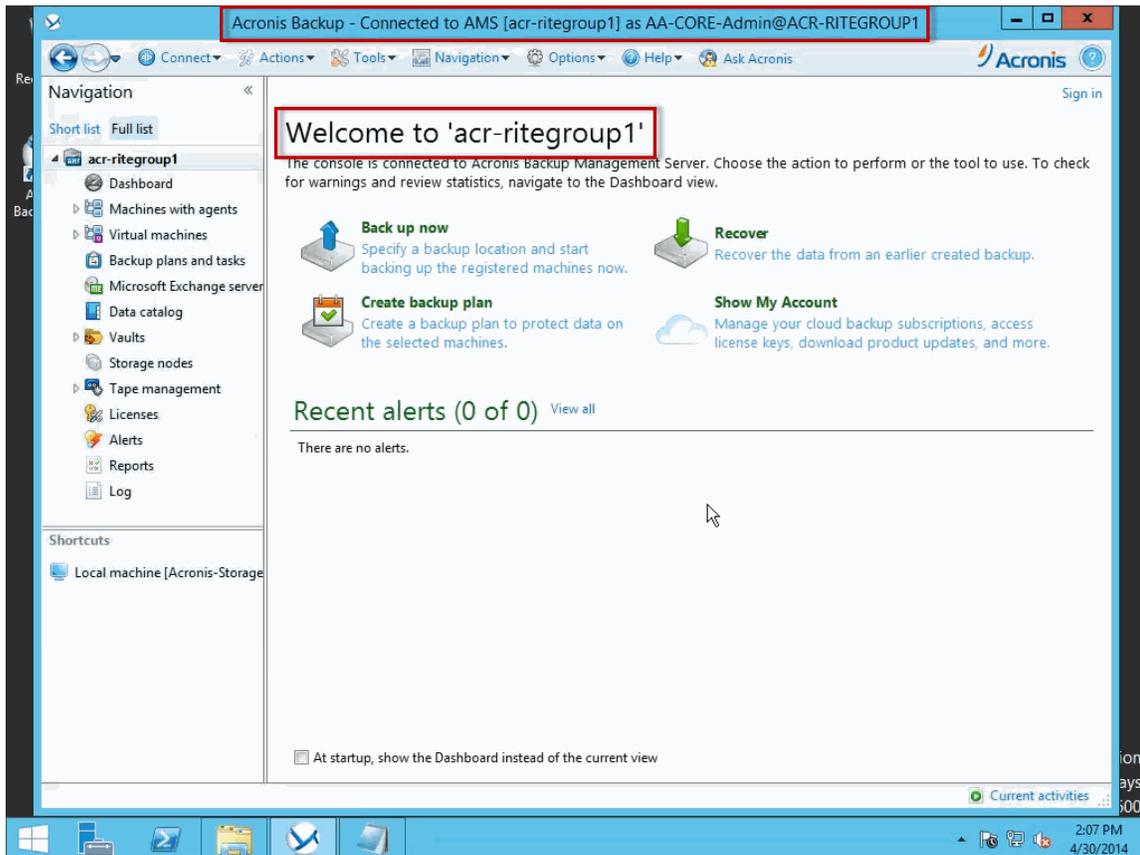


Figure 3.3

- The next step is to configure your Acronis managed vault to receive incoming backups. If you previously set up a managed vault in step 13 of *Installing the Management Components*, this step will be familiar to you. However, for performance reasons, you will be picking a different location for your de-duplication database than you did in the above-mentioned step.
 - a. From the Navigation menu, click **Vaults** and then **Centralized**. Then fill out the form like you previously did on your local vault (see Figure 3.4.1).

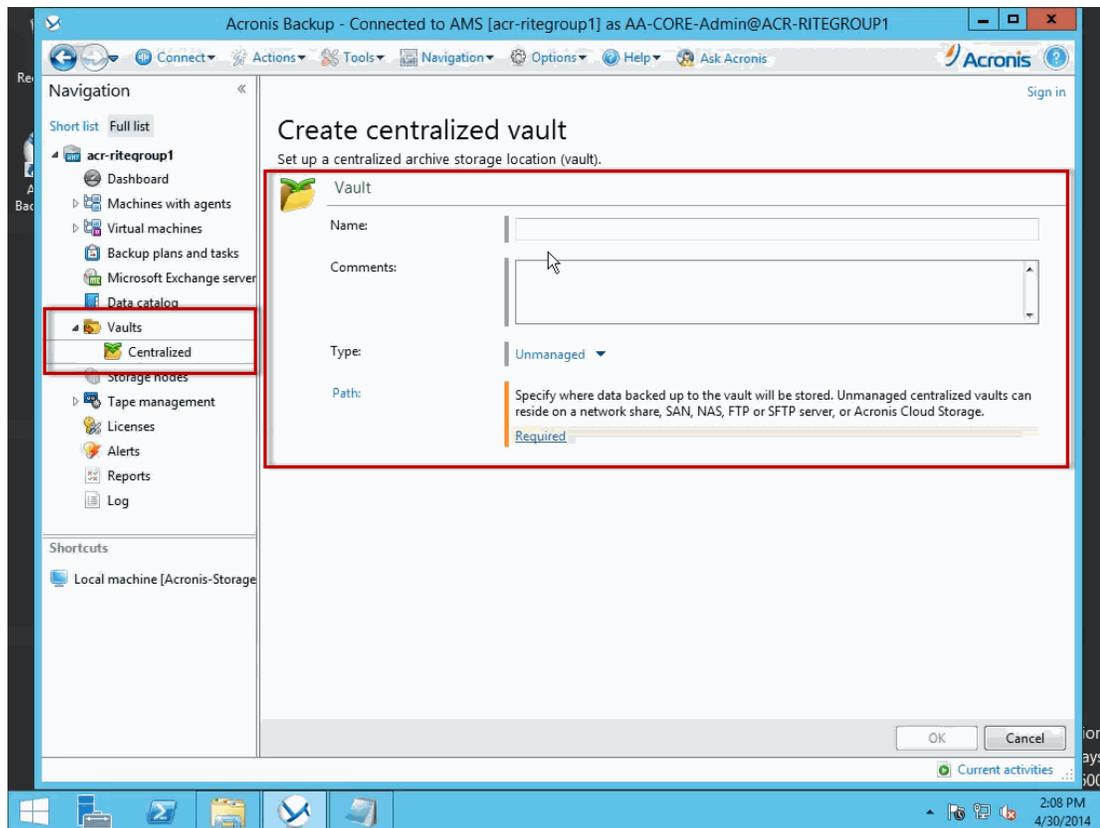


Figure 3.4.1

For help in filling out this form, refer to step 13 in the section of this document labeled *Installing the Management Components*. However, note that in steps G and H of step 13, you will need to make the following changes to complete the current step:

- In step G, specify the path to the vault by clicking the **Required** blue link. After the Vault Path window displays, click the Data(X:) value under the *Local folders* file structure. Then select the Vault folder you want as your vault destination and click **OK** (see Figure 3.4.2).

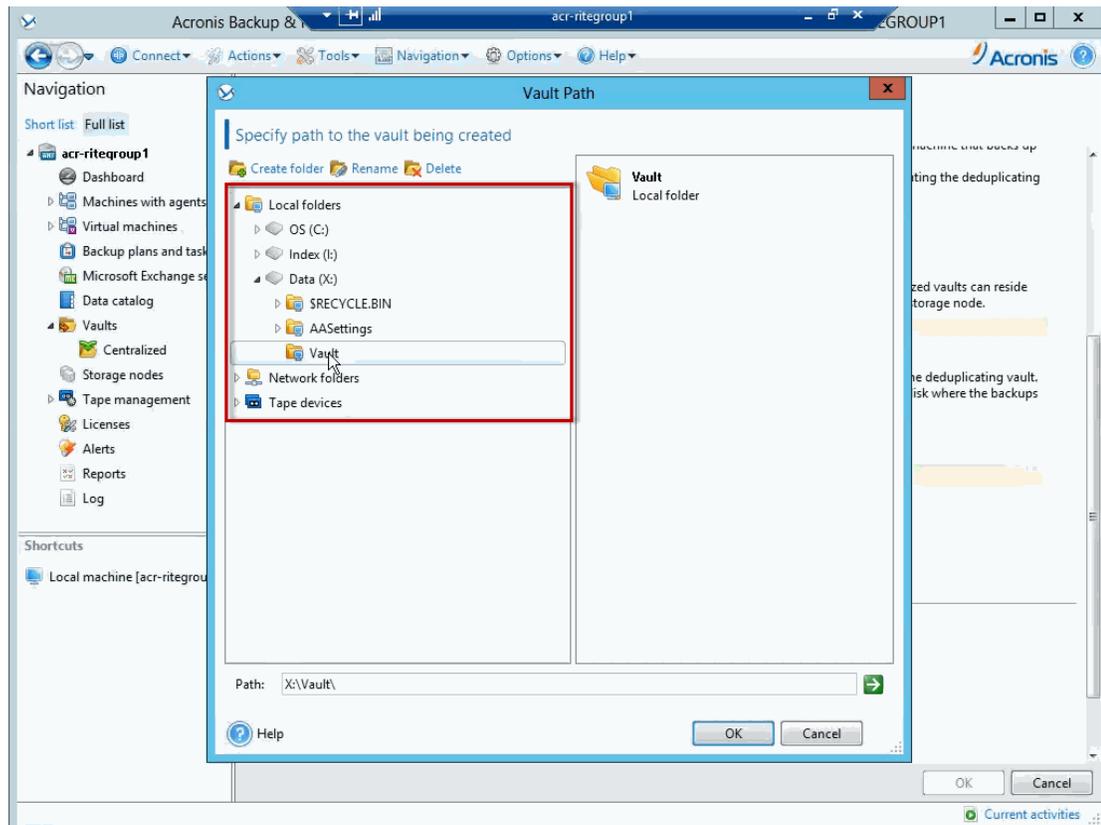


Figure 3.4.2

- In step H, you specify where the de-duplication database will be placed. Select The **Index(I:)** volume under *Local folders*, choose the **Dedupe** folder, and then click **OK** (see Figure 3.4.3).

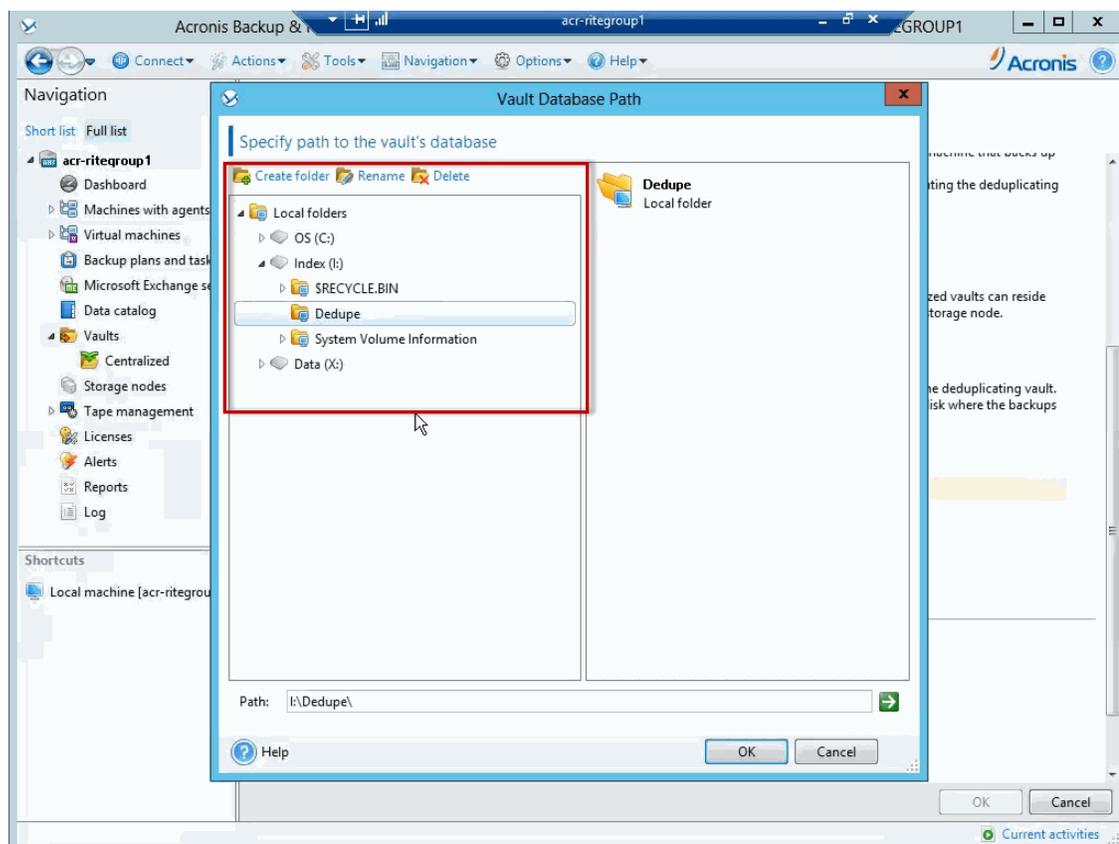


Figure 3.4.3

When you have completed the Create centralized vault form (see Figure 3.4.1), click **OK** to finish setting up your Acronis Cloud Vault. The resulting display should look similar to Figure 3.5.

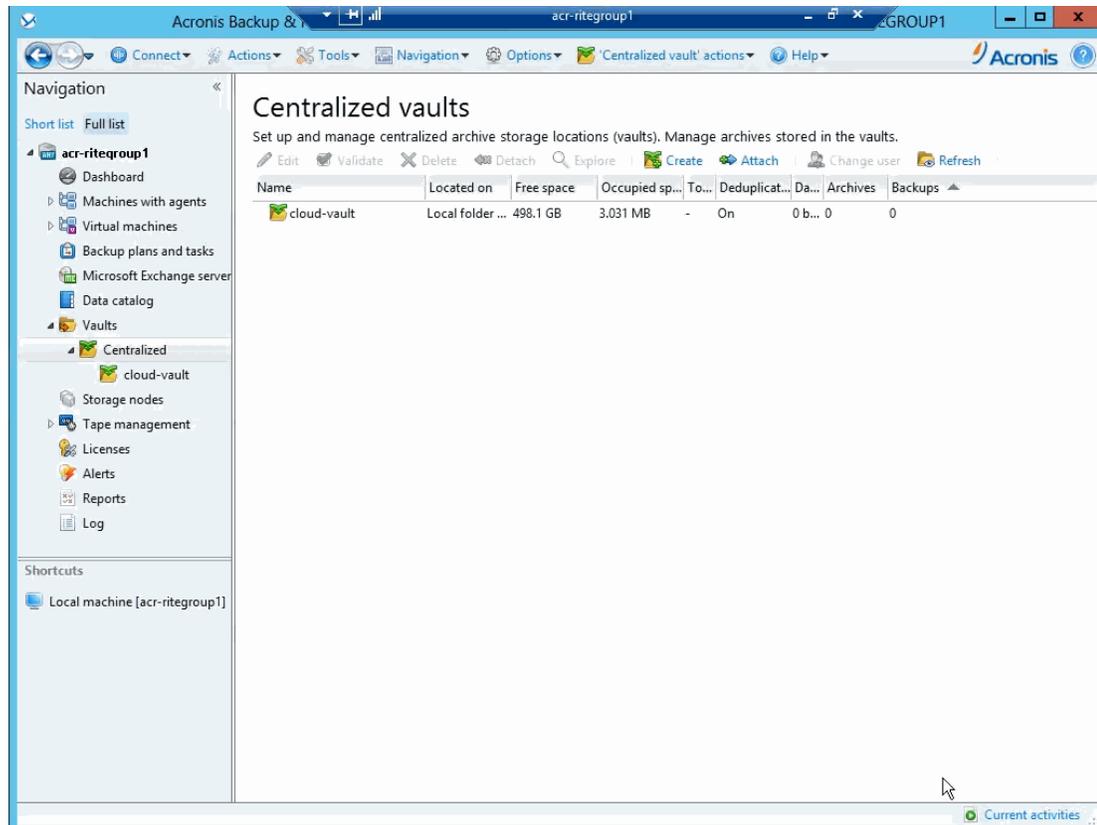


Figure 3.5

Installing the Acronis Backup Agent: Configuring backup schemes

The Acronis backup agent is the software component that is installed onto the machine you want to protect with Acronis. The Acronis backup agent will be registered with the Acronis Management Server (AMS), and the AMS will provide the licensing for the backup scheme and the storage for the local Acronis backup images.

To configure Acronis to backup locally (and also to the eFolder cloud) two backup schemes are required. The first scheme is configured to back up the protected machine to the local storage node; the second scheme is configured to back up the protected machine to the eFolder cloud. This section of the document is organized into three parts.

1. First, you will be shown how to install the Acronis backup agent onto the machine to be protected and then register the agent with the local AMS.
2. Second, on the AMS, you will be shown how to create a backup scheme for the local backup.
3. And third, you will be shown how to configure a second backup scheme that will be used to send the Acronis backup images to the eFolder cloud.

This third section is further organized into two parts: first, you will be shown how to preload data to the eFolder cloud using a seed drive, and second, you will be shown how to preload data to the eFolder cloud directly from the AMS.

Installing the Acronis backup agent

There is more than one way to deploy the Acronis backup agent onto the machine you want to protect. Two of the more common ways to deploy the agent are to either deploy the agent from the AMS onto the target machine, or to manually install the agent directly on the target machine with the Interactive Installer. These instructions will cover the latter option of installing the agent manually onto the target machine.

1. Login to the target machine as an administrator and launch the Acronis Backup Advanced 11.5 setup program. Then select **Install Acronis Backup Advanced 11.5** (see Figure 4.1).

Note: The AMS uses TCP port 9876 for local installation and communication between components. The setup program will automatically open this port through the Windows Firewall. If you are using a third-party firewall, you will need to open this port for both incoming and outgoing communication.

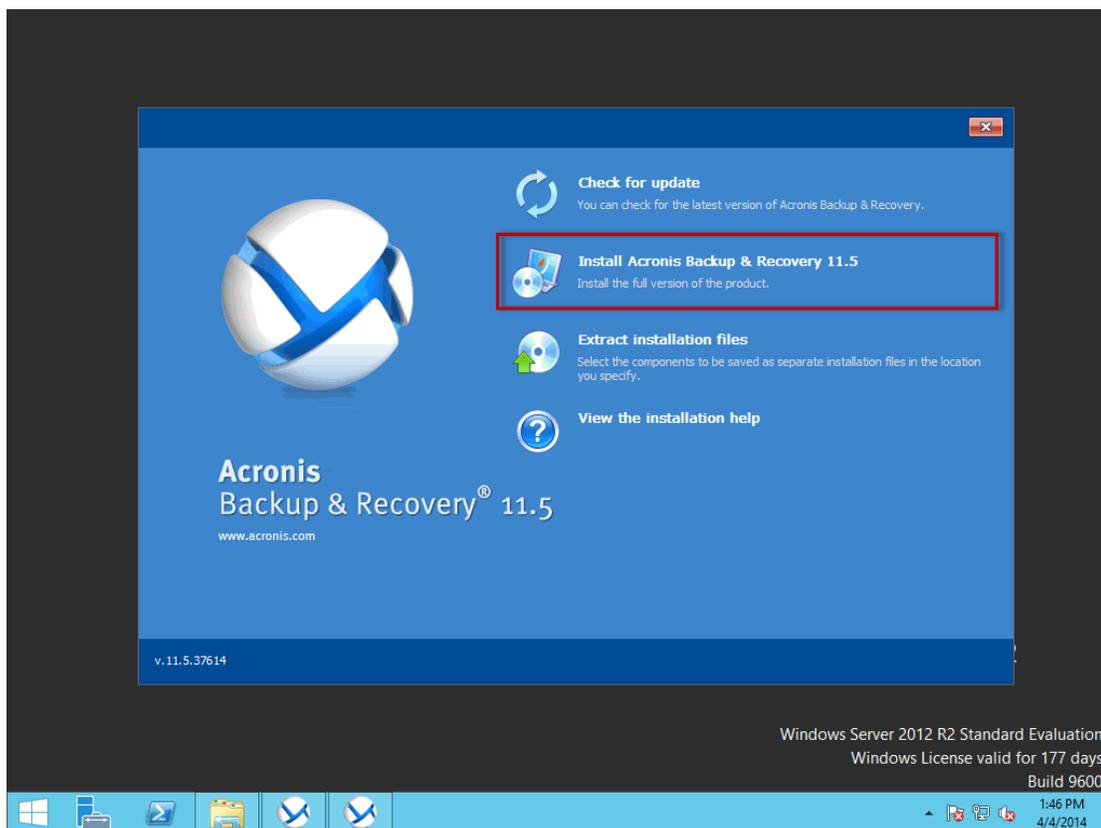


Figure 4.1

2. Read the Acronis Backup Advanced 11.5 license agreement, click the checkbox labeled **I accept this agreement** and then click **Next** (see Figure 4.2).

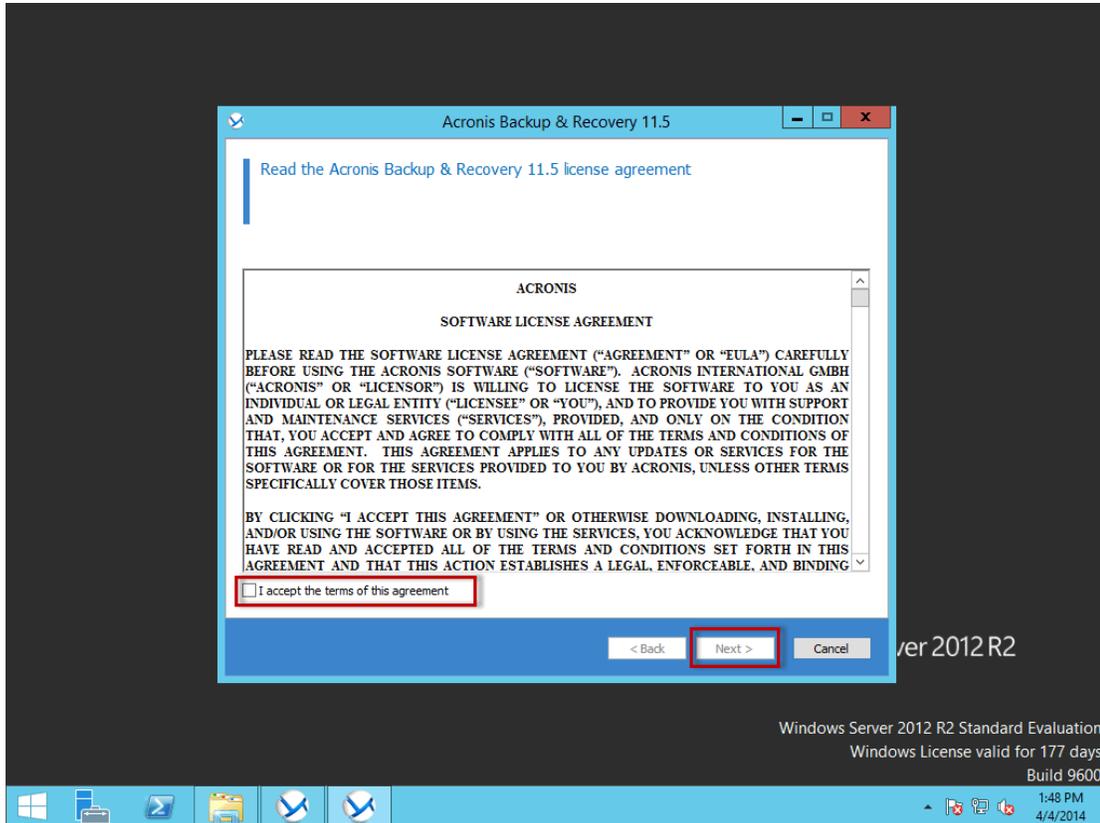


Figure 4.2

3. Choose the option needed for the installation of the backup agent. Check **Back up this machine's data** checkbox. Then click **Next** (see Figure 4.3).

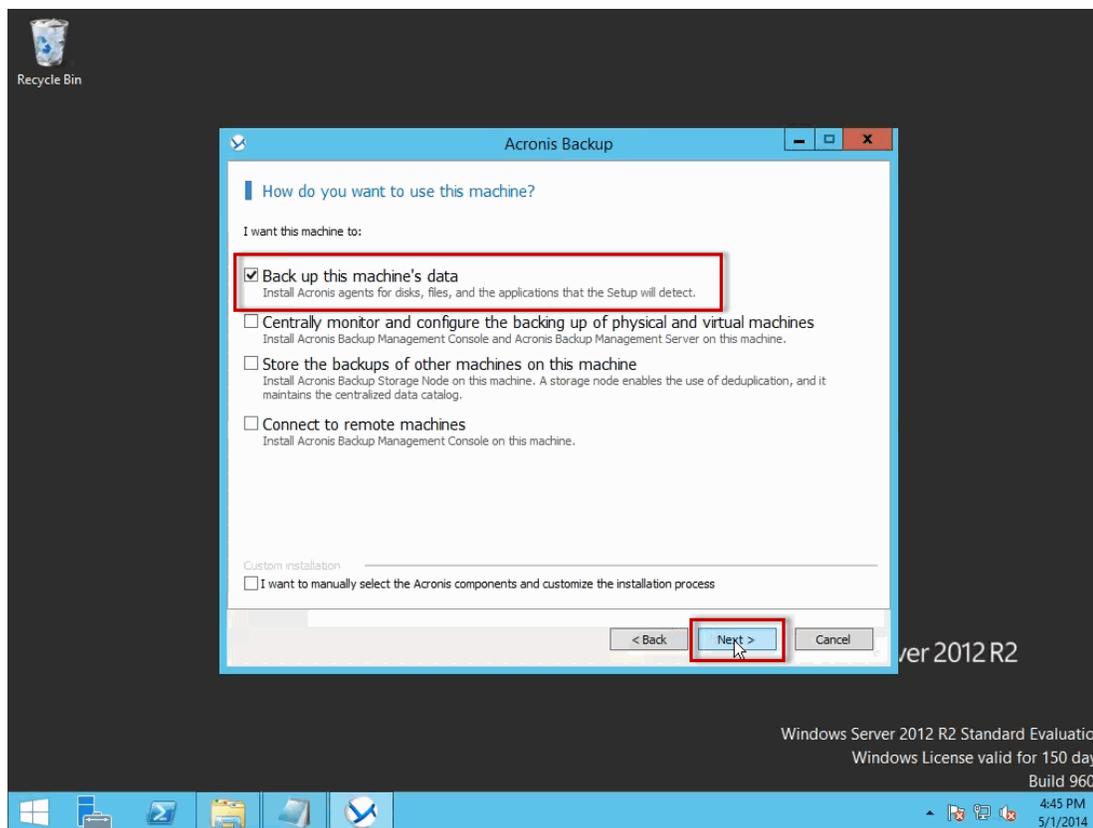


Figure 4.3

- Next, choose an installation mode, either **free trial** or **licensed**. Select the radio button next to **I purchased a license or a subscription**, then click **Next** (see Figure 4.4). **Note:** If you chose to do a free trial, you will be given a 15 day trial period. If you need more than 15 days, you must provision a license key from the eFolder Web Portal and assign it to the AMS license server installed at your customer's site. and then register this agent with that license server.

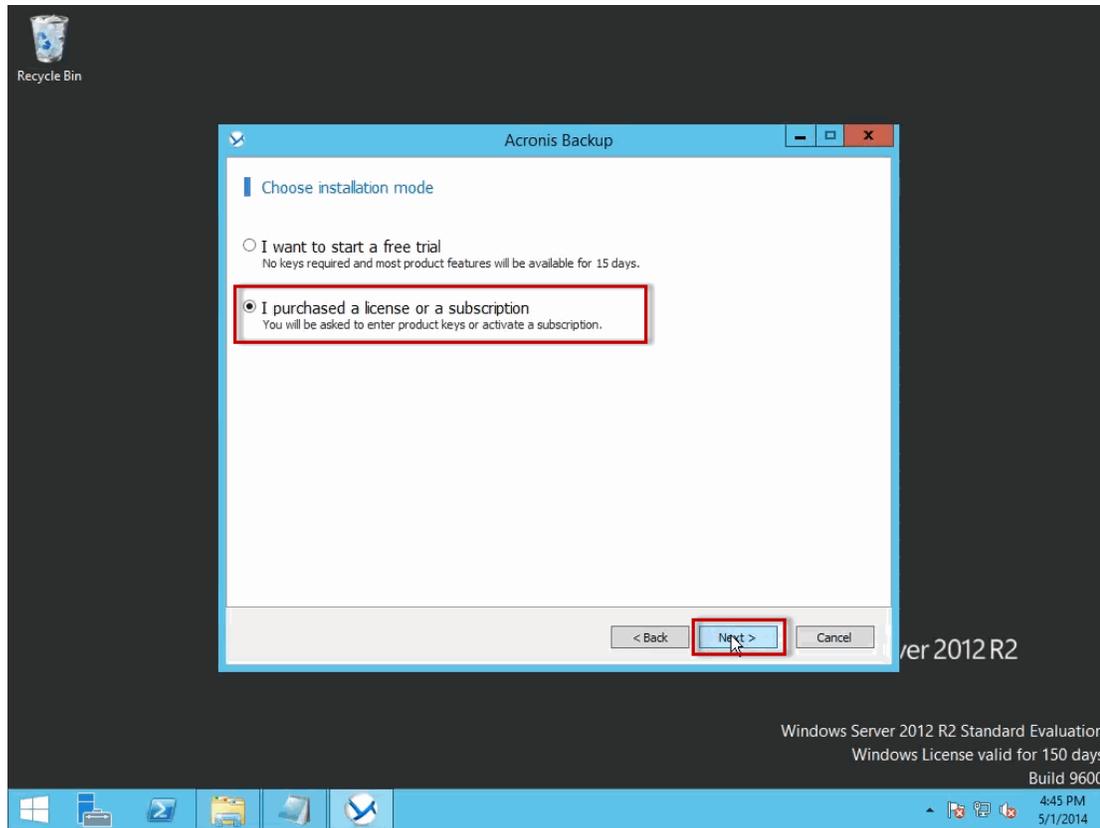


Figure 4.4

5. Click the **Add Licenses...** button on the *Provide license keys and select licenses* screen, then select the checkbox labeled **Use the following license server**. Next, in the text field to the left, add the IP Address or hostname of your AMS license server you installed previously and then press **Enter** on your keyboard (see Figure 4.5).

Note: You can also click the **Browse** button; Acronis will browse your local network, and you can select the machine running the AMS from the list of machines.

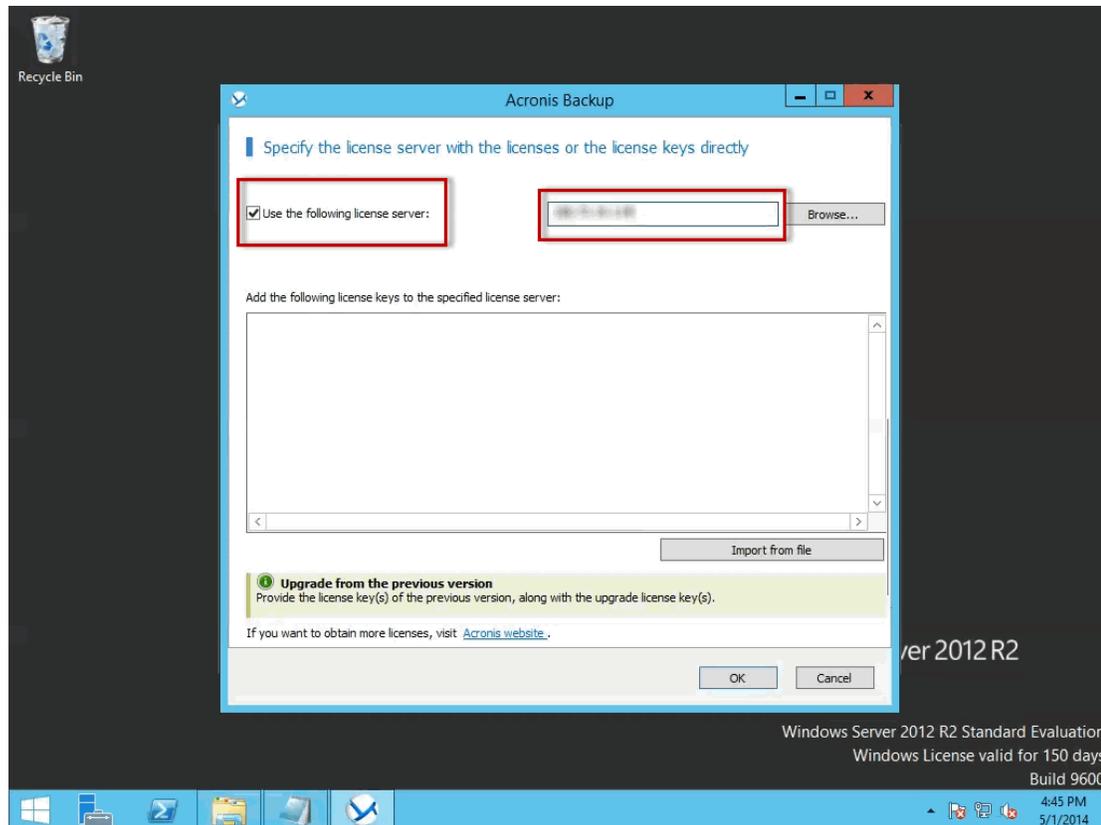


Figure 4.5

6. After the local installer has established communications with the AMS, the installer will give you the option to choose a license that is available from the AMS license server. Select the license from the drop down menu and then click **Next** (see Figure 4.6).

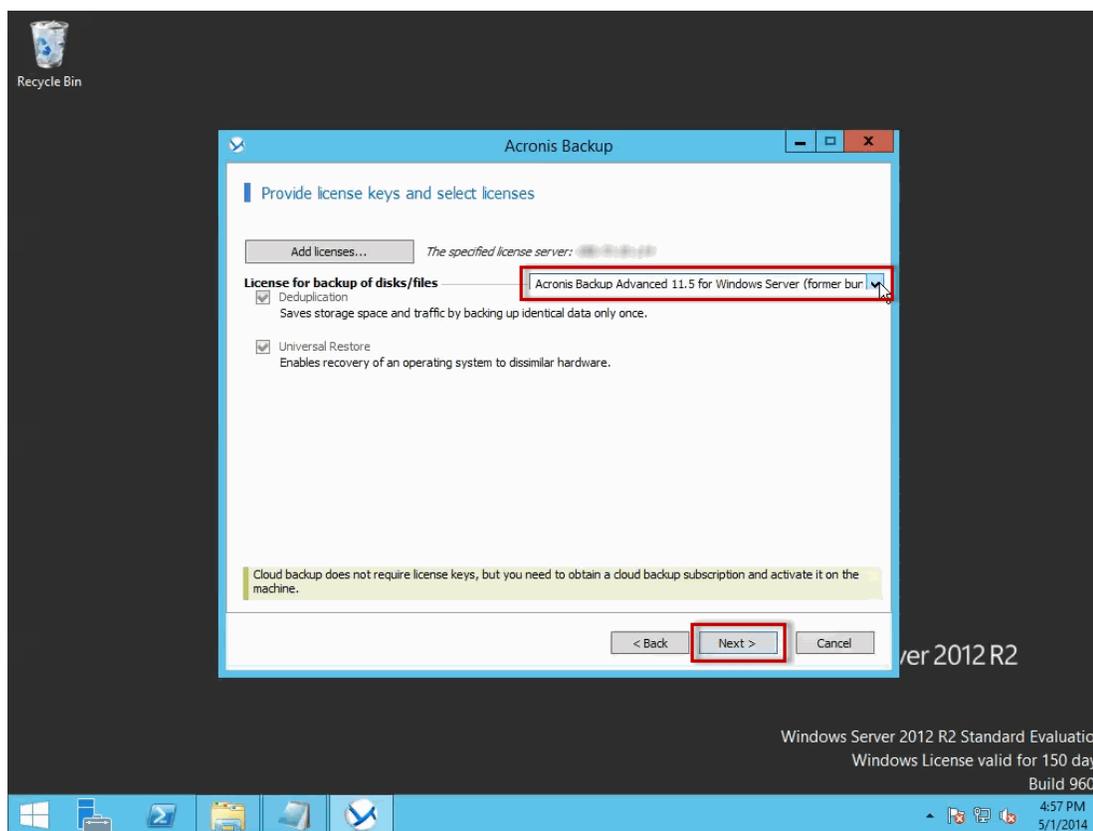


Figure 4.6

- Next, you will be asked if you want to register the agent to the local AMS. The agents are controlled from the local AMS, and you are required to register the agent onto the local AMS to backup to the local vault and to the eFolder Acronis vault. You can choose to skip this step and do it later, but we recommend that you do it now. To register now, select the radio button labeled **Register now**, then in the **Management Server (IP/name)** field, either enter the machine name of the machine that the AMS is installed on, or click **Browse** to locate the machine from the browser window. Enter a username and password that has rights on the AMS (see Figure 4.7).

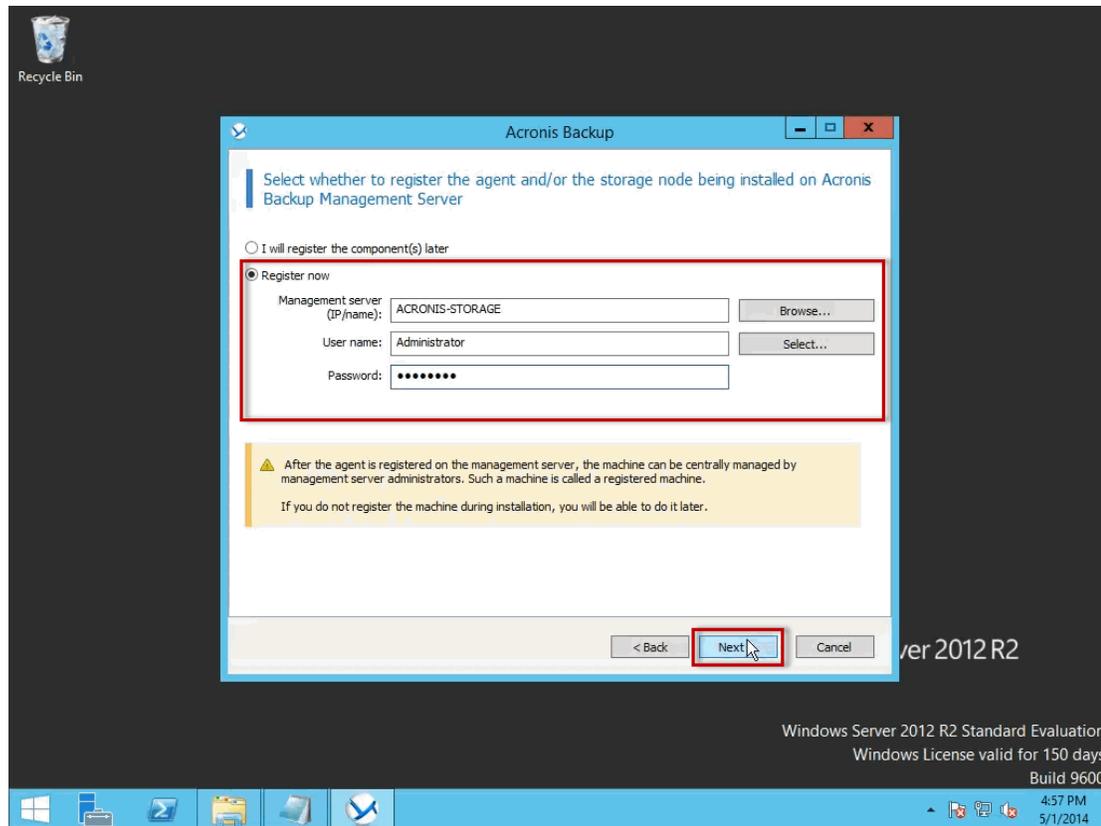


Figure 4.7

- Now you are asked if you would like to participate in the Acronis customer experience program. Choose either yes or no and then click **Next**.
- View the *Summary of the Operations to Be Performed* window, and verify that your settings are correct. Then click the **Install** button to begin the installation.
- After your installation is complete, exit out of the Acronis installer. The installation of the Acronis backup agent is now complete. To configure the Acronis backup agent that was just installed, logon to the machine running the AMS and configure the backup schemes from there, as instructed in the next section of this document.

Configuring the Local Backup Plan

This section will show you how to create a *backup plan* in your local AMS to backup your protected machines to the local AMS managed vault.

Important! The settings that you will use to configure a local backup plan will not be the same settings in the remote backup plan that backs up to the eFolder Cloud. For the remote backup job settings please see the section titled Creating a Remote Backup plan.

Note: These are recommended settings, but you can customize these settings to meet your customers' needs. Also note that these instructions differ from the ones you will follow when you set up your backup scheme to backup your protected machines to the eFolder cloud vault.

1. Using the Acronis console, connect to your locally installed AMS. Click **Backup plans and tasks** in the left hand navigation window, then click **New** and **Backup plan** to create a new backup plan (see Figure 5.1).

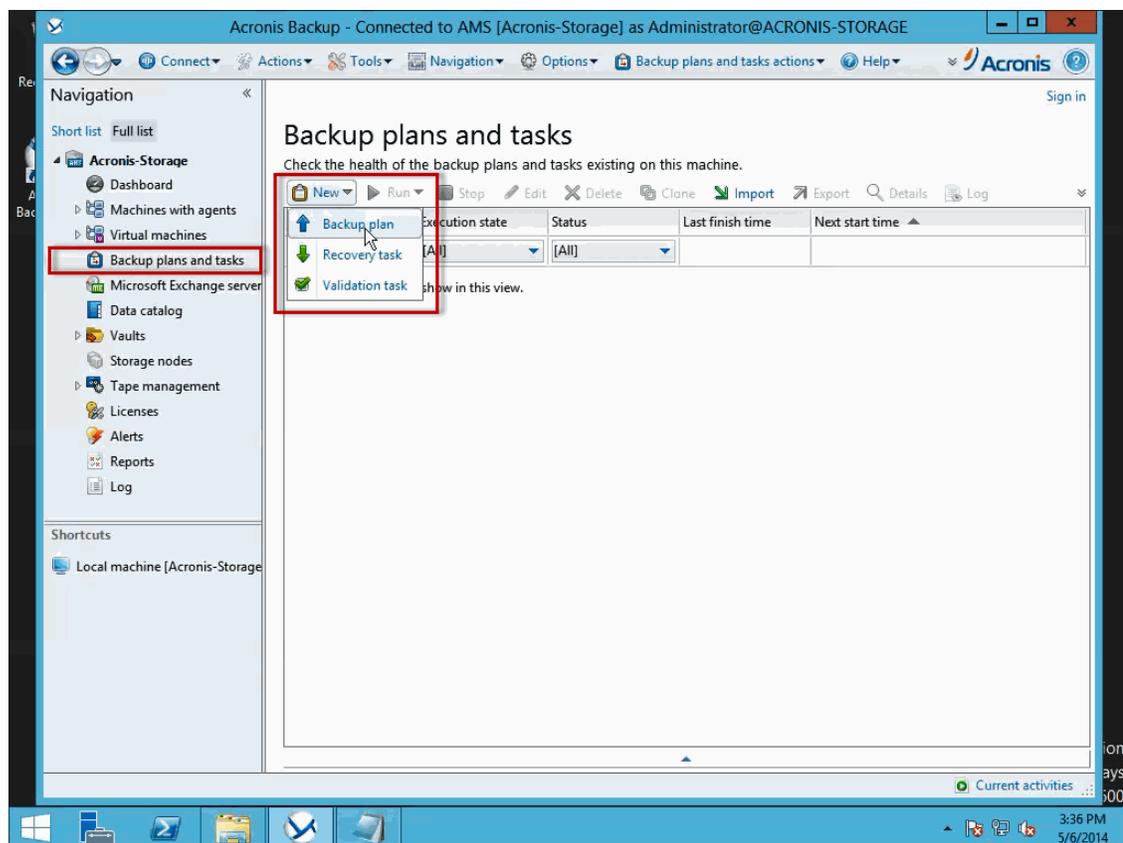


Figure 5.1

2. In the *Create backup plan* window, in the *What to back up* section, click the blue **Required** link to open the *Data to Back Up* dialog box. Now, expand the *Machines with agents* group to locate and select the machine(s) that you are going to include with this backup plan. Then click **OK**. (see Figure 5.2)

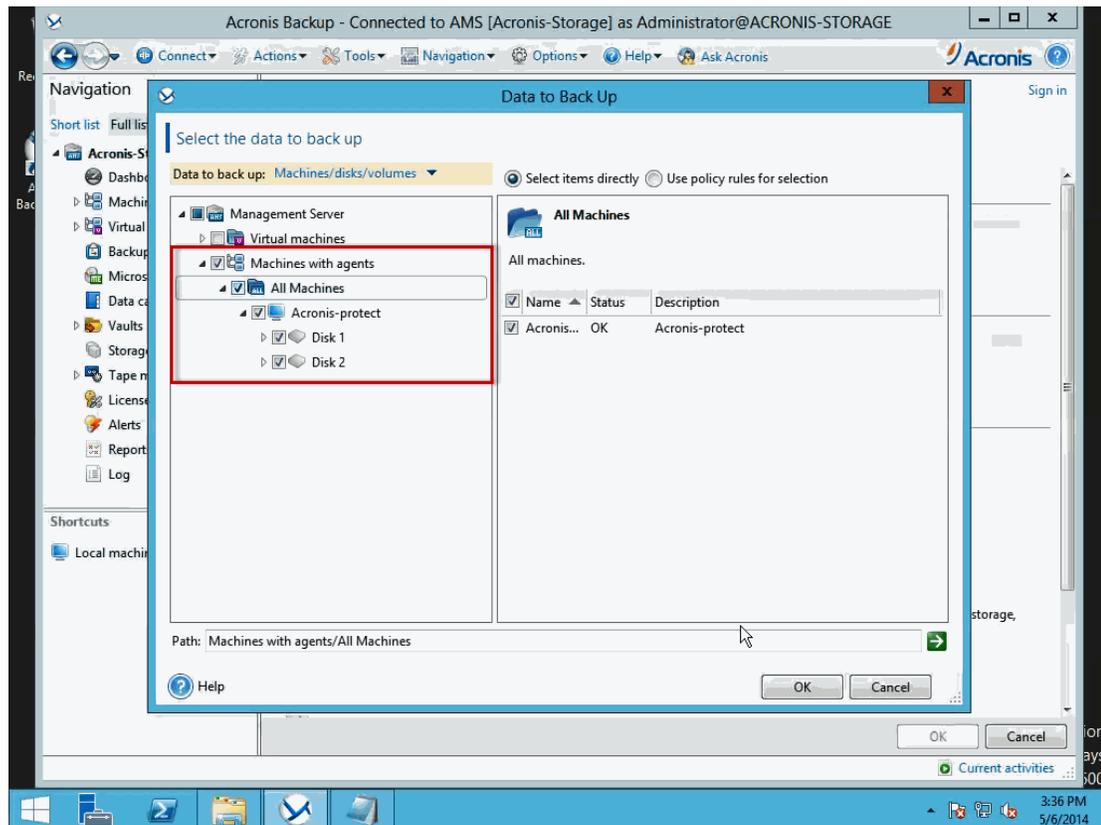


Figure 5.2

3. In the *Where to back up* section, click the blue **Required** link to open the *Location* dialog box. Ensure that the top radio button labeled **Store all machines' archives in a single location** is selected. Then expand the *Centralized* group from the left hand window and select the local vault that you created earlier. Then click **OK** to continue to the next step (see Figure 5.3).

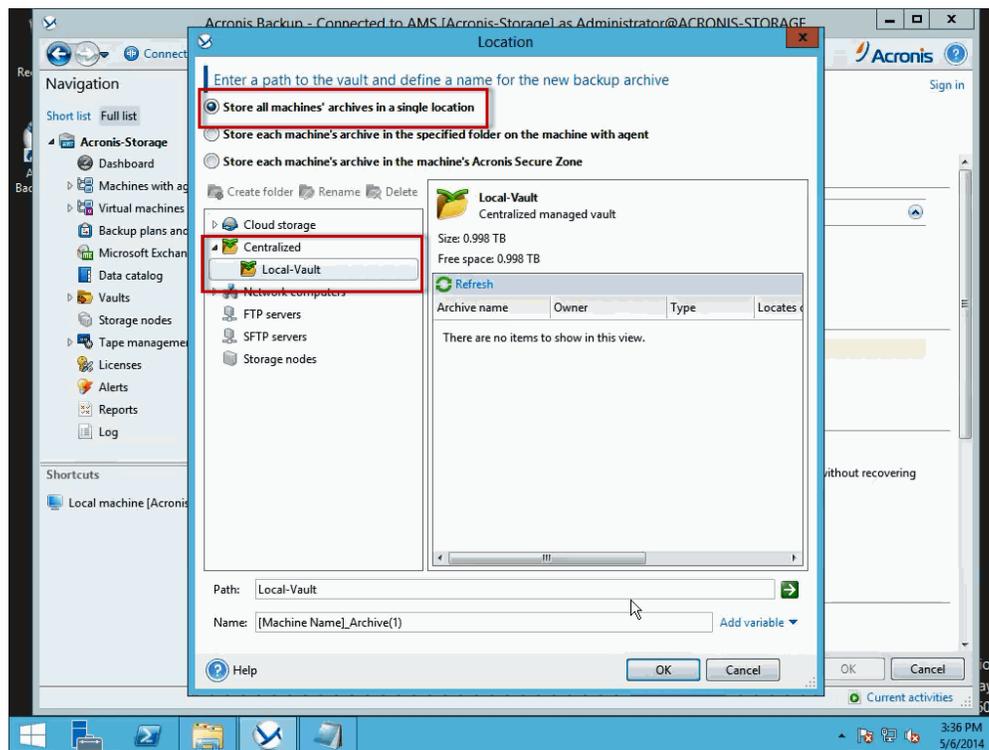


Figure 5.3

4. In the *Single-pass disk and application backup* section, you will either **enable** or **disable** the single-pass backup. A single-pass backup is a disk level backup that contains the metadata of the VSS-aware applications that are present on the disk. This metadata enables browsing and recovery of the backed-up application data without recovering the entire disk or volume as well as restoring the full disk that was backed up. For example, if you plan to backup Microsoft SQL (MSSQL), you would enable the single-pass backup to give you the ability to restore individual tables back to a MSSQL server database without having to perform a full disk restore.

Note: An additional Acronis SQL license is required to enable Single-pass backup for MSSQL. This additional license is included at no additional cost with your Acronis Backup Advanced for Servers license that are provisioned from the eFolder Web Portal. However, you must login to the eFolder Web Portal to provision the Acronis SQL license and then add that key to your eFolder Acronis license server running in the eFolder cloud. See the section of the document entitled "How to provision Acronis Licenses from the eFolder Web Portal".

Important! If you plan to provide granular recovery to an Exchange Information Store, you must back up that Exchange server with a local backup. Performing granular recovery to an Exchange Information Store is not supported from Acronis backups that are backed up to the eFolder Cloud.

5. Next, you will setup the frequency of the backups. To provide your customers with the ability to restore to multiple recovery points throughout the day, you must setup the Backup scheme to backup on an *Incremental* backup schedule. The following recommended schedule will back up the protected machine: multiple times a day (incremental backups), once a week (differential backups), and once a month (full backup).

a. Click **Backup scheme** and select **Custom** on the drop-down menu.

b. To configure the Full Backup scheme: click the **Add Schedule...** link to open the *Schedule* dialog box. In the *Run the task:* section on the left, select the **Monthly** radio button. In the *Schedule* section, select the **On:** radio button. In the **First** drop down menu (next to the **On:** radio button), select which week of the month to perform the monthly (full) backup: the first, second, third, fourth, or last week. In the **ALL** drop-down menu (to the right), select which day of the week you want to run your full backup (see Figure 5.4). For example, select **First** in the first drop-down and **Sun** in the next if you want your monthly backup to run on the first Sunday of every month. Next, you will set what time you would like your monthly backup to start. In the *During the day execute the task...* section, select the **Once at:** radio button and set the time you would like this backup to begin (see Figure 5.4). Then click **OK** to continue.

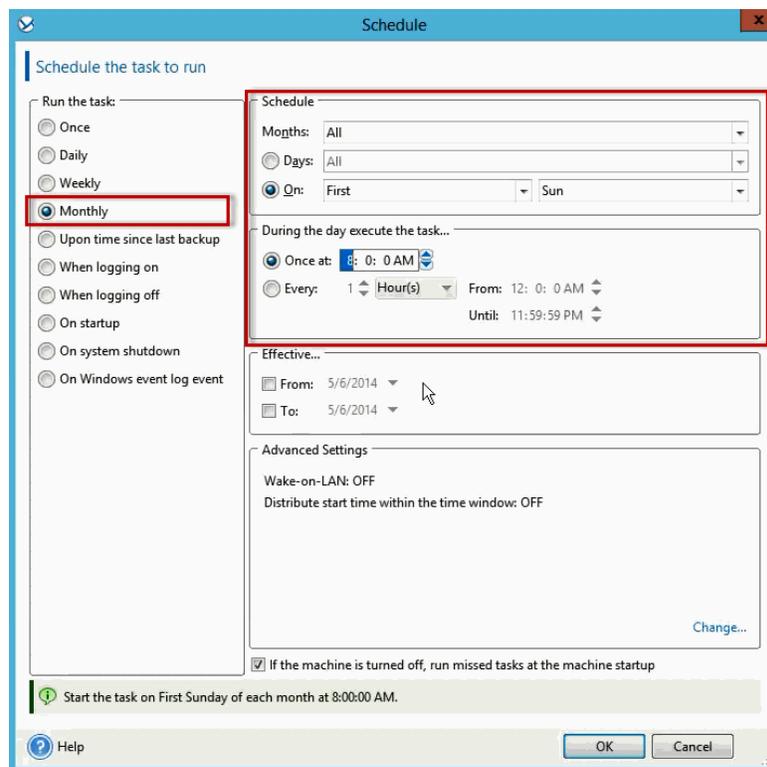


Figure 5.4

- c. To configure the Incremental backup scheme: click the **Add Schedule...** link to open the *Schedule* dialog box again. In the *Run the task:* section on the left, select the **Daily** radio button. In the *Schedule* section, ensure that **Every:** is set to 1 day(s). Next, in the **During the day execute the task...** section, select the **Every:** radio button. If you would like to backup once an hour, set the adjustable number to 1 and the drop down to *Hours*. Then select the time you would like the incremental backups to start in the **From:** field and the time you would like them to stop in the **Until:** field. Leave all other settings at their default values and click **OK** to continue (see Figure 5.5).

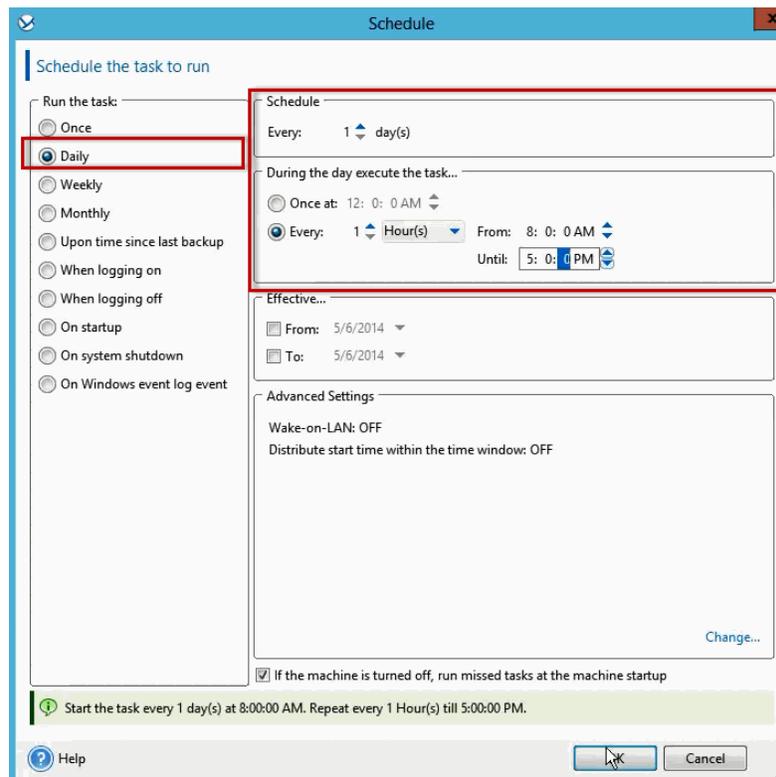


Figure 5.5

- d. To configure the Differential backups: click the **Add Schedule...** link to open the *Schedule* dialog box again. In the *Run the task:* section on the left, select the **Weekly** radio button. In the *Schedule* section, uncheck all the days except for the day you would like to run your differential (weekly backup). We suggest that you set this to the end or start of a week, like Saturday or Sunday. In the *During the day to execute the task...* section, select the **Once at:** radio button and set the time of day you would like the differential backup to start. Leave all of the other settings at their default values and click **OK** to continue (see Figure 5.6).

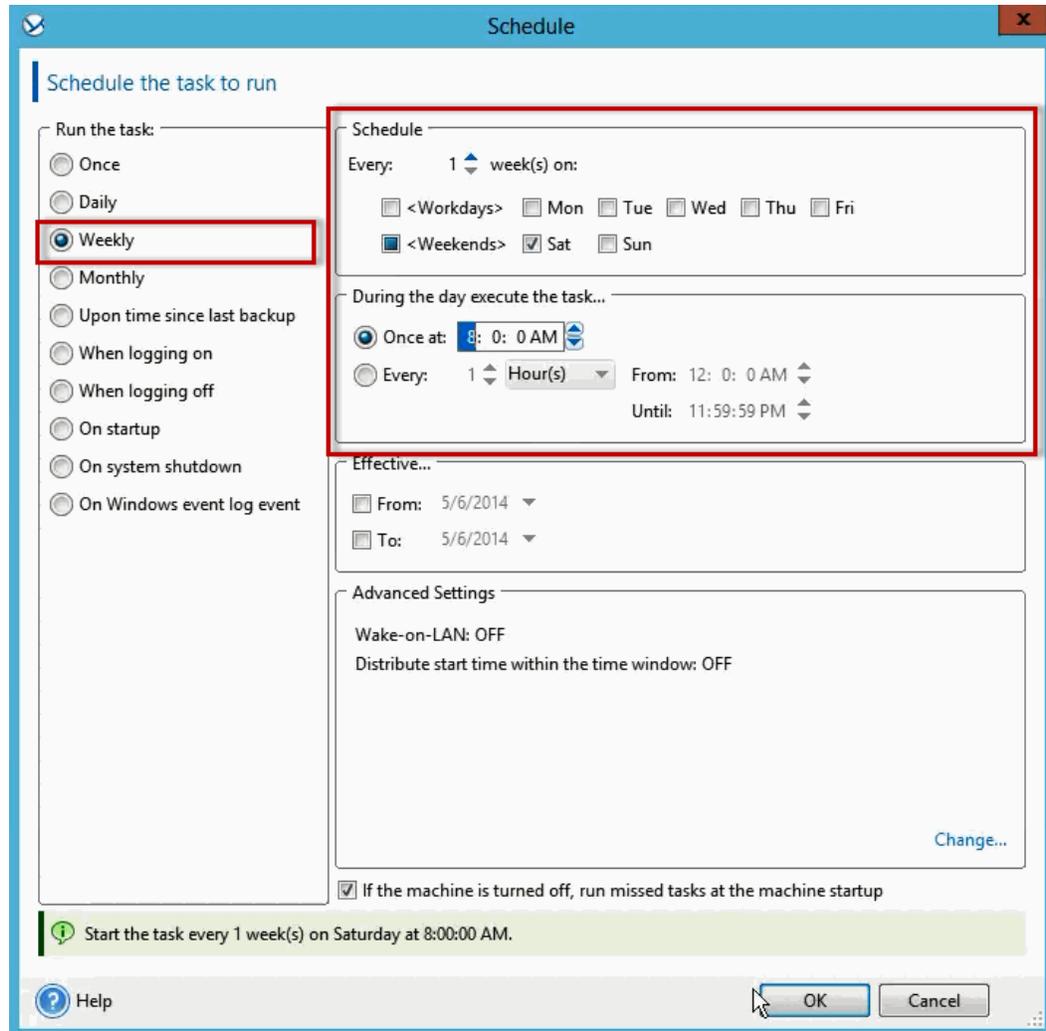


Figure 5.6

e. To configure the Clean up Archive settings: in the *Create backup plan* window click the drop down menu (see Figure 5.7) and select **Using retention rules**. The menu options will change. Select **Retention rules...** to open the Retention Rules dialog box. To keep a retention of 60 days, ensure that the **Age and size**: radio button is selected, check the checkbox labeled **Backups older than:**, type 60 in the text box, and then adjust the retention settings to **Days(s)** if it is not already set to that. Leave all other settings at their default values and click **OK** to continue (see Figure 5.8).

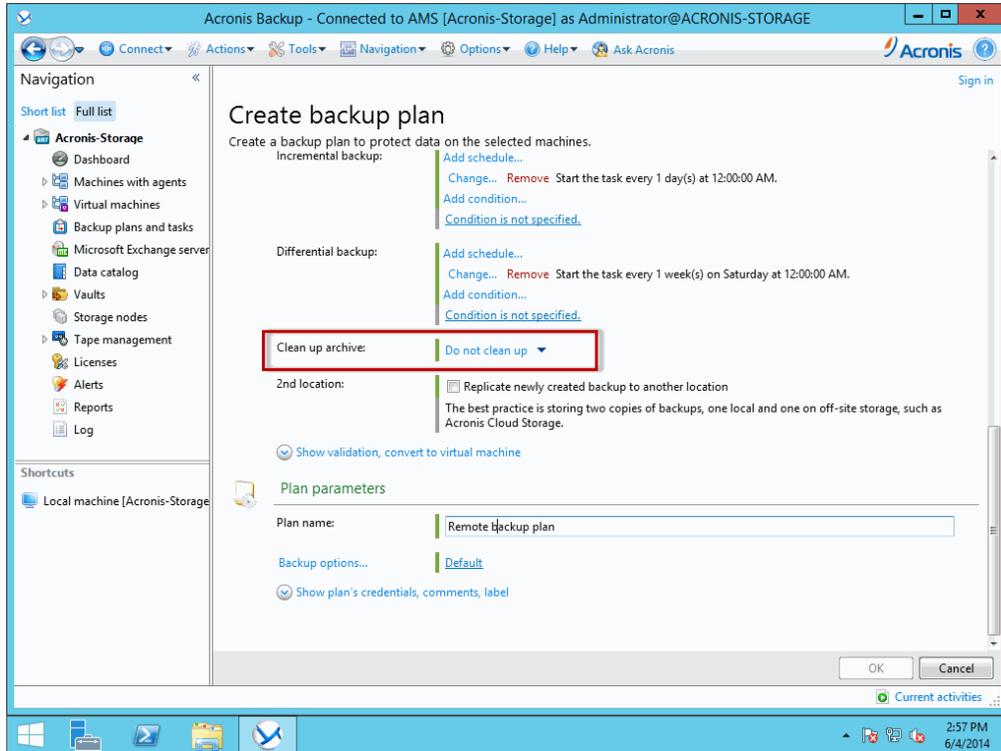


Figure 5.7

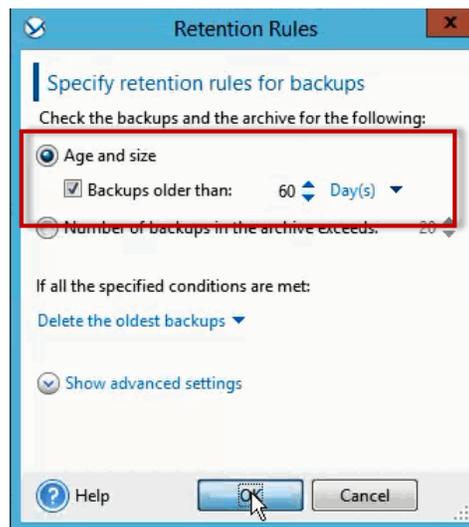


Figure 5.8

- f. Under the *Plan parameters* section, in the **Plan name:** field, enter a plan. For example, since this is your local backup plan, and you plan to also send data to the eFolder cloud, you might enter “Local backup plan” (see Figure 5.9).

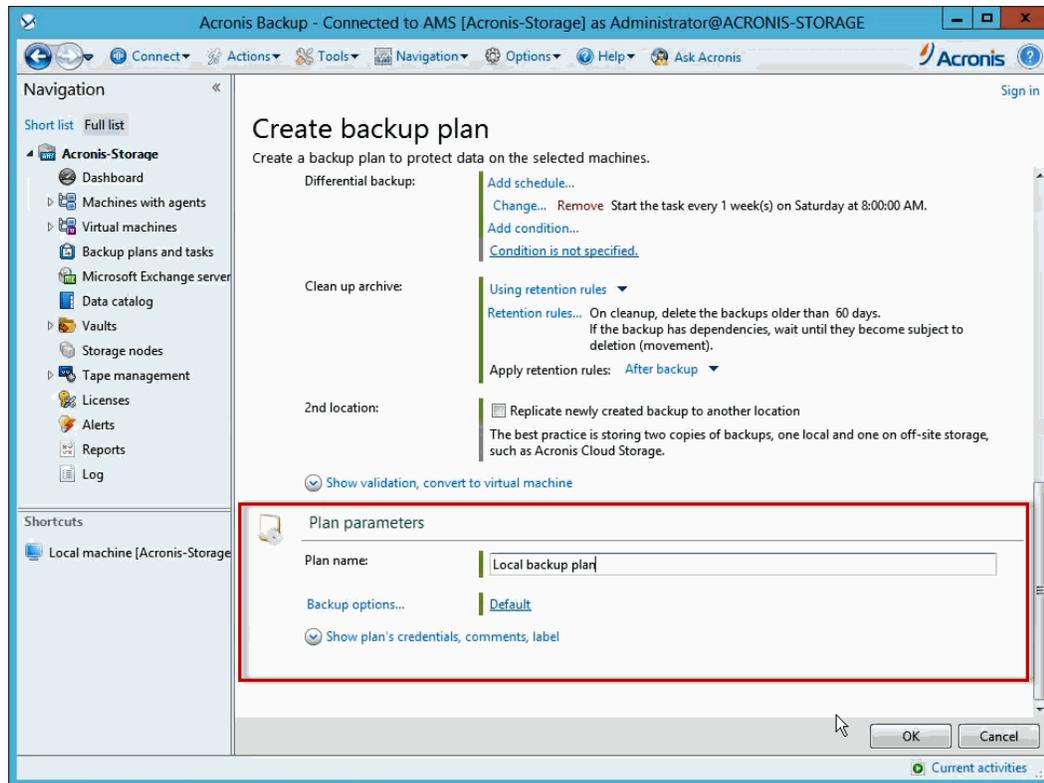


Figure 5.9

- g. Review your settings. If you are satisfied with them, click **OK** to close the Create backup plan wizard.

Creating a Remote Backup plan

When creating a remote backup plan, you need to determine if the size of your initial full backup is too large to send over the Internet to the eFolder cloud, or if you are you able to send it directly over the wire. If your full backups are too large to send over the Internet, you will need to create a managed vault with encryption enabled (seed vault) on a removable drive or portable NAS device and create a onetime full backup to this vault, then send the device to an eFolder datacenter via FedEx or UPS.

This section will show you how to create a backup plan that will create a onetime full backup onto the seed vault and then convert that backup plan to a remote backup plan after the seed vault has been processed by the datacenter staff. You will also be shown how to set up a remote backup plan to backup directly to the eFolder cloud without a seed drive.

How Acronis performs Full Backups to a Managed Vault with Deduplication

It is important for you to understand that backing up data with Acronis to a managed vault with deduplication enabled is different than other image-based backup solutions. The recommended remote backup plan that is covered in the sections entitled *Remote Backup plan with Seed Drive* and *Remote Backup plan – Backing up Directly to the eFolder Acronis Vault* instructs you to take a full backup at least once a month. If you have been using other solutions, this may throw up a red flag for you. However, after reviewing how Acronis performs a full backup to a managed vault with deduplication enabled, you will see that it is perfectly okay to take a full backup once a month.

After the initial full backup has been seeded to the eFolder Acronis vault, and Acronis performs a differential (weekly) or monthly (full) backup, it is always deduplicated at the agent level. This means that if a new full backup is performed, Acronis compares the data in the cloud with the data on the drive and only backs up uncommon data. Only non-deduplicated data will be backed up on the next full backup. For example, your vault in the eFolder Cloud is a multi-tenant vault. If Customer A's backups had already backed up a Windows Server 2012, and Customer B's backups are also backing up a Windows Server 2012 and you are going to seed that over the internet, the bits of Server 2012 that are the same as Customer A are not backed up to the eFolder Cloud.

Remote Backup Plan with Seed Drive

Here are the requirements to set up a remote backup plan with a seed drive:

- A managed vault with encryption enabled that is located on a removable drive or portable NAS device. For instructions on setting up a managed vault, see the section of this document entitled "*Configuring the Management Components.*" **Note:** You can skip the step that enables deduplication for the seed vault; be sure to name the vault differently than your local vault (for example, *Seed Vault*).
- A backup plan that is configured to backup a onetime full backup and set to manually start.

1. Make sure you have created a seed vault on a portable device that you can send to the eFolder datacenter. For instructions on setting up a managed vault, see the section of this document entitled "Configuring the Management Components." **Note:** You can skip the step that enables deduplication for the seed vault; be sure to name the vault differently than your local vault (see Figure 6.1).

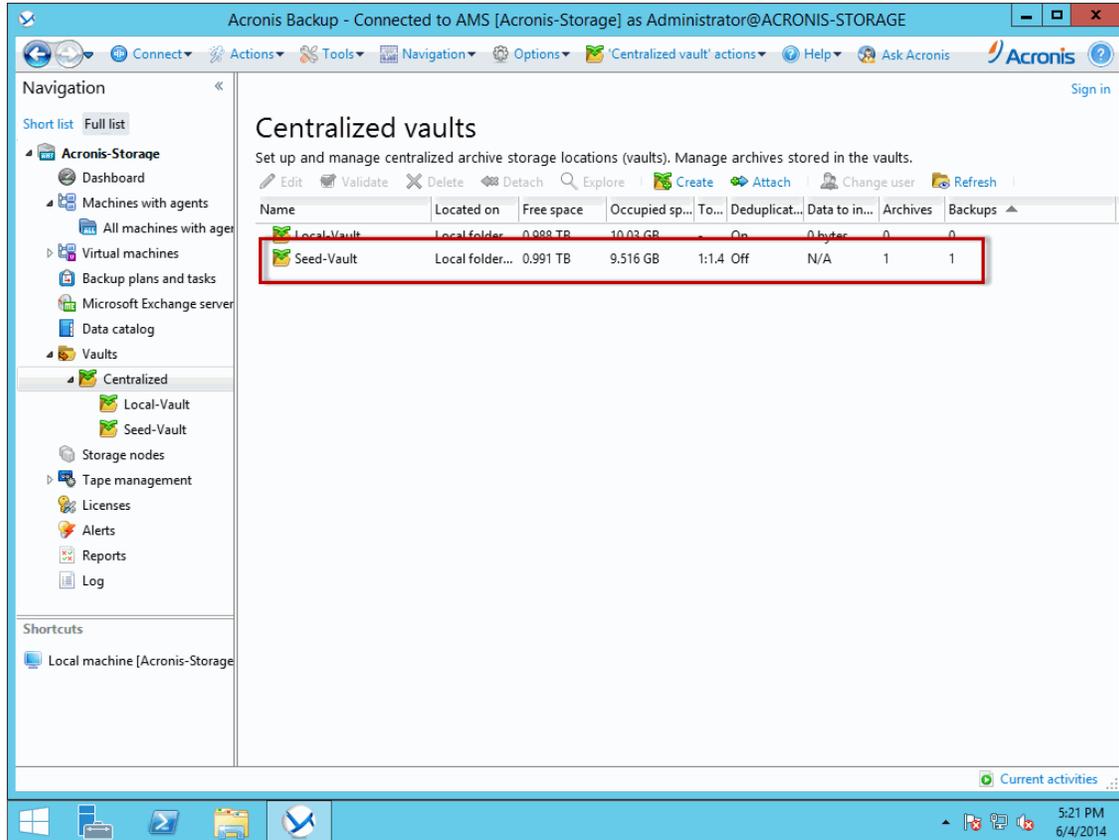


Figure 6.1

- Using the Acronis console, connect to your locally installed AMS. Click **Backup plans and tasks** in the left navigation window, then click **New** and **Backup plan** to create a new backup plan (see Figure 6.2).

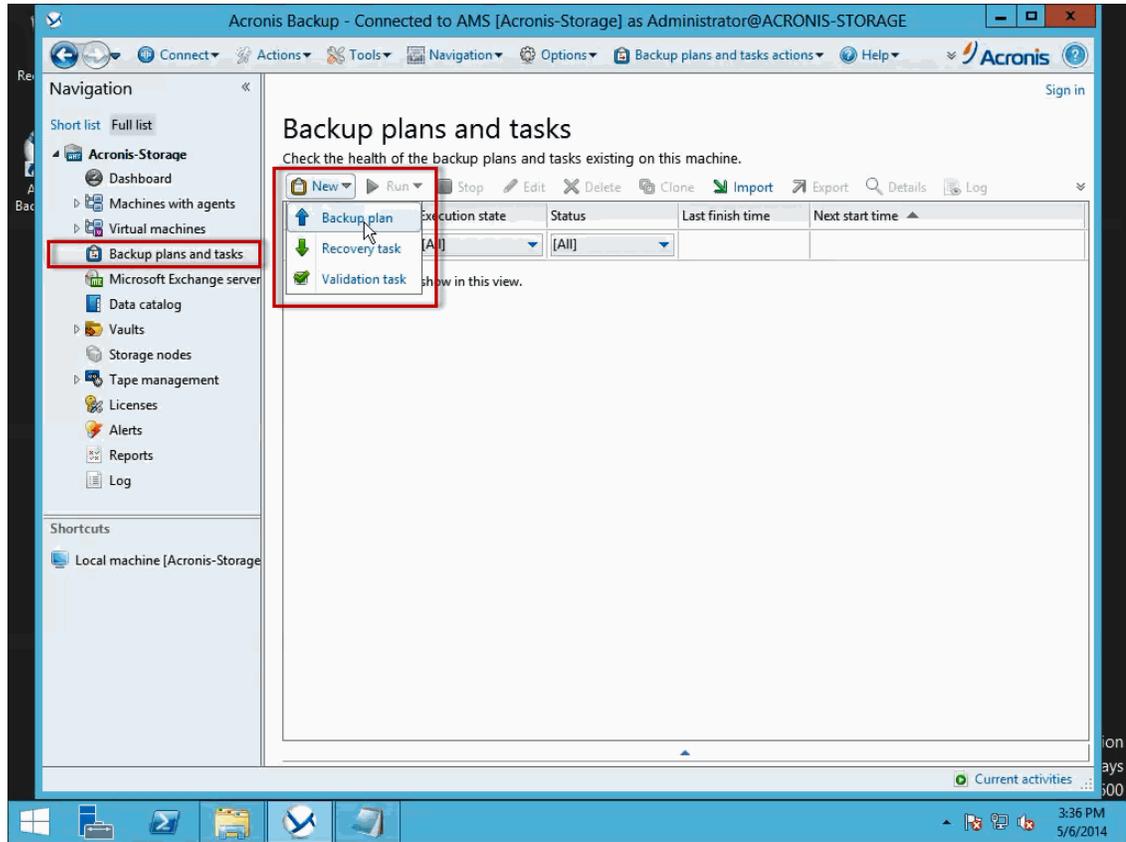


Figure 6.2

3. In the *What to back up* section of the *Create backup plan* window, click the blue **Required** link to open the *Data to Back Up* dialog box. Now, expand the *Machines with agents* group to locate and select the machine(s) that you are going to include in this backup plan. Then click **OK** (see Figure 6.3).

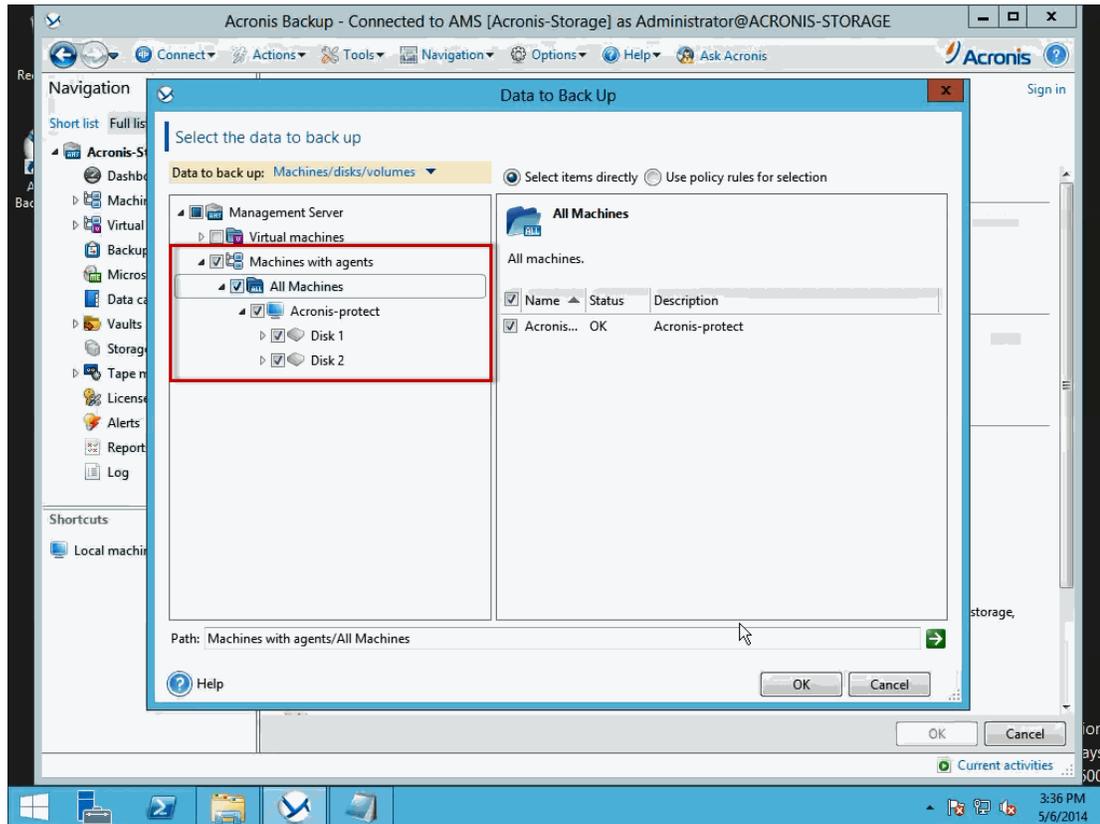


Figure 6.3

- In the *Where to back up* section, click the blue **Required** link to open the *Location* dialog box. Ensure that the top radio button labeled **Store all machines' archives in a single location** is selected. Then expand the *Centralized* group from the left window and select the seed vault you created previously. Then click **OK** to continue to the next step (see Figure 6.4).

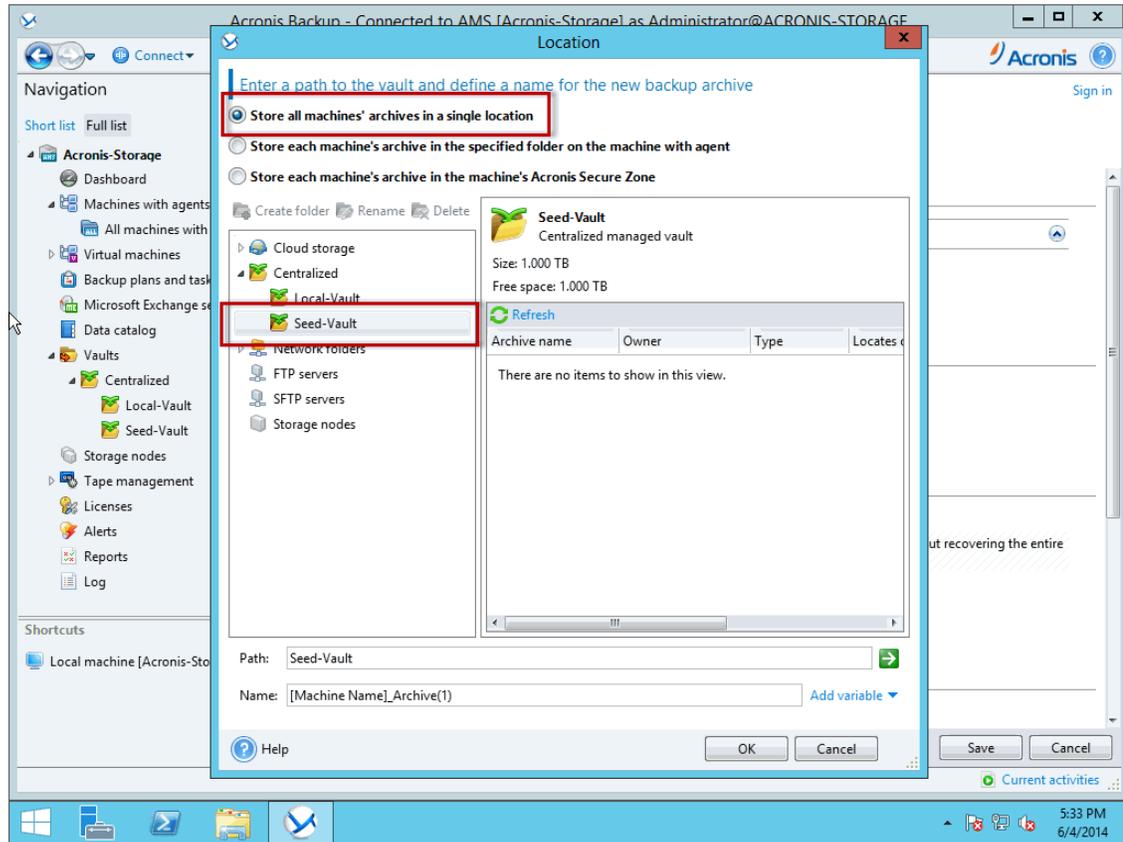


Figure 6.4

- In the *Single-pass disk and application backup* section, decide whether to **enable** or **disable** the single-pass backup (see step 4 in *Configuring the Local Backup Plan* for more information).

Important! If you plan to provide granular recovery to an Exchange Information Store, you must back up that Exchange server with a local backup. Performing granular recovery to an Exchange Information Store is not supported from Acronis backups that are backed up to the eFolder Cloud.

- Click **Backup scheme** and select **Manual Start** on the drop-down menu.
- In the *Plan name: field*, name this backup plan something similar to *Perform Seed*, then click **Save**.
- In the *Backup plans and tasks* window, select the **Perform Seed** backup job and click **Run/Full backup ('once later' scheme)** to perform your preload to the seed vault.

- After the preload is complete, you must detach the seed vault from the storage node. In the left Navigation window, expand **Vaults/Centralized** then right mouse click on your seed vault and click **Detach** (see Figure 6.5). After you click **Detach**, a conformation dialog box appears. Click **Yes** to detach the seed vault.

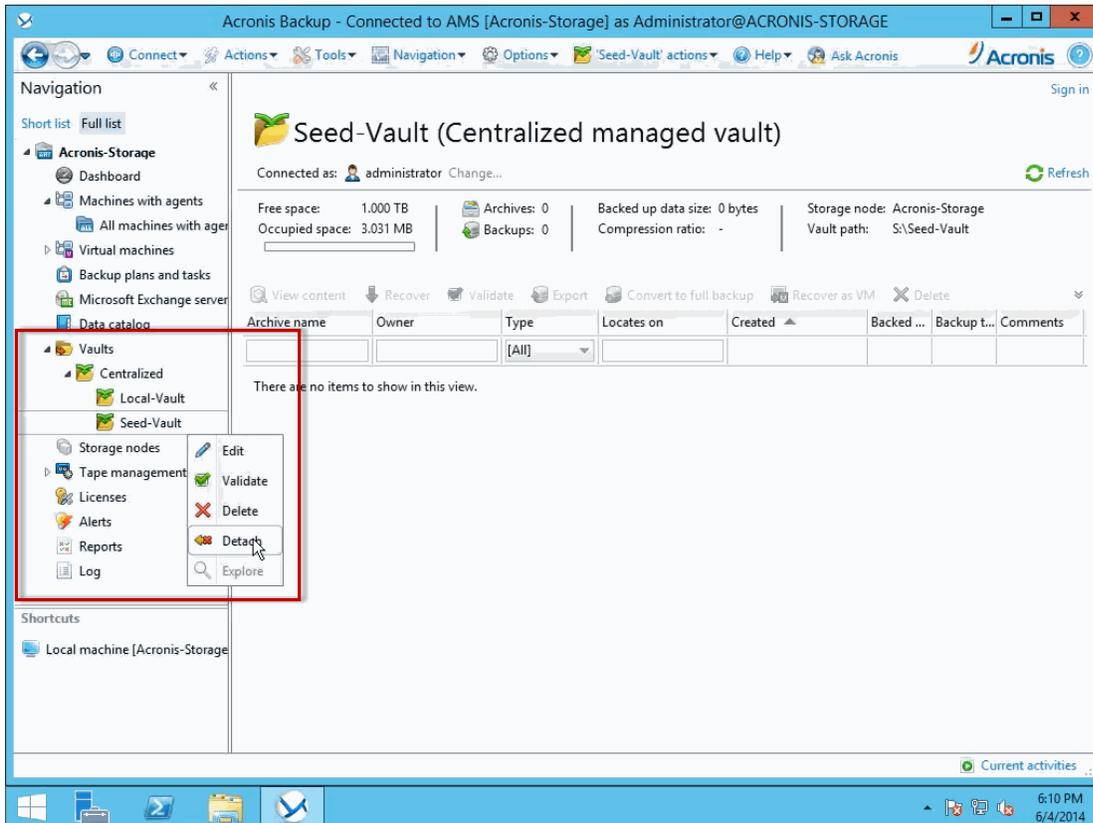


Figure 6.5

- Next, open a support ticket with the eFolder support team to obtain the data center address to which the seed drive should be sent (see the section in this document entitled “Technical Support” under “Additional Resources” for information on how to contact the eFolder support team). Work with Support to ensure the drive is properly marked and documented, and be sure to include a return prepaid shipping label.

Important! When you open the support ticket, you must include the encryption password you used when encrypting your seed vault. Failure to do so will delay the processing of your seed drive when it reaches the datacenter, as support will have to contact you for the encryption password.

Important! Before moving on to the next step, you must wait for eFolder’s datacenter staff to process the preload after the seed drive has been received at the datacenter. When the preload has been completed, Support will notify you via the support ticket that you opened.

11. After the seed vault has been loaded into your eFolder Acronis vault in the eFolder cloud, you must edit the backup plan that was used to perform the preload to the seed vault and then reconfigure it for remote backup. Connect to your local AMS and click **Backup plans and tasks** on the *Navigation* menu. Then select the **Perform Seed** backup plan you created previously and click **Edit** from the menu to open the *Edit backup plan* window.
12. In the *Where to back up* section, click the blue **Location...** link to open the *Location* dialog box. Ensure that the top radio button labeled **Store all machines' archives in a single location** is selected. In the left window, select **Storage nodes**. In the **Path:** field, enter the remote server address you were provided with when your eFolder Acronis Management Server was assigned to you.

Important! When entering the address, you must keep the "bsp://" as part of the address. Also, you must click the GREEN RIGHT ARROW to connect to the remote storage node. If you click OK it does not complete the connection and your archive will NOT be sent to the remote storage node (see Figure 6.6).

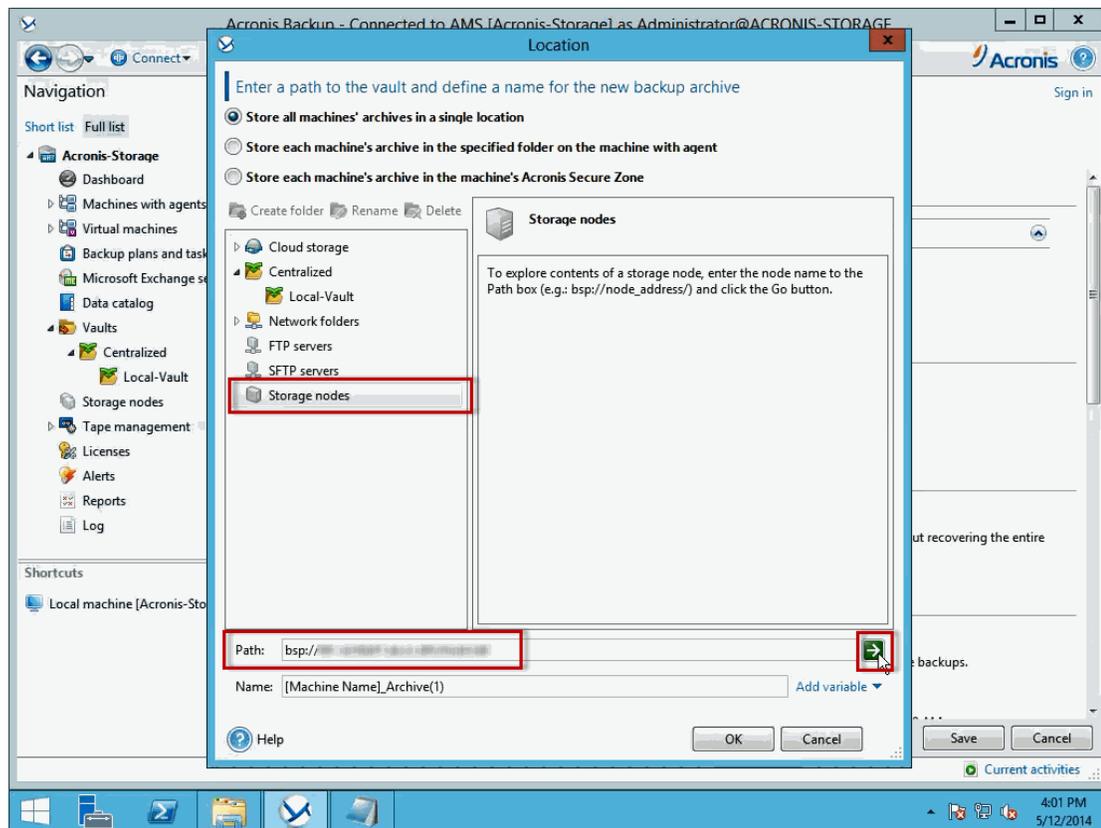


Figure 6.6

13. After clicking the **GREEN RIGHT ARROW** to connect to your eFolder AMS, the *Access Credentials* dialog box appears. Enter the username and password provided to you by eFolder when your eFolder AMS was assigned to you. After your credentials have been verified, expand the **Storage nodes** in the path window on the left. Then expand the node labeled with your AMS name and click the managed vault that you created previously. Then click **OK** to continue (see Figure 6.7).

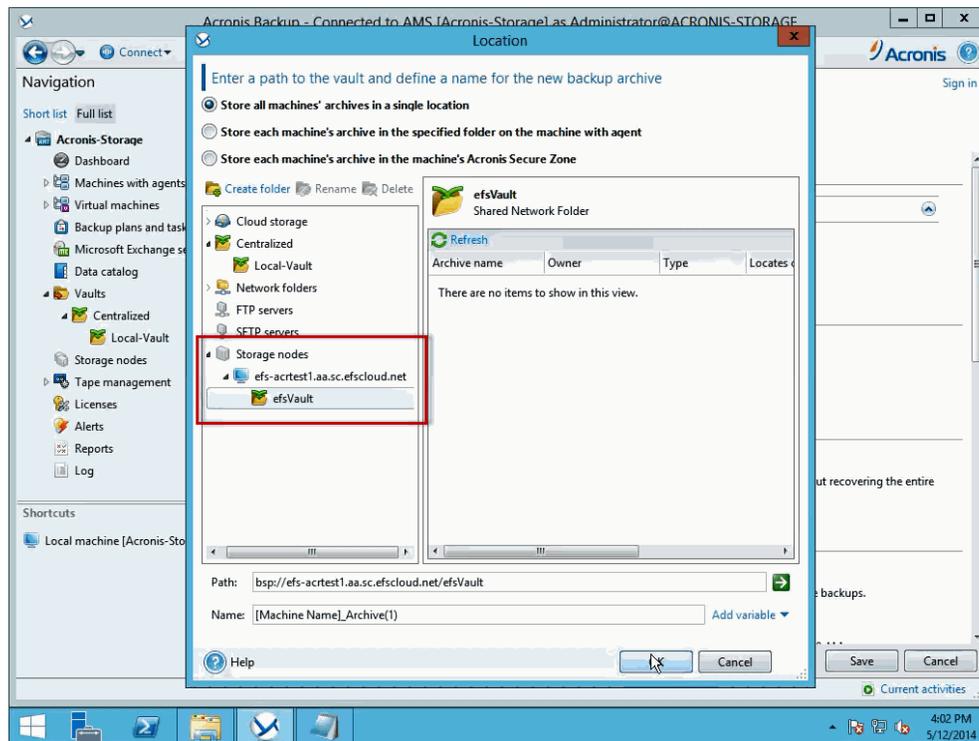


Figure 6.7

14. Because these steps are for configuring a backup plan to back up over the Internet to the eFolder Acronis vault, it is recommended that you configure the incremental backup to backup to once a day. We also recommended that when you configure the full or monthly backup set it to an arbitrary day in the month. This will help ensure that you have optimal performance when uploading more than one customer to your eFolder Acronis vault. The following steps will lead you through making these changes:

In the *How to back up* section, change the following settings:

- Backup scheme: change to **Custom** from the drop down menu.
- Full Backup: Click the blue **Add schedule...** link and either select the day of the month or the week number and day you would like to send your full backup to the eFolder Acronis vault (see Figure 6.8). Then set the time you would like the full or monthly backup to start by selecting the radio button labeled **Once at:** and set the start time. Then click **OK** to continue.

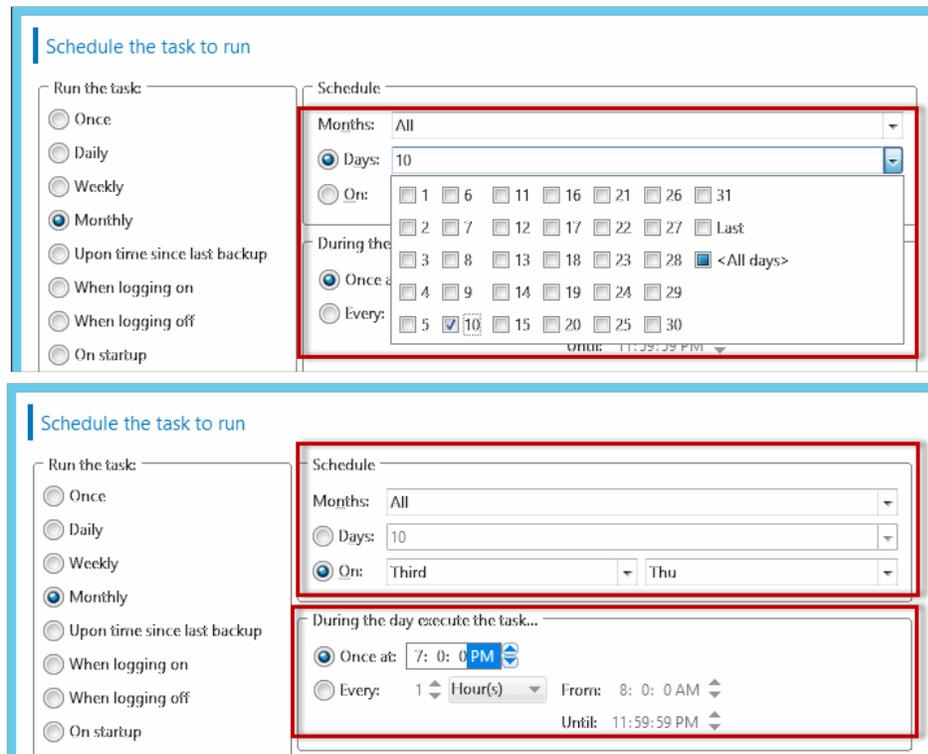


Figure 6.8

- Incremental backup: Click the blue **Add schedule...** link and select the radio button labeled **Once at:** and change the time to the start time that you want the once-a-day incremental backup to happen (see Figure 6.9). Then click **OK** to continue.

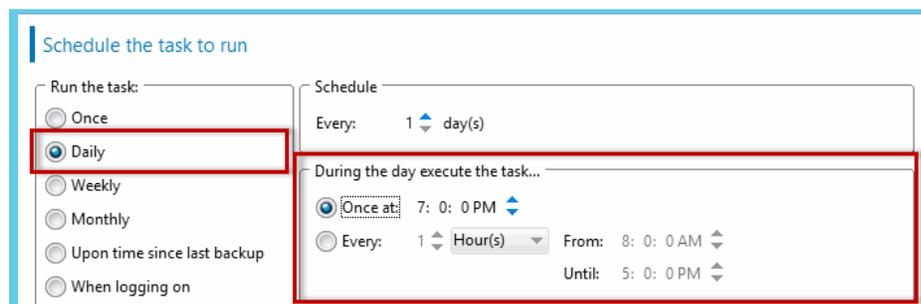


Figure 6.9

- To configure the Differential backups: Click the **Add Schedule...** link to open the *Schedule* dialog box again. In the *Run the task:* section on the left, select the **Weekly** radio button. In the *Schedule* section, uncheck all of the days except the day you would like to run your differential (weekly backup). We suggest that you set this to the end or start of a week, like Saturday or Sunday. In the *During the day to execute the task...* section, select the **Once at:** radio button and set the time of day you would like the differential backup to start. Leave all of the other settings at their default values and click **OK** to continue.

Note: To maximize performance of your eFolder Acronis vault, we recommend that you pick an arbitrary day when sending more than one customer to your remote vault.

- Clean up archive: We recommend that you change the Retention Rules to keep a minimum of 60 days' worth of archives in the eFolder Acronis vault. If your customer requires a longer retention than 60 days, that is okay—just do not set it for less than 60 days.
- Plan name: Rename this from *Perform Seed* to something like "*Remote backup plan*" to make it easier to tell the local backup from the remote backup.
- Review your settings. Then click **Save** to save your changes to the remote backup plan.

Remote Backup Plan - Backing up Directly to the eFolder Acronis Vault

If you feel that your customer has a fast enough Internet upload speed and the initial size of the full backups would transfer across the Internet in a timely fashion, then you may want to consider backing up the Acronis initial full backups directly to the eFolder Acronis vault without sending a seed drive. To do this, you can either clone your local backup job if you have one already configured and reconfigure the settings to match those in the section above (without backing up to the seed vault, of course) or setup a new backup plan if there are no plans to backup locally.

To setup a remote backup plan, perform the following steps:

- a. Using the Acronis console, connect to your locally installed AMS. Click **Backup plans and tasks** in the left navigation window, then click **New** and select **Backup plan** to create a new backup plan (see Figure 7.1).

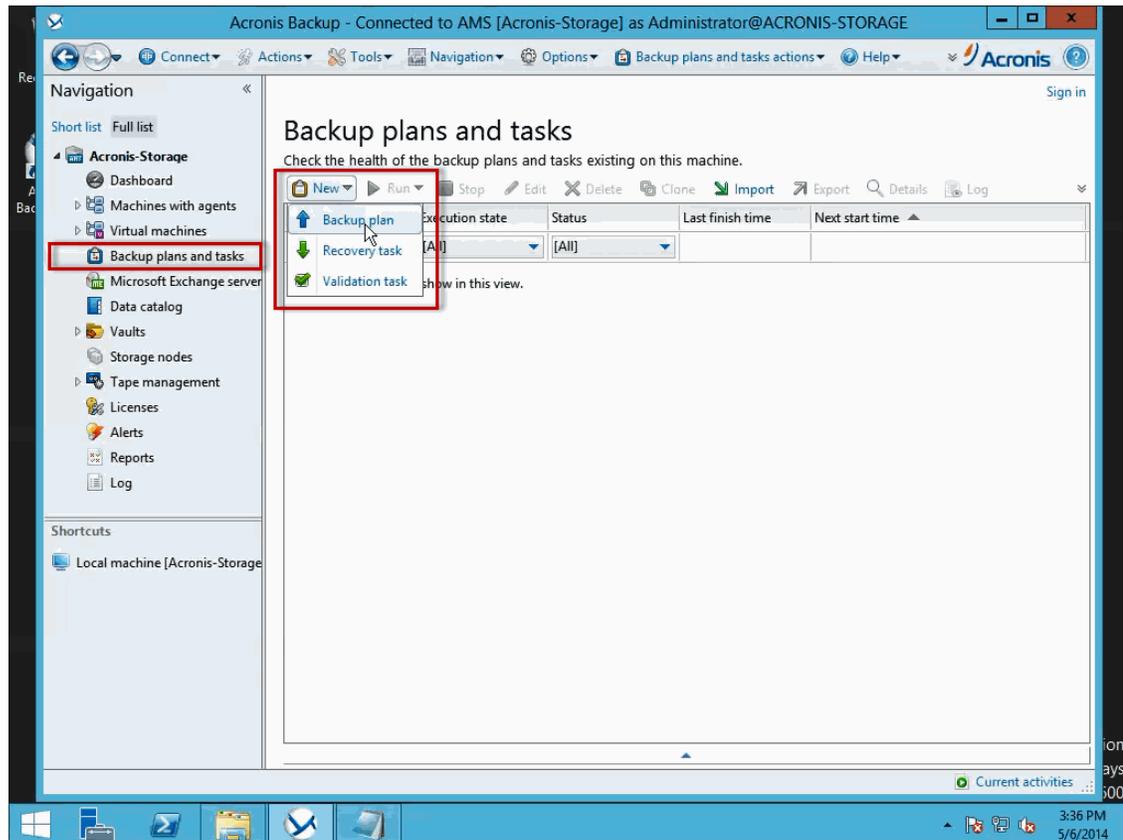


Figure 7.1

- b. In the *Create backup plan* window, in the *What to back up* section, click the blue **Required** link to open the *Data to Back Up* dialog box. Then expand the **Machines with agents** group to locate the machine(s) that you are going to include with this backup plan and click **OK** to continue (see Figure 7.2).

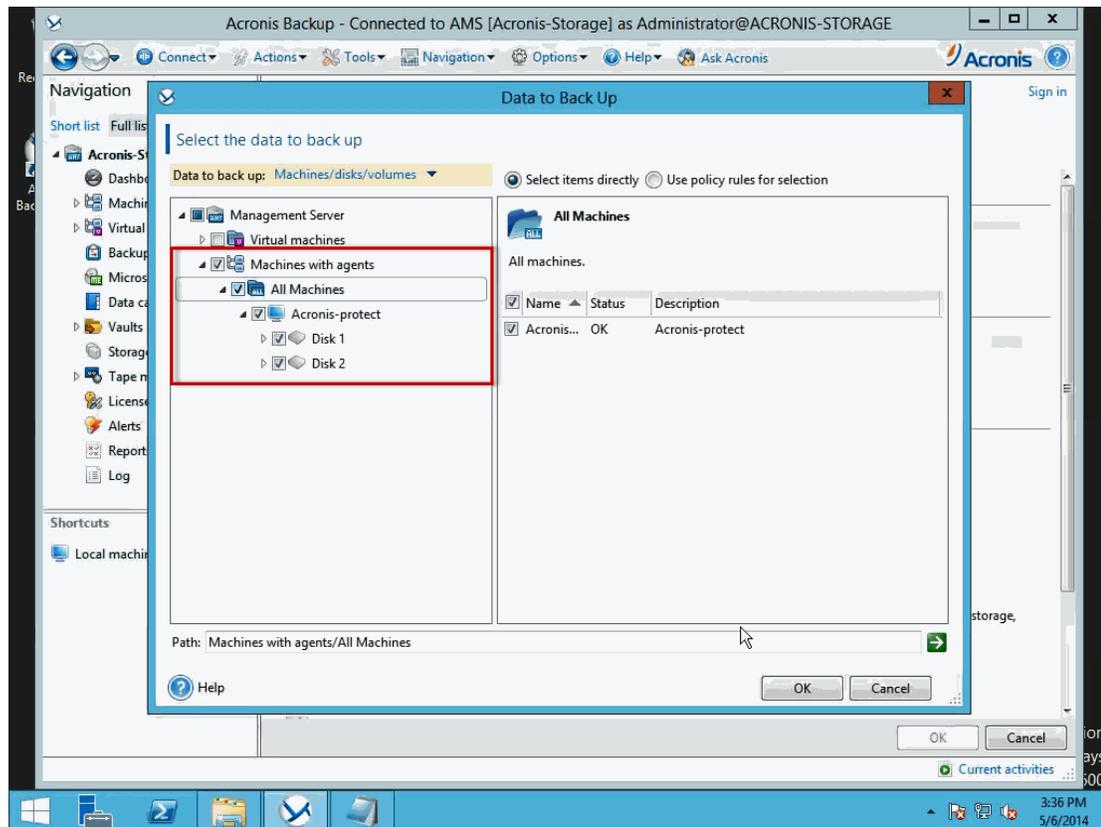


Figure 7.2

- c. In the *Where to back up* section, click the blue **Location...** link to open the *Location* dialog box. Ensure that the top radio button labeled **Store all machines' archives in a single location** is selected. In the left window, select **Storage node**. In the **Path:** field, enter in the remote server address you were provided with when your eFolder Acronis Management Server was assigned to you.

Important! When entering the address, you must keep the "bsp://" as part of the address. Also, you must click the GREEN RIGHT ARROW to connect to the remote storage node. If you click OK it does not complete the connection and your archive will NOT be sent to the remote storage node (see Figure 7.3).

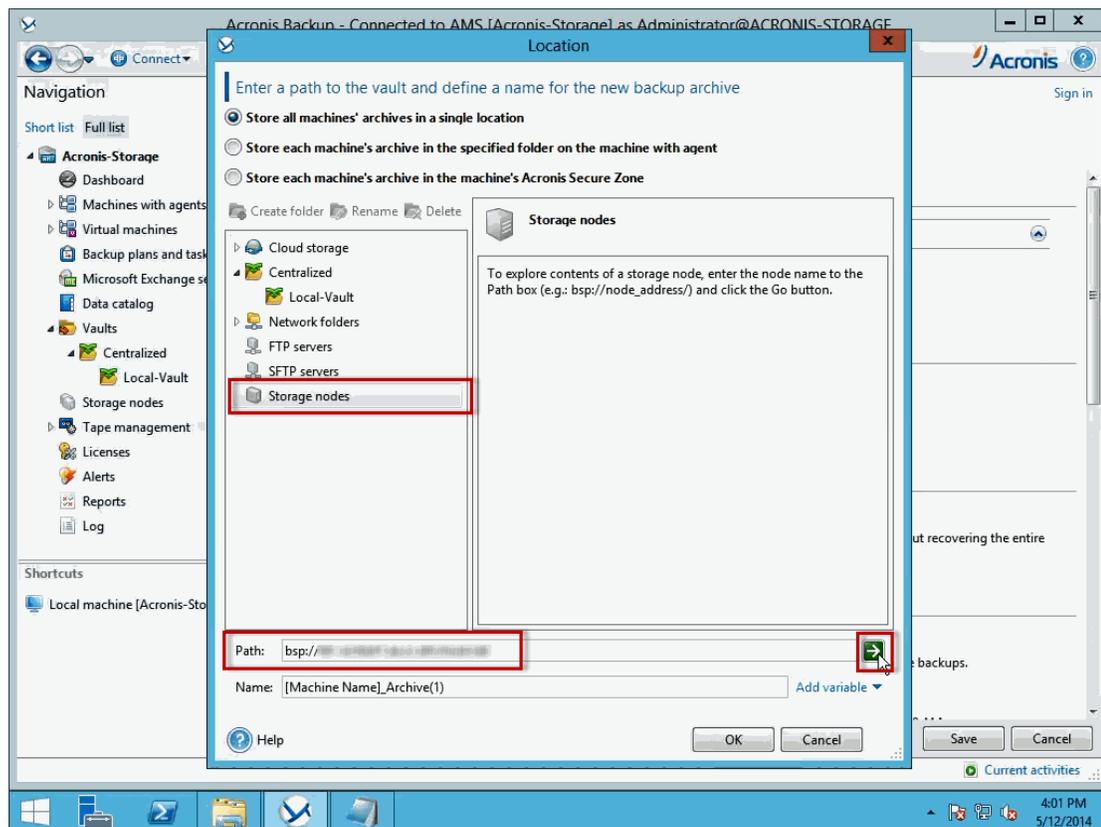


Figure 7.3

- d. After clicking the **GREEN RIGHT ARROW** to connect to your eFolder AMS, the *Access Credentials* dialog box appears. Enter the username and password provided to you by eFolder when your eFolder AMS was assigned to you.

- e. After your credentials have been verified, expand the **Storage nodes** in the window on the left, expand the node labeled with your AMS name, and click on the managed vault that you created previously. Then click **OK** to continue (see Figure 7.4).

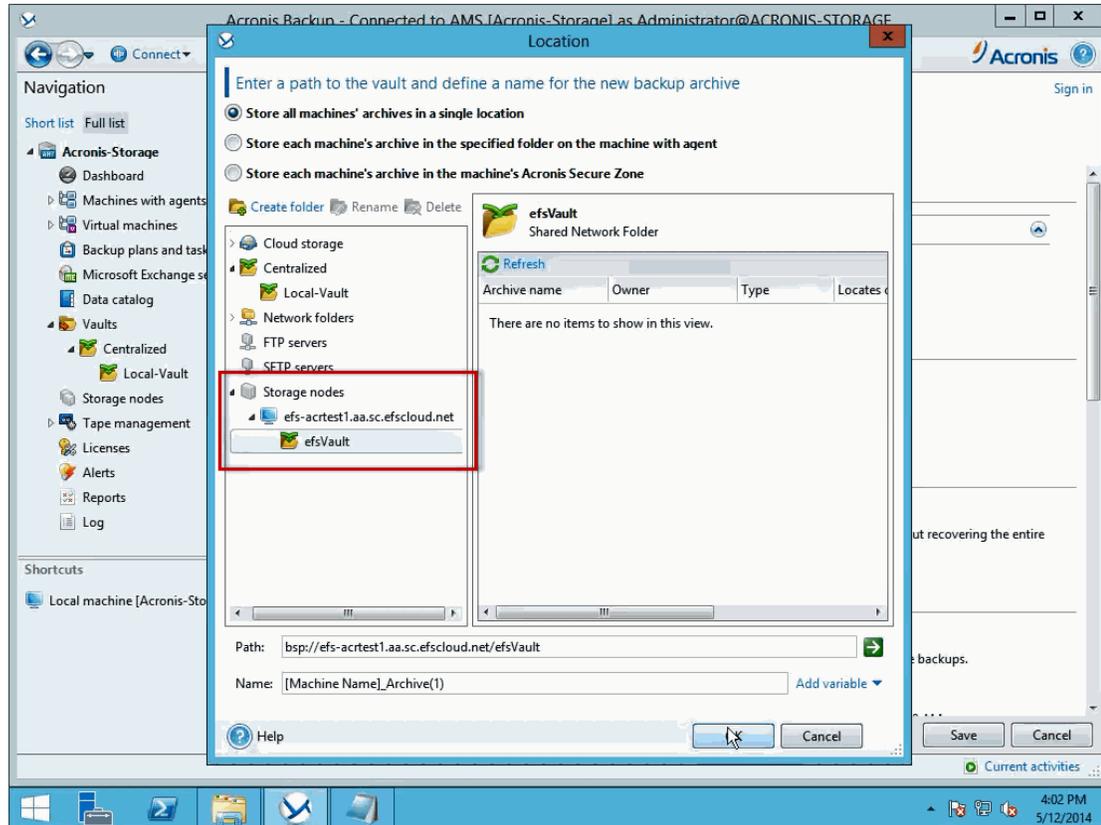


Figure 7.4

- f. In the *Single-pass disk and application backup* section, decide whether to **enable** or **disable** the single-pass backup (see step 4 in *Configuring the Local Backup Plan* for more information).

Important! If you plan to provide granular recovery to an Exchange Information Store, you must back up that Exchange server with a local backup. Performing granular recovery to an Exchange Information Store is not supported from Acronis backups that are backed up to the eFolder Cloud.

- g. Because of your customer's slower bandwidth in backing up files over the Internet to the eFolder Acronis vault, we recommend that you change the incremental backup from hourly backups to once a day. *We also recommend that you change the day the full or monthly backup happens from a standard end or beginning of the month setting to an arbitrary day in the month. This will help ensure that you have optimal performance when uploading more than one customer to your eFolder Acronis vault.* The following steps will lead you through making these changes:

In the **How to back up** section, change the following settings:

- Backup scheme: Change the selection in the drop down menu to **Custom**.
- Full Backup: Click the blue **Add schedule...** link and select the **Monthly** radio button from the **Run the task:** menu. Then choose the day of the month or the week number and day you would like to send your full backup to the eFolder Acronis vault (see Figure 7.5). Next, set the time you would like the full or monthly backup to start by selecting the radio button labeled **Once at:** and setting the start time. Then click **OK** to continue.

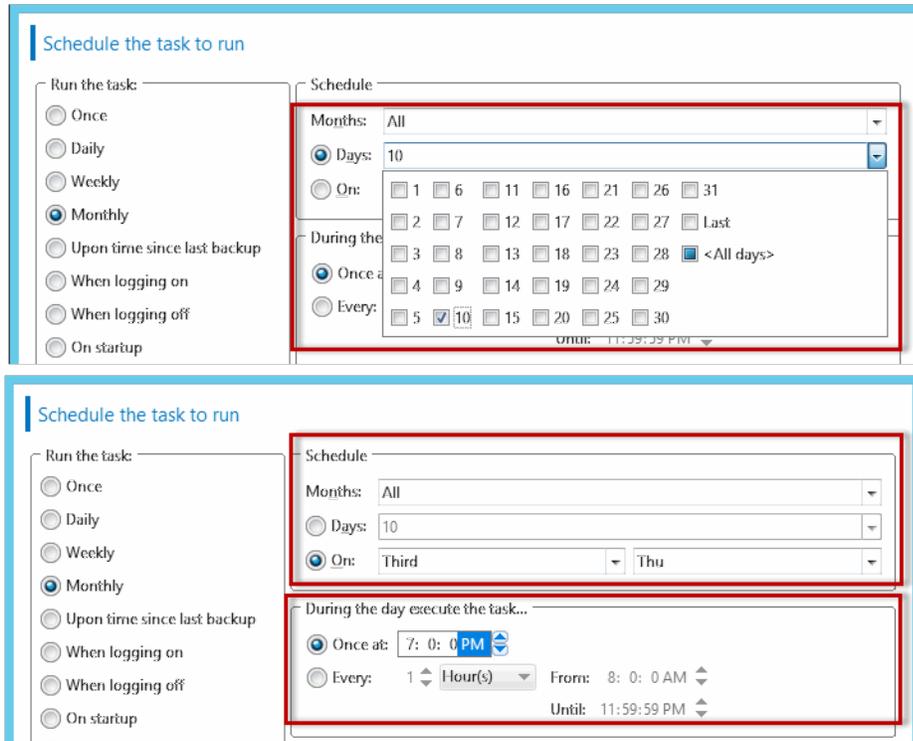


Figure 7.5

- Incremental backup: Click the blue **Add schedule...** link and select the **Daily** radio button from the **Run the task** menu. Then choose the **Once at:** radio button and set the time you would like the once-a-day incremental to run (see Figure 7.6).

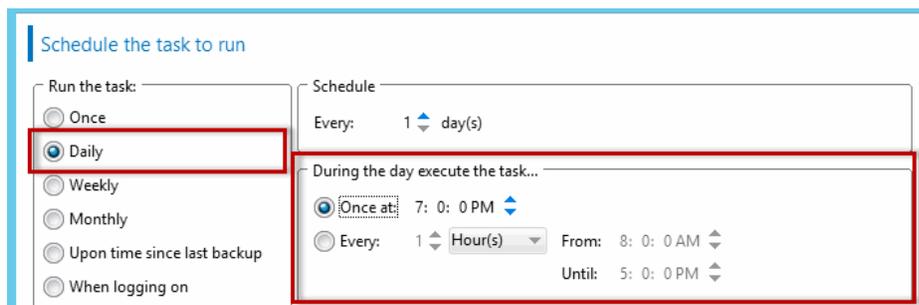


Figure 7.6

- d. Differential backup: In the *Run the task:* section on the left, select the **Weekly** radio button. In the *Schedule* section, uncheck all of the days except the day you would like to run your differential (weekly backup). We suggest that you set this to the end or start of a week, like Saturday or Sunday. In the *During the day to execute the task...* section, select the **Once at:** radio button and set the time of day you would like the differential backup to start. Leave all of the other settings at their default values and click **OK** to continue.

Note: To maximize performance of your eFolder Acronis vault, we recommend that you pick an arbitrary day when sending more than one customer to your remote vault.

- e. Clean up archive: We recommend that you change the Retention Rules to keep a minimum of 60 days' worth of archives in the eFolder Acronis vault. If your customer requires a longer retention than 60 days, that is okay—just do not set it for less than 60 days. Click the drop down menu and select **Using retention rules**. The menu options will change. Next, select **Retention rules...** to open the *Retention Rules* dialog box. To keep a retention of 60 days, ensure that the **Age and size:** radio button is selected and then check the checkbox labeled **Backups older than:** and type 60 in the text box. Then adjust the retention settings to **Days(s)** if it is not already selected. Leave all other settings at their default values and click **OK** to continue (see Figure 7.7).

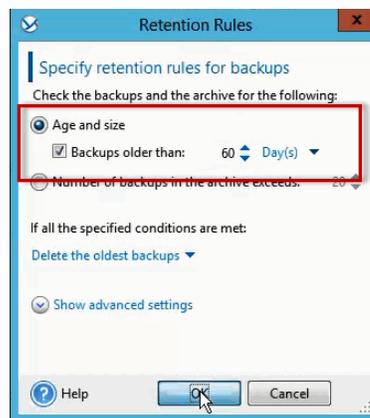


Figure 7.7

- f. Plan name: Name your backup plan to resemble something like "*Remote backup plan*" to make it easier to tell the local backup from the remote backup if you happen to be backing up locally as well.
- g. Review your settings. Then click **Save** to save your changes to the remote backup plan.

Additional Resources

Self Help

Acronis Backup Advance online help:

http://www.acronis.com/en-us/support/documentation/AcronisBackup_11.5/#14080.html

Acronis Knowledge Base: <https://kb.acronis.com/>

eFolder Knowledge Base:

<https://secure.efoldering.com/support/index.php?efolder/Knowledgebase/List/Index/>

For training videos and documentation, login to the eFolder Web Portal with your partner account.

Then mouse over the **Support** menu item and click **Partner Center**. On the *Partner Center* page, click the **Learning Center** link.

Acronis Backup Advanced download:

<https://secure.efoldering.com/support/index.php?efolder/Knowledgebase/Article/View/278/67/acronis-for-efolder-download>

Deprovisioning Acronis Agents and Licenses:

<https://secure.efoldering.com/support/index.php?efolder/Knowledgebase/Article/View/367/59/deprovisioning-acronis-licenses>

Technical Support

eFolder Support Center:

<https://secure.efoldering.com/support/index.php?efolder/Tickets/Submit>

Contact eFolder Acronis support via email and phone:

Email: acronissupport@efolder.net

When you email Support, a medium-level support ticket will be opened.

Phone: 800-352-0248, option 2, then option 1



The People Behind Your Cloud