# Choosing a Security Role and Service Plan for an Account

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

**Introduction**

This video explains how to decide which security role and service plan to assign to an account. You should understand what accounts and sub-accounts are before viewing this video. If you need training on these concepts, please see the section on accounts in the video entitled, *Overview of the Web Portal*.

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

**What you need to know about security roles**

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

Let’s begin by discussing *security* *roles*, or *roles* for short. Every account is assigned a security role. Roles determine the account management functions and the range of accounts users can see and act on when they login to the Web Portal.

For example, when a new partner signs up with eFolder, the partner’s new account is given the *Partner Senior Manager* role. This role allows partners unrestricted access to their own account and all of the accounts that have been created within their brands. It also allows them to use *all* of the partner functions in the Web Portal.

On the other hand, when *you* create a new customer or end-user account, it is automatically given the *default,* or *end-user* role, which is the most restrictive role. As a partner, you can change this role at any time in the Account Center or Account List in the Web Portal. Note that only users who have the Partner Senior Manager role can assign or changes security roles.

To change the role assigned to an account, first navigate to either the Account Center or the Account List in the Web Portal. If you are in the Account Center, check the box in front of the account and select *Set Role* from **Password / Security** submenu in the **Actions** option on the menu bar, or right click on the account to display this same menu. If you are using the Account List, click the [**s]et** link in the *Role* column for the account.

Roles are set up to help the partner manage and maintain control over their accounts. Just as the owner of a computer network does *not* give end-users access to network configuration or administrative functions, you should not give end-users a role that provides access to the same partner functions that you have to view and manage your accounts.

Because you may not have the time, bandwidth, or desire to perform all of the tasks needed to manage dozens or even hundreds of accounts, roles allow you to delegate specific levels of authority to other users of your choosing. For example, you might assign your lead technical support staff the *Partner Senior Customer Service* role that allows them to create, manage, and delete customer and end-user accounts, but prevents them from assigning security roles to accounts.

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

**Security role descriptions**

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

Let’s take a closer look at each of the seven predefined security roles. We’ll discuss them in order of authority, starting with the role with the highest level of authority first.

The *Partner Senior Manager* role is designed for partners. It is the role with the highest level of authority eFolder will give to a partner. It gives you, the partner, full control over *all* of the accounts associated with your brand, and it provides you unlimited access to *all* of the partner-related management tasks in the Web Portal. For example, you can

* Create new accounts,
* Assign any of the seven security roles to other accounts,
* Delete accounts,
* Manage accounts without restriction,
* View reports and logs,
* Set up partner notifications,
* Open a ticket with Technical Support,
* Access the Partner Center documentation and training, and so forth.

Because this role has no restrictions in terms of viewing, managing, and deleting accounts, you should be very careful about sharing this role with others. Many partners keep this role solely to themselves or assign this role to one other extremely trusted, loyal employee who has a vested interest in the business.

The next two roles are designed for customer service representatives. The *Partner Senior Customer Service* role gives users the authority to create, manage, and delete customer accounts. They can do everything the *Partner Senior Manager* role can do *except* assign security roles or impersonate an account with the Partner Senior Manager role. Again, this is a *very* high level of authority, so be selective in assigning this role.

They can impersonate all accounts at their security level or below, which will cause the Web Portal to display only those options available to the account being impersonated. In other words, when you impersonate an account, it is as if you had logged in to the Web Portal as the user for that account. This allows an administrator to do things to the account as if they were the user, such as change the account’s password or set notifications for the account.

The *Partner Customer Service* role is designed for lower-level customer service representatives. It gives them the authority to perform a more restricted set of account management tasks for a brand, such as change a password or run reports, but they *cannot* create or delete accounts or subaccounts. They can see all of the accounts for your brand, but they can only impersonate the Read-Only accounts.

You might want to assign the *Partner Customer Service* role, for example, to an account manager or sales representative who handles simple requests from customers or end-users, such as resetting a password.

The *Partner Read Only* role provides read-only access to account information. Users assigned this role cannot *change* account information, and they *cannot* impersonate an account. You might assign this role, for example, to your accountant or to lower-level sales representatives who needs to see what is going on but should be restricted from making any changes. Even though this is a “read only” role, users assigned this role still see the customer company names, user names, and Service Plans, so practice care in assigning this role.

The *Partner API* role is a web services account that allows a branded partner to use the API to access all of their customer data. It does not have permissions to log on interactively.

The *Power User* and *Default* or *User* roles are designed for end-users.

The role with the lowest-level of authority is the *Default* or *User* role. This is the role that is always assigned to an account when it is first created. Users assigned this role can backup and restore their data using the Backup Manager client on their local machine and can login to the Web Portal where they have the same functionality as the Power User, except they can only impersonate other accounts with *User* roles and cannot impersonate accounts with *Power User* role. That is the only difference between the *Power User* role and the *Default* or *User* role.

Both roles provide the ability for a user to see their own account and any other accounts under the same company. They have limited functionality in the Account Center and in the Account List, including the ability to impersonate other accounts at their same level or below. They can:

* reset the Password,
* set the User Quota,
* set Email Address and Description (but not Internal Description),
* take an account out of maintenance mode (but not put an account into maintenance mode),
* view the Online Backup Session Report and Event Log Report,
* rename the account User Name
* double click on the account to show the account details on the bottom half of the screen where they can see the Backup Session Report,
* view the Online Backup Summary Report,
* download the Online Backup Summary Report,
* view the Online Backup Log,
* download the Online Backup Log,
* view the Backup Settings History, and
* view the Status Report under **Accounts**.

While they are impersonating an account, they can edit the Notifications, Mailing Lists, and Contact Information settings, and set or change the password for that account.

Finally, they have access to menu options to download the Backup Manager, recover a pass phrase, access the online help, and email customer support.

Note that the *Power User* and D*efault* or *User* roles must be parent accounts to have access to other accounts within the same company.

Note also that even with the *Default* or *User* level of authority, users can create new sub-accounts under their own account by selecting *Create Account* under the **Accounts** menu option. Because of this and other reasons, many partners, including managed service providers, do not even tell their end-users about the Web Portal. These partners perform all account management tasks on behalf of their end users, so there is no reason for end users to access the Web Portal.

Refer to the *Comparison of Security Roles* table in the **Resources** tab of this video or in the Partner Center in the Web Portal to see the functions a particular role can and cannot perform. As a new partner, you may want to print out this table and refer to it when you are assigning roles to accounts.

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

**What you need to know about service plans**

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

A service plan is the billable eFolder service that is assigned to an account, such as the *eFolder Backup for Files* service, or the *Backup and Disaster Recovery (or BDR)* service. Each account has one and only one service plan that is associated with the account. Customers must have an account for each service they use. For example, a customer who wants to use both the *Basic* and the *Select* versions of the *Backup for Files* service must have an account for each one. This enables eFolder and partners to bill appropriately for their services. Each service typically has a different billing rate or structure.

For example, for the *Backup for Files* service, eFolder bills you only for the total aggregate space you occupy in the eFolder cloud across *all* of your accounts that are using this service, not for each individual account. The exception is for accounts that are using this service to backup data locally and not to the cloud. These accounts are charged a flat billing rate.

As another example, for the *BDR for ShadowProtect* service, eFolder bills you for *each* BDR appliance and account, according to the specific BDR hardware, configuration, and licenses that are used.

All these examples illustrate that rates are tied to service plans and any options they may have.

When you create an account and assign that account a service plan, eFolder will automatically bill you according to the terms of the assigned service plan. Because of this, you should only create an account after you have decided which service plan you want to assign to the account. Of course, as a partner, you are free to charge your customers whatever you want for the eFolder services you resell under your own brand. The difference between what eFolder charges you and what you charge your customers is your recurring revenue.

After an account has been created and is in service, there are some circumstances that merit changing the service plan that is associated with the account, such as upgrading an *eFolder* *Backup for Files* account from *Basic* to *Select* or changing an account from *Trial (Select)* to *Select.*

In contrast to security roles, which are always assigned the *Default* or *End-user* security role by the system when you create the account, you must *choose* a service plan for an account at the time you create it or the system will not allow you to finish creating the account.

Where do you assign a service plan to an account? For new accounts, if you are creating the account using the New Account wizard in the Account Center, you assign a service plan to the account in the *Plan* field on page 3 of the wizard. If you are creating the account using the *Create Account* page, you assign the plan in the *Service Plan* field near the bottom of the page.

If you need to *reassign* a service plan for an existing account, login to the Web Portal and select either *Account Center (Visual View)* or *Account List (Detailed View)* from the **Accounts** menu. If you are using the Account Center, check the box in front of the account and select *Set Service Plan* from the **Actions** option on the menu bar, or simply right click on the account to bring up the same menu. If you are using the Account List, click the **[s]et** link in the *Service Plan* column for the account.

Note that when you change an account’s service plan, you may have to perform additional tasks before the account can begin using the service. For example, if you change the *eFolder* *Backup for Files* service for an account from *Basic* to *Select*, you should review and set the versioning options in the Backup Manager.

Many eFolder services are managed through the Web Portal using the account management functions. The *Cloudfinder*, *Acronis*, *Anchor*, and *AppAssure Core* services are three exceptions. They each have their own management web site or management software. However, with *AppAssure Core*, you can also monitor the status of all COREs using the eFolder Web Portal and the Backup Manager. Acronis uses the eFolder Web Portal to provision license keys.

For those services that are managed through the Web Portal, creating an account and assigning it a service plan is, in most cases, how you enroll or “sign up” a customer or end-user for a particular service, such as the *eFolder* *Backup for Files* service. However, after you have created an account and assigned it a service, you will need to perform a few additional steps to implement the service that are specific to that service. For example, to use the *eFolder Backup for Files* service, after you create the new account, you must download and install the Backup Manager on the machine to be backed up.

As all of these details can be a little challenging to remember, refer to the *Overview of eFolder Service Plans* table in the **Resources** tab of this video or in the Partner Center in the Web Portal to see a summary of each plan, where it is managed, and how it is ordered or initiated. As a new partner, you may want to print out this table and refer to it when you are creating new accounts.

Keep in mind that the number of available service plans will expand over time as eFolder continues to offer additional services for its partners. You can see the latest list of those service plans that *you* have the authority to assign to an account by clicking the *Service Plan* drop-down in the *Create Account* page. Note that some service plans do *not* show up in your Service Plan drop-down list, such as Acronis. To use Acronis*,* you must have a signed Acronis agreement which your Account Manager can provide for you. After your Account Manager has received this signed agreement, he or she will enable this option so that you can choose this service plan when you create an account.

To stay abreast of new service offerings as they are announced, visit or subscribe to the eFolder social web sites on Facebook and Twitter, to the eFolder Blog, or to the eFolder mailing lists on the Web Portal under the **My Account, Mailing Lists** menu option, or visit the **Recent News** option in the Support Center in the Web Portal.

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

**Service plan categories**

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

Let’s take a brief look at each of eFolder’s current service offerings. For purposes of discussion, these services can be grouped into the following three categories: File backup services, backup and disaster recovery (or BDR) services, and email security. We’ll look at the available service plans under each of these categories. Note that you can read detailed descriptions of each of the services that eFolder offers by going to eFolder’s web site at [www.efolder.net](http://www.efolder.net) and clicking **Products** on the menu bar.

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

**The eFolder Backup for Files service**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_To begin, let’s look at service plans that are part of the *eFolder Backup for Files* service. For a detailed description of what this service is and how it works, please see the related video in this series entitled, *Overview of eFolder Backup for Files*.

*eFolder Backup for Files* has four available service plans: *Basic*, *Select, Trial (Basic)*, and *Trial (Select).* Accounts assigned to these plans are all managed through the Web Portal. To enroll a customer or end-user in this service, simply create a new account, assign the account one of these plans, and install and configure the Backup Manager client on the machine to be backed up, which is available for download in the Web Portal.

The Basic service plan only keeps the most recent 30 days of historical versions for each file. On desktops and laptops, the Basic plan can backup open files, such as Outlook or QuickBooks files, using VSS snapshots. On servers, the Basic plan *cannot* backup files that are open for exclusive access, such as Microsoft Exchange or SQL Server files, but it can backup other files, such as Excel and Word files.

The Select service plan allows an unlimited number of historical versions for files and can backup open files, including Exchange and SQL server files, using Microsoft VSS snapshots.

Trial backup accounts give your potential customers the opportunity to “test drive” a service. Hence, they are an invaluable sales tool. For the *eFolder Backup for Files* service, potential customers can “test drive” either the *Basic* service plan or the *Select* service plan on the actual systems they want to backup.

Trial accounts for the *eFolder Backup for Files* service are created by assigning a new account either the *Trial (Basic)* or *Trial (Select)* service plan. The *Trial (Basic)* plan is identical to the *Basic* plan, and the *Trial (Select)* plan is identical to the *Select* plan, except that trial accounts by default expire after 30 days and are limited to 10 GB of storage as a general rule. However, you can increase the storage space to a larger number and extend the expiration date up to 60 days. Note that eFolder does *not* charge you for the space your trial accounts occupy in the cloud, but you are limited to a total of 750 gigabytes across all of your *eFolder Backup for Files* trial accounts. Within that limit, you are free to allocate space across your trial accounts any way you want.

If your customer signs up for the full service, then access the Account Center or Account List in the Web Portal, and assign the *Basic* or *Select* service plan to the account, as appropriate, which will remove the expiration date. You should also adjust the storage quota as desired.

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

**An overview of how backup and disaster recovery (BDR) servers work**

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

Now let’s look at service plans that fall into the backup and disaster recovery (or BDR) category. Plans in this category typically back up entire images of servers and desktops to a central server, which is sometimes called a *BDR appliance* if the machine has been specifically built, preconfigured, and sold as a BDR. After these images are stored on the BDR, they can optionally be replicated to other BDRs, servers, or to a network storage device, and they can also be backed up to the eFolder cloud or to another location.

A BDR receives images from the agents that are installed on the individual machines. An image is an exact replica of the contents of a storage device, such as a disk drive or volume. It is a “snapshot” of your data. An image is typically made of an entire drive or machine, including all partitions, but it could be made of one or more volumes or partitions of a disk. You decide what you want to take an image of on each server that is backed up.

Images are created on the local servers by a software client or agent that resides on the servers. The agent creates images according to the schedule you set and sends them across the network to a folder on the BDR server. Incremental images are typically created and sent to the BDR multiple times throughout the day. At the end of the day, week, and month, the BDR consolidates the images into daily, weekly, and monthly image files. This reduces the storage space required on the BDR and in any other locations where the images are optionally being stored.

An image of an entire system including the operating system is called a “bare-metal” image. A bare-metal image can be installed on completely new hardware, even hardware that is dissimilar to the original machine. In other words, it can be restored to a “bare” machine that does not have the operating system installed—hence the term “bare-metal image.”

An image that is made of an entire server, such as a bare-metal image, provides an additional benefit. It can be quickly “virtualized” on the BDR when the original server fails. A new virtual server can be built from any previously backed-up image and “spun up,” or started, on the BDR machine, providing business continuity for mission critical services and applications in case of local server failure. Server images can also be backed up to the eFolder cloud, where they can also be virtualized if the BDR itself fails or is destroyed in a natural or man-made disaster. Please contact your Account Manager or eFolder technical support to sign up for this option.

The images on the BDR can also be *replicated* to another BDR or to a network storage device. Replication is different from backup. Replication sends an exact copy of the image without performing any compression, de-duplication, or encryption on that image, and it does not require that the image be de-encrypted and restored before it can be used. Replication provides for near-instant virtualization of server images on other machines that are typically located within the same network. On the other hand, cloud backup provides high data redundancy, encryption, high security, and protection against silent data corruption and local and regional disasters. For ShadowProtect BDRs, you can do both replication and backup from the same BDR. For AppAssure BDRs, you can replicate to the cloud and/or another server. For both ShadowProtect and AppAssure, it is recommended that you set an encryption password as part of the image creation process so the images are protected wherever they are stored.

In short, the eFolder BDR service category offers the following additional software and backup options that can be mixed and matched as desired in any of the following four ways:

1. *Cloud backup and recovery*: Bare-metal backups are encrypted and sent to the eFolder storage cloud for safekeeping. The backed up servers can also be virtualized in the eFolder Continuity Cloud for the ultimate in disaster recovery scenarios.
2. *Site-to-site backup and recovery*: Bare-metal backups can be replicated to another BDR (or any other Windows server). Servers can be virtualized just as quickly on the target BDR, providing the perfect option for customers with multiple sites or for building your own private storage cloud.
3. *On-site backup and recovery*: Bare-metal backups can be backed up to a NAS device or USB-disk. USB-disk backups can be rotated on any schedule.
4. *Software-only option*: The technologies powering eFolder BDRs can easily be licensed separately from our hardware, allowing you to leverage existing hardware or to build your own BDR hardware.

Now let’s look at the service plans that are available in the BDR category: *ShadowProtect BDR, Trial (ShadowProtect), ShadowProtect Standalone, AppAssure CORE, Trial (AppAssure CORE), BDR for Acronis, BDR Rescue Program,* *Multitenant Network Server, and Trial (Multitenant Network Server)*.

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

**The eFolder BDR for ShadowProtect service plans**

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

The *ShadowProtect BDR* service plan is assigned to accounts for which you or a customer has purchased a BDR appliance from eFolder that uses StorageCraft’s ShadowProtect backup and imaging software along with eFolder’s proprietary technology for online backup to the cloud and global monitoring. All eFolder BDR appliances come preconfigured with all of the software you need to quickly become operational.

The eFolder Backup Manager allows you to perform cloud backup and recovery, replication, site-to-site backup and recovery, and on-site backup and recovery. The eFolder Backup Manager monitors the ImageManager logs and the integrity of the ShadowProtect images, even if you are only using the BDR to store the server images locally so you have the option to spin up a virtual server when a server goes down. The eFolder Backup Manager reports these results to the eFolder Web Portal, which allows you to monitor backup status and storage utilization for all of your accounts, whether they are file or image backups, in one central location in the eFolder Web Portal.

For help with choosing an appropriate BDR model for a customer and calculating end-user pricing, download the *eFolder BDR for ShadowProtect Cost Wizard* from the Partner Center in the Web Portal and view the related video in this series entitled, *How to Use the BDR for ShadowProtect Cost Wizard.*

The *Trial (ShadowProtect)* service plan is identical to the *ShadowProtect BDR* service plan, except it is limited to a 30-day trial period by default, which you as the partner can extend up to 60 days, and it is limited to 500 GB of storage space per trial. For the trial, you can use either an eFolder BDR appliance or your own BDR hardware. If you like, eFolder will provide an eFolder BDR appliance for your very first BDR trial. After that, you will need to provide your own BDR hardware for trials or purchase a BDR appliance from eFolder. As with all trial accounts, you are *not* charged for the storage space these trials occupy in the cloud. You can have up to eight ShadowProtect BDR trial accounts that are active at any one time. These trial accounts are managed through the Web Portal.

When a trial-account customer is ready to sign up to continue service, you can easily convert the trial account to a regular paying account by reassigning the account to either the *ShadowProtect BDR* service plan or the *ShadowProtect Standalone* service plan which will remove the expiration date in the Account Center or Account List in the Web Portal.

The next BDR service plan is the *ShadowProtect Standalone* service plan. This is a software-only option intended for partners or customers who want to build their own BDR hardware or use existing equipment at the client site. It licenses the same ShadowProtect software and eFolder technology for online backup to the cloud and global monitoring that is provided with the *eFolder BDR for ShadowProtect* product offering. You can configure the eFolder Backup Manager to check the ImageManager logs and verify the integrity of the ShadowProtect images. You can also configure Backup Manager to do cloud backup and recovery, replication, site-to-site backup and recovery, and on-site backup and recovery.

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

**The eFolder AppAssure CORE service plan**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_The next service plan is the *AppAssure CORE* service plan. AppAssure uses its own management application to perform cloud replication. So, an eFolder account is not required to perform the backup or replication. However, you can create an eFolder account in order to use the Backup Manager and the eFolder Web Portal to monitor and report on the status of each AppAssure CORE.

You can find a training tutorial entitled “How to monitor AppAssure BDR status and utilization using the Web Portal” in Learning Center section of the Partner Center on the eFolder Web Portal.

This video explains how to create an account on the eFolder Portal with the AppAssure CORE service plan, then download and configure the Backup Manager on each of your AppAssure COREs so you can use the eFolder Web Portal to monitor the status of all of your local and cloud-hosted AppAssure services. The monitoring integration allows you to:

* Centrally monitor the status of all of your COREs from one cloud-based web portal
* Setup global alerting rules that generate emails or PSA tickets on warning or error conditions
* Setup automated billing integration with supported PSA systems

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

**The eFolder BDR for Acronis service plan**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_The next BDR service plan is the *BDR for Acronis* service plan*.* This plan is used to provision license keys for the Acronis Backup Advanced Agent, Acronis Add-on Agents, and Acronis Hypervisor or Virtual Host Agent.

For you to manually provision Acronis licenses from the eFolder Web Portal, you must agree to, sign, and return the Acronis Agreement(s) to your Account Manager.

The *Acronis Solution Guide and Best Practices* is available in the Partner Documentation section of the Partner Center of the eFolder Web Portal.

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

**The eFolder BDR Rescue Program service plan**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_The next BDR service plan is the *BDR Rescue Program.* The BDR Rescue Program is for customers who are currently backing up their BDR data to another provider’s data center or cloud and want instead to backup their BDR data to the eFolder cloud at specially reduced rates so that they can enjoy all of the technological and business benefits that storage in the eFolder cloud offers. With this service, the partner’s technical support team helps the customer to reconfigure their BDR to stop sending backups to their current destination and start sending them to the eFolder cloud using the Backup Manager.

Because customers who participate in this program receive a special discounted rate for storing their BDR data in the cloud, you can easily approach your customers about making the switch to *your* branded service for BDR backups. Note that the customer is still responsible for all of their hardware, software, and licensing issues for their BDR. To use this service, create a new account, download and install the Backup Manager on the BDR, and have your technical support team perform the required configuration.

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

**The eFolder Multitenant Network Server service plan**

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

The next BDR service plan is the *Multitenant Network Server* service plan. This plan has to do with backing up data from multiple machines to a destination server of your choosing on your network. That is what the “multitenant” means in the name of the plan—there are multiple “tenants,” or machines, that are all backing up data to this single server. To understand this plan, let’s revisit some of the configuration options in the Backup Manager. When you use the *Basic*, *Select*, or *ShadowProtect BDR* services to backup data from a local machine or BDR, you can send that data to up to three different destinations, as specified in the destination fields in the **My Account** panel in the Backup Manager.

The path in the first field, labeled *Remote Service,* is used when you want to backup data to the eFolder cloud. This field is usually already prefilled with the path to the eFolder server. The path in the third field, labeled *Local Disk*, is used when you want to backup data to a storage device that is located in the same office, frequently attached temporarily or permanently to your local machine, such as a USB drive.

The second field, labeled *Local Server*, is the field of interest to the *Multitenant Network Server* service plan. The IP address or DNS name in this field is used when you want to backup data from this machine to another server of your choosing, usually at a remote location. This destination server is called the “local server” by the Backup Manager, regardless of whether the server is on your local network, located at a remote office, or is remotely accessed across the public network.

Anytime you backup data to a “local server” using the Backup Manager, you must install the Backup Manager and the Backup Server Manager on the “local server” that will be receiving the data so that it can authenticate your machine and receive the backed up data.

Now here’s where the *Multitenant Network Server* service plan comes into play. If the “local server” is going to receive data from only one machine, you do not need this service plan. However, if you want the “local server” to receive data from two or more machines, then you must create a new account in the Web Portal and assign it the *Multitenant Network Server* service plan. Then you must configure the Backup Server Manager on the “local server” to receive data from multiple machines. This will allow the “local server” to authenticate each machine that is sending data to it. This plan does have a monthly service fee and is managed through the Web Portal.

For example, suppose you have 15 different customers, each of whom has a BDR that you want to backup to a server on your local network. To do this, create a new account for the “local server,” assign it the *Multitenant Network Server* service plan, install and configure the Backup Server Manager on the “local server,” and then configure the Backup Manager on each of the 15 machines to point to the “local server” in the *Local Server* field of the **My Account** panel. That is all there is to it.

The *Trial (Multitenant Network Server)* service plan is identical to the *Multitenant Network Server* service plan, except it is limited to a 30-day trial period by default, which you as the partner can extend up to 60 days. Because the data is being backed up to your own server, you do not need to set a storage limit for this trial account.

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

**The eFolder Email Security service plan**

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

Finally, let’s take a look at the email security category. The *eFolder Email Security* service is a cloud email security solution that requires *no* on-site hardware or software. Leveraging the eFolder Security Cloud, eFolder Email Security delivers comprehensive inbound and outbound protection from spam, viruses, spyware, and phishing attacks, while ensuring email visibility and control for administrators and dynamic, per-user filtering for employees. Optionally, you can provide your own on-site appliance to host this service, or you can buy the appliance from eFolder.

More specifically, with this service:

* Subscribers point their Mail Exchange (MX) records to the eFolder Security Cloud.
* All inbound and outbound email are filtered and scanned in the cloud.
* The vast majority of spam will be blocked and logged based upon results from eFolder’s real-time threat analysis networks.
* Messages requiring additional filtering are scanned for viruses, phishing attacks, or content violations and are put through additional statistical analysis.
* Dangerous messages and confirmed spam are blocked, while other unwanted email is placed in the message quarantine.
* Administrators and users can access the message quarantine to release messages, which automatically updates their user-approved and user-blocked lists.

Email Security is administered and managed through its own web site, allowing anytime, anywhere access. Administrators can access a rich set of statistics and logs, manage security policies, and use sophisticated logging and message search functions to support user requests.

Just as importantly, end-users can access their spam quarantine 24/7 and locate, delete, or release quarantined messages, all without administrator involvement. Finally, Active directory and LDAP integration provides automated user provisioning and deprovisioning.

To use *Email Security,* you must send a request to the eFolder support team, who will then create an account and assign it this service.

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

**A general rule-of-thumb for choosing file and BDR backup service plans**

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

Here is a general rule-of-thumb that might be helpful as you choose the most cost-effective backup service plan for a particular situation. Use the *eFolder Backup for Files* service to backup up to 500 gigabytes of data. Use the *eFolder BDR for* *ShadowProctect* service and BDR for Acronis service to backup 500 gigabytes to 3 terabytes of data. Use the *eFolder BDR for AppAssure* service to backup 3 terabytes or more of data.

Thank you for watching this video. You should now be able to choose an appropriate security role and service plan for an account.