
Introduction

This video provides a brief overview of the Web Portal for new eFolder partners. It also explains how to create new accounts.

The Web Portal is a web site that was specially designed for eFolder partners. The Web Portal is where you will go to perform almost all of your partner tasks, such as creating, viewing, and managing accounts and brands; viewing backup status and logs; generating billing reports; creating problem tickets; accessing marketing collateral; viewing pricing; and displaying articles in the Knowledgebase.

In this tour, we'll show you how the Web Portal is organized and the functions it provides.

When you became an eFolder partner, an account and an associated brand were created for you by the eFolder support team. Every new account will have an associated username and password. These account credentials should have been given to you in your welcome email or directly by the support team. You will need these credentials to login to the Web Portal.

As a partner, you can access the Web Portal in one of three ways: from the eFolder web site at www.efolder.net, from <https://backup.securewebportal.net>, or from your branded Web Portal web site link that was created for you from the branding information you supplied when you became a partner. No matter how you get there, they all point to the same Web Portal.

The Web Portal is fully branded. Product names, logos, colors, and fonts can all be customized. The brand that is displayed on the web portal after a user logs in is determined by the brand associated with the account that has logged in.

Every backup account has a set of account login credentials, which can be used to login to the Web Portal. The security role assigned to that account determines the functions and scope that are available to the user in the Web Portal after logging in. If you want to allow your customers and end-users to login to the Web Portal, either point them to your branded portal web site link, or to the generically branded link at <https://backup.securewebportal.net>.

Note that after users log in, they will always see the branded Web Portal that is associated with their account, no matter where they logged in to the Web Portal. The link to your branded Web Portal was included in your partner welcome email and will be automatically included in the welcome email that is sent out to the email addresses you specify when you create new accounts.

Many partners, especially those who are managed service providers (or MSPs), do not provide account login credentials to end-users and do not tell their end users how to login to the Web Portal because they want to have complete control over their accounts.

As a partner, you can point *potential* customers to your branded Web Portal to sign up for free trials of the Backup service. Potential customers do *not* need to login to the Web Portal to sign up for a free trial and download and install the Backup Manager client software on their local computer. Simply have them use the **Free Trial** and **Download** menu options from the login screen of your branded Web Portal to sign up for a free trial and download the Backup Manager.

A Brief Review of Accounts

The Web Portal is all about creating, monitoring, and managing accounts—your own account and those you create for customers and end-users.

To understand the Web Portal functionality, you need to understand several concepts that are associated with accounts. For example, before you create a new account, you must decide if you want to create a new parent account or a sub-account. So before beginning our tour of the Web Portal, we will review some important concepts about accounts.

An account represents a billable eFolder *service* that is being used by a customer or end-user, such as file backup, email archiving, email security, or backup and disaster recovery (or BDR). Each account has one and only one associated service plan associated with the account. For example, for the Backup for Files service, an account could use the *Basic*, *Select*, or *Trial* service plan. For additional information on the service plans that are available for each eFolder service, please see the related video in this series entitled, *Choosing a security role and a service plan for an account*, or see the *Partner Provisioning Guide* found in the Partner Center.

Accounts are either parent accounts or sub-accounts. Sub-accounts always inherit the service plan of the parent account. Therefore, the first account you create for a new customer, which is a business or organization that has signed up with you, is always a parent account and is assigned a specific service plan.

For each customer, you will create one parent account for *each* of the service plans that the customer will be using. For example, if a particular customer will be using both the *Select* and *Basic* Backup for Files services as well as the eFolder BDR service, then you would create three parent accounts for this customer—one parent account for *Select* accounts, one parent account for *Basic* accounts, and one parent account for the *BDR service*.

After you have created one or more parent accounts for a customer, create a sub-account for each of the customer's end-users or devices that will be using eFolder services. Each sub-account is tied to one of the customer's parent accounts. Select as the parent account that has the same service plan that the sub-account should have. For example, if a new computer will be using the *Select* service plan for file-level backups, then create the account as a sub-account and choose as its parent the parent account for that customer that uses the *Select* plan.

In the case of file-level backups, accounts are always tied to one and only one machine—the machine to be backed up by that account. The same account cannot be used on two or more machines. For file-level backup services, you are billed for the total aggregate disk storage that your file backup accounts use in the eFolder cloud and *not* on how many file backup accounts you have as a partner. It doesn't matter from a billing perspective how many file backup accounts you set up. However, if you try to use the same account on two or more machines, the backup service will not work and can cause very serious issues. It is very important that each computer you are backing up with file-level backups is associated with its own account.

For other eFolder services, such as the one for backup and disaster recovery (or BDR) appliances, each service must have its own parent account. For example, each BDR that you buy from eFolder must have its own dedicated parent account that has the appropriate BDR service associated with it, such as the *ShadowProtect BDR service plan*.

To summarize these important concepts, as a partner, you will sign up new customers, each of which represents a business or organization, for one or more eFolder services under one of your brands. For each *customer*, you will create one new parent account for each type of service that this customer will use. Then, for the file backup service, you will create a new sub-account for each of the customer's machines you are backing up. Finally, parent accounts as well as sub-accounts must each be tied to a single machine for file backup purposes. As a partner, you are not billed for how many file backup accounts you have; rather, you are billed for the total amount of storage space that these accounts use in the eFolder cloud.

The reason that accounts are split into parent and sub-accounts is for ease of account management and for billing purposes. Many administrative functions in the Web Portal apply not only to an account, but also to all of its sub-accounts, making it easier to manage related groups of accounts. For example, if you set a quota on a parent account, that quota will apply to both the parent account and all of its sub-accounts.

On the billing side, as a partner, you determine what you want to charge your customers for each branded service that a customer is using. These rates differ across the different services the customer is using. The rate you charge for the *Basic Backup for Files* service will likely be different than the rate you charge for the *Select Backup for Files* backup service.

When you bill your customers, you need to know how much total data each customer is backing up under each service plan so you can bill your customers accordingly. As you will shortly see, the Web Portal provides predefined billing and usage reports that make billing a much easier task. These reports are broken out by customer and show for each parent account the combined usage for that account and all of its sub-accounts. Because each parent account represents one of your branded services, this makes billing a much easier task. PSA integration, raw data export, and API access are also available so that your billing can be fully automated.

Next, let's begin our tour of the Web Portal.

The Home Page

To login to the Web Portal, click **Login** if necessary to display the login fields and enter your account credentials in the appropriate fields. If you logged in using a temporary password, you will be prompted to create a permanent password. You have successfully logged in to the Web Portal when the home page appears and the corresponding main menu option changes from **Login** to **Logout**.

The Web Portal interface can be divided into four sections: the page header containing your branding information, the main menu bar, the *Quick-Search* bar, and the information display area for the current page.

Let's start by looking at the Home page.

The top of the Home page displays recent eFolder news, product announcements, and service notifications, if you logged in using an account that represents one of our channel partners, and if the account has a security role with privileges to manage the accounts in your partnership. Please follow us on Twitter and "like us" on Facebook to stay up to date with all partner news, announcements, and special promotions. Note that normal end-user accounts do not see eFolder-specific information intended only for our channel partners when they login. They only see your logo and your brand without mention of eFolder.

The Home page displays a welcome message containing the name of your branded Web Portal, the name of the account owner on this account, and the security role that was assigned to that person.

Security roles are used to determine the functionality that is available to the account holder and the scope of accounts on which they can act. Your partner account is given the *Partner Senior Manager* role, which allows you full control over all accounts associated with your brand, including the ability to create and delete accounts, reset an account's password, and "impersonate" an account. Impersonating an account gives you the ability to view an account on the Web Portal in the same way as if you had logged in as the account holder. When you impersonate an account, you have the same privileges in the Web Portal that the account holder has, and you will see the same menu options that they will see.

Accounts are assigned the *default* security role automatically at the time they are created, but you can change the role for an account after it has been created. For example, you could create individual accounts for each of your support engineers and afterwards assign the *Partner Senior Customer Service* role to those accounts so that your support engineers could create, manage, and delete customer accounts associated with your brand. Use the *Account Center* or the *Account List*, which we will discuss later, to change the role assigned to an account.

End-users with accounts assigned the default role can only access information associated with their own account and any sub-accounts that are associated with the account. They are limited to performing a restricted set of tasks on their account, such as changing their password or viewing backup reports. To learn more about security roles, see the related video in this series entitled, *Choosing a security role and a service plan for an account*.

The *Home* page displays a historical graph of how much cloud storage your own file backup account is using. This allows you to see cloud storage utilization trends for your own individual account over time. You can select the time interval that is displayed by clicking one of the options above the graph. Note that this graph does *not* show cloud storage utilization for all accounts in your brand; it only shows cloud storage utilization trends for your own individual account.

The *Getting Started* section of the *Home* page provides a summary of the steps for downloading and configuring the Backup Manager software on the machine to be backed up by this account. This section of the home page is more relevant to end-users that login and need guidance on how to configure their file-level backups. The Backup Manager software can be downloaded at any time by selecting *Download Software* from the **Support** menu option. Please refer to the related video in this series entitled, *Installing and Configuring the Backup Manager* for training on how to perform this task.

The *Account Summary* section of the *Home* page displays the account number, the user name, and the date of the last remote backup for this account. A remote backup occurs when data is securely backed up from the local machine to the remote storage cloud. The Backup Manager also has the additional option of providing local disk-to-disk data backups, but this is not reported here.

Finally, the information at the bottom of the *Home* page displays your cloud storage quota, or how much space this account is allowed to have in the eFolder cloud, and your total cloud storage utilization. "Inf" is an abbreviation for "infinite" and indicates that the account has no storage limitations in the cloud.

At the bottom of every page in the Web Portal is the support phone number and support email address associated with the brand for the currently logged in account.

The Account Summary section also has a couple of useful links. The first one, labeled *Manage*, displays the *Account Center* screen, where you can perform various tasks on the accounts you have created as a partner. You can also access the *Account Center* by selecting *Account Center (Visual View)* from the **Accounts** menu.

Clicking the *Create* link displays the *Create Account* page, where you can create a new account for a new customer or an account or sub-account for an existing customer. You can also display this page by selecting *Create Account* from the **Accounts** menu option, or by clicking the *Create Account* icon in the quick-launch task bar. Because this is a common task, the *Home* page provides multiple ways to quickly access this function.

Use the search box in the *Quick-Search bar* to find a specific account or accounts that match your search criteria, such as all accounts matching the name of a business or a specific email address. You can restrict your search by clicking the drop-down list and selecting the field to search on in the account list, such as *Company Name*, or you can search across all fields in the drop-down list by selecting *(Auto)*. The search box in the Quick-Search bar also allows field operators where you can specify that certain fields must have certain values, for example the search string "serviceplan:select and created > 2012-12-31" would match all accounts with the *Select* service plan that were created after December 31, 2012.

The *Quick-Search* bar also has clickable icons for returning to the *Home* page, adding a new account, and opening the Support Center, where you can create trouble tickets or access the Knowledgebase, which is a searchable collection of articles and help information. The Support Center can also be accessed by selecting *Support Center* from the **Support** menu option.

The menu bar at the top of the page is displayed across all of the pages in the Web Portal, with the exception of the Support Center, which launches a separate ticketing portal that has its own interface and its own set of login credentials.

Now that we have previewed what's on the Home page, let's overview the options that are available on the menu bar.

The first menu bar option is **Home**. Clicking **Home** always takes you back to the *Home* page, which we have just previewed.

The My Account Menu Option

Selecting **My Account** on the menu bar displays options for managing your *own* account—the one that you used to login to the Web Portal. Use this option to change your contact information, password, notifications, or to sign-up for eFolder mailing lists. As a partner, you will manage your own account as well as all of the accounts you have created for others. When modifying accounts, be sure you understand when you are taking action on your own account and when you are modifying one of the other accounts that you have created.

Use the *Notifications* option if you want to be notified when certain backup events occur on an account, such as when an account has not been backed up recently, when an account is using more than a certain amount of cloud storage, or when there is a sudden change in an account's cloud storage usage. These notifications apply only to *your* account—the one associated with your login credentials. However, if you check *Total Disk Usage Notification*, you can select whether you want this notification to be sent when *just this account* is using more than the specified usage, or when *this account and all of the sub-accounts that are under this account* have a combined usage that is greater than what you specify here. Another menu option we will look at shortly will allow you to determine how you want to handle the notifications for *other* accounts under your partnership.

Use the *Mailing Lists* option to subscribe to one or more eFolder mailing lists to be informed of company news, product updates, and maintenance notices. Some of the options on this page are particularly important to subscribe to and are labeled "important" in the option description.

Use the *Contact Information* option to change the contact information for your account, including your email address and your time zone.

Use the *Change Password* option to change the password for your account and to set the security questions that will be used when you forget your password and want to have it reset. Note that the password you are changing on this page is your account password—the one that you used to login to the Web Portal and the one you use when configuring the Backup Manager. This is different than your *pass phrase*, which is used to encrypt the data that is sent from a machine to the eFolder cloud during backups.

The My Partnership Menu Option

Selecting **My Partnership** on the menu bar displays options for managing your brand or brands, handling notifications which are generated across all of the accounts in your brand—not just your own account—and setting up integration of the Web Portal with a professional services automation (or PSA) system. Integrating with a PSA system enables notifications, billing, and other information to be automatically pushed to your PSA system.

Use the *My Brands* option to display a list of all of the brands that are associated with your partnership. Most partners have only a single brand, but some partners have more than one brand. For example, a partner who is selling backup services to different vertical markets might have one brand for accounting customers, one for medical customers, and so forth; or a partner who has subsidiaries might want those subsidiaries to manage their own brands while still maintaining higher-level oversight and management. If you think you might need to create multiple brands, please contact your eFolder Account Manager for further information.

If you do have multiple brands, you can sort the listing of your brands by clicking one of the three sort filters at the top of the second column. You can also use the *Quick Search* field to search for brands meeting your search criteria.

To edit information for a brand, such as the brand's support email address or support phone number, click the *pencil* icon to the left of the brand name. The Edit Brand screen displays, where editable fields are displayed with dark black field labels, and non-editable fields with light gray field labels. Notice that some of these fields define the customer service and technical support email addresses and the technical support phone number that is provided to end-user accounts when they need technical support. Partners are responsible for providing the first line of support to end-users and must keep this information accurate and up-to-date.

Use the *Partner Notifications* option on the **My Partnership** menu to setup what you want to do with the notifications that are triggered by *any* account associated with your brand and optionally with any sub-brands. This greatly simplifies the monitoring of your accounts. You only have to configure once how you want to be notified of certain information, warning, and error events that are generated by any account that you have control over.

It is important to understand that the *Partner Notifications* page does *not* specify *when* notifications or *which* notifications should be generated for your other accounts. Each account determines that for itself on the *My Account, Notifications* page. The Partner Notifications page only determines *what* to do with the notifications after they are generated by the individual accounts, such as send an email or create a trouble ticket in a professional services automation (or PSA) system. In other words, *when* and *which* notifications will be generated is determined at the account level. What to do with these notifications is determined by the partner in the *My Partnership, Partner Notifications* screen. Regardless of the settings on the *Partner Notifications* page, individual accounts can still generate email notifications for events that they generate – these individual account email notifications will be sent to the email address that is associated with that individual account. Some partners choose to allow their end-users to be notified in this fashion. Other partners choose to hide these notifications from their end-users completely.

Finally, use the *Integration Setup* option on the **My Partnership** menu to setup integration of the Web Portal with a professional services automation (or PSA) system so that notifications, billing, and other information will be automatically sent to that system. For detailed instructions on this task, refer to the detailed PSA integration guides that are located in the *Documentation* link of the Partner Center.

The Account Center Menu Option

Selecting **Accounts** on the menu bar displays an option for creating new accounts and a couple of options for viewing and managing your accounts—one that uses the Account Center and one that uses the Account List. Both of these options provide roughly the same functionality, but they provide different interfaces. The *Account Center* is an interactive, point-and-click, intuitive-type interface. The *Account List* provides a very detailed report-like interface with embedded commands and links. Some partners prefer one over the other or use one for some tasks and the other for other tasks. In general, the *Account Center* is easier to use, but requires a few additional clicks to view all of the account information. The *Account List* shows all of the relevant account information, but it can be overwhelming except for power users, and it requires some horizontal scrolling to see all the fields. We'll take a quick look at both of these interfaces.

Use the *Account Center (Visual View)* option to display the more intuitive, menu-driven account management interface.

The main area of the Account Center is the account list. Each line in the account list represents a different account. The individual fields for the account are displayed in the labeled columns that are shown horizontally across the page.

Which fields are displayed in the list is determined by the **View:** button on the *Account Center Quick Search* bar. Clicking **View:** and making a selection quickly changes the columns of information that are displayed. There are four groups of fields you can display in the list: *account details*, *contact information*, *resource usage*, and *account status*. If you click the **View:** button repeatedly, it will toggle across these four options. Because there are over 30 fields associated with each account, the **View:** button makes it easy to see related fields of information without having to scroll left or right across the screen.

The Account Center interface is largely menu driven. First, you select an account or accounts by clicking the checkbox in front of those accounts. You can also select or de-select all accounts by clicking the checkbox at the very top. Then you choose the action you want to take on those accounts by clicking **Action** and selecting an option. For example, to disable an account for non-payment, select the account in the list, select *Account Status* and then *Disable*. Alternately, you can right click on the account to show the *Action* menu and make the selection there. For most actions you can take, the action you select will apply to *all* of the accounts you have selected.

The account list also displays the current status of each account on the far left. Move the mouse cursor over these status icons to see a description of the status. The status icons are color-coded to give you a quick visual indication of the status of your accounts. A green status means the account is "good," meaning no warnings or errors have been detected. A yellow status means "warning" and applies to accounts that require human attention and are having minor issues. A red status means "error" and

applies to accounts that require human attention and are having important issues that need to be resolved. A gray status means the account never has had a remote backup.

The status icons may also appear in other resource-usage fields in the account list to indicate the status of a particular service. For example, these icons might indicate that remote backups are good, but local backups are failing. You can use these color-coded visual indicators to quickly see which services across your accounts are having trouble or are failing and which are okay.

Click the **Options** button on the menu bar to show or hide deleted accounts, to control how colors are used, to set the size of the text that is displayed, and to choose the overall color theme that you prefer for displaying accounts.

Click the **Account Details** icon to display or hide the *Account Details Information* panel, which provides additional detailed information for the account that is currently selected. You can also double click on any account to show or hide the account details information panel. This panel is divided into four tabs: account summary, service plan, contact information, and status details. Do not confuse this icon with the *View: Account Details* menu option. They are not the same.

Use the **Search Box** to search for and display only accounts that meet the criteria or filters you specify.

And finally, click the **New** icon to start the *New Account Wizard*, which is a more user-friendly way to create a new account than manually entering data on the *Create Account* page. We will walk through using the New Account Wizard next.

Please refer to the related video in this series entitled, *Using the Account Center in the Web Portal*, for more detailed explanations of these links and icons.

The New Account Wizard

There are two ways to create a new account: using the *New Account Wizard*, or entering the data directly on the *Create Account* page. We'll walk you through both ways in this video, but first we'll show you how to use the wizard. Later, we'll show you how to create an account using the *New Account* page. The wizard is typically the easiest, fastest, and most intuitive method for most users. To start the New Account Wizard, click the **New** button in the Account Center.

When creating new accounts, there are three possible scenarios. You can create a new account for a new customer, such as when you sign up a new customer for the very first time and create their first account. You can create a new sub-account for an existing customer, such as when an existing customer has new end users that need to back up their machines. And you can create a new parent account for an existing customer, such as adding a parent account for a BDR for a customer who currently only has the Select Backup service. We will walk through the wizard for each of these three scenarios. If you are unfamiliar with any of these concepts, please see the earlier section of this video entitled, *A Brief Review of Accounts*.

To create a new account *for a new customer*, start the wizard, select *New account for a new customer* and then select the brand that you want to use for this new customer from the drop-down list, if you have more than one brand. Then click **Next**.

The next page of the New Account Wizard displays account-information fields. Fields with a red border and an asterisk next to the field name are required fields. Hovering over any of the **information** icons displayed next to a field shows helpful information about that field. Enter the company name, contact information, and select the time zone that the customer is in. Then click **Next**.

On the next page of the wizard, select the service plan this new customer account will have. If you need help determining which service plan an account should have, please see the related video in this series entitled, *Choosing a security role and a service plan for an account*, or see the *Partner Provisioning Guide* in the Partner Center. If this is a trial account, enter that number of days for the trial. The default is 30 days but you can specify up to 60 days.

Then create the login credentials for the account. The user name is the login name that the account owner uses to log in to the Web Portal and perform certain tasks in the Backup Manager. It must be unique across all user names in service by eFolder.

Next, create a password by entering one into the *New Password* field or by generating a random password. Check the **Must Change Pwd:** box if you want the password to be a temporary password that the end-user must change when logging in to the Web Portal or Backup Manager for the first time. Note that all passwords are stored in the eFolder system in a salted, strongly hashed form; this ensures that eFolder does not have the ability to disclose the plain-text version of your password to anyone under any circumstance.

Next, enter a description for the account. The first description field is a more public description that the account holder will be able to see, such as "Store inventory computer." The internal description field is a description that the account holder will *not* be able to see, such as "Accounting back office, machine #5." Some partners use the internal description field to store a cross reference ID when they export raw from the eFolder Web Portal into their other systems.

You can setup a "hard" cloud storage quota for this account, which will halt any backups for this account when the quota is reached, but it is usually better to setup a "soft" quota by setting up an email notification that is triggered when the account exceeds a certain amount of cloud storage. Do this by impersonating the account *after* it is created, selecting *Notifications* from the **My Account** menu option, checking the *Total Disk Usage Notification* field, and entering your soft quota for the account there. In this way, backups will not fail when the account storage limit is reached; rather, an email alert will be sent out at that time and backups will continue as usual.

When specifying cloud storage quotas in these fields, the default unit is megabytes, but you can manually specify another unit; for example, you could enter "10 GB" or "1 TB" and it will recognize those units.

If a user wants to impose their own "hard" quota, they can, as long as it is less than the hard quota specified by the partner for the account. However, users seldom specify their own hard quota.

If you do not want to impose a predetermined storage limit on this account, select *Infinity* in the quota fields.

Check *Notify User via Email* if you want a welcome email to be sent to the account holder's email address—the one you entered on the previous screen. Temporary passwords will be included in the welcome email, but permanent passwords will not. Therefore, if you do not check this box, or if you did check this box but you did *not* check the *Must Change Pwd:* box, you will have to communicate the account password to the account holder yourself. Partners who are managed service providers typically

do *not* check this box because they will be handling the entire setup, configuration, and account management processes for their customers and end-users themselves.

When you are finished, click **Finish** to create the new account. The email address you entered for the account is validated along with some other things, and if everything checks out okay, a message is displayed that lets you know the new account has been created. Because you created a new account for a new customer, a new customer will be created by the system and assigned a customer ID at the same time the new account is created. In fact, creating a new parent account for a new customer is how you create a new customer on the system. Because this is the customer's first account, it will automatically be made a parent account and have the service plan that you assign. You can verify that the account was created by finding it in the account list the next time you search for it in that list.

Now let's use the New Account Wizard to create a new *sub-account* for an *existing customer*. After starting the wizard, select *New sub-account for an existing customer*. A list of parent accounts you have permission to see is displayed in the *Select Parent Account* field. If that list is lengthy, only a portion of the list is displayed at a time. You can page through the list using the page navigation controls at the bottom and use the scroll bar to scroll through each page of the list. You can also search for the parent account by entering search criteria in the *Search:* field, or you can enter filter criteria by clicking the **Filter** icon and entering filter information. When you have located the parent account, click on it to select it. Then click **Next**.

On the next page of the wizard, you can either use the same contact information for this sub-account as the parent account by selecting *Use existing customer record* in the *Contact Record* field, or you can create a new contact record for this account by selecting *Create a new contact record*. If you create a new contact record for this sub-account, enter the information for each field as previously described. Either way, click **Next** when you are ready to proceed.

On the next page of the wizard, the parent account ID for the parent account you previously selected is displayed by default in the *Parent Account ID:* field. Enter information into each of the fields on this page as previously described and click **Finish** to create the account.

Now let's use the New Account Wizard to create a new *parent* account for an *existing customer*. After starting the wizard, select *New parent account for an existing customer*. A list of existing customers that you have permission to see is displayed in the *Select Customer* field. Notice that entries with the same Customer ID number in the first column all belong to the same customer. To choose an existing customer, select any account that is associated with the desired customer. Use the search box, the scroll bar, and the page controls at the bottom to locate the customer for whom you want to create the new parent account. Click the customer to select it. Then, click **Next**.

The next two pages of the wizard are identical to those we have already seen. Enter the information and make your selections on those two pages and click **Finish** on the third page to create the new account.

This completes our overview of how to create a new account using the New Account Wizard.

The Account List Menu Option

Now let's return to the Web Portal main menu. Selecting *Account List (Detailed View)* from the **Accounts** menu option displays the account list in a more report-like format with embedded links and commands. This interface is laid out in five sections going down the page. You can navigate to a particular section by selecting the corresponding link at the top of the page or by scrolling down the page.

Use the *Search Criteria* section to specify which accounts you want to display.

The *Accounts Matching Search Criteria* section displays the results of the search you performed in the *Search Criteria* section. If you have not yet performed a search, by default the last search results are displayed. If no previous search has been conducted, then all accounts that you have permission to see are displayed.

As with the Account Center visual interface, each account is displayed on a separate line. However, this interface displays *all* of the fields associated with an account in the columns going across the page. Because there are more than 30 fields of information that are displayed, you will probably have to scroll left or right to see all of the fields.

The Account List (Detailed View) interface displays embedded links and icons in many of the fields in the account list. Icons let you display information related to that field, such as the last backup log for the *Last Backup* field. Embedded links let you take various actions on a field, such as set (or reset) the information in a field, disable an account, or change a subaccount to a parent account. Power users like the detailed Account List interface because it shows all of the core information for an account on one line along with embedded links and icons that display information or change the data in those fields.

Please refer to the related video in this series entitled, *Using the Account List in the Web Portal*, for more detailed explanations of these links and icons.

The *Summary Information* section contains a summary showing the total number of accounts that you have, your total disk usage before and after compression, your average disk usage, and the average compression ratio that was achieved. Note that this information pertains to *all* accounts that match the search criteria at the top of the page. If you want to display all of your accounts, click the **Clear Search** button.

Use the *Export Data* section in the Account List to export data for all accounts that match the current search criteria to CSV for Excel, CSV, or XML formats.

Use the *Account Operations* section to specify an account by its account number and take a specific action on that account. If you know the account number, this is a quick way to perform various actions on that account.

In summary, use the Account Center or the Account List to perform the majority of your account management tasks.

The Create Account Menu Option

Returning to the Web Portal main menu, selecting *Create Account* from the **Accounts** menu option is the second way to create a new account. The first way is to use the New Account Wizard, which we have already discussed.

Just as we did for the New Account Wizard, let's walk through each of the three possible scenarios for creating an account: Create a new account for a *new* customer, which will always be a parent account; create a new parent account for an *existing* customer; and create a new sub-account for an *existing* account. Again, if any of these terms are not familiar to you, please review the earlier section of this video entitled, *A Brief Review of Accounts*.

Also note that, in the following discussion, we will not repeat the detailed explanations of the fields that are displayed when creating a new account, since we have already explained those fields in the section of this video that discussed creating an account using the New Account Wizard.

Having said that, let's walk through the three scenarios. The first scenario is to create a new account for a new customer. To do this, in the *Customer Information* section of this page, select *new customer* in the *New Customer?* field. Next, if you have multiple brands, select the brand you want to use with this customer.

In the *Contact Information* section of this page, enter the contact information for this new customer in the appropriate fields, overwriting any default information that needs to be changed, and select the time zone to be used with this customer.

In the *Account Information* section of this page, select the service plan this account will have, select "(none)" as the referring partner, create the login credentials for the account, and enter information into the other fields on this page in the same way that you did when using the New Account Wizard.

When you are finished, click **Create Account**. The new account is created, and the *Operation Results* page is displayed with the account number and login credentials for the new account.

For our next scenario, to create a new parent account for an *existing* customer, choose *existing customer* from the *Create Account* page and then select the existing customer for whom you want to create the new account. The contact information that was previously created for this customer is displayed by default. If someone else will be responsible for this account, select *New Contact* in the *New Contact?* field and enter the new information. Otherwise, just keep the existing information as is.

In the Account Information section at the bottom, notice that the *Service Plan* field is replaced by the *Parent Account ID* field. Since this is a new *parent* account for an *existing* customer, select *(none)* in the *Parent Account ID* field and select the service plan you want this parent account to have in the *Service Plan* field. Enter information into the rest of the fields as previously described and click **Create Account** to create the new parent account for this existing customer.

For our third scenario, to create a new *sub-account* for an existing customer, select *Existing Customer* on the *Create Account* page and select the existing customer for whom you want to create the new

sub-account. Leave or change the contact information as previously explained. Then click the drop-down list in the *Parent Account ID* field and select the parent ID for this sub-account.

After you select the Parent ID for this new sub-account, notice that the *Service Plan* and *Referring Partner* fields are removed from the page. This is because sub-accounts always have the same service plan as their parent account.

Complete the rest of the fields as previously explained and click **Create Account**. A new sub-account is created under the parent account you selected.

The Reports Menu Option

Now that you know how to create new accounts, using either the New Account Wizard or the *New Account* page, let's review the rest of the options on the Web Portal main menu bar.

Selecting **Reports** on the menu bar displays the all-important Dash Panel as well as a number of other pre-defined reports.

Select *Dash Panel* from the **Reports** menu option to display the Dash Panel Report. This is the most important report that is available for partners in the Web Portal. You should view this report at least every day, because it visually summarizes the status of all of the services across all of your accounts. Use this report to make sure that all of your customers' backup, replication, BDR, and email archiving services are functioning as they should be and are error free.

The Dash Panel Report shows account status information at the time you loaded the page. Click the **Refresh** button to refresh the account status and other information in the Dash Panel Report at any time.

The Dash Panel Report is divided up into sections by brand. Within each section, the accounts for that brand are displayed line by line. The columns in the list display status and other account information, as indicated by the labels at the top of the columns.

You can sort the accounts listed in the dash panel by clicking the **Sort Order** drop-down list, selecting the desired field to sort on, and clicking **Refresh**.

The checkboxes at the top of the list further control how the account entries are displayed. Checking *Group by account status* displays the accounts by groups according to their current status. Accounts with a red status are grouped together; accounts with a blue status are grouped together; and so forth. A green status means the account is "good,"—no warnings or errors have been detected. A yellow status means "warning" and applies to accounts that require human attention and are having minor issues. A red status means "error" and applies to accounts that require human attention and are having important issues. Blue status means the account has been created but has not yet been used for backup or other services.

Checking *Use friendly dates* affects the *Last Backup* and *Last Successful* fields and displays how many days it has been since those backups occurred instead of actual calendar dates. This makes it easier to tell how long an account has gone without a backup.

Checking *Show detailed status* causes one or more additional lines of information to be displayed for an account, for those accounts that use certain services, such as eFolder BDR for AppAssure or eFolder BDR for ShadowProtect.

The Dash Panel Report, like the Account List, has links and icons that indicate status and display logs and reports. For example, you can view an account in the Account List by clicking the "V" link next to the user name, or you can impersonate an account by clicking the "/" link next to the user name.

Most partners use the Dash Panel Report to see which accounts are in a red or yellow status, read the problem descriptions for those accounts in the right-most column, and then diagnose the problems by clicking the embedded icons and links in the list to display reports, logs, and other information.

Moving on to the other options on the **Reports** menu, select the *Accounts* option to generate predefined reports of your accounts, such as all billable accounts, accounts that were recently created or deleted, trial accounts, trial accounts that recently expired or will soon expire, and accounts not recently backed up. The reports are displayed using the Account List interface.

Use the *Billing Reports* option on the **Reports** menu to display the *Billing Reports* page, where you can generate Excel spreadsheets that contain detailed resource usage information that can be used for billing purposes. You can also access historical billing reports that describe the billable services utilized for all of your past billing periods.

You can generate billing reports for just one brand, or generate a zip file containing billing reports for all of your brands, if you have more than one brand. You can also select the type of report you want to create: an *Invoice Report* that is suitable for on-screen viewing and printing, a *Raw Account Data Report* that contains total cumulative resource usage information on each parent account, or a *Raw Customer Data Report* that reports the same information by customer. For invoice reports, the accounts are grouped by service plan and by parent and sub-account.

Finally you can choose what period the report should cover. You can choose to generate a report showing resource utilization as of right now, or you can choose to download a report that is automatically generated on the first of each month, showing the resource utilization as it existed on the first of that month. The last month's report is useful because it contains the same information that eFolder uses to bill you, the partner, and it contains the information you can use to bill your end-users.

When the time comes to bill your customers, use the reports generated on the *Billing Reports* page to see the usage information you need to invoice your customers. Refer to the article, *How do I bill my customers?* in the Knowledgebase in the Support Center for more details.

The *Backup Sessions* option under the **Reports** menu displays a historical listing of all of your backups for all of the accounts in your brand. Every time an account backs up, it records the results of that backup session in a backup session record. This report is useful to view the history of backups for one or more accounts, see how much data was uploaded, and see how many errors were generated and what they were. Because this report displays the backup session records for *all* of the accounts in your brand, it can be quite lengthy and slow to load and is typically *not* displayed through this menu option. Instead, this report is typically displayed only for a single account by right clicking on an account in the Account Center, selecting *Reports*, and selecting *View Online Backup Session Report*, or, if you are in the Account List, by clicking the V/link next to the entry in the *Last Backup* column for that account.

The *Active Backup Sessions* option under the **Reports** menu displays only accounts that are currently backing up data at the moment the report was generated.

The *Event Log* option under the **Reports** menu displays a list of the notification events that have occurred across all of your accounts. Because the event list can be quite long, it may take a few seconds to display. By default, the latest events are shown at the top, but you can sort the list by clicking any of the column names displayed across at the top of the list. You can also search the list to find only events that match your search criteria.

Each notification event is either an okay event, a warning event, or an error event, as indicated by the status icons that are displayed in the first column. Again, most partners prefer to view the event log for a single account from the Account Center or Account List, using the techniques just described for the *Backup Sessions* report.

The *Audit Log* option under the **Reports** menu displays a list of the changes that were made to any of your accounts. You can search and sort this listing in the same way that you did in the *Event Log*. Again, most partners prefer to view the audit log for a single account from the Account Center or Account List.

Please refer to the related video in this series entitled, *Viewing Reports in the Web Portal*, or the online help documentation for additional information on any of the reports generated by the Web Portal.

The Support Menu Option

Moving on to the next Web Portal menu option, selecting **Support** on the menu bar displays options for downloading the Backup Manager software, recovering an encryption pass phrase, creating and viewing trouble tickets, accessing the latest news and announcements from eFolder, and viewing online guides.

Regarding the first option on this menu, any machine that will be using eFolder's file-level backup services will need to have the eFolder Backup Manager client installed onto them. The *Download Software* option is used to download the appropriate setup executable file for deployment onto each machine. For backup disaster recovery appliances, or BDRs, all of the required software already comes pre-installed on the BDR. Refer to the BDR documentation for installation instructions. If you are building your own BDR, you will need to download the Backup Manager onto the BDR machine you are building.

Use the *Pass Phrase Recovery* option on the **Support** menu to initiate the recovery of your file-level backup pass phrase. Your pass phrase is different from your account password and is used to encrypt the data that is backed up into eFolder's storage cloud. Recovering your pass phrase *only* works if you chose to store your pass phrase in eFolder's cloud and protect it with a set of security questions—actions that are performed from the Backup Manager software, usually when it is first installed and configured on the local machine. To initiate recovery of your pass phrase from the Web Portal you *must* use Internet Explorer with ActiveX enabled with <https://backup.securewebportal.net/> in the trusted sites list.

You can also initiate recovery of your pass phrase from the Backup Manager itself, which is how most partners perform this function. Due to browser security restrictions, this is usually the preferred and more convenient way to recover your pass phrase. For further details on pass phrases and how they are used to encrypt data, see the video *Installing and Configuring the Backup Manager*.

Use the *Support Center* option on the **Support** menu to create or view trouble tickets, access the Knowledgebase, or view recent news and announcements from eFolder. Because the Support Center uses a separate third-party system, your credentials in the Support Center are separate from the eFolder Web Portal, and clicking this option opens a new window with menu options to submit or view support tickets and view the Knowledgebase. When you are finished with any of these options, close the Support Center's browser window to return to the Web Portal.

Select *Software Guide* from the *Help* option under the **Support** menu to view the online user guide for the Backup Manager. Select *Web Portal Guide* to view the online user guide for the Web Portal.

The Web Access Menu Option

Selecting **Web Access** on the menu bar lets you download files that have been backed up to the eFolder cloud when you are away from the computer where the files were originally backed up. This function provides you the added convenience of being able to access any of the files you have backed up to the eFolder cloud, using either the Internet Explorer web browser or the downloadable client, from anywhere in the world.

For example, suppose you are traveling and suddenly realize that you forgot to bring a presentation file with you that is stored on your local machine back home, and you cannot access that machine remotely to retrieve the file. If that local machine has been using the eFolder Backup for Files service to backup those files to the eFolder Cloud, then no problem. Simply use the *Web Access* function to download the last backed up version of the file from the eFolder Cloud. Due to browser security restrictions, the downloadable client program is the fastest and easiest way to access your data no matter where you are in the world when you are away from your local machine.

Please note that the *Online Access* option requires Internet Explorer with ActiveX enabled. The *Downloadable Client* option downloads software that will not install anything on your computer but will allow you to easily access any files backed up to the eFolder cloud.

If you need to *restore* data onto the original machine that backed up the data, do not use the *Web Access* option. Instead, click **File Manager** on the *Control Panel* page of the Backup Manager software on the original machine and restore your files from there.

The Logout Menu Option

Finally, use the **Logout** menu option to logout of the Web Portal and return to the login screen. If you do not logout of the Web Portal, you will automatically be logged out after 90 minutes of inactivity. We recommend that you logout when you are finished using the web portal to avoid unauthorized use of your account.

Thank you for watching this video tour of the Web Portal. See the other instructional videos in this series for additional training on partner-related tasks. Please continue to the next video entitled, *Installing and Configuring the Backup Manager*.

Welcome to this overview of how the eFolder *Backup for Files* service works. This video will also show you how to restore files, should the need ever arise.

eFolder Backup for Files is a service that backs up files from a computer to the eFolder cloud. More specifically, eFolder Backup for Files is a business-grade, file-level cloud backup service that provides automated backups from Windows, Mac, or Linux workstations, laptops, and servers, as well as Network-Attached Storage devices (or NAS devices), to the eFolder storage cloud. It also optionally provides local disk-to-disk (or D2D) backups or site-to-site backups at no extra charge to cost-effectively replace traditional tape or D2D solutions.

For the more technically minded, we'll now briefly overview the technology and processes that eFolder uses to provide this service. eFolder Backup for Files has been designed to be a secure, reliable, efficient, scalable, modular, and portable data backup solution. All data that is backed up is locally encrypted before being sent to the cloud using an AES 256-bit encryption algorithm, approved by the National Security Agency for encrypting top secret data. The encrypted information is sent across an authenticated and secure (SSL/TLS) Internet connection to the eFolder cloud, where it is split into redundant pieces and guarded by silent data corruption protection technologies. eFolder's cloud infrastructure uses strong cryptographic checksums and other methods to guard the integrity of the data that it receives.

Data in the cloud is hosted in secure data centers with multiple perimeter security barriers, biometric scanning, key-card-protected access, continuous surveillance, fire mitigation systems, redundant power feeds from multiple grids, UPS systems, on-site generators, and 24/7 onsite guards.

eFolder also uses additional technology that adds an additional layer of redundancy above and beyond normal data redundancy measures to offer additional protection against silent data corruption, which is the non-malicious alteration or loss of data introduced by a computing system without the error being logged. Silent data corruption can be introduced by physical failures, corrupted or buggy firmware, misdirected writes, driver bugs, filesystem bugs, and human error. eFolder uses algorithms for automatically detecting and repairing silent data corruption, including techniques such as strong block checksums, data pipeline integration checks, and encryption cipher modes that do not magnify the impact of single-bit errors.

Now let's return to a more general overview of eFolder Backup for Files. eFolder Backup for Files delivers the features managed service providers (or MSPs) require for a true business-class and fully managed offering, including military grade security and data privacy; unsurpassed reliability and data

integrity; additional on-site and cross-site backups for fast restores; tools for centralized service provisioning, reporting, billing, monitoring, and management; automated billing, ticketing, and reporting through integration to a professional services automation (or PSA) system, such as ConnectWise; audit trails, event logs, and disk usage reports; and the ability to backup data using Microsoft VSS, including the ability to backup Exchange and SQL servers.

eFolder partners re-sell the eFolder Backup for Files service under their own brand, meaning their own logo and marketing image. eFolder creates the partner's brand using the branding information provided at the time the partner signs up to sell the service. Customers and their end-users see only the partner's brand on all backup-related software and web sites. Partners can charge their customers whatever they want for their own branded backup service. eFolder charges partners only for the amount of storage they use in the cloud.

eFolder Backup for Files offers your customers peace of mind. Customers can sleep at night knowing their data is safe from local hardware failures, local or regional natural disasters, and other similar events that could threaten their most prized business possession—their business's data. The bottom line is this: a business's buildings and hardware can be replaced, but its data cannot—unless, that is, that business is using eFolder Backup for Files!

What Backup Requires

As a partner, you will need four things to use and manage the Backup service: an Internet service connection, an eFolder account, the Backup Manager software client which has been installed and configured on the machine to be backed up, and access to the Web Portal, which is a web site that eFolder provides to partners to monitor backup activity and create and manage accounts. A link to your branded Web Portal was given to you in your new-partner welcome email.

The first thing you will need to use eFolder Backup for Files is an Internet service connection. The more bandwidth and speed your Internet connection has, the faster your data will be backed up to the cloud. eFolder does not restrict data transfer speeds up to or down from the cloud, allowing you to restore or backup data as fast as your Internet connection will allow. However, you can choose to throttle back the bandwidth that the Backup service uses during certain critical periods, such as during business hours when that bandwidth is needed to run the business, by configuring the appropriate settings in the Backup Manager.

The second thing you will need to use eFolder Backup for Files is an eFolder account. Accounts are fundamental in all of eFolder's services. An account represents an eFolder service that is being used by a customer. Your first account, which is your partner account, is setup for you by eFolder at the time you become a partner. Subsequent accounts are created by you in the Web Portal when you sign up new customers and end-users. An account is what authorizes the Backup service to be implemented. It contains the information eFolder needs to provision the service, such as contact information, login credentials, the specific type of service the customer or end-user will be using, the brand and company associated with the account, and so forth.

An account is associated with one and only one service. If a customer will be using multiple services, such as Backup for Files and Email Security, they must have an account for each service. For the Backup for Files service, each and every machine that you want to backup will need to have its own eFolder

account, separate from any other machine. For the eFolder Backup for Files service, you are not charged based on the number of accounts you create—only for the total storage space that all of your backups across all of your accounts occupy in the cloud. You can create new accounts any time you desire for your customers and end-users. This puts *you* in charge of creating and managing your own accounts. eFolder created the Web Portal so that you can create, monitor, and manage your accounts.

Every account is assigned a security role, which determines the scope and functions that are available to the user of the account in the Web Portal. The account that eFolder created for you when you became a partner is given an unrestricted role that allows you to create and manage accounts on the Web Portal, display billing and usage reports, access technical support, and view documentation and training. When you create accounts for your customers and end-users, they are automatically given the default security role, which has the fewest privileges. After you have created an account, you can go into the Web Portal and change the security role assigned to the account. For example, you may want to assign your technical support staff a role that allows them to view and change account information for your brand. Security roles allow you to maintain control over your accounts and restrict access that users have to certain information and functions. For more information on accounts and security roles, please see the related video in this series entitled, *Overview of accounts, brands, customers, and roles*.

The next thing you must do to use the Backup for Files service is install and configure the Backup Manager client on every machine to be backed up. The Backup Manager client can be downloaded from the login page of your branded Web Portal. Note that you do not have to login to the Web Portal to download the client. Normally, you download the client from the machine to be backed up, but if you are a managed service provider and you want to download the Backup Manager to a large number of machines all at once (for example, through your RMM tool), then follow the procedure given in the automatic deployment and configuration guide that is available in the Partner Center, or contact technical support.

The Backup Manager is responsible for managing the backup configuration, as well as performing the actual backups. During a backup, it will establish a communications link to the eFolder cloud, confirm that you are authorized to use the Backup service using the configured account credentials, scan and identify all changed data blocks within your configured backup data set, compress and encrypt these data blocks locally, and securely transmit these data blocks to the cloud.

Use the Backup Manager to select the files and folders you want to backup. You determine what files and folders you want to backup either visually or by configuring policy rules. You can set different retention policies on a per-folder, per-file, or per-file-pattern basis. You have complete control and flexibility over what data is backed up. In addition, it does not matter if the file or folder to be backed up is located on your local computer or somewhere else on your network.

Besides selecting directories and files to backup, use the Backup Manager to:

- schedule your automated backups,
- indicate how you want to be notified when backups start and finish,
- set how many historical versions of backups you want to maintain in the cloud,
- create your pass phrase, which is a key that the Backup Manager uses to encrypt the data before it is sent to the cloud,
- monitor backups for this machine in real time,
- restore data from the cloud if the need arises, and
- perform other tasks, such as viewing backup reports.

The Backup Manager also offers another unique benefit—the ability to recover your pass phrase, which is used to encrypt your data. If you choose, you can store your pass phrase in a doubly encrypted form in the cloud and then recover your pass phrase at a later date if necessary, such as after a major disaster that destroyed your local machine, by answering a set of challenge questions that you previously created. When the pass phrase is recovered, only the account holder or authorized proxy has the ability to view the recovered pass phrase. Not even the service engineers in the data centers can view your pass phrase.

Installing and configuring the Backup manager is normally only performed once, but you can adjust or refine the configuration settings at any time by clicking the Backup Manager icon on your desktop and making the changes. Although you can change your account login and password at any time, we do not recommend that you change your *pass phrase*. Pass phrases are used to encrypt and unencrypt your data. If you change your pass phrase, previously backed up data will remain encrypted with the pass phrase that was used previously. This can result in a situation where you need both the old pass phrase and new pass phrase to access your data. In this situation, if you do want to change your pass phrase, we recommend deleting your old account completely and starting from a brand new account.

After you have installed and configured the Backup Manager, you do *not* need to start or open it for scheduled backups to occur. Backups will occur automatically according to the schedule and settings you have selected, whether the Backup Manager is open or not. In addition to your scheduled backups, you can also manually start a backup at any time by clicking the **Backup Now** button in the Backup Manager.

The fourth thing that is required to use the eFolder Backup for Files service is access to the Web Portal. The Web Portal is the administrative web site which you will visit daily or more regularly to monitor and manage all of your accounts and eFolder services. Use the Web Portal to:

- create new accounts,
- monitor the status of your accounts,
- change account settings, such as disabling an account for non-payment or increasing the disk quota for an account,
- view the Dash Panel, which provides a real-time snapshot of the status of all your accounts,
- view or export billing information,
- display backup logs and reports,
- access the Support Center to open a ticket with our U.S.-based technical support team

You can access the Web Portal in one of three ways: from the eFolder web site at www.efolder.net, from <https://backup.securewebportal.net>, or from your branded Web Portal web site link that was created for you when you became an eFolder partner. No matter how you get there, they all point to the same Web Portal. After navigating to one of these locations, if you do not see the login dialog box, click **Login** on the menu bar at the top of the page. Then enter your account username and password that was given to you when you became a partner. For more information on the Web Portal, please see the related video in this series entitled, *Overview of the Web Portal*.

How Backup works

After you install and configure the Backup Manager, you are ready to perform your first initial backup. If you have a large amount of data—say, more than 50 GB—we recommend that you use a preload to do your initial backup. This involves using the Backup Manager to encrypt and backup your data the very first time to a locally connected external USB drive or bare SATA drive. You then send the drive to the data center, where our service engineers load the data into your cloud backup account and take your account out of maintenance mode so your normally scheduled backups can continue. No other backups for this account should occur during this period. Contact technical support or consult our Knowledgebase for instructions on how to perform a preload.

If you have less than 50 GB of data to backup or have adequate bandwidth to upload your data in a reasonable time, click the **Backup Now** button in the Backup Manager to start the initial backup of your data to the cloud. The Backup Manager encrypts and compresses the data and then transfers a copy to the storage cloud. The Backup Manager is designed to be robust to common temporary failure conditions, such as low operating system resources or network disconnects, and will automatically resume the backup where it left off when the system and network connection are back online. You can also manually interrupt and resume backups from within the Backup Manager.

The initial backup will likely take much longer than any of your subsequent backups. After your initial data is loaded into the cloud, either over the Internet or through the preload procedure, only the deltas or changes to your data are backed up, which are typically much smaller in size, resulting in significantly shorter backup sessions and more efficient storage of historical versions in the cloud. These subsequent backups are called *incremental* or *historical versions*. They only upload the changes you made to your data since the last backup session.

Regarding your initial backup, your initial backup becomes the *current version* in the cloud, meaning the version which contains the most recent, updated files backed up from the local machine. The current version in the cloud contains a complete version of each file, ready to be restored at any time. The current version in the cloud is updated each time an incremental backup is received containing the changes to the local machine's files. In other words, the cloud uses the incremental backups to keep the current version in the cloud current. The current version in the cloud contains the complete and most current version of each file that is on the backup list.

For example, suppose as a new user of the Backup service, you performed an initial backup that included a PowerPoint file with 20 slides. After the initial backup, the *current* version of this file in the cloud also has 20 slides and is identical to the file on the local machine, except it has been compressed and encrypted. Suppose further that you add 5 more slides to the file before the next backup session. When the next backup session occurs, only the delta or incremental changes are sent to the cloud—not the entire file. In other words, only the data blocks on the local disk that contain the 5 additional slides are uploaded to the cloud. After this incremental backup has been successfully received and processed by the server in the cloud, the current version of the file is automatically updated with these changes, and will now have 25 slides. This is how the Backup for Files service maintains a current version of your backed-up files in the cloud.

The incremental or historical versions of changes to your files are *not* simply discarded after they have been used to update the current version in the cloud. If that were true, then you could never restore an older version of the file you backed up, say, one that was backed up a month ago. Only the latest version of the file would be available. Instead, the incremental changes are used to form a reverse chain of deltas that describe how to go backwards from the current version of the file to an older version of the file. This reverse chain design allows for arbitrarily long data retention policies that can be enforced efficiently.

Why would you want to restore an older version of the file? You might discover that a file has become corrupted, so you need to restore an older, non-corrupted version. You might inadvertently delete a file without realizing it until sometime later. Or you might discover that your computer became infected with a virus about a week ago. Keeping historical or incremental versions of files in the cloud is what enables you to restore previous versions of files. We'll explain how this works shortly.

But first, consider the following scenario. Suppose you created a document a month ago to track the weekly sales of one of your products, and you have scheduled backups to occur once a day on weekdays. You update this document every Friday afternoon with your weekly sales totals. In this scenario, the cloud now has the current version of the document—meaning the complete version of the file that has incorporated all of the changes to date—and three historical versions containing only the changes that were made each week.

Why are there only three historical versions? Remember that if no changes are made to a file, no new historical versions of the file are created, so even though daily backups have been occurring, a new historical version of the file was created only once a week after you made your weekly changes to the file.

Suppose now that you want to restore the original version of the file you created and backed up a month ago. Because the incremental, historical versions of the file were saved in the cloud, the original four-week-old version of the file can be recreated by taking the current version of the file and backing out the changes that were made from the past three weeks to this file. As long as there are historical versions of the file in the cloud going back to the point in time at which you want to perform the restore, the older version of the file *can* be restored. This reverse-delta strategy all takes place behind the scenes. When you choose to restore a particular version of a file, no additional steps are required. The system simply appears to download the correct version of the file.

You choose how much historical information you want to keep by configuring the Backup Manager. First, you decide whether to limit the number of historical versions at all. For example, a Backup account that uses the Select service plan can store an unlimited number of historical versions in the cloud. Keep in mind, though, that the storage space an account occupies in the cloud increases as you increase the number of historical versions that are stored there. The net result is an increase in your storage costs. This is why many partners limit the number of historical versions of files that an account can store in the cloud.

There are two ways to limit the number of historical versions that are stored in the cloud. The first way is to enter the maximum number of versions you want to keep. For example, enter 10 if you want the current version and the last 9 historical versions to be kept in the cloud. Historical versions beyond that number will be discarded.

The second, more intuitive and recommended way, is to limit the number of days of historical versions you want to keep. This method is preferred if your company is required to keep backups for a certain period of time for compliance reasons before they can be deleted. For example, enter 365 days if you want to be able to restore any historical version of a file that was backed up within the past year. In this example, historical versions older than a year will not be kept.

If you specify *both* a maximum number of versions and a retention period, then whichever limit is reached first is used. The more restrictive value takes precedence. Versions beyond the first limit reached will no longer be retained in the cloud.

Another useful feature that is offered by eFolder Backup for Files is the ability to restore files you have *deleted* on your local machine. For example, suppose you inadvertently deleted a file on your local machine so that it is no longer being backed up. When the server in the cloud sees that a file you had previously backed up is no longer being backed up, it marks the file as deleted and then stores the deleted file in a special area for the length of time you specified when you configured the Backup Manager for this account. You can then restore the deleted file if the retention period has not been exceeded.

eFolder Backup for Files also provides the ability to access the individual files you have backed up to the cloud from anywhere in the world at any time using the Web Portal and a browser. This feature is useful when you need to access a file when you are away from the local machine, such as when you are traveling and realize you forgot to bring a file with you. For more information on this feature, see the related video in this series entitled, *Overview of the Web Portal*.

Finally, eFolder Backup for Files provides an easy way for you to manually delete data from the cloud using an Explorer-type interface in the Backup Manager when you determine that the data is no longer needed. This is one way to clean up data that is no longer needed in the cloud and save storage costs. When you manually destroy data, the data is moved to a parallel repository where it is held for up to an additional 7 days at no cost to you, in case the destruction of data was unintentional. This is an additional safeguard against data loss.

How restore works

Knowing how data is backed up is only half the equation. Should you ever need to restore the files you have backed up, launch the eFolder Backup Manager, click the **File Manager** button on the **Control Panel** page, enter your account login credentials, click **Next**, and then click **Restore Data** to start the Restore Wizard. This easy-to-use but powerful wizard allows you to point and click on the files or directories you want to restore using an Explorer-style interface. You can restore the current version of your data, or you can perform a point-in-time restore by selecting a specific date. A point-in-time restore will automatically select the appropriate historical versions of a file that are needed to recreate the data as it existed at a particular date and time. You can restore files to their original locations or to an alternate location that you select.

If you configured the Backup Manager to backup data locally as well as to the cloud, you can restore data either from your local backups or from the cloud. As mentioned previously, there is no additional charge for backing up your data locally in addition to backing up data to the cloud, within certain limitations. The main advantage of locally backed up data is the ultra-fast speed at which data can be restored. The disadvantage is that a local disaster can wipe out this backup repository. eFolder Backup for Files offers you the benefits of both worlds at no additional charge—backup data locally for minor emergencies, and backup data to the cloud for real disasters.

However, even when you restore data from the cloud, eFolder minimizes your restore time by opening up to 15 parallel network connections to our cloud and downloading your data in parallel. This allows you to fully utilize all available download bandwidth, even on high latency network links.

The Backup Manager on your local system is used to restore your data. So what can you do if your local system has completely crashed and cannot be repaired, or what if a local disaster such as a tornado, earthquake, or flood has destroyed your system? Simply install the Backup Manager on a new system, open it, click **Help** in the menu bar, search on the phrase "Restoring after a system crash," and follow the instructions presented in the help document. Because you have previously loaded configuration data into the cloud for this account, you must follow a slightly different procedure to re-configure the Backup Manager. Do *not* use the procedure for configuring the Backup Manager for the very first time.

Thank you for watching this video overview of eFolder Backup for Files. Please continue with the next video in this series entitled, *Overview of the Web Portal*.

Questions

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



The People Behind Your Cloud