# Using the Account List in the Web Portal

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

**Introduction**

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

In this video tutorial, we will show you how to use the Account List in the eFolder Web Portal. This is an advanced training video that covers the Account List in detail. Before watching this video, you should have viewed the related video in this series entitled, *Overview of the Web Portal*.

As you recall from the overview video, the Web Portal provides two alternative interfaces for viewing and managing your accounts—the Account Center and the Account List. Both of these options provide roughly the same functionality, but they have different user 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. This video will show you how to use the more detailed Account *List* interface.

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

**A quick overview of the Account List page**

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

Access the Account List by opening the Web Portal and selecting *Account List (Detailed View)* in the **Accounts** menu option.

The Account List 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.

The *Search Criteria* section is where you enter search parameters to display the accounts you want to view or manage.

The *Accounts Matching Search Criteria* section displays the results of the search you performed in the *Search Criteria* section. This is where you will perform most of your account management tasks.

The list of accounts is presented in tabular format, with each account listed on a separate row. The columns of the table display the fields that are associated with the account, with the field names at the top. Because there are more than 30 fields of information, you may need to use the horizontal scroll bar to see all of the fields.

The individual cells in the table contain the current field values along with links and icons that allow you to display information, such as logs and status reports, and perform management functions, such as changing the setting for a field. Clickable links are always displayed in square brackets in the Account List. Power users prefer the detailed Account List interface because it displays nearly all of the information for an account on one line and because it includes embedded links and icons for viewing logs and performing management tasks.

The *Summary Information* section displays summary information for the list of accounts that were found by your search, less any deleted accounts, if you checked the **Hide deleted rows** checkbox in the **Quick Search** or **Advanced Search** panels above. Note that this information is a summary of the accounts that were found by the search, which is not necessarily all of your accounts in your partnership, so different searches will result in different summary information. The Summary Information section displays the total number of accounts, your total disk usage before and after compression, your average disk usage, and the average compression ratio that was achieved.

Use the *Export Data* section in the Account List to export the currently displayed target list of accounts to CSV, CSV for Excel, or XML formats.

Use the *Account Operations* section to perform a specific action on a specific account. This is a quick way to take action on an account when you know the account number. Even if you do not know the account number, clicking many of the embedded *Set* links labeled “S” in the Account List will cause this section to be prefilled with the appropriate account number and action so all you have to do is select the new field value. For example, clicking the *Set* link in the *Role* column enters the account number in the *Account Number* field and preselects *Set Security Role* in the *Action* field so all you have to do is select the new security role in the drop-down menu and click **Go**.

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

**The Search Criteria section**

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

Let’s take a closer look at a couple of the sections in the Account List, starting with the Search Criteria Section.

Use the Search Criteria section to search for accounts you want to display or manage. For example, you can search for all accounts belonging to a specific customer or brand so that you can view and manage those accounts. This section is particularly helpful to partners who have dozens or hundreds of customers and end-users.

You can search for accounts to display in the Account List in one of three ways. The first way is to use the *Account Quick Search* box immediately under the main menu bar at the top of the screen. This is a quick way to search for one or more accounts by account number, user name, company name, first or last name, or email address. You can also select *Auto* in the drop-down menu to narrow the search to specific fields.

For example, to search for an account with a user name of “HighlandHeights,” enter that name in the search field, select *User Name* in the drop-down menu, and click **Search**. The desired account is displayed in the Account List. The *Account Quick Search* box is available on almost every page in the Web Portal. Using it always displays the *Account List (Detail View)* page.

The second way to perform a search is to click the **Quick Search** tab in the Search Criteria section. This is useful for performing searches on the wider variety of the fields than were available with the *Account Quick Search* box. These searchable fields are displayed in the scrollable drop-down menu to the right, such as brand name, account number, or service plan name.

To demonstrate using the Quick Search function, let’s display all accounts by their Last Backup Date and then sort the list by the *Last Backup* column. To do this, leave the *Quick Search* field blank, select *Last Backup Date* in the drop-down menu, and click **Search**. All accounts that have backed up at least one time are displayed. Click the **Last Backup** header once to sort the list top-down by the most recent backups or twice to sort from the oldest backups first.

The third way to perform a search is to click the **Advanced Search** tab, which allows you to perform more advanced searches using one or more search or filter segments. Each line in the **Advanced Search** display allows you to define one segment of the search criteria. Each line or segment is then connected to the next line with an “and” or an “or” operator.

Let’s look at an example. Suppose you want to search for all ShadowProtect BDR and AppAssure CORE accounts that are associated with the DOC brand. In the first line, select *Service Plan Name* in the drop-down menu, select *CONTAINS* in the next drop-down menu, enter “ShadowProtect BDR” in the search field and select *OR* in the drop-down menu on the right. In the second line, do the same thing, except enter “AppAssure CORE” in the search field and select AND in the drop-down menu on the right. In the third line, select *Brand Name* in the drop-down menu, *CONTAINS* in the next drop-down menu, and enter “DOC*”* in the search parameter field.

Next, use the parenthesis in the drop-down menus on the left and right sides to group multiple lines together as one search or filter segment that you can combine with other segments. For our example, let’s group the first two lines together into one segment by selecting a left parenthesis in line one and a right parenthesis in line two. This ensures that the *AND* operator in line two applies to the net result of the first two lines, which are connected with the *OR* operator. This advanced search configuration will search for accounts that have *either* of the two service plans, as indicated by the OR operator, and that have the DOC brand, as indicated by the AND operator. Finally, click **Search** to perform the search and display the matching list of accounts.

Because your ability to quickly find the accounts you want to manage is so important, let’s take a moment to explain some of the operators that are found in the operator drop-down menu. The *CONTAINS* operator is used to search *text* fields for a particular phrase. For example, to search for all accounts that have the word “partner” in the *security role* field, select *Role Name* in the field name drop-down menu, select *CONTAINS* in the operator drop-down menu, type “partner” in the search field, and click **Search**. All accounts having the phrase “partner” in their security role are displayed in the account list.

In performing searches, spaces are treated as part of the string, so you can type “partner senior manager,” including the spaces, to search for that specific role. In searching text fields, the case of the text in both the search string and the target field is ignored.

Note that, for text searches using any of the three methods we have just described, you can use the wildcard characters “\*” and “?” in your search strings. An “\*” takes the place of one or more characters in the string and a “?” takes the place of a single character. For example, to search for all AppAssure accounts, regardless of whether they were *AppAssure CORE, AppAssure Partner*, or Trial (*AppAssure)* accounts, select *Service Plan Name* in the field drop-down menu, select *LIKE* in the operator drop-down menu, type *\*AppAssure\** in the search field, and click **Search**. All AppAssure accounts, regardless of the type of AppAssure service plan type, are displayed in the account list.

To search for all accounts except for AppAssure accounts, simply change the operator from *LIKE* to *NOT LIKE* and click **Search**. All accounts *except* AppAssure accounts are displayed.

The *=, <*, and *>* operators are only used on numeric fields. The *<* and *>* symbols can be combined with the *=* symbol to indicate less-than-or-equal-to and greater-than-or-equal-to operations. For example, the less-than symbol followed by the equal symbol (“<=”) means “less than or equal to.”

The IS NULL and IS NOT NULL operators are only used on date fields. IS NULL means “there is no value in the date field” and IS NOT NULL means “there is a value in the date field.” For example, to see all accounts which have an expiration date, select *Expiration Date* in the first drop-down menu, select *IS NOT NULL* in the second drop-down menu, and click **Search**. All of the accounts with an expiration date are displayed in the Account List.

The IN and NOT IN operators are only used on ID fields where you enter a series of values. For example, on the Advanced Search, select *ID: Internal Account ID* in the field drop-down menu, select *IN* in the operator drop-down menu, enter the ID number of the desired accounts, separated by a comma (such as 26447, 38127, 38823), and click **Search**. On the other hand, to search for all accounts except for 26447, 38127, 38823, change IN to NOT IN and click **Search**.

If your advanced search requires more search lines than the six that are displayed by default, you can add additional search lines by entering a larger number in the *Show search fields* box. For example, entering “8” and pressing the **Enter** key will increase the number of search lines to eight. However, because pressing **Enter** does the same thing as clicking the **Search *button***, you may need to click the **Advanced Search** tab again to see the increased number of lines.

Whether you use the **Quick Search** tab or the **Advanced Search** tab, you can exclude *deleted* accounts from appearing in your search results by checking the **Hide deleted accounts** checkbox. Deleted accounts are accounts that are no longer in service, but they are never removed from your account list for audit trail purposes and in case you later want to re-activate the account. We recommend you keep this checkbox checked unless you are trying to reactivate a deleted account.

Finally, clicking the **Clear Search** button in the Quick Search panel or the **Clear Search Fields** button in the Advanced Search panel will reset all search fields to their default values and display *all* of the accounts in your partnership in the account list, except deleted accounts if you checked the **Hide deleted accounts** checkbox.

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

**Overview of the Accounts Matching Search Criteria section**

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

The Overview of the Accounts Matching Search Criteria section of the Account List page displays a list of accounts matching your search criteria. This is where you will perform most of your account management tasks. As mentioned in the overview, each row in the table represents an account, and each column represents a field, as identified in the column header. You may have to scroll horizontally to see all of the columns. Each cell in the table shows the current value for that field along with any embedded account management links and icons that your security role is authorized to perform.

Note that partners are given a security role that allows them unrestricted access to all of their accounts and partner management functions. The fields, links, and icons that are displayed for other users depend on the security role to which those users have been assigned.

When you enter the Account List page from the main menu, the results of the last search you performed are displayed in the list of accounts. If no previous search has ever been conducted, then all accounts that you have permission to see are displayed. Otherwise, the list displays the matching accounts for the search you just performed.

By default, the entries in the Account List are sorted by the parent ID field, labeled “PID,” which groups sub-accounts under their parent account. However, you can sort the account list on any of the fields by clicking the field name in the column header. For example, to sort the list by user name in ascending order, click **User Name** at the top of the seventh column. To sort the list in descending order, click **User Name** again.

If the list of accounts is long, you can control how many accounts are displayed at a time and which account to start the display with by using the two fields at the top of this section. For example, to display six accounts at a time starting with the third account, enter “6” in the *Show* field, “3” in the *rows starting at row # field*, and click the **Refresh button to the right**. The account list then displays up to six accounts at a time, beginning with the third account.

Use the **Prev Page** and **Next Page** buttons, if displayed, to navigate vertically through the list of accounts. You can see which rows are currently displayed and the total number of rows in the search results list by reviewing the information displayed immediately above the list. Note that the Refresh button to the right of the title Accounts Matching Search Criteria will refresh the screen with the same results from the last time that you pressed the **Refresh**, **Prev Page** or **Next Page** button and may reset any changes that you made to the values in the *Show* or *row #* field.

The Account List displays every other row in the list with a light gray background to help your eye stay on the same row as you scroll back and forth horizontally. You can also specify which accounts you want to highlight in the list with a light red background by clicking the drop-down arrow in the *Highlight* field and making a selection. Selecting *No backup within interval* highlights accounts that have *not* had a backup within the first interval shown in the *NoBk Days* column. For this account, the first number is 3, so selecting this option would highlight accounts that have not had a backup within the last 3 days.

Selecting *No backup within interval and no alert* on the drop-down menu highlights accounts that have *not* had a backup within the same interval *and* have not yet been alerted.

Finally, selecting *Never backed up* highlights all accounts that have never been backed up.

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

**Columns 1 through 5 in the Account List**

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

Let’s discuss each of the columns in the search results list. The first column on the far left is used to delete or reactivate an account. Active accounts display an “[X]” in this column. To delete an active account, click **X**;then click **OK** in the confirmation window. Whenever you take any action in the Account List, a message will be displayed at the top of the page that lets you know the result of your action. Actions can be successful, or they can fail, for example, if you supplied the wrong input, or if the input is not in the correct format.

In this example, the message confirms that the account has been deleted. If you have checked the **Hide deleted rows** checkbox in the Search Criteria section, the account no longer appears in the account list. If you did not check this checkbox, the deleted account appears on a darker gray background with an “[R]” link in the delete column.

To restore (or undelete) the account after it has been deleted, click **R** in the first column. The account is restored to active status and an “[X]” appears in the first column for the account. The values in the fields of a restored account are a "snap-shot" of the account as it was when the account was deleted, so this information could very well be outdated. However, after the next backup of a reactivated account has been completed, all subsequent fields that can be in the Account List will be updated with current information. To force an update of this information sooner, click the **Test Connection** button on the **My Account** panel in the Backup Manager on the machine that is being backed up. After reactivating an account, you will also need to update any account contact information that might have changed.

Deleting an account does two things: it stops future backups for the account, and it stops billing for that account. However, the data for the account remains in the cloud for 14 days. On day 15, the data is purged, but the account itself is *never* removed from the account list and remains there as a deleted account. This provides a history and an audit trail for the account.

To reactivate an account after 14 days, restore the account and then re-seed it with a new image. Alternately, create a new account for the user instead of restoring the old account, but this requires that you enter all of the account information again.

The next column, labeled *ID*, is an internal-to-the-system account identification number that is automatically generated by the software when a new account is created. No two accounts are given the same ID. The ID is a reference number that is used internally by the system, for example, to identify the parent account for an account.

The next field is the parent ID field, labeled *PID*. The value in this field is 0 if the account is a parent account. All new accounts are parent accounts unless they are specifically created as sub-accounts. If an account is a sub-account, then the value in the *PID* field is the ID number of the parent account. For example, the first account in the current account list is a parent account because the *PID* field has a value of 0. However, the second account in the list is a sub-account of the first because its *PID* field has the ID of the first account.

If you have sorted the list on the parent ID field by clicking **PID** in the column header, then sub-accounts are listed as a group immediately below their parent account. Each sub-account displays a vertical bar and two dashes in the *Account No* field that vertically points to the parent account. Simply follow the vertical bars up to the first account that does not have a vertical bar. That account is the parent account. You can verify this by inspecting the values in the PID field for the sub-accounts. They all have the same value, and that value is the account ID of the parent account.

The link in the *PID* field labeled “S” for “set” allows you to take an existing *parent* account and make it a sub-account of another parent account or take an existing *sub*-account and assign it to a different *parent* account. To demonstrate, suppose we want to assign this sub-account to a different parent account. First, highlight the *account number* for the new parent account, press **CTRL-C** to copy this number, and click **S** in the *Parent ID* field of the account you are re-assigning. The Account List scrolls down to the Account Operations section at the bottom of the page and prefills the first two fields with the appropriate values so all you have to do is press **CTRL-V** to paste the *account number* of the new parent account in the field on the right and click **Go**.

If this seems a little confusing, just remember that the *Parent ID* field displays either the parent account’s ID number, if the account is a sub-account, or a 0 if the account is a parent account. To reassign a sub-account to another account, you must change the number in this field to be the ID of the new parent account using the *Set* link and entering the *Account Number* for the parent account.

When specifying the account number of the parent, be sure to enter the *account number* of the parent as displayed in the sixth column, *not* the internal *account ID* found in the second column. Internal *Account IDs* are *not* the same as *account numbers*, so do not confuse the two. You will never be asked to enter the internal *Account ID.* You will only enter the *Account Number* in account management tasks. If you enter the *Account ID*, no action will be taken, and a message in red text will be displayed at the top of the page.

Now let’s demonstrate how to make a parent account a sub-account of another account. Click the *Set* link in the Parent ID field, enter the *Account Number* of the desired parent in the Account Operations field and click **Go**. A message at the top confirms the action, and the account becomes a sub-account under the specified parent account. You can verify this by noting that the vertical bar in the *Account No* field points upward to the parent account and by verifying that the parent ID field contains the internal account ID of the parent account.

It is important to note that, because sub-accounts always inherit the service plan of the parent account, when making an account a sub-account of another account, if the two accounts have *different* service plans, the sub-account is *always* assigned the service plan of its new parent account. Finally, note that you cannot make your original partner account—the one given you when you became an eFolder partner—a sub-account of another account.

The next column, labeled *CID*, is the customer ID field. Whenever you create a new *customer* account in the Web Portal, that account is given a unique customer ID by the system. Every account is assigned to a customer.

To sort the Account List by customer, click **CID** at the top of this column. The list is then sorted by customer number.

Note that accounts with the same *customer ID* create a *single* billing entity. Any billing reports you create will consolidate storage space usage across all accounts assigned to that customer. This makes it easy for you to bill that customer.

As a side note, notice that the name of the customer’s business and the city, state, and zip code where the customer’s business is located are all displayed in the corresponding columns to the right.

The next column, labeled *Brand*, is the brand identifier to which the account has been assigned. Most partners only have one brand, but some partners need more than one brand to market their services to different vertical markets. This field displays the brand to which the account has been assigned.

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

**Column 6 in the Account List (including impersonating an account)**

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

The next column, labeled *Account No*, is the unique system-generated account number assigned to the account that is used for billing purposes. Each account number is assigned to one and only one service plan, which dictates how the account will be billed. The account number is what you use in many account-management functions to identify an account.

A single machine may have more than one account number if that machine is using two or more services, such as the *Select* file backup service and the *Basic* file backup service. However, the same account number should *never* be used on two or more machines. For the Backup for Files service, each machine to be backed up should have its own account. For the BDR for ShadowProtect service plan, only the BDR machine should have its own account. For AppAssure BDR service plans, if you want to use the Web Portal to monitor storage utilization in the cloud, then each Source Core machine that is replicating data to the cloud must have its own account.

Getting back to the *Account No* field, typically, account numbers are made up of the following components: the brand name plus the zip code of the account plus the number of accounts that were in that zip code at the time the account was created. For example, the account number “DOC84062003” was constructed by assembling the following components: the “DOC” brand name, followed by the zip code of the business, “84062,” followed by “003” because this is the third account that was created in this zip code for this brand.

Please note, however, that any accounts that are created by someone who has not yet been branded will not have the brand name component in their account numbers. For example, if you signed up for a trial account before becoming an eFolder Partner, the account number for the trial account is missing the brand name component because you were not yet an eFolder partner when the trial account was created. Even after you became an eFolder partner and established your own brand, the brand component in that trail account number would continue to be absent because account numbers are generated at the time they are created and do not change from that point forward. This remains true even if the trial account is converted into a full-paying account.

Another possible variation in account numbers that you might encounter is seeing a brand name in the account number that is not your own brand. For example, notice that these accounts display “DELL” in the account number instead of my account’s brand, which is “DOC.” This can occur when accounts are migrated over to your partner account by the eFolder Technical Support team from another partner’s account. Suppose, for example, that the other partner is going out of business, and you have struck an agreement for you to take over their eFolder accounts. Because the other partner’s accounts were originally created under *their* brand, the migrated accounts will display the other partner’s brand name in the *Account Number* field.

The *Account No* field has three embedded links. The first link, labeled “I” for “Impersonate,” is used to impersonate an account. Impersonating an account lets you view the Web Portal as if you had logged in using that account’s user name and password. This is done without your having to log out of your own account and log in with the other account’s login credentials. Impersonating an account is useful, for example, when you want to see what functions are available to a user in the Web Portal, such as verifying that they cannot change or delete accounts after assigning them a new security role. Impersonation is more frequently used to access the options in the **My Account** menu to configure notifications, mailing lists, and contact information for that account—things you *cannot* do from your partner Account List.

Impersonating an account is also the easiest way to change a user’s password to a password you create. After impersonating the account, select *Change Password* in the **My** **Account** main menu option to display the *Change Account Password* page. If your role allows you to impersonate the account, as yours does as a partner, you do not need to know the old password to set a new one. You can also decide if you want the new password to be a temporary password that the user will have to change the first time they log in. This is done by checking the checkbox labeled *User Must Change* on the *Change Account Password* page.

The other way to change a user’s password is to click the *Reset* link in the *Password* column (Column 20) in the Account List, but this method generates a temporary, system-generated password that is emailed to the address or addresses currently stored in the Contact Information for the account. The first time the user logs in to the Web Portal or configures the Online Backup Manager, he will have to change the password to a permanent password. To summarize, to change a user’s password to a password of your choosing, impersonate the account and navigate to the *Change Account Password* screen. To reset a password to a temporary, system-generated password that the user must change, use the *Reset* link in the *Password* column.

Suppose you receive a call from a customer or end-user saying they have forgotten their password. If you have a way to verify the identity of the caller, then you can impersonate their account, create a new password using the *Change Password* option in the **My Account** menu, give the user the new password over the telephone, and wait for that user to verify that they can log in to the Web Portal. Don’t forget that you must also change the final new password in the Backup Manager on the user’s machine if the user’s account is using a service plan that requires the Backup Manager.

If you cannot verify the identity of the caller or are unsure, then do *not* impersonate the account. Instead, click the *Reset* link in the *Password* field. The system will generate a temporary password, which you should not give out to the unverified caller, and the system will send the password in an email to the email address on file in the Contact Information for the account. Note that many partners use their support email address as the account email address. If you want the Web Portal to email the customer the new password, you should verify that the customer’s email address has been entered for the account.

Clicking **I** to impersonate an account displays the Contact Information screen for the account you are impersonating. At that point, you have the same privileges or restrictions in the Web Portal as the user you are impersonating. A message displayed on a yellow background at the top of the screen reminds you that you are impersonating the account. You can navigate around the Web Portal and perform tasks as if you were that user. When you have finished and are ready to stop the impersonation, click **Stop Impersonating**. You are returned to the Account List page for your own account. Any changes you made while impersonating the account remain intact after you stop the impersonation.

Before you can impersonate an account, you must have a security role that allows you to impersonate the account. If you logged in to the Web Portal using your partner account, you have the authority to impersonate any of the accounts that display in your account list.

The second embedded link in the *Account No* field, labeled “L” for “Audit Log,” is used to display a historical list of changes that were made to the account, such as a new password, new security role, or new service plan being assigned to the account.

Clicking **L** displays the Audit Log for the account. Notice that the user name for the account is displayed at the top of the Audit Log. The list of changes that were made to the account is displayed in tabular format with one event listed per row. The columns of the table show when the event occurred, who performed the action (or attempted to perform the action), the user name of the account on which the action was performed, the action that was taken or attempted, and any messaging data that was associated with the event.

Icons in the first column of the Audit Log provide a visual status of each event. Green checkmarks indicate successful actions with no warnings or failures. Red “Xs” indicate failed actions. They display red text in the *What Happened* column explaining why the action failed.

Use the Search box at the top of the Audit Log to filter or search for specific events by the criteria displayed in the drop-down menu. For example, you can search for who made a change by their account number, user name, or by the account number or user name of the account they impersonated. You can also search by timestamp by entering the date in the year-month-day format to show all entries for that day. Note that if the change was performed by an eFolder employee, then the word “hidden” is displayed in the *Who Did It* field.

For the columns that have a header that is underscored, clicking the column header will sort the list on that field.

For longer event lists, click the drop-down menu on the right to control how many events are displayed at a time, and then use the page links displayed below the list to navigate through the list.

You can also view the Audit Log by selecting *Audit Log* in the **Reports** menu on the Web Portal main menu bar, but the Audit Log that displays there is the *combined* Audit Log across *all* of your accounts instead of for a single account. If you just want to see the Audit Log for an individual account, clicking **L** in the *Account Number* field of the Account List is the faster and easier way to do so.

Returning to the Account List, the third embedded link in the *Account Number* field, labeled “**E**” for “Event Log,” is used to display a list of the notification events that have occurred for this account. Events are occurrences such as backups, restorations, notifications sent, or a new sub-account being created under the account. An event is anything that occurred that is associated with the account except changes to the account itself, which is recorded in the Audit Log that we just discussed. This page has the same functions and layout as the Audit Log, so we will not discuss it in detail.

You can also display the event log by selecting *Event Log* in the **Reports** menu on the menu bar, but doing so displays the combined event log across *all* of your accounts instead of for a single account.

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

**Columns 7 through 10 in the Account List**

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

The next column in the Account List, labeled *User Name*, displays the user name. The user name is used to login to the Web Portal and must also be entered into the Backup Manager for accounts that use the Backup Manager.

The link in the *User Name* field labeled “S” for “set” allows you to change the user name for the account. For example, suppose the user for this account has left the company and another user has taken his place. This means we need to change the login credentials for the account to make them private to the new user. To do this, click the *Set* link in this field and enter the new user name in the pop-up box. After entering the new user name, click **OK** to make the change. A message confirms that your action was successful, and the new user name is displayed in the *User Name* field. An additional message reminds you to change the user name on the **My Account** page of the Online Backup Manager software. When the software asks if it is the same account or a different account, please indicate that it is the *same* account.

After changing the user name, change the password for the account using one of the two methods we described previously; namely, by impersonating the account, or by resetting the password in the Account List. Then impersonate the account if you have *not* already done so and make any necessary changes to the contact information and notification settings from the **My Account** menu. Then click **Stop Impersonation**.

Finally, if this account is using a service plan that requires the Backup Manager, such as the *Files for Backup* service plan or the *BDR for ShadowProtect* service plan, enter the new user name and password into the *My Account* page in the Backup Manager on the machine being backed up. If you fail to do so, the account will *not* backup any data from that point forward. The Backup Manager *must* have the same login credentials that exist in the Web Portal for backups to occur.

To demonstrate, in this example, because the account is using the *Basic Backup for Files* service plan, open the Backup Manager on the local machine that is being backed up, click the **My Account** tab, enter the new user name and password into the Account Credentials field, and click **Test Connection**. Be sure to click the **Test Connection** button, *not* the **Change Password** button to store the credentials in the Backup Manager. If this machine has been previously backed up, a message will ask if these changes apply to the same machine, which, in this case, they do, so make the appropriate selection. This completes what you need to do in the Backup Manager unless you want to make changes to other configuration data for the new user.

Getting back to the Account List, the next column in the list, labeled “Role,” displays the security role assigned to the account. Roles determine the account management functions and the range of accounts on which users can act after they login to the Web Portal. Use the link in the *Role* field labeled “S” for “set” to change the security role assigned to the account. Clicking **S** in this field takes you to the Account Operations section at the bottom of the screen and prefills the first two fields with the account number and the action so all you have to do is click the drop-down arrow, select a new security role, and click **Go**.

Before assigning a new role, however, be sure you understand the privileges and restrictions that go along with that role. You do *not*, for example, want to assign an end-user a role that has the authority to alter or delete accounts.

Note that only a user with the Partner Senior Manager security role has the ability to set or modify the security role for an account.

The next column, labeled “SPlan” for “Service Plan,” displays the eFolder service plan for this account. You can change the service plan for parent accounts by clicking the *Set* link in this field, just as you did for changing the security role.

Sub-accounts do not display the *Set* link in the *Service Plan* field because sub-accounts always inherit the service plan of the parent account. To change the service plan of a *sub*-account, either re-assign the sub-account to a parent account of that customer that *has* the desired service plan, or convert the sub-account into a parent account and then change the service plan.

We will demonstrate both procedures. First, let’s change the service plan of a sub-account for which there is *no* parent account for the customer with the desired service plan. Suppose we want to change the service plan for this sub-account from *Select* to *Basic*. Because this is a sub-account, there is no **Set** link in the *Service Plan* field. Moreover, because there is no parent account for this customer that uses the *Basic* service plan, you must first convert this sub-account to a parent account and then assign the parent account the desired service plan.

To do this, click the **Set** link in the *parent ID* column, enter the word “none” for the parent account in the Account Operations section, and click **Go**. A message confirms that the sub-account has been converted into a parent account and a zero is displayed in the *Parent ID* field for the account. Now, change the service plan for the account by clicking the **Set** link in the *Service Plan* field, selecting the *Basic* service plan in the drop-down menu, and clicking **Go**. A message confirms that the service plan has been changed, and “Basic” is displayed in the *Service Plan* field.

To demonstrate the second procedure, let’s change the service plan for a sub-account for which there *is* a parent account for this customer that is using the desired service plan. For example, let’s change the service plan for this sub-account from *Trial* (*Basic)* to *Select*. First highlight and press **CTRL+C** to copy the Account Number for the new parent account. Then, click the **Set** link in the *parent ID* field of the sub-account, press **CTRL+V** to paste the account number of the new parent account in the Account Operations section, and

click **Go**. A message at the top confirms that the *Trial (Basic)* sub-account has been re-assigned to a new parent account which uses the *Select* service plan. You can verify this visually by following the vertical bar from the sub-account to the parent account or by noticing that the *Parent ID* field for the sub-account now has the Account ID of the new parent account.

Note that changing the service plan for a parent account automatically changes the service plans for the sub-accounts under that parent account, since sub-accounts always inherit the service plan of the parent account. For example, changing this parent account from *Basic* to *Select* automatically changes all of the sub-accounts under this parent to the *Select* service plan. Because of this, be very careful when changing the service plans of parent accounts.

For detailed help on choosing a security role or a service plan for an account, please refer to the related video in this series entitled, *Choosing a security role and a service plan for an account.*

The next column in the Account List, labeled “Last Backup,” has a time zone designator as part of the column header that corresponds to the current time zone setting that is in the Contact Information for the account that you are logged in with, such as “[EDT]” for Eastern Daylight Time. All times in the Account List are displayed using this time zone.

The *Last Backup* column displays the date and time of the last attempted backup, either successful or failed, that was performed on the account. A green checkmark in the beginning of this field indicates the last backup was successful and generated *no* errors. A red “x” indicates that the last backup was *un*successful and generated errors or warnings.

Clicking the embedded link labeled “V” for “View backup sessions” displays the Backup Sessions Report for the account that shows all of the backup sessions performed or attempted on the account during the past 14 days. If an account has a red “x” in the *Last Backup* column, clicking **V** to view the Backup Sessions Report is a convenient way to diagnose the problem. The Backup Sessions Report has a tabular format and uses functionality that is similar to what you have been using in the Account List. It has two columns, *Cli.Warns* and *Cli.Errs,* that list the number of warnings or errors, respectively, and that provide a link for additional details. Note that you can cursor over the column headers to display tooltips that further explain the information displayed in each column.

Returning to the Account List, for accounts that have previously performed backups, the *Last Backup* field contains additional clickable icons, some of which are unique to the type of the service plan that an account is using, such as the **View AppAssure CORE Details** icon, which is unique to AppAssure CORE accounts. Moving your cursor over these icons displays a tooltip that further explains the icon.

Let’s take a look at some of these icons. Clicking **View Summary Report** displays a graphical look at the backup history for the account. Clicking **View Last Backup Log** displays the most recent Backup Log which has been pushed out to the Web Portal by the Backup Manager. Clicking the **View Backup Settings** icon displays the Backup Manager configuration settings as they existed at the time of the last backup. And finally, if you bought a BDR from eFolder, clicking **View Hardware Status** displays the status of over 30 different hardware functions of the BDR, such as the temperature of the processor, temperature of the memory chips, fan speed, and so forth. Note that these icons display information that you would otherwise have to gather by physically logging in to the remote machines.

Finally, if an account has been configured to backup to destinations other than the cloud, such as to a local server or a local disk, the *Last Backup* field displays one or more non-clickable storage-mode icons that indicate the various destinations of the data. When present, these icons appear at the very beginning of the *Last Backup* field. If there are multiple backup destinations, then each destination is displayed on a separate line with its corresponding storage-mode icon as the first icon on that line.

If a storage-mode icon is absent in the *Last Backup* field, it means that the data is *only* being backed up to the cloud. If data is being backed up to multiple destinations, then the world icon is displayed in front of the information pertaining to cloud backups, the server icon is displayed in front of information pertaining to local server backups, and the disk drive icon is displayed in front of information pertaining to local disk backups.

These three storage mode icons are also used in the *Disk Space, All Disk Space,* and *Disk Space Quota* columns. Let’s look at each of these three fields next.

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

**Columns 11 through 14 in the Account List**

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

The next column, labeled “Disk GB,” displays the total disk space used by an account at each backup destination—the cloud, the local server, and the local disk—if multiple destinations are being used. Each destination is displayed on a separate line and is preceded by the corresponding storage-mode icon that we just discussed.

The next column, labeled “All Disk GB,” displays the disk space used by this account plus all of its sub-accounts—again, by destination, just like in the previous field.

The next column, labeled “Quota GB,” displays two quotas for each account that are separated by a slash. The first quota is the *Hard Quota* and is used to specify the maximum amount of storage allocated to this account by the partner. This field defaults to *infinite* for non-trial accounts, *10* GB for Basic and Select *trial* accounts, 100 GB for ShadowProtect, and 10 GB for Trial (AppAssure Core) accounts. The text “inf” for “infinite” in this field indicates an infinite or unlimited amount of storage.

The second quota is the *User Quota*. The user quota is typically left blank so users can use this field to set their own limits. However, very few users set their own quotas. It is provided for those few users who want to control their backup costs and always stay below a certain quota, no matter what.

In general, as a partner, you should only set a *hard* quota on an account if the customer has purchased a predetermined amount of storage from you. If you plan to bill your customer based on actual usage, and your customer wants to stay within a certain limit, it is better to encourage your customer to set a Total Disk Usage notification in the Web Portal rather than set a *user* quota. Doing so will allow backups to continue rather than being stopped, and the configured email address will be notified when they approach or exceed their chosen limit.

When an account reaches within 15% of either of the two quotas, an automated notification is sent to the email address in the Contact Information for the account. When the account reaches the actual quota, all backups cease, at which point you or your administrator will either have to raise the quota or delete data at the storage destination to make room for new data.

Note that the actual quota the system uses is the *minimum* of the Hard Quota and the User Quota. Of the two quotas, the more restrictive one is the one that applies.

Note that if you set a hard quota on a parent account, then that quota represents the total amount of storage that will be allowed for the parent account plus all of its sub-accounts collectively. When that quota is reached, the parent account *and* all of the sub-accounts will no longer backup data.

For sub-accounts, the actual quota the system uses is the minimum of the sub-account’s hard quota, the sub-account’s user quota, and of the amount of storage space remaining under the quota for the parent account.

Use the **Set** link to change the storage quota for an account.

The next column, labeled “Mailboxes,” is only used by accounts that have the *Select* Backup for Files service that are also using the optional eFolder Email Archiving add-on feature to backup Microsoft Exchange mail servers. Email Archiving is a separate product from the Backup for Files service and must be licensed separately. However, this service is no longer being offered through eFolder, so this field applies only to those legacy partners who still have the service. Details about this field will not be further discussed here. Email Archiving is still available through a third-party vendor. If you are interested in this service, please talk to your Account Manager.

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

**Columns 15 through 21 in the Account List**

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

The next column in the Account List, labeled “company,” displays the name of the *customer’s* company. This is an optional field that is entered when the account is created.

The column labeled “Name” displays the last name and first name of the contact for the account. This information is useful, for example, if you get a notification that an account has not backed up for several days and you want to contact the user to find out why. For example, the user could have been out on vacation for a week and no new data was created that needed to be backed up.

Click the *Email* link in this field to quickly send an email to the address or addresses on file in the Contact Information for this account. Note that this email address might not be the email address of the person in the name field. In fact, many partners prefer to enter their own email address in the *Email Address* field of the Contact Information page so that they will receive notifications about the account instead of the customer.

The next three columns, *City, State*, and *Zip*, reflect the information that was entered into the Contact Information for the account. Note that the zip code is preceded by a two-digit country designator.

Regarding the Contact Information for an account—it is important to note that only the person who logs in with the account username or those who can impersonate the account in the Web Portal can see the contact information for an account. As a partner, you must decide what information you want to enter in the fields of the Contact Information page when you create new accounts. For example, do you want to put in your own email address or the customer’s email address in the *Email Address* field or a group of email addresses that are separated with a semi-colon. Whatever you decide, you should be consistent across your accounts.

Getting back to the Account List, the next column, labeled “Passwd” for “password,” displays the current status of the password for the account. A blue *Reset* link in this field means the account has a permanent password. The word “Temp*”* in red text in front of the *Reset* link means the account has a temporary password that must be changed to a permanent password when the user logs in to the Web Portal.

Use the **Reset** link in the *Password* field to reset an account’s password to a temporary system- generated password. The new password is emailed to the email address or address list in the Contact Information for the account. The user can use this password to login to the Web Portal but will be required at that time to create a permanent password. Passwords must have at least eight characters and contain at least one number. They cannot have the word “password” in them, and they cannot have three or more sequential or repeating characters. If the account uses a service plan that requires the Backup Manager, the new password must also be entered in the Backup Manager for backups to continue. In the Backup Manager, the user will be prompted to create a permanent password if the password is still temporary.

To demonstrate, suppose a user has contacted your support team because he has forgotten his password and you want to reset his password. Simply click **Reset** in the *Password* field for the account. A message is displayed at the top of the page that includes the temporary password. You should *not* give this password to the user over the telephone unless you can verify his identity. The word “Temp” in red text also appears in front of the *Reset* link in the *Password* field to indicate that the account currently has a temporary password. Finally, the system sends an email containing the temporary password to the email address or list of email addresses that is in the Contact Information for the account.

Note that if you, the partner, have entered your own email address in the Contact Information for the account because you want all notifications sent to you, then the end-user will not receive the email with the new temporary password.

Also note that although you can reset the password for an account that is in Maintenance Mode, as indicated by the words "In Maint" in the *Failed Logins* field, you *cannot* log into the eFolder Web Portal to create a permanent password while the account is in maintenance mode. You can, however, set the new password on the *My Account* page in the Backup Manager software. An account is put into Maintenance Mode, for example, when an initial USB preload is being performed on the machine being backed up. Do *not* take an account out of Maintenance Mode if it is in maintenance mode because of a USB preload. The eFolder Technical Support team will take the account out of maintenance mode after they have finished with the USB preload.

The next column, labeled “Failed Logins,” displays the number of consecutive failed logins that have been made on the account. A user is allowed three failed successive attempts within any 24 hour period and then the account is locked and can only be unlocked in the Web Portal by a partner or administrator. Locked accounts will *not* backup, and users are *not* notified when they are locked out, but they will be notified that their account is not backing up according to their notification settings. If an account has been locked, a link labeled “U” for “unlock” is displayed in the *Failed Logins* field. Clicking this link unlocks the account and resets the number of failed login attempts to zero.

The *Failed Logins* field also displays a link labeled “M” for “maintenance mode.” Clicking this link puts the account into maintenance mode, which suspends all backups and displays the text “In Maint” in this field. If an account is unexpectedly put into maintenance mode, you should investigate why it was placed in maintenance mode before you take it out of maintenance mode. All backups are suspended for an account that is in maintenance mode. Click **U** to take an account out of maintenance mode.

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

**Columns 22 through 31 in the Account List**

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

The next column, labeled “DIS” for “disabled,” displays “No” if the account has *not* been disabled and “Yes” if it has. If the account has been disabled, an optional comment is also displayed in this field.

Disabling an account suspends future backups for the account. Even though an account is disabled, the end user can still access their previous backed up data. You may want to disable an account, for example, when the customer has failed to make payment for your services. Note that eFolder will continue to bill you, the partner, for any account that has been disabled, as that account continues to occupy space in the cloud from prior backups. To stop billing for an account, you must delete the account, *not* disable it. Note also that disabling a *parent* account will *not* automatically disable its sub-accounts. Each sub-account must be disabled separately.

To disable an account, click the link labeled “**D**” in this field. A pop-up box is displayed where you can enter an optional reason for disabling the account, such as “Payment is 45 days overdue.” The next time a backup is attempted, it will fail because the account has been disabled, but the text you entered will display in the Backup Log along with the error in the log entry.

After typing your reason for disabling the account in the comment field, click **OK**. A message at the top of the page confirms your action, and the *Disabled* field displays “Yes,” the text you previously entered, and a link labeled “EN” for “enable.” Click **EN** to enable the account and resume backups. Note that there is no expiration date on a disabled account. The account will remain disabled forever until you re-enable the account. If you disable an account because a customer has failed to pay and the customer ultimately quits entirely, then you must remember to *delete* the account so you will not continue to be billed for the data that has been previously stored in the cloud for that account.

The next column, labeled “Expires,” displays the date the account expires. This field is only used for accounts with a trial service plan. The format of the date is four digit year, two-digit month, and two-digit day, separated by dashes. Note that this same format is used for all date fields in the Account List.

To change an expiration date for a trial account, click the “S” or *Set* link beside the expiration date, enter the date in the pop-up box, and click **OK**. A message at the top of the page confirms your action, and the new expiration date appears in the *Expires* field. Note that the “**S”** option is not available on sub-accounts since the sub-accounts inherit the expiration date of the parent account.

The next column, labeled “Created,” displays the date the account was created. This field cannot be changed.

The column labeled “DEL” for “deleted” displays, for deleted accounts, the date the account was deleted. If the account has not been deleted, then “No” displays in this field. Note that deleted accounts do *not* display in the Account List if the *Hide delete rows* checkbox has been checked in the Search Criteria section. If you *cannot* see a deleted account, then look at this checkbox first, and then check your search criteria.

The next column, labeled “NoBk Sent” for “no backup sent,” displays the date that the last “no backup” notification was sent to the email address on file in the Contact Information for the account.

The column labeled “NoBk Days” for “number of no backup days” displays two numbers separated by a slash. The first number is the number of days to allow before a “no backup” alert will be sent for the first time. The second number is the number of days to wait thereafter before sending additional notifications. For example, “3/7” in this field means wait three days with no backups before sending the first “no backup” notification and continue to send notifications every 7 days thereafter if no backups continue.

The values displayed in the *Number of No Backup Days* field are those that were previously entered in the Notifications page for the account. To display this page, select *Notifications* from the **My Account** main menu option in the Web Portal and look at the values that have been entered in the No Backup Notification section. You can change these values on this page if you desire. These same entries are displayed in the Account List in the *Number of No Backup Days* field. The default values are to send the first notification three days after no backups have been received and every seven days thereafter.

The next column, labeled “Server ID,” displays the internal name of the server where the backup is stored. The default value is 0: [Region 1]. This server is assigned when you press the **Test Connection** button in the Backup Manager.

The format of this name is best explained with an example. For the server ID of “20130041: r13.slc.sc.efscloud.net,” the “20130041:” represents the data center and server: “20” indicates the Salt Lake City data center and “13” indicates the specific server in the data center. The “r13.slc” after the colon is another way to state the name of the server and the data center and the “sc.efscloud.net” is the rest of the URL. This is an informational field that cannot be modified. The information in this field is used by eFolder Technical Support in the event of an emergency restore.

The column labeled “Serial No.” for “serial number,” is only for BDR for ShadowProtect accounts. The system inserts the serial number of the BDR into this field the first time the BDR connects to the Web Portal.

The next field, labeled “Internal Desc.” for “internal description,” displays an internal description of the account that you, the partner, create. It cannot be seen by the customer. To enter an internal description for an account, click the *Set* link in this field, type a description, and click **OK.** There is a 255 character limit for this field.

The next field, labeled “User Desc.” for “user description,” displays a description that *can* be seen and modified by the user. Use the *Set* link in this field to enter a user description. There is a 255 character limit for this field.

Congratulations. You have now reviewed all of the fields in the account list, along with their embedded management links, report icons, destination icons, and status icons.

Thanks for watching this video on how to use the Account List in the Web Portal. Please see the other video overviews and how-to videos in this series for additional training on partner-related tasks.