# Overview of eFolder Backup for Files

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

**Introduction**

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

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, and
* access the Partner Center, where you can find documentation, training, and marketing collateral.

You can access the Web Portal in one of three ways: from the eFolder web site at [www.efolder.net](http://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 that 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*.