White Paper

An Enterprise Approach to Mobile File Access and Sharing

opentext™

Table of Contents

page

OpenText™ Filr offers a better alternative for end users and IT.

Anywhere, Any Device File Access with IT in Control

Like it or not, cloud-based file sharing services have opened a new world of mobile file access and collaborative file sharing users are not about to give up. And why should they?

They can get to the files they need whenever they want from any mobile device. They don't have to jump through any bureaucratic hoops to share the files, and this saves time. They collaborate more easily with colleagues and clients. They get more done.

With these productivity gains and time savings, many users might not care about the risks associated with copying corporate files to consumer-oriented cloud services. Users see regulatory compliance issues, loss of file access controls, potential security breaches, increased IT management efforts, and other cloud problems as issues for IT, not them. Users have a job to do, and no amount of policy creation and enforcement will cause them to subordinate their own productivity to enterprise concerns. To meet the need, you must give them a solution that's equal to or better than what they're using today.

OpenText™ Filr offers a better alternative for end users and IT. May be rephrase it directly—Filr is a better option for end users and IT. It gives users easy, anywhere, any-device access to corporate files, while keeping file access and sharing completely under IT control. It gives users the mobile file access and collaborative file sharing experiences they want, but through an enterprise-ready solution that leverages your existing, on-premises infrastructure. Filr eliminates the need to manage third-party services or police users by allowing you to mobilize your existing file servers, existing files, and existing file system rights.

Filr serves as the connection between those file servers and the endpoint devices your organization uses, including Windows, Mac, iOS, and Android devices. It also offers web access via popular browsers. Filr delivers easy-to-use, synchronized file mobility, while enabling your organization to retain policy-driven controls over file access and storage.

Filr Competitive Differentiators

Unlike other mobile file access and collaborative file sharing solutions, Filr has been designed with the enterprise in mind, resulting in less administration, better security, and the ability to leverage existing investments. Some of the key competitive differentiators that Filr provides to the IT departments are:

- **Support for multiple identity stores**, including Microsoft Active Directory and NetIQ eDirectory by OpenText™
- **Native file system integration** with Microsoft Windows Server and OpenText™ Open Enterprise Server (using CIFS/NCP). Files remain on existing, on-premises enterprise file servers, eliminating the need to move or duplicate files.
- **Reuse of the user access controls and quotas** that you have already established. The group and user access rights that govern your organization's home and network folders also govern user access from mobile devices.
- **Seamless integration with users' existing folders**, including home directories and network shares. This allows users to get to work on day one of using Filr.
- **Use of users' real credentials** for file access. This ensures authorized access and audit trail support.
- **Granular control over sharing.** In addition to the access control already configured in your identity management system and file systems, Filr lets you determine which files and folders users can share either internally or externally.

At a high level, the core technological capabilities for Filr are driven by its integrated virtual appliances.

Filr High-Level Architecture

At a high level, the core technological capabilities of Filr are driven by its integrated virtual appliances. Also playing key roles are its front-end, user-facing services and its integration with existing back-end enterprise services.

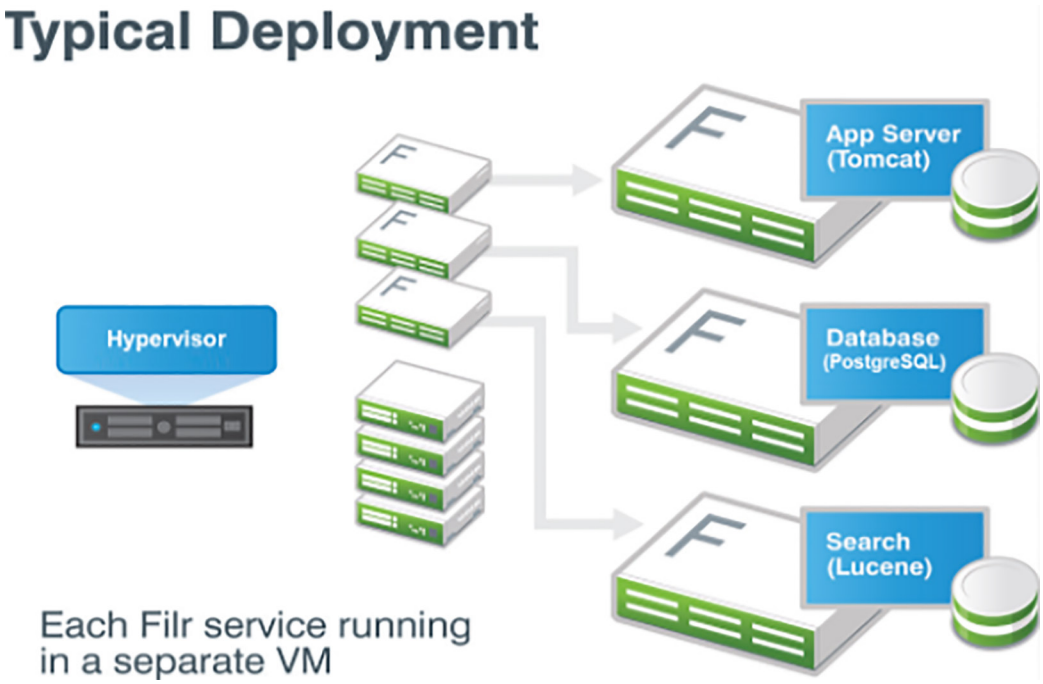
Filr Virtual Appliances

Filr consists of the following three virtual machines:

- OpenText™ Filr Appliance
- OpenText™ PostgreSQL Database Appliance
- OpenText™ Search Index Appliance
- Content Editor Appliance (available only for OpenText™ Filr advanced edition)

All three appliances are currently certified to run on VMware ESX, Windows Hyper-V, Citrix Xen, and SLES Xen. We plan to add support for other hypervisors in the future based on customer demand.

Regardless of whether users access their files through a mobile app, browser, MacBook or Windows laptop, Filr always presents an intuitive, easy-to-use interface.



FILR APPLIANCE

The Filr Appliance provides the logic and services that allow users to easily and securely access and share files. Since this appliance incorporates both the database and search index services, it can be used for small deployments or pilot projects. In typical enterprise environments, the PostgreSQL Database Appliance and the Search Index Appliance should be deployed separately.

POSTGRESQL DATABASE APPLIANCE

The PostgreSQL Database Appliance is a database that stores information about your organization's Filr deployment and users, including structural and identification information about folders and files, and user profile information. You can also use an existing PostgreSQL or Microsoft SQL database from your environment and simply point the Filr appliance to that database during the initial Filr configuration

.

SEARCH INDEX APPLIANCE

The Search Index Appliance is a high-performance Java search engine built with Lucene technology. To enable fast searches of files and folders in Filr, the Search Index Appliance scans and indexes, on a scheduled basis, all the designated folders (including their sub-folders and files) stored on your back-end file systems. It provides full-text indexing not only on file contents and file names, but also on the comments that Filr users make on specific files.

The Search Index Appliance collects all the metadata and user security access rights associated with files and folders. The indexing of metadata allows Filr users to search through millions of files and receive quick results. Separate from the search and index functionality, users can directly access files and folders to which they have rights through a real-time look-up capability provided by the main Filr Appliance. This ensures that users can always find and see the latest files added to your organization's back-end file systems, even if Filr hasn't yet indexed those files.

Filr gives you complete control over how users can access and share files and which files they can access and share.

Front-End Filr Services

Filr allows users to easily access all their files and folders from their desktop, browser, or mobile device. It has mobile apps for iPhones and iPads (iOS 14 .x and 15.x), Android phones and tablets (5 Netapp and later). Filr provides a Windows client and a Mac client for use on desktops or laptops. It also provides web access through a standard web browser, such as Firefox, Chrome, Edge, or Internet Explorer.

All these mobile apps and clients let users connect to their files from wherever they roam. Additionally, Filr uses secure socket layer (SSL) encryption via HTTPS to secure all communications with these different clients and devices.

USING FILR

Filr enables users to work with files in three main ways:

1. **Access.** Users can access the files they need in multiple ways, including from a web browser, their desktop, or a mobile device.
2. **Share.** If you enable sharing, users can share files with co-workers and grant them specific rights to those files, such as read-only or editing. Users can also easily see what others have shared with them. To the extent that your organization allows, users can also easily share with colleagues outside of your enterprise walls.
3. **Collaborate.** Users can make comments on any file they have access to or that has been shared with them. Other users with access can see those comments and add their own.

EASY-TO-USE INTERFACE

Regardless of whether users access their files through a mobile app, browser, MacBook, or Windows laptop, Filr always presents an intuitive, easy-to-use interface. The Filr user interface provides instant access to users' files through a simple click of one of the following main icons or folders:

- **My Files.** Access to and management of individual users' personal files, which in most cases will be those files stored in their network Home Directory.
- **Net Folders.** Access to users' existing NCP or CIFS network shares is based on access rights defined in the file system, as well as whether the IT administrator has allowed Filr to present these shares.
- **Shared with Me.** Access to files and folders that others have shared with the user, with access limited based on the specific privileges the owners have granted.
- **Shared by Me.** Management of the files and folders that users have shared with others, including the ability to grant additional rights or revoke rights.

While Filr can easily handle thousands of users, organizations with several thousand users can further increase performance by deploying multiple instances of the main Filr appliance behind a load balancing L4 switch.

What's New is another key user interface feature that provides an up-to-date view of the latest changes happening in the Filr system, such as new files, the latest changes to files, and information on users who have modified files. The interface also provides a search field that allows a global search of content within the Filr site, including file content, metadata, and comments. Users can set their own personal preferences on how Filr displays files and how many files will appear on a given page.

Other Features

Automatically Uploading Photos and Videos to Filr

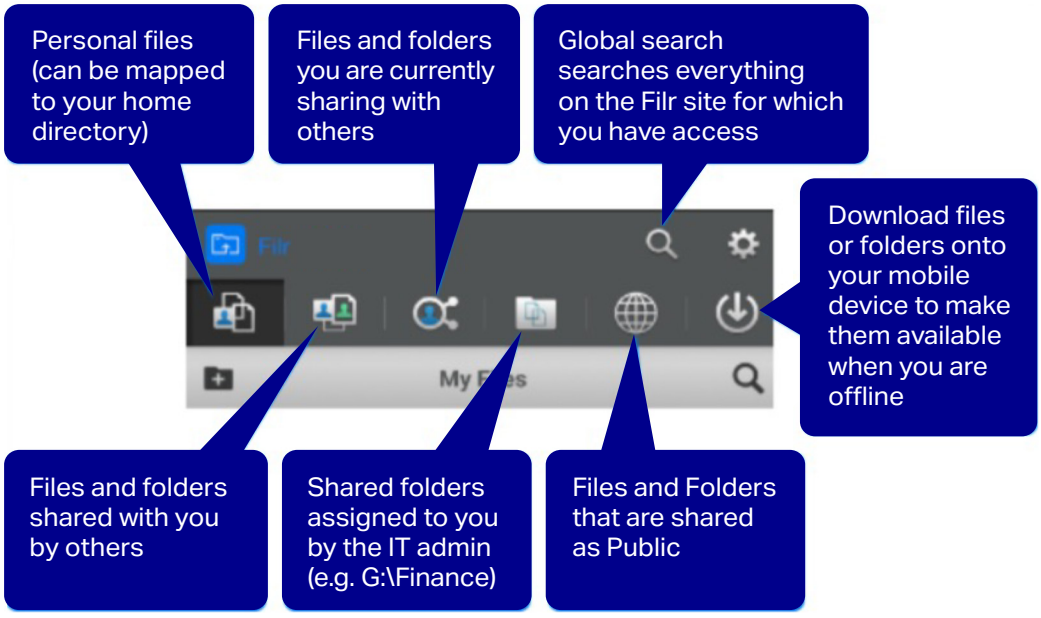
Users can upload/download files. On iOS and Android devices, you can set the Filr app to automatically upload the photos and videos from the local storage to the Filr server. Photos and videos are automatically uploaded to the Filr server without any notification to the user.

Performing Collaborative Edits

Users can also edit the files online. Filr allows to perform secure collaborative edits on your documents. Collaborative edits can be performed on all major file types such as documents, spreadsheet, and so on. Edits are done by using the Browser, and no Native application is required.

Files App Integration (iOS Only)

The Filr mobile app allows you to view most files within the app. Depending on the size and type of file, the app might need to be opened in a third-party app, or a warning might be displayed before you can view it in the Filr app.



The Windows and Mac clients for Filr not only give users access to their own files and shared files, but they also synchronize those files to the users' desktops or laptops, so the most up-to-date content is easily accessible whether users are online or offline. As an added benefit, this ensures that when users work on files stored in Filr from their laptops or desktops, those files will always be backed up to the network.

In all cases of sharing, you maintain control over your organization's content.

Organizations can also choose whether they want to enable synchronization. When enabled, Filr will synchronize the contents of My Files and Shared with Me by default. Users can also choose to have some, or all their Net Folders synchronized. Users should use care when configuring which Net Folders to synchronize so they don't consume an excessive amount of local storage. When configuring Net Folder synchronization, users will receive a warning if the configured synchronization results in an excessive amount of data being synchronized. If synchronization is disabled, organizations can rest easy knowing that they can provide access to sensitive data without that data ever being copied to devices that might get lost or stolen.

Back-End Filr Services

One of the main advantages of Filr over cloud-based file sharing solutions is that it leverages your organization's existing back-end file services and servers. Filr simply serves as the connection between your existing file servers and the endpoint devices your users use. This eliminates the need to duplicate your organization's files and file structure onto a third-party hosted solution. It also eliminates the added effort of having to manage that additional hosted file infrastructure.

Since the files remain on your existing file servers, there's no need to expand, copy or change the file system infrastructure. There's no need to expand or change your existing backup and recovery systems either. Files stay protected and under your control.

Filr supports both CIFS and NCP, enabling it to support file services provided by either Microsoft Windows Server or Open Enterprise Server

LDAP INTEGRATION

Part of the power of Filr comes from its ability to integrate with an organization's existing directory service, whether it's Microsoft Active Directory, NetIQ eDirectory or a combination of both. Filr can synchronize with these directory services to simplify the creation of Filr users, automatically pulling in each user and group's existing access controls and authentication requirements. Whatever group and user access rights govern your organization's network folders will also govern access to those resources via Filr mobile apps or clients.

Additionally, Filr uses your directory service setup as it is. It doesn't require any schema extensions or directory reconfiguration.

Filr doesn't require IT administrators to try to reinvent all their user access and file system rights—rights that they've taken years to configure and fine-tune.

IT ADMIN CONTROLS

Leveraging existing back-end file services and LDAP directory services are key to the way Filr allows you to retain control and security over your organization's files. Unlike other solutions, Filr doesn't require IT administrators to try to reinvent all their user access and file system rights—rights that they've taken years to configure and fine-tune. The directory services and file systems on your enterprise servers dictate who owns files and who has rights to files. Filr does not change those rights.

Besides using your existing user and file system rights, Filr adds additional IT admin controls. While the solution can give users anywhere and any device access to their files, you can limit that access if desired. Perhaps you only want users to be able to access certain folders from a mobile device or via web access. Maybe you're okay with users being able to view all their authorized files from any device, but you only want to allow a subset of files to be downloaded. Or it could be that you let users in one department both view and download files to their mobile devices from a certain folder, while users from a different department can only view those files. Filr gives you and your IT administrators very granular control over mobile and web user access.

It's important to note that just because users have the right to access and download their files from any device doesn't mean that they can share those files. File sharing must be turned on by the IT administrator. IT administrators have direct control over who can share files, to whom those files can be shared, and what files can be shared.

To whatever degree you turn on sharing, you will essentially be extending what users can normally do with any given file. To enable sharing without altering existing file rights, Filr lets you create proxy users in Filr to facilitate secure and authorized file sharing. You can create a proxy user for any network folder and define what access rights that proxy will have.

So, when a user decides to share a file from her home directory with a co-worker, even though that co-worker doesn't have access rights to that file, Filr recognizes the file has been shared with the co-worker and grants access via the proxy user. As mentioned before, it's entirely up to you whether this functionality is turned on and to what degree. Filr gives you complete control over how users can access and share files and which files they can access and share.

Filr Deployment and Configuration

Deployment and configuration of Filr is very straightforward, simple, and fast. The appliances are installed using a VMware vSphere client. After entering the appropriate authentication information and configuring the basic network setup, you browse to the address of the Filr appliance and click the Filr Server Configuration icon, which initiates a simple and easy-to-use wizard to perform the necessary configuration operations.

The first configuration task will be to specify whether to perform a small or large deployment. Except for testing or small sites, the large deployment option should be chosen in most cases because it can be scaled upwards while also allowing for high availability and fault tolerance. The next task is to point the Filr Appliance to the Search Index Appliance and the PostgreSQL Database Appliance (or your organization's existing PostgreSQL or Microsoft SQL database). Following that, Filr will automatically configure many of the settings, but you will have the option to change them as desired.

Once Filr is up and running, the main configuration tasks that need to be completed involve the following:

- User creation and provisioning
- Home directories
- Shared network folders
- Local users and personal storage
- File sharing Security

While Filr can easily handle thousands of users, organizations with several thousand users can further increase performance by deploying multiple instances of the main Filr appliance behind a load balancing L4 switch. You can also add additional database and index appliances to your setup as needed.

The first-time users log into Filr—whether from a mobile device, web browser, or laptop—they'll be able to immediately access their personal files without any additional setup or extensive file copying those other solutions require.

User Creation and Provisioning

The easiest way to add users to Filr is to set up LDAP synchronization with your organization's directory services. You can automatically add users to the Filr. This is done from within the Filr administration console, where Filr gives you various user and group synchronization options, as well as synchronization scheduling options. LDAP synchronization allows users to log into Filr using their corporate credentials. Filr does not store these credentials, but logs users in against your corporate LDAP directory.

You can also manually add users to Filr or import them using profile files. Filr also provides the option to allow external users to access your Filr site either as guest users or registered users or. External user access is not enabled by default.

Home Directories

A major advantage of creating Filr users via LDAP synchronization is that the synchronization process can automatically populate the My Files section of the Filr user interface with the files from users' existing network home directories. This means that the first-time users log into Filr—whether from a mobile device, web browser, or laptop—they'll be able to immediately access their personal files without any additional setup or extensive file copying those other solutions require. Also, by allowing users to work directly from their home directories, Filr enables them to work faster, create files confidently and never have to worry about duplicating files or reconciling conflicting versions.

Filr gives you granular control over which files users can and cannot share. Sharing is configurable on a per user, group, or folder basis.

Shared Network Folders

In most organizations, users have authorized access to more than just the files in their home directories. They will have access to a variety of different network folders or mapped network drives. For example, members of the marketing department might have access to various shared marketing folders. The files in these shared locations are where a lot of the collaborative work resides for an organization's different teams and departments.

You can have the contents of these shared folders or mapped drives populated for users inside the Net Folder area of the Filr user interface. To provision these Net Folders, you simply assign the desired network folders to specific groups or users. When users click on the Net Folder tab, they'll be able to access these files and folders in accordance with their corporate-defined access rights. Because they're accessing and working with the original files, they don't have to worry about accidentally creating duplicate files or reconciling multiple file versions.

Local Users and Personal Storage

As already mentioned, you have the ability to manually add users to Filr. These are referred to as local users, who might include temporary workers, contract workers or any guest user that is not stored in your organization's LDAP directory. Since local users do not have any file access rights to your network servers, they will not have access to any Net Folders in Filr. They will only have access to files that have been shared with them by internal Filr users.

However, you have the option to turn on personal storage for local users, which allows them to upload and store files in their personal My Files area of Filr. This personal storage resides in and is managed by Filr rather than on your back-end file systems. While you also have the option to turn on personal storage for your internal users as well, it's rarely needed due to the home directory integration.

File Sharing

Filr gives you granular control over which files users can and cannot share. Sharing is configurable on a per user, group, or folder basis. You can limit sharing to internal users within your organization or open it up to external users. Filr provides two main levels of external sharing.

When enabled, the first method of external sharing requires external users to create an account and authenticate with Filr. A typical scenario for external sharing would be when an internal user wants to share a file or folder with a specific individual outside the organization. The internal user would enter the person's email address in the sharing dialog for a specific file or folder. Filr would then send an invitation email to that person, prompting the person to create an account on Filr. Once the account is created, the external user can log in to access the shared item and any other items that have been shared with the external user.

External users can collaborate on files based on the permissions they receive from people who have shared items with them. External sharing makes working with contractors and other companies much more efficient. Filr provides mechanisms to allow you to monitor external user sharing.

The second method of external sharing is public sharing. Public sharing does not require any authentication, nor does it provide any file collaboration capability. When a user shares a file publicly, Filr generates a URL link that points to the file, which internal users can provide to outsiders to allow them to access the file. For example, the link for a marketing flyer or presentation file could be posted on the web or Twitter. When that link is clicked, it will take people directly to the file. This type of sharing greatly simplifies your organization's ability to push out public-facing files to targeted customers or partners, eliminating the need for users to involve you, the web development team or other groups in your organization.

In all cases of sharing, you maintain control over your organization's content. You can establish tight controls that ensure that all files are not shared outside your organization, or you can establish looser controls that allow different degrees of external access and sharing.

Filr is backed by a strong security infrastructure. All encryption is done with industry-leading SHA and AES algorithms using strong keys (2048 bits).

Security

Filr is backed by a strong security infrastructure. All encryption is done with industry-leading SHA and AES algorithms using strong keys (2048 bits). Communication between the suite of appliances is authenticated and secured using different credentials for each unique instance of every appliance.

While Filr uses SSL encryption for all communication between the Filr site and users' mobile devices, the Filr apps do not encrypt files downloaded to the devices. The main reason for this is that the mobile devices themselves would negate any encryption by Filr once a downloaded file is allowed to be used within any other app on the mobile device.

One way to deal with this is to configure Filr to prevent users from downloading files to their devices. They could still view files; they just couldn't edit them.

If you want to allow downloading, there are ways to make sure that all files downloaded to users' mobile devices are encrypted. The best way to accomplish this is to configure the mobile devices to encrypt all downloaded data.

For iOS devices with hardware encryption, this is done by creating a passcode lock. For Android 4 and later devices, this is done by turning on data encryption in the security settings. It's recommended that you enforce this data encryption using a mobile device management solution to ensure consistent policy adherence.

Filr gives users the productivity gains and time savings that mobile file access and collaborative sharing offer without exposing your organization to the risks and additional management requirements of cloud and third-party hosted solutions.

Filr also allows you to manage the Filr app on mobile devices. This can provide an alternative method of monitoring or protecting data on mobile devices. Administrators can see what devices have accessed the Filr system and can wipe Filr data from specific devices. This allows you to remove sensitive information from lost or stolen devices.

Users Get the Mobile Access They Want, and You Stay in Control

Filr gives users the productivity gains and time savings that mobile file access and collaborative sharing offer without exposing your organization to the risks and additional management requirements of cloud and third-party hosted solutions. It lets you maintain enterprise files on-premises and keeps you in complete control over file access and sharing. Filr enables your organization to stay in compliance and continue to enforce your established security and data protection measures, while users enjoy the easy, anywhere, any device file access they demand.

Learn more at
www.microfocus.com/en-us/products/filr/overview
www.microfocus.com/opentext

Connect with Us

OpenText CEO Mark Barrenechea's blog

opentext™