

Top Ten Reasons Why Your Filr Deployment Should Include File Reporter

As today's organizations wrestle with the needs of remote workers and collaboration between employees and external constituents, Micro Focus® Filr seems the perfect solution. But is your on-premises data ready for remote access and sharing? How secure is it now, and who can access it? Before you open up your environment, you should know what files you have and determine the value of the data in each part of your system. Micro Focus File Reporter can help you lay the foundation for success with Filr.

The remote access and sharing capabilities Filr provides for on-premises data have the potential to dramatically alter how users in organizations work with files. With Filr, users now have the ability to access organizational data stored on servers behind the firewall from anywhere—and using any mobile device. Filr also allows users to share these files with other users inside and outside the company.

Connecting Filr to a poorly understood file system can lead to trouble. Here are ten reasons why security-conscious organizations are coupling their Filr deployment with File Reporter:

- 1. Know exactly what's available for access and sharing.** Your organization might have terabytes of file data, so do you really know what's in your file system? Before enabling network locations for Filr, you need to know what files live in those areas and determine if you want all of the files available for remote access and sharing.
- 2. Know what rights users have in Filr-enabled network areas.** Enabling a network volume, share or folder for remote access and sharing through Filr without first knowing who has rights to that area can result in unintended consequences. Before enabling any network area for Filr, File Reporter can tell you all of the users who have rights to the network area and how those rights were derived.
- 3. Know what groups users have rights to.** Many users are members of groups and through group membership have access to sensitive files. Just because an administrator is in a group with doctors, for instance, doesn't mean that administrator should be able to share the same files the doctors can. File Reporter specifies the files users have access to through group memberships so you can take any necessary action.
- 4. Ongoing reporting.** To make sure that users continue to access and share only the files you want, File Reporter continues to report on the files located in the network areas you make accessible for remote access and sharing.

File Reporter reports on the:

- Rights of users accessing and sharing files using Filr
- Files located in Filr-enabled network locations
- Storage growth trends of Filr-enabled network locations

File Reporter and Filr both support Micro Focus eDirectory™ and Active Directory and their related file systems, enabling File Reporter to comprehensively report on all file data and rights associated with Filr.

Filr gives you remote access and sharing for your on-premises data, but before you enable Filr, you need to avoid the potential for accessing or sharing confidential data. Make Filr a success by learning what data you are storing and who has access to it with File Reporter.

- 5. Prevent sharing of copyrighted material.** Sharing copyrighted material can expose an organization to liability issues. If you have applications, media or other copyrighted files that you're not allowed to share, File Reporter can tell you where they are so you can set up the controls in Filr to prevent sharing.
- 6. Organize what to share and allow access to.** You could make individual files unshareable using Filr controls, but in many cases it's much faster and more efficient to move them into a more appropriate location using the knowledge File Reporter provides. Before you enable Filr, you can place files suitable for remote access and sharing in Filr-accessible volumes, shares or folders while placing sensitive files like software code or financial documents in areas where you won't allow sharing.
- 7. Prevent specific users from remotely accessing or sharing files.** There may be instances where you do not want to give certain individuals remote access or sharing capabilities because of their role or due to their involvement in a legal process. File Reporter can generate a report specifying all of the network areas to which the user has rights, so you can then take any needed measures.
- 8. Remain in compliance with organizational policies.** Some organizations have written policies that state they must store and access specific files on premises only. Many regulations require the same. File Reporter lets you verify that these files exist in secure locations on the network that users cannot access or share through Filr.
- 9. Know who owns the file.** Sometimes knowing who owns a file is every bit as important as the content of the file. Before you make files available for remote access and sharing, File Reporter lets you know who the owners are.
- 10. Storage allocation.** When you want to create a new area on the network for Filr remote access and sharing, instead of guessing on the size of the network area to set up, you can use File Reporter to determine a reasonable estimate of what you will need. File Reporter can learn the sizes of the files you plan to store on that volume or share, while trending reports can indicate the rate of growth on the network volume or share and when you might need to allocate more disk space.



Micro Focus
UK Headquarters
United Kingdom
+44 (0) 1635 565200

U.S. Headquarters
Seattle, Washington
206 217 7100
800 872 2829

Additional contact information and office locations:
www.novell.com

About Micro Focus

The Micro Focus product portfolios enable enterprise customers to unlock the value in their business data and logic to improve their competitive advantage through innovation.
www.microfocus.com