VERSION 1 • JANUARY 2021

ENTERPRISE FILE SHARING WITH INTEGRATED SECURITY SOLUTIONS

NEXT GENERATION FILE SHARING

FileOrbis Security Vision

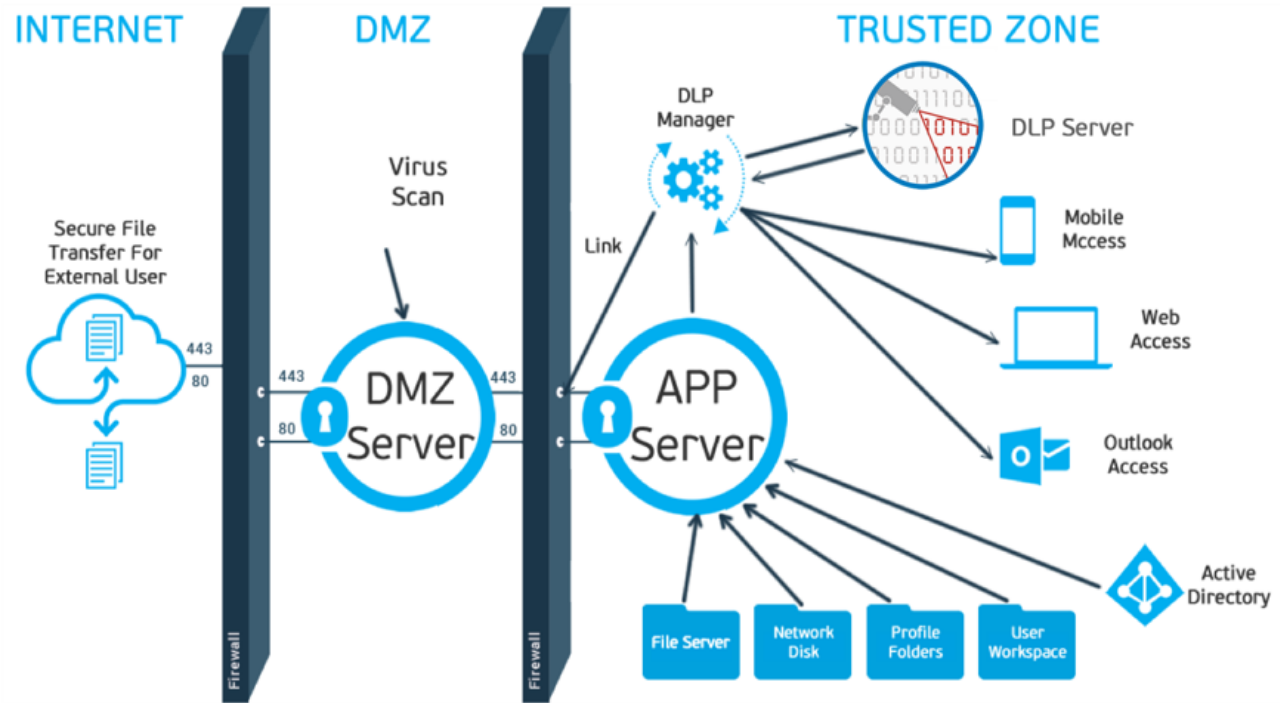
FileOrbis is currently used by various major corporates including banks, health institutions, educational institutions, and government agencies. Today, all organizations rely on FileOrbis' infrastructure and security capabilities for their file sharing and collaboration needs. In this sense, FileOrbis provides the processing and security of sensitive data, legal compliance, and secure sharing of data that all institutions value. FileOrbis provides end-to-end data protection with multiple layers of security at various stages. With FileOrbis, you can secure enterprise data and make sure they are well protected on company servers and employee devices.

Is FileOrbis Secure?

FileOrbis is completely secure and offers multiple levels of data protection.
FileOrbis delivers security processes into three stages: preliminary process, transaction process, post-transaction process. Security steps are mostly included in the preliminary processing and aim security analysis before files enter the system. All files to be uploaded in the system are received by the preliminary process and passed through security analysis before entering the system. Files found to be secure are uploaded in the system with approvals received from layers of security analysis. In the post-transaction process, end-to-end security is obtained by providing access controls, including detailed access reporting of files, permission analysis, link, and email attachment access.

FileOrbis Security Features:

- Anti-Malware Integration
- Sandbox Integration
- DLP Solutions Integration
- RADIUS Integration
- SIEM Integration
- FileOrbis "Filewall"



Integrations and FileOrbis Additional Security Controls

Anti-Malware Integration:
FileOrbis can integrate with existing anti-malware solutions used within organizations. In this way, the file is scanned according to the scanning standards determined by the anti-malware product used and trusted by the organizations, before it is taken into the system, and the operation log is added to the FileOrbis security report. The results are also instantly shown to the end-user via the information screen. FileOrbis offers an embedded, open-source solution, ClamAV.

Sandbox Integration:
By integrating with both on-premise and cloud sandbox solutions, it is ensured that the files are analyzed with hash first, and if no result is obtained from the hash query, the entire files in the system are sent to sandbox for analysis. According to the result of this operation, the process is allowed or blocked. The results are recorded, and utilized to create reports and are shown to the end-user for informational purposes. Many solutions are supported regardless of their vendor, and support for new solutions is added continuously.

DLP Integration:
Content analysis can be performed with the DLP solution used within organizations and action can be taken with the response from DLP while downloading, uploading, and previewing files to the FileOrbis system with this integration. According to the information received via DLP, the operation is allowed or blocked. The result of this operation is added in the central logs as a result.

RADIUS Integration:
FileOrbis integrates with secure 2FA/MFA authentication solutions, providing an extra layer of protection for users' corporate standards and system access. FileOrbis allows you to perform the authentication with the RADIUS protocol instead of LDAP and all RADIUS-based 2FA/MFA solutions are supported.

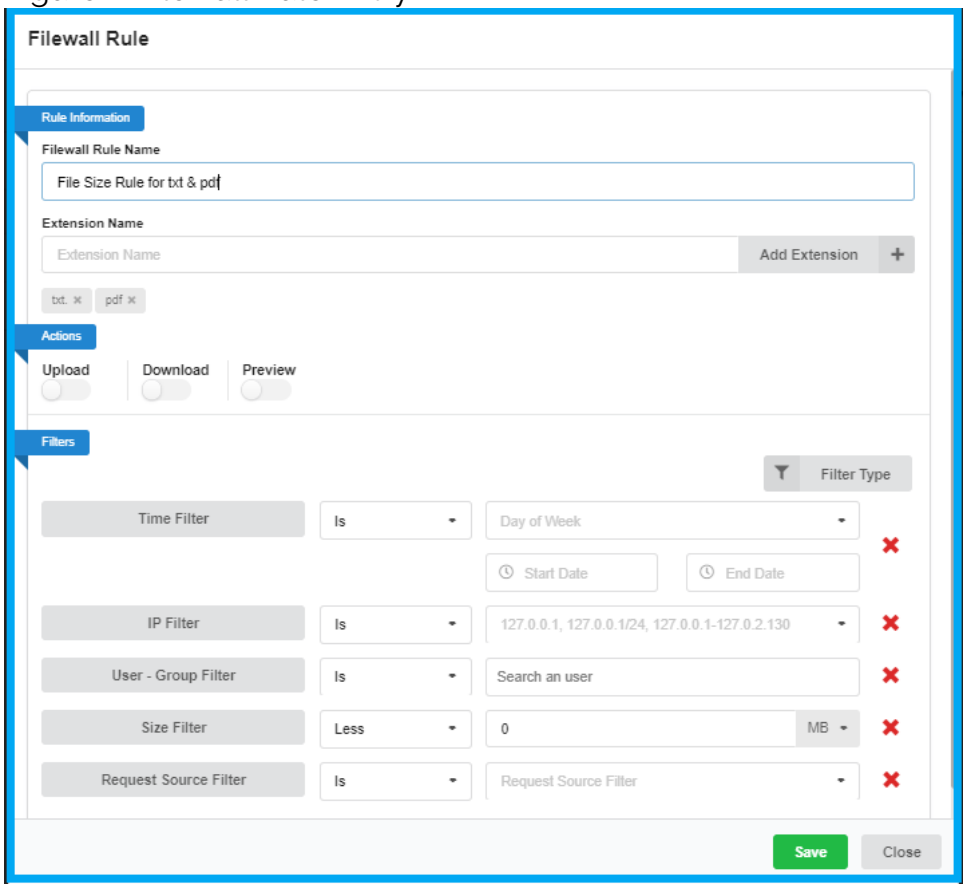
SIEM Integration:

In the FileOrbis reports section, all user and admin transactions are logged in detail. These logs can be easily and instantly transferred to SIEM products to ensure log integrity. With these recorded logs, advantages such as defining correlations and generating alarms over SIEM products are provided.

FileOrbis "Filewall":

The Filewall module, developed by FileOrbis, allows files to be identified, for known files, according to their true type and according to extensions, and to define rules accordingly. True file type detection can be done both in binary and in text-based files based on machine learning. In this way, the manipulation of file extensions is minimized. Once the true type of a file is determined, download, preview, and upload rules can be defined for these file types. In cases where the true file type cannot be determined, rules are applied according to the extension of the file. By writing rules with many details such as user, IP, FileOrbis service type, time with positive or negative logic options for each transaction, the actions of your users on file types can be determined. With this module, encrypted or macro-containing files can also be detected and the desired rules can be applied.

Figure 1: Filewall Rule Entry



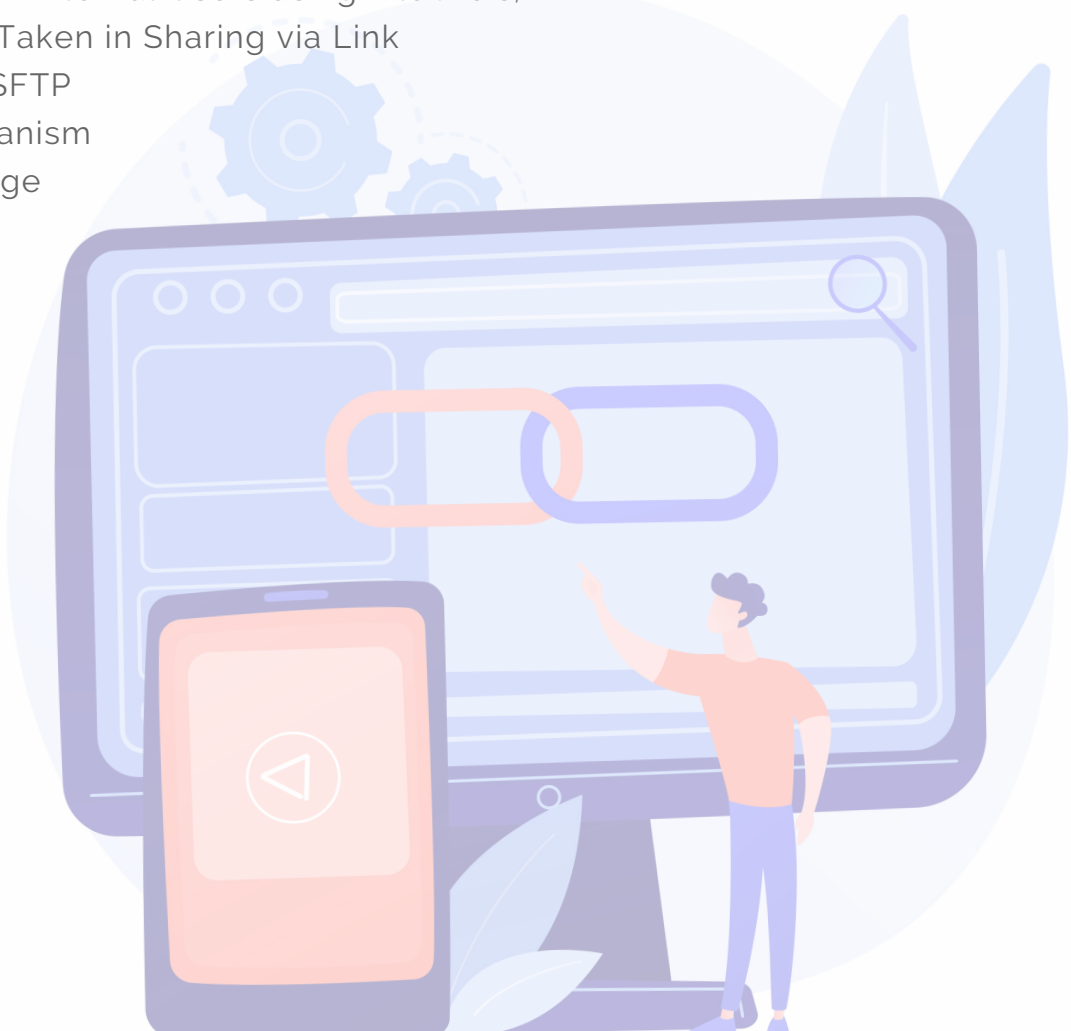
SECURE FILE SHARING BY CREATING LINK

One of the most critical issues today is to securely share corporate files and documents with internal users while sharing them with external users as well in a secure environment. Although corporates use various methods to share, it is extremely critical to provide end-to-end security control and to provide a solid structure by integrating with the existing security products of the corporate.

At this point, FileOrbis includes the security solutions used by the corporates in the process, provides an integrated structure with additional security features developed by itself, and offers the most secure methods without changing the usage habits of the users. Herein, the FileOrbis platform implements additional security controls both when sharing files/documents with external users and when receiving files/documents from external users.

Secure File Sharing with External Users using FileOrbis;

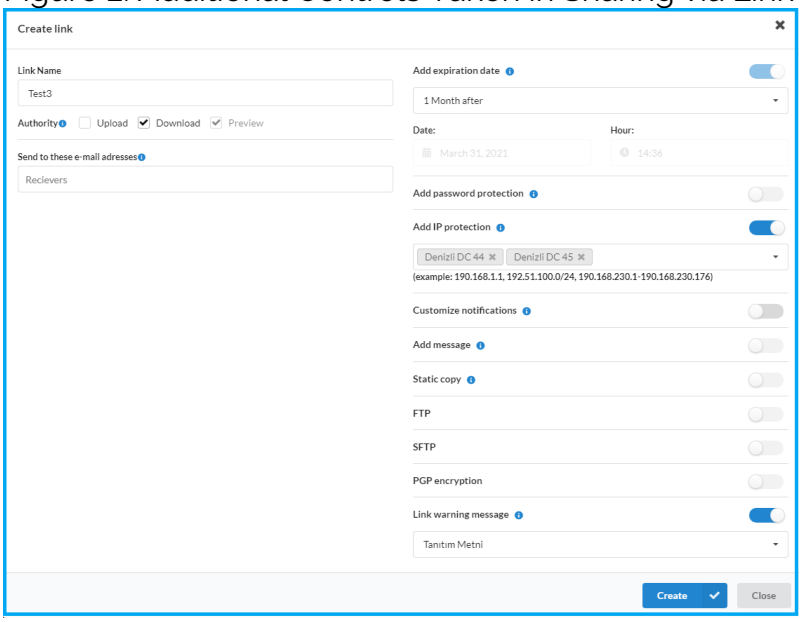
- Additional Controls Taken in Sharing via Link
- HTTP(S) / FTP(S) / SFTP
- Link Approval Mechanism
- Link Warning Message
- Watermark Feature
- Isolation Feature
- Reporting



Additional Controls Taken in Sharing via Link:

FileOrbis can provide a bidirectional exchange of files with external users. You can easily forward both files and documents to external users over a URL (HTTP / HTTPS). For this process, you can establish secure bridges with DMZ servers, as well as including all security integrations in these processes, preventing data leakage, and ensuring your data security from end to end. While allowing users to easily exchange files, you can make their access more secure with controls such as password, link expiration date, IP, warning message, approval flow at the same time.

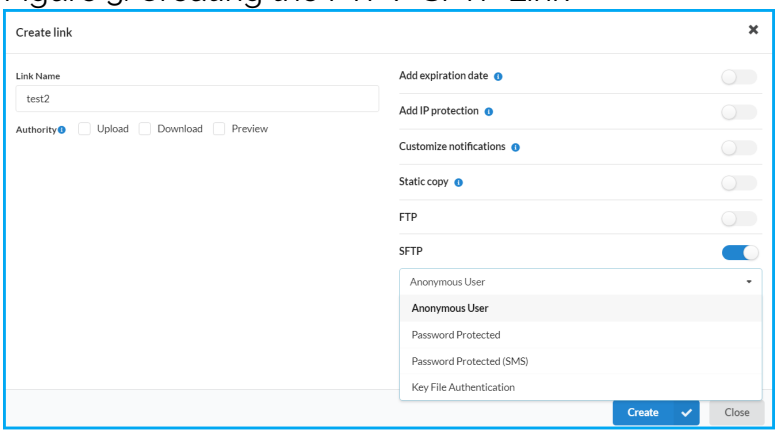
Figure 2: Additional Controls Taken in Sharing via Link



FTP/FTPS/SFTP:

As well as sending the links for which you define the restrictions and permissions to external users as HTTP/HTTPS links, you can also create ones for FTP/FTPS/SFTP protocols. Specific to the SFTP protocol, you can also access with RSA key file besides username-password. The system can generate up to 4096 bit RSA keys for you, on the other hand, you can also upload an RSA key to the system.

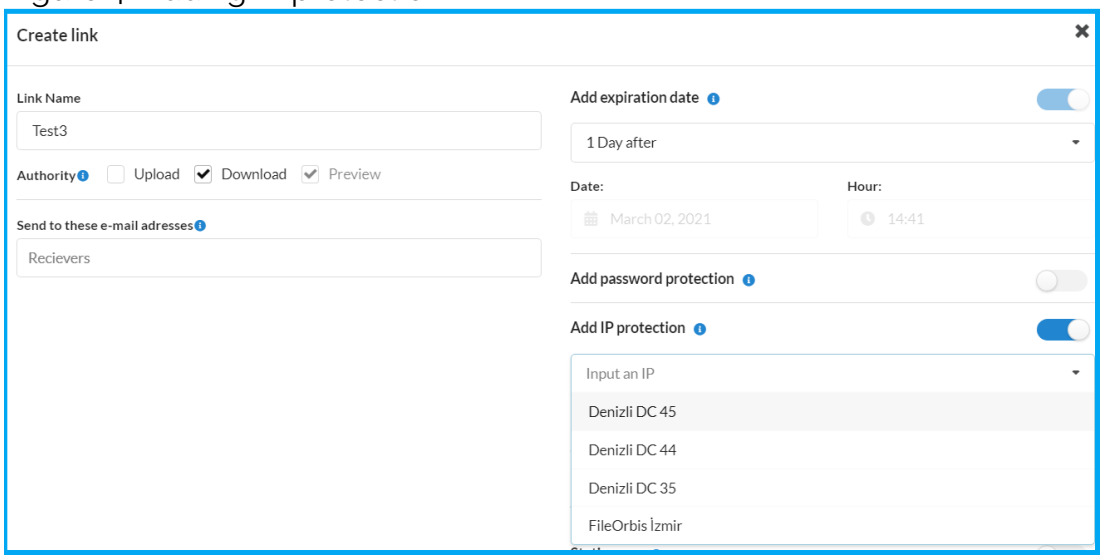
Figure 3: Creating the FTP / SFTP Link



Adding IP Protection to Link Access:

The FileOrbis IP protection feature ensures that the links created by the users can only be accessed by certain IPs. After creating a link, users can enter the IPs they want to give access to the link from the link creation screen. In particular, you can add pre-defined IPs to the pool from the administrator screen and allow users to enter the names of pre-defined IPs only.

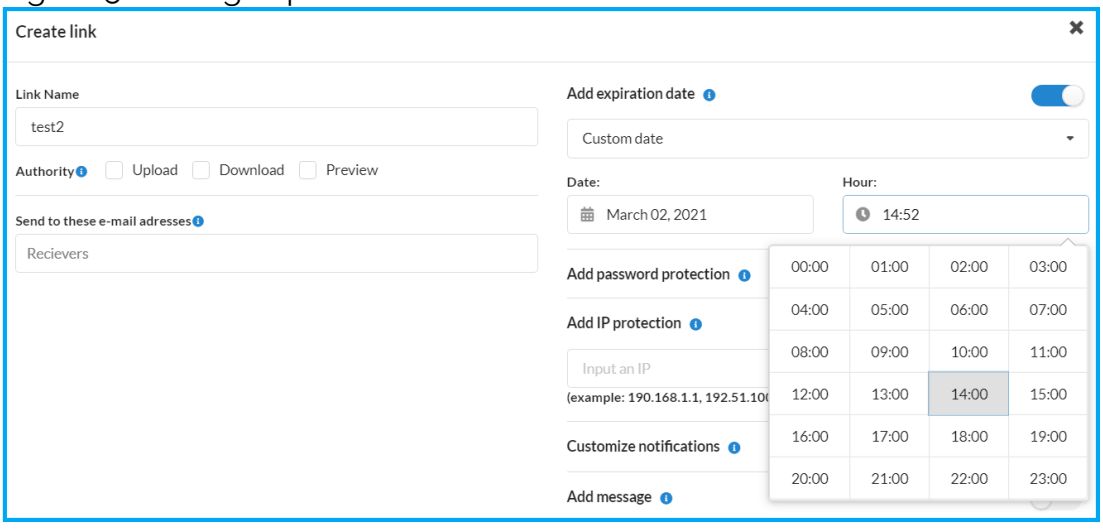
Figure 4: Adding IP protection



Adding Expiration Date to the Link:

It is a feature that allows adding expiration dates to the created links and that automatically expires the link access when the time is up. This date can be specifically set according to the day and time.

Figure 5: Adding Expiration Date



Setting a Password for Link Access by SMS or E-mail:

It is a feature that provides access to created links with instant passwords or passwords to be determined by users. For the links generated with an instant password, it ensures that the password is transmitted to the users via SMS or e-mail as soon as the link is clicked. Users who click on the link can access the link content by correctly entering the password sent to them within the specified time. The complexity of the passwords to be defined by the users to access the link can also be adjusted.

Figure 6a: Setting a Password

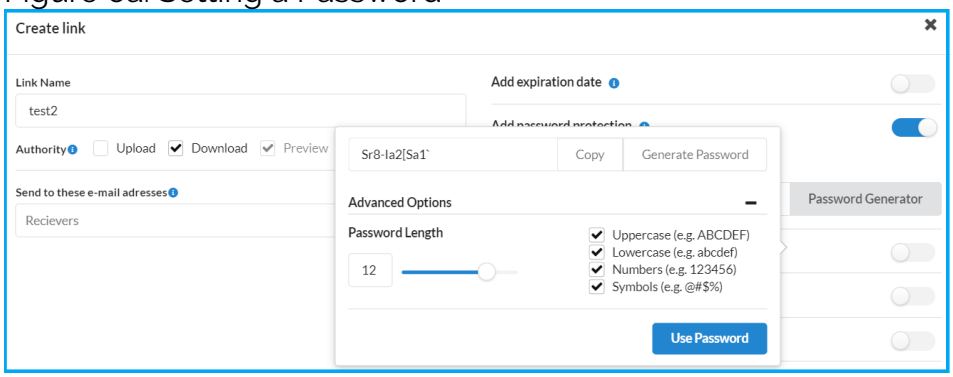
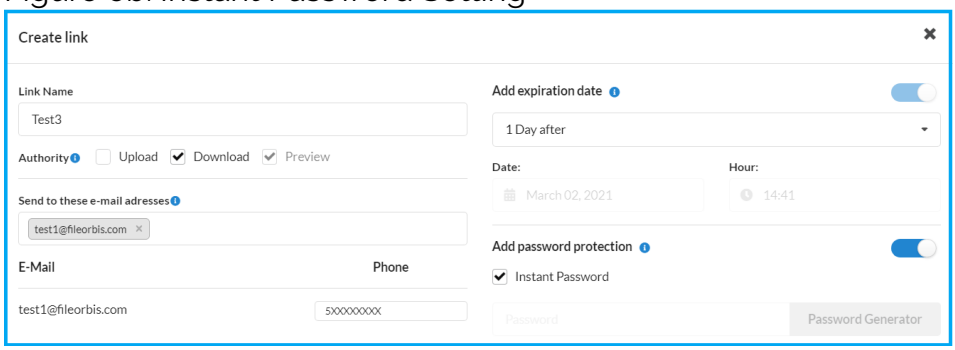


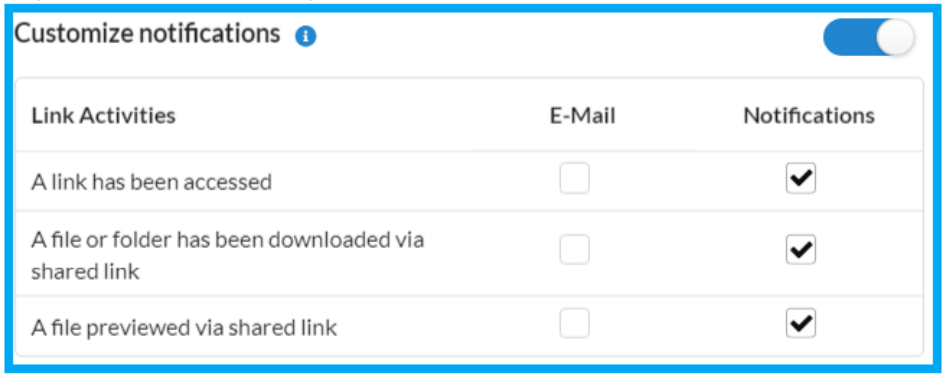
Figure 6b: Instant Password Setting



Customizing Link Notifications:

It ensures that all kinds of activities related to the links created are notified via e-mail and/or FileOrbis.

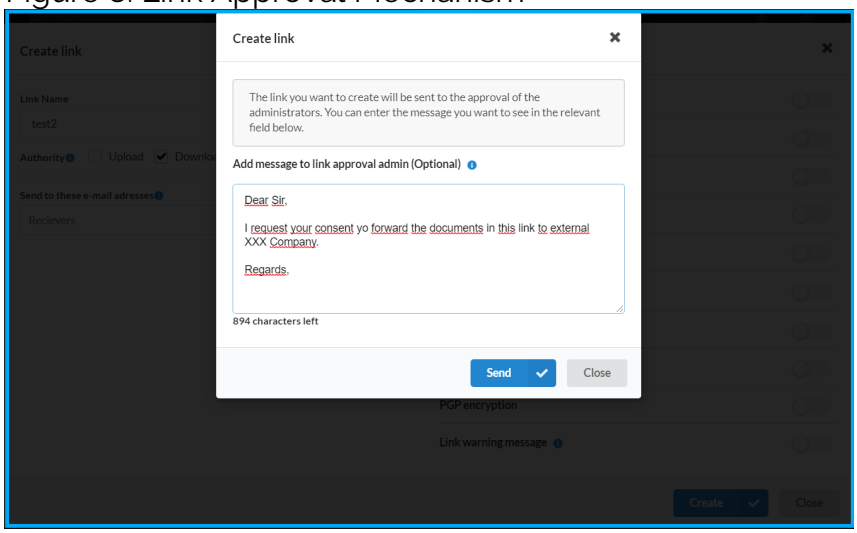
Figure 7: Customizing Notifications



Link Approval Mechanism:

FileOrbis provides easy sharing of files and folders with external users. In addition to this sharing convenience, it can also prevent incorrect or malicious access by performing content control with different integrations. One of these methods is approval control. You can put shares into approval except for predefined domains on the system. Different approval managers can be defined for each user and group, as well as automatic approval managers defined on Active Directory. Sequential approval or temporarily assigned approval flow can also be defined on FileOrbis.

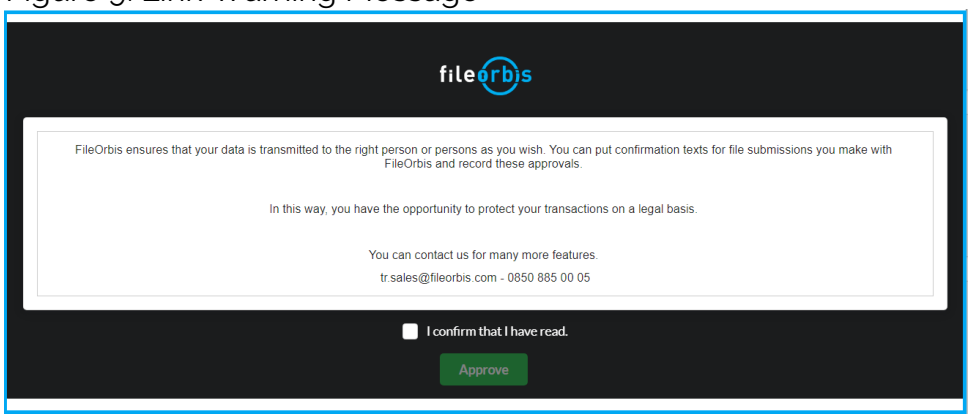
Figure 8: Link Approval Mechanism



Link Warning Message:

FileOrbis link service can show users the specified warning messages and have these messages approved. You can customize and define the warning messages according to the regulations and needs such as explicit consent, supplier data access notification, sales notification and confirmation. File access can be denied without approval and information such as the approved text itself, accessed IP, etc. are recorded. You can also forward these records to central log systems with SIEM integrations.

Figure 9: Link Warning Message



Watermark Feature:

In addition to the download and upload permission, the documents within the shared files also have preview permission. FileOrbis embedded or integrated viewers/editors can be activated for frequently used file formats such as PDF, Word, Excel, text, image, video. In this preview process, FileOrbis Watermark steps in and adds on the file a UID with different image options. This UID contains information such as IP, user, time, the file name that enables the tracking of the file. If this data is leaked by taking a screenshot, you can determine the details via this UID. Thus, it is possible to identify the first source of the leak.

Figure 10: Watermark

Isolation Feature:

FileOrbis Isolation is a kind of Digital Rights Management-DRM solution developed for domain and third-party users to securely view and edit MS Office files. The File is neither downloaded to the end-user computer nor opened with MS Office installed on the end-user computer, instead, the file is opened in a special isolated FileOrbis editor. Taking photos can be monitored by adding FileOrbis Watermark on the opened file. In FileOrbis Isolation, you can add data from the clipboard into the file you want, but it is not possible to import data to the clipboard, print the file, or save it to a local device. So, you minimize data leakage while the end-user works on MS Office files.

Reporting:

FileOrbis records 150+ operations of system administrators and users with many parameters such as contact, process, file, IP, browser, OS, interaction. FileOrbis parses all operations and internal fractures, keeping a lot of detail and allowing you to form different alarm mechanisms through these details. In addition to providing an architecture that supports integration with SIEM solutions, FileOrbis also offers these logs to the use of the admins with an easy-to-read interface. You can view the main operation log and log detail as needed and narrow your queries with the user, process, date, etc., filters. You can also download the results that you will achieve with the relevant filters as MS Excel files at that time or even have these results automatically sent in certain intervals in report form.