Forcepoint Integration with FileOrbis

Configuration Guide

Forcepoint DLP, SSE and ZT CDRaaS

Forcepoint

Table of Contents

Executive Summary **2**

Solution Overview **2**

FileOrbis Overview **3**

FileOrbis File Sharing and Collaboration Platform **4**

Forcepoint ONE Security Service Edge **5**

Forcepoint DLP and DLP SSE **6**

Forcepoint Zero Trust CDR **7**

Getting Started **8**

System Requirements 8

Intergrating Forcepoint ONE and FileOrbis **8**

Single Sign-on Steps 9

Step 1: Forcepoint ONE SSO Settings 9

Step 2: FileOrbis SSO Settings 13

Step 3: Verifying the SSO Integration 15

Configuring Forcepoint ONE Inline DLP and Malware Protection/DLP SSE Apps **17**

Policy Details in Forcepoint ONE 17

DLP Actions in Forcepoint ONE 18

Step 1: Integrating Forcepoint DLP and Forcepoint ONE with Forcepoint DLP SSE 18

Step 2: Configuring FileOrbis Policy in Forcepoint ONE 19

Step 3: Configuring DLP SSE App Rules in Forcepoint DLP 21

Step 4: Verifying DLP SSE App Rules 25

Optional: Integrating FileOrbis and Forcepoint DLP with ICAP **28**

Step 1: Configuring ICAP Settings in Forcepoint DLP Protector 28

Step 2: Configuring DLP Rules in Forcepoint DLP 29

Step 3: Configuring ICAP Settings in FileOrbis 30

Step 4: Verifying DLP ICAP Rules 32

Integrating FileOrbis and Forcepoint Zero Trust CDR **33**

Step 1: Obtain API Keys for Forcepoint Zero Trust CDR 34

Step 2: Configuring CDR Settings in FileOrbis 36

Step 3: Verifying Forcepoint Zero Trust CDR in FileOrbis 39

About the Author **42**

Executive Summary

This document highlights the integration of FileOrbis with Forcepoint, enabling secure access to applications, advanced threat protection and data security during file exchange. By leveraging the SAML integration, organizations can establish secure access through agentless or agent-based ZTNA and CASB governed by Forcepoint ONE's rules. The integration incorporates Forcepoint DLP for secure file transmission, Forcepoint CDR API for threat detection and malware protection modules within Forcepoint ONE. This integration ensures a secure and compliant environment for application access and robust defence against advanced threats.

Overall, this integration presents a remarkable opportunity for companies utilizing FileOrbis, as it enables them to securely access FileOrbis applications in adherence to the principles of Zero Trust. Moreover, it empowers them to engage in file exchange that is entirely free from the perils posed by advanced threats. By incorporating this integration, organizations can confidently conduct their file sharing activities, fully aligning with their data security policies and ensuring the utmost level of protection and trust.

Solution Overview

Instead of directly accessing FileOrbis, a seamless SAML integration has been meticulously implemented with Forcepoint ONE, ushering in a heightened level of accessibility and security. This integration enables users to access applications through the robust framework of agent-based or agentless Zero Trust Network Access (ZTNA) and Cloud Access Service Broker (CASB), all meticulously orchestrated according to the comprehensive rule set within Forcepoint ONE.

One of the notable advantages of this integration is the utilization of Forcepoint Data Loss Prevention (DLP) in conjunction with Forcepoint ONE, ensuring the safeguarding of data integrity during the critical phases of file upload and download. By capitalizing on the seamless synergy between Forcepoint DLP and Forcepoint ONE, organizations can confidently share files in accordance with their data security policies, all the while fortifying the confidentiality, integrity and availability of their valuable assets.

Moreover, to effectively combat the ever-evolving landscape of advanced threats, an added layer of security is deployed. This encompasses the seamless integration of Forcepoint CDR API (Content Disarm & Reconstruction) during both the upload and download processes. By subjecting files to thorough scrutiny and leveraging the power of advanced threat intelligence, this integration ensures that files are meticulously sanitized and stripped of any potential malicious elements, providing an uncompromising level of protection.

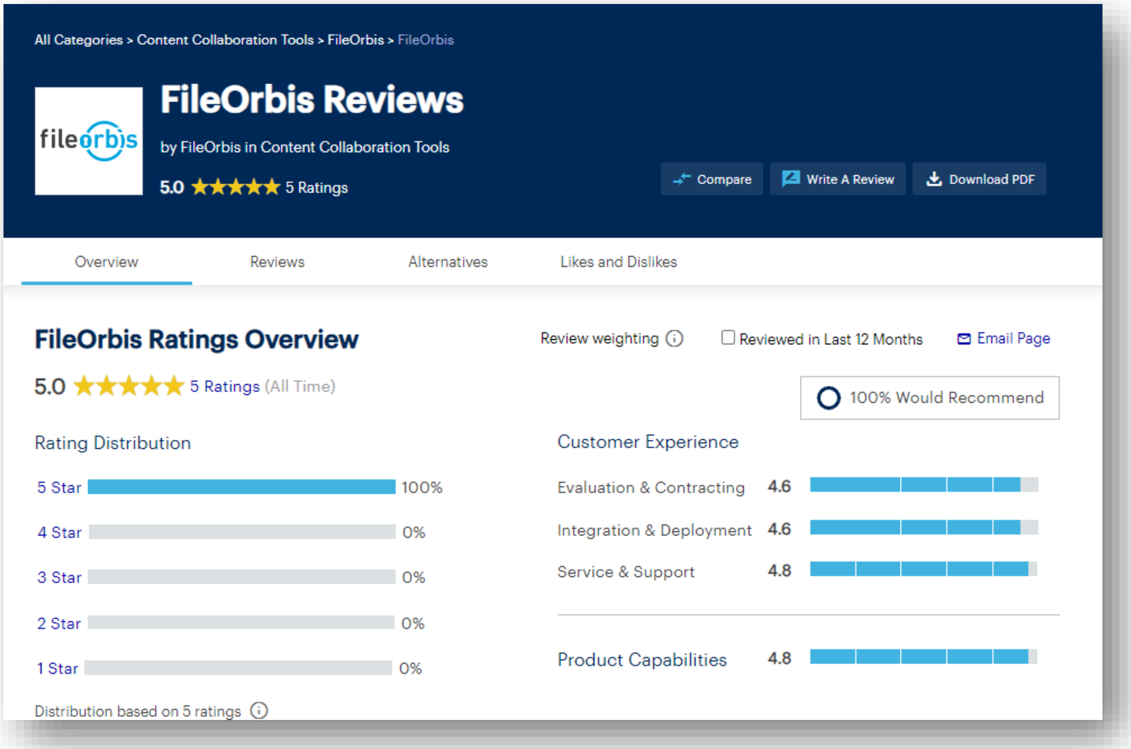
Furthermore, within the comprehensive ecosystem of Forcepoint ONE, an array of robust malware protection modules becomes available. This synergistic amalgamation of cutting-edge technologies, woven into the fabric of Forcepoint ONE, delivers an unparalleled defence against advanced threats. By incorporating these modules into the upload and download workflows, organizations can confidently operate in a highly secure environment, free from the adverse effects of sophisticated malware, and mitigate potential risks with utmost efficacy.

In summary, through the meticulous orchestration of the SAML integration with Forcepoint ONE, organizations gain the ability to securely access applications, employing both agent-based and agentless ZTNA and CASB policies, all governed by the robust rule set within Forcepoint ONE. Leveraging the powerful integration of Forcepoint DLP, Forcepoint CDR API and advanced malware protection modules, organizations can confidently upload and download files with FileOrbis, adhering to their data security policies while fortifying their defenes against the threat landscape.

FileOrbis Overview

With more than 150 enterprise customers, FileOrbis is aiming to manage the user and file relationship within an institutional framework. FileOrbis is constantly being developed to meet different industry and customer needs in terms of content management and sharing. Since 2012, FileOrbis continues to be developed with the excitement of the first day. FileOrbis focuses on high security, rich integration, ease of use and integrated management criteria to develop the most secure, integrated, fast and easy-to-use high-quality software required to meet the ever-changing needs of customers and to ensure its sustainability. It aims to be one of the first solutions that come to mind in the global market when it comes to corporate file sharing and management.

Recently FileOrbis, a leading hyper-secure content collaboration platform, has raised $2 million in funding from Revo Capital. This investment will fuel innovation and international market expansion. FileOrbis revolutionizes file and data management, empowering businesses to streamline operations and maximize digital assets. With its intelligent content management platform, users can securely store, organize, search and share files easily. Revo Capital, Turkey's largest venture capital firm, is excited to invest in FileOrbis and its exceptional team, aiming to fuel growth and technological prowess. FileOrbis strives to become a leading solution in the global content management platforms market.



All Categories > Content Collaboration Tools > FileOrbis > FileOrbis

FileOrbis Reviews

by FileOrbis in Content Collaboration Tools

5.0 ★★★★★ 5 Ratings

FileOrbis Ratings Overview

Review weighting ⓘ □ Reviewed in Last 12 Months Email Page

5.0 ★★★★★ 5 Ratings (All Time)

○ 100% Would Recommend

Rating Distribution

5 Star	100%
4 Star	0%
3 Star	0%
2 Star	0%
1 Star	0%

Distribution based on 5 ratings ⓘ

Customer Experience

Evaluation & Contracting	4.6
Integration & Deployment	4.6
Service & Support	4.8
Product Capabilities	4.8

FileOrbis File Sharing and Collaboration Platform

FileOrbis is a specialized solution designed for seamless file exchange and collaboration. It provides organizations with a secure and efficient platform to facilitate file sharing and streamline workflow processes among business partners, customers and employees.

FileOrbis is a framework for merging file servers, user profile folders, user-specific areas and network disks. It provides an access channel for all your file systems as well as an integrated management system. FileOrbis is a consolidating platform that can manage external file systems like legacy file servers or modern on-prem/cloud object storage. With FileOrbis, you both create an access channel for all your file systems and have an integrated management system. FileOrbis does not consider content management only through one perspective such as access, authorization management, file sharing, logging, etc., but helps enterprises at any point related to content management. With native content analysis capability, files are tagged and governance policies are applied based on tags.

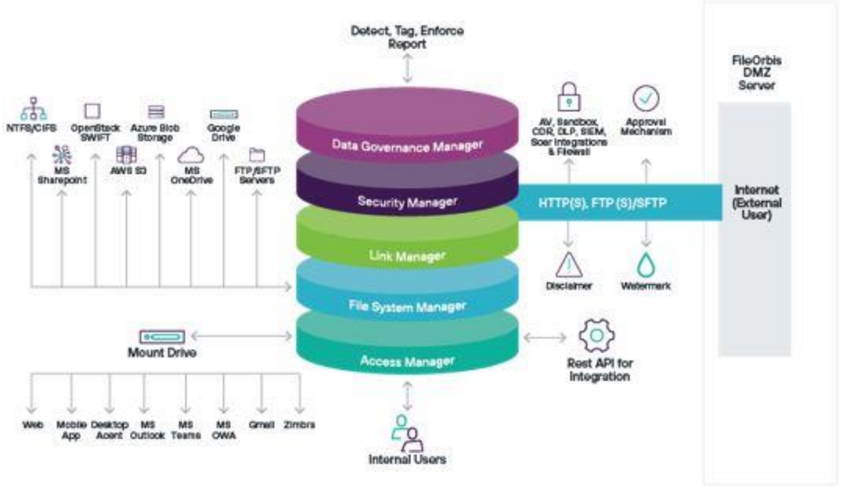
Security-Focused Approach: With a strong emphasis on security, FileOrbis offers advanced features to ensure secure file sharing. Data is encrypted, and access control mechanisms are implemented to safeguard sensitive information, enabling organizations to have peace of mind when sharing files.

Efficient Data Management: FileOrbis provides effective file management capabilities, enabling version control, tracking revision history and automating file management processes. This ensures that files are organized, easily accessible and managed efficiently.

Integration Capabilities: FileOrbis seamlessly integrates with existing workflows and systems, allowing for smooth data exchange with other applications. This integration enhances productivity and improves efficiency by eliminating the need for manual data transfer between different platforms.

Traceability and Reporting: FileOrbis offers robust traceability and reporting features, allowing organizations to track file activities and user interactions. This facilitates compliance requirements and provides audit trails for monitoring and reporting purposes.

FileOrbis is an on-premises/on-cloud content management system equipped with unique operation and control features allowing companies to:



- Enforce security scans and controls on your files.
- Conduct content and sensitive data analysis on your files.
- Share your files with internal and external users.
- Manage permissions and access for your files.
- Access your files from everywhere.

Forcepoint ONE Security Service Edge

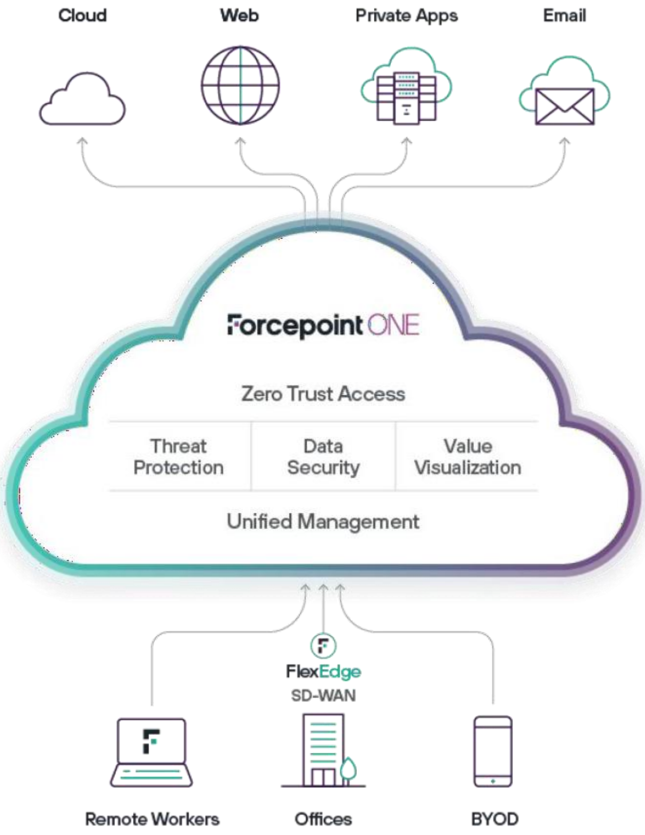
Forcepoint ONE is an all-in-one cloud platform that simplifies security for distributed organizations with remote and hybrid workers. It gives employees, contractors and other users safe, controlled access to business information everywhere – on the web, in cloud services and in private applications – while keeping attackers out and sensitive data in. Forcepoint ONE delivers this security from one unified cloud platform that integrates Zero Trust and SASE Security Service Edge (SSE) technologies so that organizations can manage one set of policies, in one console, with one endpoint agent. As a result, Forcepoint ONE makes users more productive, whether remote or in the office, and businesses more efficient.

Forcepoint SSE combines Zero Trust and SASE security technologies, including three secure access gateways and a variety of shared threat protection and data security services, all built on a cloud-native platform.

- **Secure Web Gateway (SWG)** monitors and controls any interaction with any website, including blocking access to websites based on category and risk score, blocking download of malware, blocking upload of sensitive data to personal file sharing accounts and detecting and controlling shadow IT. It is currently available as agent-based software for Windows and macOS.

- **Cloud Access Security Broker (CASB)** is an agent-based or agentless solution that enforces granular access to company SaaS based on identity, location, device and group. It blocks download of sensitive data and blocks upload of malware in real time. It also scans data at rest in popular SaaS and IaaS for malware and sensitive data and remediates as needed. The agentless option facilitates BYOD and contractor access.

- **Zero Trust Network Access (ZTNA)** is an agent-based or agentless solution that allows granular access to private applications without the use of a VPN. The agent-based solution is required for non-HTTP/S applications.



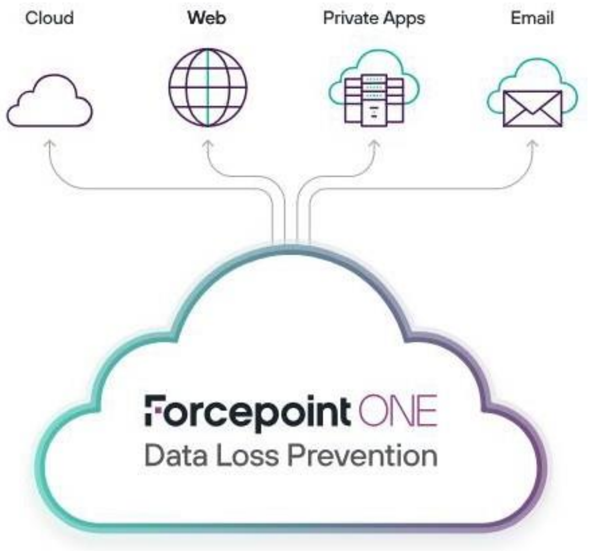
Forcepoint DLP and DLP SSE

Forcepoint DLP is the industry's most trusted solution, giving you the tools to easily manage global policies across every major channel, whether endpoint, network, cloud, web, private applications or email. We can simplify your work with the most pre-defined templates, policies and classifiers of any DLP provider in the industry. This can dramatically streamline your incident management so you can focus on what's most important, eliminating risk so that your people can be increasingly productive. Forcepoint DLP addresses risk by bringing you visibility and control everywhere your people work and anywhere your data resides.

By connecting Forcepoint Enterprise DLP to the Forcepoint ONE Security Service Edge (SSE) platform, customers can extend a new or existing enterprise DLP policy, including its advanced classifiers, data fingerprinting and enforcement settings, to the web and cloud. A unified security policy from Forcepoint protects sensitive data across all channels, including endpoints, websites, cloud services, networks, email and private apps. Forcepoint's data-first approach goes far beyond basic data protection that is often built into SASE solutions. By classifying data and organizing it into different groups rather than relying on hardcoded patterns, Forcepoint data security policies can be written once and enforced everywhere to automatically handle new instances and types of sensitive data. This end-to-end enforcement is ideal for organizations with cloud-based applications or distributed workforces.

The Data Security Everywhere approach makes a huge difference. Now you can deploy Forcepoint ONE with your Forcepoint Enterprise DLP with just a few simple clicks. You will have access to all your organization's policies immediately, all managed from within the Forcepoint Security Manager (FSM). This centralizes things so you can manage all those channels (endpoint plus CASB, SWG, ZTNA, email, network) directly from your FSM policies – one policy covering all channels.

It also means you have a single portal to manage DLP incidents and forensics. Instead of managing two (or more) separate DLPs, you can continue to use your industry-leading Enterprise DLP and your SSE channels the way you are accustomed to – all within minutes. This time savings alone can amount to hundreds of thousands of dollars. Most importantly, it will also save your organization much more in terms of preventing data loss in today's complex security and compliance environment.



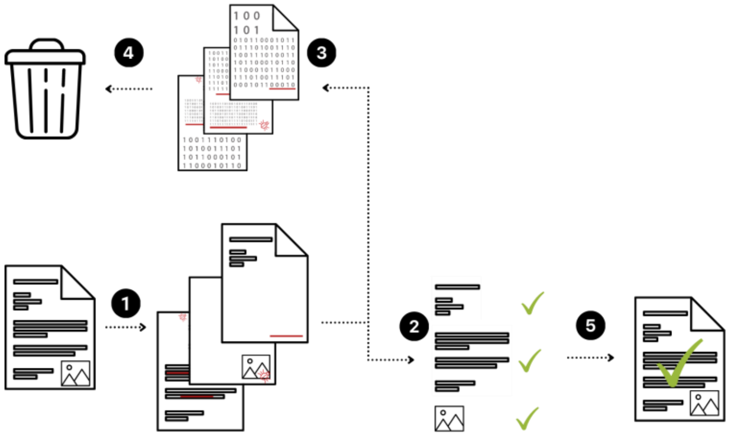
Key Benefits of Enforcing Data Security Everywhere

- Adds Forcepoint ONE SSE channels to Forcepoint Enterprise DLP, protecting data across any website, cloud application and web-based private applications.
- Applies new or existing DLP policies across CASB, SWG and ZTNA channels.
- Simplifies DLP management by leveraging over 1,700 out-of-the-box classifiers, policies and templates enabling granular enforcement for files.
- Gives security operations center (SOC) and IT teams complete incident reporting and forensic information from a single management console.

Forcepoint Zero Trust CDR

Zero Trust CDR technology is a game- changer in cybersecurity, using a three-stage Extract, Verify and Build process to deliver 100% malware-free data.

Rather than trying to detect malware, Zero Trust CDR assumes that nothing can be trusted. It works by extracting the valid business information from files, verifying the extracted information is well-structured, and then building new, fully functional files to carry the information to its destination. Zero Trust CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits.



1. Rather than identifying known malware, Zero Trust CDR takes the data and extracts the useful information from it.
2. The extracted information is transformed into an intermediary format. This advanced threat protection and ransomware prevention process makes sure no threats or attacks can reach the next stage.
3. The original data is stored or discarded, along with any malware – known or unknown.
4. Brand new data is then built in a normalized way, containing the verified information.
5. The new data replicates the original data without the threat of embedded malware and is now guaranteed to be safe.

Forcepoint Zero Trust CDR as a Service

Data – documents and images – is the preferred carrier for every conceivable kind of evasive and zero-day threat. To date the remedy has been detection-based antivirus (AV) tools, but they are trivially easy for cyber criminals to evade. It’s time to retire AV and find a better way. Zero Trust CDR as a Service (CDRaaS) is the cloud-based service for any workflow or application that needs to take data, documents and images from an untrusted source and transform it into threat-free content. Accessed via an API, there’s no scanning, no sandboxing and no waiting. CDRaaS is the fast and foolproof way to guarantee business information is free of known, evasive, zero-day and even unknown threats.

Getting Started

This section provides a high-level overview of the integration process. In this section, we will outline the stages step by step of integration between FileOrbis and Forcepoint ONE, Forcepoint DLP and CDR. We will evaluate the DLP integration with both ICAP and DLP SSE Apps options. If the organization has only Forcepoint DLP and FileOrbis solutions, we will utilize the ICAP integration. If the organization has Forcepoint ONE, FileOrbis and Forcepoint DLP solutions, they can directly utilize the Cloud DLP infrastructure instead of ICAP.

System Requirements

Ensure that the following products are already installed and configured.

- Forcepoint
  - Forcepoint DLP V10 (integrated with Forcepoint ONE)
  - Forcepoint ONE Cloud Edition
  - DLP SSE Apps DLPCONSSE
  - Zero Trust Cloud CDR API
  - Smart Agent
- FileOrbis
  - File Sharing Platform

Integrating Forcepoint ONE and FileOrbis

(Security Assertion Markup Language (SAML) is a standard for exchanging authentication information between an identity provider (IdP) and a service provider (Forcepoint). SAML-based single sign-on allows seamless user identification and authentication for end users, using your preferred IdP. When a SAML 2.0-compliant IdP has been configured, policy rules or exceptions that require user identity trigger an authentication request for clients whose identity is not already known to the service. The client request is redirected to the configured IdP for authentication. FileOrbis support SAML 2.0 and can easily integrate with Forcepoint ONE’s SSO solution. FileOrbis also support user authentication such as AD, LDAP, Windows, Radius, OAuth 2.0 and SSO.

Forcepoint ONE serves as a SAML-based identity provider (IdP) and manages identity authentication services and integrates with identity providers using the SAML protocol. Through this integration, Forcepoint ONE can verify user authentication information and authorization status. When an organization integrates Forcepoint ONE with SAML, Forcepoint ONE acts as the IdP. The organization's existing SAML-compliant identity providers transfer user identity information to Forcepoint ONE. Forcepoint ONE authenticates users and makes authorization decisions. Users can securely access resources through Forcepoint ONE via this integration. In summary, Forcepoint ONE is a SAML-integrated identity provider that uses the SAML protocol to manage authentication and authorization processes.

Through this integration, FileOrbis access will be secured with Forcepoint ONE. Additionally, it will provide access to applications under the agentless CASB and Zero Trust Network Access (ZTNA) framework.

Single Sign-on Steps

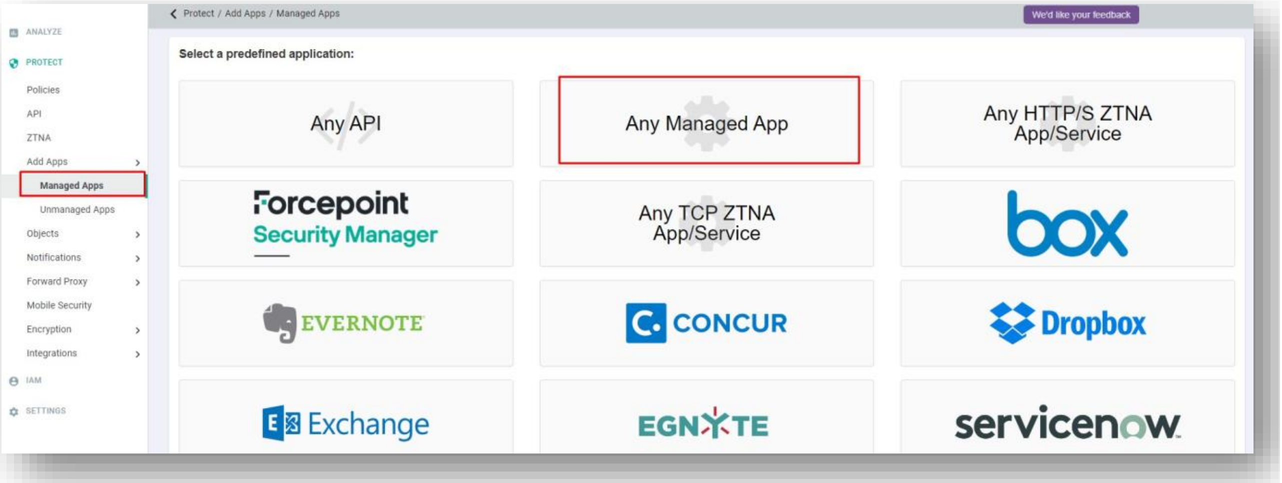
This covers the steps that users take to log in to the FileOrbis application with SSO.

- The user tries to access the FileOrbis application URL and clicks on the login with the “SAML Configuration Name” button.
- FileOrbis generates a SAML Authentication request and redirects the browser to the Forcepoint ONE SSO URL.
- The Forcepoint ONE SSO service authenticates the user when presented with valid login credentials.
- The Forcepoint ONE SSO service generates a valid SAML response and returns the information to the user’s browser.
- The Forcepoint ONE SAML response is redirected to FileOrbis.
- The FileOrbis authentication module verifies the SAML response.
- If the user is successfully authenticated and the user account exists in the system (both FileOrbis and Forcepoint ONE), the user will be successfully logged into FileOrbis.

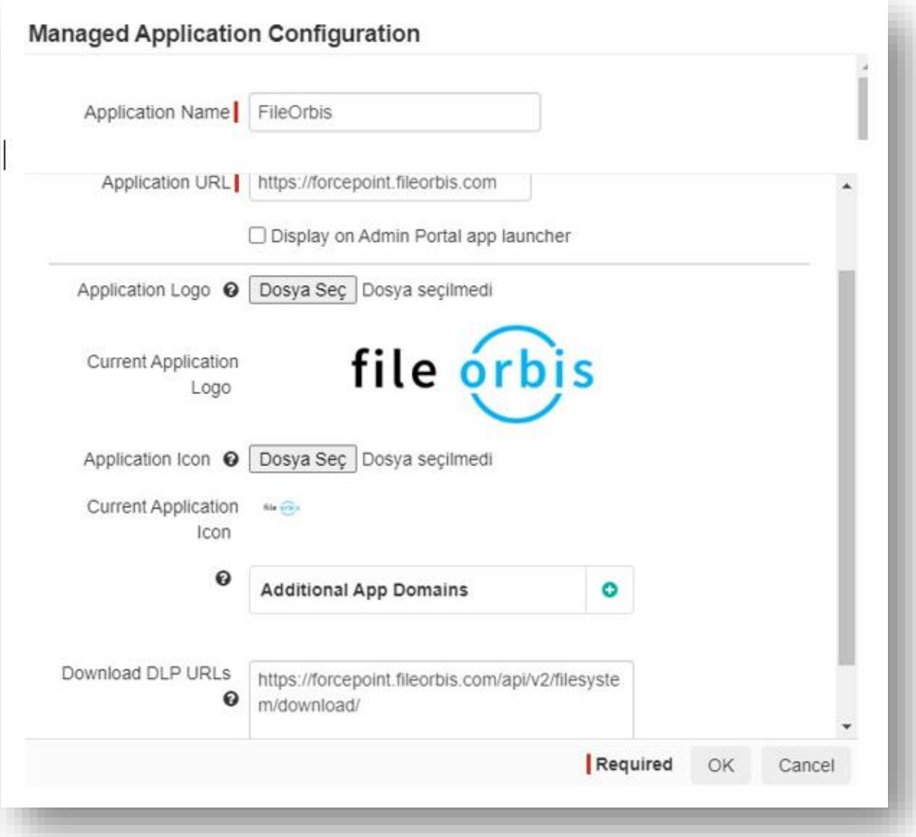
Step 1: Forcepoint ONE SSO Settings

The “Any Licensed Application” option allows customers to add SaaS applications that are not part of Forcepoint ONE’s current list of pre-defined applications. This includes any cloud applications as well as any custom applications that customers may have developed on their own servers, datacenters or IaaS/PaaS systems.

- Log in to the Forcepoint ONE portal as an admin and go to Protect > Add Apps > Managed Apps and select "Any Managed App."



- Enter the "Application Name," the "URL for the Application," upload a logo if applicable, then you can choose to enter other domains if you have more than one that is using the new application, and finally set "Download DLP URLs" that define search patterns for which URLs are related to file downloads.
  - Note: The application URL and Download DLP URL will be provided by FileOrbis.



Managed Application Configuration

Application Name: FileOrbis

Application URL: https://forcepoint.fileorbis.com

□ Display on Admin Portal app launcher

Application Logo: Dosya Seç Dosya seçilmedi

Current Application Logo

Application Icon: Dosya Seç Dosya seçilmedi

Current Application Icon

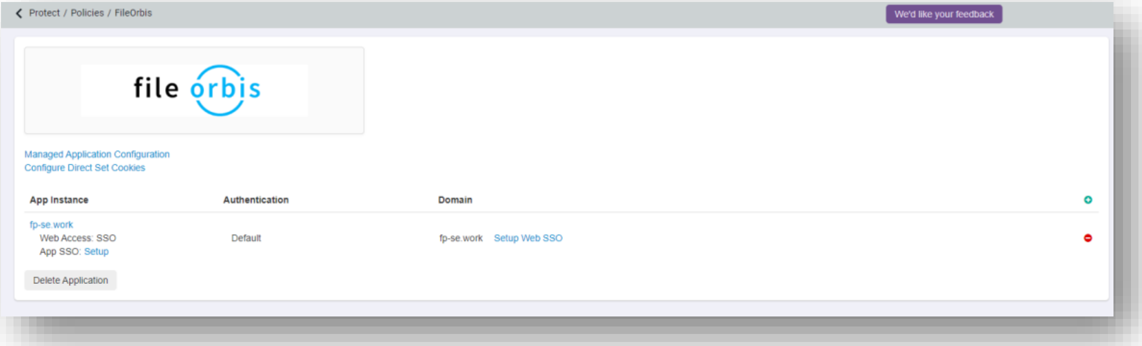
Additional App Domains

Download DLP URLs: https://forcepoint.fileorbis.com/api/v2/filesystem/download/

Download DLP URLs

Forcepoint ONE inspects the Content-Disposition header for URLs that are related to file downloads, making it possible to inspect the file and then apply DLP. Most applications set or provide this Content- Disposition header, and no additional configuration is required. However, if you have added an application (whether an existing SaaS app or a custom app) and download DLP is not working, it is likely because this Content-Disposition header is not being provided and you will need to input the search patterns designating which URLs are related to file downloads. The best way to figure out what these patterns are is to open up your network diagnostics in your browser, record the traffic and then click in the application to initiate a download. Review the network traffic and input the URL used for the download. https://yourFileOrbisurl/v2/filesystem/download

- After you finish filling out the information, click "OK" and then "Save.”

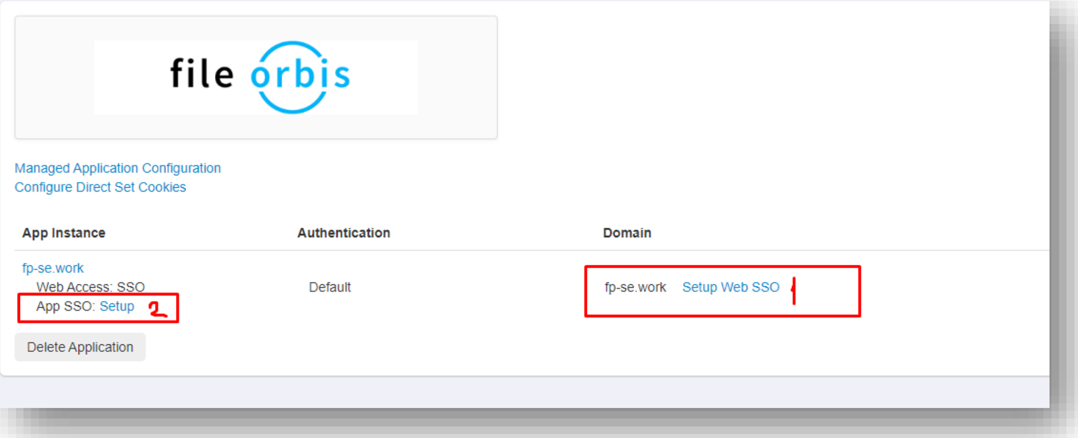


Protect / Policies / FileOrbis

Managed Application Configuration
Configure Direct Set Cookies

App Instance	Authentication	Domain
fp-se.work Web Access: SSO App SSO: Setup	Default	fp-se.work Setup Web SSO

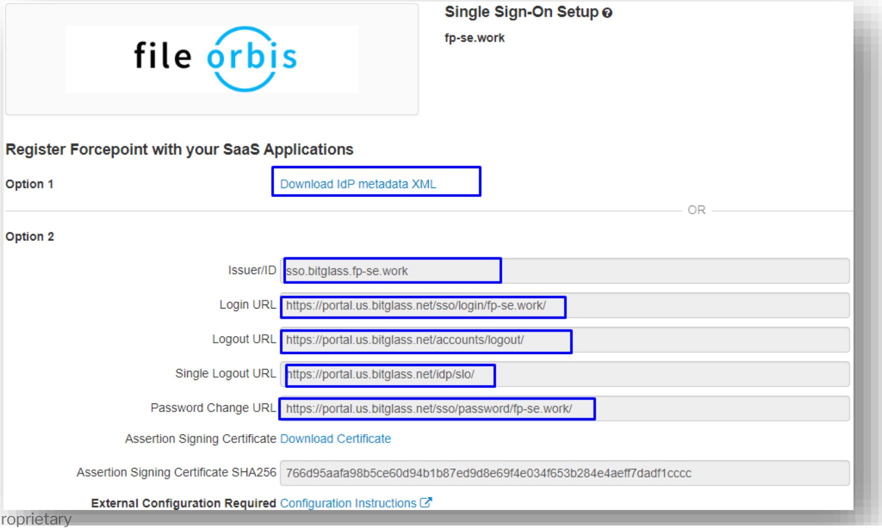
- If you choose to enable SAML SSO cutoff, you will need to register Forcepoint ONE with your custom application to recognize Forcepoint ONE as the SSO authority.



Managed Application Configuration
Configure Direct Set Cookies

App Instance	Authentication	Domain
fp-se.work Web Access: SSO App SSO: Setup 2	Default	fp-se.work Setup Web SSO 1

- After you save, select "Setup Web SSO" to go to the SSO instructions page containing the URLs you will need for registering Forcepoint ONE inside of your FileOrbis applications. Save the URLs and download the Certificate and IDP metadata XML file, which you will need for FileOrbis settings.
  - Please note that the below URLs depend on your Forcepoint ONE application tenant and will be different from this one.



Single Sign-On Setup
fp-se.work

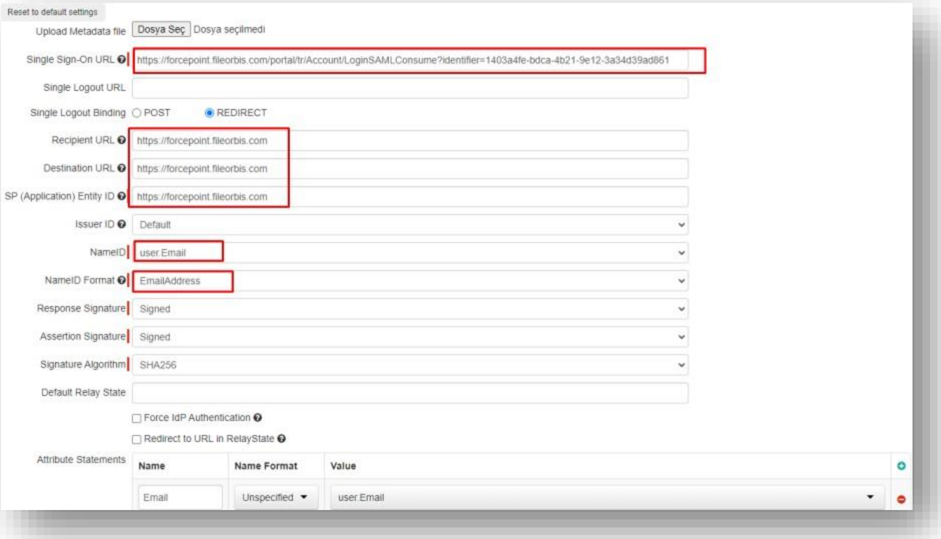
Register Forcepoint with your SaaS Applications

Option 1 Download IdP metadata XML

OR

Option 2

Issuer/ID: sso.bitglass.fp-se.work
Login URL: https://portal.us.bitglass.net/sso/login/fp-se.work/
Logout URL: https://portal.us.bitglass.net/accounts/logout/
Single Logout URL: https://portal.us.bitglass.net/idp/slo/
Password Change URL: https://portal.us.bitglass.net/sso/password/fp-se.work/
Assertion Signing Certificate: Download Certificate
Assertion Signing Certificate SHA256: 766d95aafa98b5ce60d94b1b87ed9d8e69f4e034f653b284e4aeff7dadf1cccc
External Configuration Required: Configuration Instructions



Reset to default settings

Upload Metadata file: Dosya Seç Dosya seçilmedi

Single Sign-On URL: https://forcepoint.fileorbis.com/portal/tr/Account/LoginSAMLConsume?identifier=1403a4fe-bdca-4b21-9e12-3a34d39ad861

Single Logout URL:

Single Logout Binding: ○ POST ● REDIRECT

Recipient URL: https://forcepoint.fileorbis.com

Destination URL: https://forcepoint.fileorbis.com

SP (Application) Entity ID: https://forcepoint.fileorbis.com

Issuer ID: Default

NameID: user.Email

NameID Format: EmailAddress

Response Signature: Signed

Assertion Signature: Signed

Signature Algorithm: SHA256

Default Relay State:

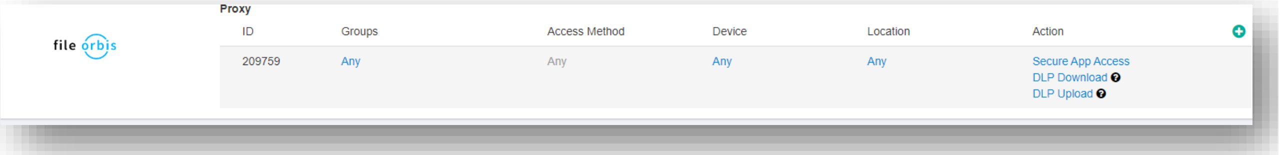
□ Force IdP Authentication

□ Redirect to URL in RelayState

Attribute Statements

Name	Name Format	Value
Email	Unspecified	user.Email

- Once the setup is complete, you will need to set up a Forcepoint ONE policy to have an admin or user access the application via Direct App Access once. This will validate the SSO authentication with the application and Forcepoint ONE.



file orbis

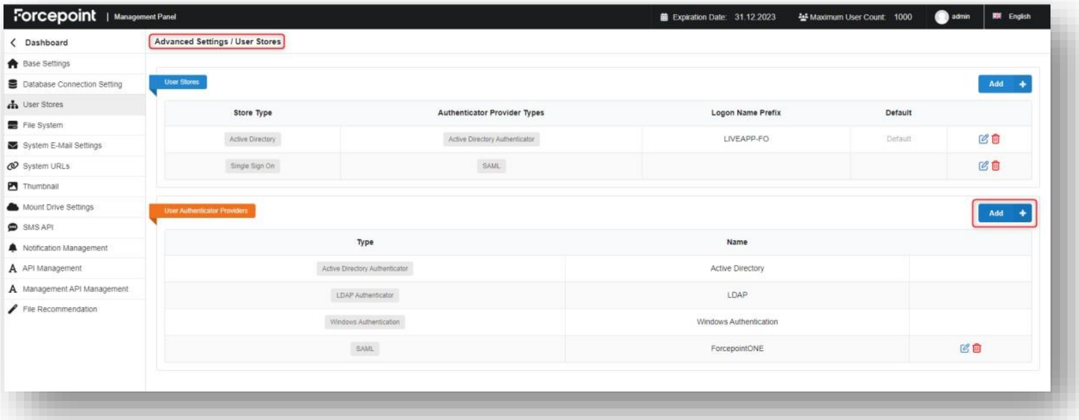
Proxy

ID	Groups	Access Method	Device	Location	Action
209759	Any	Any	Any	Any	Secure App Access DLP Download DLP Upload

Step 2: FileOrbis SSO Settings

After Forcepoint configuration completion, FileOrbis configuration can be completed as follows.

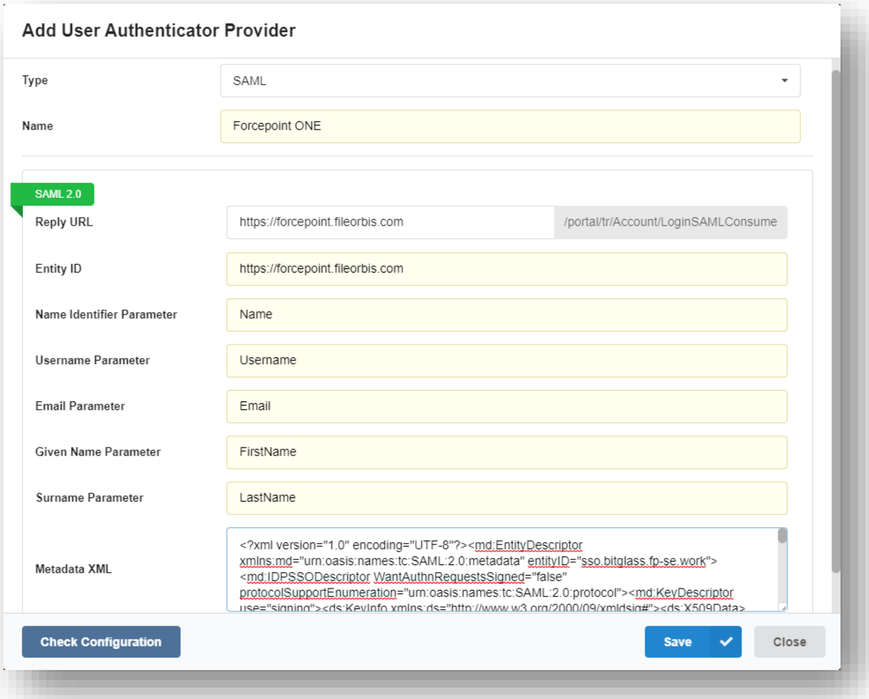
- Log in to FileOrbis, type “https://hostname:85” and press enter, then log in to the FileOrbis administration panel by entering the administrator account name and password. In SAML 2.0 or OAuth 2.0 integrations, the Single Sign-on user resource must be added to the system to ensure automatic login. Click on the highlighted “Add” button.



Store Type	Authenticator Provider Types	Logon Name Prefix	Default
Active Directory	Active Directory Authenticator	LIVEAPP-FO	Default
Single Sign On	SAML		

Type	Name
Active Directory Authenticator	Active Directory
LDAP Authenticator	LDAP
Windows Authentication	Windows Authentication
SAML	ForcepointONE

- In the pop-up, SAML must be selected in the type of field, and a suitable name must be given in the name line. The required fields are filled out as indicated below. In the MetaDataXML section, define the metadata xml information in Step 5. The Reply URL and Entity ID URL addresses should be your own app's address.

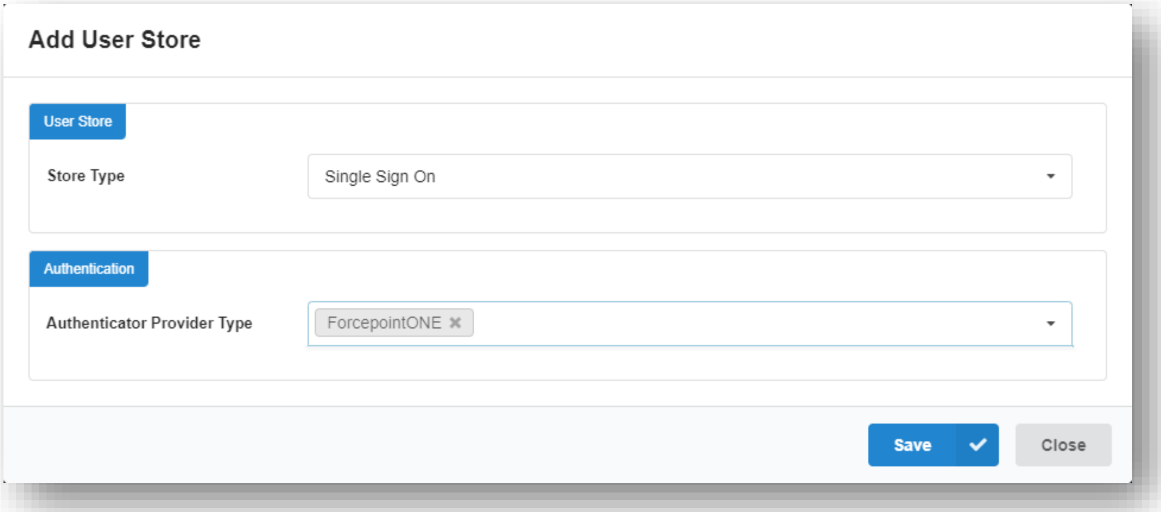


Type	SAML
Name	Forcepoint ONE
Reply URL	https://forcepoint.fileorbis.com /portal/tr/Account/LoginSAMLConsume
Entity ID	https://forcepoint.fileorbis.com
Name Identifier Parameter	Name
Username Parameter	Username
Email Parameter	Email
Given Name Parameter	FirstName
Surname Parameter	LastName
Metadata XML	<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="sso.bitglass.fp-se.work"><md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data>

- You can verify the operation was successful by clicking the “Check Configuration” button. After doing so, the FileOrbis system will be properly configured to use Forcepoint ONE SSO as an authentication source for users. The changes you made to the configuration will appear as the very last line. The necessary details are explained in the table below.

Atributes	Description
Reply URL	FileOrbis Application SAML consuming URL information
Entity ID	Customer's application URL
Name Identifier Parameter	Identifier of the user in the SAML reply
Username Parameter	The login name of the user in the SAML reply
Email Parameter	The email information of the user in the SAML reply
Given Name Parameter	Name of the user in the SAML reply
Surname Parameter	The surname of the user in the SAML reply
Metadata XML	Content of the Federation Metadata XML file downloaded from SAML settings in Forcepoint ONE

NOTE: The SAML authenticator provider can be used on Active Directory, LDAP, Azure AD and Single Sign-on user sources. A SAML configuration entered into the system can only be connected to one user resource.



Add User Store

User Store

Store Type: Single Sign On

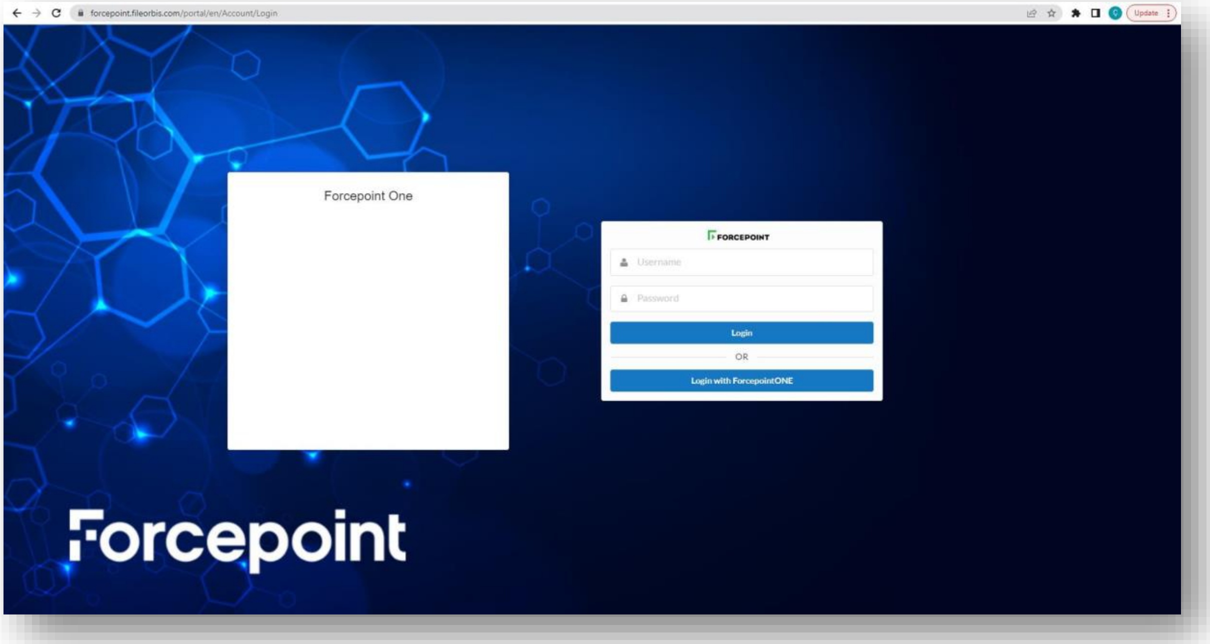
Authentication

Authenticator Provider Type: ForcepointONE

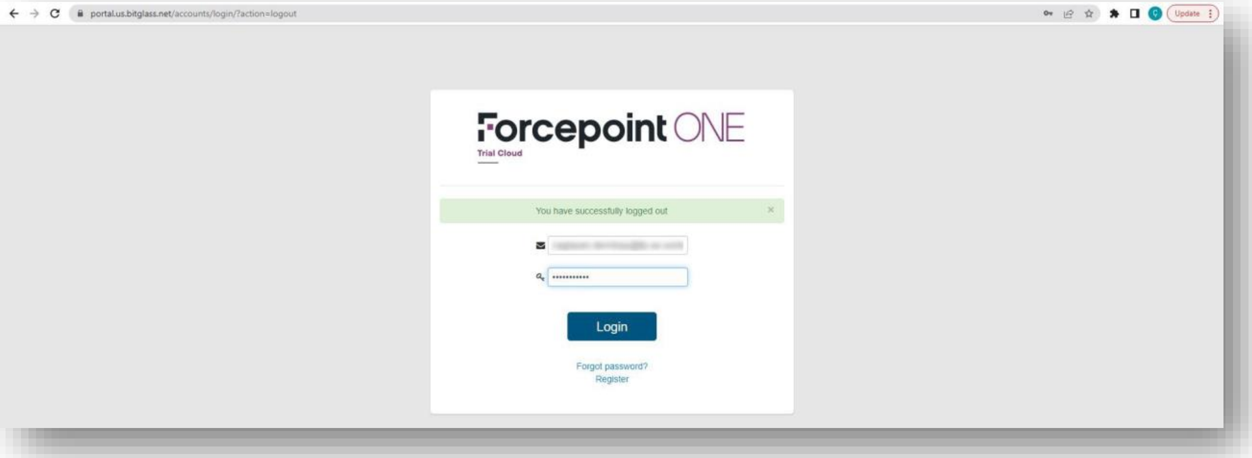
- Once the Forcepoint ONE SSO source has been added, you can add the user source. To do so, select the appropriate options in the pop-up window that appears after clicking the blue Add button in the top right corner, and then click the Save button. As soon as saving is complete, the window will close automatically. As a result, the settings you've made will be available via FileOrbis.

Step 3: Verifying the SSO Integration

Once the integration between Forcepoint ONE and FileOrbis is successfully completed and functioning properly, users are directed to the FileOrbis portal. From there, they can click on the "Login with Forcepoint ONE" button, which triggers the policy enforcement mechanism and forwards them to the Forcepoint ONE Zero Trust Network Access (ZTNA) portal.

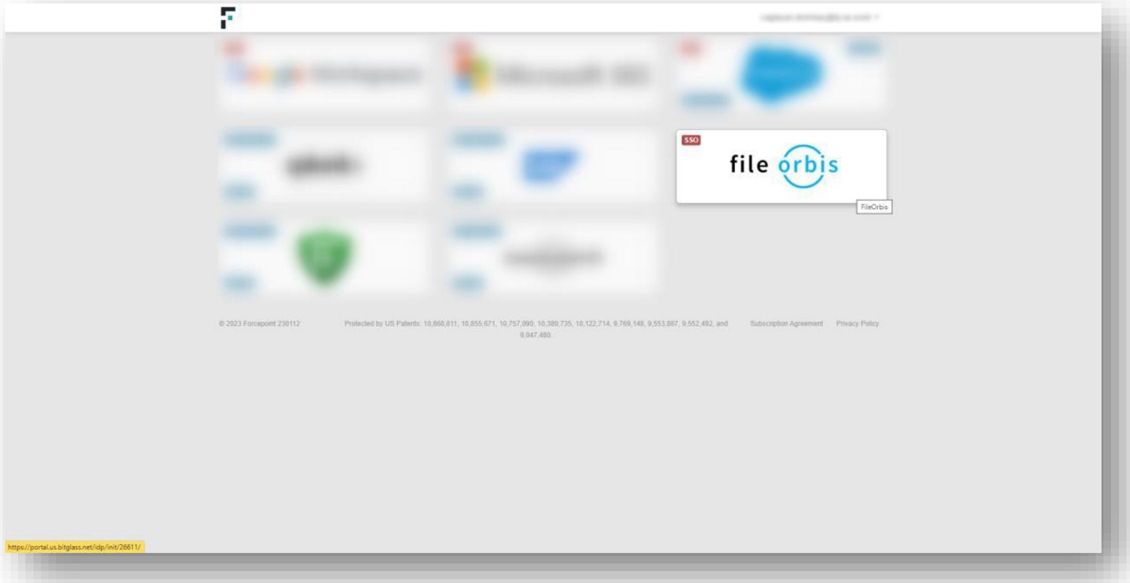

forcepoint.fileorbis.com/portal/en/Account/Login

Forcepoint ONE will request the input of a username and password, which will then be verified by the identity provider. In this scenario, Forcepoint ONE is configured as the Identity Provider solution. It is necessary for the user information to exist in both platforms. Specifically, the email addresses are used as a means of matching the user data. Initially, it is assumed that the corresponding user is defined within the Forcepoint ONE IAM portal.

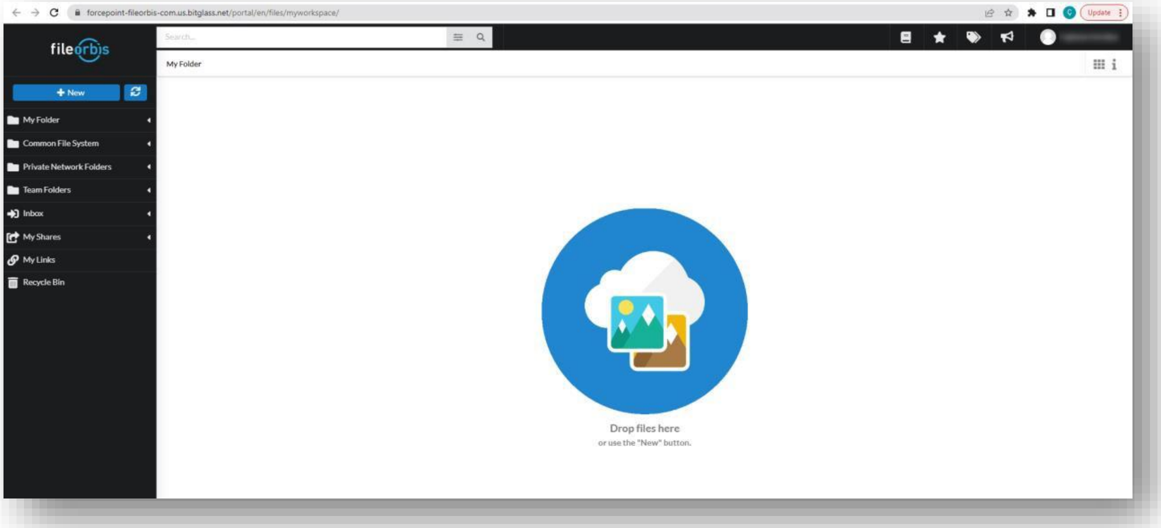

portal.us.bitglass.net/accounts/login/?action=logout

You have successfully logged out

After logging in to the Forcepoint ONE ZTNA portal, you will be able to view the FileOrbis application, as illustrated below.


SSO
file orbis
FileOrbis
© 2023 Forcepoint 230112
Protected by US Patents: 10,868,811, 10,855,671, 10,757,090, 10,389,735, 10,122,714, 9,769,148, 9,553,867, 9,552,492, and 9,047,480.
Subscription Agreement
Privacy Policy
https://portal.us.bitglass.net/idp/init/26611/

Upon clicking the FileOrbis button, you will be redirected back to FileOrbis's portal in a short period of time. This process ensures the implementation of granular data security, file security, visibility and access control for FileOrbis through the enforcement rules of Forcepoint ONE CASB.



Configuring Forcepoint ONE Inline DLP and Malware Protections / DLP SSE Apps

Once the Single Sign-on (SSO) authentication has been successfully validated, you can utilize SSO access control and perform inline Data Loss Prevention (DLP) actions for both upload and download activities. To apply DLP actions, you will select the Secure App Access option, which connects users to applications through Forcepoint ONE's proxy. Consequently, users are implicitly denied direct access to the cloud application. This configuration allows for the implementation of data leakage prevention measures.

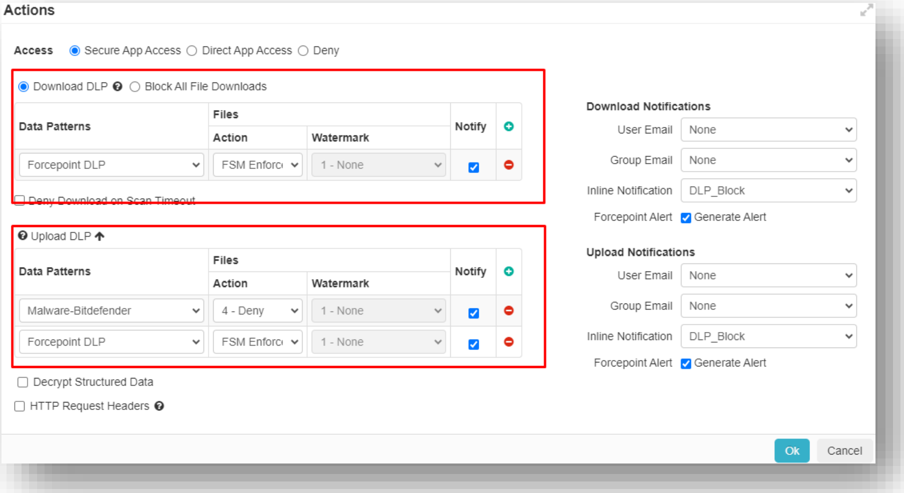
Forcepoint ONE SSE offers DLP patterns that can be utilized to control file uploads and downloads within FileOrbis. These control methods can be achieved through two different approaches, based on the policies defined within Forcepoint DLP. The first method involves leveraging the combined capabilities of Forcepoint ONE, Forcepoint DLP and the Forcepoint DLP SSE App module. The second method entails integrating Forcepoint DLP with FileOrbis through the Internet Content Adaptation Protocol (ICAP). In this guide, we will focus on evaluating the first option, which involves utilizing the Forcepoint DLP SSE Apps module (DLPCONSSE).

Policy Details in Forcepoint ONE

Once Forcepoint ONE and Forcepoint DLP are connected via the Forcepoint DLP SSE Apps module, you can use the Forcepoint DLP data pattern while configuring CASB policies for FileOrbis. Refer to Configuring contextual access control and Configuring proxy policy actions to create a policy or edit an existing one.

While creating CASB policies, if you select Forcepoint DLP as the data pattern in any of the Actions dialog for Secure App Access, then:

- The “FSM Enforced” option gets populated in the Action field as the action is configured on the FSM. This is the only option available for selection.
- If an action other than “Allow” that is not supported by the application is returned when using the Forcepoint DLP data pattern, Forcepoint ONE translates it as a Deny.
- To send notifications when the Forcepoint DLP returns an action other than Allow, click Notify.



Access ● Secure App Access ○ Direct App Access ○ Deny

● Download DLP ○ Block All File Downloads

Data Patterns	Files		Notify
	Action	Watermark	
Forcepoint DLP	FSM Enforc	1 - None	☑

☐ Deny Download on Scan Timeout

Upload DLP

Data Patterns	Files		Notify
	Action	Watermark	
Malware-Bitdefender	4 - Deny	1 - None	☑
Forcepoint DLP	FSM Enforc	1 - None	☑

☐ Decrypt Structured Data

☐ HTTP Request Headers

Download Notifications

User Email	None
Group Email	None
Inline Notification	DLP_Block
Forcepoint Alert	☑ Generate Alert

Upload Notifications

User Email	None
Group Email	None
Inline Notification	DLP_Block
Forcepoint Alert	☑ Generate Alert

Along with the Forcepoint DLP pattern, you can also configure other data patterns created under the **Protect** > **Objects** > **DLP Objects** page. Refer to Configuring proxy policy actions.

DLP Actions in Forcepoint ONE

For applications added via the "Any Licensed Application" option, you will be able to apply inline DLP actions on both download and upload.

Download Actions: Download actions are the same as other apps that are part of Forcepoint ONE's predefined list. To learn more about each of the actions in more detail, please view the Proxy Policy Actions guide page.

- Allow: Will allow the file to be downloaded and log the event for visibility purposes.
- Encrypt: Results in the downloaded file being encrypted with a user-specific password. This password is defined on a per-user basis and can be changed in their account profile.
- DRM-Read only: Converts the file to a DRM'd html file that is read only and cannot be edited.
- Block: Blocks the file from being downloaded. A block file message is downloaded instead.
- Deny: Will deny the "download" action outright instead of attempting to download a block message. This is useful for situations where you are trying to control things such as malware.

Upload Actions: Upload actions can support the standard allow/block as well as encryption when possible.

- Allow: Will allow the file to be uploaded and log the event for visibility purposes.
- Encrypt: This feature is available for custom applications that can support encryption. Files uploaded will be encrypted by Forcepoint ONE during upload. If the application cannot handle/support a file being encrypted on upload, the encryption process will fail and the file will be uploaded without modification. In order to view/work on the file, the file must be downloaded through the Forcepoint ONE proxy to be decrypted.
- Block: Will block the file from being uploaded; a block message is uploaded instead.
- Deny: Will deny the "upload" action outright instead of attempting to convert the file to a block message. This is useful for situations where you are trying to control things such as malware.

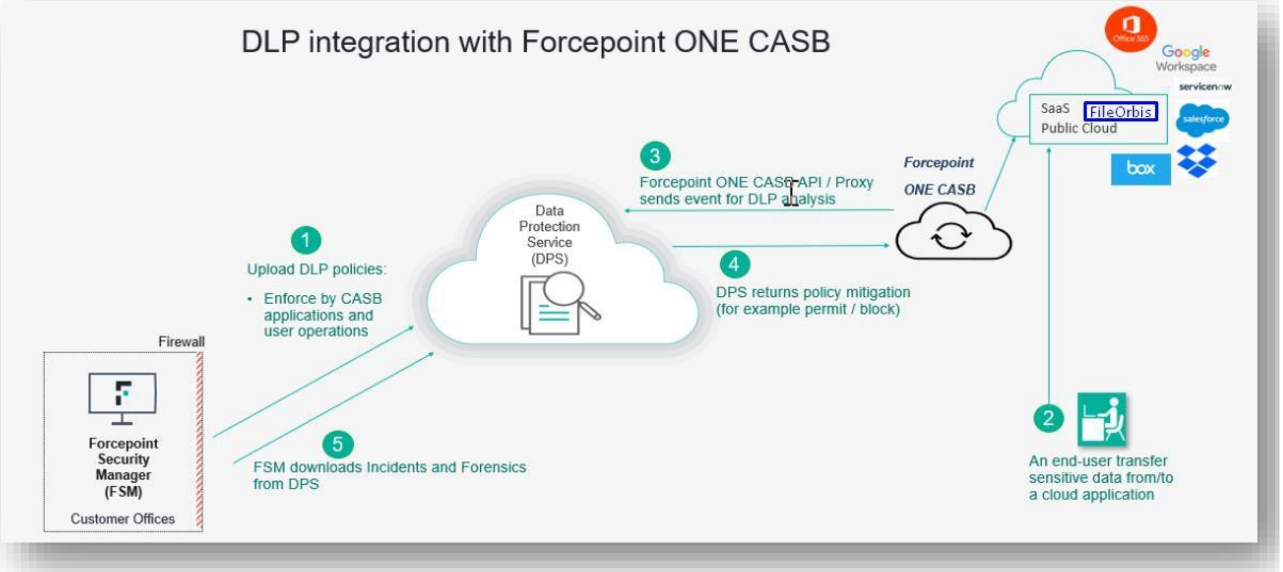
Step 1: Integrating Forcepoint DLP and Forcepoint ONE with the Forcepoint DLP SSE Apps

Forcepoint ONE has strong out-of-the-box DLP capability. With this feature, files and text are scanned upon upload and download for sensitive data and blocked, tracked, encrypted or redacted as appropriate. Over 190 predefined DLP rules help to streamline regulatory compliance and provide quick time to value. Forcepoint ONE also has easy integration with Forcepoint Enterprise DLP to enable data security everywhere – on the endpoint, in the network, on the web and in cloud applications.

Forcepoint Enterprise DLP offers unified policy control that manages channels from one single policy. With just a few clicks for integration between Forcepoint DLP and Forcepoint ONE, it simplifies policy configuration by applying new or existing policies across all Forcepoint ONE SSE channels. Unified reporting for DLP incidents gives you an intuitive, single view of all incidents across all channels. Centralized DLP forensics for CASB, SWG and ZTNA provides full forensic artifacts of all data exfiltration attempts upon upload/download/share/chat across all channels.

In this step, we assume that the integration between Forcepoint DLP and Forcepoint ONE has been completed. For details, please refer to following link.
https://help.forcepoint.com/dlp/fone_integration/forcepoint_dlp_and_forcepoint_one_casb/index.html

In this step, we assume that the integration between Forcepoint DLP and Forcepoint ONE has been completed. For details, please refer to following link. https://help.forcepoint.com/dlp/fone_integration/forcepoint_dlp_and_forcepoint_one_casb/index.html

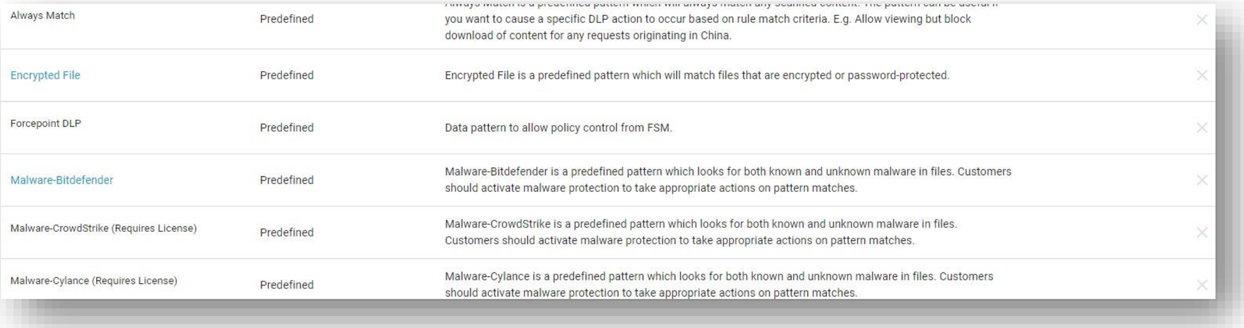

DLP integration with Forcepoint ONE CASB
Office 365
Google Workspace
servicenow
SaaS
FileOrbis
Public Cloud
salesforce
box
Forcepoint
ONE CASB
3
Forcepoint ONE CASB API / Proxy sends event for DLP analysis
Data Protection Service (DPS)
1
Upload DLP policies:
• Enforce by CASB applications and user operations
4
DPS returns policy mitigation (for example permit / block)
Firewall
Forcepoint Security Manager (FSM)
Customer Offices
5
FSM downloads Incidents and Forensics from DPS
2
An end-user transfer sensitive data from/to a cloud application

- Policies are uploaded from the FSM to the cloud-hosted Data Protection Service (DPS).
- The end user transfers sensitive data from/to a web/cloud application that is under monitoring.
- This triggers the Forcepoint ONE CASB/SWG to send event details to the DPS for analysis.
- DPS returns the policy mitigation (for example: block or permit) post analysis.
- Forcepoint Security Manager (FSM) downloads the incident and forensic information, which can be viewed in the reporting section.

Step 2: Configuring FileOrbis Policy in Forcepoint ONE
Forcepoint ONE also provides Advanced Threat Protection (ATP) via partnerships with Crowdstrike and Bitdefender. Once any of these ATP options have been purchased, you will be able to implement threat protection into your application policies (protecting against both known and unknown malware).

A new predefined data pattern named Forcepoint DLP is available under the **Protect** > **Objects** > **DLP Objects** page once a valid DPS license is uploaded to Forcepoint ONE. After uploading and validating the DPS license in the Forcepoint ONE portal, you can now use the Forcepoint DLP data pattern in Secure App Access policy action modals as a Data pattern in all your CASB policies.

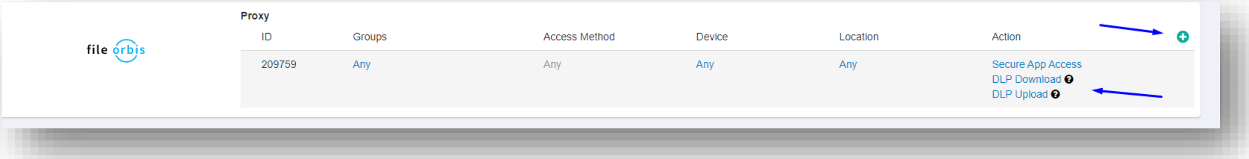
You can see these data patterns on the **Protect** > **Objects** > **DLP Objects** page.



Always Match	Predefined	Always Match is a predefined pattern which will always match any scanned content. The pattern can be useful if you want to cause a specific DLP action to occur based on rule match criteria. E.g. Allow viewing but block download of content for any requests originating in China.	×
Encrypted File	Predefined	Encrypted File is a predefined pattern which will match files that are encrypted or password-protected.	×
Forcepoint DLP	Predefined	Data pattern to allow policy control from FSM.	×
Malware-Bitdefender	Predefined	Malware-Bitdefender is a predefined pattern which looks for both known and unknown malware in files. Customers should activate malware protection to take appropriate actions on pattern matches.	×
Malware-CrowdStrike (Requires License)	Predefined	Malware-CrowdStrike is a predefined pattern which looks for both known and unknown malware in files. Customers should activate malware protection to take appropriate actions on pattern matches.	×
Malware-Cylance (Requires License)	Predefined	Malware-Cylance is a predefined pattern which looks for both known and unknown malware in files. Customers should activate malware protection to take appropriate actions on pattern matches.	×

Users utilizing the FileOrbis application, as shown in the image below, will be able to perform uploads and downloads according to Forcepoint DLP policies, and malware analysis by the selected ATP module will be conducted for these files.

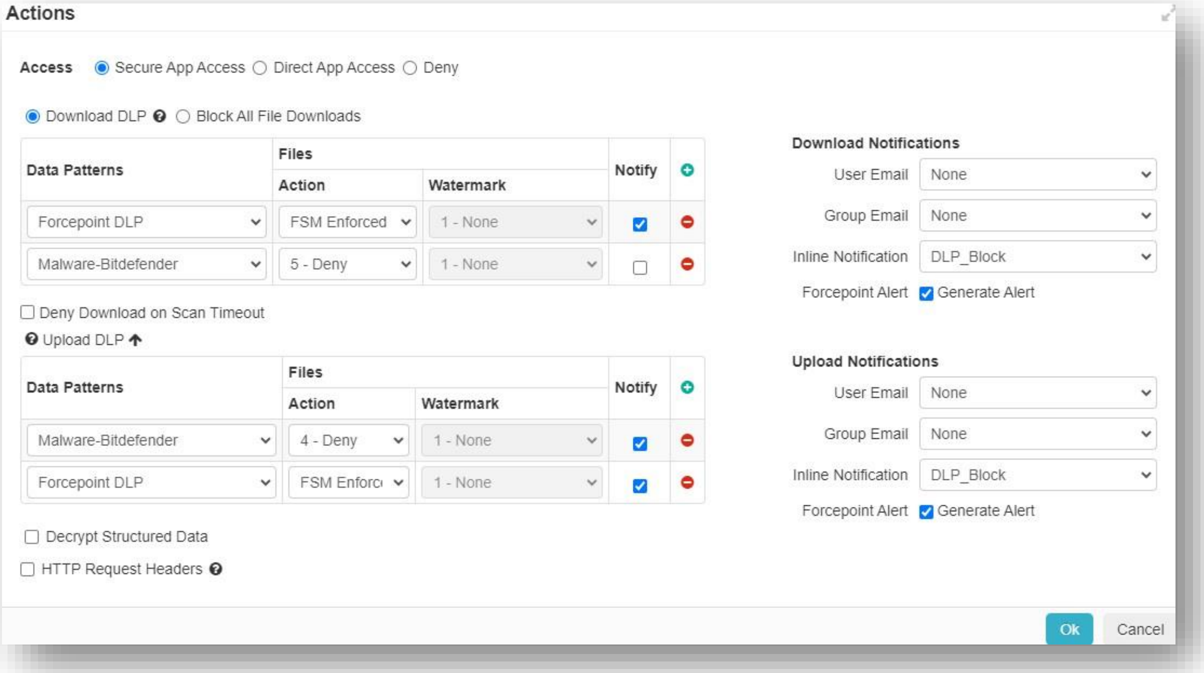
While creating CASB policies for FileOrbis, if you select Forcepoint DLP as the data pattern in any of the Actions dialog for Secure App Access, then:



Proxy

ID	Groups	Access Method	Device	Location	Action
209759	Any	Any	Any	Any	Secure App Access DLP Download DLP Upload

- The "FSM" Enforced option gets populated in the Action field as the action is configured on the FSM. "FSM Enforced" is the only option available for selection.
- If an action other than Allow that is not supported by the application is returned when using the Forcepoint DLP data pattern, Forcepoint ONE translates it as a Deny.
- To send notifications when the Forcepoint DLP returns an action other than Allow, click Notify.
- All other fields in the upload or download DLP table are set to their default value and grayed out and are not supported with Forcepoint DLP.
- Along with the Forcepoint DLP data pattern, you can also configure other data patterns created under the **Protect** > **Objects** > **DLP Objects** page. Refer to Configuring proxy policy actions.



Actions

Access ● Secure App Access ○ Direct App Access ○ Deny

● Download DLP ○ Block All File Downloads

Data Patterns	Files Action	Files Watermark	Notify
Forcepoint DLP	FSM Enforced	1 - None	☑
Malware-Bitdefender	5 - Deny	1 - None	□

□ Deny Download on Scan Timeout

Upload DLP

Data Patterns	Files Action	Files Watermark	Notify
Malware-Bitdefender	4 - Deny	1 - None	☑
Forcepoint DLP	FSM Enforc	1 - None	☑

□ Decrypt Structured Data

□ HTTP Request Headers

Download Notifications

User Email: None

Group Email: None

Inline Notification: DLP_Block

Forcepoint Alert: ☑ Generate Alert

Upload Notifications

User Email: None

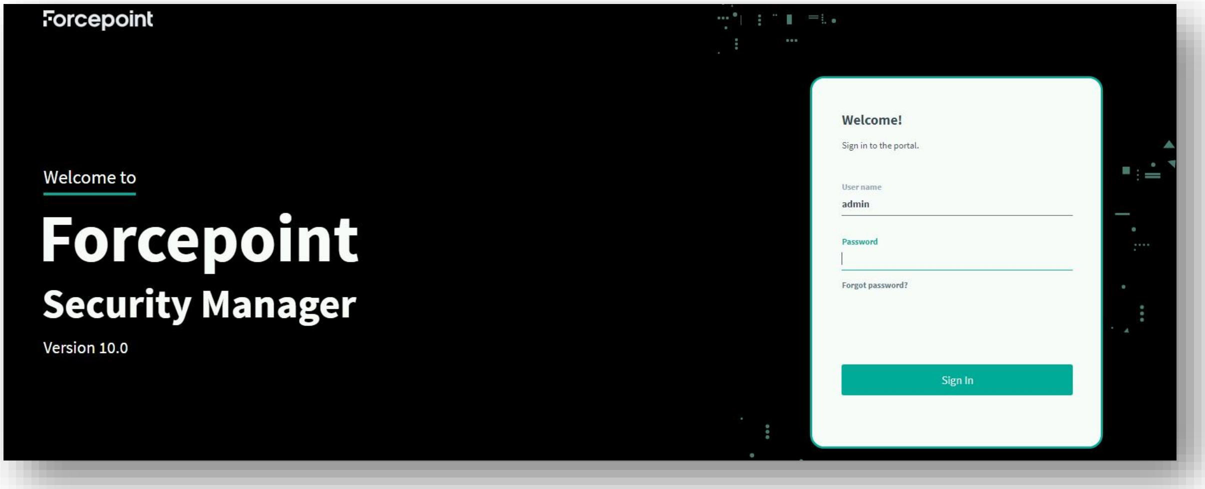
Group Email: None

Inline Notification: DLP_Block

Forcepoint Alert: ☑ Generate Alert

Step 3: Configuring DLP SSE App Rules in Forcepoint DLP

Please log in to DLP - Forcepoint Security Manager (FSM)



Welcome to

Forcepoint

Security Manager

Version 10.0

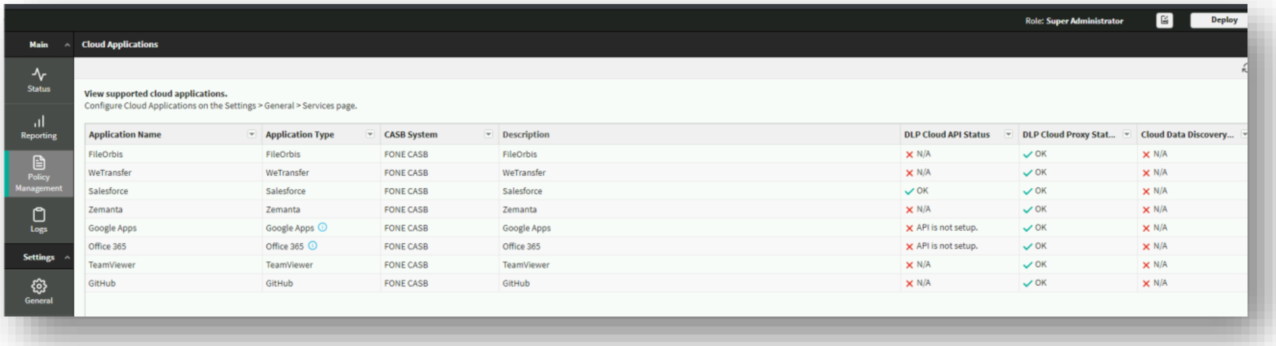
Welcome!

Sign in to the portal.

User name: admin

Password

After successfully connecting to the Forcepoint ONE CASB system on the Cloud Applications tab of the FSM, the FSM Cloud Applications resource screen displays a list of all configured (predefined and custom) cloud applications from the Forcepoint ONE portal. To open the cloud applications list, open the FSM, then navigate to the **DATA** > **Policy Management** > **Resources** > **Cloud Applications** page. Depending on your cloud apps, the table shows something like the following. Please ensure that FileOrbis is in the Application list.



View supported cloud applications.
Configure Cloud Applications on the Settings > General > Services page.

Application Name	Application Type	CASB System	Description	DLP Cloud API Status	DLP Cloud Proxy Stat...	Cloud Data Discovery...
FileOrbis	FileOrbis	FONE CASB	FileOrbis	✗ N/A	✓ OK	✗ N/A
WeTransfer	WeTransfer	FONE CASB	WeTransfer	✗ N/A	✓ OK	✗ N/A
Salesforce	Salesforce	FONE CASB	Salesforce	✓ OK	✓ OK	✗ N/A
Zemanta	Zemanta	FONE CASB	Zemanta	✗ N/A	✓ OK	✗ N/A
Google Apps	Google Apps ⓘ	FONE CASB	Google Apps	✗ API is not setup.	✓ OK	✗ N/A
Office 365	Office 365 ⓘ	FONE CASB	Office 365	✗ API is not setup.	✓ OK	✗ N/A
TeamViewer	TeamViewer	FONE CASB	TeamViewer	✗ N/A	✓ OK	✗ N/A
GitHub	GitHub	FONE CASB	GitHub	✗ N/A	✓ OK	✗ N/A

- **Application Name:** The unique name given to the specific cloud application.
- **Application Type:** The name of the cloud application. The application type can be shared by multiple cloud applications in Forcepoint DLP.
- **Description:** The short description given to the cloud application.
- **DLP Cloud API Status:** Displays the status of cloud application's API setup:
  - If the application supports API scanning and API scanning is configured in the Forcepoint ONE portal, then the status displayed as API is not set up.
  - If the application supports API scanning and API scanning is configured in the Forcepoint ONE portal, then the status is displayed as OK.
  - If the application does not support a DLP Cloud API connection, then the status is NA.
  - If there is an issue with the connection, the appropriate message is shown. Move the mouse over the status message to see more information.

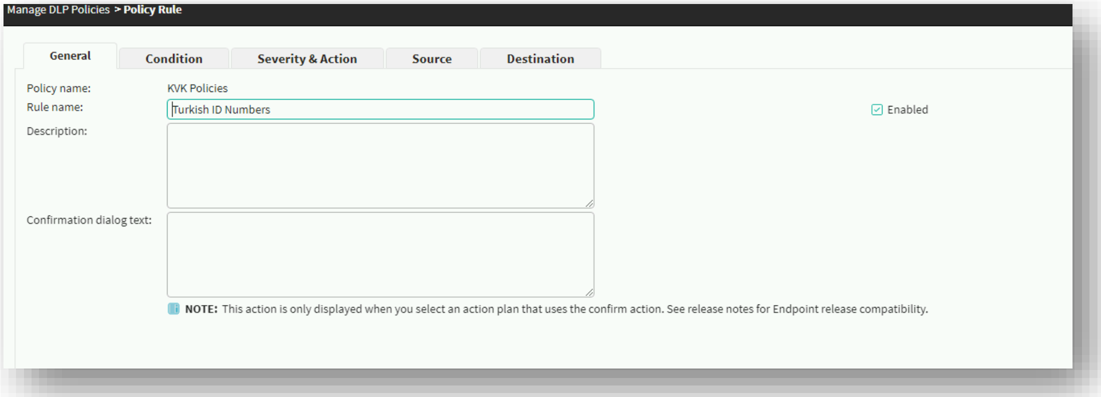
- **DLP Cloud Proxy Status:** Displays the status of the cloud application's proxy setup:
    - If the application supports a proxy connection, the status is OK.
    - If the application does not support a proxy connection, the status is NA.
    - If there is an issue with the connection, the appropriate message is shown. Move the mouse over the status message to see more information.

If you want to view the cloud application(s) in the Forcepoint ONE portal, click the link at the bottom of the page to open the Forcepoint ONE portal's **Protect** > **Policies** page.

When configuring DLP Cloud policy rules, you must select DLP Cloud Applications as the destination, and you must select one or both of the DLP Cloud Applications channels – DLP Cloud API and DLP Cloud Proxy.

Before configuring DLP Cloud API policies, you should download and install the Forcepoint DLP Patch for Cloud API Destinations file from the DLP Core Version 10.0 page to avoid errors when you set a DLP Cloud API Destination related policy that impacts File creation/modification. Refer to the installation steps present in the zip file.

- In the FSM, navigate to **Data** > **Policy Management** > **DLP Policies** > **Manage Policies**.
- Expand a policy in the tree view and click a rule, then select Edit or select **Add** > **Rule**.



Policy name: KVK Policies

Rule name: Turkish ID Numbers

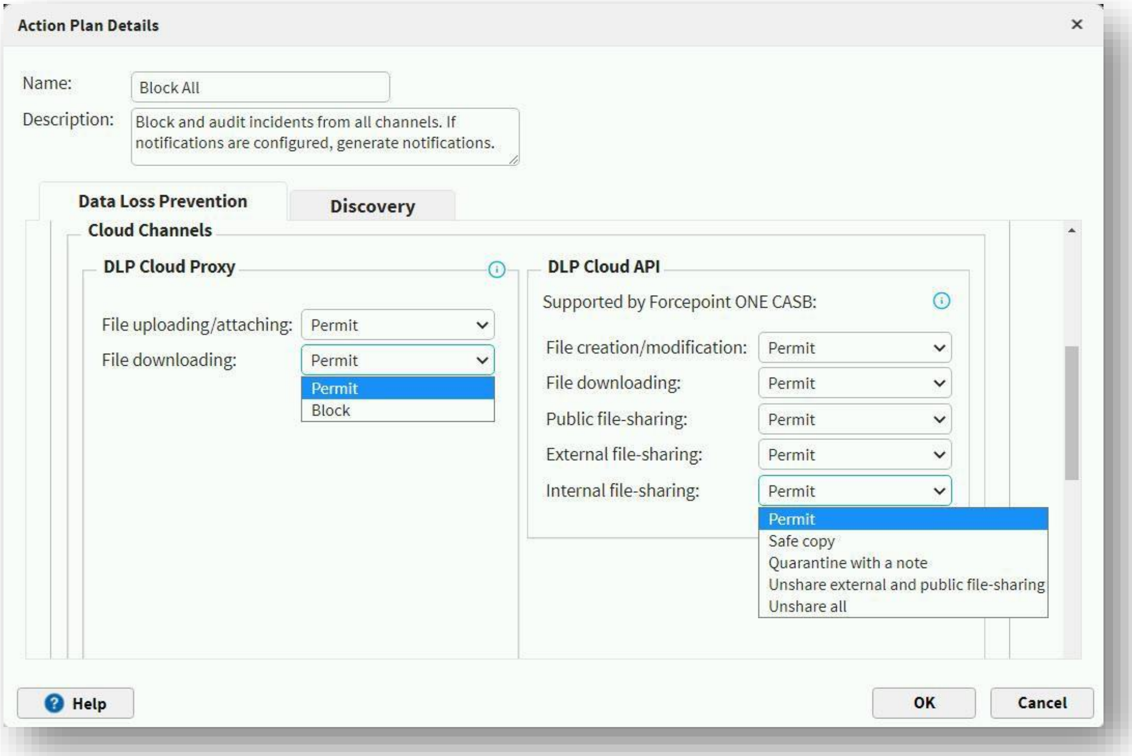
☑ Enabled

Description:

Confirmation dialog text:

NOTE: This action is only displayed when you select an action plan that uses the confirm action. See release notes for Endpoint release compatibility.

- On the Policy Rule page configure the rule through the General, Condition, Severity and Action, Source and Destination tabs.
- Configuring a rule for a cloud application is similar to any DLP rule but requires specific configuration settings in the Severity & Action and Destination tables. For more information about creating a DLP policy rule, see the Forcepoint DLP Administrator Guide.
- On the Severity & Action tab, select an action from the Action Plan drop-down menu and click the button to the right of the drop-down menu to open the Action Plan Details page.
- On the Data Loss Prevention tab, in the Cloud Channels section, select the actions for the available operations.



Name: Block All

Description: Block and audit incidents from all channels. If notifications are configured, generate notifications.

DLP Cloud Proxy

File uploading/attaching: Permit

File downloading: Permit

DLP Cloud API

Supported by Forcepoint ONE CASB:

File creation/modification: Permit

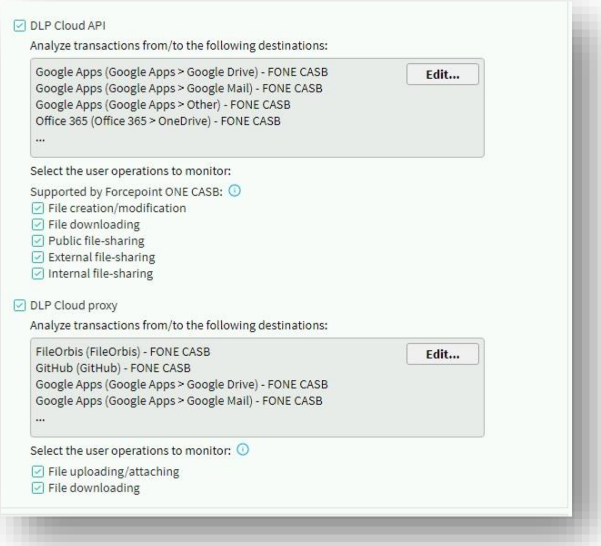
File downloading: Permit

Public file-sharing: Permit

External file-sharing: Permit

Internal file-sharing: Permit

- For DLP Cloud Proxy, you can select the following actions:
  - Permit: Allow the operation.
  - Block: Block the operation.
- For DLP Cloud API, you can select the following actions:
  - Permit: Allow the transaction.
  - Save Copy: Save a copy of the file to a cloud archive that is accessible by adminstrators.
  - Quarantine With a Note: Quarantine the file and leave a message in place of the original file.
  - Unshare External and Public File-sharing: Remove sharing permissions for external addresses.
  - Unshare All: Remove all sharing permissions from the file.
  - Click OK to save the changes made on the Action Plan Details page.
- On the Destination tab, under the DLP Cloud Applications section, select DLP Cloud API, DLP Cloud proxy, or both. For each channel, select at least one cloud application (or All) and at least one operation, as follows:
  - Click Edit.
  - Select one or more cloud applications in the Available Elements list. If you want to use all of the cloud applications, leave this as All and then continue with step 6e to select an operation.
  - Click the right arrow button to move FileOrbis and selected cloud applications to the Selected Elements list.



☑ DLP Cloud API

Analyze transactions from/to the following destinations:

Google Apps (Google Apps > Google Drive) - FONE CASB
Google Apps (Google Apps > Google Mail) - FONE CASB
Google Apps (Google Apps > Other) - FONE CASB
Office 365 (Office 365 > OneDrive) - FONE CASB
...

Select the user operations to monitor:

Supported by Forcepoint ONE CASB:

- ☑ File creation/modification
- ☑ File downloading
- ☑ Public file-sharing
- ☑ External file-sharing
- ☑ Internal file-sharing

☑ DLP Cloud proxy

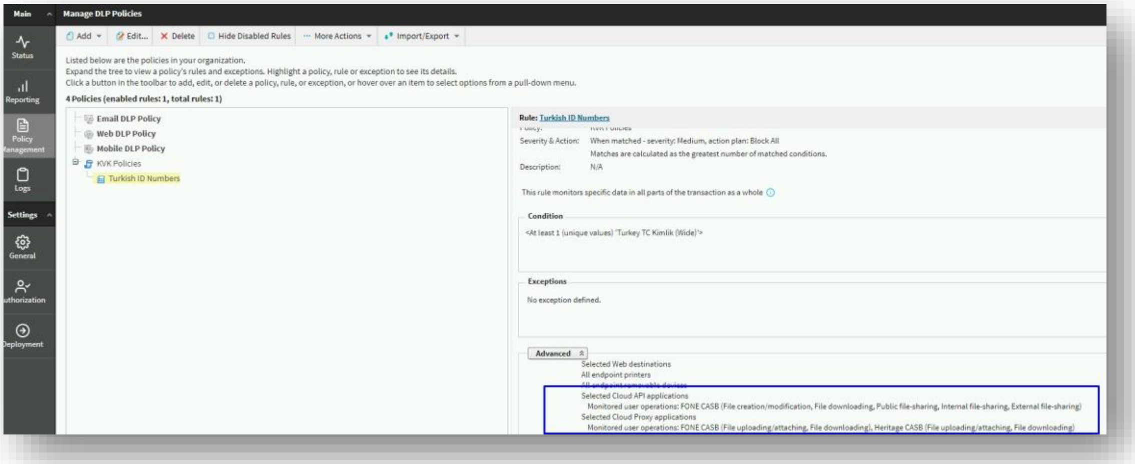
Analyze transactions from/to the following destinations:

FileOrbis (FileOrbis) - FONE CASB
GitHub (GitHub) - FONE CASB
Google Apps (Google Apps > Google Drive) - FONE CASB
Google Apps (Google Apps > Google Mail) - FONE CASB
...

Select the user operations to monitor:

- ☑ File uploading/attaching
- ☑ File downloading

  - Click OK. The cloud applications and FileOrbis are now shown in the box under the channel name.
- Select user operations to monitor:
  - For DLPCloud API, Forcepoint ONE supports the following operations to monitor:
    - File creation/modification
    - File downloading (Note: File downloading is supported only by Google Workspace)
    - Pubilic file sharing
    - Exnternal file sharing
    - Internal file sharing
  - For DLP Cloud proxy, Forcepoint ONE supports the following operations to monitor:
    - File uploading/attaching
    - File downloading
- Click Next to show a summary of the rule.
- Click Finish to save the rule.
- To deploy all the configuration changes, click Deploy. In the Manage DLP Policies screen, the file summary (right pane) shows whether DLP Cloud Applications are selected as a Destination.



Listed below are the policies in your organization.
Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or exception to see its details.
Click a button in the toolbar to add, edit, or delete a policy, rule, or exception, or hover over an item to select options from a pull-down menu.

4 Policies (enabled rules: 1, total rules: 1)

- Email DLP Policy
- Web DLP Policy
- Mobile DLP Policy
- KVK Policies
  - Turkish ID Numbers

Rule: Turkish ID Numbers

Policy: KVK Policies

Severity & Action: When matched - severity: Medium, action plan: Block All
Matches are calculated as the greatest number of matched conditions.

Description: N/A

This rule monitors specific data in all parts of the transaction as a whole

Condition

<At least 1 (unique values) 'Turkey TC Kimlik (Wide)'>

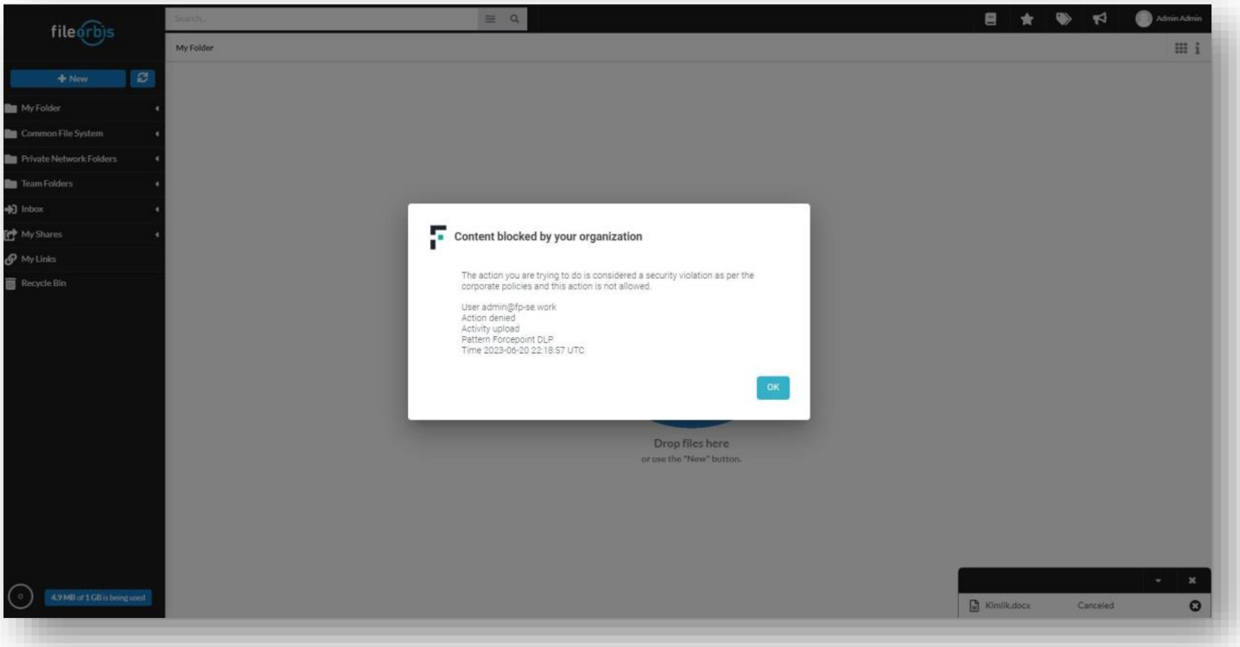
Exceptions

No exception defined.

Selected Web destinations
All endpoint printers
All endpoint removable devices
Selected Cloud API applications
Monitored user operations: FONE CASB (File creation/modification, File downloading, Public file-sharing, Internal file-sharing, External file-sharing)
Selected Cloud Proxy applications
Monitored user operations: FONE CASB (File uploading/attaching, File downloading), Heritage CASB (File uploading/attaching, File downloading)

Step 4: Verifying DLP SSE App Rules

Please log in to the FileOrbis portal, then try to upload some data that can match the rules you have defined in the previous section. If the data being uploaded conforms to the DLP rules, the user will observe a denial message for this operation, as illustrated in the accompanying image.



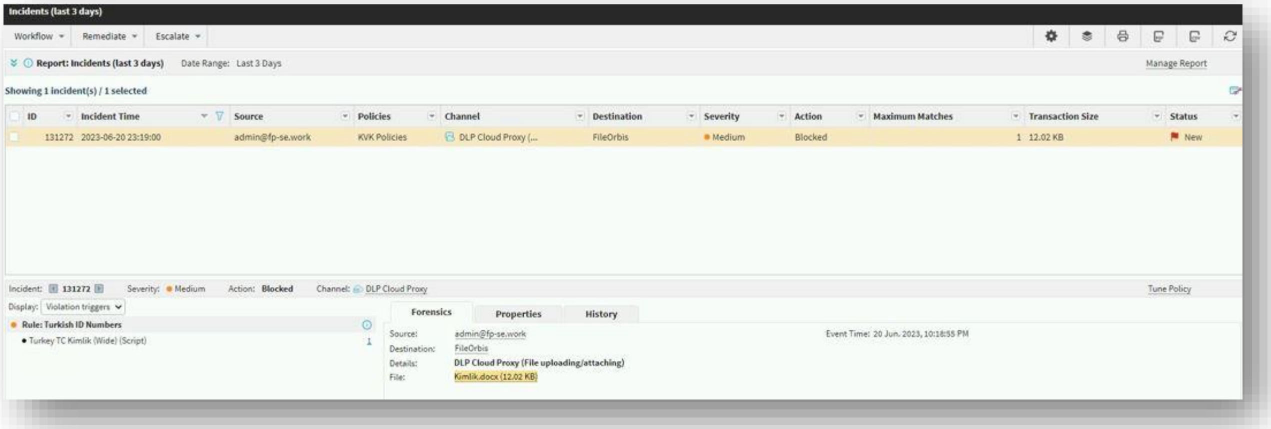
Content blocked by your organization

The action you are trying to do is considered a security violation as per the corporate policies and this action is not allowed.

User admin@fp-se.work
Action denied
Activity upload
Pattern Forcepoint DLP
Time 2023-06-20 22:18:57 UTC

Now you can review the incidents by viewing and managing logs for the Cloud Applications on the Forcepoint ONE portal and the Forcepoint DLP FSM Manager.

In the Forcepoint SLP FSM, the following logs can be found under **Reporting** > **Data Loss Preventon Reporting** > **Incidents**.



Incidents (last 3 days)

Report: Incidents (last 3 days)   Date Range: Last 3 Days

Showing 1 incident(s) / 1 selected

ID	Incident Time	Source	Policies	Channel	Destination	Severity	Action	Maximum Matches	Transaction Size	Status
131272	2023-06-20 23:19:00	admin@fp-se.work	KVK Policies	DLP Cloud Proxy (...	FileOrbis	● Medium	Blocked	1	12.02 KB	New

Incident: 131272   Severity: ● Medium   Action: Blocked   Channel: DLP Cloud Proxy

Display: Violation triggers

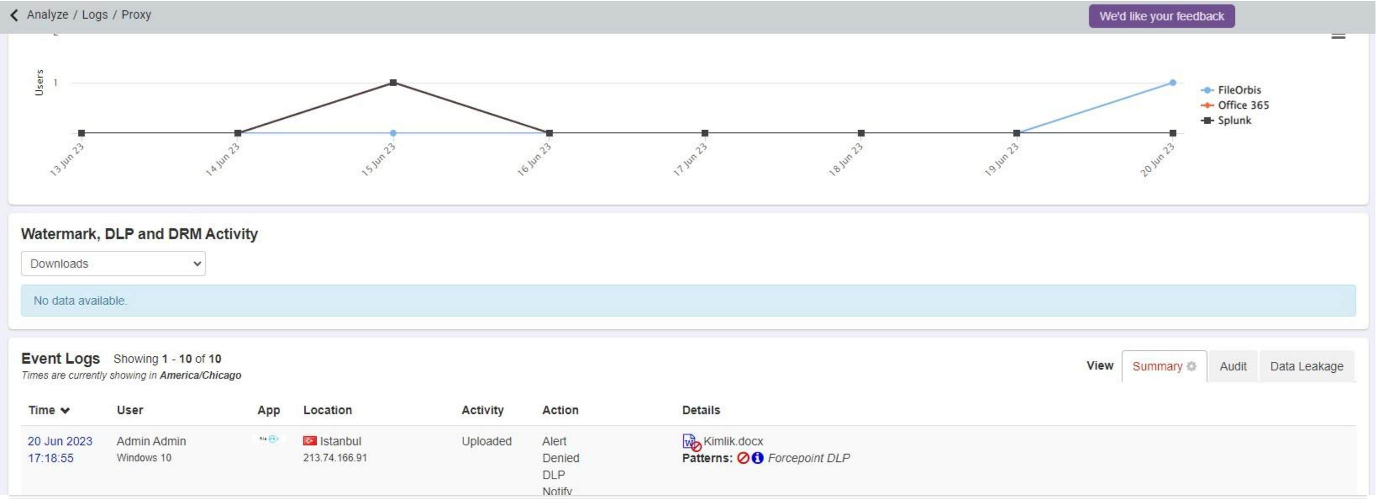
● Rule: Turkish ID Numbers
- Turkey TC Kimlik (Wide) (Script)   1

Source: admin@fp-se.work   Event Time: 20 Jun. 2023, 10:18:55 PM
Destination: FileOrbis
Details: DLP Cloud Proxy (File uploading/attaching)
File: Kimlik.docx (12.02 KB)

For Forcepoint ONE, the following logs can be found under **Analyze** > **Logs**.

Proxy Logs: The Proxy Logs are where admins go to review all user activity (events, logs, etc.) in all protected applications associated with inline access control and DLP policies. The Event Logs section displays every transaction related to your SaaS application and data inline through the proxies.

After accessing the Proxy Logs or API logs page, under the Event Logs section, you can click the time stamp of the log to view the log details as shown below.



Watermark, DLP and DRM Activity

No data available.

Event Logs Showing **1** - **10** of **10**

Times are currently showing in ***America/Chicago***

Time	User	App	Location	Activity	Action	Details
20 Jun 2023 17:18:55	Admin Admin Windows 10		Istanbul 213.74.166.91	Uploaded	Alert Denied DLP Notify	Kimlik.docx **Patterns:** *Forcepoint DLP*

Time	20 Jun 2023 17:18:55
User	Admin Admin
Email	admin@fp-se.work
User Group	System Administrator, Bitglass Admins
Device	Windows 10
Device GUID	-
App	File Orbis
App Instance Name	fp-se.work
IP Address	213.74.166.91
Location	Istanbul
Activity	**Cloudstorage, Uploaded, Web**
Action	Alert , Denied , DLP , Notify
Details	
Policy ID	209759

File Name	Track History 20 Jun 2023 17:18:55 **Kimlik.docx** ***Forcepoint DLP*** **(*kvk policies*)**
File Extension	docx
File Size	13 KB
DLP Match Location	File
URL	**forcepoint.fileorbis.com/api/v2/filesystem/upload**
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Transaction ID	ZJIlz9x9DuXYM0sKW_Tw-QAAAj0
Threat	-
Hash	**- Kimlik.docx** SHA1: None SHA256: 0fbaed3bcff0af7d57522b757d25b75786251d3d697ec850c3bde7c8dd48455d MD5: None Search VirusTotal Search Google
Justification	-

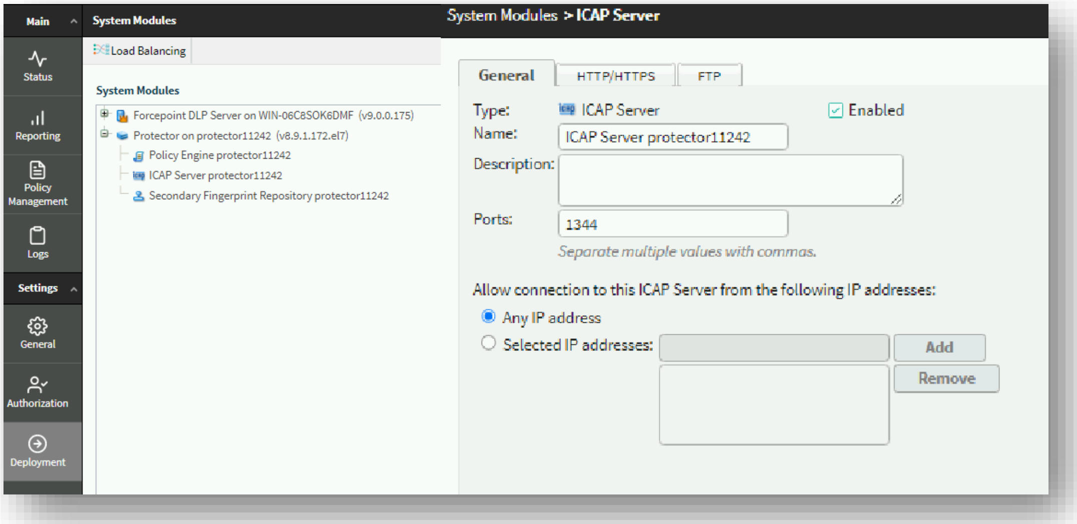
Optional: Integrating FileOrbis and Forcepoint DLP via ICAP

Note: This integration applies where the Forcepoint ONE, Forcepoint DLP and Forcepoint DLP SSE solution is not available. This section provides an overview of how to configure the integration between Forcepoint DLP and FileOrbis, along with configuring DLP polices. FileOrbis provides customers the ability to send files via ICAP (over TLS) to Forcepoint DLP. This allows customers who have Forcepoint DLP tools to consolidate their policies into one central DLP via the Forcepoint DLP Protector. The Forcepoint DLP Protector is a soft application that intercepts and analyzes traffic on a variety of channels, such as email, HTTP and FTP. Forcepoint DLP also supports DLP context scanning with third-party proxies and data sharing solutions through the ICAP protocol. With this integration, FileOrbis can work with the Forcepoint DLP solutions to scan every file that is uploaded to or downloaded or previewed from an on-premises or cloud-based enterprise content management (ECM) system to improve the security of your data.

Step 1: Configuring ICAP Settings in Forcepoint DLP Protector

The protector supports Internet Content Adaptation Protocol (ICAP) and can be integration points for third-party solutions that support ICAP, such as some web proxies and file sharing applications like FileOrbis.

To configure an ICAP server for the protector, log in to the FSM, then go to Deployment and select the Protector > ICAP server on the System Modules screen.



System Modules > ICAP Server

System Modules
- Forcepoint DLP Server on WIN-06C8SOK6DMF (v9.0.0.175)
- Protector on protector11242 (v8.9.1.172.el7)
  - Policy Engine protector11242
  - ICAP Server protector11242
  - Secondary Fingerprint Repository protector11242

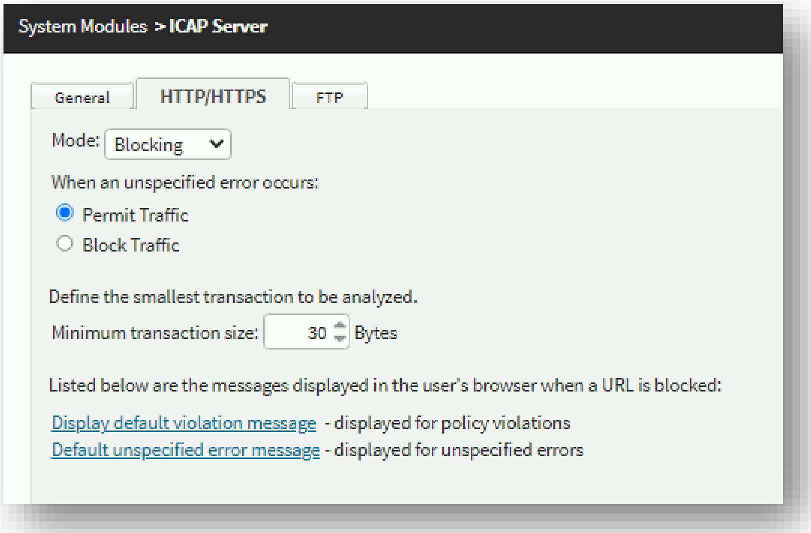
Type: ICAP Server ☑ Enabled
Name: ICAP Server protector11242
Description:
Ports: 1344
Separate multiple values with commas.

Allow connection to this ICAP Server from the following IP addresses:
● Any IP address
○ Selected IP addresses:

The “Edit ICAP” window is displayed. Use the General tab of the Edit ICAP page to configure the module name and description.

- Select or clear Enabled to enable or disable this module.
- Enter the module Name.
- Enter a Description of the module.
- Enter the Ports used by this ICAP server. These are the ports over which the system should monitor ICAP transactions. Separate multiple values with commas (for example, 1333,1334).
- Under “Allow connection to this ICAP Server from the following IP addresses,” select whether this ICAP server should allow connections from All IP addresses or Selected IP addresses.

- For the selected IP addresses option, enter an IP address to allow, then click Add. Repeat this process to allow additional IP addresses.
- The page also displays the module type, which cannot be changed.



System Modules > **ICAP Server**

Mode: Blocking

When an unspecified error occurs:

● Permit Traffic
○ Block Traffic

Define the smallest transaction to be analyzed.

Minimum transaction size: 30 Bytes

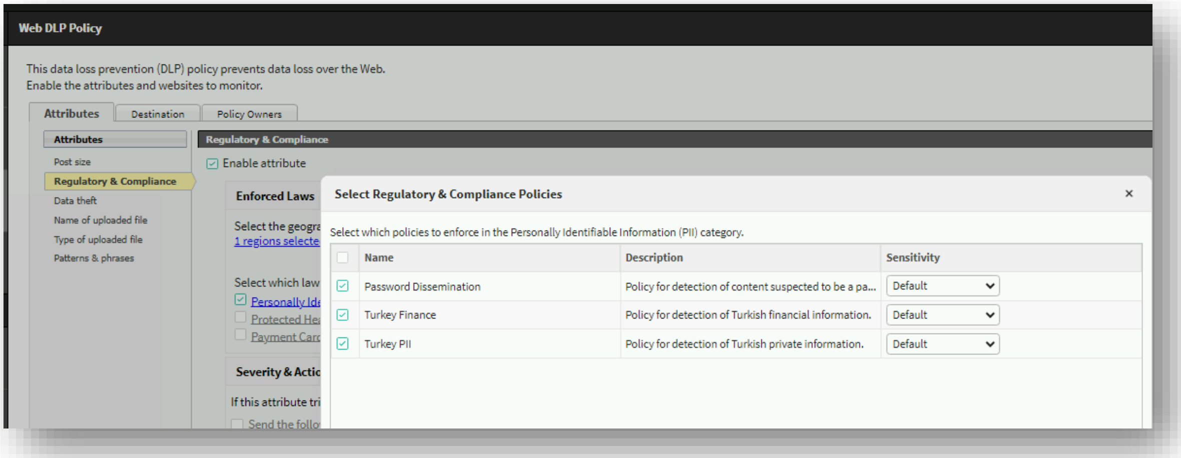
Listed below are the messages displayed in the user's browser when a URL is blocked:

Display default violation message - displayed for policy violations
Default unspecified error message - displayed for unspecified errors

- Monitoring mode monitors HTTP traffic but does not block it.
- Under “When an unspecified error occurs,” review the action to take when an unspecified error occurs during data analysis and traffic cannot be analyzed.
- Permit traffic allows HTTP traffic to continue unprotected. Select the “minimum transaction size” to monitor, in bytes.

Step 2: Configuring DLP Rules in Forcepoint DLP

To facilitate file analysis through ICAP, it is imperative to establish policy guidelines and rules within Forcepoint DLP that align with our specific requirements.



Web DLP Policy

This data loss prevention (DLP) policy prevents data loss over the Web.
Enable the attributes and websites to monitor.

☑ Enable attribute

Enforced Laws

Select the geogra
1 regions selecte

Select which law
☑ Personally Ide
□ Protected He
□ Payment Carc

Severity & Actic

If this attribute tri
□ Send the follo

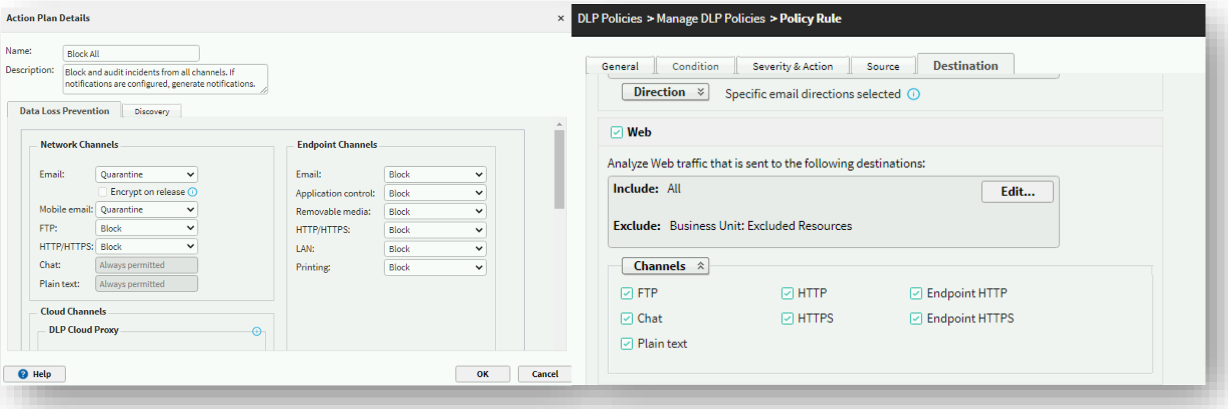
Select Regulatory & Compliance Policies ×

Select which policies to enforce in the Personally Identifiable Information (PII) category.

□	Name	Description	Sensitivity
☑	Password Dissemination	Policy for detection of content suspected to be a pa...	Default
☑	Turkey Finance	Policy for detection of Turkish financial information.	Default
☑	Turkey PII	Policy for detection of Turkish private information.	Default

.

Within the rule, it is essential to activate the HTTP/HTTPS channel in the Destination field, while ensuring that the Action field defines the appropriate course of action for the Network DLP HTTP/S channel. A configuration resembling the depiction presented in the accompanying illustration can be employed to achieve this objective.



Action Plan Details

Name: Block All

Description: Block and audit incidents from all channels. If notifications are configured, generate notifications.

Data Loss Prevention | Discovery

Network Channels

- Email: Quarantine
- □ Encrypt on release
- Mobile email: Quarantine
- FTP: Block
- HTTP/HTTPS: Block
- Chat: Always permitted
- Plain text: Always permitted

Endpoint Channels

- Email: Block
- Application control: Block
- Removable media: Block
- HTTP/HTTPS: Block
- LAN: Block
- Printing: Block

Cloud Channels

DLP Cloud Proxy

DLP Policies > Manage DLP Policies > **Policy Rule**

General | Condition | Severity & Action | Source | **Destination**

Direction: Specific email directions selected

☑ **Web**

Analyze Web traffic that is sent to the following destinations:

Include: All

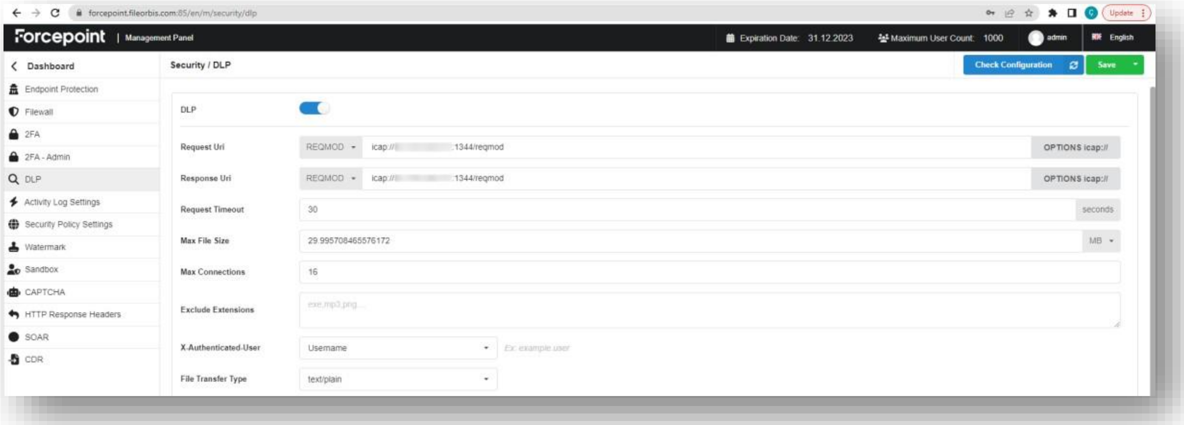
Exclude: Business Unit: Excluded Resources

Channels

- ☑ FTP
- ☑ Chat
- ☑ Plain text
- ☑ HTTP
- ☑ HTTPS
- ☑ Endpoint HTTP
- ☑ Endpoint HTTPS

Step 3: Configuring ICAP Settings in FileOrbis

The Forcepoint DLP integration on FileOrbis is performed from the **Management Panel** > **Security** > **DLP** menu.

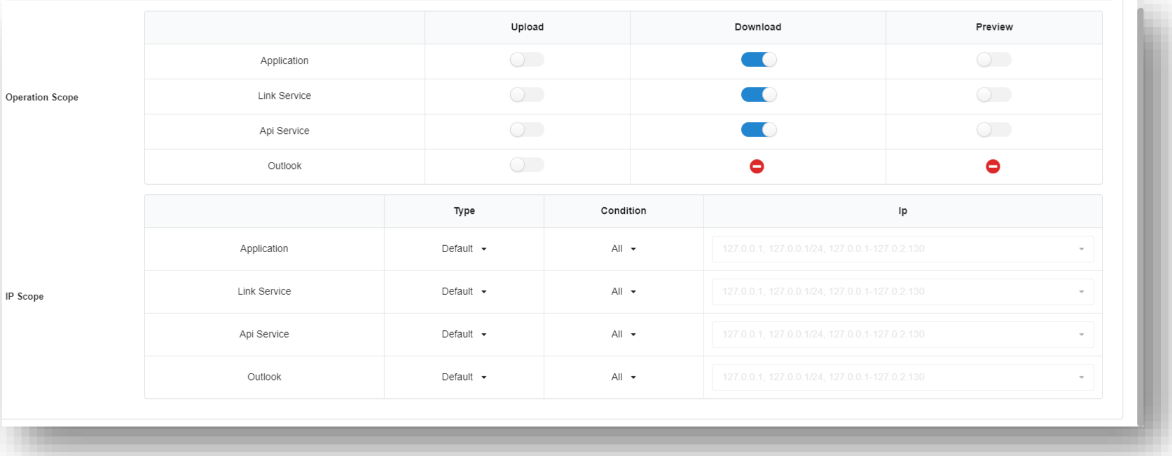


forcepoint.fileorbis.com:85/en/m/security/dlp

Forcepoint | Management Panel — Expiration Date: 31.12.2023 — Maximum User Count: 1000 — admin — English

Security / DLP

DLP	●
Request Uri	REQMOD icap://[redacted]:1344/reqmod — OPTIONS icap://
Response Uri	REQMOD icap://[redacted]:1344/reqmod — OPTIONS icap://
Request Timeout	30 seconds
Max File Size	29.995708465576172 MB
Max Connections	16
Exclude Extensions	exe,mp3,png...
X-Authenticated-User	Username — Ex: example.user
File Transfer Type	text/plain



Operation Scope

	Upload	Download	Preview
Application	○	●	○
Link Service	○	●	○
Api Service	○	●	○
Outlook	○	⛔	⛔

IP Scope

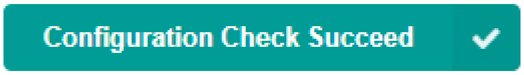
	Type	Condition	Ip
Application	Default	All	127.0.0.1, 127.0.0.1/24, 127.0.0.1-127.0.2.130
Link Service	Default	All	127.0.0.1, 127.0.0.1/24, 127.0.0.1-127.0.2.130
Api Service	Default	All	127.0.0.1, 127.0.0.1/24, 127.0.0.1-127.0.2.130
Outlook	Default	All	127.0.0.1, 127.0.0.1/24, 127.0.0.1-127.0.2.130

Note: In the absence of a block rule in the DLP rules, user transactions can proceed normally on FileOrbis. Any DLP events that occur during these transactions will be displayed and logged.

However, if a block rule exists in the DLP rules, the user's operations on FileOrbis will be blocked. Reports regarding these blocked operations will be generated and can be viewed in both the DLP and FileOrbis Reports sections.

Attributes	Description
Excluded Extensions	It can be configured to prevent the specified extensions from being sent to the ICAP query in DLP.
IP Scope	DLP rules are requested to be active or not based on IP and XFF information.
Request Timeout	The maximum response time of the request service on DLP can be given.
Process Scope	DLP will be active in the uploading, downloading and previewing processes in web applications, link services, API services and Outlook add-in applications.
Maximum Number of Connections	The maximum number of ICAP queries waiting for the DLP query queue can be given.
Maximum File Size	The maximum file size that can be sent to ICAP protocol for DLP query is given.
Request UrL	The ICAP server and port information used should be written, E.g., icap://icap server ip address:1344/reqmod
Response Url	The icap server and port information used should be written, e.g., icap://icap server ip address:1344/reqmod
Default Actions	If the rules are active, FileOrbis prevents operations before sending them to DLP.
X-Authenticated-User	This is used to display user information in the desired format when DLP incidents occur.

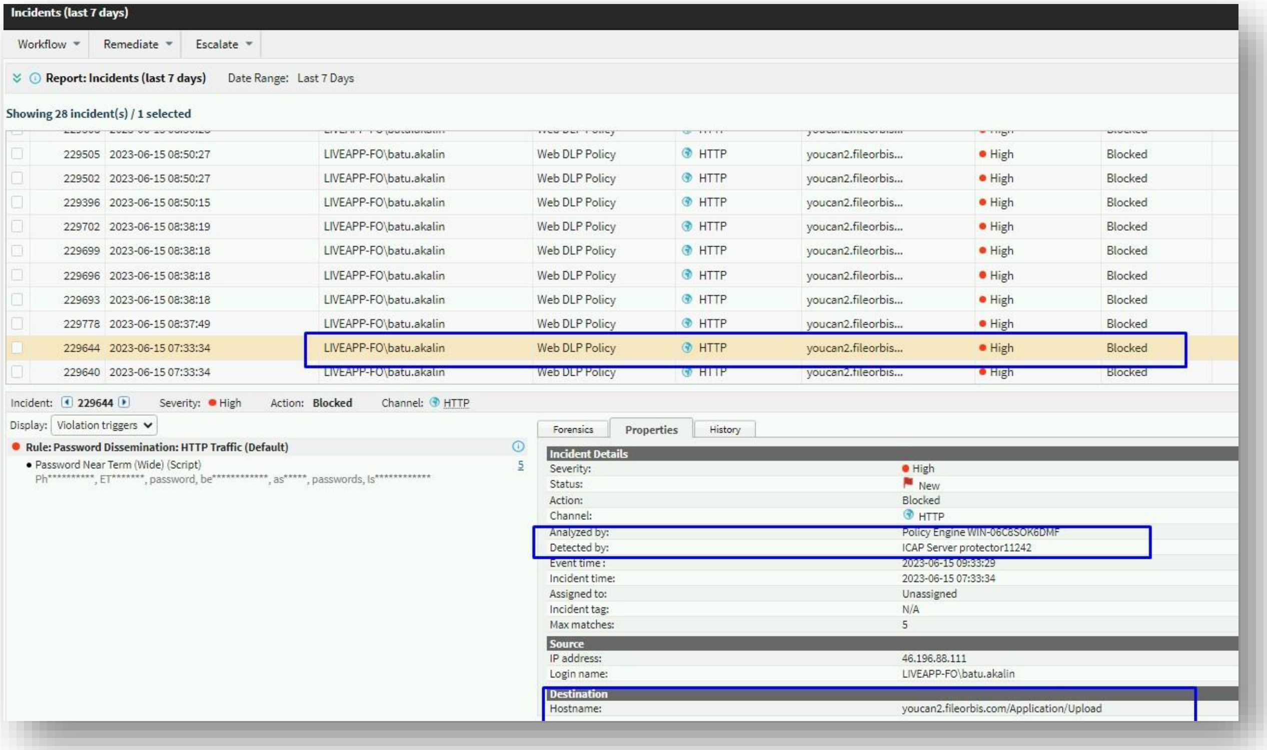
There is one final step, and that is to click the **Check Configuration** button in the top right. Verify the button will look like this after a while.



Step 4: Verifying DLP ICAP Rules

Please log in to the FileOrbis portal, then try to upload some data that can match the rules you have defined in the previous section. If the data being uploaded conforms to the DLP rules, the user will observe a denial message for this operation, as illustrated in the accompanying image. You can view a list of data loss prevention incidents from the FileOrbis data upload or download, and their details through the ICAP.

In the Forcepoint Security Manager, go to the **Data** > **Main** > **Reporting** > **Data Loss Prevention** page.



Report: Incidents (last 7 days) Date Range: Last 7 Days

Showing 28 incident(s) / 1 selected

□	229505	2023-06-15 08:50:27	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229502	2023-06-15 08:50:27	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229396	2023-06-15 08:50:15	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229702	2023-06-15 08:38:19	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229699	2023-06-15 08:38:18	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229696	2023-06-15 08:38:18	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229693	2023-06-15 08:38:18	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229778	2023-06-15 08:37:49	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229644	2023-06-15 07:33:34	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked
□	229640	2023-06-15 07:33:34	LIVEAPP-FO\batu.akalin	Web DLP Policy	HTTP	youcan2.fileorbis...	● High	Blocked

Incident: 229644 Severity: ● High Action: **Blocked** Channel: HTTP

Display: Violation triggers

● **Rule: Password Dissemination: HTTP Traffic (Default)**

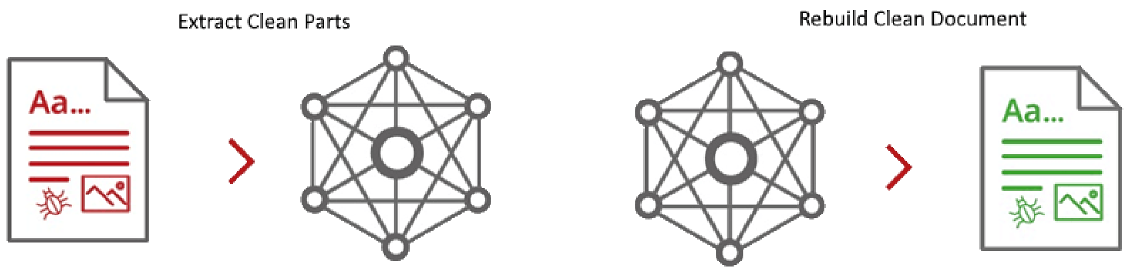
- Password Near Term (Wide) (Script) 5
  Ph**********, ET*******, password, be************, as*****, passwords, Is************

Incident Details	
Severity:	● High
Status:	New
Action:	Blocked
Channel:	HTTP
Analyzed by:	Policy Engine WIN-06C8SOK6DMF
Detected by:	ICAP Server protector11242
Event time :	2023-06-15 09:33:29
Incident time:	2023-06-15 07:33:34
Assigned to:	Unassigned
Incident tag:	N/A
Max matches:	5
Source	
IP address:	46.196.88.111
Login name:	LIVEAPP-FO\batu.akalin
Destination	
Hostname:	youcan2.fileorbis.com/Application/Upload

Integrating FileOrbis and Forcepoint Zero Trust CDR

This section details the configuration steps needed for FileOrbis to send data to, and receive data from, Forcepoint Zero Trust CDR via API.

All Forcepoint CDR products use a common transformation engine. The engine consists of three key parts. These are the extract, verify and rebuild stages, as seen in the infographic. This process ensures that the user experience is maintained (the before and after look visually the same). However, the file has now been “cleaned” through a normalization process, where Forcepoint’s CDR only transforms known safe parts of the file format.



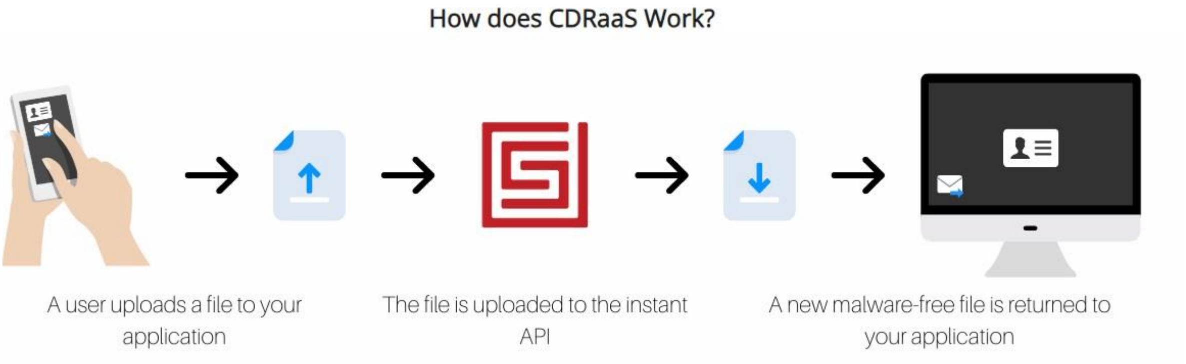
The purpose of this integration is that during all file upload and download to be made through FileOrbis, FileOrbis sends the file to Forcepoint's SaaS CDR solution via the API and within a few seconds the file is returned to FileOrbis as cleaned and 100% malware free.

Together, Forcepoint and FileOrbis present a unified answer to the problem of Zero Trust at the content layer. Here, FileOrbis is joined with Forcepoint Zero Trust CDR. Combining FileOrbis and Forcepoint Zero Trust CDR is like taking two approaches to enterprise content sharing security and putting them together.

FileOrbis facilitates secure content collaboration between users inside and outside of a company's network, while Forcepoint Zero Trust CDR helps businesses strengthen their security and centralize their access controls. Organizations benefit from increased adaptability and scalability in content collaboration thanks to the integration of these two technologies, which provides easy and secure access to files from anywhere in the world.

With Forcepoint Zero Trust CDR, businesses have fine-grained control over who can see what within their organization's content. With FileOrbis, users can safely store, sync and collaborate on files from any location. When these two technologies are combined, they allow for increased security, better collaboration and data access, and scalability for content sharing networks. FileOrbis and Forcepoint Zero Trust CDR help businesses protect their data from unauthorized access while still facilitating seamless collaboration between employees. Organizations now have a complete toolkit for achieving Zero Trust thanks to this integration.

Step 1: How to Obtain API Keys for Forcepoint Zero Trust CDR


How does CDRaaS Work?

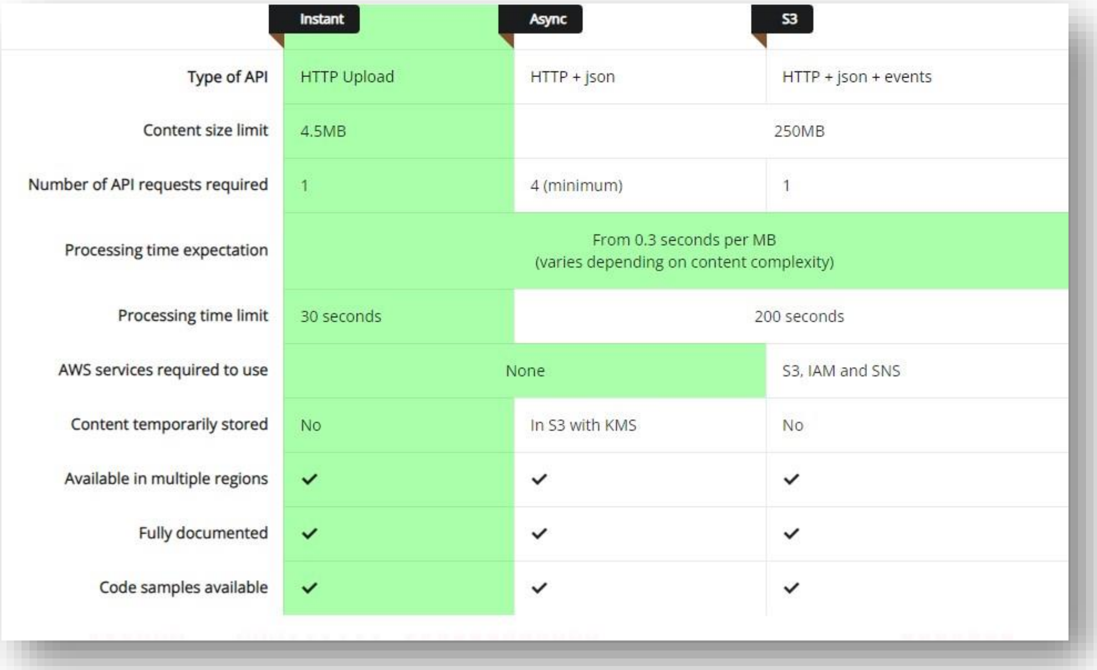
A user uploads a file to your application

The file is uploaded to the instant API

A new malware-free file is returned to your application

To integrate, we have the choice of three cloud API variants. In this section we have used Instant API for demonstration purposes.

- The Instant API enables simple uploading and immediate downloading, doesn’t require any additional infrastructure and is suitable for files that are under 5MB.
- The Async API supports file sizes up to 250MB. It enables large files to be processed and allows more advanced scenarios such as uploading from one system and then downloading the safe documents from a separate system.
- The S3 API lets us pull and push data from and to your S3 buckets. Just tell us how to access them, and we’ll do the rest. You can set it up so that processing happens automatically whenever items are added to a bucket. The S3 API is an excellent fit for event-driven workflows. You can submit large files and have the new files uploaded to a separate bucket, which could even be in a separate AWS account.



	Instant	Async	S3
Type of API	HTTP Upload	HTTP + json	HTTP + json + events
Content size limit	4.5MB	250MB	
Number of API requests required	1	4 (minimum)	1
Processing time expectation	From 0.3 seconds per MB (varies depending on content complexity)		
Processing time limit	30 seconds	200 seconds	
AWS services required to use	None		S3, IAM and SNS
Content temporarily stored	No	In S3 with KMS	No
Available in multiple regions	✓	✓	✓
Fully documented	✓	✓	✓
Code samples available	✓	✓	✓

The fastest and simplest way to access Zero Trust CDR as a Service is through the Instant API. It doesn't require any special infrastructure and allows for quick uploading and downloading.

The Instant API is only appropriate for content up to 4.5MB in size. The other Zero Trust CDR APIs may be more suitable for processes that don't want or need to wait for a complete response.

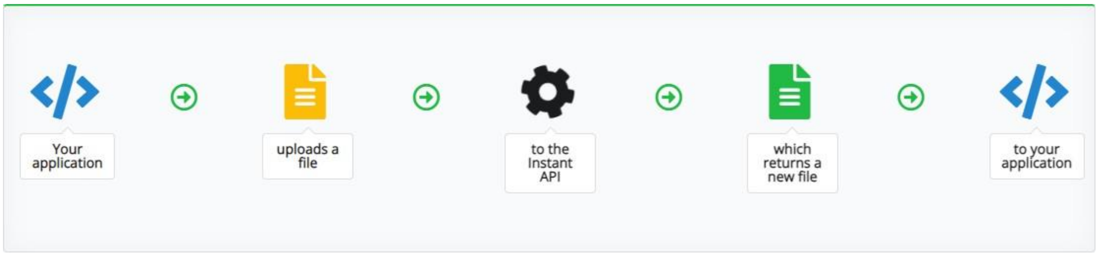
You can upload files using the Zero Trust CDR APIs and download new files in return. The new file will contain all the valuable information but none of the potentially harmful materials that can be present in that file format. This is the primary distinction between our newest Zero Trust CDR technology and current anti-virus detection-based methods. Malicious content is simply left behind.

Requirements

- FileOrbis Application
- Forcepoint Zero Trust CDR API Keys (Please contact Forcepoint Sales Team)

Flow diagrams

- The normal flow of Instant API



Limits (only for demo keys)

We have some limits in place to help maintain a good level of service for everyone. If you have any concerns about these limits, please get in touch with a Forcepoint sales representative.

- File size: The maximum supported file size is about 4.5MB (roughly 4,700,000 bytes as it depends on the full request size including headers)
- Complexity: Files will be processed for up to 30 seconds; very rarely this may not be enough to complete processing
- Traffic: All accounts are subject to a generous throttling profile

Charging

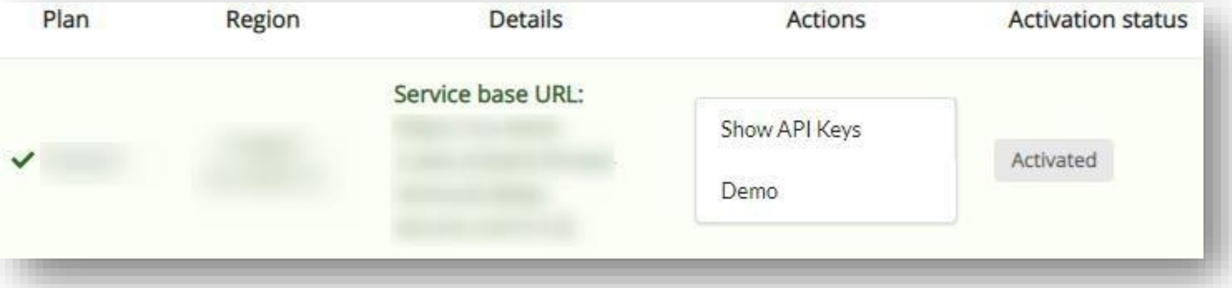
The API calls to/upload will be charged per MB. Some errors can be caught before charges are incurred. These are limited to the format of the request body and headers. Please note that issues such as an invalid PDF can not be detected in advance and will be charged. You will be responsible for all charges incurred within your own infrastructure – wherever that may be. This includes any network data transfer charges. If your calls are made in the same region as the API endpoint then, as of the time of writing, data transfer is free.

Authentication

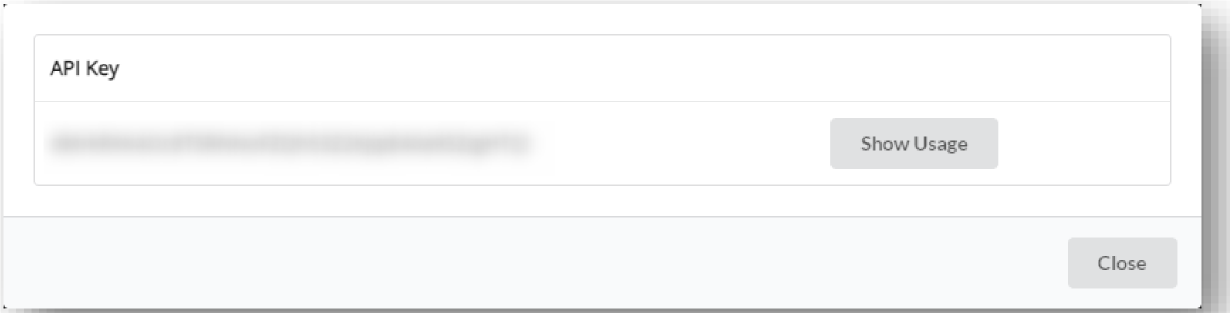
Every API call requires authentication, which is performed using an API Key with the name x-api-key in the request header.

Recommendations (Only for demo keys)

We suggest enforcing a 4.5MB limit when a user first uploads a file if you are sending user-uploaded data to the API. API keys will be provided by the Forcepoint sales team, so before proceeding please obtain your API keys. Your license will include the Service URL, API key and any other information you need to use the service. If you want to use 30-day demo keys, please visit http://threat-removal.deep-secure.com



Plan	Region	Details	Actions	Activation status
✓ [redacted]	[redacted]	Service base URL: [redacted]	Show API Keys Demo	Activated

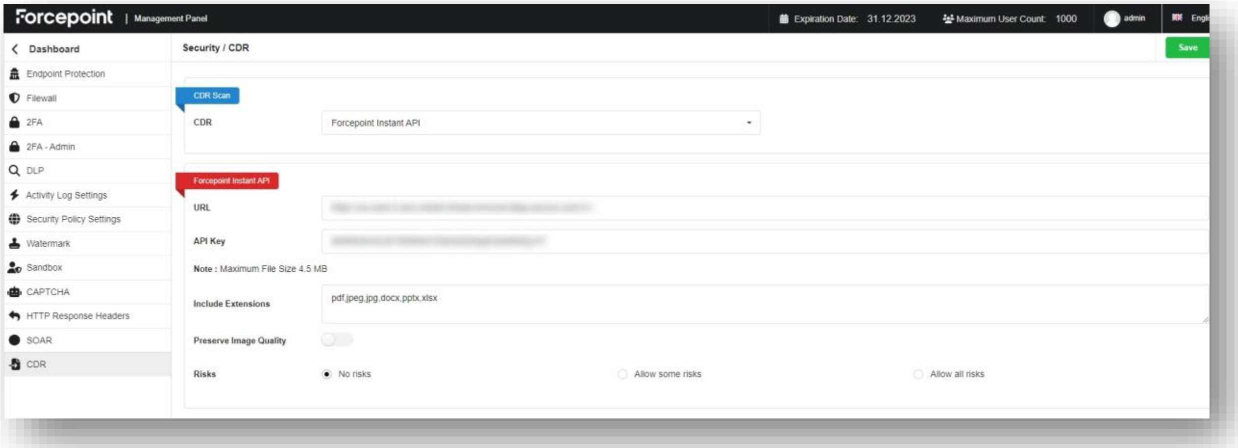


API Key

[redacted]

Step 2: Configuring CDR Settings in FileOrbis

FileOrbis uses the Instant API as well. The administrator can integrate with Forcepoint Zero Trust CDR in the **Administration Panel** > **Security** > **CDR** section.



Security / CDR

CDR Scan

CDR: Forcepoint Instant API

Forcepoint Instant API

URL: [redacted]

API Key: [redacted]

Note : Maximum File Size 4.5 MB

Include Extensions: pdf,jpeg,jpg,docx,pptx,xlsx

Preserve Image Quality

Risks: ● No risks ○ Allow some risks ○ Allow all risks

Attributes	Description
CDR	Forcepoint Instant API
URL	Please enter the Service Base URL address provided from the Deep Secure web site. https://threat-removal.deep-secure.com/
API Key	Enter the API key by clicking "Show API Keys" button
Include Extenstions	Supported File Types - Word (DOCX) - PowerPoint (PPTX) - Excel (XLSX) - Adobe (PDF) - Image formats (PNG, JPG, JPEG 2000, BMP, GIF, TIFF)
CDR	Forcepoint Instant API
Preserve Image Quality	Image files can hide data to enter or leave an organization undetected. Image steganography hides data in images. Some types of steganography are impossible to detect. As more information is stored, the image changes, limiting the ability to hide information. By adding meaningless information to the image using steganography, we can destroy any attacker-hidden information. If you want to preserve the image quality and accept the risk of steganography (or are sure there in no steganography in the image), you can give the service a list of file types to transform without anti-steganography disruption. The feature is found in the options object under **Images** > **Quality** > **Preserve API definition details**.
Risk	The APIs can be set to “allow” particular risks. The supplied list of allowed risks is used to customize the transformation to suit your particular risk profile.

Note: File extensions to be included for Forcepoint are separated by commas and added to the “Included Extensions” field. Note: CDR violations can be monitored from usage reports and security violation reports.

Available Risk

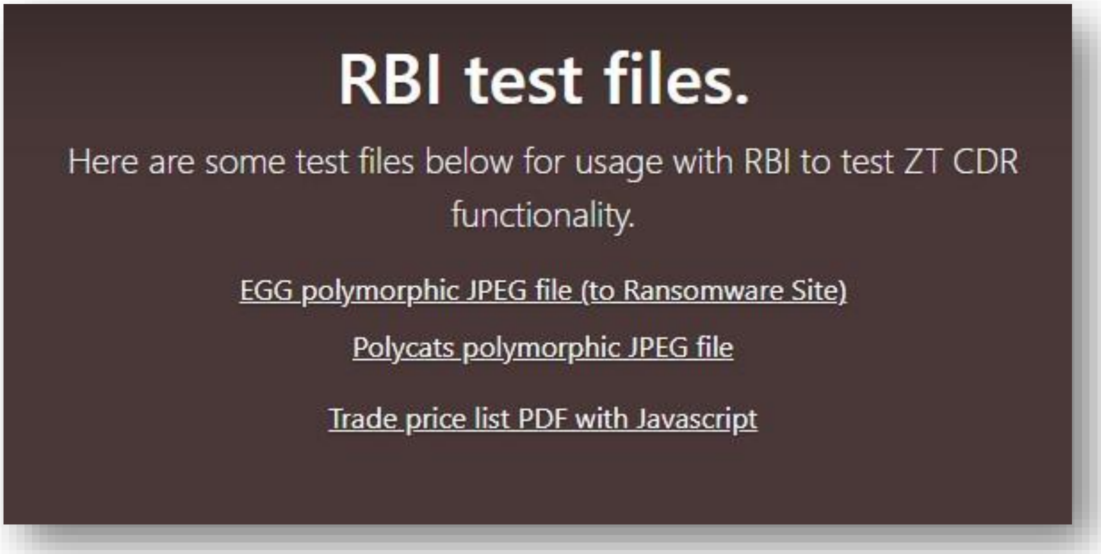
The supported risks are listed in the below chart. The name of the risk is given along with the content type of the data it supplies.

Risk	Applies To	Details	Fallback
exe/macro/ms/excel	application/vnd.ms-excel.sheet.macroEnabled.12 application/vnd.ms-excel.template.macroEnabled.12 application/vnd.ms-excel.addin.macroEnabled.12	Preserve macros in Microsoft Excel spreadsheet. See information on Microsoft Ofiice macros.	XLSX
exe/macro/ms/powerpoint	application/vnd.ms-powerpoint.presentation.macroEnabled.12 application/vnd.ms-powerpoint.template.macroEnabled.12 application/vnd.ms-powerpoint.addin.macroEnabled.12 application/vnd.ms-powerpoint.slideshow.macroEnabled.12	Preserve macros in Microsoft PowerPoint presentantions. See information on Microsoft Office macros.	PPTX
exe/macro/ms/word	application/vnd.ms-word.document.macroEnabled.12 application/vnd.ms-word.template.macroEnabled.12	Preserve macros in Microsoft Word documents. See information on Microsoft Office macros.	DOCX
poly/text/xml	application/xml	Allow XML documents even though they are text that could also be interpreted as an alternative file format. See risks of structured data files.	
poly/text/json	application/json	Allow JSON documents even though they are text could also be interpreted as an alternative file format. See risk of structured data files.	
structured/no-schema/xml	application/xml	Allow XLM documents without schema validation. See risk of structured data files.	
structured/no-schema/json	application/json	Allow JSON documents without schema validation. See Risk of structured data files.	
steg/image/jpeg	image/jp2		
steg/image/jpeg2k	image/jxr		
steg/image/bmp	image/bmp		
steg/image/gif	image/gif		
steg/image/png	image/png		
steg/image/webp	image/webp		
steg/image/pdf	application/pdf	Allow PDF documents with images that have not had steganography distruption applied to them. See Risk of preserving image quality.	

Step 3: Verifying Forcepoint Zero Trust CDR in FileOrbis

Here are some test files in the following link for usage with RBI to test ZT CDR functionality.
https://d1feca3rl8vt87.cloudfront.net/testfiles/index.html

The files at this URL are for demo purposes, but each of them contains some sample threats that cannot be detected by malware analysis systems and sandbox systems. Although the files here are harmless examples, we recommend that you be careful while performing this process.



RBI test files.

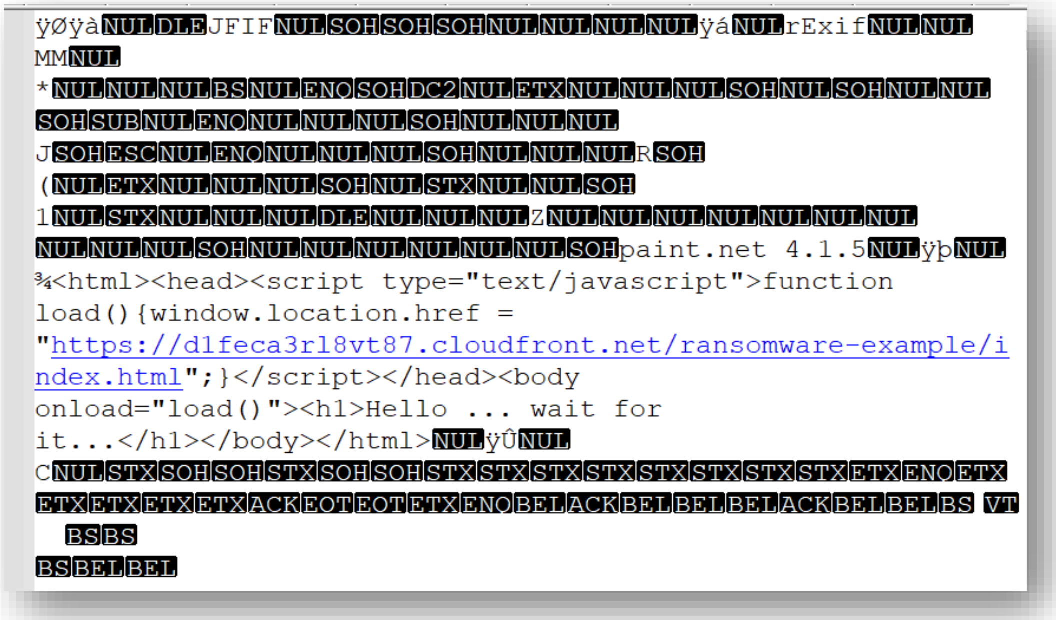
Here are some test files below for usage with RBI to test ZT CDR functionality.

EGG polymorphic JPEG file (to Ransomware Site)

Polycats polymorphic JPEG file

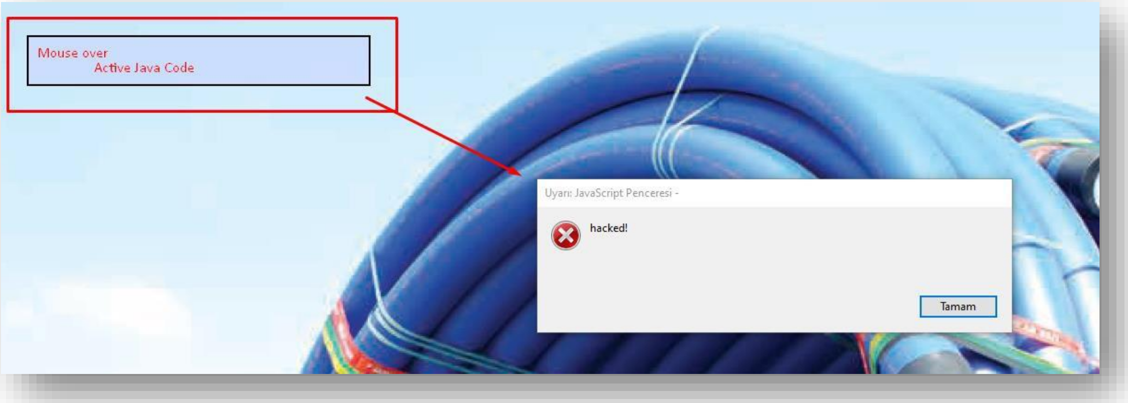
Trade price list PDF with Javascript

Please download the "EGG polymorphic JPEG file", then open with Notepad++, then you will be able to see a sample malicious URL. Please keep the file, we will need it when testing on FileOrbis.



```
ÿØÿàNULDLEJFIFNULSOHSOHSOHNULNULNULNULÿáNULrExifNULNUL
MMNUL
*NULNULNULBSNULENQSOHDC2NULETXNULNULNULSOHNULSOHNULNUL
SOHSUBNULENQNULNULNULSOHNULNULNUL
JSOHESCNULENQNULNULNULSOHNULNULNULRSOH
(NULETXNULNULNULSOHNULSTXNULNULSOH
1NULSTXNULNULNULDLENULNULNULZNULNULNULNULNULNULNUL
NULNULNULSOHNULNULNULNULNULNULSOHpaint.net 4.1.5NULÿþNUL
¾<html><head><script type="text/javascript">function
load(){window.location.href =
"https://d1feca3rl8vt87.cloudfront.net/ransomware-example/i
ndex.html";}</script></head><body
onload="load()"><h1>Hello ... wait for
it...</h1></body></html>NULÿÛNUL
CNULSTXSOHSOHSTXSOHSOHSTXSTXSTXSTXSTXSTXSTXSTXETXENQETX
ETXETXETXETXACKEOTEOTETXENQBELACKBELBELBELACKBELBELBS VT
  BSBS
BSBELBEL
```

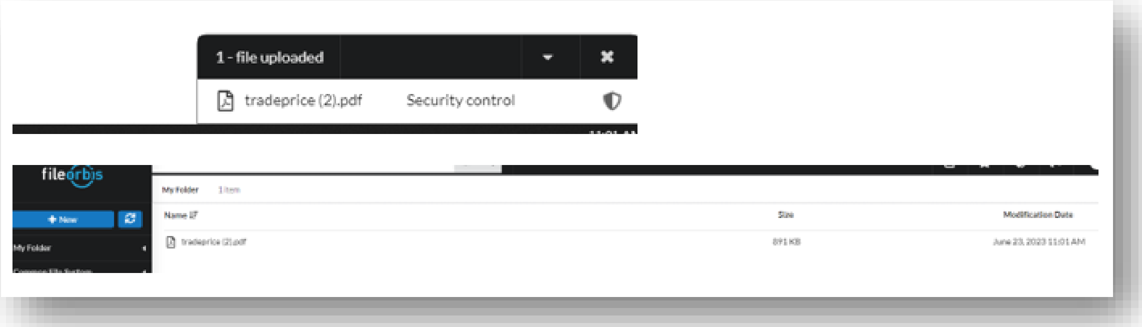
Please download the “Trade Price List PDF… file,” then open with Acrobat Reader, then you will see a sample funny JS message “Hacked” when you move your mouse over to the place shown in the picture. Please don't worry because these are harmless codes. But you should know that this is how advanced attacks happen today. Please keep the file, we will need it when testing on FileOrbis.



hacked!

Now, if you wish, let's see how the CDR solution cleans these files while sending or receiving such files on FileOrbis.

Now let's log in to the FileOrbis portal and try to upload one of our samples to the FileOrbis platform. As you can see from the picture below, the file will be scanned by the CDR during upload or download, and depending on the FileOrbis policies, the activity will be completely blocked or cleaned without being blocked.



1 - file uploaded

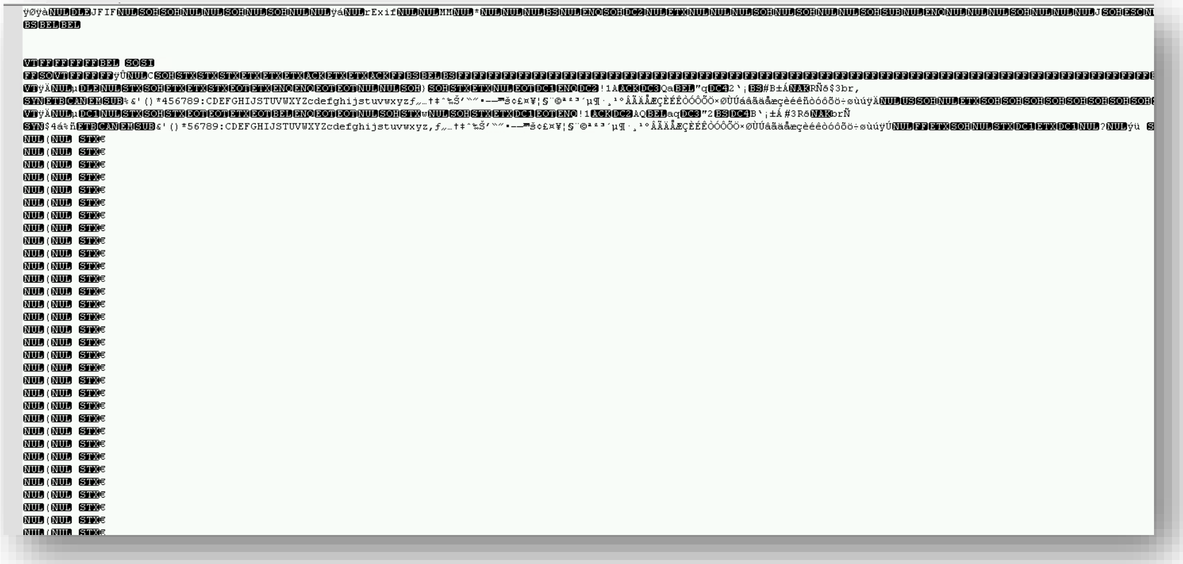
tradeprice (2).pdf Security control

My Folder 1 item

Name ↓F	Size	Modification Date
tradeprice (2).pdf	891 KB	June 23, 2023 11:01 AM

If we look at the file in the case of a cleaning scenario, you will see that the content in the PDF file remains, but the relevant hacking code is now cleared.

When attempting to upload or download an EGG polymorphic JPEG file and opening it with Notepad++, you will notice that the malicious URL has been removed from the file's text representation. However, when viewing the picture itself, no visible changes will be apparent.



```
ÿØÿàNULDLEJFIFNULSOHSOHNULNULSOHNULSOHNULNULÿáNULrExifNULNULMMNUL*NULNULNULBSNULENQSOHDC2NULETXNULNULNULSOHNULSOHNULNULSOHSUBNULENQNULNULNULSOHNULNULNULJSOHESCN
BSBELBEL


VTFFFFFFFFBEL SOSI
FFSOVTFFFFFFÿÛNULCSOHSTXSTXSTXETXETXETXACKETXETXACKFFBSBELBSFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
VTÿÄNULµDLENULSTXSOHETXETXSTXEOTETXENQENQEOTEOTNULNULSOH}SOHSTXETXNULEOTDC1ENQDC2!1AACKDC3QaBEL"qDC42`¡BS#B±ÁNAKRÑð$3br,
SYNETBCANEMSUB%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzƒ„…†‡ˆ‰Š′‶″•–—™š¢£¤¥¦§¨©²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄNULUSSOHNULETXSOHSOHSOHSOHSOHSOHSOHSOHS
VTÿÄNULµDC1NULSTXSOHSTXEOTEOTETXEOTBELENQEOTEOTNULSOHSTXwNULSOHSTXETXDC1EOTENQ!1ACKDC2AQBELaqDC3"2BSDC4B`¡±Á#3RðNAKbrÑ
SYN$4á%ñETBCANEMSUB&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz,ƒ„…†‡ˆ‰Š′‶″•–—™š¢£¤¥¦§¨©²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚNULFFETXSOHNULSTXDC1ETXDC1NUL?NULýü S
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
NUL(NUL STX€
```

About the Author

Kemal Artikarslan has been working with the Forcepoint Turkey team since 2011 as a Sr. Sales Engineer. With over 20 years of experience in software development, data security, network security, and system security he specializes in catering to the needs of large-scale corporations, Telco, and financial companies. His role involves identifying the requirements of organizations within the scope of all Forcepoint solutions and generating tailored solutions for them.

Caglayan Derinbay has been working at FileOrbis as a Senior Technical Account Manager. He has more than 15 years of background of architecturing mixed solutions and providing consulting to meet the needs of organizations.

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.