

Fortiro Connector for ABBYY Vantage

Integrating document forensics with intelligent document processing for enhanced security and efficiency.

By: Deepak Goyal (Partner Innovation and Enablement Specialist At ABBYY)

Table of Contents

About Fortiro Connector for ABBYY Vantage 3

System Requirements and Limitations..... 4

Installing the Connector 4

Integration of Fortiro in ABBYY Vantage..... 5

 API authentication for Fortiro 5

 Fortiro API operations and sequence..... 5

 Configuring the Connector in Vantage 6

High Level workflow of Process skill 9

About Fortiro Connector for ABBYY Vantage

The Fortiro and ABBYY Vantage Connector is a powerful integration that brings together Fortiro's advanced document forensics capabilities with the ABBYY Vantage's Intelligent Document Processing (IDP) platform. This connector enables organizations to leverage Fortiro's proprietary methods for detecting fraud indicators in documents, while benefiting from ABBYY Vantage's robust data extraction, workflow automation, and document analysis features.

Fortiro Protect analyses documents to detect indicators of fraud through its API and web-based User Interface (UI). It provides critical information such as identified fraud indicators, data points within the document that triggered these indicators, and an overall Fraud Score. The Fraud Score reflects the level of risk based on the identified fraud indicators and their quantity, helping organizations to assess the likelihood of document fraud accurately.

ABBYY Vantage is an IDP platform that automates the extraction of data from documents, streamlines workflows, and enhances document analysis with high accuracy and efficiency. It enables businesses to process vast amounts of documents quickly and reliably, improving operational efficiency and reducing manual intervention.

The integration of Fortiro Protect with ABBYY Vantage allows businesses to:

- **Optimize document processing workflows:** Combine the strengths of Fortiro's forensic analysis with ABBYY Vantage's automation capabilities to create a comprehensive document management and fraud prevention system.
- **Seamlessly detect and manage document fraud:** Automatically identify suspicious documents and route them to fraud teams for further investigation or reject highly fraudulent documents without additional review.
- **Enrich fraud prevention strategies:** Use the detailed fraud analysis and scores from Fortiro Protect to enhance existing fraud detection solutions.

This connector empowers organizations to achieve higher standards of security and efficiency in their document processing and fraud detection efforts, ensuring reliable and effective handling of sensitive information.

System Requirements and Limitations

You will require an ABBYY Vantage account, a valid subscription for ABBYY Vantage, and a Vantage user that is assigned the Skill Designer role to configure and to run your workflow.

You will also need an Fortiro Protect account that has the permissions required to access API.

ABBYY Vantage Fortiro Connector works with:

- ABBYY Vantage 2.6 or later,
- Fortiro Protect Tenant.

Installing the Connector

ABBYY Vantage Integration with Fortiro is a script that runs in an Output or Custom Activity of a Process Skill.

The current version of ABBYY Vantage Integration with Fortiro is configured by modifying the script (see Configuring the Connector below).

Integration of Fortiro in ABBYY Vantage

API authentication for Fortiro

API Authentication is performed using API Keys. IP whitelisting can be performed upon request. API Keys are passed through HTTP headers when sending requests to Fortiro.

As part of the integration effort, Fortiro will send API Keys in an encrypted zip file to your developers. The API Key then needs to be included in the X-API-Key header on all requests.

#IMPORTANT# The API key should be treated as a 'secret' and should therefore not be stored directly in code hence API key is stored in Environment Variables in ABBYY Vantage.

Fortiro API operations and sequence

There is a common sequence of API operations that will apply to most requests sent to Fortiro:

1. Generate a GUID (Globally Unique Identifier)
2. Generate upload link (repeatable)
3. Upload file (repeatable)
4. Create Scan UID.
5. Check status of Scan.
6. Retrieve Score for scan.

#Important# The most up-to-date version of the swagger documentation can be found at below link using API key or please refer to API guide provided by Fortiro:

Production: <https://api.protect.fortiro.com/app/v2/protect/v2/api-docs>

Staging/Pre Production: <https://api.protect-staging.fortiro.com/app/v2/protect/v2/api-docs>

Configuring the Connector in Vantage

To configure ABBYY Vantage connector for Fortiro, you should follow below steps.

Step 1:

Configure the document skill to be used by adding “Fraud Check” fields as it will be required to show the data received from Fortiro during manual review.

Important#: Name of “Fraud Check” fields can be customized and configured in process skill as per need also the export of “Fraud Check” fields can be customized.

“Fraud Check” fields are as below:

Link: Link to Fortiro Protect UI for document analysis.

Score: Based on Fortiro document forensic score is calculated to indicate the risk level.

Parameters/Scan_UID: This fields show the scan ID generated by Fortiro for the particular document and can be used to refer the document in Fortiro UI when needed.

Parameters/Transaction_Status: This field is to capture the status of particular transaction status in Fortiro.

The screenshot displays the configuration for a 'Fraud Check' field. It is organized into three sections:

- Link:** A text input field containing the URL: `https://ABBYY.app.protect-us.fortiro.com/scan-results/2d88d088-86b1-40c1-aeb0-ee0926b89d83`.
- Score:** A dropdown menu currently set to 'High Risk'.
- Parameters:** A section containing two fields:
 - Scan_GUID:** A text input field containing the GUID: `2d88d088-86b1-40c1-aeb0-ee0926b89d83`.
 - Transaction_Status:** A dropdown menu currently set to 'SUSPICIOUS'.

Step 2:

Configure the custom script rule in Fraud Check/Score field to highlight the field for manual review in case of **High Risk** and **Low Risk** flag is raised by Fortio.

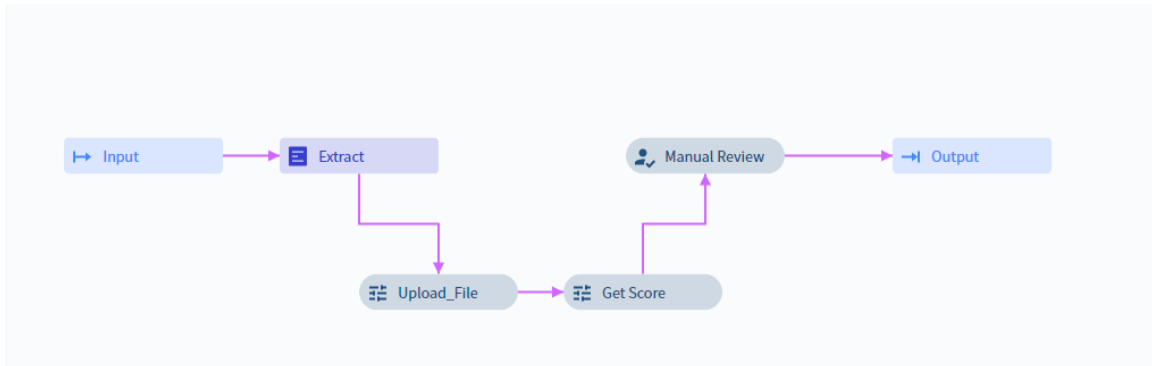
```

1 var scoreFld = Context.GetField("Fraud Check/Score");
2
3
4 //if the score field doesn't contain a value or the value is NORMAL or TRUSTED then no issue
5 if(!scoreFld.Value || scoreFld.Value === "NORMAL" ){Context.CheckSucceeded = true;}
6 else if(scoreFld.Value === "Low Risk" || scoreFld.Value === "High Risk"){
7     Context.CheckSucceeded = false;
8     Context.ErrorMessage = "Fraudulent document detected: " + scoreFld;
9 }
10 else{
11
12     Context.CheckSucceeded = false;
13     Context.ErrorMessage = "Field value doesn't match allowed values: " + scoreFld;
14 }

```

Step 3:

Configure Process skill to create 2 custom activities one to upload the file into Fortiro API and another to check status and another to get status and score.



Step 4:

Create two environment variables for API Key & Protect URL

To manage variables, click on Configuration and open the Environment Variables tab. Here you can view a list of existing variables, edit them, and create new variables.

Each variable name must be unique within a tenant. Its length should not exceed 255 characters and the length of the variable's value should not exceed 16000 characters.

To create a new variable, do the following:



1. Click **Create** Variable.
2. Specify its name, value, and an optional **description** for it.
3. Click **Save**.



Tenant Administration

General
Identity Provider
Public API Client
Security Log
Environment Variables
IP Restrictions

Environment Variables

Environment variables can be used by skills to adjust their behavior to the current Vantage instance, e.g. secrets are used to store credentials to connect to third-party services in this environment.

+ Create Variable  

Type	Name	Value	Description
Secret 	Fortiro API Key	*****	Not specified
Secret 	Fortiro Protect URL	*****	Not specified

Step 5:

To ensure secure communication and efficient integration, in last step we stored the environment variables for the API Key and the Protect URL. These variables will be utilized within custom activities to avoid exposing sensitive data directly in the code. For the first custom activity (Upload File), retrieve the environment variables as demonstrated below:

1. API Key: Retrieve the Claude API key securely in the environment variables using `Context.GetSecret("Claude_API_key")`.
2. Protect URL: Retrieve the target endpoint URL securely as `Context.GetSecret("Protect_URL")`.

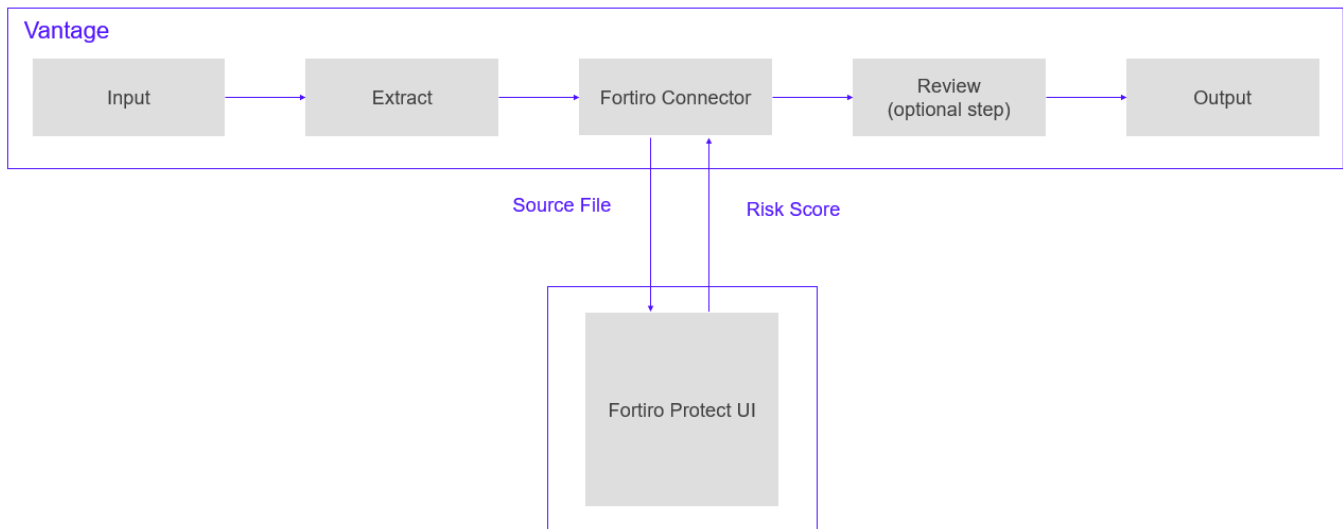
These variables will then be accessed within the custom activities, ensuring both security and flexibility in the integration.

```
1 // Below parameters need to be configured
2 const apiKey = Context.GetSecret("Fortiro API Key"); // API key from Environment Variable
3 const authToken = Context.GetSecret("Fortiro API Key"); // Auth token from Environment Variable
4 const baseUrl = Context.GetSecret("Fortiro Protect URL"); // Base URL from Environment Variable
5 const document = Context.Transaction.Documents[0]; // Assuming a single document per transaction
6 const fileContent = document.SourceFiles[0]; // Get the source file content
7 const scan_name = Context.Transaction.Id // Scan name is stored in fortiro which is transaction ID from Vantage
```

In second custom activity (Get Score) configure variables as shown below which includes the tenant ID received from Fortiro team.

```
1 // Below parameters need to be configured
2 const apiKey = Context.GetSecret("Fortiro API Key"); // API key from Environment Variable
3 const authToken = Context.GetSecret("Fortiro API Key"); // Auth token from Environment Variable
4 const baseUrl = Context.GetSecret("Fortiro Protect URL"); // Base URL from Environment Variable
5 const document = Context.Transaction.Documents[0]; // Assuming a single document per transaction
6 const scanGUID = document.GetField("Fraud Check/Parameters/Scan_GUID").Text; // Scan GUID to be used
7 const tenantID = "ABBY";
```


High Level workflow of Process skill



- **File Reception:** A document file is received and enters the processing workflow.
- **Data Extraction with ABBYY Vantage:** The file is sent to extraction activity. It will extract the relevant data from the document using its Intelligent Document Processing (IDP) capabilities.
- **Custom Activity: Send to Fortiro for Forensic Analysis:** The source file is sent to Fortiro Protect via a custom activity using the Fortiro API. Fortiro Protect analyzes the document for potential fraud indicators.
- **Custom Activity: Retrieve Fraud Risk Score:** A custom activity checks the status of the forensic analysis via the Fortiro API. The risk score and transaction status are retrieved from Fortiro Protect.
- **Fraud Detection Rule Evaluation:** The retrieved fraud risk score is evaluated against predefined rules. If the score indicates a high likelihood of fraud, the document is flagged for manual review.
- **Manual Review:** The flagged document undergoes manual review by a fraud team to verify the fraud indicators. If the document is cleared after manual review, it proceeds to the next step.
- **Output Creation:** Once cleared, an output file containing the extracted data is created. This output file can be used for further processing or storage.

This workflow ensures that documents are thoroughly analysed for fraud, leveraging the strengths of both ABBYY Vantage's data extraction and Fortiro Protect's forensic analysis, while providing a mechanism for manual review of flagged documents to ensure accuracy and security.