# Table of Contents

Overview ......................................................................................................................................................................... 3  
FTK Connect – Demisto Integration Flow Diagram ......................................................................................................... 3  

1  FTK Connect ............................................................................................................................................................. 4  
  1.1  Prerequisites ................................................................................................................................................... 4  
  1.2  FTK Connect Workflow Setup ......................................................................................................................... 4  

2  Cortex XSOAR (Demisto) .......................................................................................................................................... 8  
  2.1  Prerequisites ................................................................................................................................................... 8  
  2.2  Cortex Playbook Set Up Configuration ......................................................................................................... 11  
  2.3  Manual Incident creation .............................................................................................................................. 16  
  2.4  Cortex XSOAR Results ................................................................................................................................... 17  
  2.5  FTK Connect Results ...................................................................................................................................... 19  
  2.6  Validation Summary ...................................................................................................................................... 21  

Contact Exterro ............................................................................................................................................................. 22
Overview

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today. We deliver a fully integrated Legal GRC platform that enables our clients to address their privacy, regulatory, compliance, digital forensics, and litigation risks more effectively and at lower costs. We provide software solutions that help some of the world’s largest organizations, law enforcement and government agencies work smarter, more efficiently, and support the Rule of Law.

FTK Connect – Cortex XSOAR Integration Flow Diagram
1 FTK Connect

1.1 Prerequisites

- A Case should be created.
- Collection templates should be created based on the user requirements.

1.2 FTK Connect Workflow Setup

1. Login into the FTK Central application and select FTK Connect.
2. Click Create.
3. Provide the **Automation Name**.
4. Provide the **Description**.
5. Click **Actions**.
   - The **Actions** section is displayed.
6. Select the API Trigger option for the Trigger field.

7. Select Case Details from the left pane.
   - The Case Details section is displayed in the middle pane.

8. Select the Existing option for Case field.

9. Select the required Case from the Case drop-down field.

10. Select Collection from the left pane.
    - The Collection section is displayed in the middle pane.

11. Select the required Collection Template.
12. Click **Schedule**.
13. Click **Finish**.

The workflow will be created. The Automation ID generated for the workflow should be used to configure the Playbook parameters in Cortex XSOAR platform.
2 Cortex XSOAR

2.1 Prerequisites

- The **EnterpriseApiKey** should be generated using the below URL:

  \(<\text{ftkcapp}/\text{api/security/}\<\text{user_id}>/\text{getenterpriseapiguid}\>

  **Example:**

  Upon executing the above URL for the `user_id=1000`, the EnterpriseApiKey will be generated as `f34d469a-b121-41b8-b154-22dc176439c7`. 

  ![XML example](image-url)
• The following configurations should be made in the Cortex server:

i. Login into Cortex server.

ii. Click on 🔄 from the navigation menu (left side).

iii. Search for the AccessData integration.

iv. Click against the AccessData integration.
The AccessData pop-up is displayed.

v. Configure the Name, Web Protocol, and Service URL.

vi. Provide the EnterpriseApiKey for the API authentication key field.

vii. Click Save & Exit.
2.2 Cortex Playbook Set Up Configuration

A Playbook should be created for each workflow to trigger the corresponding incident response.

To create a Playbook:

1. From the Cortex server, click from the navigation menu (left side).
2. Click New Playbook.
   - The New Playbook pop-up is displayed.
3. Provide the Playbook Name.
4. Click Save.
5. From the **Task Library** section, expand the AccessData integration section.

6. Search for the term ‘workflow’.

7. Click on **Add** against the `accessdata-trigger-workflow` task.
8. Provide the value for **Automationid** field. (This can be obtained by following the steps in the FTK Connect Workflow Setup section)

9. Click on against the **targetips** field.

10. Map the required field (present under the Incident details section) for the **targetips** parameter (Example: Source IP). This should be done in order to set the value of Agent IP with the required incident.

11. Click **OK**.

• The **Task Details** page is displayed.
12. Establish connection between the **Playbook Triggered** and the newly created task.
13. Click on 🔄.
   - The **Playbook Settings** section is displayed.

14. Expand the **Playbook Triggers** option and select the required **Incident type**. *(Example: CrowdStrike Falcon Incident).*

15. Click **Save Playbook**.
2.3 Manual Incident creation

1. From the Cortex server, click on 🏛️ from the navigation menu (left side).
2. Click on New Incident.
   - The New Incident pop-up is displayed.

3. Enter incident Name and choose the required incident Type. (Example: CrowdStrike Falcon Incident).
4. Enter the agent IP address for Source IP field.
5. Click Create new Incident.
2.4 Cortex XSOAR Results

The following are the results displayed for the above configurations:

**Incident section:**

![Incidents Table](image_url)
**Incident Details page:**

- Incident ID: #27 memory collection incident 10 - Incident Info
- Case Details:
  - Type: Custom
  - Severity: @ Unknown
  - Owner: @ Admin
  - Source Instance: admin
  - Playbook: ftk-connect-memory-collection-demo
- Timeline Information:
  - Occurred: July 14, 2022, 08:28 PM
  - Last Updated: July 14, 2022, 08:30 PM
- SLA: N/A
- Investigation Data:
- Evidence (0):
  - This incident does not contain evidence.

**Incident Status:**

- Task Status:
  - Task #1: accessdata-trigger-workflow
  - Task Info:
    - Comments:
      - Created: accessdata-trigger-workflow workflowId="133" targetType="172.31.87.198" using-brand="AccessData"
      - Results
        - Result: true
        - Status: true
  - Task #1 Done: accessdata-trigger-workflow
2.5 FTK Connect Results

The following results are obtained in the Job monitor and collection when an incident triggers the Playbook.

FTK Connect Job Monitors (Status: In-Progress):
Manage Collections Page:

Collection Details page:
2.6 Validation Summary

- Individual collection template can be created for each Agent Scan Type (Software Inventory, Agent Remediation, Volatile Job, Threat Scan, Memory Acquisition, Memory Analysis)
- Individual automation workflow is created for each collection template in the FTK connect application.
- The Agent scan type collections will be triggered based on the incident type configured for the Playbook.

Above flow is an One-to-One mapping
Contact Exterro

If you have any questions, please refer to this document, or any other related materials provided to you by Exterro. For usage questions, please check with your organization’s internal application administrator. Alternatively, you may contact your Exterro Training Manager or other Exterro account contact directly.

For technical difficulties, support is available through support@exterro.com.

Contact:
Exterro, Inc.
4145 SW Watson Ave., Suite 400
Beaverton, OR 97005.
Telephone: 503-501-5100
Toll Free: 1-877-EXTERRO (1-877-398-3776)
Fax: 1-866-408-7310
General E-mail: info@exterro.com
Website: www.exterro.com

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Exterro, Inc. The trademarks, service marks, logos or other intellectual property rights of Exterro, Inc and others used in this documentation (“Trademarks”) are the property of Exterro, Inc and their respective owners. The furnishing of this document does not give you license to these patents, trademarks, copyrights or other intellectual property except as expressly provided in any written agreement from Exterro, Inc.

The United States export control laws and regulations, including the Export Administration Regulations of the U.S. Department of Commerce, and other applicable laws and regulations apply to this documentation which prohibits the export or re-export of content, products, services, and technology to certain countries and persons. You agree to comply with all export laws, regulations and restrictions of the United States and any foreign agency or authority and assume sole responsibility for any such unauthorized exportation.

You may not use this documentation if you are a competitor of Exterro, Inc, except with Exterro Inc’s prior written consent. In addition, you may not use the