# Content Integrity Control with EFT

**THE INFORMATION IN THIS ARTICLE APPLIES TO:**

- EFT v7.0.3 and later

**DISCUSSION**

The Internet Content Adaptation Protocol (ICAP) is an HTTP-like protocol that is used for virus scanning and content filtering. According to RFC 3507, ICAP is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for some sort of transformation or other processing ("adaptation"). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses.

EFT's ICAP functionality is invoked through Event Rules, sending files to antivirus or data leak prevention (DLP) servers that detect file pass/fail based upon user-defined rules. Users can configure rules on a DLP server to send a reply to EFT with access denied if the file contains social security numbers (SSNs) or credit card numbers (CCNs), for example. Antivirus servers scan the files for viruses and return a response to EFT whether a virus was found or not.

- On a DLP server, you can define rules to search files for SSNs or CCNs. For example, if you send a file containing a valid CCN, the DLP server will flag it and return a denied message to EFT. (To test this rule, you can put the universal test credit card number 4111 1111 1111 1111 in a text file and send it through the DLP via an EFT Event Rule.)
- On an antivirus server, you can specify violation text in ICAP response headers: “X-Virus-ID:INFECTED” or ”X-Response-Info:blocked” or both (semicolon-separated).

If a file isn't completely processed/analyzed by an antivirus or DLP server due to the size of the file being larger than what is supported by that particular server, EFT does not return an error or any type of indicator from the File: Scan Action. For example, MyDLP will process a maximum of 10 MB of data; if a flag is embedded in a file that is over the 10 MB limit, MyDLP will not detect the policy violation.

For example, suppose EFT sends an 11 MB file to myDLP, which has a max processing capacity of 10 MB. The myDLP server has a policy to return a failure for any files containing credit card numbers. The 11 MB file has a credit card number embedded at the end of file.

As a result, the myDLP server would return to EFT that the Action was a success, because the myDLP server did not process the credit card number.

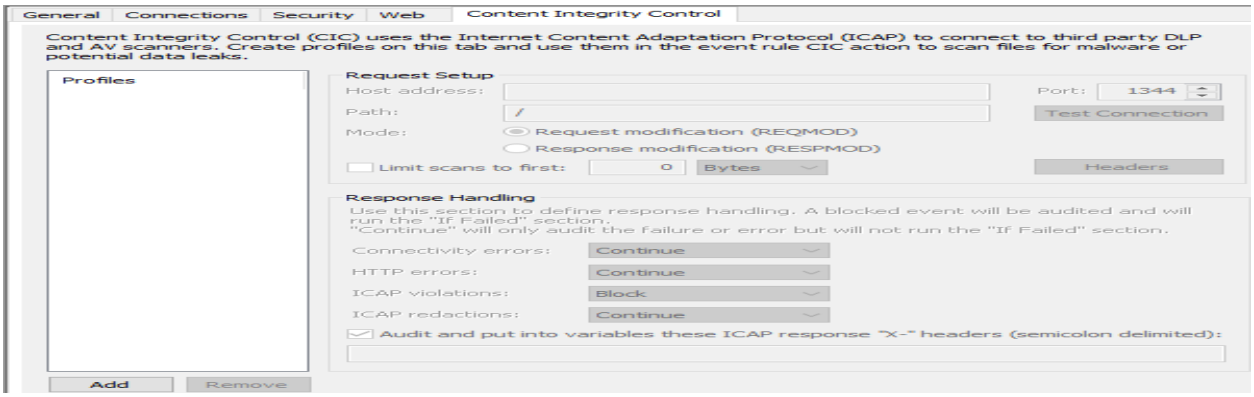
The File: Scan Action is used to send a file to an antivirus or data loss prevention scanner for processing. When this Action is added, a file that triggers the Event Rule is sent to an ICAP server for scanning. When the file passes the scan, other Actions can occur, such as moving the file to another location. If the file fails the scan, processing can stop, or other Actions can occur, such as sending an email notification. EFT fully supports RFC3507 section-3.1 and section-4.8. EFT can adapt the outgoing response if the ICAP server indicates that adaptation is necessary.

"File Uploaded" and "Workspace Created" events are triggered after a file is uploaded and after a Workspace is created. Only after the event is triggered will the action begin communication with the ICAP server, and then redacts the file, if needed. Therefore, there may be delays between when a Workspace is created and a file is redacted. Use the "File Uploaded" event to trigger the action, then use the "File: Scan" action and "Fail" to prevent the message from being sent. Use the "Before Download" event trigger to scan the file before it's downloaded.

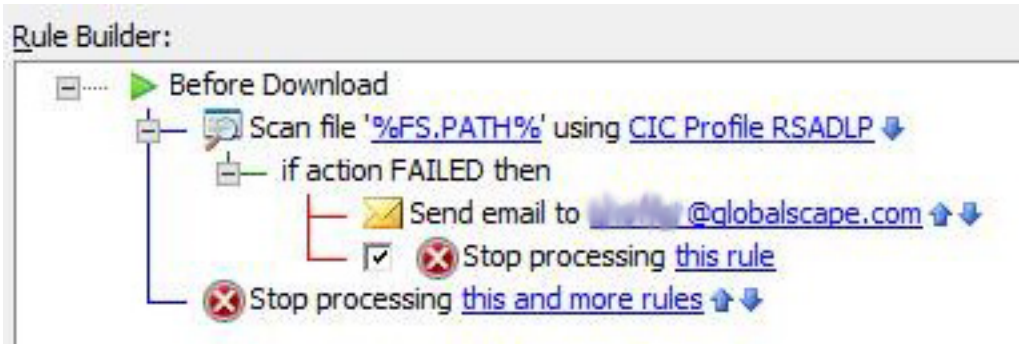
**How does "File: Scan" work in Event Rules?**

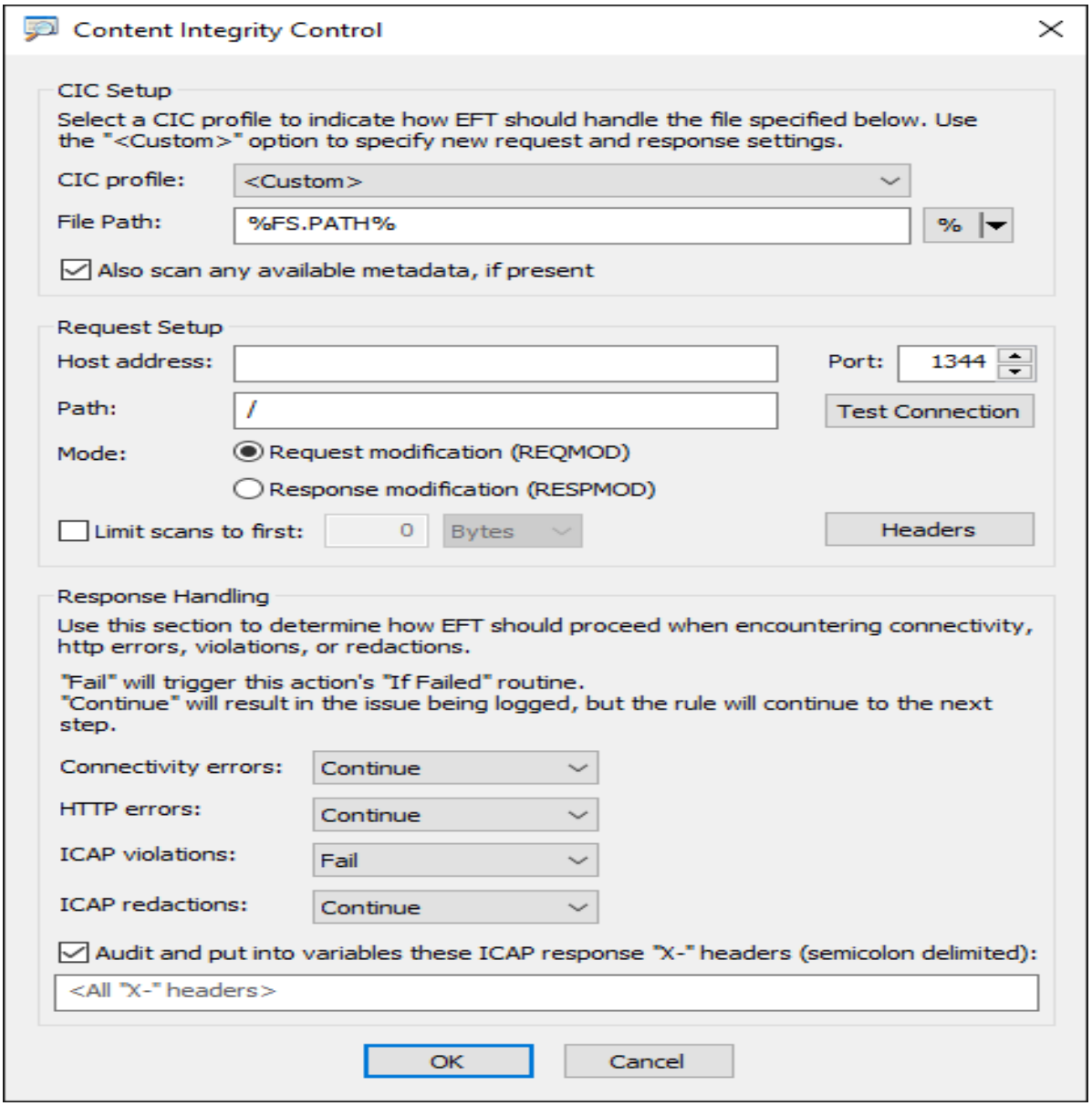
The "File: Scan" Action allows ICAP clients to pass HTTP messages to ICAP servers to scan the file(s) in the Event Rule that is passing through EFT. (Refer to "File: Scan Action" in the help for your version of EFT for details of configuring an event rule using this action.)

You can create reusable profiles on the Site's **Content Integrity Control** tab to use in Event Rules. (Refer to "Create a CIC Profile" in the help for your version of EFT for details of configuring CIC on the site.)



Or you can create the CIC profile "on the fly" when creating the event rule.



# Content Integrity Control with EFT

**Important info about how EFT uses the File Scan Action**

- Using the File: Scan action with encrypted files will not return an accurate result. Copy/move the files to a folder that is not encrypted to process with the ICAP server.
- ICAP servers don't all offer the same features. The action was tested with:
  - Clearswift version 5
  - Symantec DLP version 14.5.0.24028
  - Kaspersky version 5.5
- When using the File: Scan action, EFT needs to use POST in HTTP requests. (See Advanced Properties below.)

## ICAP Options

In v8.0.5 and later, EFT supports the use of the ICAP "Options" method. The ICAP "OPTIONS" method is used by the ICAP client to retrieve configuration information from the ICAP server. In this method, the ICAP client sends a request addressed to a specific ICAP resource and receives a response with options that are specific to the service named by the URI. All OPTIONS requests MAY also return options that apply to all services.

**Advanced Properties**

Advanced properties have been created to address issues that some customers may encounter.

- ICAPUsePOST - Specifies whether to use PUT(0 - default) or POST(1) in CIC HTTP requests (any value above 0 will be converted to 1) https://kb.globalscape.com/Knowledgebase/11375
- ICAPAllowMultipleMethodsForOneURI - When the AP is true, then ICAP client allows you to use ICAP Services with multiple methods (REQMOD and RESPMOD) on the same URI.
- ICAPConnectionTimeoutInMs - Sets the maximum timeout value, in ms, for the CIC module to wait for connections to and reading responses from remote ICAP server. Default 20000 (20 sec). (Setting the timeout higher than maximum will cause EFT to crash during file upload.)
- ICAPUsePreview - Specifies whether to use Preview (1 - default) or not(0) in CIC HTTP requests (any value above 0 will be converted to 1). With some ICAP servers, disabling

# Content Integrity Control with EFT

PREVIEW is needed to process files.

Refer to knowledgebase article https://kb.globalscape.com/KnowledgebaseArticle11375.aspx for information about enabling an advanced property.

**Wireshark capture of OPTIONS RESPMOD from Clearswift:**

```
PTIONS icap://192.168.100.79:1344/policy_service_resp ICAP/1.0 Host: 192.168.100.79 ICAP/1.0
200 OK Server: Traffic Spicer 2.4.0 ISTag: "CSICAP/v2.4.0/cd7ac05/CSAdapter" Methods: RESPMOD
Preview: 0 Allow: 204 Max-Connections: 980 Transfer-Preview: * Encapsulated: null-body=0
X-Include: X-Client-IP, X-Server-IP, X-Authenticated-User, X-Authenticated-Groups
```

**Wireshark capture of OPTIONS REQMOD from Kaspersky:**

```
PTIONS icap://192.168.100.81:1344/av/reqmod ICAP/1.0 Host: 192.168.100.81 ICAP/1.0 200 OK
ISTag: "KAVPROXY" Date: Fri, 05 Feb 2021 20:53:22 GMT Methods: REQMOD Allow: 204 Service:
KAV-ICAP-Sever/5.5 Preview: 0 Max-Connections: 5000 Service-ID: KAVIcap X-Include:
X-Client-IP Transfer-Preview: * Transfer-Ignore: Options-TTL: 300 Encapsulated: null-body=0
```

**Wireshark capture of OPTIONS RESPMOD from Symantec:**

```
PTIONS icap://192.168.100.82:1344/RESPMOD ICAP/1.0 Host: 192.168.100.82 ICAP/1.0 200 OK
ISTag: "Vontu14.5" Methods: RESPMOD Options-TTL: 3600 Preview: 0 Transfer-Preview: * Allow:
204 X-Include: X-Client-IP, X-Authenticated-User Encapsulated: null-body=0 Max-Connections:
16
```

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11581/Content-Integrity-Control-wi...