Configuring Email Gateway to Consume External Threat Feeds

This chapter contains the following sections:

- Overview of External Threat Feeds, on page 1
- How to Configure Email Gateway to Consume External Threat Feeds , on page 2
- Obtaining External Threat Feeds Feature Key , on page 3
- Enabling External Threat Feeds Engine on Email Gateway, on page 3
- Configuring an External Threat Feed Source, on page 4
- Handling Messages Containing Threats, on page 6
- Configuring a Sender Group for Handling Messages containing Threats , on page 7
- Configuring Content or Message Filters for Handling Messages Containing Threats, on page 7
- Attaching Content Filter to Incoming Mail Policy, on page 14
- External Threat Feeds and Clusters, on page 14
- Monitoring External Threat Feeds Engine Updates, on page 15
- Viewing Alerts, on page 15
- Displaying Threat Details in Message Tracking, on page 15

Overview of External Threat Feeds

The External Threat Feeds (ETF) framework allows the email gateway to consume external threat information in:

- STIX format communicated over TAXII protocol.
- JavaScript Object Notation (JSON) format from the Cisco XDR portal.

The ability to consume external threat information in the email gateway, helps an organization to:

- Proactively respond to cyber threats such as, malware, ransomware, phishing attacks, and targeted attacks.
- Subscribe to local and third-party threat intelligence sources.
- Improve the efficacy of the email gateway.

You need a valid feature key to use the ETF feature on your email gateway. For information on how to obtain a feature key, contact your Cisco sales representative.

STIX (Structured Threat Information eXpression) is the industry standard, structured language to represent cyber threat information. A STIX source consists of an indicator that contains a pattern used to detect malicious or suspicious cyber activity.

TAXII (Trusted Automated eXchange of Indicator Information) defines a set of specifications to exchange cyber threat information via services (TAXII servers) across different organizations or product lines.

The following versions of STIX/TAXII are supported for this release - STIX 1.1.1 and 1.2 with TAXII 1.1.

The Cisco XDR portal allows you to create custom feeds for the continuous gathering of observables and to consume them in your email gateway using the feed URL. A feed is a simple list of observables in JSON format. The feeds are created and managed in the **Intelligence** > **Feeds** page in the XDR portal.

Following is a list of STIX and XDR Indicators of Compromise (IOCs) supported for this release:

- File Hash Watchlist (describes a set of hashes for suspected malicious files)
- IP Watchlist (describes a set of suspected malicious IP addresses)
- Domain Watchlist (describes a set of suspected malicious domains)
- URL Watchlist (describes a set of suspected malicious URLs)

How to Configure Email Gateway to Consume External Threat Feeds

Perform these steps in order:

Steps	Do This	More Information
Step 1	Obtain an External Threat Feeds feature key.	Obtaining External Threat Feeds Feature Key , on page 3
Step 2	Enable the ETF engine on your email gateway.	Enabling External Threat Feeds Engine on Email Gateway, on page 3
Step 3	Configure an ETF source to allow your email gateway to fetch threat feeds in STIX format from a TAXII server.	Configuring an External Threat Feed Source, on page 4
Step 7	Handle messages that contain threats using: • HAT • Content or Message filters	Handling Messages Containing Threats, on page 6

Steps	Do This	More Information
Step 8	Attach the content filters that you configured to detect malicious domains, URLs, or file hashes in messages to an incoming mail policy.	Attaching Content Filter to Incoming Mail Policy, on page 14

Obtaining External Threat Feeds Feature Key

Managing Email Gateways using the Smart Software Licensing Mode

If you are an existing or new user using the Smart Licensing mode on your email gateways, you are automatically provided with an External Threat Feeds feature key.

Enabling External Threat Feeds Engine on Email Gateway

Before you begin

Make sure that you have a valid feature key to you use the ETF feature on your email gateway.

Procedure

Step 1 Click **Security Services > External Threat Feeds**.

Step 2 Click **Enable**.

Step 3 Scroll to the bottom of the license agreement page and click **Accept** to accept the agreement.

Note
If you do not accept the license agreement, ETF is not enabled on your Cisco Email Security Gateway.

Step 4 Check **Enable External Threat Feeds**.

Step 5 (Optional) Select **Yes** to add a custom header to all messages that are not scanned for threats by the ETF engine because of an ETF engine lookup failure.

Step 6 Submit and commit your changes.

What to do next

Configure an ETF source. See Configuring an External Threat Feed Source, on page 4.

Configuring an External Threat Feed Source

An ETF source is used to download information about a collection of threats that is available on a TAXII server. You need to configure an ETF source to allow your email gateway to fetch threat feeds in STIX format from a TAXII server.

Note You can configure a maximum of eight ETF sources in your email gateway.

You can configure an ETF source using the Poll service that consists of a 'polling path' and a 'collection name.'

Before you begin

- Make sure that you have enabled the ETF engine on your email gateway.
- Make sure that you open ports - 80 HTTP and 443 HTTPS on your firewall to allow your gateway to consume external threat feeds. For more information, see Firewall Information.

Procedure

Step 1 Click **Mail Policies** > **External Threat Feeds Manager**.

Step 2 Click **Add Source**.

Step 3 Enter the required parameters described in the following table to configure an ETF source.

Parameter Source Details	Description
Source Name	Enter a name for the ETF source.
Description	Enter a description for the ETF source.
TAXII Details	
Hostname	Enter the hostname of a fully qualified domain name or an IP address of a TAXII server.
Polling Path	Enter the polling path that identifies the polling service in a TAXII server, for example, /taxii-data.
Collection Name	Enter the name of a collection of threat feeds that is hosted on a TAXII server, for example, guest.Abuse_ch.
Polling Interval	Enter a polling interval to define the frequency of fetching threat feeds from a TAXII server. The minimum value is 15 minutes and the default value is 60 minutes.

Parameter Source Details	Description
Age of Threat Feeds	Enter the maximum age of a threat feed that can be fetched from a TAXII server. The value for the age must be between one through 365 days.
Time Span for Poll Segment	Enter the time span for each poll segment. The minimum time span for a poll segment is 1 day. The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field. You can use the 'Time Span for Poll Segment' option in the following scenarios: • If there is no known limitation on the age of threat feeds for a TAXII server, use the value entered in the 'Age of Threat Feeds' option. • If there is a known limitation on the age of threat feeds for a TAXII server, use the known limit value. • If you do not know the known limitation on the age of threat feeds for a TAXII server, use the default value of 30 days. • If the value you enter in the 'Age of Threat Feeds' option is not supported by the TAXII server, you can spilt the age of threat feeds into different poll segments based on the time span entered. For example, if the age of the threat feeds is 100 days and the TAXII server has a fixed limit on the age of threat feeds (for example, '40 days'), enter 40 as the time span for poll segment **Note** If the time span for the poll segment is a small value (for example, '5 days',) the polling of the threat feed source can take a long time to complete, and this may impact the performance of your gateway.
Use HTTPS	Select **Yes** if you want to connect to a TAXII server using HTTPS.
Configure Credentials	Select **Yes**, if you want to access a TAXII server using the user credentials that you created in the TAXII server. Enter the username and password.
Proxy Details	

Parameter Source Details	Description
Use Global Proxy	Select **Yes** to connect the email gateway to a TAXII server using a proxy server. You can configure a proxy server in any one of the following ways: • Security Services > Service Updates page in the web interface • `updateconfig` command in the CLI

Step 4 Submit and commit your changes.

After you configure an ETF source, your email gateway begins to fetch threat feeds from a TAXII source.

What to do next

- You can also configure an ETF source using the **`threatfeedsconfig > sourceconfig`** subcommand in the CLI.
- (Optional) Click **Suspend Polling** ( ) icon in the Mail Policies > External Threat Feeds Manager page to suspend the polling service for a configured ETF source.
- (Optional) Click **Resume Polling** ( ) icon in the Mail Policies > External Threat Feeds Manager page to resume the polling service for a configured ETF source.
- (Optional) Click **Poll Now** in the Mail Policies > External Threat Feeds Manager page to fetch the threat feeds from the last successful polling interval immediately.
- See Handling Messages Containing Threats, on page 6.

Handling Messages Containing Threats

You can handle messages that contain threats in your email gateway using:

- HAT
- Content or Message filters

Related Topics

- Configuring a Sender Group for Handling Messages containing Threats , on page 7.
- Configuring Content or Message Filters for Handling Messages Containing Threats, on page 7.

Configuring a Sender Group for Handling Messages containing Threats

You can configure an existing sender group to handle messages that originate from malicious IPs using the verdict obtained from the ETF engine.

Procedure

Step 1 Go to **Mail Policies** > **HAT Overview** page.

Step 2 Click an existing sender group that you want to configure to handle messages that contain threats.

Step 3 Click **Edit Settings**.

Step 4 Select the required ETF source to filter malicious IP addresses.

Step 5 (Optional) Click **Add Row** to add another ETF source.

Step 6 Submit and commit your changes.

Configuring Content or Message Filters for Handling Messages Containing Threats

You can configure one or more of the following content or message filters, to take appropriate actions on messages that contain threats based on the verdicts obtained from the ETF engine:

- URL Reputation - to detect URLs categorized as malicious by the ETF engine.
- Domain Reputation - to detect domains categorized as malicious by the ETF engine.
- Attachment by File Info - to detect files categorised as malicious by the ETF engine based on the file hash.

Related Topics

- Detecting Malicious Domains in Messages Using Content Filter, on page 8.
- Detecting Malicious Domains in Messages Using Message Filter, on page 9
- Detecting Malicious URLs in Messages Using Content Filter, on page 9
- Detecting Malicious URLs in Messages Using Message Filter, on page 11
- Detecting Malicious Files in Message Attachments Using Content Filter, on page 12.
- Detecting Malicious Files in Messages Attachments Using Message Filter.

Detecting Malicious Domains in Messages Using Content Filter

Use the 'Domain Reputation' content filter to detect domains categorized as malicious in messages by the ETF engine and take appropriate actions on such messages.

Before you begin

- Optional) Create an address list that contains only domains. To create one, go to **Mail Policies > Address Lists** page in the web interface or use the `addresslistconfig` command in the CLI. For more information, see Mail Policies.
- (Optional) Create a Domain Exception List. For more information, see Creating Domain Exception List.

Procedure

Step 1	Go to **Mail Policies > Incoming Content Filters**.
Step 2	Click **Add Filter**.
Step 3	Enter a name and description for the content filter.
Step 4	Click **Add Condition**.
Step 5	Click **Domain Reputation**.
Step 6	Select **External Threat Feeds**.
Step 7	Select the ETF source(s) to detect malicious domain(s) in the header(s) of a message.
Step 8	Select the required headers to check for the reputation of the domain.
Step 9	(Optional) Select the list of allow listed domains that you do not want the email gateway to detect for threats for this content filter.
Step 10	Click **OK**.
Step 11	Click Add Action to configure an appropriate action to take on messages that contain malicious domains.
Step 12	Submit and commit your changes.

Creating Domain Exception List

A Domain Exception List consists of a list of addresses that contain only domains. You can use a Domain Exception List if you want the email gateway to skip the domain check for all configured Domain Reputation content or message filters.

Procedure

Step 1	Go to **Security Services > Domain Reputation**.
Step 2	Click **Edit Settings** under Domain Exception List.
Step 3	Select the required address list that contains domains only.
Step 4	Submit and commit your changes.

What to do next

You can also create a Domain Exception List using the domainrepconfig command in the CLI. For more information, see the *CLI Reference Guide for AsyncOS 12.0 for Cisco Email Security Appliances*.

Detecting Malicious Domains in Messages Using Message Filter

As an example, use the following message filter rule syntax to detect malicious domains in messages using the ETF engine, and take appropriate actions on such messages.

Syntax:

```
quarantine_msg_based_on_ETF: if (domain-external-threat-feeds (['etf_source1'],
 ['mail-from', 'from'], <'domain_exception_list'>)) { quarantine("Policy"); }
```

Where

- `'domain-external-threat-feeds'` is the Domain reputation message filter rule.
- `'etf_source1'` is the ETF source(s) used to detect malicious domain(s) in the header(s) of a message.
- `'mail-from','from'` are the required header(s) used to check for the reputation of the domain.
- `'domain_exception_list'` is the name of a domain exception list. If a domain exception list is not present it is displayed as "".

Example

In the following example, if the domain in the 'Errors To:' custom header is detected as malicious by the ETF engine, the message is quarantined.

```
Quaranting_Messages_with_Malicious_Domains: if domain-external-threat-feeds
(['threat_feed_source'], ['Errors-To'], "")) {quarantine("Policy");}
```

Detecting Malicious URLs in Messages Using Content Filter

Use the 'URL Reputation' content filter to detect URLs in messages categorized as malicious by the ETF engine and take appropriate actions on such messages.

You can configure the 'URL Reputation' content filter for ETF in any one of the following ways:

- Use the 'URL Reputation' condition with any appropriate action.
- Use the 'URL Reputation' action with any or no condition.
- Use the 'URL Reputation' condition and action.

The following procedure is used to detect malciicous URLs using the 'URL Reputation' condition and action:

Note

- If you only want to use the 'URL Reputation' condition with any appropriate action, do not follow steps 11-20 of the procedure.
- If you only want to use the 'URL Reputation' action with any or no condition., do not follow steps 4-10 of the procedure.

Before you begin

- Make sure that you enable URL filtering on your email gateway. To enable URL filtering, go to *Security Services* > *URL Filtering* page in the web interface. For more information, see Protecting Against Malicious or Undesirable URLs.
- Make sure that you enable Outbreak Filters on your email gateway. To enable Outbreak Filters, go to *Security Services* > *Outbreak Filters* page in the web interface. For more information, see Outbreak Filters.
- Make sure that you enable Anti-Spam engine on your email gateway. To enable the Anti-Spam engine, go to *Security Services* > *Anti-Spam* page in the web interface. For more information, see Managing Spam and Graymail.
- (Optional) Create a URL list. To create one, go to *Mail Polices* > *URL Lists* page in the web interface. For more information, see Protecting Against Malicious or Undesirable URLs.

Procedure

Step 1	Go to **Mail Policies > Incoming Content Filters**.
Step 2	Click **Add Filter**.
Step 3	Enter a name and description for the content filter.
Step 4	Click **Add Condition**.
Step 5	Click **URL Reputation**.
Step 6	Select **External Threat Feeds**.
Step 7	Select the ETF source(s) to detect malicious URLs.
Step 8	(Optional) Select the list of allow listed URLs that you do not want the email gateway to detect for threats.
Step 9	Select the required **Check URLs within** option to detect malicious URLs in the message body and subject and/or message attachments.
Step 10	Click **OK**.
Step 11	Click **Add Action**.
Step 12	Click **URL Reputation**.
Step 13	Select **External Threat Feeds**.
Step 14	Make sure that you select the same ETF source(s) that you selected in the condition (Step 7).
Step 15	(Optional) Select the same list of allow listed URLs that you selected in Step 8.
Step 16	Select the required **Check URLs within** option to detect malicious URLs in the 'message body and subject' and/or 'message attachments'
Step 17	Select the required action that you want to perform on the URLs within the message body and subject and/or message attachments. **Note** In Step 16, if you choose the 'Check URLs within' option as 'Attachments', you can only strip the attachment from the message.
Step 18	Select whether you want to take actions on all messages or unsigned messages.
Step 19	Click **OK**.

Step 20 Submit and commit your changes.

Note
If you have configured URL Reputation content filters for Web Based Reputation Score (WBRS) and ETF on your email gateway, it is recommended to set the order of the WBRS URL Reputation content filter higher than the order of the ETF URL Reputation filter, to improve the performance of your emal gateway.

Detecting Malicious URLs in Messages Using Message Filter

As an example, use the 'URL Reputation' message filter rule syntax to detect malicious URLs in messages using the ETF engine, and to defang the URL.

Syntax:

```
 defang_url_in_message: if (url-external-threat-feeds (['etf_source1'],
 <'URL_allowedlist'>,
<’message_attachments'> , <’message_body_subject’> ,))
 { url-etf-defang(['etf-source1'], "", 0); } <’URL_allowedlist’> ,
<’Preserve_signed’>)}
```

Where

- `'url-external-threat-feeds'` is the URL Reputation rule.
- `'etf_source1'` is the ETF source(s) used to detect malicious URLs in the messages or message attachments.
- `'URL_allowedlist'` is the name of a URL allowed list. If a URL allowed list is not present, it is displayed as "".
- `'message_attachments'` is used to check for malicious URLs in the message attachments. A value of '1' is used to detect malicious URLs in the message attachments.
- `'message_body_subject'` is used to check for malicious URLs in the message body and subject. A value of '1' is used to detect malicious URLs in the message body and subject.

Note A value of "1,1" is used to detect malciocus URLs in the message body, subject, and message attachments.

- `'url-etf-defang'` is one of the actions that you can take on messages that contain malicious URLs.

  The following examples are the ETF-based actions that you can apply on messages that contain malicious URLs:

  - url-etf-strip(['etf_source1'], "None", 1)
  - url-etf-defang-strip(['etf_source1'], "None", 1, "Attachment removed")
  - url-etf-defang-strip(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect(['etf_source1'], "None", 1)
  - url-etf-proxy-redirect-strip(['etf_source1'], "None", 1)

- url-etf-proxy-redirect-strip(['etf_source1'], "None", 1, " Attachment removed")
- url-etf-replace(['etf_source1'], "", "None", 1)
- url-etf-replace(['etf_source1'], "URL removed", "None", 1)
- url-etf-replace-strip(['etf_source1'], "URL removed ", "None", 1)
- url-etf-replace-strip(['etf_source1'], "URL removed*", "None", 1, "Attachment removed")

- `'Preserve_signed'` is represented by '1' or '0'. '1' indicates that this action applies to unsigned messages only and '0' indicates that this action applies to all messages.

In the following example, if a URL in the message attachment is detected as malicious by the ETF engine, the attachment is stripped.

```
Strip_Malicious_URLs: if (true) {url-etf-strip(['threat_feed_source'], "", 0);}
```

Detecting Malicious Files in Message Attachments Using Content Filter

Use the 'Attachment File Info' content filter to detect files in message attachments categorized as malicious by the ETF engine, and take appropriate actions on such messages.

Note The ETF engine performs a lookup based on the file hash of a file.

You can configure the 'Attachment File Info' content filter for ETF in any one of the following ways:

- Use the 'Attachment File Info' condition with any appropriate action.
- Use the 'Strip Attachment by File Info' action with any or no condition.
- Use the 'Attachment File Info' condition and 'Strip Attachment by File Info' action.

The following procedure is used to detect malicious files in message attachments using the 'Attachment by File Info' condition and 'Strip Attachment by File Info' action:

Note

- If you only want to use the 'Attachment File Info' condition with any appropriate action, do not follow steps 10-15 of the procedure.
- If you only want to use the 'Strip Attachment by File Info' action with any or no condition., do not follow steps 4-9 of the procedure.

Before you begin

(Optional) Create a File Hash Exception List. To create one, go to Mail Policies > File Hash Lists page in the web interface. For more information, see Creating File Hash List, on page 13.

Procedure

Step 1	Go to **Mail Policies > Incoming Content Filters**.
Step 2	Click **Add Filter**.
Step 3	Enter a name and description for the content filter.
Step 4	Click **Add Condition**.
Step 5	Click **Attachment File Info**.
Step 6	Select **External Threat Feeds**.
Step 7	Select the ETF source(s) to detect malicious files using file hashes.
Step 8	(Optional) Select the list of file hashes that you do not want the email gateway to detect for threats.
Step 9	Click **OK**.
Step 10	Click **Add Action**.
Step 11	Click **Strip Attachment by File Info**.
Step 12	Select **External Threat Feeds**.
Step 13	Make sure that you select the same ETF source(s) that you selected in the condition (Step 7).
Step 14	(Optional) Select the same list of file hashes that you selected in Step 8.
Step 15	Submit and commit your changes.

Creating File Hash List

Procedure

Step 1	Go to **Mail Policies > File Hash Lists**.
Step 2	Click **Add File Hash List**.
Step 3	Check the required file hash type - ‘SHA256’ or ‘MD5' or all of the above.
Step 4	Enter the file hashes (that you selected in Step 3) separated by commas or in new lines.
Step 5	Submit and commit your changes.

Detecting Malicious Files in Messages Attachments Using Message Filter

As an example, use the following message filter rule syntax to detect files in message attachments categorized as malicious by the ETF engine, and take appropriate actions on such messages.

Syntax:

```
Strip_malicious_files: if (file-hash-etf-rule (['etf_source1'], <'file_hash_exception_list'>))

{ file-hash-etf-strip-attachment-action (['etf_source1'], <'file_hash_exception_list>,
 "file stripped from message attachment"); }
```

Where:

- `'file-hash-etf-rule'` is the Attachment File Info message filter rule
- `'etf_source1'` is the ETF source(s) used to detect malicious files in the messages based on the file hash.
- `'file_hash_exception_list'` is the name of a file hash exception list. If a file hash exception list is not present, it is displayed as “”.
- `'file-hash-etf-strip-attachment-action'` is the name of the action that you want to apply on messages that contain malicious files.

In the following example, if a message contains a message attachment detected as malicious by the ETF engine, the attachment is stripped.

```
Strip_Malicious_Attachment: if (true) {file-hash-etf-strip-attachment-action
(['threat_feed_source'], "", "Malicious message attachment has been stripped from
the message.");}
```

Attaching Content Filter to Incoming Mail Policy

You can attach one or more of the content filters that you configured to detect malicious domains, URLs, or file hashes in messages to an incoming mail policy.

Procedure

Step 1 Go to **Mail Policies** > **Incoming Mail Policies**.

Step 2 Click the link below **Content Filters**of a particular mail policy.

Step 3 Select **Enable Content Filters (Customize Settings)**.

Step 4 Select the Content Filters that you created for detecting malicious domains, URLs or file hashes.

Step 5 Submit and commit your changes.

What to do next

After you attach the content filter to an incoming mail policy, your email gateway begins to take actions on messages based on the verdicts received from the ETF engine.

External Threat Feeds and Clusters

If you use centralized management, you can enable the ETF engine and mail policies at the cluster, group, and machine level.

Monitoring External Threat Feeds Engine Updates

If you have enabled service updates, the ETF engine updates are retrieved from the Cisco update servers. However, in some scenarios (for example, you have disabled automatic service updates or automatic service update is not working), you might want to manually check for ETF engine updates.

You can manually update the ETF engine in any one of the following ways:

- Go to **Security Services > External Threat Feeds** page in the web interface, and click **Update Now**.
- Use the `threatfeedupdate` command in the CLI.

To know the details of the existing ETF engine, see the 'External Threat Feeds Engine Updates' section in the Security Services > External Threat Feeds page in the web interface or use the threatfeedstatus command in CLI.

Viewing Alerts

The following table lists the alerts generated by the ETF engine, including a description of the alert and the alert severity.

Component/Alert Name	Message and Description	Parameters
ETF ENGINE ALERT	Unable to fetch the observables from the source: $source_name after 3 failed attempts. Reason for failure: $reason	**'source'** - The name of the TAXII source. **'reason'** - The reason why the polling failed.
	Information. Sent when polling feeds from a TAXII source fails.	
ETF ENGINE ALERT	The storage limit of $count observables exceeded for the observable type: $type.	**$count** - The allowed number of observables per type. **$ type** - The type of the observable.
	Information. Sent when the number of permitted observables exceeded.	

Displaying Threat Details in Message Tracking

You can view the message details that contain threats corresponding to the selected IOCs from the selected ETF source(s).

Before you begin

- Make sure that you enable the Message Tracking feature on the email gateway. To enable Message Tracking, go to **Security Services > Centralized Services > Message Tracking** page in the web interface.
- Content or Message filters for detecting threats in messages are operational.

Procedure

Step 1 Go to **Monitor** > **Message Tracking**.

Step 2 Click **Advanced**.

Step 3 Check **External Threat Feeds** under Message Event.

Step 4 Select the required IOC(s) to track messages containing threats corresponding to the selected IOCs.

Step 5 (Optional) Select **All External Threat Feed Sources** to view the messages that contain threats based on the available and deleted ETF source(s) configured in the email gateway.

Step 6 (Optional) Select **Current External Threat Feed Sources** and choose the required ETF source(s) to view the messages that contain threats based on the available ETF source(s) configured in the email gateway.

Step 7 (Optional) Enter the name of a particular ETF source in the 'External Threat Feed Sources' field to view messages that contain threats based on this ETF source.

Step 8 Click **Search**.