



# **DIGITAL THREAT MONITORING [DTM]**

**KEYWORDS REFERENCE GUIDE:  
SELF-SERVE KEYWORD MANAGEMENT  
HOW TO USE DTM FILTERS  
COMMON ERRORS**

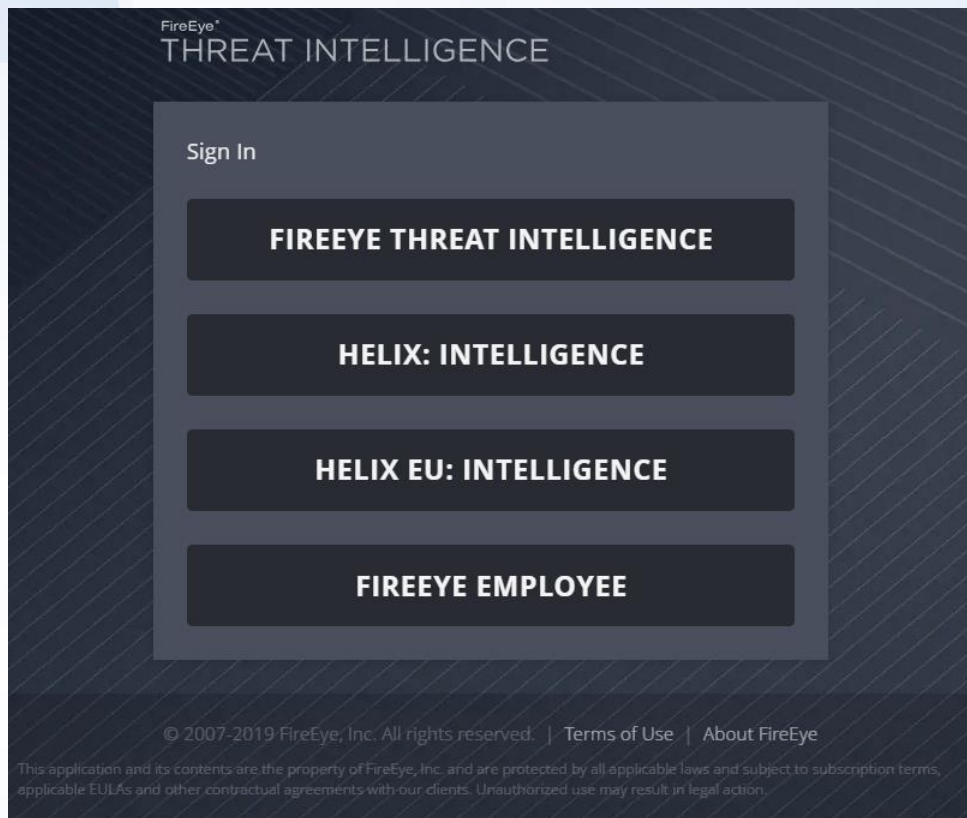


# TABLE OF CONTENTS

- Self-Serve Keyword Management
  - Importing/Exporting keywords
  - Individually or in bulk
- Keyword Options
  - Category/Type
  - Filters
- Deleting keywords
  - Individually or in bulk
  - How to use DTM Filters

# LOGIN TO FIP

- Log into FireEye Intelligence Portal (FIP)
- <https://intelligence.fireeye.com>



# ACCESSING DIGITAL THREAT MONITORING

- From the FIP home page select the Dashboard or Keywords option.

The screenshot displays the Threat Intelligence Dashboard. At the top, a navigation bar includes links for Intelligence, News Analysis, Tools, Alerts, Support, and Admin. The 'Dashboard' link is highlighted. Below the navigation bar, the main content area is divided into several sections. On the left, a 'TRENDS AND FORECASTING' section features an article titled 'Not Business as Usual: Risks and Best Practices for Business Disruption and Unplanned Remote Work' dated Mar 24, 2020. On the right, a 'RECENT KAYSlice/COOLPANTS ACTIVITY' section reports on signals of a possible return of TEMP.METASTRIKE following a brief hiatus, dated early February 2020. Below these sections is a table of key metrics:

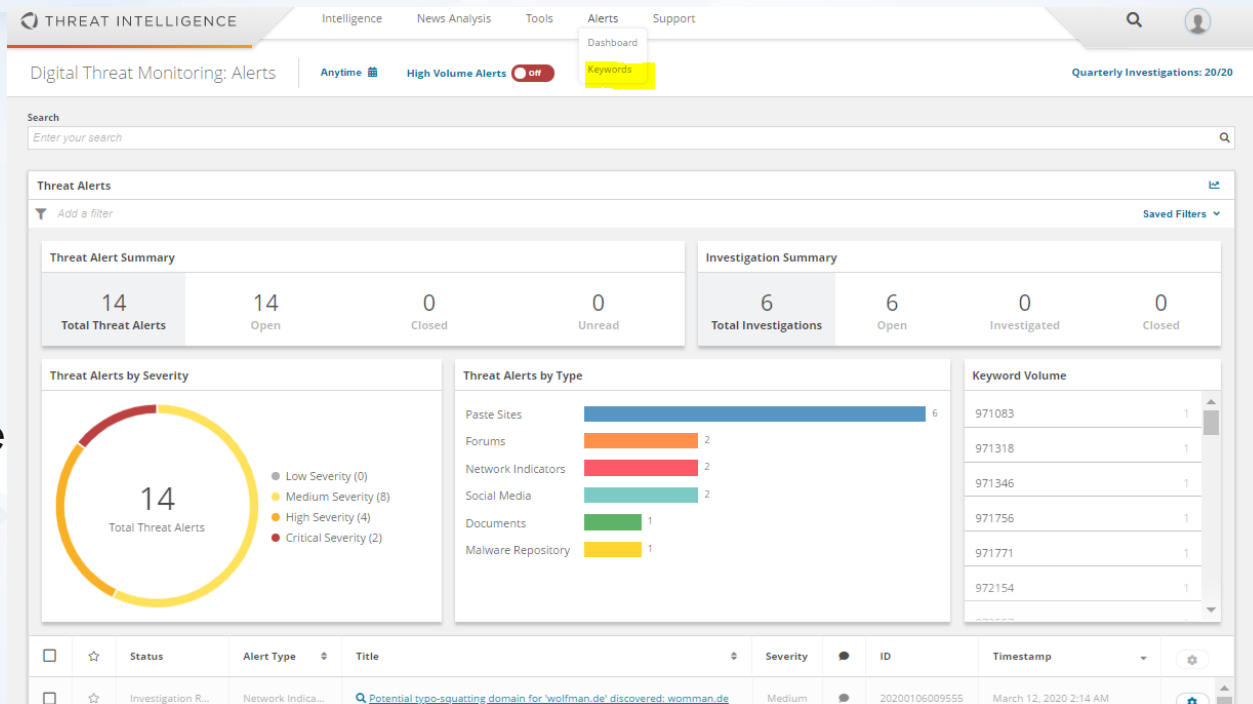
Actor		Malware		Industry		Region		Subscription		Intel Products	
95 Actors	1,192 Reports	443 Profiles	2,118 Reports	21 Sectors	4,078 Reports	37 Regions	3,362 Reports	9 Subscriptions	70,094 Reports	22 Product Types	45,624 Reports

Below the metrics table is a 'LATEST INTELLIGENCE' section with a dropdown menu set to 'Threat'. It contains three article cards:

- TRENDS AND FORECASTING** (CP, FS, OP): 'Social Engineering Based on Stimulus Bill and COVID-19 Financial Compensati ...' dated Mar 27, 2020.
- EVENT COVERAGE/IMPLICATION** (CP, FS, OP): 'Managing Email Phishing Risks During the Coronavirus (COVID-19) Epidemi ...' dated Mar 27, 2020.
- EVENT COVERAGE/IMPLICATION** (FS, CE): 'CHERRYSTEM Malware Identified in Campaign Targeting Chinese Interes ...' dated Mar 27, 2020.

# DTM LANDING PAGE

- The dashboard provides access to your alerts, alert filters and use statistics.
- From here you can pass through to the keyword management modal and enter single or multiple keywords, or completely replace your keyword list by using the bulk upload function.



# EXPORTING KEYWORDS: MAKE A BACKUP COPY FIRST

- Select Actions
- Select Export Keywords
- This will export an excel file containing all of the current keywords

THREAT INTELLIGENCE Intelligence News Analysis Tools Alerts Support Admin

Digital Threat Monitoring: Keywords

DTM Demo X Actions ^

Threat Keywords

<input type="checkbox"/>	Keyword	Category	Type	Description	Filter	Created
<input type="checkbox"/>	205.185.216.1/24	Network Info	IP Addresses			21 days ago

Filter...

Add Keywords  
Export Keywords  
Delete selected

# ADDING KEYWORDS

- Select Actions
- Select Add Keywords
- The “Add Keywords” modal will open

The screenshot displays the Threat Intelligence dashboard. The top navigation bar includes 'Intelligence', 'News Analysis', 'Tools', 'Alerts' (selected), 'Support', and 'Admin'. A search icon and a user profile icon are on the right. The main heading is 'Digital Threat Monitoring: Keywords'. Below this, there's a 'DTM Demo' dropdown and an 'Actions' button. The 'Threat Keywords' table has columns: Keyword, Category, Type, Description, Filter, and Created. A row is visible with the keyword '205.185.216.1/24' under 'Network Info' and 'IP Addresses'. An 'Add Keywords' modal is open, showing options to 'Add Keywords', 'Export Keywords', and 'Delete selected'.

THREAT INTELLIGENCE

Intelligence News Analysis Tools Alerts Support Admin

Digital Threat Monitoring: Keywords

DTM Demo x Actions

Threat Keywords

<input type="checkbox"/>	Keyword	Category	Type	Description	Filter	Created
<input type="checkbox"/>	205.185.216.1/24	Network Info	IP Addresses			21 days ago

Filter...

Add Keywords

Export Keywords

Delete selected

# ADD KEYWORDS: TWO OPTIONS

- The **Add Keywords** modal provides options for “Enter Keywords” (single or small groups) and “Replace Keywords” (bulk uploads).

Add Keywords

ENTER KEYWORDS

REPLACE KEYWORDS

[Keyword Reference Guide](#)

Enter Keywords using the form below to drive monitoring and Threat Alerting results on areas of interest to your organization. Fields with an “\*” are required.

\*Keyword(s) [ 0 ]

Enter keywords and press “return” after each. Fields below apply to each keyword entered.

Filter ⓘ

Use filters to reduce alert volume for targeted results. Regular expressions are supported.

\*Category ⓘ  
Choose a Category  
Select the category of keyword you would like uploaded to help drive relevant results.

\*Type  
Choose a Type  
Select the type of keyword you would like uploaded to help drive relevant results.

Description

Use to add context (e.g. when a keyword has more than one meaning).

Cancel

Review



# ENTER KEYWORDS OPTION

- Select “Enter Keywords” to input single or small batches of keywords
  - Here, keywords are added **TO** the current list of keywords
  - Additions do not over-write the current list of keywords
  - Maximum number of keyword entries is subscription dependent
    - Unlimited for standalone subscribers
    - 100 for standard intel subscribers

## Add Keywords

ENTER KEYWORDS

REPLACE KEYWORDS

[Keyword Reference Guide](#)

Enter Keywords using the form below to drive monitoring and Threat Alerting results on areas of interest to your organization. Fields with an “\*” are required.

\*Keyword(s) [ 0 ]

Enter keywords and press “return” after each. Fields below apply to each keyword entered.

Filter ⓘ

Use filters to reduce alert volume for targeted results. Regular expressions are supported.

\*Category ⓘ

\*Type

Choose a Category

Choose a Type

Select the category of keyword you would like uploaded to help drive relevant results.

Select the type of keyword you would like uploaded to help drive relevant results.

Description

Use to add context (e.g. when a keyword has more than one meaning).

Cancel

Review

# KEYWORD MAPPING CATEGORY TO TYPE

Category	Type
▪ BIN Number	➤ BIN Number
▪ Brand & Product	➤ Product or Service
	➤ Project Name
▪ Network	➤ Domains
	➤ Emails
	➤ IPs
	➤ URLs
▪ Organizational Identity	➤ Critical Facilities
	➤ Organizational Names
	➤ Subsidiaries/DBA
	➤ VIPs
▪ Social Media	➤ Twitter
▪ Supply Chain	➤ Vendors or Partners

# ENTER KEYWORDS OPTION

- Enter the keyword(s)
- Enter the filter (optional)
  - Use filters to reduce alert volume for targeted results. Regular expressions are supported.
- Choose the keyword category
  - Keyword Types are dependent on category
- Next, select the keyword type
- Enter a short description, which helps if you engage an analyst or if FireEye needs to refine your filter.

## Add Keywords

[ENTER KEYWORDS](#) [REPLACE KEYWORDS](#) [Keyword Reference Guide](#)

Enter Keywords using the form below to drive monitoring and Threat Alerting results on areas of interest to your organization. Fields with an "\*" are required.

\*Keyword(s) [ 1 ]

Illudium Q-36 Explosive Space Modulator

Enter keywords and press "return" after each. Fields below apply to each keyword entered.

Filter

"Marvin the Martian" AND "K-9"

Use filters to reduce alert volume for targeted results. Regular expressions are supported.

\*Category

Brand and Products

Select the category of keyword you would like uploaded to help drive relevant results.

\*Type

Products or Service

Select the type of keyword you would like uploaded to help drive relevant results.

Description

Use to add context (e.g. when a keyword has more than one meaning).

Cancel

Review

Click "Submit" When Finished

For More Details on Using Filters, Please See Section Starting on Slide #18

# REPLACE KEYWORDS OPTION: BULK UPLOADS

- Select “Replace Keywords” to bulk upload keywords
  - **NOTE:** New bulk uploads delete your current list of keywords via overwriting
  - There is currently no built-in backup, aside from saving your initial bulk uploads, so please be careful
  - Maximum number of keyword entries is subscription dependent
    - Unlimited for enterprise clients
    - 100 for all other Intel subscribers

## Add Keywords

[ENTER KEYWORDS](#) **REPLACE KEYWORDS** [Keyword Reference Guide](#)

Enter Keywords using the form below to drive monitoring and Threat Alerting results on areas of interest to your organization. Fields with an “\*” are required.

\*Keyword(s) [ 0 ]

Enter keywords and press “return” after each. Fields below apply to each keyword entered.

Filter ⓘ

Use filters to reduce alert volume for targeted results. Regular expressions are supported.

\*Category ⓘ

Select the category of keyword you would like uploaded to help drive relevant results.

\*Type

Select the type of keyword you would like uploaded to help drive relevant results.

Description

Use to add context (e.g. when a keyword has more than one meaning).

CancelReview

# REPLACE KEYWORDS: BULK UPLOADS

- Select “View Template”, which will download an Excel file containing the DTM Keywords template. Use this for bulk uploading large numbers of keywords.
- Max number of bulk uploads on the Keywords Profile is 14,999


## Add Keywords

[ENTER KEYWORDS](#)[REPLACE KEYWORDS](#)

Replace all keywords by uploading a document list. Download a blank template to make a document list by using the VIEW TEMPLATE link below.

Upload Document

[VIEW TEMPLATE](#)

 Drop file here or click to browse

Uploaded document list replaces existing keywords

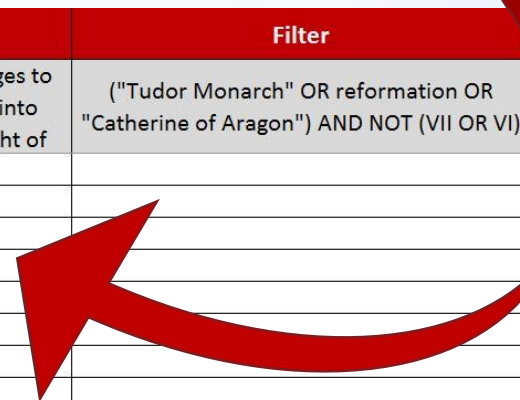
CANCEL

SUBMIT

# REPLACE KEYWORDS: BULK UPLOADS

- The **FireEye DTM Keywords Profile** enables bulk uploads with columns for Keywords, Category, Type, Description, and Filters built in, to include drop downs for choosing available options, as shown below.

Keyword	Category	Type	Description	Filter
King Henry VIII	High Profile Personnel Facilities	VIPs	Henry is known for his radical changes to the English Constitution, ushering into England the theory of the divine right of	("Tudor Monarch" OR reformation OR "Catherine of Aragon") AND NOT (VII OR VI)



# REPLACE KEYWORDS: BULK UPLOADS

- Enter the keyword(s)
- Choose the keyword category
  - Keyword Types are dependent on category
- Next, select the keyword type
- Enter a short description, which helps if you engage an analyst or if FireEye needs to refine your filter.
- Enter the filter (optional)

Keyword	Category	Type	Description	Filter
King Henry VIII	High Profile Personnel Facilities	VIPs	Henry is known for his radical changes to the English Constitution, ushering into England the theory of the divine right of	("Tudor Monarch" OR reformation OR "Catherine of Aragon") AND NOT (VII OR VI)

# REPLACE KEYWORDS: BULK UPLOADS


- Drag and drop your completed DTM Keywords file into the “Upload Document” box and select “Submit”.
- Reminder: this action deletes and replaces all your current keywords.

## Add Keywords

[ENTER KEYWORDS](#) [REPLACE KEYWORDS](#)

Replace all keywords by uploading a document list. Download a blank template to make a document list by using the [VIEW TEMPLATE](#) link below.

Upload Document

 Drop file here or click to browse

Uploaded document list replaces existing keywords

CANCEL

SUBMIT



# ERROR MESSAGES

- If there is an issue with your keyword entries or bulk upload you will get an error message.
- Please review the “Common Errors” in the third section for tips on how to identify and correct common errors
- If you are unable to resolve any errors please contact:  
[DigitalThreats@FireEye.com](mailto:DigitalThreats@FireEye.com)

Add Keywords

ENTER KEYWORDS

REPLACE KEYWORDS

[Keyword Reference Guide](#)

Enter Keywords using the form below to drive monitoring and Threat Alerting results on areas of interest to your organization. Fields with an "\*" are required.

\*Keyword(s) [ 1 ]

"Illudium Q-36 Explosive Space Modulator"

Enter keywords and press "return" after each. Fields below apply to each keyword entered.

Filter ⓘ

"Marvin the Martian" AND "K-9"

Filter is invalid. If you are experiencing continued issues and need direct assistance, please email [DigitalThreats@FireEye.com](mailto:DigitalThreats@FireEye.com)

\*Category ⓘ

Brand and Products

Select the category of keyword you would like uploaded to help drive relevant results.

\*Type

Products or Service

Select the type of keyword you would like uploaded to help drive relevant results.

Description

Use to add context (e.g. when a keyword has more than one meaning).

Cancel

Review



# HOW TO USE DTM FILTERS AND QUERIES EFFECTIVELY

# QUERIES & FILTERS

- Terms vs Phrases
- Queries
- Boolean Operators “OR” “AND” “NOT”
- Wildcard Searches “\*” “?”
- Advanced search tools

# TERMS

- There are two types of terms:
- Single words
  - Rabbit
  - Acme
- Phrases - a group of words surrounded by double quotes such as “Acme Inc”
  - “Bugs Bunny”
  - “Marvin the Martian”
  - “Illudium Q-36 Explosive Space Modulator”
- Multiple terms can be combined together with Boolean operators to form a more complex query (see below)

# QUERY

- What is a Query?
- A query is a combination of Keywords, and optional values, in an expression with Boolean operators (AND, OR, NOT). Grouping is supported.
  - Term: Rabbit
  - Query: Rabbit AND Fudd
    - The result contains Rabbit and Fudd
  - Phrase: “Bugs Bunny”
  - Query: “Bugs Bunny” AND “Elmer Fudd”
  - The result contains Bugs Bunny and Elmer Fudd

# BUILDING FILTERS:

## BOOLEAN OPERATORS “OR” “AND” “NOT”

- Three most common operators
  - “OR” The default operator between two terms (used if none is provided). The content matches if either term is found.
    - Example:
      - Bunny OR wabbits - the content must contain Bunny or wabbits
  - “AND” The AND operator matches if both terms are found in the content.
    - Example:
      - “Tweety” AND “Sylvester” - the content must contain Tweety and Sylvester
  - “NOT” The NOT operator excludes the term after it from being present in the content
    - \*\*\*For clarity we recommend using AND NOT instead of just NOT
    - Example:
      - “ACME Inc” AND NOT “Eight Shooter” - the content must contain ACME Inc and eliminates all documents with a reference to Eight Shooter.

# TWO GENERAL PATHS: AND vs NOT

- NOT function eliminates unwanted noise and leaves the rest
  - Like panning for gold
- Recommended first
  - Pros
    - Targets the noise and excludes it
    - Less chance of missing something significant
  - Cons
    - Iterative process – Whack-a-Mole
    - Eliminate noisiest distractors first one at a time

# AND vs NOT CONTINUED

- AND Function – Performing Surgery
  - Pros
    - Only alerts if all conditions are met
    - Very specific and minimal noise
  - Cons
    - Greater risk of missing something significant.
    - Filter can be very long and complex



# BUILDING AN EFFECTIVE AND NOT ALERT FILTER

- Questions to ask before building an AND NOT Threat Alerts filter?
  - Is the term/name unique – run a google search on the entire text string (“Mark Twain”). Do you get millions of hits, if yes - will need to build a filter.
- Review alerts for common false positives
- Choose terms that are specific to the false alerts
  - The biggest offenders are often associated online gaming sites.
    - Filter on terms like dragons or denizens or gamers or players
    - Terms that would not normally be present in client document
- Be careful not to choose terms that could filter out true positives
  - The term players would be a poor choice for a casino client

# BUILDING AN EFFECTIVE AND ALERT FILTER

- Questions to ask before building an AND Threat Alerts filter?
  - Does the potential impact of missing something increase the threshold for false positives?
  - How much effort are you willing to expend parsing through false positives?
- What “bad word(s)” could be used in a filter to associate your keyword with:
  - Nefarious activity
  - Information of interest
- Is the term linked to a single country, region or event
  - Utilize the native language term/character/symbol where possible.
  - Use the term translated into suspect language(s) (Russian/Chinese/etc.)

# FILTERS: LESS IS OFTEN MORE - BE CONCISE

- Filters limit results, so be judicious
- What type of filters (key terms or phrases) would uncover activity of interest? For example:
  - Credit Cards
    - Track OR Dump OR BIN\* OR Record OR Download OR Sell OR File etc.
  - PII
    - Name\* OR Birth\* OR Phone OR District OR County OR Address OR School OR Social OR Gender OR Sex OR Email OR zip
  - Application
    - API OR "API key\*" OR vulnerabilit\* OR authentication OR scrap\* OR OAuth OR key\* OR "credential stuffing" OR "API scraping"

# WEB PRESENCE

- VIPS/EXEC/Board members
  - Conduct google check, if millions of hits consider adding an association:
    - Company name
    - Position (CEO/CIO)
    - Title
    - Activity linked to a particular
      - High visibility news media activity
      - Incident
      - Specific group targeting (Hacktivism)
  - Example “Mark Twain”
    - “Mark Twain” AND NOT (writ\* OR humor OR book)
    - “John Doe” AND (CEO OR “ACME Parts” OR “Wiley Coyote sighting”)

# WILDCARD SEARCHES "\*" "?"

- DTM supports wildcard searches within **single terms** (not within phrase queries).
- You can use single "?" or multiple "\*" character wildcard searches.
  - To perform a single character wildcard search use "?"
    - Dal?ks will return common variations: "Daleks" or "Daliks"
  - To perform a multi-character wildcard search use the "\*" symbol
    - Donald.D\*.org will capture terms like: Donald.Duck.org & Donald.Ducks.org
- Note: Currently wildcards are only available in filters – **Not keywords**
- Note: You cannot use the "\*" symbol as the first character of a search.

# FUZZY SEARCHES "˜"

- To complete a fuzzy search use the tilde, "~", symbol at the end of a single word term (filter only).
- For example, to search for a term similar in spelling to eight "gun" use the fuzzy search:
  - Gun~
  - This search will find terms like fun and gut.

# PROXIMITY SEARCHES "🐕"

- To do a proximity search use the tilde, "~" symbol at the end of a Phrase.
- For example to search for "Marvin" and "K-9" within 10 words of each other in a document use the search:
  - "Marvin K-9"~10
  - This will find documents with reference to Marvin and his faithful dog K-9 within 10 words of each other.

# GROUPINGS

- Parentheses can be used to group clauses to sub-queries.
- Examples:
  - organization: “ACME Rabbit Detector” AND (Bugs OR Bunny)
    - Must contain Acme Rabbit Detector and Bugs or Bunny
  - (acme.com OR acme.biz) AND NOT (hares OR *Lepus* OR lagomorph) Must contain Acme.com or acme.biz, but not those records that contain hares OR *Lepus* OR lagomorph.
- For details on the Lucene language please visit the official guide at:  
[https://lucene.apache.org/core/7\\_5\\_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html#package.description](https://lucene.apache.org/core/7_5_0/queryparser/org/apache/lucene/queryparser/classic/package-summary.html#package.description)





# COMMON ERRORS



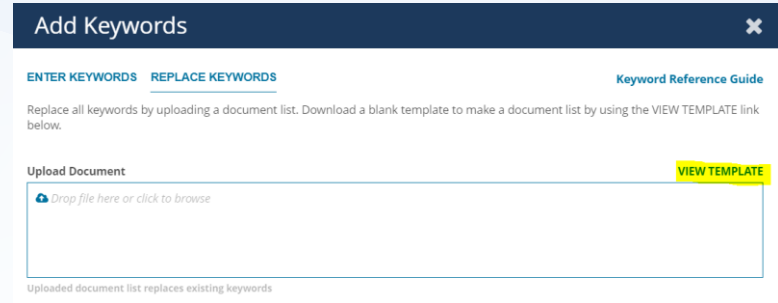
# COMMON ERROR TYPES

- Bulk Upload Errors
- Keywords
- CIDR Blocks
- Filters
  - Syntax
  - Length
  - Non-Latin character rendering issue
  - Syntax Capitalization error correction



# BULK UPLOAD ERRORS

- If you get the following Error when trying to bulk upload your keywords:
  - *There was a problem importing your keywords. Please ensure the format matches the template provided.*
- This usually means:
  - The bulk upload sheet is encrypted.
  - Decrypt and reload the document.
- The spreadsheet may be corrupted or is an older version which is no longer supported.
  - Download a new template from the portal “View Template” and import data in the new form. Upload new data.



The screenshot shows a web interface titled "Add Keywords" with a dark blue header and a close button (X). Below the header, there are two tabs: "ENTER KEYWORDS" and "REPLACE KEYWORDS", with the latter being the active tab. To the right of the tabs is a link labeled "Keyword Reference Guide". The main content area under the "REPLACE KEYWORDS" tab contains the text: "Replace all keywords by uploading a document list. Download a blank template to make a document list by using the VIEW TEMPLATE link below." Below this text is a section titled "Upload Document" which includes a large rectangular area with a cloud icon and the text "Drop file here or click to browse". To the right of this area is a yellow button labeled "VIEW TEMPLATE". At the bottom of the interface, a small note states: "Uploaded document list replaces existing keywords".

# DON'T TRY TO STACK KEYWORDS

- Do not use
  - Parenthesis ()
- Do not combine a term and its acronym
  - For example: Electronic Supply Unit (ECU)
  - These should be individual keywords
- Do not use Boolean operators in keywords
  - For example: "Electronic Supply Unit" OR "ES" OR "ESU"
  - These should be individual keywords

~~\*Keyword(s) [ 1 ]~~

~~Electronic Control Unit (ECU) X~~

Enter keywords and press "return" after each.

\*Keyword(s) [ 2 ]

Electronic Control Unit X

"ECU" X

|

Enter keywords and press "return" after each.

# CIDR BLOCKS ERRORS

- CIDR Block notation is required for all IP addresses
- For single IP append /32
  - 192.168.1.1/32
- No spaces are allowed
  - 192.168.1.1 /32
  - 192.168.1.1/32
  - In the bulk upload tool trailing spaces are very easy to find by using the excel “edit” (F2) tool.

# FILTER ERRORS

- By default the keyword is linked to the filter by the “AND” function

- Do not place an “AND” before the initial filter term.
- Correct: (BBQ OR Auto OR “Three-Wheeler”)
- Incorrect: AND (BBQ OR Auto OR “Three-Wheeler”)

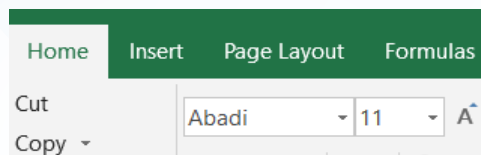
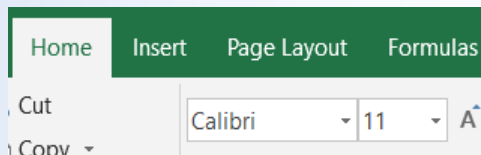
Filter
(BBQ OR Auto OR “Three-Wheeler”)
AND (BBQ OR Auto OR “Three-Wheeler”)
NOT (Harrison OR Gerald) AND NOT (Joe OR Bob)
AND NOT (“Jane Some” OR “Janet Some”)

- The preferred use of the “NOT” function should be “AND NOT”

- If the initial Boolean Operator is NOT the AND is implied.
- For all follow-on operators use the “AND NOT”
- Correct: NOT (Harrison OR Gerald) AND NOT (Joe OR Bob)
- Incorrect: AND NOT (“Jane Some” OR “Janet Some”)
- Verify that all Boolean operators are in all uppercase: OR, AND , AND NOT

# FILTER ERRORS CONTINUED

- Filters have a max length of 758 characters
- Non-Latin Character Sets sometimes do not render correctly in FiP
  - If this happens use the bulk upload template to change the character set from the default Calibri to Abadi and then back to Calibri. This will correct the character rendering issue.



# SYNTAX CAPITALIZATION ERROR CORRECTION

- If the AND, OR, AND NOT functions are not properly capitalized it will generate an error with the system
- To fix this issue you will need to correct the capitalization and amend the filter.
- To amend the filter change the order of any two filter terms. This will cause the system to create a new filter ID
  - Original filter: (br3ach\* or breach)
  - New filter: (breach OR br3ach\*)





**THANK YOU!**