



# XKEYSCORE Workflows

05 March 2009



# What is a workflow?

- Workflows automate queries.
  - One-time
  - Standing
- Every search type can be a workflow.
  - Same functionality and capability
- Follow on actions
  - Email alert
  - Download actions
  - Metadata summary

# Who can submit a workflow?



- Anyone!
- One owner per workflow
  - Multiple-users can be notified
- If ownership needs to be changed, a ticket can be submitted to the team.
- Future: sharing workflows
  - Right now, only the owner has the results in their “My Results” view.



# What can I do with a workflow?

- Workflows can be configured to run once
- Workflows can be configured to run daily
  - Every 1, 2, 3, 4, 6, 8, 12 or 24 hours
  - You can set an offset to start running at a certain hour
- Download results
- Email results and email alerts
- MAILORDER results
- MySQL report



# Why do I want a workflow?

- XKEYSCORE has a rolling buffer of data
- Repetitive queries
- Sigdev purpose
  - Fingerprint and appid testing
- Queries take a long time during high times
- Follow on actions
  - Google Earth data
  - Statistics
  - Customizable – write a script!

# How do I setup a workflow?



This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

**XKEYSCORE** Welcome: [switch users](#)

Preferences [Help](#)

**Welcome to the New XKEYSCORE Home Page!**  
If you have questions or bug reports please go to [XKEYSCORE New GUI Forum](#)  
To use the old GUI, click [here](#)

**HUMAN RIGHTS ACT, USSID 18 AND USSID 9**

I (SYSTEM) queries require a justification to ensure Human Rights Act (HRA), USSID 18 and USSID 9 compliance. Please enter information as prompted by the query interface. An audit trail has been established and will be searched as part of Menwith Hill Station's response to any complaint brought under HRA and as part of the USSID 18 and USSID 9 process. Please note that SENSITIVE TARGETING APPROVAL (STA) is required for HRA before submitting any query which includes terms specific to a person or company (eg name, address, identity details such as communications address, passport/bank account number) who EITHER (a) is defined as a UK, British Dependent Territory (BDT) or Second Party "person" or (b) is located in the UK, or a BDT or Second Party country. STA is also required for wildcard pulls that are inevitably going to retrieve a substantial proportion of such entities (e.g. wildcarding on a UK city code). Full legal guidance is available from the HRA Compliance Officer at Menwith Hill Station.

This system is audited for USSID 18 and Human Rights Act compliance  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

# How do I setup a workflow?



First, s  
workflc

Workflow Central Request Wizard

Please select a Search Type.

|          |  |
|----------|--|
| Full Log | Every session collected, indexed by "standard" DNI meta-data (to/from IP, port, casenotation, application id, sigad, etc). |
|----------|--|

Search Type Help

Cancel ◀ Prev ▶ Next Submit

a

# How do I setup a workflow?



Workflow Central Request Wizard

**Basic Information**

Query Name: Find\_my\_appid

Query Justification: Testing appid signature

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-03-04 00:00 Stop: 2009-03-05 23:59

Recurring Search **One Time Search**

Basic Features Help

Cancel Prev Next Submit

Runs once over  
a set datetime  
range

ring or one-  
ist be unique per user  
must have a justification  
justifications



# How do I setup a workflow?



Select  
search

Select a  
field to  
search

**Workflow Central Request Wizard**

**Add Search Fields**

Search Values are **ANDed** by default.

To **OR** Search **Fields**:

- \* Use the Multiple Field Search tab (below the input fields).
- \* Select all the fields you wish to search.

To **OR** Search **Values**:

- \* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to [here](#).

| Search Field                     | Search Value | Remove |
|----------------------------------|--------------|--------|
| From IP Address OR To IP Address | 1.2.3.4      |        |
| Attribute Info                   |              |        |
| From IP Address                  |              |        |
| To IP Address                    |              |        |
| <b>From Port</b>                 |              |        |
| To Port                          |              |        |

Single Field Search   **Multiple Field Search**

[Search Value Help](#)

Cancel   ◀ Prev   Next   Submit

Want to

or every field,  
you must select  
the PLUS key



# Group by option

- Group by
- Red
- Retu

ta results.

Workflow Central Request Wizard

Group Search Fields

Would you like to group any fields?

No

Yes

Group By Type

Table Unique Values:  [Group By Type Help](#)

Global Unique Values:

Columns to Group By

Datetime:

Client IP (X-Forwarded-For):

Username:

Attribute Info:

From IP Address:

To IP Address:

From Port:

To Port:

From Country (IP):

To Country (IP):

From City (IP):

To City (IP):

From Latitude (IP):

Cancel   Submit

This option groups each row in a table after a table and concatenates the results.

Select the fields you want to group by.



# Select databases

Workflow Central Request Wizard

Select the Database(s) to query

xks- :q0 (xks- :q0)

xks- :qsummary (xks- :qsummary)

Content must exist

Check All

Uncheck All

Basic Features Help

Cancel Prev Next Submit

If this is selected, results are only returned if the content still exists at site.



# Follow on Actions

- All
- All
- local
- All

content) to another

Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

No

Yes

| Script            | Script Arguments  | Add                              |
|-------------------|---|----------------------------------|
| Email Alert       | Email To: <input type="text"/>                          | <input type="button" value="+"/> |
| Email Alert       | ROWR: <input type="checkbox"/> Return Only With Results |                                  |
| SQL Report        |   |                                  |
| Download Sessions |   |                                  |

Cancel ◀ Prev ▶ Next Submit

On completion of the content  
 you will be able to



# Email alert

Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

No

Yes

| Script      | Script Arguments  | Add |
|-------------|---|-----|
| Email Alert | Email To: <input type="text"/><br>ROWR: <input type="checkbox"/> Return Only With Results | +   |

Cancel Prev Next Submit

Comma delimited email addresses.

This option only sends an email if you workflow has results.

# SQL report



Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

No

Yes

| Script     | Script Arguments  | Add                              |
|------------|---|----------------------------------|
| SQL Report | Type: <input type="text"/> <input type="button" value="v"/><br>Email To: <input type="text"/><br>Email Subject: <input type="text"/><br>Email Content: <input type="text"/><br>Email Attachment: <input type="checkbox"/> Email Attachment<br>ROWR: <input type="checkbox"/> Return Only With Results<br>Filename: <input type="text"/><br>Mail Order Trigraph: <input type="text"/><br>SQL: <input type="text" value="SELECT FROM %\{OUTPUT\_TABLE\} WHERE GROUP BY"/><br>GZIP: <input type="checkbox"/> Compress Contents | <input type="button" value="+"/> |

Cancel   Submit

CSV or HTML

This must be a VALID SQL statement. Email metadata that a user can set.

Example.

```
SELECT casenotation, sigad
FROM %\{OUTPUT\_TABLE\}
WHERE sigad!=
GROUP BY casenotation
```



# Download Results

## Workflow Central Request Wizard

### Follow-on Actions

Would you like to add any follow on actions

- No  
 Yes

| Script            | Script Arguments   | Add                              |
|-------------------|--|----------------------------------|
| Download Sessions | User ID: <input type="text"/><br>Email To: <input type="text"/><br>Email Subject: <input type="text"/><br>Email Content: <input type="text"/><br>ROWR: <input type="checkbox"/> Return Only With Results<br>Filename: <input type="text"/><br>Mail Order Trigraph: <input type="text"/><br>GZIP: <input type="checkbox"/> Compress Contents<br>Send To Agility: <input type="checkbox"/> Send To Agility | <input type="button" value="+"/> |

Cancel ◀ Prev

▶ Next Submit



# You're almost done!

Workflow Central Request Wizard

**Workflow Review**

This query (Find\_my\_appid) will search the **Full Log** table in database(s):  
**xks-jychan:q0**

The query will run **CONTINUOUSLY** executing every **6 hours** beginning at **5:00 EST**

The query will execute the following search criteria:

```
<and>
  <field>From IP Address</field>
  <value>1.2.3.4</value>
</and>

<and>
  <field>To Port</field>
  <value>80</value>
</and>

<and>
  <field>AppID (+Fingerprints)*</field>
  <value>search/google*</value>
</and>
```

Workflow Values    Workflow XML

Cancel    < Prev    Next    Submit





# Workflow Pending

This system is audited for USSID 18 and Human Rights Act compliance  
 TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108  
 XKEYSCORE Welcome: [redacted] [switch users](#)

Home Workflow Central Search Results Statistics Tagging Preferences Help

**Navigation Menu**

- Explorer
  - Home
  - Workflow Central
    - Request
    - My Workflows
  - Search
    - Classic
      - MultiSearch
      - Classic A-M
      - Classic N-Z
    - Common
      - Category DNI
      - Document Metadata
      - Email Addresses
      - Extracted Files
      - Full Log DNI
      - HTTP Activity
      - Phone Number Extractor
      - User Activity
    - Dictionary Hits
    - File Transfer
    - MultiSearch
      - IP Addresses
      - Mac Address
      - Username
    - Network Management
    - Search Wizard
    - UserActivity
    - VoP
    - Wireless
  - Results
    - My Recent Results
    - My Previous Results
    - My Ongoing Results
    - My Downloads
  - Statistics
    - Link Summarization
  - Tagging
    - Local Tagging
    - Tech Extractor Tagging

**My Workflows**

Help Actions

| Query Type | Query Name    | Last Modified      | State   | Actions |
|------------|---------------|--------------------|---------|---------|
| full_log   | Find_my_appid | 2009-03-05 14:44:5 | pending |         |

**State** **Actions**

pending

Page 1 of 1 Page Size: 30 Displaying 1 - 1 of 1

This system is audited for USSID 18 and Human Rights Act compliance  
 TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108



# Workflow Approved

This system is audited for USSID 18 and Human Rights Act compliance  
 TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

**KEYSCORE** Welcome: [REDACTED] [switch users](#)

Home Workflow Central Search Results Statistics Tagging Preferences Help

**Navigation Menu**

- Explorer
  - Home
  - Workflow Central
    - Request
    - My Workflows
  - Search
    - Classic
      - MultiSearch
      - Classic A-M
      - Classic N-Z
    - Common
      - Category DNI
      - Document Metadata
      - Email Addresses
      - Extracted Files
      - Full Log DNI
      - HTTP Activity
      - Phone Number Extractor
      - User Activity
    - Dictionary Hits
    - File Transfer
    - MultiSearch
      - IP Addresses
      - Mac Address
      - Username
    - Network Management
    - Search Wizard
    - User Activity
    - VoIP
    - Wireless
  - Results
    - My Recent Results
    - My Previous Results
    - My Ongoing Results
    - My Downloads
  - Statistics
    - Link Summarization
  - Tagging
    - Local Tagging
    - Tech Extractor Tagging

**My Workflows**

Help Actions ▾

Query Type

- full\_log

**Workflow: Find\_my\_appid**

```
<?xml version="1.0" encoding="UTF-8"?>
<query_jobs>
  <internal_gui>1</internal_gui>
  <datetime_created>1236264295</datetime_created>
  <job>
    <xks_userid>[REDACTED]</xks_userid>
    <xks_user_name>[REDACTED]</xks_user_name>
    <xks_password>18837b706121a0ca</xks_password>
    <search_type>full_log</search_type>
    <query_name>Find_my_appid</query_name>
    <query_justification>Testing appid signature </query_justification>
    <datetime>
      <interval>6</interval>
      <offset>5</offset>
    </datetime>
    <sql>
      <where>
        <and>
          <field>fm_ip</field>
          <value>1.2.3.4</value>
        </and>
        <and>
          <field>to_ap</field>
          <value>80</value>
        </and>
        <and>
          <field>fingerprint</field>
          <value>search/google*</value>
        </and>
      </where>
      <group_by>to_ip</group_by>
      <indexes>unique key(to_ip)</indexes>
    </sql>
    <advanced>
      <content_must_exist>true</content_must_exist>
      <routing>
        <database>xks-jychan:q0</database>
      </routing>
    </advanced>
  </job>
</query_jobs>
```

Cancel Save/Submit

Page 1 of 1 Page Size: 30

Displaying 1 - 1 of 1

This system is audited for USSID 18 and Human Rights Act compliance  
 TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

log

Wizard

e



# Common mistakes

- From IP and To IP with the same value.
- In this view, terms are ANDed together.
- Use Multiple Field Search Tab.

**Workflow Central Request Wizard**

**Add Search Fields**

Search Values are **ANDed** by default.

**To OR Search Fields:**

- \* Use the Multiple Field Search tab (below the input fields).
- \* Select all the fields you wish to search.

**To OR Search Values:**

- \* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to [here](#).

| Search Field                     | Search Value | Remove |
|----------------------------------|--------------|--------|
| From IP Address OR To IP Address | 1.2.3.4      |        |
| Attribute into                   |              |        |
| From IP Address                  |              |        |
| To IP Address                    |              |        |
| From Port                        |              |        |
| To Port                          |              |        |

Single Field Search | **Multiple Field Search**

[Search Value Help](#)

Cancel ◀ Prev ▶ Next Submit



# Common mistakes

- Using the multiple field search does not break this up into 3 search<->value pairs.
- Enter each term separately in the single field search.

**Workflow Central Request Wizard**

**Add Search Fields**

Search Values are **ANDed** by default.

To **OR** Search **Fields**:

- \* Use the Multiple Field Search tab (below the input fields).
- \* Select all the fields you wish to search.

To **OR** Search **Values**:

- \* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to [here](#).

| Search Field    | Search Value | Remove |
|-----------------|--------------|--------|
| From IP Address | 1.2.3.4      | X      |
| To IP Address   | 5.6.7.8      | X      |
| From Port       | 80           | X      |
|                 |              |        |

**Single Field Search**
 Multiple Field Search

[Search Value Help](#)

Cancel Prev  Next Submit



# Common mistakes

- This will return ALL casenotations.
  - a will be defeated by “!a” but a does equal “!b”
- All the defeated values must be ANDed together.

**Workflow Central Request Wizard**

**Add Search Fields**

Search Values are **ANDed** by default.

To **OR** Search **Fields**:

- \* Use the Multiple Field Search tab (below the input fields).
- \* Select all the fields you wish to search.

To **OR** Search **Values**:

- \* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to [here](#).

| Search Field | Search Value | Remove |
|--------------|--------------|--------|
| Casenotation | !a           | ✖      |
| Casenotation | !b           | ✖      |
| Casenotation | !c           | ✖      |
| Casenotation | !d           | ✖      |

# Common mistakes



## Workflow Central Request Wizard

### Add Search Fields

Search Values are **ANDed** by default.

#### To **OR** Search **Fields**:

- \* Use the Multiple Field Search tab (below the input fields).
- \* Select all the fields you wish to search.

#### To **OR** Search **Values**:

- \* Type 'OR' between each value (no quotes).

See Search Value Help below for more details or for a description of boolean logic go to [here](#).

| Search Field | Search Value | Remove |
|--------------|--------------|--------|
| Casenotation | lc           | ✖      |
| Casenotation | ld           | ✖      |
| SIGAD        | AUC-993      | ✖      |
|              |              | +      |

### Select the Database(s) to query

- AUS sites
- F6 sites
- NZ sites

Content must exist

Check All

Uncheck All

Basic Features Help

- If you are selecting specific SIGADs, only select the sites that have data from that SIGAD.

■ Queries will return faster.

Single SIGAD selected

- Less work for the system.

Cancel



# Common mistakes

- If you select the SQL Report option, make sure you put a valid SQL statement!

SQL statement filled in:  
 SELECT casenotation,  
 count(\*)  
 FROM %~~{~~OUTPUT\_TABLE}  
 WHERE casenotation!="  
 GROUP BY casenotation

Workflow Central Request Wizard

Follow-on Actions

Would you like to add any follow on actions

No  
 Yes

| Script     | Script Arguments  | Add |
|------------|---|-----|
| SQL Report | Type: CSV<br>Email To: analyst@work.com<br>Email Subject: My Workflow Results<br>Email Content: Bad SQL - empty<br>Email Attachment: <input type="checkbox"/> Email Attachment<br>ROWR: <input type="checkbox"/> Return Only With Results<br>Filename:<br>Mail Order Trigraph:<br>SQL: SELECT casenotation, count(*)<br>FROM % <del>{</del> OUTPUT_TABLE}<br>WHERE casenotation!="<br>GROUP BY casenotation<br>GZIP: <input type="checkbox"/> Compress Contents | +   |

Cancel Prev Next Submit



Questions?  
[xks\\_workflow@r1.r.nsa](mailto:xks_workflow@r1.r.nsa)