# (U//FOUO) TRAFFICTHIEF Configuration Read Me

**(U) Overview**

(S//REL) TRAFFICTHIEF (TT) is the NSA corporate alerting and tipping system. Independent collection systems such as XKEYSCORE provide real-time messages, called events (tips), to the TRAFFICTHIEF server. TRAFFICTHIEF receives these tips in real-time when targets are actively communicating, enhances messages with geo-location information and then immediately alerts analysts to this activity.

**(U) Pre-Configuration Requirements**

(U/FOUO) Before configuring *xks.config* for TRAFFICTHIEF tipping, you must:

1. (S//SI//REL) Confirm Unified Targeting Tool (UTT) tasking is delivered from a Site Selection Distribution Manager (SSDM). Please refer to the *UTT Configuration Read Me* for configuring UTT tasking.

2. (S//SI//REL) Confirm the UTT sends selector targeting information to the SSDM to manage selector tasking at a field site. The SSDM receives load and update requests from UTT and is responsible for any site-specific processing that must be performed before forwarding the appropriate subset of information to the site-local collection system.

3. (C) Confirm that port 443 is open if tips will be sent via socket to the TT server (e.g., using the `alert_trafficthief` plugin).

   ***NOTE:*** (U//FOUO) If tips will be sent over MAILORDER (i.e., using the alert_mailorder plugin), then port 443 does not need to be opened.

4. (C) Confirm MAILORDER is configured to pick up MAILORDER files from the *$XSCORE_DATA_DIR/outputs/mailorder* directory on the Master server. To do this, create a MAILORDER ticket to set up the pick-up directory for your Master XKS server:

   a. Type `go mailorder` in the URL field of a browser on a high-side computer.

   b. Click `PATHMASTER Remedy Ticket` near the top right of the screen. The *Remedy Ticket Submission* screen will appear.

   c. In the bottom half of the Remedy Ticket Submission screen is two yellow *Submit Remedy Ticket* buttons. Click the top button of the two. (This ticket pertains to New Data-Flow). The ITSC login screen will appear.

d. Enter the SID of your alternate POC and then click `Continue`. A screen containing contact information for you and your POC will appear.

e. Add/Edit the contact information as appropriate and then click `Continue` to go to the *Data transport service* screen.

f. Click `Dataflow request` and then click `Continue`. The *Request for New Data Flow on an Existing Transport System* screen will appear.

g. Enter as much information as you can. In the *Data Flow Change Description* field, specifically indicate that the pick-up directory should be:
/export/data/xkeyscore/outputs/mailorder

h. Click `Submit`. You will receive a confirmation e-mail indicating the ticket has been received and more information may be requested before the ticket can be completed. Overall, the process might take anywhere from a few days to a week to complete.

**(U//FOUO) Using Socket to Send 5I's Tips to TRAFFICTHIEF**

(U//FOUO) Follow these steps to configure the *xks.config* file use Socket to send 5I's Tips to TRAFFICTHIEF:

1. (U//FOUO) Log on as the user `oper`.
2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.
3. (U//FOUO) In the *Inputs* section of *xks.config*, set the following configurations:
   a. `alert_output = true` : This turns tipping "on."
   b. `alert_output_type = socket` : This indicates that all output will be sent via secure socket.
   c. `alert_instance = sitename` : This helps the analyst determine where the tip came from. The `sitename` name is included in the XML of the actual tip sent to TRAFFICTHIEF.
   d. `alert_host = 7.216.26.130:443` : This is the IP address and port number where the alerts are sent.

   ***Note:*** (U/FOUO) Which ever value is set equal to `alert_instance` is the value that is put into the instance field of the actual alert.
4. (U//FOUO) Type `wq!` and then press `Enter` to exit *xks.config*.

5. (U//FOUO) Perform the following commands only after making changes in *xks.config*. At the command prompt, type:

   a. `xks setup plugins` : This ensures any applicable changes to plugin configurations will take effect.

   b. `xks rsync push_config` : This pushes the latest configuration files to the slaves in the cluster.

   c. `xks proc saferestart` : After setup is complete, this restarts `process_data_parent's` for the new configuration to take effect. This process loads all the dictionaries and fingerprints and then performs dictionary scanning, metadata extraction, databasing of metadata, and archival of content. When the parent is finished reloading, it will do a staggered restart of its children based on which slave the parent is running on.

**(U//FOUO) Using Socket to Send NOFORN Tips to TRAFFICTHIEF**

(U//FOUO) Follow these steps to configure the *xks.config* file use Socket to send NOFORN Tips to TRAFFICTHIEF:

1. (U//FOUO) Log on as the user `oper`.

2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.

3. (U//FOUO) In the *Inputs* section of *xks.config*, set the following configurations:

   a. `alert_output = true: This turns tipping "on."`

   b. `alert_output_type = socket` : This indicates that output will be sent via secure socket.

   c. `alert_instance = sitename` : This is the location where the tip came from. The sitename is retrieved from the actual XML of the tip that is generated.

   d. `alert_host = 7.216.26.2:443` : This is the IP address and port number where the alerts are sent.

   ***Note***: (U//FOUO) The instance in the actual alert is filled in with the value assigned to `alert_instance` in *xks.config*.

4. (U//FOUO) Type `wq!` and then press `Enter` to exit *xks.config*.

5. (U//FOUO) Perform the following commands only after making changes in *xks.config*. At the command prompt, type:

   a. `xks setup plugins` : This enables the `alert_traffichief` plugin with the configurations established in Step 3 above .

   b. `xks rsync push_config` : This pushes the latest configurations to the slaves in the cluster.

   c. `xks proc saferestart` : After setup is complete, this restarts `process_data_parent's` for the new configuration to take effect. This process loads all the dictionaries and fingerprints and then performs dictionary scanning, metadata extraction, databasing of metadata, and archival of content.

**(U//FOUO) Using MAILORDER to Send 5I's Tips to TRAFFICTHIEF**

(U//FOUO) Follow these steps to configure the xks.config file to use MAILORDER to send 5I's Tips to TRAFFICTHIEF:

1. (U//FOUO) Log on as the user `oper`.

2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.

3. (U//FOUO) In the *Inputs* section of *xks.config*, set the following configurations:

   a. `alert_output = true` : This turns tipping "on."

   b. `alert_output_type = mailorder` : This indicates that output will be sent via MAILORDER.

   c. `alert_instance = sitename` : This is the location where the tip came from. The sitename is retrieved from the actual XML of the tip that is generated.

   d. `alert_host =` : This is the IP address where the alerts are sent. No IP address is required because, in this case, tips are being sent via MAILORDER.

   ***Note***: (U//FOUO) The instance in the actual alert is filled in with the value assigned to `alert_instance` in *xks.config*.

4. (U//FOUO) Type `wq!` and then press Enter to exit *xks.config*.

5. (U//FOUO) Perform the following commands only after making changes in *xks.config*. At the command prompt, type:

   a. `xks setup plugins` : This ensures any applicable changes to plugin configurations will take effect.

b. `xks rsync push_config` : This pushes the latest configuration files to the slaves in the cluster.

c. `xks proc saferestart` : After setup is complete, this restarts process_data_parent's for the new configuration to take effect. This process loads all the dictionaries and fingerprints and then performs dictionary scanning, metadata extraction, databasing of metadata, and archival of content.

**(U//FOUO) Using MAILORDER to Send NOFORN Tips to TRAFFICTHIEF**

(U//FOUO) Follow these steps to configure the *xks.config* file to use MAILORDER to send NOFORN Tips to TRAFFICTHIEF:

1. (U//FOUO) Log on as the user `oper`.
2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.

   a. `alert_output = true` : This turns tipping "on."

   b. `alert_output_type = mailorder` : This indicates that output will be sent via MAILORDER.

   c. `alert_instance = sitename` : This is the location where the tip came from. The sitename is retrieved from the actual XML of the tip that is generated.

   e. `alert_host =` : This is the IP address where the alerts are sent. No IP address is required because, in this case, tips are being sent via MAILORDER.

   ***Note:*** (U//FOUO) The instance in the actual alert is filled in with the value assigned to `alert_instance` in *xks.config*.

3. (U//FOUO) Type `:wq!` and then press `Enter` to exit *xks.config*.
4. (C) Perform the following commands only after making changes in *xks.config*. At the command prompt, type:

   a. `xks setup plugins` : This ensures any applicable changes to plugin configurations will take effect.

   b. `xks rsync push_config` : This pushes the latest configuration files to the slaves in the cluster.

   c. `xks proc saferestart` : After setup is complete, this restarts process_data_parent's for the new configuration to take effect. This process loads all the dictionaries and fingerprints and then performs dictionary scanning, metadata extraction, databasing of metadata, and archival of content.