



Using the FlowCollector User Interface

This chapter tells you how to use the FlowCollector user interface (NFUI) to review application statistics and resource definitions, such as for threads, filters, and protocols, or to create and modify FlowCollector resource definitions.

This chapter includes the following sections:

- [Starting the NFUI, page 3-1](#)
- [Using the NFUI, page 3-2.](#)



Note

The NFUI contains embedded help menus to assist you in navigating through the NFUI and understanding menu operations. The Help menus explain all of the options available for retrieving, configuring, and reviewing FlowCollector runtime configuration parameters and statistics. To display the **Help** menu, enter **h** from within any menu.

Starting the NFUI

FlowCollector should be running before you start the NFUI, otherwise, no FlowCollector application statistics or resource definitions are available for review.

To start the NFUI, enter the following command:

```
$    $NFC_DIR/bin/NFUI
```

The system displays the main menu of the NFUI (see [Figure 3-1](#)).

Figure 3-1 FlowCollector User Interface, Main Menu

```

----- NetFlow FlowCollector UI -----

MAIN MENU

1.  Threads
2.  Filters
3.  Protocols
4.  Source Ports
5.  Destination Ports
6.  UDP Ports
7.  Source ASNs
8.  Destination ASNs
9.  Source(s) IP Address(es)
10. Application Statistics
11. Dump Configuration
h.  Help
q.  Quit

Enter Item Number [1 - 11, (h)elp, (q)uit]:

```

Using the NFUI

Some of the main menu entries, such as the **Threads**, **Filters**, and **Protocols** configuration parameters, provide access to submenus where you can create new definitions or modify existing definitions. When you enter the number for one of these entries and press **Return**, the NFUI displays the submenu for that configuration parameter. For example, when you select item 1 from the main menu, the NFUI displays the **Threads** submenu (see [Figure 3-2](#)).

Figure 3-2 Threads Submenu

```

----- SUB MENU (Threads) -----

1.  List of Thread IDs
2.  Review Thread
3.  Modify Thread
4.  Create Thread
5.  Delete Thread
h.  Help
q.  Quit to main menu

Enter Item Number [1 - 5, (h)elp, (q)uit]:

```

All of the submenus have a format similar to that of the main menu shown in [Figure 3-1](#). The user interface displays some information and then prompts you to act on that information. For each NFUI prompt, you enter a number or an alphanumeric entry in the command entry line, and then press **Return**.

Each submenu contains an item that allows you to quit the current menu and return to the main menu. In the main menu, the **Quit** option exits the NFUI.

In those submenus where the NFUI prompts you to enter a complete entry, such as a thread or filter ID, the NFUI displays a list of the items you can use as a reminder. For example, when you select item 2 (**Review Thread**) in the **Threads** submenu (see [Figure 3-2](#)), the NFUI prompts you for a response, as shown in [Figure 3-3](#).

Figure 3-3 User Interface Prompt

2. Retrieve attributes of a Thread

Thread ID (Hit <CR> to see list of threads):

If you know the name of the thread you want to review, type it, then press **Return**. For example, if you entered the thread name **CALLREC**, the NFUI would display information similar to that shown in [Figure 3-4](#).

Figure 3-4 Thread Attributes

2. Retrieve attributes of a Thread

Thread ID (Hit <CR> to see list of threads):**CALLREC**

```
Thread CALLREC
  Aggregation    CallRecord
  Period         10
  Port           9995
  DataSetPath    /opt/CSCOnfc/Data
  State          Active
  Compression    N
  Binary         N
  MaxUsage       500
```

----- SUB MENU (Threads) -----

- 1. List of Thread IDs
- 2. Review Thread
- 3. Modify Thread
- 4. Create Thread
- 5. Delete Thread
- h. Help
- q. Quit to main menu

Enter Item Number [1 - 5, (h)elp, (q)uit]:

If you do not know the name of any threads, press **Return**, and the NFUI displays a list of all the defined thread names (see [Figure 3-5](#)).

Figure 3-5 Sample Thread ID List

2. Retrieve attributes of a Thread

Thread ID (Hit <CR> to see list of threads):<CR>

```
PROTO
CALLREC
DETHM
SRCPORT
DEINTER
```

Thread ID:

When you are creating or modifying a FlowCollector configuration parameter, such as a thread, filter, or protocol definition, the NFUI prompts you through each of the steps in the process and provides the applicable units (where appropriate) and the default value (where appropriate) in angle brackets (< >). For example, if you were modifying an existing thread, one of the steps in the process involves setting the Period parameter, where 10 minutes is the default.

```
Period (minutes) <10>:
```

When you come to the end of the process, the NFUI prompts you to confirm the created or modified configuration parameter. For example, if you are creating a new filter definition, the NFUI prompts you through all the steps, and then prompts you to confirm that you want to save the new filter:

```
Are you sure you want to create this filter? [Y/N]:
```

By entering **N** (no) and pressing **Return**, you cancel the save action (and lose any changes).

Information Displays

Some of the main menu entries display read-only resource definitions and statistics. You set resource definitions by editing one or more FlowCollector configuration files in the `$NFC_DIR/config` directory.

Displaying Lists of Defined Ports and Autonomous System Numbers

When you select one of the following main menu items in bold, the NFUI displays a read-only list of numbers similar to that shown in [Figure 3-6](#).

Figure 3-6 FlowCollector User Interface, Read-Only Options

```
----- NetFlow FlowCollector UI -----

MAIN MENU
1.  Threads
2.  Filters
3.  Protocols
4.  Source Ports
5.  Destination Ports
6.  UDP Ports
7.  Source ASNs
8.  Destination ASNs
9.  Source(s) IP Address(es)
10. Application Statistics
11. Dump Configuration
h.  Help
q.  Quit

Enter Item Number [1 - 11, (h)elp, (q)uit]:
```

For example, if you select item 4 (**Source Ports**) from the main menu, the NFUI displays information similar to that shown in [Figure 3-7](#).

Figure 3-7 Sample List of Source Ports

```
*** List of existing Source Ports ***

21:ftp
88
50, 100
1024, 1999:Other_Reserved_Ports
20000, 29999:My_Range
40000, 49999:My_Range

Press Return to continue ...
```

The content of the source and destination port or autonomous system number lists is determined by the definitions in the **nfknown.name** file that corresponds to the main menu selection item:

- **nfknown.sreports** (source ports)
- **nfknown.dstports** (destination ports)
- **nfknown.srcasns** (source autonomous system numbers)
- **nfknown.dstasns** (destination autonomous system numbers).

The process used to modify these files is described in the [“Defining Protocols” section on page 5-24](#).

Displaying a List of Defined UDP Port Numbers

When you select item 6 (**UDP Ports**) from the main menu, the NFUI displays information similar to that shown in [Figure 3-8](#).

Figure 3-8 Sample List of UDP Ports

```
*** List of existing UDP Ports ***

9995
9996

Press Return to continue ...
```

The UDP port numbers are the ports on which FlowCollector is expecting NetFlow data. In a default FlowCollector installation, ports 9995 and 9996 are automatically configured as the UDP ports. You can define other UDP port numbers (see [“Creating a Thread” section on page 5-8](#)). The content of the UDP ports list is determined by the active thread definitions in the **nfconfig.file** file.

Displaying a List of Source IP Addresses

When you select item 9 (**Source[s] IP Address[es]**) from the main menu, the NFUI displays information similar to that shown in [Figure 3-9](#).

Figure 3-9 Sample List of Source IP Addresses

```
*** List of Existing Export Devices ***

192.168.1.1
192.168.2.2
192.168.3.3
192.168.4.4
192.168.5.5
192.168.6.6

Press Return to continue ...
```

The list represents those IP addresses from which FlowCollector has received NetFlow data.



Note

In the case of packets filtered by source (address-based filtering), the list in the display is static and shows all the addresses (or names) from which the FlowCollector is configured to accept packets.

Displaying Application Statistics

When you select item 10 (**Application Statistics**) the NFUI displays a table of statistics on FlowCollector operation (see [Figure 3-10](#)).

Figure 3-10 Sample Application Statistics

```
10. Retrieve application stats
FlowCollector has been up since Wed May 20 13:56:49 1999

Port      Packets rcvd(wrap)    Records (wrap)    Discarded    Missed Recs (wrap)
----      -
9995      0 (0)                 0 (0)             0             0 (0)
9996      70748 (0)             2122440 (0)       0             0 (0)
```

[Table 3-1](#) lists and describes the fields of the application statistics.

Table 3-1 Application Statistics Field Descriptions

Field	Description
Port	The port number of the UDP port FlowCollector uses to listen for NetFlow data.
Packets rcvd (wrap)	The number of packets received on this port, and the number of times this counter has wrapped. This counter wraps after it has reached 4,294,967,295.
Records (wrap)	The number of flow records FlowCollector has detected, and the number of times this counter has wrapped. This counter wraps after it has reached 4,294,967,295.

Table 3-1 Application Statistics Field Descriptions (continued)

Field	Description
Discarded	The number of packets FlowCollector has discarded. FlowCollector discards unsolicited packets or packets in an invalid version or format. In its default configuration, FlowCollector accepts NetFlow export packets from any IP address. If necessary, you can use the ACCEPT_PACKETS_FROM configuration parameter to specify the source IP addresses or defined ROUTER_GROUPNAME labels from which FlowCollector should receive NetFlow export packets, thus allowing FlowCollector to discard “unsolicited” packets from unspecified sources. For information on how to do this, see the “Preventing FlowCollector from Accepting Unsolicited Packets” section on page 5-37.
Missed Recs (wrap)	The number of flow records that FlowCollector should have detected but did not, and the number of times this counter has wrapped. This counter wraps after it has reached 4,294,967,295. This value is derived from the sequence numbers (when present) in each packet. If a UDP port has only received Version 1 datagrams or Version 7 datagrams with shortcut mode enabled (or a combination of these two), the Missed Records column for that UDP port displays a -1 to indicate that this field does not apply. If a UDP port has received any Version 5 or Version 7 (with shortcut mode disabled) datagrams, the Missed Records column for that UDP port displays the true count of missed records. If there are no missed records, the Missed Records column for that UDP port displays a zero.

Saving the Current Configuration

When you select item 11 (**Dump Configuration**), the NFUI saves the current FlowCollector configuration parameter values in a log file. In a standard installation, the default log file is named **nfc.log** and is located in the **\$NFC_DIR/logs** directory.



Note

If you edited the **nf.resources** file to change the path name of the log file, the **nf.resources** variable **NFC_LOG** represents the location of the log file.