Configuring Audit Logging

The 128T Networking Platform can maintain a history of all configuration changes in its *event log*, which can subsequently be used to support compliance audits, forensics on network issues related to configuration (misapplied or otherwise), and traceability. This document covers:

1. Enabling the Audit Log (using the PCLI or the GUI)
2. Using the Event Viewer in the GUI

Basic Configuration

The configuration for audit logging is done within the `system > audit` branch within a `router` hierarchy, by setting the `enabled` property within the `administration` branch to `true`. In most cases, the only configuration that is required for enabling audit logging is to add it to the `router` element for your Authority's conductor. For cases where a 128T router is not managed by a conductor, its audit logging configuration is similarly added to the `system > audit` branch of its `router` hierarchy.

Sample Configuration

Here is a sample configuration showing the minimum required configuration to enable audit logging.

> Note: configuration not related to audit logging has been filtered out for illustrative purposes.

```
admin@labsystem1.fiedler# show config running authority router fiedler system

config
    authority
        router  fiedler
            name    fiedler
            system
                audit
                    administration
                        enabled  true
                    exit
                exit
            exit
        exit
    exit
exit
```

Viewing the Audit Log

In 4.1.0 software, the only way at present to view the contents of the audit log is via the GUI (on the conductor or router as configured above).

To view the contents of the audit log, navigate to the **Tools** page and choose **Event History**. The Event History viewer shows all of the events that this 128T has accumulated, including audit log events. Audit log events are of type **ADMIN**; you can use the built-in filtering mechanism to limit the Event History search results to ADMIN type events to find events of interest.