Using the Checkpoint Collector Control Application

# Moving The Controller Executable And Config File

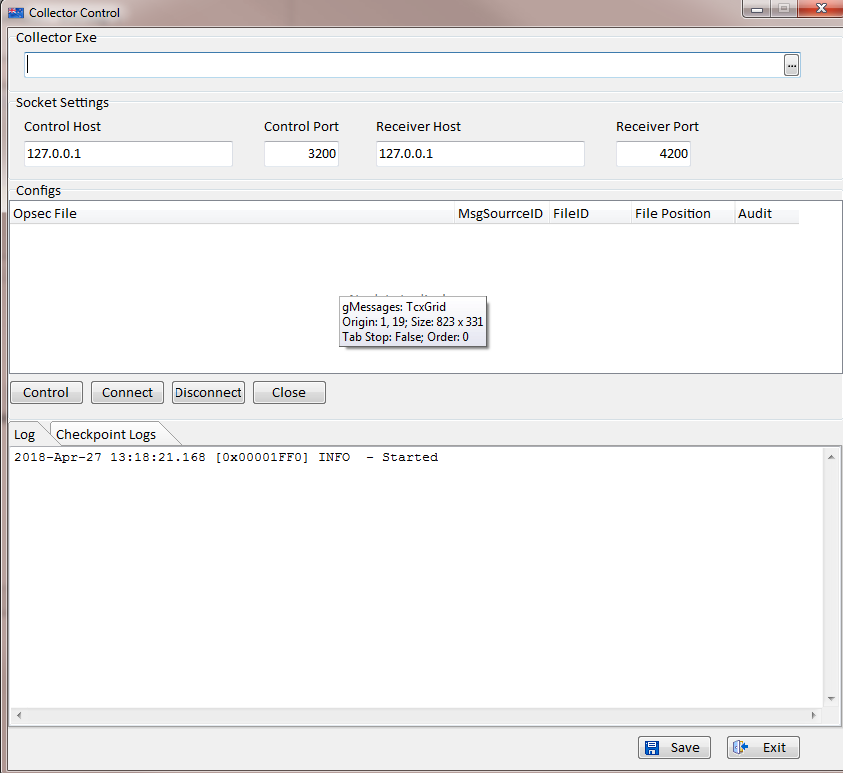
To run connect to the checkpoint instance you will need to things.

1. The **chkptconsole.exe** application located in the <Program Files>\LogRhythm\LogRhythm System Monitor directory.
2. The opsec config file.

Create an new folder somewhere on the machine (I used d:\CheckpointCert when testing, but you can call yours anything) and copy these two files into this directory.

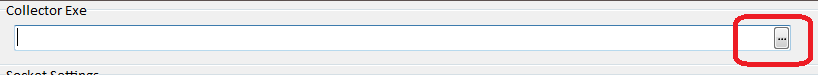
# Running The Controller

The next step is to run the controller application. You will see the main screen like so:

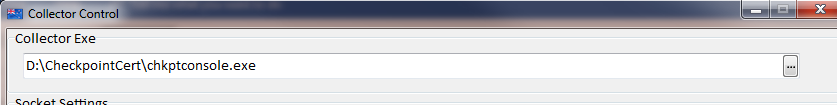


## Setting Up Collector

The first thing you need to do is tell it where the collector exe is. In the Collector exe section you click on the find file button:

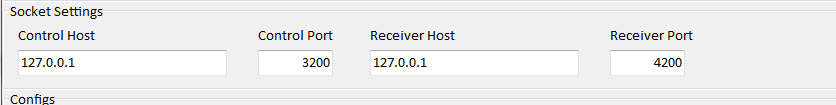


Then use the open file dialog to navigate to the folder you created earlier which should contain the exe and config files. Select the chkptconsole.exe file like so:



## Setting Up The Control Ports And Host

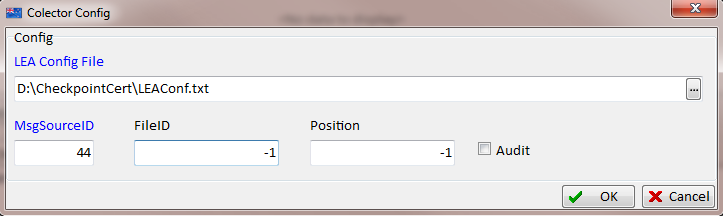
Generally the default socket settings are fine. But if you whish to use other ports or a network card you can set them appropriately.



## Adding A Config

Next we need to add a config file and a Message Source ID. Any positive integer will do for the Message Source ID. Since the logs won’t be going into the system, it won’t matter. There just needs to be one.

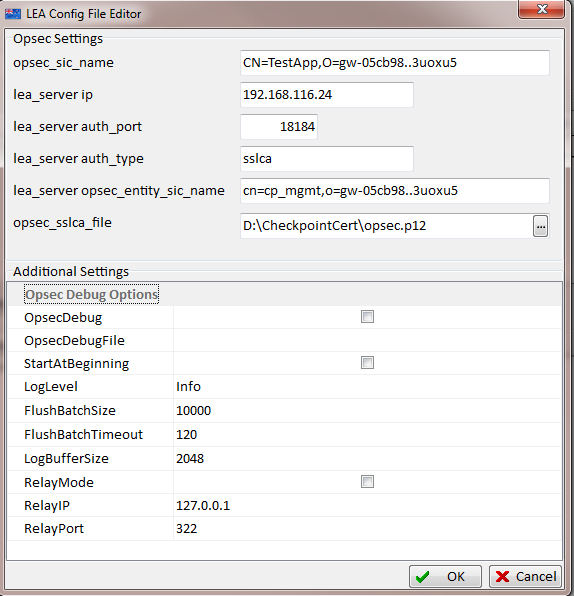
Right click on the Configs grid and select **New**. You will see a screen like the one below:



Fill in the config file (use the one you copied into the folder earlier) and set the MsgSrc ID. Leave the FileID and Position/ Check Audit if you want Audit logs instead of Firewall/Blade Logs.

Once you click OK you should see a new entry in the grid.

Highlight the new entry and select **Edit LEA Config File.** You will see the following screen:



Use this to fine tune the collector settings. By default the collector will start collection at the end of the current log file. Use StartAtBeginning to force it to collect from the start. This way you will not have to wait for the Firewall to generate an event before seeing data.

FlushBatchSize (default 10K) and FlushBatchTimeout (default 120 seconds) work together to control the rate at which the collector sends logs to the controller port. It will send a batch of logs every 10K logs or every 120 seconds – whichever condition occurs sooner. So, if you have a low volume system, or just want to see the data faster, reduce the FlushBatchTimeout setting.

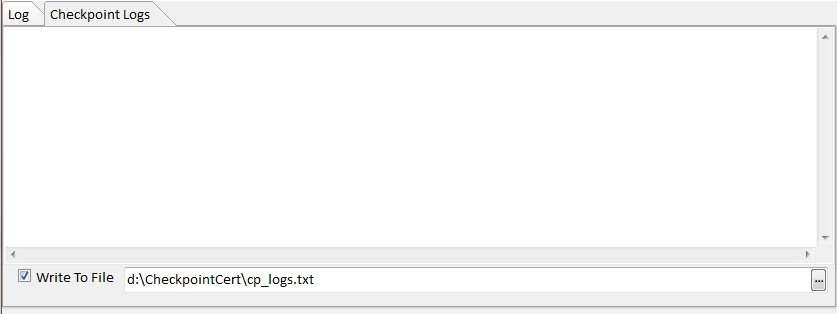
Relay mode is used to tell the collector *not* to connect to a checkpoint log server but instead to wait for messages from a Relay Client application. This is useful for running tests without a checkpoint system available.

Once you have set it up the way you need it to operate click OK. You can then save the opsec config to a new file, or overwrite the existing.

**Note**: If you save to a new file you will need to update the config entry in the grid accordingly.

## Setting Up Log Reception

Go to the Page Control at the bottom of the screen and select Checkpoint Logs:



When the collector picks up log records it posts them to the controller which displays them here.

You also have the option to write these logs to a file. You should do this if you need to inspect/play them back later.

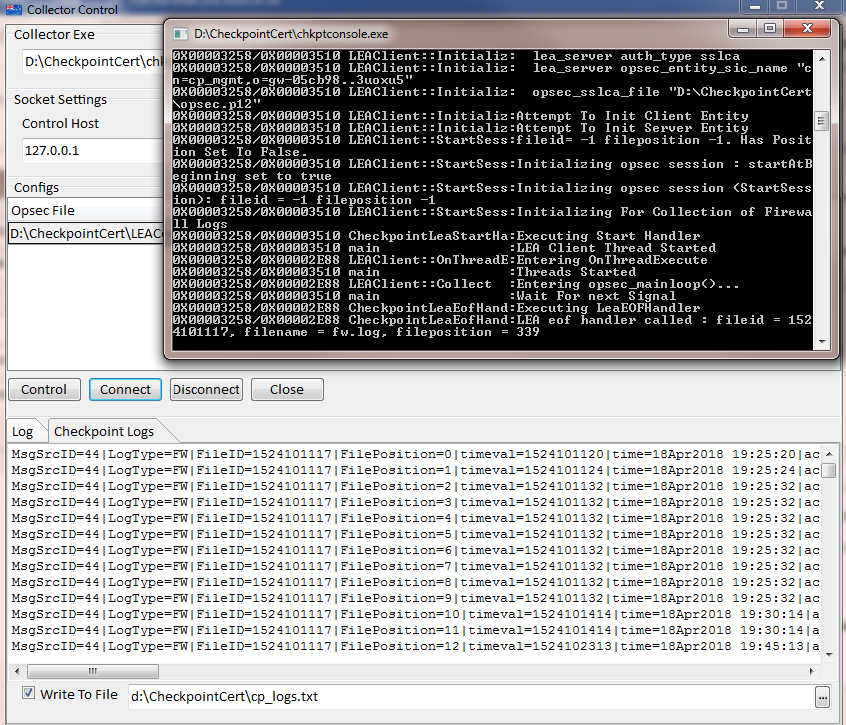
Once you have configured the Controller Click on the **Save** button.

# Running the Collector



First, Click the **Control** button. This will open the control and data receiver ports.

Next click on the **Connect** button. If everything is setup correctly the collector will start and logs will begin to appear in the logs window:



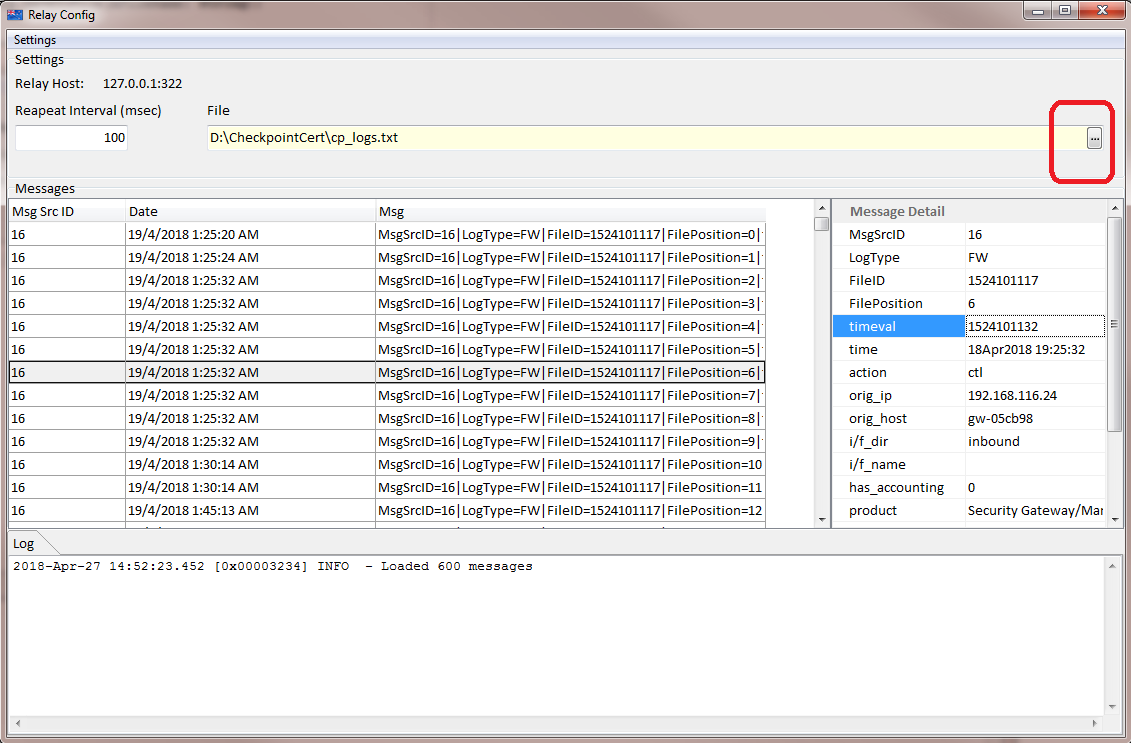
Click on **Disconnect** to shutdown the controller.

Finally click **Close** to shut down the control sockets.

**Note:** Some temp files may be created in <Program Files>\HoodedClaw folder. If this presents a permissions issue then you can copy the two exes out of this folder and into the same folder as the controller and config and run them from there.

# Using The Relay Client To View The Logs

If you have set the controller to log to a file you can view this file in the Relay Client. Start the Relay Client application, and select the find file button to select the logs file you set up earlier.



Once the grid is loaded highlight a message to see it’s message detail on the right.