ArcSight

ArcSight, Inc.

Date Created: 3/29/2010

Using the ArcSight Test Alert SmartConnector to Send Events to an ESM Manager

For content development and test scenarios, you might want to use the Test Alert SmartConnector to send specific types of events to an ESM Manager.

- You can use Test Alert to manually define events and send them.
- You can also use the Test Alert **Replay** feature along with a set of canned events to create an example event flow that mimics a live network. You can use this setup to replay events in test scenarios so that channels like "Today" or "Live" show a steady flow of events, other than just system events

The following topics explain how configure the Test Alert SmartConnector and use it to define and send events manually or replay canned events on an ESM Manager.

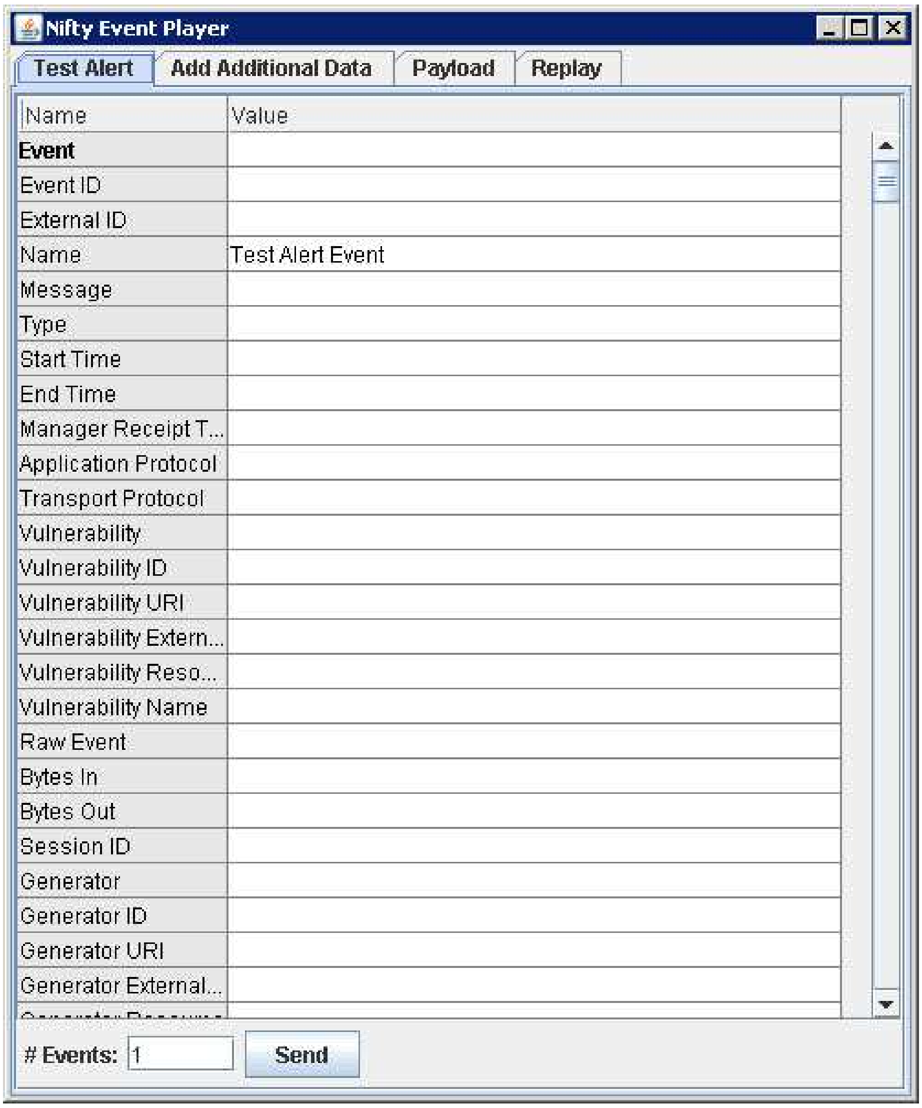
Multiple test alerts and event players can be configured to send events to the same Manager.

Install and Start the Test Alert SmartConnector

1. Download and install ArcSight SmartConnectors.
2. Choose **Test Alert** as the SmartConnector to install. (Point to the appropriate ESM Manager host and port as part of installation procedure.)

How to Define and Send Test Alert Events Manually

1. Start the Test Alert SmartConnector.
2. The Test Alert dialog is displayed with some default settings. (**Event Name** is set to have "Test Alert Event" and the **# of Events** to send is set to "1")



Name	Value
Event	
Event ID	
External ID	
Name	Test Alert Event
Message	
Type	
Start Time	
End Time	
Manager Receipt T...	
Application Protocol	
Transport Protocol	
Vulnerability	
Vulnerability ID	
Vulnerability URI	
Vulnerability Extern...	
Vulnerability Reso...	
Vulnerability Name	
Raw Event	
Bytes In	
Bytes Out	
Session ID	
Generator	
Generator ID	
Generator URI	
Generator External...	

Events: 1

3. To send a single event to the ESM Manager with the given defaults (**Event Name:** Test Alert Event), just click **Send**.

4. You can supply values for all the fields as needed and modify the number of events sent to satisfy your testing purposes.

   For example, if you are testing a rule that should trigger whenever a particular server (e.g., goldmine) is accessed, you might send events with the **Target Host Name** defined to match the server (**Target Host Name:** goldmine).

How to Configure an Event Player

To use the Test Alert "Event Player" feature, you'll need a set of replay events in a specially formatted replay file. For information on how to collect events and create this replay file, please see ***ArcSight Knowledge Base Article Number*: *2675***.

Once you have your replay file, you are ready to configure and use the Test Alert Smart Connector as an Event Player. Let's get started!

1. Drop one or more replay files into your SmartConnector Home directory ArcSightSmartConnectors-<*version*>`/current/` folder.

   If you have replay files set up in folders or subdirectories, you can drop the entire top-level folder into that same SmartConnector Home directory. Test Alert will recognize and display replay files in the top-level folder and all subfolders.

   Once you have made the replay files available, you can enable and disable specific files as described in the next steps.

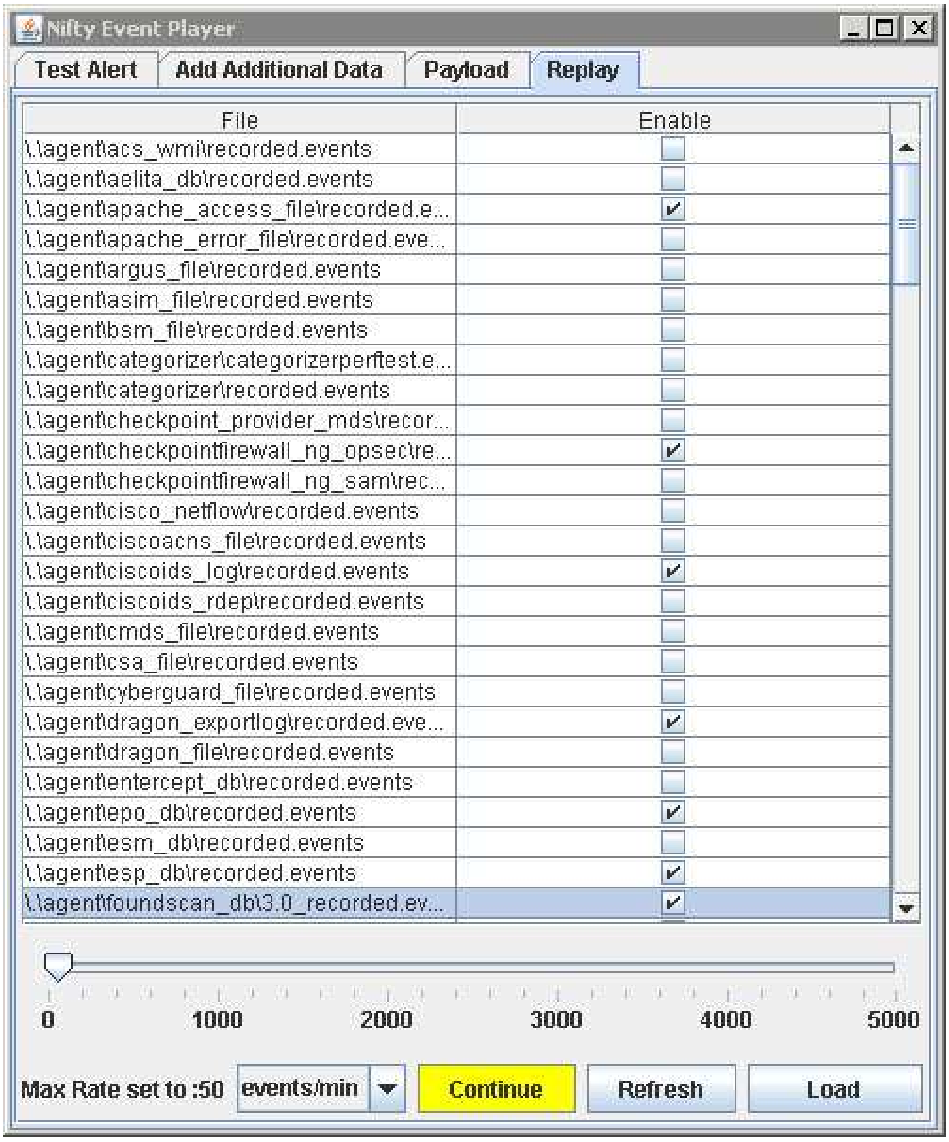
2. Start the Test Alert SmartConnector.
3. Click the **Replay** tab on the Connector dialog. If you put the replay files in the right place, they will show up here under **File**.
4. Select which replay files to enable.

   Click the **Enable** checkbox next to one or more replay file to choose event types to send.

5. Set the rate at which your replay events will be sent to the ESM Manager.
   - Use the drop-down menu at the lower left to set the rate metric to either events/min (events per minute) or events/sec (events per second).
   - Drag the slider to right to increase the number of events sent per minute or second. Drag the slider to the left to decrease the number of events sent.

   The Connector polls these settings frequently and adjusts event flow rate accordingly. You can adjust the rate of the event flow at any time.

6. Click **Continue** to start sending events to the Manager.



File	Enable
\.\agent\acs_wmi\recorded.events	☐
\.\agent\aelita_db\recorded.events	☐
\.\agent\apache_access_file\recorded.e...	☑
\.\agent\apache_error_file\recorded.eve...	☐
\.\agent\argus_file\recorded.events	☐
\.\agent\asim_file\recorded.events	☐
\.\agent\bsm_file\recorded.events	☐
\.\agent\categorizer\categorizerperftest.e...	☐
\.\agent\categorizer\recorded.events	☐
\.\agent\checkpoint_provider_mds\recor...	☐
\.\agent\checkpointfirewall_ng_opsec\re...	☑
\.\agent\checkpointfirewall_ng_sam\rec...	☐
\.\agent\cisco_netflow\recorded.events	☐
\.\agent\ciscoacns_file\recorded.events	☐
\.\agent\ciscoids_log\recorded.events	☑
\.\agent\ciscoids_rdep\recorded.events	☐
\.\agent\cmds_file\recorded.events	☐
\.\agent\csa_file\recorded.events	☐
\.\agent\cyberguard_file\recorded.events	☐
\.\agent\dragon_exportlog\recorded.eve...	☑
\.\agent\dragon_file\recorded.events	☐
\.\agent\entercept_db\recorded.events	☐
\.\agent\epo_db\recorded.events	☑
\.\agent\esm_db\recorded.events	☐
\.\agent\esp_db\recorded.events	☑
\.\agent\foundscan_db\3.0_recorded.ev...	☑

Max Rate set to :50 events/min

After you click **Continue**, that button option will be **Pause**. Click **Pause** to temporarily stop sending your replay events to the Manager from this SmartConnector. Click **Continue** to restart the flow of replay events.

Note: If you need to reconfigure, you can shut down this SmartConnector from your local system (just close the Test Alert dialog or do **Ctl-C** in the command window that's running the command), and then run **runagentsetup** in the bin directory. Otherwise, be sure to keep the command window and Connector dialog open. Just minimize them, if needed, to get them out of the way.

Both the command window and the Connector dialog need to stay open to keep the replay connector running and sending events.

7. Now, start the ESM Console, if you haven't already.
   - To view your new SmartConnector, choose **Connectors** in the Navigator, look under /Shared/All Connectors/<*FolderName*> where <*FolderName*>is the

"location" name you provided when you installed the Test Alert connector. You can control the Connector through the Console via right-click commands on the connector like Send Command > Status > <*command*> and Send Command > Event Flow > <*command*>

- To view events, look at various **Dashboards** and **Active Channels**. Your Test Alert replay events should show up on monitors and channels now.

How to Re-register a Connector (after a Manager update)

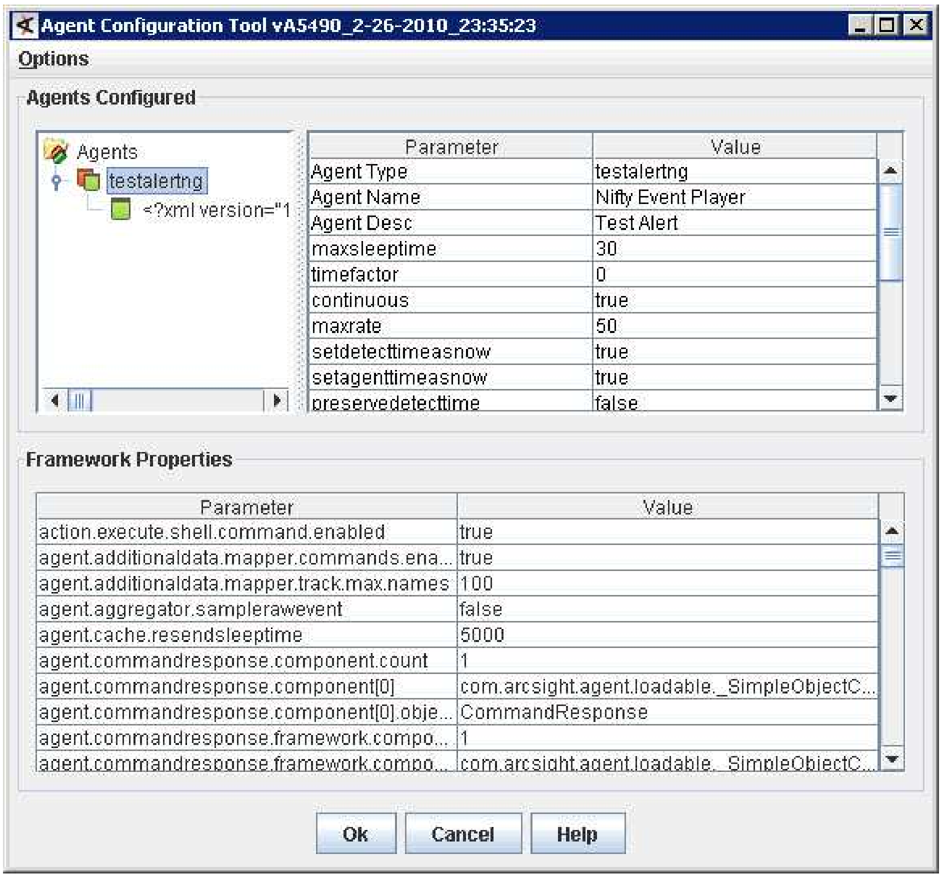
If a new Manager is installed, you have to unregister the original SmartConnector, "create" a new one for registration purposes, and register the new connector to the new Manager. This is done on the machine where the connector is installed:

1. Stop the current SmartConnector.

   How you do this will depend on how the connector was started. If you started the connector from the command line, just click the close (X) button in upper-right of the dialog. The command window in which the connector was running will show shutdown messages and then the command prompt at ArcSightSmartConnectors-`<version>/current/bin` directory.

2. From the bin directory, run the following command: **arcsight agentsetup**

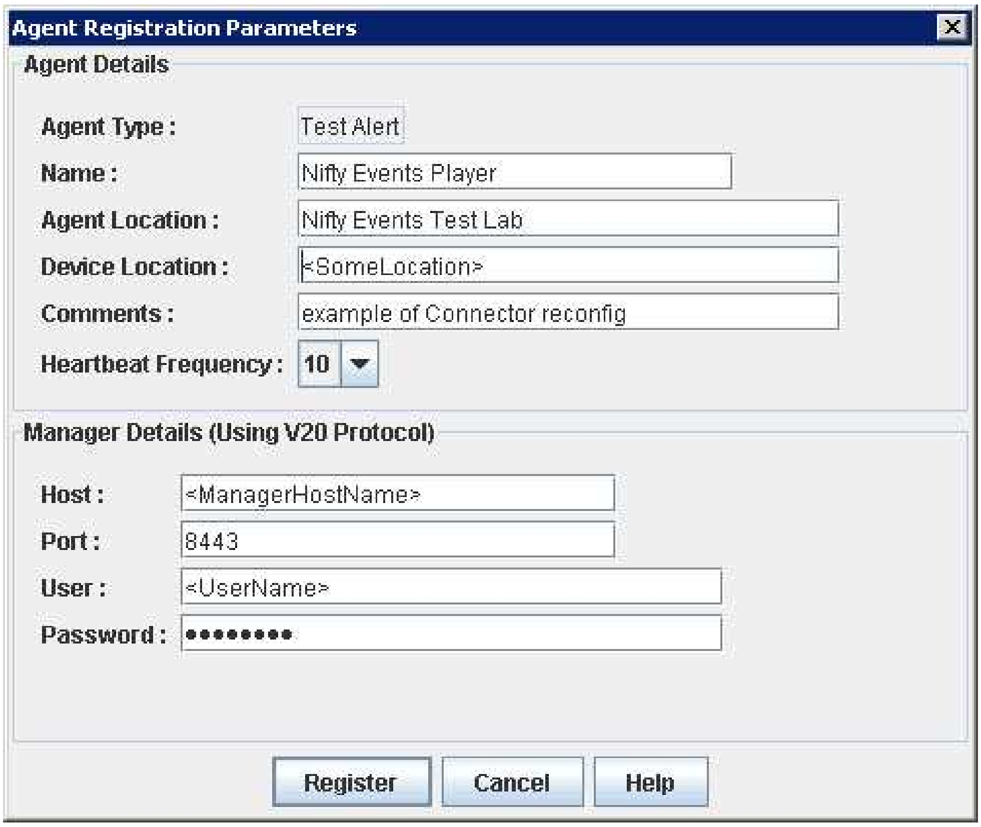
   You can choose to use the wizard or not. We recommend clicking **No** here. This brings up the Agent Configuration Tool dialog.



Parameter	Value
Agent Type	testalertng
Agent Name	Nifty Event Player
Agent Desc	Test Alert
maxsleeptime	30
timefactor	0
continuous	true
maxrate	50
setdetecttimeasnow	true
setagenttimeasnow	true
preservedetecttime	false

Parameter	Value
action.execute.shell.command.enabled	true
agent.additionaldata.mapper.commands.ena...	true
agent.additionaldata.mapper.track.max.names	100
agent.aggregator.samplerawevent	false
agent.cache.resendsleeptime	5000
agent.commandresponse.component.count	1
agent.commandresponse.component[0]	com.arcsight.agent.loadable._SimpleObjectC...
agent.commandresponse.component[0].obje...	CommandResponse
agent.commandresponse.framework.compo...	1
agent.commandresponse.framework.compo...	com.arcsight.agent.loadable._SimpleObjectC...

3. On this dialog under "Agents Configured", right-click the current connector and select **Add Additional Destination**. This brings up a dialog where you can register a new connector.



Agent Registration Parameters

Agent Details

Agent Type : Test Alert

Name : Nifty Events Player

Agent Location : Nifty Events Test Lab

Device Location : <SomeLocation>

Comments : example of Connector reconfig

Heartbeat Frequency : 10

Manager Details (Using V20 Protocol)

Host : <ManagerHostName>

Port : 8443

User : <UserName>

Password : •••••••••

4. Provide a name for the new connector or "agent" (that differs from that of the previous one). Optionally, provide agent location and device location. Enter the User and Password for the Manager.

   Click **Register**. The new connector will show up under "Agents Configured"

5. Remove the old connector. Right-click on it and choose **Remove Agent**.

   Note: Be sure not to remove the old connector until after you set up a new one, otherwise the icon representing the connector will disappear altogether and you won't get the configuration options you need.)

6. Click **OK** to close the dialog and save these changes.

7. Re-start the Connector.