Sentry II 9.0 Feature
User Logon/Logoff Monitoring & Reporting

Sentry II User Logon/Logoff Monitoring & Reporting Steps:

Are you frustrated with trying to work with Windows Event Logs to get a simple, straight-forward view of your interactive User Logon/Logoff activity across your corporate set of Windows workstations?

With Sentry II release version 9.0.17, Sentry II introduces a new Agentless monitoring feature for User Logon/Logoff activity on Windows servers and workstations. Now a Sentry II Windows Agent is capable of monitoring other Windows servers or workstations for interactive User Logon/Logoff activity and there is a new User Logon/Logoff report that you can schedule to run automatically or run on a 'ad-hoc' basis and get a simple, straight-forward view of this activity.

To Use this feature:

- Deploy and/or update one or more of your Sentry II Windows Agents to the latest version 9.0.17 or later. In 'Configure->Servers/Agents & Devices', select one or more of these Agents and for each, click Edit to change the entry.

- Set the 'Agentless Srvrs/Wrks:' checkbox.

- Click the button with the single computer icon to the right of the check box and pop-up a text box where you enter the comma-delimited list of server/workstation names that you want this selected Agent to monitor for interactive User Logon/Logoff activity. You can copy and paste or import this list from other sources.

- Click OK on the pop-up to save the server/workstation list. The list is saved in a text file in the "…\Sentry II\WSList" folder using the naming convention for the file of 'AgentName[]WorkstationList.txt'. Since this is a text file, you can also external to Sentry II edit and change the comma-delimited list if the file. Fo example, if you have a population of workstations that change frequently, you could run a script under Sentry II's CustomWatch that would query Active Directory and update the list file. Sentry II will detect automatically the changed file and update the appropriate Agent.

- Click Save on the 'Configure->Servers/Agents & Devices' so that the state of the 'Agentless Srvrs/Wrks:' checkbox is saved. You can control whether the selected Agent monitors the servers/workstations in the last based on the state of the checkbox. To successfully have an Agent monitor other servers/workstations you need to have both the checkbox set and a workstation list text file, named as described, in the "…\Sentry II\WSList" folder.

- You can designate multiple Agents to do this monitoring and thus handle a large population of workstations. Each Agent can handle monitoring up to 500 servers/workstations for this interactive User Logon/Logoff activity. For example, designate 20 different distributed Agents, each monitoring 500 workstations, and monitor a total population of 10,000 workstations!

- The Agents that are designated to do the Agentless monitoring do need 'Admin" rights to make the remote RPC calls. The Agent by default runs under the 'Local System' account. Go to the machine(s) with the designated Agent(s), change the 'Sentry II Agent Service->Property->Logon' to 'Administrator' type credentials, and then restart the Agent service.

- When the Agent detects changed state of any the servers/workstations it is monitoring, data is sent to the Sentry II Server where it is written to the "ServerMetrics" table in the database.

- You can go to 'Report->Schedule Periodic Reports' and schedule the 'User Logon/Logoff' report to run periodically and report on one or more users and/or workstations; or go to 'Report->Run/Analyze & View' and run an 'ad-hoc' report and report on one or more users and/or workstations for any time-frame.

- A 9.0.17 or later Agent will automatically and unconditionally monitor its own server/workstation for interactive User Logon/Logoff activity. This information will also be displayed as part of the pop-up information box when you hover with the mouse over the server/workstation name in the 'Sentry II->System Monitor' and 'Display->Network Status' displays.

- Information displayed and reported for a User Logon includes: (1) the server where the User was authenticated, (2) whether the session is a local 'console' session or a remote 'RDP' session, and (3) if a remote 'RDP' session then the name of the remote client machine.

- If you are not getting User Logon/Logoff information from workstations you think you have configured correctly, Go to 'Monitor->System Monitor' and click the button in the 'Log' column for the designated Agent. In the pop-up, set the checkbox to enable Agent logging to disk. After about 20 minutes, Upload the Agent log through the same pop-up (this time click the 'green' checkmark), and then get the log from the Sentry II Server "...\Sentry II\AgentLogs\..." folder and take a look at it. If you are seeing "Access Denied" then you have not set the designated Agent service 'Logon' property to use 'Admin' credentials as described in step above. If you see 'Network Path Not Found' errors, this implies that the workstations are turned off, not visible, or otherwise not reachable. Contact Breakout Support if you are still having problems.

- There is a modest license fee for this 'agentless' monitoring based on the number of workstations to be monitored 'agentlessly'. The 1st 10 workstations are free. Workstations beyond that require a paid license based on the total count.

- In subsequent updates we will be adding additional "agentless" monitoring features such as basic CPU, Disk and Memory monitoring. If there is some workstation monitoring feature you would like to see, please email support to let us know your ideas.