

Agent health check enhancements *Detailed Document*

Abstract

This document is to guide the user about the EventTracker Agent Updates **ET82UA16-012** and its functionalities.

Target Audience

EventTracker users, Support Team.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

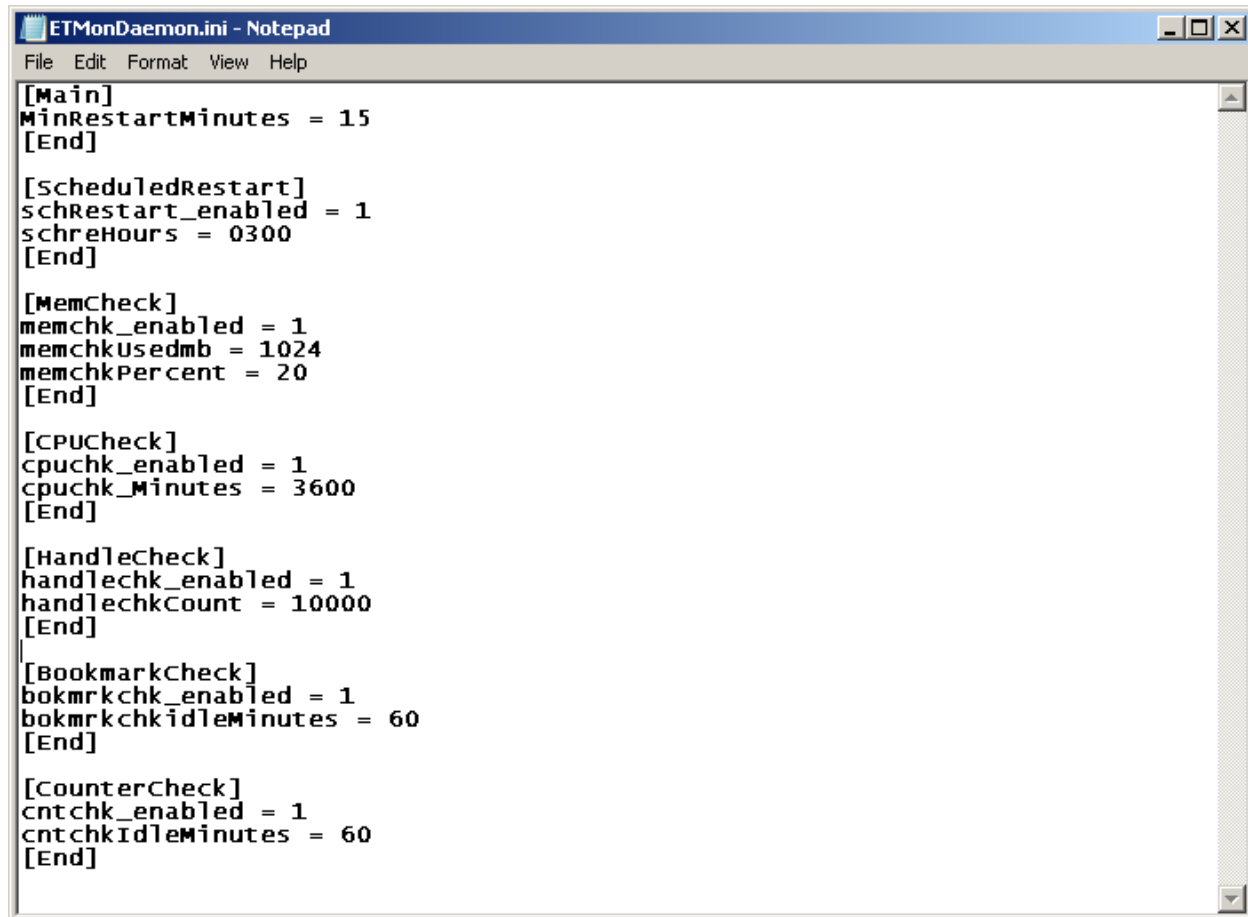
© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

How the EventTracker Agent update works?

The update includes few Agent Health Check Enhancements. Once the user applies the EventTracker Agent update **ET82UA16-012**, a new service named '**EventTracker Monitoring Daemon**' gets added. It monitors the EventTracker agent activities including Memory, Handles, CPU Time, Registry Bookmark and Counter Check (evtViewerLog.etw).

The EventTracker Agent update will perform the below mentioned functions:

1. The watch dog service (**EventTracker Monitoring Daemon**) will be created on target agent and manager system to monitor the EventTracker Agent service.
2. If EventTracker agent service is down, then the daemon service will start the agent service and send a trap to reporting manger.
3. If the Agent Memory is consuming more than 1GB then the daemon service will restart the agent service and send a trap to reporting manger.
4. If the Agent CPU time is more than 6 Hour then the daemon service will restart the agent service and send a trap to reporting manger.
5. If the agent handle count crossed more than 10,000 then the daemon service will restart the agent service and send a trap to reporting manger.
6. If the Registry (Bookmark) is not updated for 1 hour, then the daemon service will restart the agent service and send a trap to reporting manger.
7. If the ETW file (evtViewerLog.etw) is not updated for 1 hour, then the daemon service will restart the agent service and send a trap to reporting manger.
8. Schedule restart of agent service by 3:00 AM every day.
9. The trap will contain information like system name and OS type.
10. The threshold values are hardcoded. If the user wants to change the threshold values then the user should provide a custom ETMonDaemon.ini in [\\install directory\Prism Microsystems\EventTracker\Agent](#) folder, which holds the threshold values as shown below:

A screenshot of a Notepad window titled "ETMonDaemon.ini - Notepad". The window contains the following configuration text:

```
[Main]
MinRestartMinutes = 15
[End]

[ScheduleRestart]
schRestart_enabled = 1
schreHours = 0300
[End]

[MemCheck]
memchk_enabled = 1
memchkUsedmb = 1024
memchkPercent = 20
[End]

[CPUCheck]
cpuchk_enabled = 1
cpuchk_Minutes = 3600
[End]

[HandleCheck]
handlchek_enabled = 1
handlchekCount = 10000
[End]

[BookmarkCheck]
bokmrkchk_enabled = 1
bokmrkchkidleMinutes = 60
[End]

[CounterCheck]
cntchk_enabled = 1
cntchkIdleMinutes = 60
[End]
```

Audit Trail event

- Event ID 3520 will be generated when the agent is started or restarted successfully, with Event Type as Information. The same event id will be generated when the default threshold is crossed by the agent.

Sample Description:

Sample 1:

Event Type: Information

Log Type: Application

Category Id: 2

Description:

EventTracker Monitoring Daemon:

System Name: R154-VM1

Operating System Type: Windows 7

EventTracker Agent service started successfully.

Agent health check enhancements

Sample 2:

Event Type: Information

Log Type: Application

Category Id: 2

Description:

EventTracker Monitoring Daemon:

System Name: R154-VM1

Operating System Type: Windows 7

CounterCheck is not updated from last 60 min, restarted the agent service.

- When the agent fails to start or restart agent service, then it generates the event id 3520, with Event Type as: Error.

Sample Description:

Sample 1:

Event Type: Error

Log Type: Application

Category Id: 2

Description:

EventTracker Monitoring Daemon:

System Name: R153VM1

Operating System Type: Windows Server 2008 R2

Handle threshold crossed the limit of (1200), stopping the agent service failed.