System iNtrusion Analysis & Reporting Environment

# Release Notes for Snare Enterprise Agent for MSSQL v1.2/1.3

## About this document

This document provides release notes for the Snare Enterprise Agent for MSSQL version 1.2 and version 1.3.

# Snare Enterprise Agent for MSSQL v1.3.4

**Snare Enterprise Agent for MSSQL v1.3.4 was released on 8th May 2015.**

## Change Log

This release includes the following:

## Security Updates

- **Updated the OpenSSL library**

  Maintenance update for OpenSSL to patch to OpenSSL-1.0.1m that includes bugs and security fixes.

## Snare Enterprise Agent for MSSQL v1.3.3

**Snare Enterprise Agent for MSSQL v1.3.3 was released on 19th March 2015.**

### Change Log

This release includes the following bug fixes:

### Bug Fixes

- **Snare core memory usage keeps increasing**

  There was an issue with the comparison of the error code returned by the UDP connection used to send logs. Due to this issue the agent was dropping UDP connections frequently considering it erroneous. This issue is fixed in this release and the agent now correctly checks the status of a UDP connection and does not drop it when it is temporarily unavailable.

- **Agent uses lot of CPU and then crashes**

  There was an issue with the handling of the internal cache of the agent. This issue in some cases can cause the agent to crash if the MSSQL agent is frequently unable to send logs (i.e. destination server is down and/or busy network). This issue is fixed in this release. Now agent correctly handles internal cache in all cases when destination server is down and/or network is busy.

# Snare Enterprise Agent for MSSQL v1.3.2

**Snare Enterprise Agent for MSSQL v1.3.2 was released on 20th February 2015.**

## Change Log

This release includes the following updates and bug fixes.

## Bug Fixes

- **External domains and querying admin group**

  Made changes to the "Check Group" button on objectives page. Previously, SQL agent was not able to access active directory domain groups/users if this button is pressed and SQL agent needs to access as per objective requirement. This issue can cause the inclusion/exclusion of un/wanted events during objective matching. The issue is fixed now and "Check Group" button now properly accesses and shows the active directory domain groups/users.

- **Snare Agent becomes non-responsive when restricting web access**

  *Restrict remote control of SNARE agent to certain hosts* option on "Remote Control Configuration" is properly handled now. Previously, if this option was selected then the GUI in the browser (I.e the Remote Control Interface) becomes non-responsive even for allowed IPs. This non-responsive GUI issue was more likely to happen once Snare receives GUI requests from non-allowed IP address. This issue is fixed now and as a result of this change GUI will only remain available to allowed IPs and the GUI requests from non-allowed IPs will be silently ignored.

  Note: This issue *was not* inhibiting the log data collection and sending to destination server(s).

# Snare Enterprise Agent for MSSQL v1.3.1

**Snare Enterprise Agent for MSSQL v1.3.1 was released on 4th February 2015.**

## Change Log

This release includes the following updates and bug fixes.

## Security Updates

- **Updated the OpenSSL library**

  Maintenance update for OpenSSL to patch to OpenSSL-1.0.1k that fixes some bugs including denial of service attack and memory leaks.

# Snare Enterprise Agent for MSSQL v1.3.0

**Snare Enterprise Agent for MSSQL v1.3.0 was released on 10th December 2014.**

## Change Log

This release includes the following updates and bug fixes.

## Security Updates

- **Updated the OpenSSL library**

  Maintenance update for OpenSSL to patch to Openssl-1.0.1j.

## Bug Fixes

- **SQL agent memory grows and network connection restarts**
  Corrected an issue where the agent can frequently fail to send log messages using TCP/UDP connection when there is a high load in sending log messages. This can also manifest when there is not enough bandwidth available for the agent to send the logs. Normally this will be a temporary situation that resolves itself as soon as agent gets sufficient bandwidth. In Some situations this connection issue was treated as connection failure, causing agent to close the UDP/TCP connection and then retry after 30 seconds. Subsequently, it could cause the internal cache of the agent to grow rapidly in busy environment.

  The agent now detects if it is a temporarily failure then agent retries to send the log messages in next cycle without closing the UDP/TCP connection.

- Also fixed a memory and handlers leak issues with while loading objectives. The memory issue could be more noticeable if agent needed to enumerate a large number of domain users. In previous versions, this can cause agent to frequently hit the 'Memory Usage Limit' and force a restarting the service.

# Snare Enterprise Agent for MSSQL v1.2.9

**Snare Enterprise Agent for MSSQL v1.2.9 was released on 14th October 2014.**

## Change Log

This release includes the following updates and bug fixes.

## Security Updates

- **Updated the OpenSSL library**

  Updated the OpenSSL library to latest version 1.0.1i due to the following reported CVE's on OpenSSL:

  - Crash with SRP ciphersuite in Server Hello message (CVE-2014-5139)
  - Race condition in ssl_parse_serverhello_tlsext (CVE-2014-3509)
  - Double Free when processing DTLS packets (CVE-2014-3505)
  - DTLS memory exhaustion (CVE-2014-3506)
  - DTLS memory leak from zero-length fragments (CVE-2014-3507)
  - OpenSSL DTLS anonymous EC(DH) denial of service (CVE-2014-3510)
  - OpenSSL TLS protocol downgrade attack (CVE-2014-3511)
  - SRP buffer overrun (CVE-2014-3512)

  Refer to the following link full details on the patches https://www.openssl.org/news/secadv_20140806.txt

## Bug Fixes

- **Memory leak for Agents on Windows 2003**
  A memory leak was reported and identified in the Windows 2003 32 bit and 64 bit Snare agents. The issue may manifest with the agent using more than 20MB of memory and in some cases over 400MB. The issue appears to only manifest if the SSL or TCP was in use and the destination server was not very responsive either due to server load or network congestion. The Windows 2008 and later versions were also updated with a related memory leak however no customers had reported this particular issue. As the MSSQL Agent agent uses the same code it was updated to include the same patch. If a customer has seen unusual memory usage then they should upgrade to the latest MSSQL agent.

- **Deadlock potential if agent and destination server using TLS**
  If the agent and destination server were configured to use TLS there was a potential for a deadlock to occur with the sending of events if the receiving server was slow or there was network congestion resulting in both ends of the SSL session waiting on a response. The agent has been updated to time-out the session after 10 seconds and re-establish a new connection if does not get a response from the servers TLS connection. This could affect all previous MSSQL agents using SSL/TLS.

# Snare Enterprise Agent for MSSQL v1.2.8

**Snare Enterprise Agent for MSSQL v1.2.8 was released on 29th August 2014.**

## Change Log

This release includes the following bug fixes and improvements.

## Bug Fixes

- **Check Group issues for standalone mode**

  On the Objective page, the functionality behind the "Check Groups" button has been changed for MSSQL agents running in standalone mode. It will display all database/Active Directory (AD) users/groups that are associated with the specific objective. Previously, the MSSQL agent was showing database/AD users/groups only in cluster mode and when database instance name is not MSSQLSERVER.

- **Check Group option does not work for another domain**

  On the Objective page, the functionality behind the "Check Groups" button has been changed to show an error message on the page when the MSSQL agent cannot communicate to another domain. As a result of this change, if there is an Active Directory (AD) group on another domain ( ie a one way trust is in place) and the MSSQL agent cannot access that domain (due to permission restrictions or network problems etc.) then it will show the error message when the "Check Groups" button is pressed. Previously, the MSSQL agent was silently ignoring that domain without showing any error message to the user and the filter may not have been applied correctly which would result in more events being produced than desired.

  For example,a filter of the following structure was used:

  - `{sysadmin:^svc_*}` - this would be to exclude all service accounts from the audit logs starting with svc_.
  - The group details of the sysadmin role in SQL Server contained the following users and a one way trust is in place from the altdom domain to the mydomain, I.e. the altdom domain does not trust the mydomain but the mydomain trusts the altdom domain.
    - sa
    - svc_sqlserver
    - mydomain\adminsqlgroup
    - altdom\adminsqlgroup

  In this case the altdom domain is not queryable from the MSSQL Agent and will fail to determine the contents of the altdom\adminsqlgroup. This was resulting in the filter not being applied correctly to any users of the sysadmin role. This has been corrected so the filter will be applied to all enumerated user accounts and an error displayed for any group that can not be enumerated. If your environment has accounts from other untrusted domains and you wish filtering to be applied to include or exclude them, then the accounts from the other domain will have to be explicitly defined in the local sysadmin sql role so the agent can detect them and filtering can be applied correctly.

## Enhancements

- **Improved -x command output in cluster mode**

  The functionality of -x switch (used to generate the Snare configuration file (.inf) with current configurations) has been updated to support cluster mode of the MSSQL agent. As a result of this change, the MSSQL

agent is now able to generate the .inf file (extracting the current configurations) with -x switch when running in cluster mode as well as standalone mode.

For example to export the configuration file, from your c:/program files/SnareMSSQL execute:

```
>snaremssql -x template.inf
```

- **Enhanced debug messages**

  When running the agent in debug mode from the command line the message output has been enhanced. To run debug mode, from your c:/program files/SnareMSSQL execute (snare service must be stopped first):

  ```
  >snaremssql -c -d9
  ```

  After each iteration when the MSSQL agent grabs new log messages, it now prints out the following to the console:

  - the number of database connections checked
  - number of raw messages grabbed
  - number of raw messages that did not match the objectives
  - remaining number of messages added to send cache to be sent to destination(s).

  Example:

  ```
  Checked 2 DB connections, Messages count (Raw Grab) 75, Messages count (After objectives match) 34, Messages count (Ignored by objects count (Added to send cache) 34
  ```

  This helps to diagnose if there is a problem with the objective settings with the match criteria.

# Snare Enterprise Agent for MSSQL v1.2.7

**Snare Enterprise Agent for MSSQL v1.2.7 was released on 24th June 2014.**

## Change Log

This release includes the following bug fixes.

## Bug Fixes

- **Registry handle leak**

  Fix the registry handle leak issue that was causing the increasing number of registry handles. In the severe case, this issue could cause the frequent restart of the SnareMSSQL service.

- **Man-in-the-middle attack in OpenSSL pre v1.0.1h**
  An attacker can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server. The attack can only be performed between a vulnerable Snare MSSQL Agent (pre v1.2.7) and a vulnerable third party log collector. This Snare MSSQL Agent is not vulnerable to this attack if pre v1.2.7 MSSQL Agent is communicating with the Snare Server, and can only happen if logs are sent to a server that is also vulnerable. MSSQL Agent v1.2.7 is built using OpenSSL v1.0.1h that fixes this issue on the Snare MSSQL Agent side. Customers are also encouraged to update their log collectors to OpenSSL v1.0.1h so that vulnerability can be removed from both sides.

# Snare Enterprise Agent for MSSQL v1.2.6

**Snare Enterprise Agent for MSSQL v1.2.6 was released on 23rd May 2014.**

## Change Log

This release includes following bug fix.

## Bug Fixes

- **SQL 2012 and INF installation**

  An issue was found for stand alone and the cluster based installation using .inf file for SQL 2012 servers. The issue caused the no objectives to be installed from the supplied .inf file during silent or manual install. The other parameters of the .inf file were unaffected. If the objectives were encrypted in the .inf file they were not being replicated across the clustered SQL instances during installation. This issue was present in all previous versions of the agent.

- **Dropping events.**

  Fixed the issue where the agent starts dropping TLS connections when there are high volumes of data. This issue specifically affects busy machines where the agent needs to send high volumes of log data. In some circumstances the agent may experience a frequent drop of the TLS connections to the SIEM server which can have a secondary affect and cause the agent cache to quickly reach capacity. In the worst case scenario the agent can start dropping events.

***NOTE: Snare Enterprise Agent for MSSQL v1.2.5 was released unofficially.***

## Snare Enterprise Agent for MSSQL v1.2.4

**Snare Enterprise Agent for MSSQL v1.2.4 was released on 16th May 2014.**

### Change Log

This release includes following bug fixes.

### Bug Fixes

- After the implementation of Group Policy from Snare Enterprise Agent for MSSQL v1.2, the installation setup wizard updates the existing objectives and persistent objectives to start from 1 instead of 0 as set in the registry. This version fixes the bug where the persistent objectives were not properly updated during the installation and Snare Enterprise Agent for MSSQL becomes unable to load persistent objectives.
- For SQL Server 2012 installations, Microsoft added a new namespace root. Due to this change prior versions of Snare Enterprise Agent for MSSQL are not able to identify the instances correctly for SQL Server 2012 during a custom install using pre-defined objectives via the .inf file (the setup information file). This update correctly installs the objectives as defined in the .inf file for each SQL instance on the server.

# Snare Enterprise Agent for MSSQL v1.2.3

**Snare Enterprise Agent for MSSQL v1.2.3 was released on 15th April 2014.**

## Change Log

This release includes following bug fixes.

## Bug Fixes

- **Network resource leak.**

  An issue has been identified where the Snare Windows agents may grow in its usage of UDP ports on the host. The issue appears to be a timing one and related to the destination server not being reliable in some fashion. A network error had to be triggered along with an internal recheck of the agents configuration within a short time period to manifest in this way. The issue would only appear in some circumstances of load and network issues. The symptom would manifest as in growing number of sockets while it retried the destination connection and would result in the UDP sockets in most cases (and much lower chance of TCP port due to the TCP handshake) to grow. The issue could be caused by high latency/over a VPN, a bad link, a firewall packet issue, traffic shaping devices or the server having physical issues. Any of these options could trigger this behaviour. This issue seems to have mostly affected busy Domain Controllers and other high activity systems and has been seen on Windows 2003, 2008 and Windows 7 systems for the Snare for Windows agent. If any of these symptoms are present then it is important that customers upgrade to prevent a possible outage or downtime of the system. This issue has only affected the Windows Agent to date however the SQL agent uses part of the same code base and could be affected. The versions that could be affected are 1.2.0, 1.2.1,1.2.2; version 1.2.3 resolves this issue.

- **OpenSSL library update**

  The OpenSSL library version used by the agents has been updated to 1.0.1g due to the recent Heartbleed vulnerability discovery. The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. Client implementations using vulnerable versions (such as the agents) are exposed to minimal risk and have shown no signs of being vulnerable with testing. The SSL communications the agent uses to the server can not be hijacked to inject the Heartbleed payload and the our Micro web server interface is not vulnerable. However IA believes keeping our software up to the recommended patch levels very important so we have patched the software. This issue has only affected the Snare MSSQL Agent versions 1.1.0, 1.2.0, 1.2.1 and 1.2.2 where the SSL capabilities were added; version 1.2.3 resolves this issue.

# Snare Enterprise Agent for MSSQL v1.2.2

**Snare Enterprise Agent for MSSQL v1.2.2 was released on 3rd April 2014.**

## Change Log

### New Features

- **Evaluation license version of agent**

A hard coded expiry time has been added to the evaluation agents to allow customers to trial the enter feature set. Agents running after this time will not emit any events to its configured server(s), however they still may be viewed in the GUI (the Latest Events window).

An evaluation agent will expire after one month. The expiry date is displayed on the main screen of the GUI, in addition to the days remaining.


*Note: This does not affect the full Snare Enterprise Agents, provided to customers.*

## Bug Fixes

- Fix install problem when existing binary is locked by operating system and unable to be overwritten with new version.

## Snare for MS SQL v1.2.1

**Snare Epilog for Windows v1.2.1 was released on 6th March 2014.**

### Bug Fixes

- There was an issue (specifically noted when agent's GUI is running in Internet Explorer 10) that the GUI takes longer than usual to load, and may sometimes become non-responsive.

# Snare for MS SQL v1.2.0

**Snare for MS SQL v1.2 was released on 3rd February 2014.**

## Change Log

### New Features

- **Apply Agent Settings through Group Policy**

In a large network environment, having large number of Snare agents with no Snare Agent Management Console(AMC) can sometimes be a difficult task to maintain and apply new settings on all agents.

This release makes the task of applying new settings much easier with sites that with to use group policy. Now network domain administrators can update the settings of Snare Enterprise Agent for MSSQL through Microsoft ® Group Policy Editor. The updated settings will be applied to Snare Enterprise Agent for MSSQL based upon Group Policy update preferences. Moreover, Snare Enterprise Agent for MSSQL supports two levels of group policies, i.e. Super Group Policy and Snare Agent Group Policy.

Super group policy is useful when different types of Snare agents (Snare Epilog, Snare for Windows and Snare Enterprise Agent for MSSQL) are running on a network. Using super group policy, network domain administrators can update the settings of all types of Snare agents running on a network using Microsoft ® Group Policy Editor. For example, network domain administrators can use Microsoft ® Group Policy Editor to update all types of Snare agents on network to send the log to a Snare Server running at 10.1.1.1 on TCP port 6161. Once this super group policy is applied, all Snare agents will now send logs to the Snare Server running at 10.1.1.1 on TCP port 6161. This release comes with Super Group Policy Administrative Template (ADM) (available upon request) that network domain administrators can use to update all major settings of all types of Snare agents running on the network. Figure 1 shows the updating of destination log servers using super group policy administrative template.

Snare Enterprise Agent for MSSQL group policy is useful when there is a need to update the settings of all Snare Enterprise Agent for MSSQL agents running in a network. Unlike, super group policy, Snare Enterprise Agent for MSSQL group policy only updates the settings of all Snare Enterprise Agent for MSSQL agents. For example, network domain administrators can use Microsoft ® Group Policy Editor to update all Snare Enterprise Agent for MSSQL agents on network to send the log to a Snare Server running at 10.1.1.1 on TCP port 6161. Once this Snare Enterprise Agent for MSSQL group policy is applied, all Snare Enterprise Agent for MSSQL agents will send logs to the Snare Server running at 10.1.1.1 on TCP port 6161. Snare Enterprise Agent for MSSQL also comes with Snare Enterprise Agent for MSSQL Group Policy Administrative Template (ADM) (available upon request) that network domain administrators can use to update all settings of all Snare Enterprise Agent for MSSQL agents running on the network. Figure 1 also shows the updating of destination log servers using Snare Enterprise Agent for MSSQL group policy administrative template.

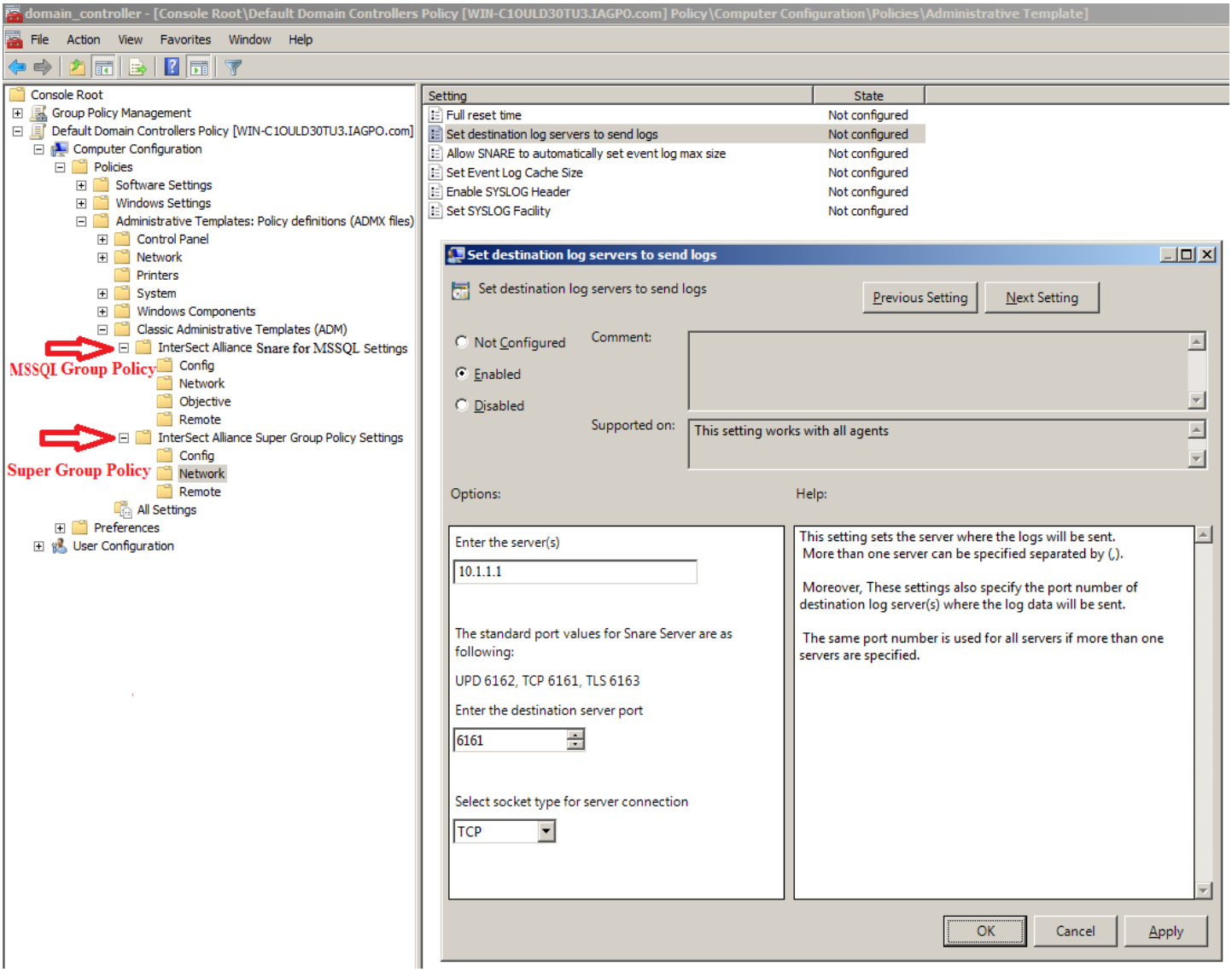


**Figure 1: Update Snare Agents Network Settings through Agent Group Policy and Super Group Policy**

- **Enhanced Event Throttling**

Snare Enterprise Agent for MSSQL includes enhanced event throttling capabilities. It includes three useful settings in this regard, as shown in Figure 2.

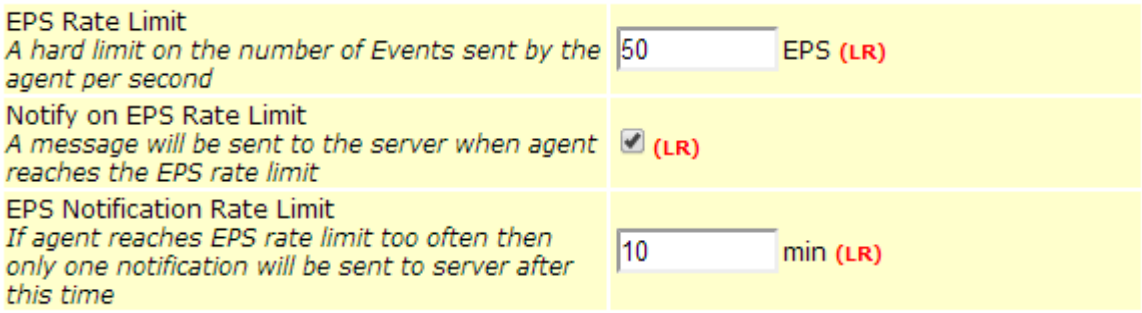


**Figure 2: EPS Event Throttling Setting**

The *EPS Rate Limit* is a hard limit on the number of events sent by the agent per second to any destination server. For example, if EPS rate limit is set to 50 (as it is in Figure 2) then Snare Enterprise Agent for MSSQL will only send maximum 50 log messages in a second to any destination server. This EPS rate limit applies only to sending the events not capturing the events. The EPS rate limit settings are to help to reduce the load on slow network links or to reduce the impact on the destination servers during unexpected high event rates. For example, if a destination server goes down due to any expected reason then all Snare Enterprise Agent for MSSQL agents running on the network build the cache of log messages (assuming TCP has been configured) and as soon as destination server becomes available, all Snare Enterprise Agent for MSSQL agents will send log messages from their caches at a rate not faster than the EPS rate limit.

If *Notify on EPS Rate Limit* option is selected then a message will be sent to the destination server(s) whenever Snare Enterprise Agent for MSSQL reaches the EPS rate limit. The message also include the EPS rate limit value. The frequency of EPS rate limit notifications can be controlled through 'EPS Notification Rate Limit' setting. For example, if EPS notification rate limit is set to 10 minutes then only one EPS notification message will be sent every 10 minutes to the destination server(s) regardless of how many times Snare Enterprise Agent for MSSQL reaches the EPS rate limit.

## Bug Fixes

- Resolved the issue with 'server status' on current events page that prevented server status information being displayed in some cases.