System iNtrusion Analysis & Reporting Environment

# Release Notes for Snare Enterprise Agent for Windows v4.2

## About this document

This document provides release notes for the Snare Enterprise Agent for Windows release.

# Snare Enterprise Agent for Windows v4.2.10

**Snare Enterprise Agent for Windows v4.2.10 was released on 20th February 2015.**

## Change Log

This release includes the following updates and bug fixes.

## Bug Fixes

- **Match function ignores "," for input of multiple values in source search term and user search term**

  Fixed the issue with objective where comma separated values for "Source Search Term" were not treated separately. Due to this issue, Snare was not able to distinguish between the single and multiple input values for the "Source Search Term" field of an objective. Therefore Custom Event Logs were affected. After the fix, Snare is able to distinguish between single and multiple input values for "Source Search Term".

- **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 Windows v4.2.9

**Snare Enterprise Agent for Windows v4.2.9 was released on 4th February 2015.**

## Change Log

This release includes the following updates and bug fixes.

## Security Upates

- **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 Windows v4.2.8

**Snare Enterprise Agent for Windows v4.2.8 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

- **UDP connection goes offline and agent send cache starts growing**
  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 it self 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.

# Snare Enterprise Agent for Windows v4.2.7

**Snare Enterprise Agent for Windows v4.2.7 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 32 bit and 64 bit Snare agents on Windows 2003. 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. If a customer has seen unusual memory usage then they should upgrade to the latest Windows 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 Windows agents using SSL/TLS.

# Snare Enterprise Agent for Windows v4.2.6

**Snare Enterprise Agent for Windows v4.2.6 was released on 21st August 2014.**

## Change Log

This release includes following bug fix.

## Bug Fixes

- **Regular expression (RegEx) matching memory fix**

  If regular expression matching option is selected for objective(s) then in Snare Enterprise Agents prior to v4.2.6, it can cause an internal application crash every 10 minutes. It may log an application crash error in the Windows application log and a restart of the Snare service every 10 minutes. The issue was related to mishandling of the memory associated with the regular expression.

# Snare Enterprise Agent for Windows v4.2.5

**Snare Enterprise Agent for Windows v4.2.5 was released on 26th June 2014.**

## Change Log

This release includes following bug fixes.

## Bug Fixes

- **Registry handle leak**

  Fix the registry handle leak issue that was causing the increasing number of registry handles. In severe cases, this issue could cause the frequent restart of the Snare 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 Windows Agent (pre v4.2.5) and a vulnerable third party log collector using TLS. This Snare Windows agent is not vulnerable to this attack if a pre v4.2.5 Snare is communicating with a Snare Server. Snare v4.2.5 is built using OpenSSL v1.0.1h that fixes this issue on Snare Windows 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.

- **Objective exclude filter bug**

  Objectives allow events to be included or excluded depending on various matching criteria. A bug in previous versions resulted in the exclude option only taking full effect when applied to the 'Event ID' match objective. All other exclude options were ignored if a wild card match objective was performed after the excluded match objective. This fix ensures the exclude option works correctly on the whole event including "event id", "general match", "user name" and "event source" fields, so that a wild card match objective after the exclude objective does not permit the excluded data.

# Snare Enterprise Agent for Windows v4.2.4

**Snare Enterprise Agent for Windows v4.2.4 was released on 23rd May 2014.**

## Change Log

This release includes following bug fix.

## Bug Fixes

- **Caching of logs may be lost after the destination server is made available after an outage**

  An issue has been identified and fixed where the agent was unable to bookmark current event logs in the registry if 'Status' registry key does not exist. This could effect caching operation of the agent where TCP or TLS is in use and result in cached events not being sent to the server where the server has had an outage or interruption. If caching TCP or TLS is in use then it is important to apply this patch update as soon as possible. This issue effected versions 4.2.0 to 4.2.3. If the installation was an upgrade from a previous install then this issue may not have affected your installation. To validate if this issue is present on your system then use regedit to check the existence of the registry key path for HKEY_LOCAL_MACHINE | SOFTWARE | InterSect Alliance | AuditService |Status. For customers using UDP protocol for sending to the SIEM server, you are unaffected by this issue as there is no caching.

- **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.

# Snare Enterprise Agent for Windows v4.2.3

**Snare Enterprise Agent for Windows v4.2.3 was released on 15th April 2014.**

## Change Log

This release includes following bug fix.

## 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 connectivity 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 Snare Enterprise Agent for Windows. Any network based operation on the host may be affected along with the servers operation. 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 versions 4.1.3, 4.1.4, 4.2.0, 4.2.1 and 4.2.2; version 4.2.3 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 our Micro web server interface is not vulnerable. However IA believes keeping our software up to the recommended patch levels is very important so we have patched the software. This issue has only affected the Windows Agent versions 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.2.0, 4.2.1 and 4.2.2 where the SSL capabilities were added; version 4.2.3 resolves this issue.

# Snare Enterprise Agent for Windows v4.2.2

**Snare Enterprise Agent for Windows v4.2.2 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 agents to allow customers to test their 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 truncate list delimiter being exported to server as a CRLF instead of a tab.
- Fix truncate list and rate limit parameters write to registry
- Fix truncate list import from .INF file bug.
- Update MSI build procedure to be compatible with Windows 2012 R2, 32 and 64 bit architectures
- Fix install problem when existing binary is locked by operating system and unable to be overwritten with new version.

# Snare Enterprise Agent for Windows v4.2.1

**Snare Epilog for Windows v4.2.1 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 Enterprise Agent for Windows v4.2.0

**Snare Windows Agent v4.2 was released on 3rd February 2014.**

## Change Log

### New Features

Please note that the following new features are available for Snare Enterprise Agent for Windows only.

- **Regular expression for general match support**

By default, Snare matches the value in an event using a basic wild-card search (i.e. using '?' for single characters, and '*' for multiple). The General Match search term in an objective may now be set to interpret the string as a Perl Compatible Regular Expression. This allows for a much more detailed and flexible search criteria to be configured.
Some common useful regular expressions include:

Event contains email address:
```
([a-z0-9_\.-]+)@([\da-z\.-]+)\.([a-z\.]{2,6})
```

Event contains URL:
```
(https?:\/\/)?([\da-z\.-]+)\.([a-z\.]{2,6})([\/\w \.-]*)*\/?
```

Event contains IP address:
```
(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)
```

Event contains hex-numbers:
```
#?([a-f0-9]{6}|[a-f0-9]{3})
```

This can be embellished with more specific matching to capture error numbers in tightly specific ranges.

This feature allows highly targeted objectives allowing sophisticated forensic analysis and reporting, particularly when small details get lost in noisy log environments.

- **Truncation of verbose event support**

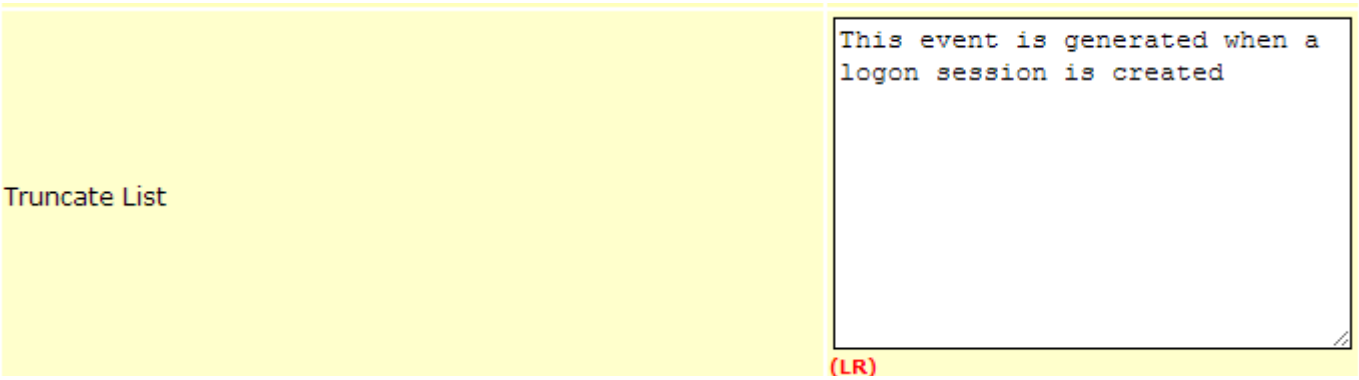
Some events generated by Windows can be triggered with a high frequency and contain verbose information of repeated text which may not be of much interest to the audit subsystem. To reduce the load on the target servers, these events may be truncated at a specific point in the string text. This means the event is not discarded from an audit point of view, but reduces the amount of unnecessary message data across the network.

An example of this is the Windows Logon event 4624. This occurs very regularly on a busy domain controller. Each of these messages contains a large event description which is repeated regularly (this example comes from an rsyslog logfile):

```
Feb  3 13:29:41 win08r2entx64.Snare.ia#011MSWinEventLog#0111#011Security#01162959#011Mon Feb 03
13:29:31                                          2014#0114624#011Microsoft-Windows-Security-
Auditing#011SNARE\WIN08R2ENTX64$#011N/A#011Success
Audit#011win08r2entx64.Snare.ia#011Logon#011#011An   account   was   successfully   logged   on.
```

```
Subject:  Security ID:  S-1-0-0  Account Name:  -  Account Domain:  -  Logon ID:  0x0
Logon Type:  3  New Logon:  Security ID:  S-1-5-18  Account Name:  WIN08R2ENTX64$  Account
Domain:  SNARE  Logon ID:  0x403524c  Logon GUID:  {3D6A4CB3-AC1B-D5DD-363A-447C40BEBEB7}
Process Information:  Process ID:  0x0  Process Name:  -  Network Information:  Workstation
Name:  Source Network Address:  ::1  Source Port:  63984  Detailed Authentication
Information:  Logon Process:  Kerberos  Authentication Package: Kerberos  Transited Services:
-  Package Name (NTLM only): -  Key Length:  0  This event is generated when a logon session
is created. It is generated on the computer that was accessed.  The subject fields indicate
the account on the local system which requested the logon. This is most commonly a service such
as the Server service, or a local process such as Winlogon.exe or Services.exe.  The logon
type field indicates the kind of logon that occurred. The most common types are 2 (interactive)
and 3 (network).  The New Logon fields indicate the account for whom the new logon was
created, i.e. the account that was logged on.  The network fields indicate where a remote
logon request originated. Workstation name is not always available and may be left blank in some
cases.  The authentication information fields provide detailed information about this specific
logon request.  - Logon GUID is a unique identifier that can be used to correlate this event
with a KDC event.  - Transited services indicate which intermediate services have participated
in this logon request.  - Package name indicates which sub-protocol was used among the NTLM
protocols.  - Key length indicates the length of the generated session key.
```

As can be seen, this is a large amount of redundant information being stored in the audit server. By adding an entry to the “Truncate List” configuration as follows:




results in the same log truncated from where the configured text “This event is generated when a logon session is created” begins. This event will now appear in the audit server as:

```
Feb  3 13:38:09 win08r2entx64.Snare.ia#011MSWinEventLog#0111#011Security#01163011#011Mon Feb 03
13:37:50 2014#0114624#011Microsoft-Windows-Security-
Auditing#011SNARE\WIN08R2ENTX64$#011N/A#011Success
Audit#011win08r2entx64.Snare.ia#011Logon#011#011An account was successfully logged on.
Subject:  Security ID:  S-1-0-0  Account Name:  -  Account Domain:  -  Logon ID:  0x0
Logon Type:  3  New Logon:  Security ID:  S-1-5-18  Account Name:  WIN08R2ENTX64$  Account
Domain:  SNARE  Logon ID:  0x404e49f  Logon GUID:  {3D6A4CB3-AC1B-D5DD-363A-447C40BEBEB7}
Process Information:  Process ID:  0x0  Process Name:  -  Network Information:  Workstation
Name:  Source Network Address: ::1  Source Port:  64139  Detailed Authentication
Information:  Logon Process:  Kerberos  Authentication Package: Kerberos  Transited Services:
-  Package Name (NTLM only): -  Key Length:  0  <truncated 2524 bytes>#01131391
```

Note the event now logs the number of bytes removed from the event entry. This feature can save substantial server resources including storage and cost where licenses charge per megabyte are in effect.

- **USB event support enhanced on Windows 08 platforms**

Tracking USB device connection/disconnection is difficult using only the Windows event log. Depending on the device in question, the events generated when activate varies widely in their number and amount of detail. A second mechanism has been implemented to complement the event logs. This registers the agent directly with the operating system so to be notified on the arrival and detach events for all USB devices. As

some of these events are outside the Event Log system, they are flagged as “Snare Generated” in the resulting event message string. USB auditing is supported on Windows XP, 2003,2008 and 2012.

- **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.

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

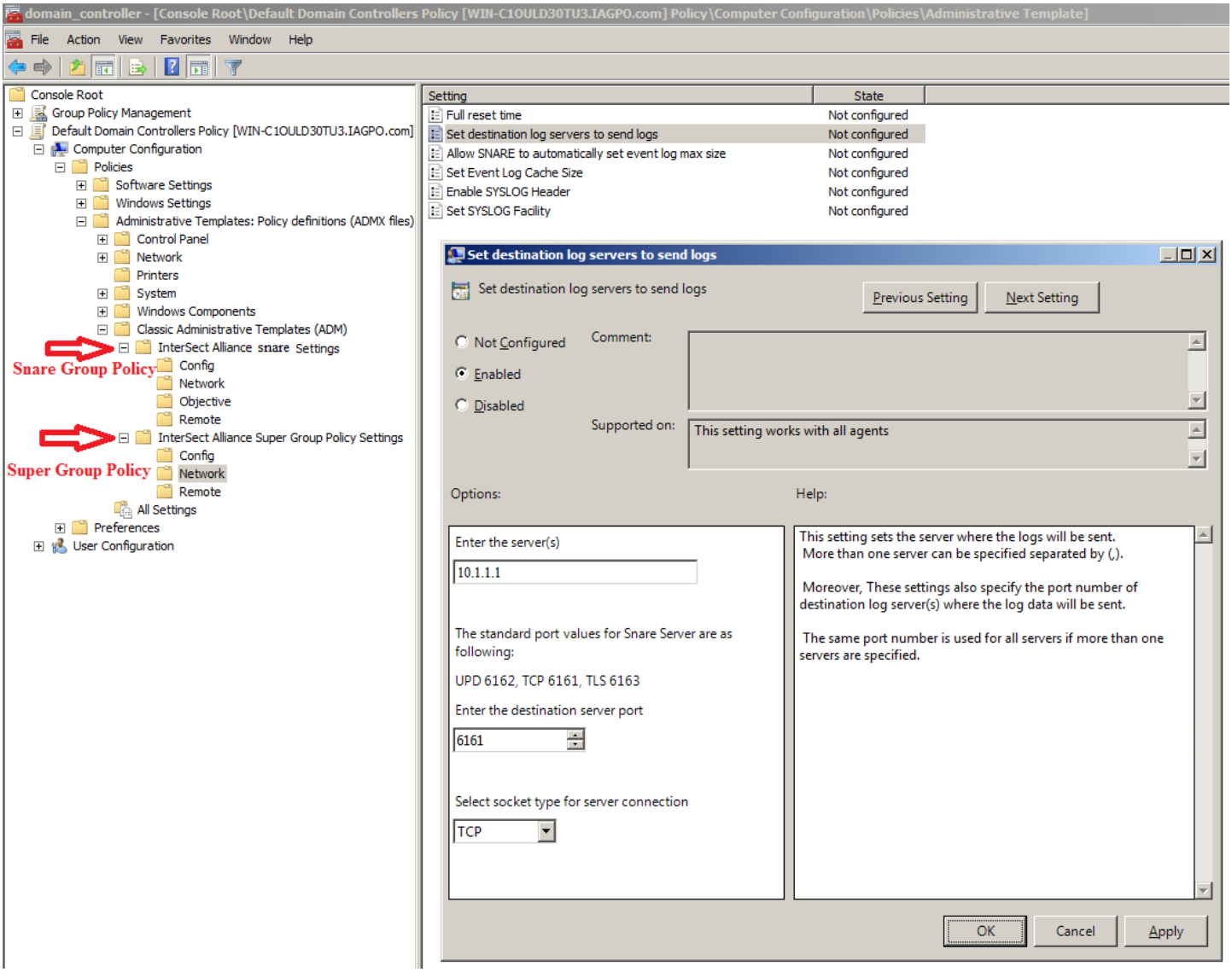



**Figure 1: Update Snare Agents Network Settings through Agent Group Policy and Super Group Policy**

- **Enhanced Event Throttling**

Snare Enterprise Agent for Windows v4.2 also comes with enhanced event throttling capabilities. It includes three useful settings in this regard, as shown in Figure 2.

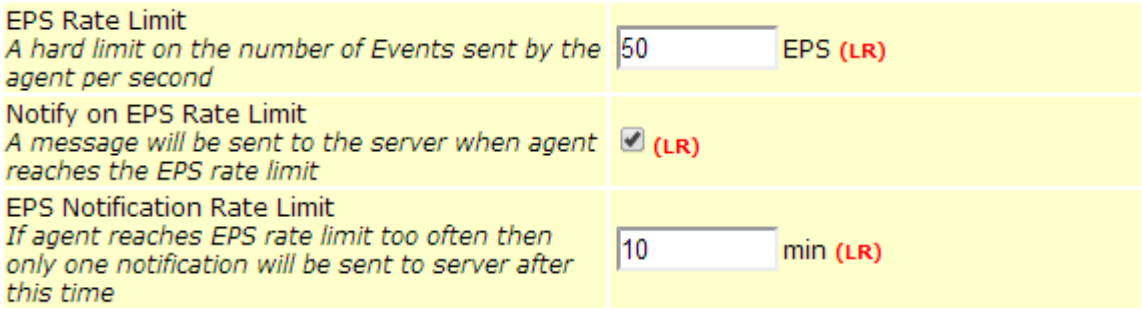



**Figure 2: EPS Event Throttling Setting**

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 Windows 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 for system maintenance or due to an unexpected reason then all Snare Enterprise Agent for Windows agents running on the network build the cache of log messages (assuming that TCP has been configured) and as soon as destination server becomes available, all Snare Enterprise Agent for Windows will send log messages from their caches at a rate no 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 Windows 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 Windows 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.

**Note:** All ***Snare Servers*** communicating with this agent release should be updated to the patch version **6.2.2** so the **Agent Management Console (AMC)** can take advantage of the new features described here.