System iNtrusion Analysis & Reporting Environment

Release Notes for Epilog for Windows v1.7/v1.8

About this document

This document provides release notes for Snare Enterprise Epilog for Windows release v1.7 and 1.8.

Snare Enterprise Epilog for Windows v1.8.4

Snare Enterprise Epilog for Windows v1.8.4 was released on 19th February 2016.

Bug Fixes

Loading configuration file via Epilog installer does not load all details

- There was an issue with importing configuration files via the command line options, such as in silent and automated installations. The Log Configurations and the EPS Rate Limit were not updated correctly on the agent or in the registry. This is now fixed in this release.

Security Updates

- **Updated the OpenSSL library**

  Maintenance update for OpenSSL to patch to OpenSSL-1.0.1r.

Snare Enterprise Epilog for Windows v1.8.3

Snare Enterprise Epilog for Windows v1.8.3 was released on 21st October 2015.

Bug Fixes

- **Epilog dropping log messages**

  Epilog may keep reading a log files if the status of the destination(s) was down while operating while using TCP or TLS. Due to this, log messages may be dropped if all destinations are down for extended period of time and internal cache becomes full. The internal cache mechanism has been corrected in this release. Epilog has implemented some additional checks to regularly checks the status of destination(s) and only reads from the monitored logs if at least one destination is able to receive log messages.

- **Epilog stops sending logs to Snare Server TLS connection**

  An issue was identified with the current open file handle of the monitored log file in particular the DNS debug log file. Due to this issue, in some cases, the other processes may be unable to get exclusive write lock to the log file and hence prevent the log file from being updated due to a read lock being present on a file.

  This issue is fixed in this release and now Epilog explicitly releases all file locks periodically to avoid any deadlock situation on file locks. This allows other applications to obtain their exclusive file write lock to update their log files and Epilog will resume processing the file once the other application frees its file lock.

Snare Enterprise Epilog for Windows v1.8.2

Snare Enterprise Epilog for Windows v1.8.2 was released on 4th September 2015.

Bug Fixes

- **Snare service does not keep login credentials used during installation**

  There was an issue with handling the existing service account settings of the agent during reinstallation of the agent. Due to this issue the setup was unable to transfer the updated login credentials to the service during installation. Moreover, this error was only logged in the install log file if setup was run with '/log' switch. The agent installer setup now properly handles the existing service account settings and updates the login credentials accordingly.

  Additionally, the setup will always create an install log regardless if the '/log' parameter is provided or not. The log file is generally less than 10 kilobytes so wont consume much disk space If the '/log' parameter is provided then a log file will be generated using the supplied name and path provided in the '/log' parameter. Otherwise the log file will be created using the agent name and be located from the where the installer is run from. If an error occurs during the installation then an error message will be displayed in the UI at the end of the installation. This error message is 'suppressible' from the UI via the '/SuppressMsgBoxes' option if provided during command line installation.

- **Error reading Logs from Log0 instead of Log1 after GPO**

  The agent had an issue with reading the logs parameter from the Agent Group Policy registry settings only the local registry settings was working correctly. As the Epilog agent was not able to read or process this GPO setting correctly it would not allow the ADM templates to be used to configure all of the log file monitoring settings pushed out by GPO correctly. This issue is now fixed so that Epilog correctly reads the logs GPO settings for both Agent Group Policy (AGP) and local registry.

- **Epilog not working with multi line event using separator**
  The agent was updated to allow a multi-line separator to match on text at the beginning of a log entry using a carrot (^) prefix. This update extends the existing matching for multiple line records which are based on matching a string of characters on a separate line.

- **Need to ignore directories when listing all matching files**
  An issue in the Log Configuration settings and the way Epilog treated the special directory structure during a directory search. This issue would manifest as matching the dot or dot dot directories (for example representing current directory and root directory) may be shown as regular files. This would only cause an issue when the monitoring matching was set to the First Matching files when the *Log Format Name* was set to generic wildcard, such as * or *.* but would not be an issue when matching a specific file type log like *.log. As such this did not affect files where the *Log Format Name* included the file extension of the file to watch.

Snare Enterprise Epilog for Windows v1.8.1

Snare Enterprise Epilog for Windows v1.8.1 was released on 31st July 2015.

Enhancements

- **Add CLI feature to add remote access restriction**

  Added the feature /REMOTELOCAL=[0|1] to the installer command line parameter set to allow the specification of local host only connections to the agent web GUI.

Security Updates

- **Updated the OpenSSL library**

  Maintenance update for OpenSSL to patch to OpenSSL-1.0.1p.

Bug Fixes

- **Web pages start taking too much time to load (spinning issue)**

  Due to an issue in the handling of web GUI requests the web GUI pages can hang or be very slow. This issue is fixed in this release and now web GUI interaction should be responsive as expected.

- **The wildcard includes are matching everything in Objective Configuration**

  An issue with objectives would occur if there was no match with the objective(s) but treated as match, causing Epilog to send unnecessary data to server. Now a wildcard (* for all) or (? per character) match data as intended when including matched events only. This issue did not affect the events excluded set in the objective configuration.

Snare Enterprise Epilog for Windows v1.8.0

Snare Enterprise Epilog for Windows v1.8.0 was released on 30th June 2015.

New Features

- **New HostIP features and checkbox on the Network Configuration screen.**

  Enabling this setting will cause the agent to use the first network adaptor as listed in the network configuration as the source of the events. The agent will periodically (about ten minutes) check this setting and pick up any changes that occur via a manual change of IP or DHCP reassignment. The value of the IP address will be displayed in the "Override detected DNS Name with" field once selected. If the host does not have a valid IP address, i.e. DHCP has not been responded to, then the syslog message will default to the system's hostname which is the default setting for the agent.

  The Installation Wizard on the network configuration screen now allows the setting of HostIP and the entry of the destination IP, Port and protocol settings.

- **The silent installer can accept new command line parameters**

  The following options are available from the silent installer:
  /HOSTIP=0|1 to turn on the address resolution feature
  /DESTINATION=<ip address> to add a destination address
  /DESTPORT=<port number> to specify a destination port
  /PROTOCOL=<0|1|2> for the socket protocols udp, tcp and ssl respectively
  /REMOTEALLOW=0|1 to allow web access
  /ACCESSKEY=<password> to set a web password from the command line install.

Enhancements

GPO Settings and ADM templates

- Updated ADM Templates to support new UseHostIP Option. See Secure Area for updated templates.

Bug Fixes

- **Escalating Memory for all matching file settings when many files**
  Fix a potential memory issue where there is a large number of files in a directory and the option 'all matching files' is selected.

- **Send comments not working**
  Issue with Epilog and the Log Configuration option 'Send Comments'. This option was ignored in all cases, causing Epilog to ignore any text starting with '#'. This issue is fixed in this release and now Epilog properly treats this option and sends or does not send comments as per the options selected for each log.

Security Fix

- **Denial of Service to Web interface on Agents**
  Security Denial of Service vulnerability to correct malformed HTTP post exploit that can cause the agent to crash or hang.

Snare Enterprise Epilog for Windows v1.7.12

Snare Enterprise Epilog for Windows v1.7.12 was released on 21st May 2015.

Change Log

This release includes the following:

Bug Fix

- **Selecting All Matching Files when location had a high number of files uses high memory**

  Extensive memory consumption occurred on the Epilog agent when the Log Configuration was configured to monitor a high number of files with the All Matching Files option selected. This issue effected v1.7.10 and 1.7.11.

Snare Enterprise Epilog for Windows v1.7.10

Snare Enterprise Epilog for Windows v1.7.10 was released on 19th March 2015.

Change Log

This release includes the following:

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.

- **Multi-Line Format option not working correctly with the All Matching Files option**

  An issue was found with the handling of the internal log watcher of Epilog for post v1.7.5 of Snare Enterprise Epilog for Windows (Snare Log Configuration page on the Remote Control Interface). This issue causes Epilog to ignore Multi-Line Format input options when specified with different directory watch options. Furthermore, this issue could also cause Epilog to log events in a different format (i.e. log single line events when multi-line option is given). This issue is fixed in this release and now Epilog correctly handles all the combinations of single, fixed and multi-line options with all directory watch options.

- **Epilog 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 Epilog 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.

- **Exporting the epilog configuration to console does not work**

  There was an issue with -x command line switch not correctly sending output to the console e.g `epilog -x`. Due to this issue Epilog was unable to print current settings on console if -x switch was used without the input of output file name. This issue is fixed in this release and now Epilog can print the current settings on console if no output file name is specified along with -x.

Snare Enterprise Epilog for Windows v1.7.9

Snare Enterprise Epilog for Windows v1.7.9 was released on 20th February 2015.

Change Log

This release includes the following updates and bug fixes.

Bug Fixes

- **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 Epilog for Windows v1.7.8

Snare Enterprise Epilog for Windows v1.7.8 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 Epilog for Windows v1.7.7

Snare Enterprise Epilog for Windows v1.7.7 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 Epilog for Windows v1.7.6

Snare Enterprise Epilog for Windows v1.7.6 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

- **Log Handling**

  An issue was identified with Epilog not processing log files in certain cases when directory scanning was active. The Log handling has been updated to fix a potential problem where parts of a log file may not be processed correctly. The problem only occurred in version 1.7.5 where multiple log files were being monitored with a match all log objective rule using wild card matching.

- **Logging multiple files within a directory**

  Fixed the issue with logging multiple files within a directory. Previously Epilog was not correctly logging the changes in file size and consequently was not able to grab all the changes to the files of a directory.

- **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 Epilog 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 Windows Epilog 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 Epilog agents using SSL/TLS.

Snare Enterprise Epilog for Windows v1.7.5

Snare Enterprise Epilog for Windows v1.7.5 was released on 26th June 2014.

Change Log

This release includes the following feature enhancement and bug fixes.

New Feature

- **Log multiple files in a directory**

  Epilog v1.7.5 is able to log multiple files within a directory. By specifying a directory path, now Epilog will be able to log all, first or last file within a directory. User can specify a wild-card format specifier to filter the files. Using this feature, now users only need to create a single log monitor for all files within a directory; whereas all previous versions of Epilog were able to track only the last file within a directory.

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 Epilog 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 Epilog Agent (pre v1.7.5) and a vulnerable third party log collector using TLS. This Epilog Agent is not vulnerable to this attack if pre 1.7.5 Epilog is communicating with Snare Server and can only happen if logs are sent to a server that is also vulnerable. Epilog v1.7.5 is built using OpenSSL v1.0.1h that fixes this issue on the Epilog 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 Epilog for Windows v1.7.4

Snare Enterprise Epilog for Windows v1.7.4 was released on 23rd May 2014.

Change Log

This release includes the following bug fixes.

Bug Fixes

- **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 Epilog for Windows v1.7.3

Snare Enterprise Epilog for Windows v1.7.3 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. This issue has not been reported with the Epilog agent but as it shared the same code base as the Windows agent it could potentially occur. 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 versions 1.7.1 and 1.7.2; version 1.7.3 resolves this issue.

- **Memory leak.**

  The agent reloads its configuration on a regular basis. It was found that the monitored log file database was being reloaded each time causing a minor memory leak. This issue has been resolved in this release.

- **GUI formatting fix**

  A bug on set log page that was causing to display misplaced '>' character if Line separating event is terminated by '>'.

- **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 Snare Epilog versions 1.6.2, 1.7.0, 1.7.1 and 1.7.2 where the SSL capabilities were added; version 1.7.3 resolves this issue.

Snare Enterprise Epilog for Windows v1.7.2

Snare Enterprise Epilog for Windows v1.7.2 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 Snare Evaluation 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 install problem when existing binary is locked by operating system and unable to be overwritten with new version.

Snare Enterprise Epilog for Windows v1.7.1

Snare Enterprise Epilog for Windows v1.7.1 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 Epilog for Windows v1.7.0

Snare Enterprise Epilog for Windows v1.7 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 wish to use group policy. Now network domain administrators can update the settings of epilog through Microsoft ® Group Policy Editor. The updated settings will be applied to Epilog based upon Group Policy update preferences. Moreover, Epilog 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 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 logs 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 be updated to send their logs to the Snare Server running at 10.1.1.1 on TCP port 6161. This release comes with a Super Group Policy Administrative Template (ADM) (available on 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.

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

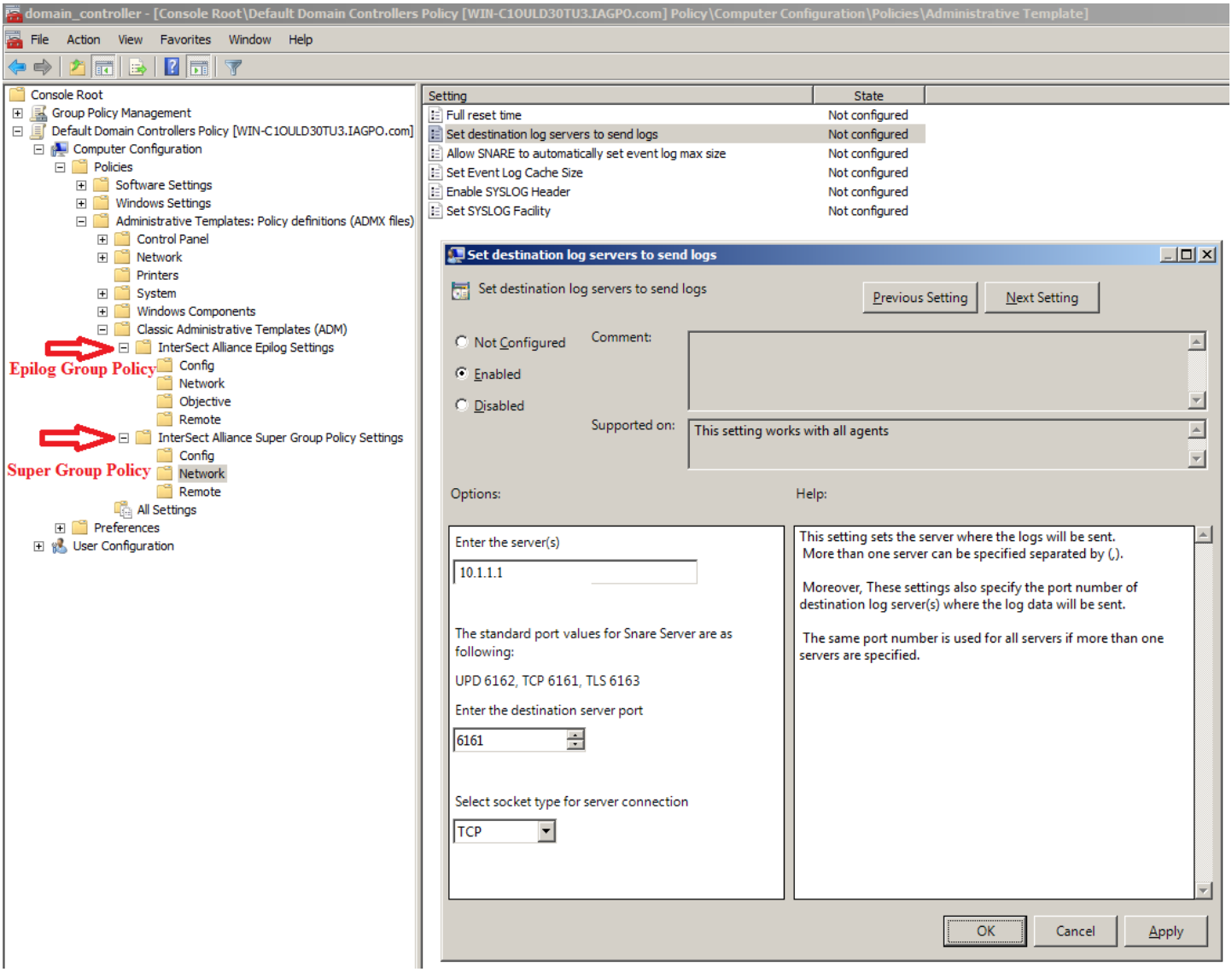

Figure 1: Update Snare Agents Network Settings through Agent Group Policy and Super Group Policy

- **Enhanced Event Throttling**

This release includes enhanced event throttling capabilities. It includes three useful settings in this regard, as shown in Figure 2.

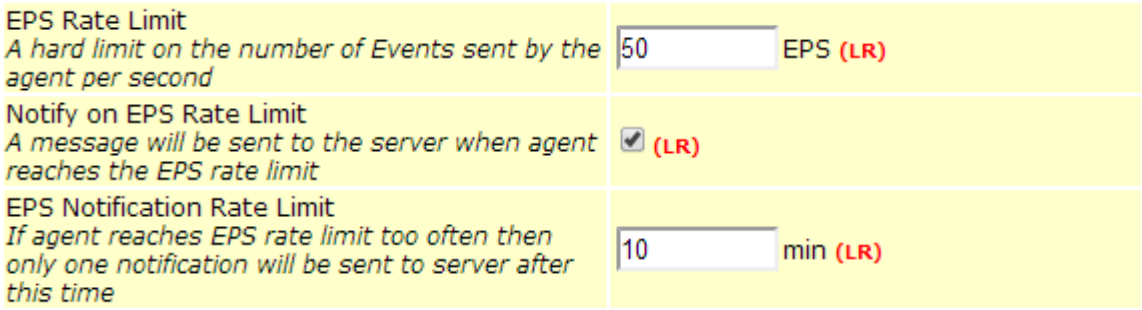

Figure 2: EPS Event Throttling Setting

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 epilog 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 an unexpected reason then all epilog 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 epilog agents 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 epilog reaches the EPS rate limit. The message also includes 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 epilog 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.