# SNARE Agent for MS SQL V 1.2.8 - Release Notes

SnareMSSQL is a program that facilitates the central collection and processing of MSSQL audit records. Log information, gathered from trace files, is converted to tab delimited text format, then delivered over UDP to a remote server.

SnareMSSQL is currently configured to deliver audit information to a SYSLOG server running on a remote (or local) machine. A configuration utility allows you to set the appropriate syslog target and priority, as well as the target DNS or IP address of the server that should receive the event information. It should be noted that many syslog servers are not designed to cope with the sorts of volume of data that multiple snare agents can potentially generate.

The SnareMSSQL service will automatically start after you have completed the initial configuration process. We recommend that you configure appropriate access controls on the SnareMSSQL registry entries using regedt32.exe - perhaps restricting the permission to read or modify the keys and values to Local or Domain Administrators only. SnareMSSQL stores it's registry settings in: HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\SnareMSSQL

To skip to the details for Version 1.2.8 please click here.

***Version History:***

| | |
|---|---|
| SnareMSSQL 0.2 | - Beta release |
| SnareMSSQL 0.3 | - Added filtering for trace events generated by the agent |
| | - Improved resource handling |
| SnareMSSQL 0.4 | - Greatly improved functionality including support for named instances and the use of authentication settings |
| | - Added per-objective trace file handling |
| SnareMSSQL 0.5 | - Added support for database and instance name |
| | - Improved event display in remote control interface |
| SnareMSSQL 0.5.4 | - Recompiled to remove VC80 dependency |
| SnareMSSQL 0.5.5 | - Fixed bug in trace file management |
| | - Greatly improved trace file management |
| | - Minor speedups |
| SnareMSSQL 0.5.6 | - Added advanced trace filter |
| | - Added expectation reporting to Query Tracking |
| SnareMSSQL 0.5.7 | - Extended field reporting |
| | - Expanded objective capabilities |
| | - Enhanced Error Reporting |
| SnareMSSQL 0.5.8 | - Fixed user filter |
| | - Added DatabaseName include/exclude filter |
| SnareMSSQL 0.5.9 | - Fixed backwards compatibility when updating agent |
| | - Added logging feature to installer |

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477

symtrex inc.
*Network Security Specialists*

| | |
|---|---|
| SnareMSSQL 0.6.0 | - Change Username to reflect LoginName, NTUserName and SessionLoginName added to Strings field. This will ensure SQL logins are captured correctly |
| | - Added Trace Path override field to Network Configuration |
| | - Added EventID lookup to remote control interface |
| | - Added local MSSQL enumeration (instance/DB/table) page to remote control interface |
| SnareMSSQL 0.6.1 | - Refined "use of user rights" logging, added ability to track Data Manipulation events, with or without tracking SELECT statements |
| | - Added Permissions field to output |
| | - Minor wording changes in the remote control interface |
| SnareMSSQL 0.6.2 | - Greatly improved SQL2000 support |
| | - Updated instance detection and enumeration |
| SnareMSSQL 0.6.2.1 | - Updated authentication routine to support Windows Authentication |
| SnareMSSQL 0.7.0.0 | - Added ability to configure trace size, file count and location |
| | - Added "Audit to local file" feature and configuration options |
| | - Added ability to pull user names from a given domain group by placing the name in square brackets, e.g. [domain admins]. Currently on startup only |
| | - Added TDF configuration feature for SMO trace support |
| SnareMSSQL 0.7.1.0 | - Added heartbeat capability. Each heartbeat contains a list of the currently monitored instances and their respective SQL versions. The heartbeat interval is variable. |
| | - Added a variable polling interval for the AD group lookup ability |
| | - Added ability to include Trace, Service and Debug log information in the regular stream of audit events for logging and analysis |
| | - Added support for running in a clustered environment |
| | - Added IA Supported features (e.g. TCP, multiple destinations) |
| SnareMSSQL 1.0.0 | - Extended the AD Group Lookup feature to allow domain identification using either Netbios or full DNS syntax, e.g. [FLATNAME\group],[group@dns.name.local] |
| | - Added silent install features, including encryption of sensitive data |
| | - Added full cluster installation support |
| | - Added logging feature to installer |
| | - Added upgrade only and reinstall options to installer |
| | - Added /DomainInfo window to check domain trusts and domain contollers |
| SnareMSSQL 1.0.1 | - Added the Success field to the capture list |
| SnareMSSQL 1.0.1.1 | - Bug Fix, EventID Lookup |
| SnareMSSQL 1.0.1.13 | - Fixed "Service Account Filter" problem |
| | - Added default behavoir for empty Objective User Filter |
| SnareMSSQL 1.0.1.14 | - Added Memory Monitor to watch the agent's Working Set memory usage |
| SnareMSSQL 1.0.1.15 | - Fixed Delimiter problem on installation |
| | - Added quotes to string values when generating a template file (snaremssql.exe -x) |
| SnareMSSQL 1.0.1.16 | - Added ApplicationName and HostName fields to the output |
| SnareMSSQL 1.0.1.17 | - Added Client Identifying Data Scrubbing |

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

| | |
|---|---|
| SnareMSSQL 1.0.1.18 | - Fixed bug in group member filtering |
| | - Added per objective UI for CID Scrubbing |
| | - Fixed potential loop in Service Log |
| | - Added flood protection to non-audit logs |
| SnareMSSQL 1.0.1.19 | - Added cleanup code for unused trace files |
| | - Added message flood protection for agent logs |
| SnareMSSQL 1.0.1.20 | - Added cleanup code for old trace files |
| | - Fixed message flood protection for agent logs |
| SnareMSSQL 1.0.1.21 | - Added Latest Hearbeat timestamp to Latest Events window |
| | - Fixed SQL2012 instance enumeration |
| | - Patched web interface to address unexpected drop outs |
| | - Fixed unquoted service path for standalone installs (cluster installs use quotes), for both fresh installs and upgrades |
| | - Changed some install Error messages to Warnings |
| SnareMSSQL 1.0.1.22 | - Fix Check Groups function for default instance (MSSQLSERVER) |
| SnareMSSQL 1.0.2.0 | - GUI deadlock fix |
| | - Mutex crash fix |
| | - Server status indicator added |
| | - Cluster support improved |
| | - Heartbeat to local file added |
| SnareMSSQL 1.1.0.0 | -TLS support added |
| | -EPS message sent to server |
| | -Bug fixes regarding error messages 105 and 108 in windows event log viewer |

**Snare for MS SQL Version 1.2**

**New Features**

- **Apply Agent Settings through Group Policy**

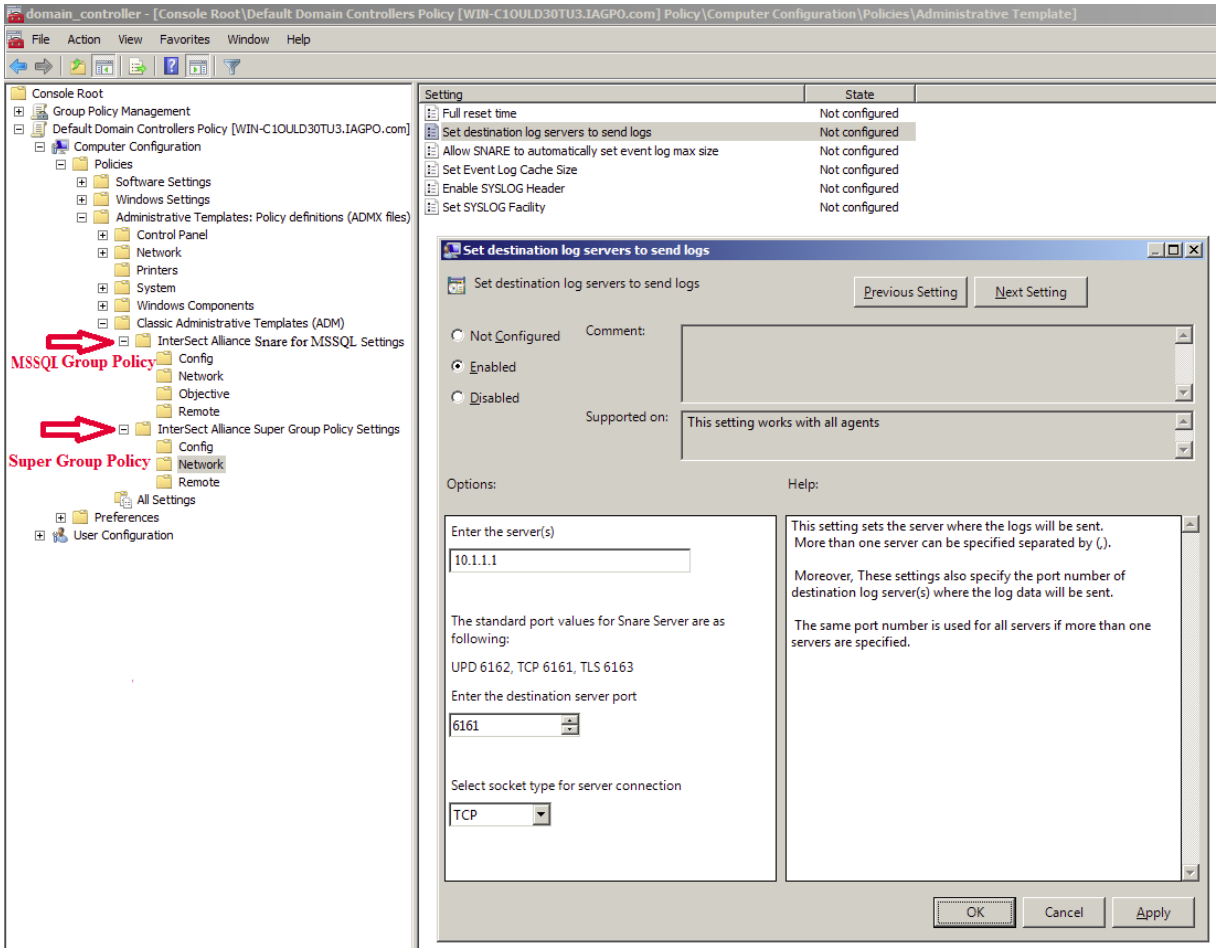
In a large network environment, having large number of Snare agents with no Snare Agent Management Console(AMC) can sometimes be a difficult task to maintain and apply new settings on all agents.

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 for MSSQL through Microsoft R Group Policy Editor. The updated settings will be applied to Snare for MSSQL based upon Group Policy update preferences. Moreover, Snare for MSSQL supports two levels of group policies, i.e. Super Group Policy and Snare Agent Group Policy.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

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




Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

symtrex inc.
*Network Security Specialists*

● **Enhanced Event Throttling**

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

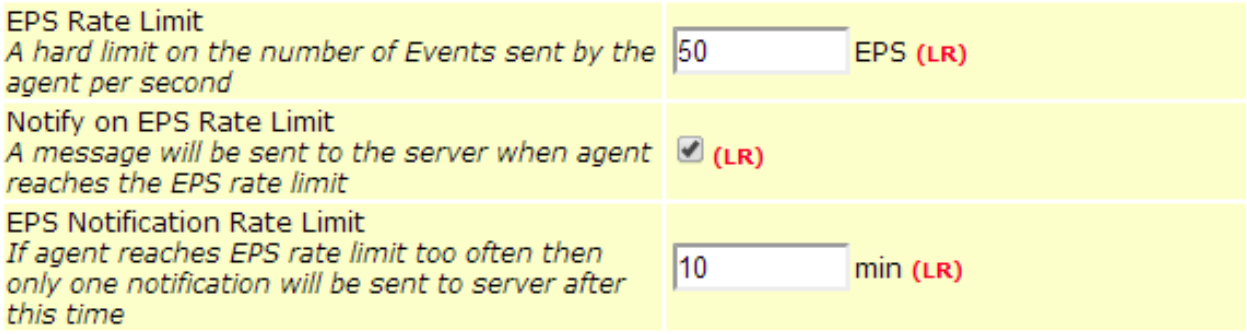



Figure 2: EPS Event Throttling Setting

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 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 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 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 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 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.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

***Bug Fixes—Version 1.2.1***

- 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

***Bug Fixes—Version 1.2.2***

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

***Bug Fixes—Version 1.2.3***

- **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.**

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

***Bug Fixes—Version 1.2.4***

- 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.

***Bug Fixes—Version 1.2.6***

- ***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.

***Bug Fixes—Version 1.2.7***

- ***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.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

***Release Version 1.2.8***

***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.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com

***Release Version 1.2.8***

***Enhancedments***

- **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.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477
www.symtrex.com
sales@symtrex.com