Knowledge Base Article #ETM807
ETM® (Enterprise Telephony Management) System v6.3 Release Notes

This document contains important information about release 6.3 of the ETM® System. The ETM System includes the ETM Communications and Application Appliances, ETM Server software, and the ETM applications: the Performance Manager, the Voice Firewall, the Usage Manager, AAA Services for the Voice Firewall, the Voice IPS (Intrusion Prevention System), and the Call Recorder.

Changes in v6.3

User account security and logon settings—A number of enhancements were made to user account security and logon options: These include configuration options to: limit the frequency of user password changes; disable a user account after a certain number of password expiration warnings; limit the number of concurrent session; timeout idle connections; and allow CAC card login.

Run-as user option for the ETM Database-An option is now provided to specify a different database account for the run-as user rather than allowing the ETM Server to run as the application owner.

Ability to set the IP header DSCP value for appliance to server communications.

Performance Monitor—A new Performance Monitor Tool, launched from the ETM System Console, provides a dashboard view of the health and status of the Appliances/Spans so issues can be quickly identified without the need to open the Performance Manager. Right-clicking a resource in the Performance Monitor provides a menu of options for further troubleshooting and corrective action.

Syslog Alert Tool—The Syslog Alert desktop popup tool automatically visually alerts security personnel by a desktop popup any time the ETM System generates a 911 alert, or other types of Syslog alerts of interest. This is a separately licensed application.

Internal CDR Import and Reporting (CUCM, Avaya, BAMS, any single-line CDR)—You can now configure the ETM System to import Call Detail Records (CDR) for calls that did not pass through an ETM Appliance, such as station-to-station calls. You can define a parse file for any switch that produces standard single-line ASCII CDR. Multi-line formats such as CME Syslog are not supported in this release. While you cannot apply ETM Voice Policies to these calls, you can run Usage Manager reports against them. This is a licensed add-on feature.

Increased Number of Policy Objects—Optimization and new Appliance hardware decrease Policy installation time and increase the number of phone number Objects that can be included in installed Policies. The number of objects that can be used in Policies depends on the ETM Appliance Card model on which you are installing the Policies.

1012, 1024, and 1090 Appliances—30,000 phone numbers.

8240 Controller Cards in 2100/3200 Appliance—30,000 phone numbers.

8540 Controller Cards in 2100/3200 Appliance, 5000-series SIP appliances, and the SIP AXP implementation —50,000 phone numbers.

Enhanced 911 alerting—Alerts can now include the appliance local time in addition to or instead of the server time. Alerts for 911 calls fire at the beginning of the call and are now automatically refired at the end of the call when all call information is available.

Tree Navigation Enhancements—You can now search for servers in the ETM System Console tree and for any component in the Performance Manager tree pane. You can also jump from Spans to their owning components (Switch, Platform, Span Group).

Manual Performance Manager tree pane refresh option—In deployments with large numbers of appliances connected to a single server and suboptimum network conditions, constant automatic status updates of the Performance Manager tree pane can cause the Performance Manager to become sluggish or nonresponsive. A new manual refresh option was added to accommodate these environments.

Oracle 11G R2 Support—Oracle 11G R2 is now supported along with Oracle 10G. Oracle 9i is no longer supported.

8540 Controller Card and Associated DTI—A new controller card for the 2100/3200 appliances is now available with increased processing power and memory that can accommodate up to 50,000 policy objects per Span.

Collection Server timestamps now reflect appliance local time—Instead of using GMT, the Collection Server now encodes timestamps in filenames and meta files as local appliance time.

Database Repository support— Multi-instance database support now ensures the data in databases from different servers can be consolidated using an external tool, to allow data warehousing without data contention.

Enhanced support for special recording treatment of specified extensions—Formerly, a Protected Extensions list allowed you to define a list of 60 extensions to which calls were never to be recorded, based on inbound SMDR. This capability has been expanded into an SMDR Extensions list. You can now use inbound SMDR to create a whitelist or blacklist of extensions for which call recordings require special treatment, such as being flagged as sensitive (subject to privacy restrictions) or being deleted. You can also now define up to 1000 such entries, and can use ranges. Each range counts as one entry, vastly expanding the number of actual extensions that can be represented.

Optional file compression of recordings on Collection Server—You can optionally choose to have voice recordings compressed for storage on the Collection Server, to conserve disk space.

Optional automatic purging of files from the Collection Server—You can optionally enable automatic purging of files based on the age of the file to free disk space for newer recordings.

Syslog Alerting—Syslog policy and system event alerts are now supported. Alerts can be sent to multiple Syslog servers.

New model 5060 Call Recording Cache (CRC) Appliance available—The 5060 provides more processing power and larger storage than the 1060 CRC.

IPv6 Support for Last Resort—When using Last Resort to restore an appliance, IPv6 is now supported.

Issues Resolved in v6.3

- 26294— Restarts due to time and timezone changes
- 26292 Card replacement results in call records associated with that card becoming unavailable for reporting
- 6686— GUI allows empty Card name
- 1459– Clock Adjustments/Time Changes can cause loss of short calls/distort call times
- 7203— Consistent allowed characters for Import Set name

Special Configuration Instructions

Upgrading from a previous version—Ensure you obtain and follow published upgrade instructions for your version. See the SecureLogix Knowledgebase at http://support.securelogix.com/knowledgebase or contact Customer Support to obtain a copy. Of particular importance for this release, additional database

permissions must be granted to use the repository or run-as user features, prior to attempting to upgrade the ETM database, and the default ETM Instance must be manually entered into the **twmns.properties** file rather than using the Set As Default function in the Database Maintenance Tool.

Database Maintenance Tool—Prior to beginning an upgrade, note Database Object connection information. When you upgrade to this release, existing Database Objects in the Database Maintenance Tool are removed and must be redefined after the ETM Software is upgraded. This is due to the changes for Database Repository support. When recreating the Database Objects, a new field called Database Schema must be populated. For a standalone database (not a Repository), set this field to the username of the database (the same name you use to log into the database). For information on using Database Repositories, see the SecureLogix Knowledgebase at http://support.securelogix.com, keyword "repository".

Default password restrictions--When upgrading to v6.3, the password properties setting defaults to the less restrictive settings (8 characters minimum, 1 uppercase character minimum, 1 numeric character minimum, 0 special characters required, unlimited opportunities to reset expired passwords, no password reset frequency restrictions). For customers upgrading from v5.3, the password restrictions will be relaxed to these default settings. Ensure you apply stricter settings (15 characters, 1 upper case, 1 numeric, and 1 special) if desired.

Hostname and BAMS configuration—When specifying a BAMS server using an IP address, if the address is converted into a hostname, this hostname (instead of the IP address) must also be used in the **known_host** file that is used for enabling SSH communications with the BAMS server.

Ensure you copy custom information into the new twms.properties file rather than overwriting it with a backup--When upgrading from 5.3 to 6.3, the new 6.3 **twms.properties** file includes entries for BAMS Repository and CDR Importer Processed folders. If you simply copy backed up 5.3 **twms.properties** file over the 6.3 version, the ETM Server will fail to start up since these properties are expected and required.

Upgrade 1060 CRCs first—When upgrading appliances to v6.3, 1060 CRC appliances should be upgraded prior to other appliances. This ensures proper configuration of the enhanced Call Recorder SMDR Extensions feature.

Ensure you upgrade all clients before attempting to use them to connect to the v6.3 Management Server--v5.3 clients will not connect to the v6.3 ETM Server due to login mechanism changes. The error message when attempting to login is "Invalid login, Please try again".

Last Resort—To support the Last Resort feature using IPv6 on a given appliance, the v6.3 P2 package must first be installed on that appliance.

Collection Server search database—The v6.3Collection Server uses a database to store Call Recording information for searches using the Web Portal. This database is built when the 6.3 Collection Server is installed and by request from the user. Depending on the number of recordings stored on the Collection Server, this operation could take several hours. A rough estimate (that varies based on the performance of the given server) is that it takes approximately 1 hour to build the database for every 500,000 call recordings. During the time that the Collection Server is building the database, it will be unavailable for all other actions such as uploading new recordings. Therefore, choose an appropriate time to install the 6.3 Collection Server or to initiate rebuilds of the database. Note that a rebuild of the database on a periodic basis may be useful to keep the database in sync with the stored recordings if call recordings are periodically moved or removed from the Collection Server using processes outside of the Collection Server.

SS7 Signaling Listener Ports—When configuring fully-associated signaling links on SS7 Bearer Spans, ensure that a unique listener port is selected for each Span on a Card, or port conflicts will occur. During the "out-of-the box" configuration of Cards, the Appliance software selects unique listener ports based on the Span number on the Card. If you change these port assignments, assign a distinct value for each Span. See the *ETM® System Installation Guide* for details.

IMPORTANT INFORMATION for installing on Windows Vista, Windows 7 or Server 2008—A feature called User Account Control (UAC) was introduced in Windows Vista, Windows 7 and

Windows Server 2008 that limits application software to standard user privileges and only provides administrator level privileges if authorized by an Administrator-level user. In addition to requiring administrator privileges to perform administrative functions, UAC also introduced File and Registry Virtualization, which causes user-level programs to write data and registry settings to a virtual area for the given user, rather than to a system directory (such as Program Files) or the registry. Various functions, scripts, and installations in the ETM System may be adversely affected.

To prevent issues, do one of the following when installing on one of these operating systems:

- Ensure a user with Administrator privileges installs the ETM System applications and then run the applications as Administrator rather than local user.
- Install the ETM System in a directory that is not a system directory (for example, not in Program Files).
- Disable the UAC feature on your operating system.

Delayed interface responsiveness—On Windows, an additional delay averaging 20 seconds may be encountered when any of the ETM System Software Components attempts to open a network connection to a remote machine. This delay is due to the lack of a DNS Server definition or an invalid DNS server definition in the Windows Internet Protocol (TCP/IP) Properties for the applicable networking interface, exacerbated by the Java 1.5 Virtual Machine use of a SOCKS networking protocol that requires additional DNS lookups.

To avoid this delay, do one of the following:

- Specify a valid DNS Server in the Windows Internet Protocol (TCP/IP) Properties for the applicable networking interface.
- On each remote client computer, add an entry for the ETM Server computer to the HOSTS file. For example, if the Server is **zephyr.securelogix.com** with an IP address of 10.1.1.202, you would add the following entry:

  10.1.1.202 zephyr zephyr.securelogix.com

SMDR recording file lock—When recording SMDR data to a file, the recording mechanism locks the file until the maximum record count is reached (10,000). While the file is locked for writing, the CDR importer cannot import the file. This is intended behavior. However, in low-volume environments, the amount of time the file is locked to reach the max record count may be unacceptable. If a smaller count is needed, add the following command-line switch to the # Java switches to supply to the Java Virtual Machine line in the **ETMManagementService.cfg** file and then restart the Server:
-Dsmdr.RecorderRecordsPerFile=<value>

SMDR Recording File Directory not automatically created— When you configure an Appliance to record raw SMDR, the directory where the files are stored is not automatically created. Manually create the following directory before enabling SMDR recording on the Switch:**<INSTALL_DIR>/ps/smdr-recording**

Known Limitations in v6.3

Unable to import LDAP data set from an IPv6 address—A known issue with the LDAP Java SDK prevents the Directory Manager from connecting to the LDAP source via IPv6.

Management Server and Report Server do not start on an IPv6-only system—If IPv4 networking is removed or disabled on the system on which the Management Server and Report Server are installed, the services will not start. When using IPv6, ensure that IPv4 networking is also installed and enabled.

An ETM System console installed on an IPv6-only system cannot connect to remote Management Servers— If IPv4 networking is removed on the client host on which a remote ETM System Console is installed, the Client cannot connect to the ETM Server. When using IPv6, ensure that IPv4 networking is also installed and enabled.

Emergency Group contents—When defining a custom Emergency Group for a Firewall Policy, do not use Directory Filters, or the Firewall Policy may fail to install.

Masking/Redirection Plan for E1 DASS2/DPNSS—Various issues exist with Masking/Redirection Plan functionality on E1 DASS2 and DPNSS Spans.

In-progress calls logged by analog at startup—When an analog 1012/1024 Span starts up following a restart or reboot, any calls that are currently in-progress generate new call logs. Since Spans are not frequently restarted or rebooted, this issue is not likely to occur often.

Potential for Inbound SMDR correlation mismatches—On rare occasions, under heavy load on Merlin PBXs, unanswered calls may be miscorrelated with answered calls that have like duration.

No Dirty Policy indicator for Call Recorder Policies when URIs are changed in the Directory—When a URI associated with a Listing used in an installed Call Recorder Policy is changed, the Dirty Policy indicator fails to display for the Policy. The Dirty Policy indicator displays correctly when phone numbers are changed and for other Policy types. If you modify the URI in a Listing used in an installed Call Recorder Policy, ensure you reinstall the Policy.

Version History

For information about previous releases of the ETM System, see the SecureLogix Knowledge Base at *http://support.securelogix.com*, keyword "release notes."

Last Update: 5/7/2012

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • http://support.securelogix.com