Knowledge Base Article #ETM616, Rev B
ETM® (Enterprise Telephony Management) System v6.1.0 Release Notes

This document contains important information about release 6.1.0 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 v6.1.0

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.

LDAP Authentication— You can configure the ETM System to authenticate users against your corporate LDAP Directory Server. Microsoft Active Directory and Sun ONE Directory Server using LDAP v3 are supported.

Call Recording enhancements—SIP Call Recording of up to 30 concurrent G.711 and/or G.729 calls is now supported on the 5000 series appliances and the AXP SIP solution. A new **Do Not Record** policy action enables you to write rules to explicitly exclude certain calls from recording. Formerly, rules could only specify calls to be recorded. Formerly, if a call matched a Record rule but then the call type changed to one not specified by any rule in the policy, recording stopped and the recording was deleted. This is still the default behavior, but an option has been added to the **Attributes** tab of the Policy to allow you to select between that behavior and **Keep the Recording when Call Type Changes**.

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.

AXP Platform Support for SIP Functionality—The ETM SIP appliance software functionality has been ported to run on AXP on an NME or SRE in a Cisco ISR. All native appliance functionality is provided, including Call Recording. An HA implementation is not available in this release.

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.

Issues Resolved in v6.1.0

- TT 6703 – Web Portal: Login Failure message from previous attempt not cleared for new login attempt
- TT 6988 - CRC error on download cancel
- TT 7507 - SIP: High Availability: No diagnostic log messages when isolating the processing node
- TT 7520 - SIP: On a SIP appliance package install, no indication that the install was complete.
- TT 7527 - SIP: Signal Proxy panic in LinkStat process
- TT 7546 - SIP: High Availability: Disconnecting the eth3 (Trunk) cable from processing node gives Signal Proxy panic when Signal Proxy is restarting
- TT 7547 - SIP: High Availability: reconnecting the trunk cable on a non-processing node should give 'cable connected' message in diagnostic log
- TT 7548 - SIP: High Availability: Diagnostic log message should be shown when eth1 (shared private) cable is disconnected
- TT 7578 - SIP Sub-Span GUIs use name "Span: 1" rather than the actual span name
- TT 7574 - Inaccurate error text for media port range error
- TT 7580 - SIP: Slow memory leak in Signal Proxy
- TT 7581 - SIP: Node connect/reconnect memory leak in Call Processor
- TT 7655 - Cursor not automatically placed in **New Listing** dialog box
- TT 7681 - Collection Server Default filter encodes call timestamps using wrong time zone

Special Configuration Instructions

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 or Server 2008—A feature called User Account Control (UAC) was introduced in Windows Vista 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>

For graduated SIP software upgrades, Call Recording functionality requires components to be upgraded in a specific order— If you want to upgrade one SIP Appliance proxy component first and let it run for an extended amount of time before upgrading the other proxy component, then the Signaling Proxy should be the first upgraded to ensure media continues to be natted. This is not an issue if both components are upgraded in a timely manner.

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 v6.1

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.

SIP Appliance CRC and Span System Statistics are inflated—The SIP Span CRC system statistics value for **Recordings in Progress** and the SIP Recording Span statistics value for **Active Recordings** do not get

updated properly for recordings that are attempted, but do not actually proceed. Therefore, these values may be greater than the actual number of active recordings.

SIP Call Recording Threshold Detector calculation issue—Erroneous values are generated for the Call Recording threshold detector on SIP Spans.

Cannot authenticate user when LDAP server is using IPv6—If the LDAP server uses an IPv6 IP address, LDAP authentication fails. Only IPv4 LDAP servers are supported in this release.

Serial SMDR GUI settings available for SIP Spans, but only IP SMDR is supported—Ignore the Serial SMDR settings.

IP Subnets not correctly applied in Call Recording Policies on SIP Spans— Call Recording policy processing on SIP Spans does not match on IP Subnet values in the **Source** or **Destination** column. Do not use Subnets in Call Recording Policies on SIP Spans.

SIP Call Recording files corrupted if 3DES Encryption is disabled—If you are using Call Recorder on SIP appliances, ensure you have encryption enabled.

Erroneous Outbound SMDR checkbox on SIP Span Recording tab—Outbound SMDR is not used for Call Recording on any Span type in this release. Ignore the Outbound SMDR checkbox.

SIP Call Recording limits—

- G.711 and G.729 codecs only
- Single stream only (last one in SDP list for multiple audio streams)
- 30 simultaneous recordings max
- Local CRC only

IPv6 not supported on the SIP AXP solution—AXP blades do not support IPv6, and therefore IPv4 must be used for addressing of the blade itself and of SIP Trunks on a SIP AXP application.

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: 9/1/2010

SecureLogix Corporation

13750 San Pedro, Suite 230 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

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