Knowledge Base Article #ETM537
ETM® (Enterprise Telephony Management) System v7.0.0 Release Notes

This document contains important information about release 7.0.0 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 v7.0.0

Unified Trunk Application Integrated with IOS on ISR G2—The new Unified Trunk Application (UTA) provides simultaneous support for TDM and SIP (and other VoIP protocol) trunks through one ETM application interface. This functionality is enabled by integration with functionality embedded in a new IOS release for Cisco Integrated Services Routers (ISRs) G2 [IOS 15.2.(2) T]. The UTA application runs on an SRE module in the router, or on a SecureLogix UTA appliance. Besides its unified trunk type support, the IOS integration enables the UTA application to provide full ETM SIP appliance functionality without being inline.

Adaptive IPS—A new feature in the Voice IPS application provides detection and policy enforcement for multiple calls from same previously unknown inbound source. Previously, one or more specific numbers or sets of numbers had to be specified in IPS Rules based on calling source and destination. Now, the Voice IPS can identify, track, and report a pattern of calls from a previously unidentified number that may be of interest.

Ability to Exclude Terminated Calls from IPS Rules—The **Disposition** field in IPS Rules can now be negated so that terminated calls are not counted. This is particularly valuable for tracking unanswered calls.

DTMF Pattern Detection and Policy Enforcement—Mid-call DTMF patterns are now an available criteria in Voice IPS and Voice Firewall Policies. Voice IPS Policies can also specify **NO DTMF** as a rule criteria, to flag calls with no digits when they are expected, such as into an IVR. The interdigit timing of the digits is stored with the pattern in the ETM Database to enable offline data analysis for timing patterns of interest, such as those that might denote a robodialer.

Multi-Policy Push— The ETM Performance Manager now supports simultaneous selection of multiple Policies for installation. This places the Policies in a queue, from which they are sequentially installed. Additionally, an option is provided to reinstall all “Dirty” Policies. This places them in the client-side queue. **NOTE:** Since this is a client-side queue, the ETM Performance Manager must remain open and connected for the duration of the installation of all queued Policies.

SIP Masking— The inline ETM SIP application now provides the ability to replace the source number and the source display number for a call, on both the SecureLogix appliance or the inline implementation on a Cisco ISR.

Reliability Enhancements for Inline SIP Application—Enhancements to improve reliability on the inline SIP application include a system watchdog application that monitors for certain application errors and automatically restarts impaired processes and a packet-filter application to protect it against packet floods.

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. Not supported on Oracle XE.

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

Oracle 11G XE R2 Support—Oracle 11G XE R2 is now supported along with Oracle 10G, 10G XE, and 11G R2. Run-As users and Database Repositories are not supported on Oracle XE.

Call Recording on All Channels on an 8540 Controller Card with Optional Add-On Hardware—8540 controller cards in the ETM 2100/3200 appliances support Call Recording on half of the available channels on the Card (48), due to resource limitations. The 8540 Controller Card can optionally be upgraded with a DSP daughter card that enables recording on 96 channels. To accommodate this increased capacity, the 5160 CRC can now support up to 200 simultaneous recordings. (The 1060 CRC supports 120)

Issues Resolved in v7.0.0

- ETM-26523 Reports: CDR Importer Calls not displayed if the Card field is included
- ETM-26398 CP SPAN Task Panic
- ETM-26396 CP ProxyCommMgr Panic
- ETM-26383 DBT - The View All Tasks menu item under Repository, Managed Databases is enabled when a Standalone database is selected
- ETM-26381 ESC: Configure CDR Import Trunk: Specify Directory Location dialog: Help button displays nothing.
- ETM-26320 Database Exceptions (ORA-20001) while running Lerdorf
- ETM-26278 Subnet conversion is missing for some of the tables when upgrading from 5.2 to 6.0+
- ETM-18939 SSB: Termination/Call End race condition results in panic
- ETM-18610 SIP Appliance: Issues with SIP Trunk Signaling Port Settings
- ETM-18368 SIP CR: Error Logs created on CRC for calls that do not send audio
- ETM-18350 SIP: Remote Clients list not used to limit ssh connections
- ETM-18212 SIP Media Timeout Rule does not fire properly if the action is Terminate
- ETM-18158 Restarted Collection Server fails to purge when Minimum Disk Space not available
- ETM-18154 Error log produced at span startup if no Protected Extensions defined

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.

Web Portal Installer—Ensure you stop the Apache Tomcat service prior to upgrading the Web Portal application, or the **webetm.war** file will not be replaced, and the old version of the Web Portal will still be installed.

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.

Upgrade 1060 CRCs first—When upgrading appliances to v7.0.0, 1060 CRC appliances should be upgraded prior to other appliances. This ensures proper configuration of the Enhanced Protected Extensions feature.

Last Resort—In order to support the Last Resort feature using IPv6 on a given appliance, v 6.1.79 or later must be installed on that appliance.

Collection Server search database—The ETM Collection Server uses a database to store Call Recording information for searches using the Web Portal. This database is built when the 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 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 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 anchored. 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**

Web Portal Installer limitation—When upgrading the Web Portal, since the installer does not create **jakarta-tomcat-5.5.9\webapps\webetm** directory, it is not replaced by the installer. To work around this issue:

1. Stop Tomcat.
2. Install the upgrade.
3. Copy <**install_dir>\jakarta-tomcat-5.5.9\webapps\webetm\WEB-**INF\server-defn.xml file to a safe directory.
4. Delete the **<install_dir>\jakarta-tomcat-5.5.9\webapps\webetm** directory.
5. Start the Tomcat service.
6. Copy the original server-defn.xml file back into the new WEB-INF directory,
7. Restart the Tomcat service.

Upgrading HA Appliances from a Version Prior to 7.0.0—No automated remote upgrade is available for HA appliance deployments running a version prior to v7.0.0. For instructions for upgrading appliances in an HA deployment, see the SecureLogix Knowledge Base, keyword “upgrade’. All future software releases will support remote upgrade of HA appliances running v7.0.0 or later.

UTA supported in a Single Application Configuration Only (No HA) —The UTA is only supported in a single node configuration in which the Call Processor, Signaling Processor, and Media Processor reside on a single appliance or SRE platform.

Known Limitations in v7.0.0

Web Portal—

- Undetermined shown for multiple call types —When searching for calls on a Collection Server in the Web Portal, if recordings exist that contain multiple call type values, the call type field in the Search results for these calls shows "Undetermined".

- Java Heap Space Exception for large query result (thousands of calls)—If a large number of calls (thousands or more) match a search via the Web Portal (CRC or Collection Server), a Java Heap Space exception may occur. To resolve this issue, initiate a new Web Portal session and repeat the search using a smaller start time range to reduce the number of matching recordings.
- Preview of Compressed Recordings Fails—If recordings are being compressed at the Collection Server, previews of these recordings using the Web Portal will sometimes cause an error in the media player indicating that the wav file is corrupt. The preview media is played properly even when this error occurs. The problem does not occur when compressed recordings are played in their entirety.
- Collection Server search results do not provide wav file size—Web Portal results for call recordings stored on a CRC display the size of the wav file. This field is left blank for Collection Server results. Filtering based on wav file size when searching a Collection Server is ignored (the filter criteria will not be used).
- Preview fails for calls less than 10s. If you attempt to preview a recording from the Collection Server using the Web Portal and the recording is less than the preview length (default of 10 seconds), the recording will not download properly. The file will download and play properly if the play option (entire recording) is selected.

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 UTA and 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. On UTA, the CRC Recordings In Progress value always reflects 0.

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.

SIP (including UTA) Call Recording limits—

- G.711 and G.729 codecs only
- Single stream only (last one in SDP list for multiple audio streams)
- Limit of 80 simultaneous recordings on the 5100 and 100 on other ETM SIP appliances

- Limit of 50 simultaneous recordings on the 5001 SIP AXP application and all 5003/5004 UTA application on both the SRE module and the SecureLogix 5000-series UTA appliance.
- 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: 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