

Knowledge Base Article #ETM9141

ETM[®] (Enterprise Telephony Management) System v7.0.1

Release Notes

This document contains important information about release 7.0.1 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 v7.0.1

64-Bit Linux Management Server support—The ETM Management Server can now be installed and run on 64-bit Linux. Solaris is no longer supported.

64-bit Windows Management Server support—The ETM Management Server can now be installed and run in 64-bit mode on Windows. Previous versions could only be run in 32-bit mode on Windows. Note: the Web Portal and Collection Server still run only in 32-bit mode.

UCS Management Server support—The ETM Management Server is now supported on UCS servers that meet minimum system requirements.

Virtual UTA support—Up to 15 virtual instances of the UTA application can now run on one platform that meets minimum system and resource requirements, including the ETM 5000 series. Each instance supports up to 50 simultaneous calls.

SRE-V support—The ETM inline SIP and UTA applications now support SRE-V rather than AXP on the SRE module.

Lighter Transportable Call Recording Kit—The Transportable Call Recording Kit has been redesigned to weigh less than 100 lbs., while providing the same functionality.

Issues Resolved in v7.0.1

- ETM-26885 - Adaptive IPS: Valgrind errors found in appliance software
- ETM-26854 - 5160 Cache produces a warning log at the old recording limit of 120 calls
- ETM-26842 - Inline SIP: Media Inactivity timeouts occur for SIP calls with active media
- ETM-26841 - Inline SIP: Following a Video call, the Media proxy consumes 100% of the CPU it is running on
- ETM-26840 - ETM-26840 – CDR Importer stops working and purging of processed files fails
- ETM-26836 - Inline SIP: Call type not set according to the Codec.xml file for user-configured dynamic codecs
- ETM-26832 – Directory Manager: Cannot search for listings containing alpha access codes
- ETM-26823 - Appliance: Integrate HA and RPM cleanup scripts into build RPMs
- ETM-26822 - Appliance: Threaded panics are not logged to the MS until the next process restart
- ETM-26820 - UTA: Following package push there is no visible reminder to upgrade the SP/MP applications
- ETM-26817 - UM: Inline SIP: Bootup cleanup tasks not executed
- ETM-26815 - High-Speed Fax Calls sometimes get Undetermined call type
- ETM-26813 - Installer: The twms.properties file in the ps_skel folder is incorrect.

- ETM-26810 - SPF: TCP Call messaging delayed or prevented
- ETM-26809 – Inline SIP on SRE: CSTLock Panic over config change/restart
- ETM-26808 - MS: AppManager.exe is not populating the Java Home registry key when adding a new service
- ETM-26806 – Inline SIP: 2-node HA configuration: Upgrade: MP panic on upgrade from build 64 to 65 - different panic from 26803
- ETM-26804 - Inline SIP: 2-node HA configuration: Upgrade: SP panic on upgrade
- ETM-26803 - Inline SIP: 2-node HA configuration: Upgrade: MP panic on upgrade
- ETM-26792 - Inline SIP: 2-node HA configuration: MP Panic when following upgrade from patched version
- ETM-26789 - UTA CR: Video Call recorded even though policy indicated only Voice should be recorded
- ETM-26733 - ESC: Call monitor display not behaving as in previous releases - rows not expanding/collapsing as they should
- ETM-26696 - SIP/UTA: SP/MP Restarts when config pushed down
- ETM-18210 - WebETM/Collection Server: Preview fails for calls less than 10s

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, before you attempt to upgrade the ETM database, additional database permissions must be granted to use the repository or run-as user features, and the default ETM Instance must be manually entered into the **twms.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 v7.0.1 from a version prior to 7.0.0, 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
```

Imported SMDR recording file lock—When recording imported 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.

Oracle XE—Run-As users and Database Repositories are not supported on Oracle XE.

Known Limitations in v7.0.1

Web Portal—

- Collection Server search results show **Undetermined** for calls with multiple call types — During a Web Portal search for calls on a Collection Server, if recordings exist that contain multiple call type values, the call type field for these calls in the Search results 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 sometimes cause an error in the media player indicating that the wav file is corrupt. This is cosmetic; 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).

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.

Inline 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.

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

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

Inline SIP and 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 and the 5000-series UTA appliances
- Limit of 50 simultaneous recordings on the Inline SIP and UTA applications on the SRE module.
- Local CRC only

UTA: Tracking of non-phone number URIs—Calls that use non-phone number URIs (the user portion of the URI does not contain a phone number) are not tracked by the UTA appliance.

IPv6 not supported on the SIP and UTA SRE solutions—SRE blades do not support IPv6, and therefore IPv4 must be used for addressing of the blade itself and of SIP Trunks on an SRE-resident ETM application.

CAC Card Login under Windows 64-bit and Linux OS—CAC Card login is not supported when running the ETM Management Server under Windows 64-bit systems or Linux systems.

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: 6/4/2012

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>

ETM, TeleWatch Secure, TWSA, We See Your Voice, SecureLogix, SecureLogix Corporation, the ETM Emblem, the SecureLogix Emblem and the SecureLogix Diamond Emblem are trademarks and/or service marks or registered trademarks and/or service marks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2012 SecureLogix Corporation. This product is protected by one or more of the following patents:
US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 B2, US 6,760,421 B2,
US 6,879,671 B1, US 7,133,511 B2, US 7,231,027 B2, US 7,440,558 B2, US 8,150,013 B2, CA 2,354,149, DE 1,415,459 B1,
FR 1,415,459 B1, and GB 1,415,459 B1.

The ETM System includes: Data Encryption Standard software developed by Eric Young (ey@mincom.oz.au),
© Copyright 1995 Eric Young. All Rights Reserved.