



## Knowledge Base Article #ETM1521

# ETM<sup>®</sup> (Enterprise Telephony Management) System v9.0.0 Release Notes

This document contains important information about release 9.0.0 of the ETM<sup>®</sup> System. The ETM System includes the ETM Communications Applications and software, Application Appliances, ETM Server software, and the ETM applications: the Performance Manager, the Voice Firewall, the Usage Manager, the Voice IPS (Intrusion Prevention System), and the Call Recorder.

### Changes in v9.0.0

**Oracle 18c and 19c Support**—The ETM System Database now supports Oracle 18c and 19c, in addition to 12.2.

**Updated Linux Version for the UTA Appliance**—The UTA Appliance operating system has been updated to Red Hat Linux v6.

**Updated JDK on the ETM Management Server**—The ETM Management Server has been updated to the Correto 8 OpenJDK.

**Enhanced Management Server Audit Logging**—Audit logging on the ETM Management Server has been enhanced to provide additional visibility to Administrators/Auditors.

### Issues Resolved in v9.0.0

- **ETM-27434**—Subsequent Client Login fails following execution of an ad hoc report and then logout.
- **ETM-27435**—Intermittent Exception when Managing Billing Plans, Contacts, Intervals, etc., and then executing **Report->Preview/Print/Save As**.

### Special Configuration Instructions

- **Upgrading from a previous version**—
  - You must have v7.1.1 Build 41 or later installed prior upgrading to v9.0.0.
  - You cannot upgrade the UTA Appliance from a previous version to v9.0.0, due to the operating system upgrade. You must uninstall the previous version and then install the 9.0.0 UTA appliance.
  - **Follow published upgrade instructions**--Ensure that you obtain and follow published upgrade instructions. See the SecureLogix Knowledge Base at <https://support.securelogix.com/knowledgebase.htm> or contact SecureLogix Technical Support to obtain a copy.
- **Run As User must be granted CREATE SEQUENCE permission**—If you are using a run-as (non-owner) database account for the ETM Server, grant that account CREATE SEQUENCE permission or the Call and Policy Log tools will be unavailable.
- **IMPORTANT INFORMATION for installing on Windows**—The ETM System is installed by default at **C:\apps\SecureLogix**. If you choose a different installation directory, be aware of the following. A feature called User Account Control (UAC) in Windows 7 and later and Server 2008 and later 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 Windows:

- Ensure that 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.
- **Enhanced Policy Push**—Depending on various factors such as the size of the policy, the number of spans to which the policy is being pushed, and network throughput, it is possible to exhaust the Java heap space on the Management Server if the number of Policy Threads is set too high. If the Management Server fails due to an out of memory condition while pushing policy, reduce the number of policy threads (and/or increase the amount of Java heap space).
- **Deadlock prevention**—In rare cases, a database deadlock error may occur. If this error is seen, a mechanism to prevent its recurrence can be enabled. To enable the locking mechanism when creating the working tables, perform the following steps.
  1. In the Management Server configuration file (**ETMManagementService.cfg/ETMManagementServer.cfg**), add the following value the **Switches** line:

```
-Dslc.report_dbtable_locks=true
```
  2. In the Report Server configuration file (**ETMReportService.cfg/ETMReportServer.cfg**), add the following entry to the **RMID\_Switches** line:

```
-C-Dslc.report_dbtable_locks=true
```
- **Java Heap Space settings on a Linux Management Server**—The **ETMManagementService.cfg** file contains settings related to the Java Heap space. These settings are as follows:
  - **-Xms** = the initial (and minimum) java heap size. **Xms** value cannot exceed **Xmx** value.
  - **-Xmx** = the maximum java heap size.
  - **PermSize** = initial (and minimum) additional separate heap space to support the **Xmx** value mentioned above. The heap space stores the objects and the **PermSize** space keeps required information about those objects. Therefore, the larger the heap space, the larger the **PermSize** must be.
  - **MaxPermSize**=the maximum perm space allocated.
- By default, **MaxPermSize** is 32MB for **-client** and 64MB for **-server**. However, if you do not specifically set both **PermSize** and **MaxPermSize**, the overall heap size does not increase unless it is needed. If you set both **PermSize** and **MaxPermSize**, the extra heap space is allocated at server startup and remains allocated.
- **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<sup>®</sup> System Installation Guide* for details.
- **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.

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>
```

- **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 v9.0.0

- **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.
- **Delayed database connection with “spinning globe” when running reports**—If you encounter this issue, old database partitions need to be removed. Contact SecureLogix Technical Support for assistance.
- **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 that you reinstall the Policy.



- **SIP Offline Mode**—SIP offline mode does not support SIP Trunk configurations in which multiple trunks are defined that use the same IP address and port for the ETM appliance node.
- **“Redirected” Policy Disposition only effective for inline SIP applications**—A Policy Disposition of **Redirected** is provided and appears as available for all application types. However, this Disposition is only processed for inline SIP applications.
- **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.
- **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.
- **Scheduled Reports “Save to Tree”**—On some client systems, an error has been seen while attempting to save a Scheduled Report to the Tree. Workarounds include scheduling the report from a different client or using other actions such as Email or Save to Disk.
- **UTA Call Manager sometimes fails to reconnect to Call Processor**—On some UTA appliances, an issue has been seen following appliance package push or Call Processor restart in that the Call Manager will not always reconnect to the Call Processor. To resolve this issue, restart the Call Manager service.
- **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.
- **ETM-27398—Reports:** Exceptions occur when saving to tree and when viewing/printing/save as from tree.
- **ETM-27368—Reports:** SQLSyntaxError occurs querying data by the **Egress Trunk Channel** field.
- **ETM-27327**—Calls terminated by an IPS Rule that includes **Call Duration** are not included in the **Prevented Count** in the IPS Real-Time Monitor, but they are correctly terminated.
- **ETM-27350**—UTA:: CID Restricted calls do not trigger IPS or Recording Policy Rules.
- **BAMS**—The BAMS feature is not supported in this release.

## Version History

For information about previous releases of the ETM System, see the SecureLogix Knowledgebase at <http://support.securelogix.com/knowledgebase.htm>, keyword "release notes."

**Last Update:** 10/20/2020





SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • [securelogix.com](http://securelogix.com)

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

ETM, We See Your Voice, SecureLogix, SecureLogix Corporation, and the SecureLogix Emblem are registered trademarks or registered trademarks and registered 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 2018-2020 SecureLogix Corporation. All Rights Reserved.

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. U.S. Patents Pending.

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