



Knowledge Base Article #ETM5762

ETM® (Enterprise Telephony Management) System v10.3.0 Build 11 Release Notes

This document contains important information about release 10.3.0 of the ETM® System. This release is for Federal customers who require JITC testing. 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.

What's New in v10.3.0

- **Encrypted LDAP Support for LDAP Logins and LDAP Directory Imports**—The ETM System now supports LDAP v3 with LDAPS/SSL. Active Directory is supported. (Sun One Directory is no longer supported.)
- **Extended TNS NAMES String Length**—The character limit on the TNS NAMES length in the Database Maintenance Tool has been increased to 300 characters.
- **Lock Idle User Accounts**—Idle user accounts can be locked by a configurable setting in the **Server Properties** Tool.
- **Management Server/Client Installer Signed with a Certificate**—Installation of the ETM Management Server and Client is now signed by a certificate.
- **Improved UTA Appliance Framework**—The UTA Appliance has been updated to support additional monitoring features, such as SIPcli, multiple paniclog files, syslog debug, and others.
- **New SRTP Cipher Suites for Encrypted Call Recording**—The UTA Appliance supports new SRTP Cipher Suites for Encrypted Call Recording: AEAD_AES_128_GCM and AEAD_AES_256_GCM.
- **UTA Appliance RPMs/Packages Signed with a Certificate**—Installation of the UTA Appliance is now signed by a certificate.
- **Update AES Encryption**—Communication between the ETM Management Server and ETM System Console now support additional AES cypher suites.
- **Updated Linux Version for the UTA Appliance**—The UTA Appliance operating system has been updated to Oracle Linux 9. No other Linux versions are supported in this release.

Issues Resolved in v10.3.0

- **Issue #187249055**—**PREP** and **EXPAND** sections are now supported by the UTA Appliance Dialing Plan.
- **Issue #187930768**—**techsupport.sh** script sometimes caused disk space to be exhausted.
- **Issue #188111749**—UTA: Terminated Ghost Calls stay active in the Call Monitor and do not get logged as ended on the Management Server.
- **Issue #188398534**—Appliance messages received at the Management Server are sometimes delayed, causing delayed Call Monitor and ASCII Management Interface (AMI) output.



Special Configuration Instructions

- **Upgrading from a previous version—**
 - You must have v8.3.0 or later installed prior upgrading to v10.3.0.
 - You cannot upgrade the UTA Appliance from a previous version, due to the operating system upgrade. You must uninstall the previous version and then install the 10.3.0 UTA Appliance.
 - When upgrading deployments from a previous version that use LDAP Authentication, prior to upgrading to v10.3.0, include Default Authentication on one or more administrator accounts. Default Authentication may be needed to log in to the system after upgrade, and then reconfigure LDAP Authentication.
 - **Follow published upgrade instructions—**Ensure that you obtain and follow published upgrade instructions. See the SecureLogix Knowledgebase 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.
- **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
```
- **Collection Server search database—**The ETM Collection Server uses a database to store Call Recording information. 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**—A Windows feature called User Account Control (UAC) 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, install the ETM System in a directory that is not a system directory (for example, not in Program Files).
- **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 v10.3.0

- **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.

- **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.
- **Issue #187729082**—The **Show Hourly Statistics** button is not displayed in the **Call Recording Status** section of the Call Processor **Health & Status** window until the Call Processor is restarted.
- **BAMS**—The BAMS feature is no longer supported.

Version History

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

Last Update: 11/1/2024



SecureLogix Corporation

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

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

ETM, We See Your Voice, SecureLogix, SecureLogix Corporation, and the SecureLogix Emblem are 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 2018-2024 SecureLogix Corporation. All Rights Reserved.

SecureLogix technologies are protected by one or more of the following patents: US 11,349,987 B2, US 11,356,551 B2, and US 11,647,114 B2.