



Knowledge Base Article #ETM481

ETM[®] (Enterprise Telephony Management) System v7.2.0 Build 51 Release Notes

This document contains important information about release 7.2.0 Build 51 of the ETM[®] 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 v7.2.0

AS-SIP Support—The ETM System now supports Assured Service-Session Initiation Protocol (AS-SIP) with the Unified Trunk Application (UTA). This provides the ability to monitor, manage, alert, and record calls of interest in real time on AS-SIP trunks across local or distributed Department of Defense (DoD) networks.

Updated Java Version—The Java JRE used by the system for the ETM Management Server and Client applications has been updated to Java 1.8 Update 162. When upgrading an existing system, both Management Server/Report Server systems and Client systems must be upgraded. v6.3.0 Clients will not connect to a v7.2.0 Management Server.

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 available as 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. A per-Span configuration option is also available to store mid-call DTMF digits for each monitored call in the ETM Database for offline analysis. When this option is enabled, the interdigit timing of the digits is also stored with the pattern 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.

Enhanced Policy Installation—ETM Policy installation has been enhanced to complete on average 10 times faster than in previous releases.

Enhanced Call Monitor—The Call Monitor has been enhanced with complex filtering, performance improvements, and additional statistics.

MTU Configurability—The interface MTU is now configurable via an ETM Command on the Card: The **ethconfig** command allows for setting the MTU, auto-negotiation, duplex mode, and speed.

64-bit Windows Management Server Support—The ETM Management Server now supports only 64-bit OSs and runs in 64-bit mode. Previous versions could only be run in 32-bit mode. Due to the upgraded JRE included in this release, the ETM Management Server, Report Server, and Client applications are no longer supported on 32-bit systems.



Diagnostic Log Restricted to Admin Users—Viewing the **Diagnostic Log** now requires the **Manage Server** user permission.

Ability to Throttle Rule-Fired Alerts—The ETM Server now supports threshold-based throttling of Rule-fired Track messages. (Applies to Real-Time Alert, SNMP, SYSLOG, and Email Tracks. Logging always continues as normal.)

Checksum Files for Card Software Packages—There is now a corresponding **sha256** checksum file for each Card software package (for example, **ETM_5003_7.2.358.pkg.sha256** corresponds with the **ETM_5003_7.2.358.pkg**.) The corresponding checksum file must be present in the **pkg** folder in order to push a package down to a Card. To ensure the integrity of the software package file, the Management Server computes the checksum of the package file when software installation is initiated to make sure it corresponds to the checksum in the **sha256** file.. If they do not match, the package file will not be pushed and an error will be logged.

Last Login Time Displayed on Login—When a user logs into the system, a popup appears showing that user's last login time.

Logging Improvements— User access to System Properties/Tools/Reports is now logged. Failed login attempts are now also logged to the **Diagnostic Log**. Unnecessary filenames/paths/variables have been removed from logs.

Uniqueness of Changed Password Enforced—Password changes now require an 8-character difference from the previous password.

Updated UTA Appliance Package—The UTA Appliance package has been updated to build 367 to modify certain file permissions, address a call recording memory leak, and address issue #ETM-27422, described below.

Issues Resolved in v7.2.0

- ETM-18155—ORA-00060 Deadlock Error in System Error Log.
- ETM-26523—Reports: CDR Importer Calls were not displayed if the Card field was included.
- ETM-26383—DBT: The **View All Tasks** menu item under **Repository | Managed Databases** was enabled when a Standalone database was selected.
- ETM-26840—CDR Importer stopped working and purging of processed files failed
- ETM-26832—Directory Manager: Could not search for listings containing alpha access codes.
- ETM-26815—High-speed fax calls sometimes got Undetermined call type.
- ETM-27148—Switch Configuration changes were not properly pushed down if SMDR Provider was configured.
- ETM-27113—Null Pointer Exception when user entered an invalid username/password.
- ETM-27079—Removed Oracle Error Number 604 from the list of **DBShutdownCodes**.
- ETM-26983—Reports: The Local Start & End Times are now represented in reports in the Appliance's Time zone.
- ETM-26964—Appliance disconnected due to MTU mismatches.
- ETM-26849—Reports: Filter based on the Span for CDR Importer calls failed.
- ETM-26661—ESC: When user account had been locked out, the user was presented with the 'Invalid login' message rather than an indication that the account is locked.



- ETM-18158—Restarted Collection Server failed to purge when Minimum Disk Space was not available.
- ETM-18154—Error log ws produced at span startup if no SMDR Extensions were defined.
- ETM-27018—Policy Matching failed for international numbers using NNP.
- ETM-27034— Policy Matching for Rules using a Directory Range failed for international numbers using NNP.
- ETM-27291—Enhanced Span Disconnected Event.
- ETM-27289—Reports: Grouping by Call Duration added 1 hour to all durations.
- ETM-27267—Reports: Group by Time caused report failure.
- ETM-27263—Call Monitor: Highlighted calls did not remain highlighted in non-Fixed Row Count mode.
- ETM-27261—Call Monitor's "Active Call Count" field may have been misleading.
- ETM-27248—Call Monitor: Viewing Multiple TDM spans in Fixed Row Mode showed no more than 24 channels.
- ETM-27236—Call Monitor displayed call data in an inconsistent manner.
- ETM-27296—The Call Monitor had a sorting issue.
- ETM-27315— When multiple copies of the Call Monitor were brought up containing the same span, different results appeared in the different monitor windows.
- ETM-27302—Calls showed different start times in reports. When grouping calls in a report, the calls were appearing with different start times depending on whether they were grouped by Start Time or Local Start Time.
- ETM-27308—Call type Undetermined was being shown as the value Unknown in Reports on calls on TDM circuits.
- ETM-27300—Null pointer exceptions were occurring in reports.
- ETM-27313—Duplicate scheduled reports occurred when editing a scheduled report. A second scheduled report was being created (as opposed to just the existing report being modified in place). Both reports executed at their scheduled times.
- ETM-27316—Sorting of Listings in Directory Manager was not working properly.
- ETM-27319—The ability to create shortcuts in Usage Manager was missing.
- ETM-27422—UTA: Call Recording Post processing Panic. The panic and other errors were caused by not properly handling “late” arriving media packets at the end of a call.
- Collection Server TSAP filter processing fixes—Some string handling changes were made for some file/path names to resolve an issue in which the Collection Server service would not run if the TSAP filter was selected.

Special Configuration Instructions

- **Upgrading from a previous version—**
 - You must have v6.3.0 installed prior upgrading to v7.2.0.
 - **Follow published upgrade instructions--**Ensure that you obtain and follow published upgrade instructions. See the SecureLogix Knowledgebase at



<http://support.securelogix.com/knowledgebase.htm> or contact SecureLogix Technical 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 in all instances for Deadlock prevention.

- **New permission required when upgrading from v6.3.0**—Of particular importance when upgrading from v6,3,0, a new permission is required release to facilitate the Deadlock prevention capability (see below). This permission is required on all ETM systems (even those in which Deadlock prevention is not activated) and must be granted prior to beginning the upgrade. To grant this permission, connect to the database as SYSDBA and grant **Execute** permission to the ETM user on the **DBMS_LOCK** package. For example, assuming the ETM System user account is **ETMUSER**:

```
GRANT EXECUTE ON DBMS_LOCK to ETMUSER
```

- **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_dhtable_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_dhtable_locks=true
```
- **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**—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:

```
-Dsmldr.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 v7.2.0

- **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.
- **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: 5/14/2020



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 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),
© Copyright 1995 Eric Young. All Rights Reserved.