Knowledge Base Article #ETM5761

ETM® (Enterprise Telephony Management) System v8.3.1 Build 105 Release Notes

This document contains important information about release 8.3.1 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 v8.3.1

- **AES Encryption**—Communication between the ETM Management Server, ETM System Console, and the UTA Appliance can now be encrypted with AES.
- **Upgraded log4j Logging Utilities**—The log4j logging utilities have been upgraded to log4j2.
- **Updated Linux Version for the UTA Appliance**—The UTA Appliance operating system has been updated to Red Hat Linux v7.
- **ESXi v7.x Support for UTA**—The UTA Appliance is now supported on ESXi v7.x.
- **Stored Password Encryption Method Updated**—Stored passwords are now hashed with SHA256.
- **Regex Filter/Search Support**—Filtering/searching on any string-based field in the Directory Manager and other tools now supports regular expressions.

Issues Resolved in v8.3.1

- **UTA CP/CRC synchronization issue**—On the hardened UTA appliance, if the Call Recording Cache (CRC) process was restarted, it got out of sync with the Call Processor (CP) process, and the two would no longer communicate properly. This prevented all subsequent Call Recordings from being processed and turned into .wav files. Prior to this fix, the workaround was to restart the CP, which would lead to the connection between the CP and CRC being re-synchronized.
- **ETM-27441**—The Media Proxy entered a divide-by-zero panic loop if the recorded call contained a large difference in packets due to silence suppression. This issue occurred when a call was transferred to a Cisco Unity VM system, which does not send silence packets during the time that it is recording a message. This packet discrepancy led to a panic loop when attempting to post-process the captured media.

Special Configuration Instructions

- **Upgrading from a previous version**—
  - You must have v6.3.0 or late installed prior upgrading to v8.3.1.
  - You cannot upgrade the UTA Appliance from a version to prior to v8.3.0, due to the operating system upgrade. You must uninstall the previous version and then install the 8.3.1 UTA appliance.
  - **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. Of particular importance for this release if you are upgrading from

v6.3, 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_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 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:

  ```
  -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 v8.3.1

- **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 https://support.securelogix.com/knowledgebase.htm, keyword "release notes."

Last Update: 9/11/2022

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