Knowledge Base Article #ETM67715

ETM® (Enterprise Telephony Management) System v11.0 Release Notes

This document contains important information about release v11.0 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.

New Capabilities in this Release

- **Updated Linux Version Support for the ETM® Server and Client Applications**—The ETM Management Server, Report Server, and Client applications now support deployment on Oracle Linux 9. No other Linux versions are supported in this release.
- **Updated Linux Version Support for the SIP Proxy Application**—The SIP Proxy Application now supports deployment on Oracle Linux 9. No other Linux versions are supported in this release.
- **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.

Issues Resolved in this Release

- **Issue #186226780**—SIP Proxy Appliance: If the Media Proxy is active, and the Signal Proxy is restarted (or panics), the active media ports (actively processing media packets for active calls) at the time of the restart are put into a quarantine state. These quarantined ports will not be used for subsequent media processing, even though they are used as part of new calls.
- **Issue #186469608**—SIP Proxy Appliance: IPS mid-call terminations based on Duration are not logged up to the Management Server. When IPS Policy mid-call terminations occur due to exceeding a specified duration, the termination does not get logged up to the Management Server. The call itself gets properly terminated, and the Appliance logs the Call End properly, the fact that the call ended due to a termination is not logged.
- **ETM-27451**—The Linux ETM System Console and Database Maintenance Tool GUIs exhibit slow responsiveness when performing various operations such as starting tools, selecting buttons, navigating between tabs, closing windows, etc.

Special Configuration Instructions for this Release

- **Upgrading from a previous version**—
  - You must have v9.0.0 or later installed prior to upgrading to v11.0.
  - Clients from previous versions cannot connect to a v11.0 Management Server. You must upgrade all remote clients to v11.0 before trying to use them to connect to the upgraded Management Server, due to the LDAP login enhancements.
  - You cannot upgrade the SIP Proxy Appliance to 11.0 from a previous version, due to the operating system upgrade. You must uninstall the previous version and then install the v11.0 SIP Proxy Appliance running Oracle Linux 9.
  - When upgrading deployments from a previous version that use LDAP Authentication, prior to upgrading to v11.0, 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 Knowledge Base at https://support.securelogix.com or contact SecureLogix Technical Support to obtain a copy.

- **New permission required when using an Oracle 18/19 database**—When using an Oracle 18/19 Database, a new permission is required. "GRANT CREATE JOB" to the User (or Run-As User if in use). This allows Scheduled Tasks in the Database Maintenance Tool to run properly for Oracle 18/19 Databases. This permission is added by default when using the ETM Database creation scripts (for any type of Database), but if you are upgrading from an older version of the ETM System with an existing Oracle 11/12 Database to an Oracle 18/19 Database and not rerunning the scripts, or are creating the Database manually without using the scripts, you must manually add that permission.
- **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) Windows 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).
- **Syslog messages now use UDP**—Due to the upgrade to log4j2, syslog messages will now use UDP rather than TCP transmission. If necessary, configure syslog servers to receive UDP-based syslog messages.
- **Error adding an authorized Card on a Linux Management Server**—In some instances on a Linux Management Server, an error occurs when attempting to add a Card to the **Authorized Cards** list, and the Management Server goes into Standby. To mitigate this issue:

  - **ETMManagementServer.cfg**—On the **switches** line, change **-Djava.awt.headless=false** to -**Djava.awt.headless=true**".
  - **ETMReportServer.cfg**:
    - On the **switches** line, append **-Djava.awt.headless=true** to the end of the line.
    - On the **RMID_Switches** line, append **-C-Djava.awt.headless=true** to the end of the line (notice -**C-D** for this switch).

  Restart the Management Server for these changes to take effect.
- **Verify several packages are installed on Linux Management Server installation**—During installation, several packages are not always installed on Linux systems that the ETM System needs: **libXpm**, **libXtst**, and **libXrender**. Verify that these packages are installed, and use a yum update if they are missing.
- **Configuring the Enhanced Java Security Policy**—A means to restrict Java processing to only the processing required by the ETM System has been implemented, using special configuration. See the following article in the Knowledge Base: #ETM57716—Configuring the Enhanced Java Security Policy in ETM® System v9.0.3. The instructions are the same for v11.0.

- **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® 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

-
- **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 SIP Proxy applications**—A Policy Disposition of **Redirected** is provided and appears as available for all application types. However, this Disposition is only processed for SIP Proxy 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.
- **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.
- **BAMS**—The BAMS feature is no longer supported.
- **ETM® Web Portal**—The ETM Web Portal is not supported in this release.

Current Application Versions as of this Release

- ETM Client and Server applications—11.0 Build 9
- Appliance packages:
  - UTA—8.3.1-153
  - SIP Proxy—11.0-27
  - All other Appliance types*—7.1.90

  **Does not apply to the EOL 1060.*

Version History

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

Last Update: 5/8/2024

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 • support.securelogix.com