Knowledge Base Article #ETM67718

ETM® (Enterprise Telephony Management) System v13.1.0 Release Notes

This document contains important information about release v13.1.0 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.

What's New in this Release

- **Updated Java Version**—The ETM® Management Server, Report Server, ETM System Console, and Database Maintenance Tool now use Java version 25, specifically Amazon Corretto 25.0.2.10.1.
- **Windows Server 2025 Support**—The ETM Management Server now supports deployments on Windows Server 2025.
- **Handling of SIP URIs that Include Parameters in the User Portion of the URI**—SIP URIs may include parameters, such as the verstat parameter, in the User portion of the URI. These parameters are now discarded when transforming the user portion of the SIP URI into an E.164 phone number.
- **Handling of the '+' Character in Dialing Plan**—The Appliance Dialing Plan was enhanced to read and use the '+' character within existing Dialing Plan functionality. This allows processing of phone numbers that include + as part of special digit strings, such as steering codes.
- **Nimbus Look & Feel**—The ETM System Console and Database Maintenance Tool now use the Java Nimbus Look and Feel when rendering GUI elements.
- **ETM Management Server Duplicate Instance Detection**—This now uses a port probe rather than a lock file.
- **Updated Security Procedures, Configurations, and Scripts**—Updated security procedures, configurations, and scripts have been created to further secure ETM Management Server and ETM System Client deployments for customers that require this enhanced security posture. The Enhanced Java Security Policy functionality from previous releases is no longer used.

Issues Resolved in this Release

- The appliance "restart purge" **ASCII Management Interface** command caused Dialing Plan files to be removed from the Appliance, and not automatically reloaded. This issue is now resolved.
- The Appliance "show status" **ASCII Management Interface** command would not show the correct number of active calls. This issue is now resolved.
- Dialing Plan files could become "lost" in various scenarios. Dialing Plan file recovery/reset mechanisms are now in place.
- A UTA Appliance race condition could occur between Call Recording completion and Collection Server upload that would cause the recording file to be changed to a ".bad" file extension. This issue has been resolved.

Special Configuration Instructions for this Release

- **Upgrading from a previous version**—
  - You must have v9.0.0 or later installed prior to upgrading to v13.1.

- After upgrading to version 13.1 from a version prior to 13.0, the new System ID associated with the Management Server must be used to obtain a new License File. To obtain the License file, provide your System ID to SecureLogix Technical Support and let them know whether you purchased the Call Recorder or the CIDA feature. The System ID is located in a file named **sysid.txt** in the ETM installation directory. If it is not present:
  - On Windows, change to the ETM installation directory and type **SysID.exe.**
  - On Linux, cd to the ETM installation directory and type **./GetSystemID**
- Clients from versions prior to 13.0 cannot connect to a v13.1.0 Management Server. You must upgrade all remote clients to v13.1.0 before trying to use them to connect to the upgraded Management Server, due to the Java update.
- You cannot upgrade a SIP Proxy or UTA Appliance running a version prior to 11.0 to 13.1.0, due to the operating system upgrade. You must uninstall the previous version and then install the v13.1.0 SIP Proxy or UTA Appliance running Oracle Linux 9.
- When upgrading deployments that use LDAP Authentication from a version prior to v11.0, before upgrading to v13.1.0, 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.

- **Configuring HTTPS for UTA**—See the following article in the Knowledge Base: #ETM57881—Configuring HTTPS for UTA in ETM® System v13.0.0. This document also applies to v13.1.
- **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).
- **Appliance command "slc reconfig"**—The appliance ETM/AMI command **slc reconfig** can be used to rebuild the appliance configuration files without going through a full appliance reconfiguration using the

/opt/slc/ETM_5000_configure.pl script. However, there are some items to be aware of when using this command:

- For SIP appliances, the command reads the **/opt/slc/etm-default-configsp.txt** file to generate the initial configuration. For UTA appliances, the command reads the **/opt/slc/etm-default-configcm.txt** file to generate the initial configuration. If the needed file is not present on the system, the "**slc reconfig**" command will fail. Those files are created when **ETM_5000_configure.pl** script is executed on an 11.1 appliance; however, appliances that were initially configured while an 11.0 appliance will create a file named **/opt/slc/etm-default-config.txt** (for both SIP and UTA). In order to run the **slc reconfig** command in this case, the **etm-default-config.txt** file must be renamed or copied to **etm-default-configsp.txt** (SIP) or **etm-default-configcm.txt** (UTA). For example, within the AMI tool, the command "slc mv /opt/slc/etm-default-config.txt /opt/slc/etm-default-configsp.txt" could be executed to rename **etm-default-config.txt** to **etm-default-configsp.txt**. The files can also be renamed or copied within the Linux shell.
- When the **slc reconfig** command is run, all of the appliance-only config items (items that are set by ETM/AMI commands and not from the Management Server GUI) will be reset to their default values. Therefore, items that may have been previously modified through ETM/AMI commands such as **netfilter**, **logmsg count**, **sip reject**, **tcp response**, **tcp timeout**, etc, will need to be reset. In particular, now that **netfilter** defaults to being disabled, it should be re-enabled to secure the appliance.
- When the **slc reconfig** command is run, the Dialing Plan file mappings within the appliance will also be lost. Therefore, the Dialing Plan files must be re-pushed to ensure proper Dialing Plan functionality.

- **Enable the Appliance firewall after installation and configuration**—Since Netfilter/Iptables will be disabled when the appliance is first configured, it must be enabled when configuration is complete. After getting the appliance set up and configured (and allowing access to particular Remote Hosts as needed), use the **netfilter enable** command to activate the firewall.
- **Syslog messages now use UDP**—Due to the upgrade to log4j2, syslog messages 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 mode. 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.
- **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. 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

- **Issue #189031047**—SIP/UTA: During package push within 11.1 or 13.x, it is possible to corrupt the backup config file on the SP/CM/MP. The **slc reconfig** command can be used to recover from this issue.
- **Issue #189031059**—Local variable initialization issues may prevent proper log content from being sent up to the Management Server: In some instances, local variable initialization errors may prevent call information from being properly sent up to the Management Server.
- **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—13.1.0 Build 23
- Appliance packages:
  - UTA—13.1-12
  - SIP Proxy—13.1-12
  - 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: 5/12/2026

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