Knowledge Base Article #ETM831

ETM® (Enterprise Telephony Management) System v7.1.3 Release Notes

This document contains important information about release 7.1.3 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.

IMPORTANT: The ETM System supports only 64-bit operating systems; 32-bit systems are no longer supported.

Changes in v7.1.3

Phone Number included in Adaptive IPS alerts—The phone number that triggered the Adaptive IPS Rule breach is now included in Realtime, Email, and Syslog alerts. (Not available in SNMP alerts.)

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.

Issues Resolved in v7.1.3

ETM-27409—The ETM Adaptive IPS feature sometimes failed to count calls of approximately 6 seconds or less in duration against the accumulations, so the phone numbers for such short-duration calls may not have been added to the blacklist. This has been resolved.

Known Issues in This Release

ETM-27433—SMDR Properties not added to the **Properties** table for database instances with names other than "ETM." Contact SecureLogix Technical Support for instructions for working around this issue.

Upgrade Instructions

See the following articles in the SecureLogix Knowledge Base:

- "ETM002 - ETM System v7.1.3 Upgrade Instructions for Windows"
- "ETM501 - ETM® System v7.1.3 Upgrade Instructions for Linux"

Note: To upgrade to this release, you must have v7.1.1 Build 41 or later installed.

Special Configuration Instructions for v7.1.3

- **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.
- **TCP Timeout for SIP Option Pings**—You can now set the TCP Timeout on the ETM SIP Appliance to a value greater than that set on your router to ensure Option pings are properly received and read. The default is 60 seconds.

  To modify the TCP Timeout value:

  – AMI into the Signaling Proxy node and issue the following command:

    set tcp timeout <*time_in_ms*>

    For example, to set the timeout to 90 seconds, the command would be:

    set tcp timeout 90000

To view the current TCP Timeout value:

- AMI into the Signaling proxy node and issue the following command:

  show tcp timeout

- **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) in Windows 7 and later and Server 2008 and later 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).
  - Disable the UAC feature on your operating system.

- **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).

- **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.

- **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

- **Hostname and BAMS configuration**—When specifying a BAMS server using an IP address, if the address is converted into a hostname, this hostname (instead of the IP address) must also be used in the **known_host** file that is used for enabling SSH communications with the BAMS server.
- **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, exacerbated by the Java Virtual Machine use of a SOCKS networking protocol that requires additional DNS lookups.

  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>
- **For graduated SIP software upgrades, Call Recording functionality requires components to be upgraded in a specific order**— If you want to upgrade one SIP Appliance proxy component first and let it run for an extended amount of time before upgrading the other proxy component, then the Signaling Proxy should be the first upgraded to ensure media continues to be anchored. This is not an issue if both components are upgraded in a timely manner.
- **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**

- **UTA supported in a Single Application Configuration Only (No HA)** —UTA is only supported in a single node configuration in which the Call Processor, Signaling Processor, and Media Processor reside on a single appliance or router blade.
- **Oracle XE**—Run-As users and Database Repositories are not supported on Oracle XE.

Known Limitations in v7.1.3

- **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.
- **Usage Manager "Save to Tree"**—On Windows if the Management Server is installed using the Local System account, using **Save to Tree** to save a report causes an exception to be produced and the operation fails. Also, after selecting a Report in the tree and then selecting **Print**, **Preview**, or **Save As**, the Management Server takes an exception and goes into Standby mode and the operation fails.

  To avoid this issue if your organization uses the **Save to Tree** feature:

  - Install the Management Server using an actual Windows user account rather than the Local System account.
- **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 inline SIP applications**—A Policy Disposition of **Redirected** is provided and appears as available for all application types. However, this Disposition is only processed for inline SIP applications.
- **Web Portal**:
  - **Collection Server search results show Undetermined for calls with multiple call types**—During a Web Portal search for calls on a Collection Server, if recordings exist that contain multiple call type values, the call type field for these calls in the search results shows "Undetermined".
  - **Java Heap Space Exception for large query result (thousands of calls)**—If a large number of calls (thousands or more) match a search via the Web Portal (CRC or Collection Server), a Java Heap Space exception may occur. To resolve this issue, initiate a new Web Portal session and repeat the search using a smaller start time range to reduce the number of matching recordings.
  - **Retrieval of Compressed Recordings with Chrome only**—f recordings are being compressed at the Collection Server, they cannot be previewed or retrieved via the Web Portal. If you are using compressed recordings on the Collection Server, use Firefox or Internet Explorer to search for and access recordings from the Collection Server.
  - **Collection Server search results do not provide .wav file size**—Web Portal results for call recordings stored on a CRC display the size of the **.wav** file. This field is left blank for Collection Server search results. Filtering based on **.wav** file size when searching a Collection Server is ignored (those filter criteria will not be used).
  - **Web Reports no longer supported**—Although reporting options are still presented in the ETM Web Portal, they are no longer supported.
  - **Web Portal navigation issues**—Web Portal page navigation during a recording search causes the search to start over and the navigation is ignored; Previous search results or error messages remain displayed

when performing a new search or changing to a new Call Recording Device; Web Portal **Reset** button issues; Web Portal version mismatch error is displayed upon logout, rather than login (This is cosmetic).

- **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.
- **Inline SIP Appliance CRC and Span System Statistics are inflated**—The SIP Span CRC system statistics value for **Recordings in Progress** and the UTA and SIP Recording Span statistics value for **Active Recordings** do not get updated properly for recordings that are attempted, but do not actually proceed. Therefore, these values may be greater than the actual number of active recordings. On UTA, the CRC **Recordings In Progress** value always reflects 0.
- **Inline SIP Call Recording Threshold Detector calculation issue**—Erroneous values are generated for the Call Recording threshold detector on SIP Spans.
- **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.
- **IP Subnets not correctly applied in Call Recording Policies on Inline SIP Spans**— Call Recording policy processing on inline SIP Spans does not match on **IP Subnet** values in the **Source** or **Destination** column. Do not use Subnets in Call Recording Policies on inline SIP Spans.
- **Inline SIP Call Recording files corrupted if 3DES Encryption is disabled**—If you are using Call Recorder on inline SIP appliances, ensure you have encryption enabled.
- **Inline SIP and UTA Call Recording limits**:
  - G.711 and G.729 codecs only
  - Single stream only (last one in SDP list for multiple audio streams)
  - Limit of 100 simultaneous recordings on ETM SIP and UTA appliances
  - Limit of 50 simultaneous recordings on UTA on the ISR service module.
  - Local CRC only
- **UTA: Tracking of non-phone number URIs**—Depending on ISR/ASR configuration, calls that use non-phone number URIs (the user portion of the URI does not contain a phone number) may not by tracked by UTA.
- **IPv6 not supported when UTA installed on a service module in the router**— When installed on a service module in the router, UTA does not support IPv6.
- **CAC Card Login under Windows 64-bit and Linux OS**—CAC Card login is not supported when running the ETM Management Server under Windows 64-bit systems or Linux systems.
- **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.

Version History

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

Last Update: 6/22/2020

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 • https://support.securelogix.com