Knowledge Base Article #ETM4931
ETM® (Enterprise Telephony Management) System v6.1.2 Release Notes

This document contains important information about release 6.1.2 of the ETM® System. The ETM System includes the ETM Communications and Application Appliances, ETM Server software, and the ETM applications: the Performance Manager, the Voice Firewall, the Usage Manager, AAA Services for the Voice Firewall, the Voice IPS (Intrusion Prevention System), and the Call Recorder.

Changes in v6.1.2

Performance Monitor—A new Performance Monitor Tool, launched from the ETM System Console, provides a dashboard view of the health and status of the Appliances/Spans so issues can be quickly identified without the need to open the Performance Manager. Right-clicking a resource in the Performance Monitor provides a menu of options for further troubleshooting and corrective action.

Syslog Alert Tool—The Syslog Alert desktop popup tool automatically visually alerts security personnel by a desktop popup any time the ETM System generates a 911 alert, or other types of Syslog alerts of interest. This is a separately licensed application.

Authorization/Access Code Support for Station-Side CDR Import—The Station-Side CDR Import feature has been enhanced to support importing SMDR access codes from the CUCM flat file or other SMDR to enable departmental billback on these records. Additionally, the Directory Manager now supports alphanumeric values for manually defined Access Codes.

Database Repository support— Multi-instance database support now ensures the data in databases from different servers can be consolidated using an external tool, to allow data warehousing without data contention.

Issues Resolved in v6.1.2

- ETM-26319 Spans added to newly created switch get into disconnect cycle
- ETM-26315 Outbound media dropped after SIP session refresh
- ETM-26295 Error creating a new CDR Importer: 'ORA-02289: sequence does not exist'
- ETM-26294 Restarts due to time and timezone changes
- ETM-26293 Pre-6.0 to 6.1.1 Upgrade fails for crc_application table
- ETM-26292 Card replacement results in call records associated with that card becoming unavailable for reporting
- ETM-18563 SSB: HA: MP has no failover capability based on port carrier status
- ETM-18203 Restarting the ETM Services clears the Disable Real-Time SMDR Data Correlation checkbox
- ETM-18200 5160 CRC panics and does not recover
- ETM-26349 Outbound SMDR Requests not being made from Firewall Policy

Special Configuration Instructions

Database Maintenance Tool—Prior to beginning the upgrade, note Database Object connection information. When you upgrade to this release, existing Database Objects in the Database Maintenance

Tool are removed and must be redefined after the ETM Software is upgraded. This is due to the changes for Database Repository support. When recreating the Database Objects, a new field called Database Schema must be populated. For a standalone database (not a Repository), set this field to the username of the database (the same name you use to log into the database). For information on using Database Repositories, see the SecureLogix Knowledgebase at http://support.securelogix.com, keyword "repository".

Web Portal Installer—Ensure you stop the Apache Tomcat service prior to upgrading the Web Portal application, or the **webetm.war** file will not be replaced, and the old version of the Web Portal will still be installed.

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.

Upgrade 1060 CRCs first—When upgrading appliances to v6.1.2, 1060 CRC appliances should be upgraded prior to other appliances. This ensures proper configuration of the Enhanced Protected Extensions feature.

New NIC driver requires appliance reboot—v6.1.2 SIP appliances include a Network Interface Card driver that facilitates high capacity networking, and thus allows a larger number of simultaneous SIP calls. In order to load this new NIC driver, the SIP appliance must be rebooted following upgrade to v6.1.2.

Last Resort—In order to support the Last Resort feature using IPv6 on a given appliance, the 6.1.2 P2 package must be installed on that appliance.

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 Vista, Windows 7, or Server 2008—A feature called User Account Control (UAC) was introduced in Windows Vista and Windows Server 2008 that 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 one of these operating systems:

- Ensure 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.

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 1.5 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

SMDR recording file lock—When recording 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 natted. 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**

Web Portal Installer limitation—When upgrading the Web Portal, since the installer does not create **jakarta-tomcat-5.5.9\webapps\webetm** directory, it is not replaced by the installer. To work around this issue:

1. Stop Tomcat.
2. Install the upgrade.
3. Copy <install_dir>\jakarta-tomcat-5.5.9\webapps\webetm\WEB-INF\server-defn.xml file to a safe directory.
4. Delete the **<install_dir>\jakarta-tomcat-5.5.9\webapps\webetm** directory.
5. Start the Tomcat service.
6. Copy the original server-defn.xml file back into the new WEB-INF directory,
7. Restart the Tomcat service.

Known Limitations in v6.1.2

Web Portal—

- Undetermined shown for multiple call types —When searching for calls on a Collection Server in the Web Portal, if recordings exist that contain multiple call type values, the call type field in the Search results for these calls 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.
- Preview of Compressed Recordings Fails—If recordings are being compressed at the Collection Server, previews of these recordings using the Web Portal will sometimes cause an error in the media player indicating that the wav file is corrupt. The preview media is played properly even when this error occurs. The problem does not occur when compressed recordings are played in their entirety.
- 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 results. Filtering based on wav file size when searching a Collection Server is ignored (the filter criteria will not be used).
- Preview fails for calls less than 10s. If you attempt to preview a recording from the Collection Server using the Web Portal and the recording is less than the preview length (default of 10 seconds), the recording will not download properly. The file will download and play properly if the play option (entire recording) is selected.

SIP Media Timeout Rule does not fire properly if the action is Terminate—If a Media Timeout attribute is added to a Firewall policy rule and the action is Terminate, the rule will not properly fire when matched. The rule firing will not be logged and the termination will not be attempted.

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 you reinstall the Policy.

SIP Appliance CRC and Span System Statistics are inflated—The SIP Span CRC system statistics value for **Recordings in Progress** and the 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.

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 SIP Spans— Call Recording policy processing on SIP Spans does not match on IP Subnet values in the **Source** or **Destination** column. Do not use Subnets in Call Recording Policies on SIP Spans.

SIP Call Recording files corrupted if 3DES Encryption is disabled—If you are using Call Recorder on SIP appliances, ensure you have encryption enabled.

SIP Call Recording limits—

- G.711 and G.729 codecs only
- Single stream only (last one in SDP list for multiple audio streams)
- 30 simultaneous recordings max
- Local CRC only

IPv6 not supported on the SIP AXP solution—AXP blades do not support IPv6, and therefore IPv4 must be used for addressing of the blade itself and of SIP Trunks on a SIP AXP application.

Version History

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

Last Update: 8/22/2011

SecureLogix Corporation

13750 San Pedro, Suite 230 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • http://support.securelogix.com