ETM® System

Knowledge Base Article #ETM035

Upgrading to v7.1.1 Build 41 from v5.2.x or Later of the ETM® System on Windows

Synopsis

This article explains how to upgrade to v7.1.1 build 41 from v5.2.x or later of the ETM® System on Windows. If you are upgrading from an earlier version, contact SecureLogix Customer Support before beginning the upgrade.

****

IMPORTANT NOTES

- Ensure that you are running a supported version of Oracle before you continue. Oracle 10g v10.2.0.1 or later (Enterprise, Standard, or XE) and 11g R2 (Enterprise, Standard, or XE) are supported.
- If you upgraded from one version of Oracle to another prior to beginning the ETM System upgrade, ensure that you replaced the ODBC driver in the ETM Software installation directory with the upgraded Oracle driver version. This includes Oracle patch updates. Copy **ojdbc14.jar** (10G) or **ojdbc6.jar** (11G)—from **<ORACLE_HOME>\jdbc\lib** to The ETM System Installation directory.
- **<INSTALL_DIR>** is used in these instructions to refer to the directory where the ETM System is installed. By default, the ETM Applications are installed at the following path: **C:\Program Files\SecureLogix\ETM**. Your installation location may vary.

****

Steps

1. **Connect to the database via the Database Maintenance Tool.** Verify that no errors exist before beginning the upgrade. If errors are present, contact SecureLogix Customer Support before you continue. See the *ETM® System Administration Guide* for instructions for using the Database Maintenance Tool, if necessary.
    - Due to a new feature introduced in v7.0.0, if you are upgrading from a version prior to that, the Database Object in the ETM System Console is lost upon upgrade and must be recreated. Before you begin the software installation, note the following information:
        a. Server IP Address
        b. Port Number

SecureLogix
We see your voice™

c. Database Name*

d. User Name*

e. Password*

* This information can be found in the **twms.properties** file in the **<INSTALL_DIR>**. Locate the lines that read:

```
## The instance name

## The user id to log into the database

## The passphrase to log into the database.
```

2. **Shut down any running ETM System applications.**

   - Shut down all ETM Management Server and Report Server instances, using the Windows Services Control Panel.

   - If multiple ETM Management Server or Report Server instances are running on the machine, deregister all application instances with the Service Control Manager using the **AppManager.exe** utility as follows:

     a. Open a command prompt window and change to the ETM Server installation directory.

     b. Obtain a list of the registered application instances by typing the following at the prompt:

     ```
     AppManager /list /type:both
     ```

     c. For each instance ID in the list, type the following command at the prompt:

     ```
     AppManager /remove /type:both /ID:<instance_id>
     ```

3. **Install the ETM System v7.1.1 build 41 software**. Run the installer (**setup.exe**) from the software CD and follow the onscreen prompts. The installer automatically removes the previous version and backs up certain files that may have been user-modified.

   - **IMPORTANT** Be sure to upgrade all remote ETM System Clients before trying to use them to connect to the upgraded ETM Server.

   - When the ETM Management Server is uninstalled, the following files are automatically backed up from the <INSTALL_DIR> to the <INSTALL_DIR>\Backup\MS_<DATE_TIME> directory:

     – **delivery.properties**

- **ETMManagementService.cfg**
- **npconfig.properties**
- **PagerService.properties**
- **smdr.properties**
- **twms.properties**
- **\ps\software_repository\smdr**—Entire directory, which contains the SMDR parse files. If a file with a default name has been user-modified, it must be restored to the ETM Server **<INSTALL_DIR>\ps\software_repository\smdr** directory after upgrade. User-defined files with custom names are not deleted nor overwritten during upgrade and therefore do not need to be restored.
- **\ps\software_repository\ini**—Entire directory, which contains the Dialing Plans. Upon upgrade, the Dialing Plans installed on the Appliances are not deleted, but user-modifications to the Dialing Plans need to be copied to new Dialing Plan file in the **<INSTALL_DIR>\ps\software_repository\ini** directory on the ETM Server and then reinstalled on the Spans.

- When the ETM Report Server is uninstalled, the following files are automatically backed up to the **<INSTALL_DIR>\Backup\RS_<DATE_TIME>** directory:
  - **ETMReportService.cfg**
  - **twms.properties**

  Refer to the *ETM® System Installation Guide* for detailed software installation instructions, if necessary. PDFs of all of the ETM System user guides are located on the ETM software CD in the top-level **Documentation** folder.

4. **Restore custom configuration files.**

   - Use a tool such as **CompareIt** to identify customization in the backed-up **.properties**,**. cfg**, and **.ini** files listed in step 2. Copy those changes into the newly installed files so that any updates in the files are retained. Do not copy over the new files, because they may contain new settings for this release.
   - **SMDR parse file**—Copy the custom SMDR parse file(s) to the **<INSTALL_DIR>\ps\software_repository\smdr** folder (*not necessary if the files had custom names, since they were not overwritten nor deleted*).

5. **Upgrade the database.**

   a. **New permission required when upgrading from a version prior to 7.0.2**—Of particular importance when upgrading from a version prior to v7.0.2, 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 Server user on the **DBMS_LOCK** package. For example, assuming the ETM Server user account is ETMUSER:

   ```
   GRANT EXECUTE ON DBMS_LOCK to ETMUSER
   ```

   To verify that the permission was successfully granted, type:

   ```
   select * from dba_tab_privs where table_name='DBMS_LOCK';
   ```

   b. **Run As User must be granted CREATE SEQUENCE permission**—If you are using a run-as (non-owner) database account for the ETM Server, PRIOR TO BEGINNING THE UPGRADE, grant that account

   ```
   CREATE SEQUENCE
   ```

   permission or the Call and Policy Log tools will be unavailable. Also grant the following additional permissions to that account:

   ```
   ALTER SESSION
   CREATE PROCEDURE
   CREATE SESSION
   CREATE MATERIALIZED VIEW
   CREATE TABLE
   CREATE VIEW
   ```

   c. Start the ETM Database Maintenance Tool

   d. Create a new Database Object using the information you noted in step 1, if you are upgrading from a version prior to 7.0.0 (If you are upgrading from 7.0.0 or later, see the next step).

      i. Expand the **Systems** node.

      ii. Unless otherwise instructed by SecureLogix personnel, right-click **Standalone Databases** and select **New Standalone Database.**

      iii. Type the Server IP Address and port noted in step 1.

      iv. In the **Database Instance** box, type the Database name noted in step 1.

v. In the **Database Schema** box, type the user name noted in step 1.

e. Connect to the database using the user name and password noted in step one.

f. You are prompted to upgrade the database. Click **Yes**. (If any errors occur while upgrading the database, note the error and call Customer Support at the number at the bottom of this article.)

g. Right-click the data instance the ETM Server uses and click **Set as Default**. (Not necessary if you returned the backed up **twms.properties** file to the **<INSTALL_DIR>**, since that information is already included in the file.)

6. **Recreate multiple Management Server and Report Server instances, if these are used.** If multiple instances of the MS and RS are in use, use the **AppManager** utility to recreate the instances removed in Step 1. Refer to *"*Creating Multiple Application Instances" in the *ETM® System Technical Reference* for detailed instructions.

   - If multiple instances were in use before the upgrade, the instance-specific **twms.properties** files were not changed nor deleted and therefore should require no modification. Recall that the values in the global **twms.properties** file are used unless explicitly overridden by a value in the instance-specific file; therefore, any new fields in the global file are implemented in the instances. If a specific instance needs a different value, specify that value in the instance-specific file. If all instances need a different value, you can change it once in the global file and it will apply to all instances.

7. **Start the ETM System applications and verify operation.** Perform the following for each set of Server instances:

   a. Start the ETM Server and Report Server. Check for errors in the **error** and **serverfatal.log** files. The **server-fatal.log** is stored in the root of the **<INSTALL_DIR>** and is only present if the ETM Server terminates unexpectedly. The error logs are stored in the **<INSTALL_DIR>\ps\errors** directory.

   b. If no errors appear, start the ETM System Console, log in to the Server, and then open the Performance Manager.

   c. Verify that all Cards have reconnected and no errors are present. If errors are present, contact SecureLogix Customer Support for assistance before continuing.

8. **Upgrade the Card software.** After the Cards connect to the Server, upgrade the Card software.

   IMPORTANT:

   - ETM 1010, 1020, 1030, and 1040 Appliances cannot be upgraded to v7.1.1 and have not been tested nor warranted to work with the 7.1.1 Server. The last release that supported connections

from these Appliances was v5.2.

- It is imperative that you do not reboot or power cycle the Card while the software is being downloaded until the upgrade and software installation is complete, or the firmware may become corrupted, rendering the Card inoperable and requiring Last Resort Card recovery. The Card automatically reboots when the upgrade is complete. If you believe the Card has become unresponsive, be certain that 15 minutes have elapsed since you began. If possible, connect via the Console port and call SecureLogix Customer Support. Do not manually power cycle or reboot the Card.

- How long a Card upgrade takes varies depending on the size of the package and which firmware devices are being reprogrammed. During a Card upgrade, the compact flash (hard drive) is first reprogrammed; and then, depending on the upgrade, the boot flash and one to six other firmware devices may be reprogrammed. The firmware devices are verified against the new code; if different, they are reprogrammed. Verification can take from 20 to 120 seconds per device (depending on the size of the device) and reprogramming can take from 30 to 240 seconds per device.

- **Upgrade 1060 AND 5160 CRCs first—**When upgrading appliances to v7.1.1, 1060 and 5160 CRC appliances should be upgraded prior to other appliances. This ensures proper configuration of the Enhanced Protected Extensions feature.

- **Last Resort—**In order to support the Last Resort feature using IPv6 on a given appliance, Appliance package v6.1.79 or later must be installed on that appliance prior to beginning the upgrade.

- **IMPORTANT Information about upgrading the inline SIP application:**

  - **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 upgraded first to ensure media continues to be anchored. This is not an issue if both components are upgraded in a timely manner.

  - **Upgrading HA Appliances from a Version Prior to 7.0.0—**No automated remote upgrade is available for HA SIP appliance deployments running a version prior to v7.0.0. For instructions for upgrading appliances in an HA deployment, see the SecureLogix Knowledge Base, keyword “upgrade’. Remote upgrade of HA appliances running v7.0.0 or later is supported.

  - When installing software on an inline SIP Appliance, additional steps are required compared to other appliance models. You first push the software package to the Call

Processor at the Card level, which then makes it available on the signaling and media proxy nodes. You must then activate the new software on each of the proxy nodes.

For instructions, see “Upgrading 5000 Series SIP Appliance Software” on the SecureLogix Knowledge Base at http://www.securelogix.com/support/article.htm?articleid=APP606

- **IMPORTANT Information About Upgrading PRI NFAS and SS7 Spans**:
  - PRI NFAS and SS7 Spans on Cards running v7.1.1 cannot communicate with other NFAS PRI or SS7 Spans on Cards that are running prior versions. Therefore, it is recommended that all of the Cards whose Spans belong to a given NFAS PRI group or SS7 group be upgraded at the same time.

To upgrade the Card Software

a. Contact SecureLogix Customer Support to obtain the current versions of the Appliance software packages, released as Appliance-only updates. The current Appliance software versions are v7.1.50 for SIP and UTA, and v7.1. 49 for all other Appliance types.

b. Place the extracted files in the **<INSTALL_DIR>/SecureLogix/ETM/ps/software_repository\package** directory.

c. In the **Platform Configuration** subtree, right-click the Card, and then click **Manage Software**. You can upgrade multiple same-model Cards at once. The **ETM Platform Software Installation** dialog box appears.

d. Under the **Software Package** box, click **Modify**. The **Software Version Selection** dialog box appears, listing packages that apply to the selected Card type.

- For 1012 and 1024 Appliances, use the **ETM_1012_7.1.49.pkg**.
- For 1060 Appliances, select **ETM_1060_7.1.49.pkg**.
- For the 1090 Appliance, use the **ETM_1090_7.1.49.pkg**.
- For Signaling Link Cards, select **ETM_3070_7.1.49.pkg**.
- For 8240 Cards in the 2100 and 3200 Appliances, select **ETM_3000_7.1.49.pkg**.
- For 8540 Cards in the 2100 and 3200 Appliances, select **ETM_4000_7.1.49.pkg**.
- For 5000 Series SIP Appliances and the inline SIP application on the ISR module, select **ETM_5000_7.1.50.pkg**. (Ensure that you follow the instructions noted above in “Important Information About Upgrading the Inline SIP Application.”)

- For the Unified Trunking Application (UTA) regardless of platform, select the **ETM_5003_7.1.50.pkg**.

e. Click the software package to install, and then click **OK**. You are returned to the **ETM Platform Software Installation** dialog box.

f. Be sure that the **Install** box is selected, and then click **OK**. The software is downloaded to the Card. You can view the progress of the upgrade in the **Status Tool** and **Diagnostic Log**.

9. **Update the CCMI file**. Download the new CCMI file from the SecureLogix website, place it into the ETM Directory, and import the new CCMI file: https://support.securelogix.com/ccmi_login.htm

10. **Upgrade dial plans to 7.1.1.** Copy the user modifications into the new v7.1.1 file and install it on corresponding Spans.

11. **Remove backup files.** When the upgrade is complete and the ETM System is verified to be operating correctly, both manually and automatically created backup directories can be deleted to free the hard drive space they use.

12. **Upgrade the ETM® Web Portal, if Used.**

- **Web Portal Installer**—Ensure that 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.

- **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:

a. Stop Tomcat.

b. Install the upgrade.

c. Copy **<install_dir>\jakarta-tomcat-5.5.9\webapps\webetm\WEB-INF\server-defn.xml** file to a safe directory.

d. Delete the **<INSTALL_DIR>\jakarta-tomcat-5.5.9\webapps\webetm** directory.

e. Start the Tomcat service.

f. Copy the original **server-defn.xml** file back into the new **WEB-INF** directory,

g. Restart the Tomcat service.

13. **Upgrade the ETM® Collection Server (if Used).**

- **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 (which 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 upgrade 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.

NEXT STEPS

- If you purchased the Caller ID Authentication (CIDA) feature, refer to the *ETM® System Caller ID Authentication (CIDA) Guide* for instructions for licensing and configuring the feature. (**Note**: The CIDA feature is only supported onT1 PRI on the 3200 and 2100 appliances.. It is not supported on the 1090.

- Refer to the *ETM® System Administration and Maintenance Guide* for instructions for configuring the Enhanced Policy Push feature.

- Refer to the 7.1.1 Build 41 Release Notes in the SecureLogix Knowledge Base for instructions for configuring Deadlock prevention and for other special configuration instructions: http://download.securelogix.com/library/ETM888-ETM_System_v711_Release_Notes.pdf.

Last Update: 1/29/2015

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 • http://support.securelogix.com

SecureLogix
We see your voice™