UtilityIQ 6.0 Installation Guide

Advanced Metering Manager

Firmware Upgrader

Meter Plugins

Meter Program Configurator

UtilityIQ 6.0 Installation Guide
February 28, 2025
REV 000
6.0

Confidentiality notice

Trademark notice

Contact us

For more information about Itron or Itron products, go to:

Email: support@itron.com

Itron Customer Center: customer.itron.com

Products and documentation: products.itron.com

Itron Technical Support North America: 1-877-487-6602

For regional technical support, go to www.itron.com and select your country and language.

For suggestions, questions, or other feedback concerning Itron product documentation, contact us at: ItronDocumentation@itron.com.

Contents

New in this document

Revision	Date	Description
REV 000	November 1, 2024	First date of publication.

1 Overview

This document describes how to perform a fresh installation of the following products that are part of the UtilityIQ 6.0 core product family:

- Advanced Metering Manager (AMM) with its associated applications
- Meter Plugins
- Firmware Upgrader (FWU)
- Meter Program Configurator (MPC) with its associated applications

These products must be installed in an environment that is already running shared service components. See Installation prerequisites on page 11 and the *SSC Installation Guide* for more information.

> To make sure you have the correct versions of software, refer to the *GenX Compatibility and Requirements Matrix* before beginning your installation. That document specifies supported versions for all Itron and third-party products.

Other products have their own installation documents. See Related documentation on page 10 for a list of documents you may be interested in.

The file `croc-cli`, which may be part of your UtilityIQ software package, is the part of the software that allows AMM to communicate with Communications Module Utility (CMU). Refer to the *Communications Module Utility (CMU) User Guide* for more information.

Before you start

The software is to be installed on servers that have already been set up with a supported operating system and Oracle.

> **Important!** To make sure you have the correct versions of software, refer to the *GenX Compatibility and Requirements Matrix* before beginning your installation. That document specifies supported versions for all Itron and third-party products.

Directory structures and naming conventions described in this document correspond to those used by the Itron Operations team. Itron recommends that your organization use the same paths, structures, and names. Doing so means that Itron can provide more accurate support when needed. Fill out a Worksheet as discussed in Installation worksheet on page 76, to keep track of all of the elements that comprise your installation.

Some example commands are provided in this document. Your organization may want to develop scripts to facilitate the creation of certificates, configuration, and installation.

Itron highly recommends that you first install your entire set of applications in a test environment before cutting over to the production environment. Your test environment should replicate your production environment as much as possible including infrastructure, database, and testing of meters. It is important that you test the components for scalability and performance using the appropriate hardware resources.

For all considerations for application upgrades, refer to Upgrading to UtilityIQ 6.0 on page 70 .

Installation overview

Installation tasks on page 8 lists each of the installation tasks in the order they should occur.

It is recommended that before you start, you plan your entire installation and then gather all software packages, SSL certificates, security packages, and licenses at the same time. Refer to the documents listed in Related documentation on page 10 as needed.

Table 1 Installation tasks

Installation task	Instructions
1. Read through the *SSC 2.11 Installation Guide*. Make sure the hosts are ready for installation. You can install the SSC products during the same sessions as the UtilityIQ products.	*SSC 2.11 Installation Guide* and *GenX Compatibility and Requirements Matrix*
2. Gather all the host names, passwords, database user names, and other information you need and record it all in a spreadsheet or worksheet. You will use this information to populate properties files, create schemas, and configure. All of the information listed in this overview to your worksheet.	Installation worksheet on page 76.
3. Work with the DBA to create names and passwords for the database roles and application users.	*SSC 2.11 Installation Guide*
4. Obtain software files, including any needed keykeep files (for application-level security) and licenses.	Contact your Itron project manager.
5. Generate CSRs to obtain SSL certificates from Symantec (formerly VeriSign) or Comodo for applications that need them. Create SSL keystores to put into the `thirdparty/certs` directory.	*SSC 2.11 Installation Guide*
6. Create directory structure for all applications you intend to install, not just UtilityIQ.files	*SSC 2.11 Installation Guide*
7. Download software files to a storage directory called **sw** and unzip them into the **release** staging area.	*SSC 2.11 Installation Guide*
8. Install Tomcat and JDK onto each application server where they are needed.	*SSC 2.11 Installation Guide*

Table 1 Installation tasks (continued)

Installation task	Instructions
9. CinfigurationManager (*cfgmgr*)	*SSC 2.11 Installation Guide*
10. Install and start TIBCO EMS.	*SSC 2.11 Installation Guide*
11. Install CAAS (*caas*).	*SSC 2.11 Installation Guide*
12. Install DMS (*dms*).	*SSC 2.11 Installation Guide*
13. Install Registrar (*reg*).	*SSC 2.11 Installation Guide*
14. Install Trap Forwarder/Trap Receiver (*tmb*).	*SSC 2.11 Installation Guide*
15. Install Zing	*SSC 2.11 Installation Guide*
16. Install Trap Router (*traprouter*)	*SSC 2.11 Installation Guide*
17. Install Gateway	*SSC 2.11 Installation Guide*
18. (Optional) Install MQTT Broker	*SSC 2.11 Installation Guide*
19. Install Advanced Metering Manager (AMM) DB (*db*).	Installing the AMM database (DB) on page 22
20. Install GMR (*gmr*) and Meter Plugins (*meterplugins*).	Installing AMM Global Meter Reader (GMR) on page 25
21. Install AMM Middle Tier (*mt*).	Installing Middle Tier (MT) on page 37
22. Install AMMWSRoute (*ammwsroute*).	Installing AMMWSRoute on page 45
23. Install AMMJMSRoute	Installing AMMJMSRoute on page 46
24. (Optional) Install Firmware Updater (*fwu*).	Installing Firmware Upgrader (FWU) on page 48
25. (Optional) Install Meter Program Configurator (*mpc*).	Installing Meter Program Configurator (MPC) on page 57
26. Install all other products.	Refer to the separate installation guides for these applications, found at: **https://access.itron.com**
27. Start up all applications.	Starting and stopping applications on page 66

Audience

This guide is intended for an installation project team comprised of experts. It assumes that team members are certified, where applicable, and have thorough knowledge of and substantial experience with the following areas:

- Red Hat Linux or CentOS
- Multi-terabyte databases

- JMS server/TIBCO EMS
- Data center operations
- SSL certificates

Related documentation

You can find all Itron product documentation at products.itron.com in the Documentation & Release Notes section. Related documents you may find helpful are:

- *GenX Compatibility and Requirements Matrix* for the product family and version you are installing
- *AMM Integration Guide*
- *AMM Events*
- AMM, FWU, and MPC User Guides
- *Gateway Installation Guide*
- *HAN Communications Manager (HCM) Installation Guide*
- *Network Center Installation Guide*
- *ODS Installation Guide*
- *Ports and Protocols*
- Release notes for all of the products and versions you are installing
- *SensorIQ Installation Guide*
- *Shared Service Components (SSC) Installation Guide*
- *Sizing Guidelines for UtilityIQ*

2 Installation prerequisites

The following must be in place to install and run UtilityIQ:

- CNAMEs for the UtilityIQ hosts. This is in addition to existing SSC and other needed hosts.
- Supported version or versions of Java.
- Supported versions of shared service components (SSC). These can be installed during the same session as UtilityIQ; they need to run in order for UtilityIQ to run, but they do not need to run in order for UtilityIQ to be installed.
- All required software components for all of the products being installed.
- Google Maps API
- Oracle database setup
- SSL certificates and keykeep.store files and/or Hardware Security Modules (HSMs) for all applicable products.

CNAMEs

CNAMEs that resolve to the DNS server are required for all hosts.

In the current version of UtilityIQ software, Web service applications (that is, applications with the “wsroute” name) share the CNAME and SSL certificates and reside on the same host as the main product application.

Required versions of Java

All applications now come with an embedded version of Java, it no longer needs to be manually installed.

Software requirements

Shared Services Components (SSC) software

The following SSC components are required to run the UtilityIQ products discussed in this document. Refer to the *SSC Installation Guide* and the *GenX Compatibility and Requirements Matrix* for the products and versions you are installing.

You can either install and configure the SSC products first, or install all products at the same time. Follow the recommended start/stop order shown in Starting and stopping applications on page 66 before starting up the applications.

These are the SSC products required to run AMM, FWU, and MPC:

- Central Authentication and Authorization Service (caas)
- ConfigurationManager (Cfgmgr)
- Device Management Service (dms)
- Network Abstraction (NA) Proxy (naproxy)
- Registrar (reg)
- TIBCO Conf files. Always make sure you have installed the newest TIBCO Conf files whenever you install or upgrade.
- TIBCO Enterprise Message Service (TIBCO EMS)
- Trap Forwarder (tmb)
- Trap Router (traprouter)

UtilityIQ software

Software components required for a UtilityIQ core installation are:

- AMM Database (db)
- AMM Global Meter Reader (gmr)
- AMM Middle Tier (mt)
- AMMWSRoute (ammwsroute)
- AMMJMSRoute (ammjmsroute)
- Meter Plugins (meterplugins)
- FWU (fwu)
- MPC (mpc)
- MPCWSRoute (mpcwsroute)

If you are installing other components, such as Outage Detection System (ODS), Network Center, HAN Communications Manager (HCM), or SensorIQ, refer to their separate installation documents.

Google Maps API

The Google Maps API Client ID is required for displaying Google Maps in AMM. If your AMM application is hosted by Itron, there is no need to change the Itron-provided Client ID.

The Google Maps API comes with a key called a Client ID. This is the only key that works with the applications described in this document. Licensed and Managed Services customers who install and manage their own services can either provide their own Client ID, or contact customer support to request that their domain be added to the Itron Client ID

Refer to https://developers.google.com/maps/documentation/business for more information on acquiring the API.

The Google Maps API uses a number of domains for its Maps components, which may affect your organization's firewall configuration and prevent end users from seeing maps in applications including AMM and Network Center. Google provides a list of domains used by the Google Maps family. If you already obtained a Google Maps API for an earlier installation of AMM, it will work with the 6.0 installation, so you do not have to get a new Google Maps API.

Planning Oracle database schemas

About schemas

You do not have to create new database schemas for products that are being upgraded to 6.0. Instead, you will run the upgrade scripts at the end of the installation procedures to upgrade the existing schemas. If you are installing any new applications for the first time, you *create* schemas for those.

Schemas are created or updated after the software is installed and are generated automatically based on properties you configure in the properties files. If you are upgrading schemas from earlier versions, you can overwrite the properties to incorporate the original naming scheme. Keep a record of the user names, passwords, Oracle service name, database host name, and machine names for any schema created and add them to the Worksheet.

- The privileged user creates the schema owners, roles, and application users for all applications. The schema owner is granted the product owner role and has DDL privileges (defining the database structure or schema).
- The application user has DML privileges (managing data) within schema objects created by the schema owner.

Each schema has two possible roles. (These roles are created automatically when the application starts up. If you want to see the naming structure, review the properties files.)

- The "rw" role which has DML privileges on objects owned by the schema owner. The rw role is assigned to the application user.
- The "ro" role, which is read-only. The ro role can be granted to any user who needs read-only access to the data in the schema. Itron does not supply a script to create read-only users.

One owner and one application login is defined for each of the following:

- AMM. AMM requires an owner and application user for the master schema and any additional segments.

- CAAS
- DLCA
- FSU-SAM
- FWU
- MPC
- ODS

One owner is defined for each of the following:

- HCM
- NEC
- NEM
- SensorIQ

Your DBA must create tablespaces for all schemas.

The privileged user

Your DBA grants should have granted administrator privileges to create a privileged user who can perform schema creations during the software installation process. These privileges are often assigned to the SYSTEM user, for example. (This document will refer to this user as *privileged_user* in the commands where this level is needed).

Your previous installation should already have this user in place, either through the `uiqroot` script or by granting options to the SYSTEM user.

For each application that requires schemas, after the software has been installed, the privileged user creates schemas with the **create-schema** command to create the schema user, application user, and their associated roles.

The privileged user must be granted the following DBMS options:

```
GRANT SELECT ANY DICTIONARY TO &user_name with admin option;
GRANT RESOURCE TO &user_name with admin option;
GRANT create materialized view to &user_name with admin option;
GRANT create synonym to &user_name;
GRANT execute on dbms_utility to &user_name with grant option;
GRANT execute on dbms_stats to &user_name with grant option;
GRANT execute on dbms_lock to &user_name with grant option;
GRANT execute on dbms_job to &user_name with grant option;
GRANT execute on dbms_pipe to &user_name with grant option;
GRANT execute on dbms_lob to &user_name with grant option;
GRANT DEBUG CONNECT SESSION TO &user_name with admin option;
```

Creating a privileged user with uiqroot

In AMM, the **`cr_uiqroot.sql`** script creates a privileged user that has the above options granted, who is able to create or update schema user database rights and privileges.

To use **`cr_uiqroot.sql`** to create the user, you must do it after the database components of AMM have been installed and then come back to CAAS and DMS to create schemas using it.

The script will be located in `/usr/ssn/db/CURRENT/schema/oracle` after the installation.

The App user

Once schemas are created, the applications then access the database with the logins that have been created and the privileged user is typically no longer needed and may be locked. The app user will run **`upgrade.sh`** from `/usr/ssn/<component>/CURRENT/database/bin` to upgrade the schemas whenever necessary.

SSL Keystores

Many of the Itron applications require SSL keystores containing keys and SSL certificates obtained from your organization's Certificate Authority (CA). SSL certificates contain information about the certificate's owner to let the client browser know that the information coming from the Web server is trusted. The UtilityIQ applications that require CNAMEs also require SSL certificates.

See the *Shared Services Components (SSC) 2.11 Installation Guide* for information on all of the products that require SSL keystores.

If you are *not* planning to install the referenced software, you do *not* need to order an SSL certificate for it. If you have unexpired SSL keystores in place for the previous installation, you can use them in the current installation.

The first step in creating a keystore is to generate a CSR and submit it to a Certificate Authority such as Comodo or Symantec (formerly VeriSign). This can take some time, so it is a good idea to start the process as soon as you know you will be installing the products.

Important! Itron supports SSL certificates from Symantec and Comodo only.

After you receive the certificates, use procedures described in the *SSC 2.11 Installation Guide* to create keystores for each product that requires them.

The keystores are then put in `/usr/ssn/thirdparty/certs` in each associated host. The keystores must be in place before you start up the application.

Keykeep.stores or KeySafe for secure connections between devices and the back office

A `keykeep.store` keystore file or KeySafe (if using a hardware security module, or HSM) contains Itron private keys and certificates required for secure communication between the application server and endpoints (meters, APs, NICs, Relays, and other devices).

See the *Shared Services Components (SSC) Installation Guide* for information on all of the products that require keykeeps or HSMs.

For Customers Who Do Not Use KeySafe

If you do not use KeySafe, you should already have `keykeep.store` and `sckeystore.jceks` files from the previous installation. If they have not expired, they can be reused for 6.0. All of the secure associations from the previous installation must also be copied over to the 6.0 DATA directories as described for each installation section. See the *Shared Services Components (SSC) Installation Guide* for a list of all locations of files and SSL keystores.

The `keykeep.store` or `sckeystore.jceks` keystore is a file-based keystore that is a container of the Network Manager (NM) Entity, Permit, and Broadcast certificates, including all related private keys used for secure operations with grid devices and the back office. Itron provides the `keykeep.store` file to the customer.

Ask for the necessary `keykeep.store` files before you begin software installation. Typically, you use one file and copy it or soft-link to it for each application that needs the `keykeep.store` file. FSU-SAM and DLCA use the `jceks` format. See the *SSC Installation Guide* for information on installing a keykeep.

For Customers Who Use KeySafe

Your KeySafe administrator is responsible for creating a dedicated slot on the HSM for the certificate and private key. You must contact the KeySafe administrator to find out the slot ID and the slot PIN before you configure the applications to look for key material.

cs2_pkcs11.ini file for KeySafe

Your KeySafe administrator must give you a `cs2_pkcs11.ini` file to install on each host that requires communication with the HSM, as discussed in Keykeep.stores or KeySafe for secure connections between devices and the back office on page 16. The file should be installed at the following location in the directory structure:

```
usr/ssn/thirdparty/utimaco
```

If the path does not already exist, create it and copy the file into it when you receive it from the KeySafe administrator.

Export and add the environmental variable `CS2_PKCS11_INI` to the `.bash_profile.`

```
export CS2_PKCS11_INI=/usr/ssn/thirdparty/utimaco/cs2_pkcs11.ini
```

Refer to the *GenX Security Products Installation and Configuration Guide* for more information.

Share properties across all application servers

The installer creates properties files that apply across multiple components and reside in the file called `shared.properties` in `/usr/ssn/CONF/CURRENT`, which is generated during every installation. Every time you install a product, new information is merged into the `shared.properties` file.

The `shared.properties` file should be kept in sync with all servers hosting AMI applications. There are two ways to handle this:

- Every time you install an application on a separate server, copy the modified `shared.properties` file to `/usr/ssn/CONF/CURRENT` on all servers.
- Put `/usr/ssn/CONF` on an NFS share for all servers.

For information about the files created by the installer, see the *SSC 2.11 Installation Guide*.

If installing on multiple hosts

The **configure** command causes a file called `client_props.generated` to be created. This file is populated with any configuration key from an application's `masterlist.component` file that is annotated to be exported. An application that needs the configuration key will merge `client_props.generated` into the `config.properties` file when the application is started.

If you are running applications on different hosts, after running the **configure** command, open `/usr/ssn/CONF/CURRENT/client_props.generated` on the each separate host. Copy the properties into a merged master `client_props.generated` file that contains all properties across all hosts.

Place the merged file into `/usr/ssn/CONF/CURRENT` on each host. Each time you install or upgrade any application, copy the newly generated properties in `client_props.generated` and add them to the master `client_props.generated` file and copy the master file to `/usr/ssn/CONF/CURRENT` on each host.

Gateway users in CAAS

These users should be created in CAAS before installing GMR, MT, MPC, or FWU.

GMR:

1. You will move an XML file in GMR, `gmr01_system_account.xml` to `/usr/ssn/DATA/caas/xmldoc`, to complete the user creation. See Create a Gateway

user for AMM. on page 42.

FWU:

1. You will move an XML file in FWU, `fwu_system_account.xml` to `/usr/ssn/DATA/caas/xmldoc`. See Integrate FWU into CAAS for single sign-on. on page 54.

MPC:

1. You will move an XML file in MPC, mpc_`system_account.xml` to `/usr/ssn/DATA/caas/xmldoc`. See Integrate MPC into CAAS for single sign-on. on page 62.

3 Creating the installation directory structure

You should have already created the directory structure as described in the *Shared Services Component (SSC) 2.11 Installation Guide*. If you have not, go to that document and follow the instructions. Itron recommends that each customer create the structure as described in that document. This structure will match that of the Itron operations group, making it easier to support and troubleshoot if necessary, and more importantly, allow you to copy/paste commands from this and other installation manuals.

Perform all procedures in this section as user **ssn**.

Directory structure overview

The directory structure under `/usr/ssn` contains a set of basic directories:

- **sw**. The `sw` directory is a storage area for all saved software files.
- **release**. The `release` directory is a staging area where you run installation and configuration scripts on software files.
- **thirdparty**. This contains third-party products such as certificates and Tomcat.
- **CONF**. This contains links to properties files for each component you install. **CONF/CURRENT is the only directory in which you may directly edit properties files**.
- **DATA**. This contains subdirectories for each component you install. Here you will store `keykeep.store` files and other persistent data, which will remain in the directory through upgrades.
- **install_logs**. This contains log files for all of the applications you install, activate, and configure.

Setting up directories for a UtilityIQ installation

To install AMM, FWU, and MPC, create the following subdirectories in `/usr/ssn/release`:

ammjmsroute	**fwu**	**mt**
ammwsroute	**gmr**	**mpc**
db	**meterplugins**	**mpcwsroute**

> **Note:** If upgrading, be aware that you will no longer create a separate host for `ammwsroute`. It must be on the same host as MT.

These subdirectories are in addition to ones you have already made for the SSC applications. If you have not done so yet, go to the *SSC Installation Guide* and build the directory structure according to its instructions.

1. Create a version in each subdirectory.
   a. For each component being installed, create a subdirectory named after the version you are installing.

      cd /usr/ssn/release/*component_name*

      mkdir *version_number*

   b. Do this for each component in `/usr/ssn/release.`

      Make directories *only* for applications you will be installing. Name the directories after the version numbers on the package you are installing as shown in the following examples.

      Example: Version subdirectories in staging area

      Note that the following are example build numbers only. Use the version and build numbers on the software files you receive.

      cd /usr/ssn/release

      mkdir ammjmsroute/2.1.0b2000097

      mkdir ammwsroute/3.1.0b2000151

      mkdir db/6.0.0b2001593

      mkdir fwu/4.18.0b2000465

      mkdir gmr/6.0.0b2001593

      mkdir meterplugins/1.12.0b2000568

      mkdir mpc/4.18.0b2000307

      mkdir mpcwsroute/2.1.0b2000060

      mkdir mt/6.0.0b2001593

      Next you will create new CURRENT links for the new directories.

2. Create CURRENT symlinks to the new version you are about to install.

   In the `release` subdirectory, you will create a CURRENT symbolic link to the version you are going to configure for the upcoming installation.

   cd /usr/ssn/release/*component_name*

   ln –s *version_number* CURRENT

Example:

```
cd /usr/ammwsroute/release/ammwsroute
ln -s 3.1.0b2000151 CURRENT
...
```

Continue through `/usr/ssn/release` and do this for each component you are about to install.

3. Unzip the software files into the staging area (release directory).

   Unpack each software file into its respective directory by using the `unzip` command (or `tar` command in the case of TIBCO EMS) to extract files from `/usr/ssn/sw` to each component subdirectory in `/usr/ssn/release`.

   Example:

   ```
   cd /usr/ssn/sw
   unzip ammwsroute-3.1.0b2000151.zip -d
   /usr/ssn/release/ammwsroute/CURRENT
   ```

   Do this for every application you are planning to install.

4 Installing the AMM database (DB)

AMM consists of the following applications, all of which must be installed for AMM to work:

- Database (db)
- Global Meter Reader (gmr). See Installing AMM Global Meter Reader (GMR) on page 25.
- Meter Plugins (meterplugins). See Installing AMM Global Meter Reader (GMR) on page 25.
- Middle Tier (mt). See Installing Middle Tier (MT) on page 37.

Installing DB

JAVA should be installed in the `third party` directory.

1. Install and activate DB

   `cd /usr/ssn/release/db/CURRENT/packages/db`

   `./install /usr/ssn --activate`

2. Edit `db.properties`

   vi /usr/ssn/CONF/CURRENT/db.properties

   Make changes to the properties shown in db.properties on page 22. Other properties in `/usr/ssn/db/CURRENT/etc/masterlist.component` may also be reviewed and if needed, copied into `db.properties` with modification; however, it is expected that you will not need to change defaults found in that file.

   If the override is not in db.properties, then no change is needed. Change is needed only when editing the property in the override file.

   Table 2 db.properties

Property	Description
`DB_TABLESPACE_PROFILE`	The name of the tablespace profile for your database. This value is **`default`**. Consult your Oracle administrator for confirmation on this value.
`DB_JAVA_HOME`	Path to JAVA_HOME for application. This is public so an end user can override the location/directory if needed. Default is `${APP_INSTALLDIR}/db/CURRENT/install_data/jre/CURRENT`

Table 2 db.properties (continued)

Property	Description
DB_GOOGLE_MAP_CLIENT_ID	Copy this property from /usr/ssn/db/CURRENT/etc/masterlist.component and replace the default value with your own client ID. Refer to Google Maps API on page 12 for more information about the Google Maps Client ID.
DB_GOOGLE_MAP_VERSION	The Google map version used by the application. Version number is 3.25

3. Review amm.properties.

   The amm.properties file contains values that affect three applications that make up AMM: DB, GMR, and MT.

   vi /usr/ssn/CONF/CURRENT/amm.properties

   Caution: If you make changes to amm.properties and stop and start AMM, you must also stop and restart DMS.

   The amm.properties file generates after each of the AMM applications is installed. Refer to AMM.Properties on page 79 for information on all amm.properties.

   You must, at a minimum, modify any value labeled OVERRIDE_REQUIRED.All others may be left with the default values unless you have intentionally decided to change schema user names and passwords.

4. Review shared.properties.

   The shared.properties file regenerates every time you install an application. Review all properties and make sure you configure at least the OVERRIDE_REQUIRED properties. If a property is not identified as OVERRIDE_REQUIRED, you do not have to change it unless you need to, if, for example, your firewall administrator assigns a different port or if you decide to use a different name for a host.

   To review and edit shared.properties:

   vi /usr/ssn/CONF/CURRENT/shared.properties

   As you continue to install more applications, the installation merges more properties into the shared.properties file. To see all shared properties available, refer to Shared properties on page 84.

5. Configure DB.

   Run the configure script after you have saved the properties files.

   cd /usr/ssn/db/CURRENT

   ./configure

If you did not modify an override or if any of the prerequisite checks fail, the configure script will fail. If that happens, the installer will provide feedback about what is missing.

6. Preview.

   After all properties are set, optionally run **`/usr/ssn/db/CURRENT/bin/preview`** to preview the properties that will be passed on startup and the files they are found in. Change them if necessary.

7. (Optional) Create privileged user.

   a. You can use a SYSTEM login with all the grants assigned as described in The privileged user on page 14, or you can create a privileged user with the `cr_uiqroot.sql` script to perform schema creation tasks. This can also be done by granting privileges as described in The privileged user on page 14.

      ```
      cd /usr/ssn/db/CURRENT/schema/oracle/
      sqlplus SYSDBA/password@yourdb
      @cr_uiqroot.sql password
      ```

      Where *password* is the password for the privileged user.

   b. Create the product owner role:

      ```
      sqlplus SYSDBA/password@yourdb
      @cr_product_owner.sql
      ```

5 Installing AMM Global Meter Reader (GMR)

GMR is a requirement of AMM.

Installing GMR

1. Install and activate GMR.

   cd /usr/ssn/release/gmr/CURRENT/packages/gmr

   ./install /usr/ssn --activate

2. Edit `gmr.properties`.

   vi /usr/ssn/CONF/CURRENT/gmr.properties

   Make changes to the properties shown in the following table. Other properties in `/usr/ssn/gmr/CURRENT/etc/masterlist.component` may also be reviewed and if needed, copied into `gmr.properties` with modification; however, it is expected that you will not need to change defaults found in that file unless specified in this section.

   Table 3 gmr.properties

Properties	Description
AMM_THIN_NET_ENCRYPTION_TYPES	Defines the encryption algorithm to be used.
CONCURRENT_TRAP_PROCESSING_WORKERS_MIN_POOL_SIZE	Concurrent workers for IMU500S trap processing. Minimum pool size. Default is 2.
CONCURRENT_TRAP_PROCESSING_WORKERS_MAX_POOL_SIZE	Concurrent workers for IMU500S traps processing. Maximum pool size. Default is 20.
CONCURRENT_TRAP_PROCESSING_WORKER_IDEAL_TIMEOUT_SECONDS	Concurrent workers for IMU500S traps processing. Timeout in seconds. Default is 60 seconds.
CONCURRENT_TRAP_PROCESSING_JOB_QUEUE_SIZE	Concurrent workers for IMU500S traps processing. Job queue size. Default size is 2000.
GMR_ALLOW_UNSECURE_TRAPS	Allows GNR to process unsecured traps. Default state is false.

Table 3 gmr.properties (continued)

Properties	Description
GMR_ENABLE_TASK_ THROTTLING	Enable capacity manager task throttling based on task priority. Default is false.
GMR_HIGH_PRIORITY_TASK_ CAPACITY_RESERVED_ PERCENTAGE=50.00	High priority task capacity reservation, used when task throttling enabled
GMR_TASK_CAPACITY_BASED_ ON_PRIORITY	Percentage assigned for High priority tasks. Percentage float values separated by '/'. Task Capacity priority order HIGH/NORMAL/LOW Default is **55.00/30.00/15.00**
GMR_NEM_QUEUE_POLICY	NEM queue is disabled by default.
GMR_NODE_ID	Default is **1,** which does not have to be changed if you have only one GMR server. If you have two GMRs, change the GMR_NODE_ID for each one— the value will be **2** for gmr02.
GMR_HOST	There is no need to change this parameter if you are running one instance of GMR: **gmr01.${SHARED_DOMAIN_NAME}** If you have more than one GMR, each host should be different. (**gmr01**, **gmr02**)
GMR_ASYNC_DEVICE_ RESPONSE_WAIT_TIMEOUT_IN_ MINS=5	Allows to configure how long the Device should wait for async response before marking it as timeout.
GMR_JMX_WEBSERVER_ KEYSTORE	This is the SSL keystore for GMR. Default is **${SHARED_CERT_LOCATION_DIR}/gmr01.jks**
GMR_JMX_WEBSERVER_ PASSWORD	JMX webserver password. Default is U6yQ0VTLoyH2BusDRX4Z4w==
GMR_JMX_WEBSERVER_ KEYPASSWORD	Password for the SSL keystore for GMR. Default is **U6yQ0VTLoyH2BusDRX4Z4w==**

Table 3 gmr.properties (continued)

Properties	Description
GMR_JVM_ARGS	The GMR_JVM_ARGS property has the following required options: `-server -XX:+PrintGCDetails -XX:+PrintGCTimeStamps -XX:+PrintGCDateStamps -Xloggc:${INSTALL_BASEDIR}/logs/gc.log -XX:+UseLargePages -Dsun.rmi.dgc.server.gcInterval=0x7FFFFFFFFFFFFFFE -Dsun.rmi.dgc.client.gcInterval=0x7FFFFFFFFFFFFFFE -XX:NewSize=1536m -XX:CMSInitiatingOccupancyFraction=80 -XX:+UseCMSInitiatingOccupancyOnly -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -Dehcache.disk.store.dir=${DATA_DIR}/ehcache_data -Duser.country=US -Duser.language=en -Doracle.jdbc.maxCachedBufferSize=22 -XX:-OmitStackTraceInFastThrow -XX:+UseZingMXBeans`
GMR_CONFIRM_DEVICE_IDENTITY	Options are `manufacturer` or `utility` or **`false`**|**`none`**|**`no`**. – **`manufacturer`** is only available for DLMS installations. – **`utility`** is only available for c12 meters. For c12 meters, this setting must correspond to a sysvar on the NIC that controls whether or not the device identity is read from ST1 (manufacturer info) or ST5 (utility info). If `manufacturer` or `utility`, GMR will include the manufacturer serial number or the utility device ID in all requests to the device. If the NIC cannot verify the provided identifier, the request will fail. Using manufacture and utility in a mixed deployment is not supported at this time. Default is **no**.
GMR_COAP_GATEWAY_ACCOUNT_NAME	Account name of COAP Gateway. Default account name is **gmr${GMR_NODE_ID}-coap-gw**
GMR_COAP_GATEWAY_ACCOUNT_PASSWORD	Encrypted version of the COAP Gateway password. Default is **b**
GMR_ERT_JOB_SHOULD_FILL_GAPS	Controls whether to perform gap filling before reconciliation. Default is **true.**
GMR_ERT_GAP_FILL_WINDOW_MINUTES	Randomization window (in minutes) for ERT Gap Filling Job. Time to wait to fill gaps before performing reconciliation. Default is **90**minutes.

Table 3 gmr.properties (continued)

Properties	Description
GMR_ERT_JOB_SHOULD_RECONCILE_RESULTS	Sets whether to perform reconciliation of results Default is **true.**
GMR_ERT_INTERVAL_THRESHOLD_MINUTES	Defines max number of minutes from the top of the hour (XX:00) in which a register reading is considered for generating interval reads. For example, if this is set to 10 minutes, then an interval is derived from a register read of 9:50 AM and 11:10 AM for the 10:00 AM to 11:00 AM interval, but if the best register read is 9:49 AM and 11:10 AM then no interval is generated for the 10:00 AM to 11:00 AM interval reading. Default is **10** minutes.
GMR_ERT_DEVICE_PROCESS_MAX_BATCH_SIZE	Controls the maximum batch size of ERT devices when doing ERT data processing. Default is **50.**
GMR_ERT_DEVICE_STATUS_POLLING_FREQUENCY_IN_SECONDS	Defines how frequently the DB is polled to check the ERT device trap received status for ERT current register read. Reconcile job is started after receiving all expected results. Modifying the value for faster pollDlmsRegisterReadProcessoring can have impact on DB performance. This value should be larger then GMR_TASK_MONITORING_FREQUENCY_SECONDS (default to 60s) Default is **180.**
GMR_ERT_MAX_WAIT_TIME_COUNTER	Defines the maximum wait time before a reconcile job for ERT current register read is started. This value should combine with GMR_ERT_DEVICE_STATUS_POLLING_FREQUENCY_IN_SECONDS. For example, if the ERT device status table is checked five times continuously and the total trap received number did not increase, a reconcile job is started. Then maximum wait time in this case is GMR_ERT_MAX_WAIT_TIME_COUNTER * GMR_ERT_DEVICE_STATUS_POLLING_FREQUENCY_IN_SECONDS = 15 mins Default is **5** minutes
GMR_ERT_MIDNIGHT_READ_BOUNDARY_IN_SECONDS	Used to determine if an ERT hourly register read falls within the midnight boundary. Range is from 0-86400 seconds (1 day). For example, 60 means one minute before/after midnight Default is **60** seconds.
AMM_ERT_TRAP_PROCESSING_BUFFER_MINUTES	Allows for some extra time to receive and process traps before performing reconciliation.

Table 3 gmr.properties (continued)

Properties	Description
AMM_ERT_FW_TRAP_RETRY_BUFFER_MINUTES	Allows for some time to counter traps retry window in FW before performing reconciliation.
GMR_PRI_MAX_FUTURE_INTERVAL_DATE_DAY_COUNT	Defines the number of days after the current date used to set the maximum PACT date. If the PRI load survey response contains day blocks later than this maximum PACT date, then these day blocks are dropped and not processed. If the value is set to 0, then this check is disabled. Any integer value in the range of 0-1000 is allowed for validation Default is **0**.
GMR_PRI_MAX_PAST_INTERVAL_DATE_DAY_COUNT	Defines the number of days before the current date that is used to set the minimum PACT date. If the PRI load survey response contains day blocks earlier than this minimum PACT date, then these day blocks are dropped and not processed. If the value is set to 0, then this check is disabled. An integer value in the range of 0-1000 is allowed for this validation. Default is **0**.
GMR_NICNAC_SECURITY_HSM_CS2_PKCS11_INI	Allows properties to be used to set the cs2_pkcs11.ini file location if using an HSM. The Utimaco driver will determine this setting. It is recommended you do not change this and make sure the `cs2_pkcs11.ini` file is always in the recommended location. The default is `/etc/utimaco/cs2_pkcs11.ini`.
GMR_EXPORT_JOB_MAX_DAYS GMR	Computes the allocated memory for an export job based on the max days of data to be exported. An integer value in the range of 1-45 is allowed for this validation. Default is **30**
GMR_MT_HOST	If MT and GMR are on the same machine, add and modify this property Copy the property from this table or from `/usr/ssn/gmr/CURRENT/etc/masterlist.component` and change the value to **`localhost`**.
GMR_MQTT_BROKER_ENABLED	If you are using the MQTT Broker: Copy this property from this table or from `/usr/ssn/gmr/CURRENT/etc/masterlist.component` to `gmr.properties` and change the value to **`true`**.

Table 3 gmr.properties (continued)

Properties	Description
GMR_MQTT_FILE_STORE_DIRECTORY	If you are using the MQTT Broker: Copy this property from this table or from /usr/ssn/gmr/CURRENT/etc/masterlist.component to gmr.properties and change the value to the path indicating the location where intermediate messages (data or ACKs) are stored on the disk if GMR is unable to access the broker for some reason.
GMR_MQTT_USER_NAME	If you are using the MQTT Broker: Copy this property from this table or from /usr/ssn/gmr/CURRENT/etc/masterlist.component to gmr.properties and change the value to **gmr${GMR_NODE_ID}-mqtt.**
GMR_MQTT_PASSWORD	If you are using the MQTT Broker: Copy this property from this table or from /usr/ssn/gmr/CURRENT/etc/masterlist.component to gmr.properties and change the value to the encrypted form of the password used with the GMR_MQTT_USER_NAME.
GMR_MQTT_CLIENT_ID	Default is **gmr-${GMR_HOST}**. This is a unique ID used for the MQTT client.
GMR_NICNAC_SECURITY_HSM_ENABLED	A NICNAC security property. Default is **false**.
GMR_NICNAC_SECURITY_HSM_PKCS11_PERMIT_SLOT	A NICNAC security property. Defines the failover and load balancing configuration of HSM slots for KeySafe. It is required if GMR_NICNAC_SECURITY_HSM_ENABLED equals true
GMR_NICNAC_SECURITY_HSM_PKCS11_ENTITY_SLOT	A NICNAC security property. Defines the failover and load balancing configuration of HSM slots for COP. Required if GMR_NICNAC_SECURITY_HSM_ENABLED equals true. Default is **set_if_hsm_enabled**.
GMR_NICNAC_SECURITY_HSM_PKCS11_ENTITY_PIN	A NICNAC security property. The encrypted password to use with the KeySafe slot. Required if GMR_NICNAC_SECURITY_HSM_ENABLED equals true.
GMR_NICNAC_SECURITY_HSM_CS2_PKCS11_INI	Location of the CS2 PKCS11 ini file.
GMR_NICNAC_SECURITY_HSM_PKCS11_PERMIT_PIN	A NICNAC security property. The encrypted password to use with the COP slot. Required if GMR_NICNAC_SECURITY_HSM_ENABLED equals true.
GMR_NICNAC_SECURITY_ENCRYPTIONSERVICE_ENABLED	It enables/disables the security encryption service. Default is **true.**

Table 3 gmr.properties (continued)

Properties	Description
GMR_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ HOSTNAME	A NICNAC security encryption service property. Required if GMR_ NICNAC_SECURITY_ENCRYPTIONSERVICE_ENABLED is set to true. Default is **cryptkeeper.${SHARED_DOMAIN_NAME}**
GMR_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ PORTNUMBER	A NICNAC security encryption service property. Required if: GMR_ NICNAC_SECURITY_ENCRYPTIONSERVICE_ENABLED is set to true. Default is **9423**
GMR_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ USERNAME	gRPC user name. Default is **gmr-ck**.
GMR_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ AUTHENDPOINT	Required to configure gRPC authentication/authorization. Default is **https://${GMR_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ HOSTNAME}:9443/cryptkeeper/auth/accessToken**.
GMR_GAS_ANCHOR_READ_TIME	Configure the time of the daily anchor read. Format must be hh:mm. When not set, anchor read time will default to midnight.
GMR_GAS_ANCHOR_READ_ TIMEZONE	Configure the timezone of the daily anchor read. Timezone must be from the list of timezones in the TZ database: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones When not set, time will be relative to the meter's local timezone.

3. Review amm.properties.

   The `amm.properties` file contains values that affect three applications that make up AMM: DB, GMR, and MT.

   `vi /usr/ssn/CONF/CURRENT/amm.properties`

   Caution: If you make changes to `amm.properties` and stop and start AMM, you must also stop and restart DMS

   The `amm.properties` file generates after each of the AMM applications is installed. Refer to AMM.Properties on page 79 for information on all `amm.properties`.

You must, at a minimum, modify any value labeled OVERRIDE_REQUIRED. All others may be left with the default values unless you have intentionally decided to change schema user names and passwords.

4. Review `shared.properties`.

   The shared.properties file regenerates every time you install an application. Review all properties and make sure you configure at least the OVERRIDE_REQUIRED properties. If a property is not identified as OVERRIDE_REQUIRED, you do not have to change it unless you need to, if, for example, your firewall administrator assigns a different port or if you decide to use a different name for a host.

   To review and edit `shared.properties`:

   `vi /usr/ssn/CONF/CURRENT/shared.properties`

   As you continue to install more applications, the installation merges more properties into the `shared.properties` file. To see all shared properties available, refer to Shared properties on page 84.

5. Configure GMR.

   Run the `configure` script after you have saved the properties files.

   `cd /usr/ssn/gmr/CURRENT`

   `./configure`

   If you did not modify an override or if any of the prerequisite checks fail, the configure script will fail. If that happens, the installer will provide feedback about what is missing.

6. Preview.

   After all properties have been set, run `/usr/ssn/gmr/CURRENT/bin/preview` to preview the properties that are being passed on startup and the files they are found in. Change them if necessary.

7. Integrate GMR into CAAS for single sign-on

   After you have completed the installation, you can integrate GMR into CAAS. This enables single sign-on and lets you open AMM from a dropdown menu.

   Copy `gmr01_system_account.xml` from GMR to the CAAS host.

   `cd /usr/ssn/gmr/CURRENT/etc`

   `cp gmr01_system_account.xml /usr/ssn/DATA/caas/xmldoc`

   Loading this file creates roles and privileges.

8. Install Meter Plugins on the GMR Server

   Meter plugins must be installed on both the MT and the GMR host(s). If you are running both applications on the same host, you can install one instance of Meter Plugins.

Refer to Installing Meter Plugins on page 44.

Creating DB schemas

Execute the `schema-creation` script:

If your privileged user is SYSTEM

```
cd /usr/ssn/db/CURRENT/db_setup/bin
./create-schemas --execute --privuser system --privpassword
<systempassword>
```

If your privileged user is uiqroot

If you have created a privileged user called **uiqroot**:

```
cd /usr/ssn/db/CURRENT/db_setup/bin
./create-schemas --execute --privuser uiqroot --privpassword
<uiqrootpassword>
```

This procedure is performed once but can be run again if there are problems with database privileges.

Install the schema:

```
cd /usr/ssn/db/CURRENT/db_setup/bin
./fresh-install
```

If upgrading, upgrade the schema instead:

Execute the schema-creation script when doing a fresh installation or an upgrade.

```
cd /usr/ssn/db/CURRENT/db_setup/bin
./upgrade
```

Next

Install GMR. Go to Installing AMM Global Meter Reader (GMR) on page 25.

Configure SSH for MT and GMR

GMR uses JCraft JSCH (Java Secure Channel) to SCP files to MT for exports. JCraft JSCH is a third-party package and only supports certain SSH parameters (such as security). When you configure the connection between GMR and MT, it must be within the bounds of what JSCH supports. See http://www.jcraft.com/jsch/ for more information.

If MT and GMR are on the same machines

Configure GMR to use **`localhost`** for the MT server. This must be changed for the `GMR_MT_HOST` property in `gmr.properties`.

Make sure that the AMR export directory (`/usr/ssn/DATA/mt/export/amr/`) for MT is writable by the GMR user.

If MT and GMR are on separate machines

If the AMM MT and GMR are installed on different machines, you must configure SSH to ensure that AMM export files can be transferred from the GMR host to the MT host, where they can be opened.

To configure SSH

1. Create a password with the `encrypt` utility:

   `cd /usr/ssn/db/CURRENT/install_data/utils`

   `encrypt *cleartextpassword*`

   where *cleartextpassword* is an unencrypted open-text password.

2. On the GMR server(s), change the following property in the `amm.properties` file:

   AMM_WEBAPP_SCP_PASSWORD=*encrypted_password*

   where:

   encrypted_password is the result of Step 1 above.

3. On the MT server, ensure the `ssn` user can log in from each GMR host to the MT host via SSH and can **`scp`** files into `/usr/ssn/DATA/mt/export/amr`.

Log files for GMR

Based on the deployment configuration, one log file is created per GMR instance. Each deployment has at least one GMR instance defined.

The file naming format is as follows:

`date (YYYYMMDD)–unique Hash number–GMR number–log.xml`

Example:

`20100620-f3edcbec-f16c-415b-b091-68db33b4a8cb-2-log.xml`

The log file always includes the created interval/register/event export files. The following log file example is from a `gmr01`, which had matching criteria in the export job for Segment 3 and Segment 4:

```
<?xml version="1.0"?>
<ExportLog xmlns="urn:com:ssn:schema:export:SSNExportLog.xsd"
StartTime="2010-06-27T00:00:00.000-07:00" EndTime="2010-06-
30T00:00:00.000-07:00" Meters="39" IntervalReadings="20413"
RegisterReadings="236" Events="609" Logs="0">
   <FileSummary>
       <XMLFiles>
           <File>amr/info/20100704-1e4d1bd2-6ed6-4486-a838-
2adb669e5abc-3-1.xml</File>
```

```
            <File>amr/info/20100704-1e4d1bd2-6ed6-4486-a838-
2adb669e5abc-4-1.xml</File>
        </XMLFiles>
    </FileSummary>
    <ExportException>
    </ExportException>
</ExportLog>
```

Keystores for GMR

SSL certificate

The GMR server requires an SSL keystore named **`gmr01.jks`** for the JMX console, residing in `/usr/ssn/thirdparty/certs.` (If you are running more than one GMR, each GMR host needs its own keystore named after the server.)

Refer to **SSL certificate and Keystore configuration** in the *SSC Installation Guide* for information on generating and installing certificates.

Keykeep.store file

If you are not using a Hardware Security Module (HSM) to securely store credentials required for authentication and authorization, Itron provides a unique keystore called a `keykeep.store` for the applications that require it. This keystore contains Itron-generated private keys required for secure communication between the application server and endpoints (meters, APs, NICs, Relays, and other devices). Installation of the keystore occurs after the applications are installed.

After installation is complete, put the GMR `keykeep.store` file in `/usr/ssn/DATA/gmr/nicnackeystore`. (This directory matches the `NICNAC_SECURITY_KEYSTORE_DIRECTORY` property described in the gmr.properties on page 25.) If the directory does not exist, create it.

See the *SSC Installation Guide* for more details about installing `keykeep.store` files.

If you are using an HSM, make sure you have added the NICNAC properties described in the gmr.properties on page 25, and refer to *GenX Security Products Installation and Configuration Guide* .

Start GMR (as SSN)

You can start GMR now or wait until all applications have been installed. For information about starting and stopping all components, see Starting and stopping applications on page 66.

If you are upgrading, startup and stop order may be different from a fresh installation. Refer to the upgrade instructions for details.

1. Start the application:

   cd /usr/ssn/gmr/CURRENT/bin

   ./init.sh start

2. Confirm application is up and running with no fatal errors by reviewing `/usr/ssn/gmr/CURRENT/logs/gmr-start.log`

Next

Install MT. Continue with Installing Middle Tier (MT) on page 37.

6 Installing Middle Tier (MT)

The Middle Tier (MT) of AMM contains all the user-facing components of AMM. There are three software packages that comprise MT: `mt`, `meterplugins`, and `ammwsroute`. MT must be installed before AMMWSRoute.

All three must be installed on the same host.

Installing MT

1. Install and activate MT.

   `cd /usr/ssn/release/mt/CURRENT/packages/mt`

   `./install /usr/ssn --activate`

2. Review mt.properties.

   `vi /usr/ssn/CONF/CURRENT/mt.properties`

   Make changes to the properties shown in the following table. Other properties in `/usr/ssn/mt/CURRENT/etc/masterlist.component` may also be reviewed and if needed, copied into `mt.properties` with modification; however, it is expected that you will not need to change defaults found in that file with the exceptions of those listed in the table.

Table 4 mt.properties

Property	Description
`MT_MULE_INSTALLDIR`	Location of the third-party Mule product. Default is **`/usr/ssn/thirdparty/mule/CURRENT`**
`MT_TOMCAT_INSTALLDIR`	Location of Apache Tomcat installation. Default is **${APP_INSTALLDIR}/thirdparty/tomcat/apache-tomcat-9.0.85**
`MT_TOMCAT_WEBAPP_MAX_THREADS`	Maximum thread attribute of tomcat connector elements (webapp only, not webservice) in server.xml. Default is **`100`**.
`MT_TOMCAT_WS_MAX_CONCURRENT_REQUESTS`	Maximum concurrent tomcat webservice requests Default is **`100`**.

Table 4 mt.properties (continued)

Property	Description
MT_TOMCAT_WS_CONNECTOR_EXTRA_THREADS	Number of extra threads above MT_TOMCAT_WS_MAX_CONCURRENT_REQUESTS for the tomcat webservice Connector. Required to allow more than the max threads to make it through the connector to the SemaphoreValveForPort. Default is **10**.
MT_SSL_CERT_KEYSTORE	This is the SSL keystore for MT. The default value is **${SHARED_CERT_LOCATION_DIR}/mt.jks** There is no need to change the default if you have followed the naming conventions for the MT keystore. The keystore and its password include ammwsroute.
MT_SSL_CERT_KEYSTORE_PASSWORD	This is the password for the SSL keystore. It is an encrypted version of **changeit**. There is no need to change this default if you have followed the instructions in the installation documents. If you do choose to assign a new password to the MT keystore, be aware that changeit is a Tomcat default and must be modified everywhere it appears. This requires an experienced network administrator and instructions are not provided in the documentation for such a change.
MT_PROGRAM_READ_JOB_DURATION_HOURS	Total duration in hours that a device will stay in initializing and continue to attempt program read requests. The default is **-1**, which means that there is no end to the attempt to read. Setting this value to a positive number can cause the device to go into Init Failed when the time ends, requiring a manual retry initialization.
MT_DLCA_APP_PASSWORD	**T**his is a secret key to encrypt/decrypt data between MT and DLCA. Used specifically for Master Meter security key. Default is **${SHARED_MASTERMETER_PSK}** See the *DLCA Installation Guide* for more information.
MT_IEC_METERS_AVAILABLE	**For customers using IEC meters:** This value Indicates whether or not the AMM user interface displays IEC meter features. Options are **true/false** and default is **false**. If you are using IEC meters in your environment, you will need to add this property to mt.properties and set the value to **true**. Copy the property from /usr/ssn/mt/CURRENT/etc/masterlist.component or manually add it if needed and change the value.

Table 4 mt.properties (continued)

Property	Description
MT_NEM_ENABLED	This property is in `masterlist.component` but may need to be changed. The property name `MT_NEM_ENABLED` implies that it is specific to the NEM application. However, this property controls the functionality of the AMM diagnostics link and also applies to Network Center. If set to `false`, the diagnostics link in Device details will not appear irrespective of whether Network Center or NEM is installed. It must be set to **`true`** for the diagnostics link to appear irrespective of whether NC or NEM is installed. Default is **`true`**. If you need to change this, go to `/usr/ssn/mt/CURRENT/etc/masterlist.component` and copy this property into `mt.properties` to override the default.
MT_MPC_ENABLED	Defines whether the UI should attempt to integrate with MPCn. It is true/false.Default is **true**.
MT_IEC_METERS_AVAILABLE	Defines whether the UI should display features of IEC. Values are true/false. Default is **false**.
MT_PREVIOUS_SEASON_REGISTER_AVAILABLE	Defines whether the UI should display the previous season's register read feature. Values are true/false. Default is **false**.
MT_ERT_PROXY_READ_WINDOW_MINUTES	Randomization window (in minutes) for ERT proxy read job Time to wait before kicking off an ERT gap filling job. Default is **90**.
MT_EXPORT_JOB_MAX_DAYS	GMR computes the allocated memory for an export job based on the max days of data to be exported. Any integer value in the range of 1-45 is allowed for this validation. Default is **30**
AMM_ERT_TRAP_PROCESSING_BUFFER_MINUTES	Allow some extra time to receive and process traps before starting data reconciliation.
AMM_ERT_FW_TRAP_RETRY_BUFFER_MINUTES	Allow some time to counter trap retry window in FW before starting data reconciliation
MT_EHCACHE_MAX_HEAP_SIZE	The maximum bytes ehcache can use in local heap memory. Percents (25%, 50%) or fixed number (100M, 50g) are allowed **Increasing this value may cause performance issues, decreasing this to a very low number may break the UI pagination functionality.** Default is **25%.**

3. Review amm.properties.

   The `amm.properties` file contains values that affect three applications that make up AMM: DB, GMR, and MT.

   `vi /usr/ssn/CONF/CURRENT/amm.properties`

   > **Caution:** If you make changes to `amm.properties` and stop and start AMM, you must also stop and restart DMS.

   The `amm.properties` file generates after each of the AMM applications is installed. Refer to AMM.Properties on page 79 for information on all `amm.properties`.

   You must, at a minimum, modify any value labeled OVERRIDE_REQUIRED. All others may be left with the default values unless you have intentionally decided to change schema user names and passwords.

4. Review shared.properties.

   The `shared.properties` file regenerates every time you install an application. Review all properties and make sure you configure at least the OVERRIDE_REQUIRED properties. If a property is not identified as OVERRIDE_REQUIRED, you do not have to change it unless you need to, if, for example, your firewall administrator assigns a different port or if you decide to use a different name for a host.

   To review and edit `shared.properties`:

   `vi /usr/ssn/CONF/CURRENT/shared.properties`

   As you continue to install more applications, the installation merges more properties into the `shared.properties` file. To see all shared properties available, refer to Shared properties on page 84.

5. Configure MT.

   Run the `configure` script:

   `cd /usr/ssn/mt/CURRENT`

   `./configure`

6. Manually create the webapps manager directory.

   Look for `/usr/ssn/mt/CURRENT/webapps/manager` and if it does not exist, create it manually:

   `mkdir -p /usr/ssn/mt/CURRENT/webapps/manager`

7. Preview.

   Run **`/usr/ssn/mt/CURRENT/bin/preview`** to preview the properties that are being passed on startup and the files they are found in. Change them if necessary.

8. Integrate MT into CAAS for single sign-on.

   After you have completed the installation, you can integrate MT into CAAS. This enables single sign-on and lets you open AMM from a dropdown menu.

   Copy `amm_caas_role_priv.xml` from the MT to CAAS host.

   `cd /usr/ssn/mt/CURRENT/etc`

   `cp amm_caas_role_priv.xml /usr/ssn/DATA/caas/xmldoc`

   Loading this file creates roles and privileges.

9. Load plugins.

   a. All plugins for your deployment must be copied into `/usr/ssn/DATA/dms/plugins`.

      In `/usr/ssn/DATA/dms/`, create a subdirectory called **`plugins,`** if it does not exist already:

      `cd /usr/ssn/DATA/dms`

      `mkdir plugins`

   b. Refer to the plugins that you've configured in the file `dms.properties`, which was generated when you installed DMS, described in the *SSC 2.9 Installation Guide*.

      If upgrading, copy all existing plugins from `/usr/ssn/dms/CURRENT/lib` into `/usr/ssn/DATA/dms/plugins`. This brings the existing plugin files from the old location into the new location

      `cd /usr/ssn/dms/CURRENT/lib`

      `cp dms-plugins-<application-version>.jar /usr/ssn/DATA/dms/plugins`

   c. Locate the **dms-plugin** directory generated by the MT installation and copy the plugin jar files to the DMS plugins location:

      `cd /usr/ssn/mt/CURRENT/dms-plugin`

      `cp *.jar /usr/ssn/DATA/dms/plugins`

      For example, if your `dms.properties` file indicates these applications:

      `DMS_ENABLED_PLUGINS=amm-plugin,fwu-plugin,registrar-plugin`

      you need to put a plugin jar file for each of those applications into `/usr/ssn/DATA/dms/plugins`.

10. Install routing rules.

    Routing rules specific to this application are generated in the etc directory. Copy them into the `TRAPROUTER_ROUTE_CONFIG_DIR /xmldocs` location specified in the traprouter.properties file in /usr/ssn/CONF/CURRENT. (See the Trap Router section in the *SSC 2.9 Installation Guide* for details.)

To copy the routing rules file:

```
cd /usr/ssn/mt/CURRENT/etc
cp amm_trap_routing_rules.xml /usr/ssn/DATA/traprouter/xmldocs/
```

11. Create a DMS user for AMM.

    Copy `amm_system_account.xml` to the CAAS `xmldoc` directory:

    ```
    cd /usr/ssn/gmr/CURRENT/etc
    cp amm_system_account.xml/usr/ssn/DATA/caas/xmldoc
    ```

12. Create a Gateway user for AMM.

    The installation generates an XML file that creates a CAAS user for AMM. This is required for Gateway. The GMR system account file also contains users for Cryptkeeper and MQTT. You must have already created the user in CAAS as described in Gateway users in CAAS on page 17.

    Copy `gmr01_system_account.xml` to the CAAS `xmldoc` directory:

    ```
    cd /usr/ssn/gmr/CURRENT/etc
    cp gmr01_system_account.xml /usr/ssn/DATA/caas/xmldoc
    ```

Keystores for MT

MT requires an SSL keystore named `mt.jks` in `/usr/ssn/thirdparty/certs` on the MT server.

Refer to **SSL Certificate and Keystore Configuration** in the *SSC Installation Guide* for information on generating and installing certificates.

(Optional) Create the Drop Box directory

The import file drop box is an FTP server into which device and location import files can be dropped on a regular basis. Create the drop box on the server hosting AMM MT. Once the directory is created, you can import files from the drop box, in addition to the file system from the AMM UI.

From the AMM UI, all import files stored in this directory are visible and can be uploaded. During device deployment, many such import files are generated, often daily, and stored to streamline device provisioning.

To create the default drop box directory

1. Enter the following command:

   ```
   sudo -E mkdir -p /var/ftp/pub
   ```

2. Set ownership to be the `ssn` account:

   ```
   sudo -E chown ssn:ssn /var/ftp/pub
   ```

3. Download the VSFTPD daemon software from the following site:

   http://vsftpd.beasts.org/

   vsftpd is part of the Red Hat distribution **`sudo yum install vsftpd`**.

4. Configure the VSFTPD daemon to use the `/var/ftp/pub` directory as the default FTP location.

Start MT (as ssn)

For information about starting and stopping all components, see Starting and stopping applications on page 66.

> **Caution:** If you make changes to `amm.properties` after the initial startup and stop and start AMM, you must also stop and restart DMS.

If you are upgrading, startup and stop order may be different from a fresh installation. Refer to the upgrade instructions for details.

Start the application:

```
cd /usr/ssn/mt/CURRENT/bin
./init.sh start
```

Next

Install MeterPlugins. Continue with Installing Meter Plugins on page 44.

7 Installing Meter Plugins

Meter plugins must be installed on both the MT and the GMR host(s). If you are running both applications on the same host, you can install one instance of Meter Plugins.

1. Install and activate meter plugins.

   ```
   cd /usr/ssn/release/meterplugins/CURRENT/packages/meterplugins
   ./install /usr/ssn --activate
   ```

2. Review the properties files and copy them to the CMU machine:

   Properties files for each meter type are created in `/usr/ssn/meterplugins/CURRENT/lib`.

   There are no changes to make to `/usr/ssn/conf/meterplugins.properties.`

   a. Review the properties for your meter type and make changes if necessary. The properties are documented within each file.

   b. If you make any changes to the meter properties files, copy the customized files from `/usr/ssn/meterplugins/CURRENT/lib` to the Communication Module Utility (CMU) machine's Windows folder where the `croc-cli` JAR file resides. Any time Meter Plugin properties are updated on the servers, these files must be copied to CMU.

3. Configure

   Run the `configure` script after you have saved the properties files.

   ```
   cd /usr/ssn/meterplugins/CURRENT
   ./configure
   ```

Next

Make sure Meter Plugins are on both the GMR and MT hosts.

Next, install AMMWSRoute. Continue with Installing AMMWSRoute on page 45.

8 Installing AMMWSRoute

AMMWSRoute is the web services component of AMM. It is required by AMM and is installed on the MT host. In AMM 4.11, AMMWSRoute handled both SOAP web service and JMS message processing. Starting with AMM 4.12, this has been split into two applications and the JMS portion was moved to AMMJMSRoute. (See Installing AMMJMSRoute on page 46.)

If you are upgrading from an earlier version of AMMWSRoute, note that AMMWSRoute requirements have changed. Refer to Upgrading Trap Router on page 75.

Make sure that MT is installed and configured before you install AMMWSRoute. AMMWSRoute must be installed on the MT host.

1. Install and activate ammwsroute

   `cd /usr/ssn/release/ammwsroute/CURRENT/packages/ammwsroute`

   `./install /usr/ssn --activate`

2. Review ammwsroute.properties.

   There is no need to change the default configurations in `ammwsroute.properties` in `/usr/ssn/CONF/CURRENT/`

3. Configure AMMWSRoute.

   Run the **`configure`** script:

   `cd /usr/ssn/ammwsroute/CURRENT`

   `./configure`

4. Start AMMWSRoute.

   `cd /usr/ssn/ammwsroute/CURRENT/bin`

   `./init.sh start`

Next

Install AMMJMSRoute. Continue with Installing AMMJMSRoute on page 46.

9 Installing AMMJMSRoute

AMMJMSROUTE routes public and legacy API calls to the associated MT server and provides an increased number of sessions. Before UtilityIQ 4.12, this functionality was part of AMMWSRoute.

1. Install and activate ammjmsroute.

   `cd /usr/ssn/release/ammjmsroute/CURRENT/packages/ammjmsroute`

   ./install /usr/ssn --activate

2. Review ammjmsroute.properties. There is no need to change the default configurations in `ammjmsroute.properties` in `/usr/ssn/CONF/CURRENT/`

Table 5 ammwsroute.properties

Property	Description
`AMMJMSROUTE_INTERNAL_EVENT_VERSION`	Internal API version number for AMM JMS messages. Do not change this unless advised to by Itron. Default is **`1.9`**
`AMMJMSROUTE_EVENT_VERSION`	Public API version number to be used when publishing JMS messages. Do not change this unless advised to by Itron. Default is **`2.7`**
`AMMJMSROUTE_SSL_CERT_KEYSTORE`	Location of the SSL keystore, `ammjmsroute01.jks`. Default is **`${SHARED_CERT_LOCATION_DIR}/ammjmsroute.jks`**
`AMMJMSROUTE_SSL_CERT_KEYSTORE_PASSWORD`	Encrypted password for the keystore. Default is the encrypted form of **changeit**. *changeit* is the recommended password for SSL keystores. If you use any other password, you will need to change it in any existing Tomcat files and properties files. Do not change the default unless you have the expertise that enables you to locate and change the defaults. If you do change this password, it must be encrypted. The encrypt tool is in `/usr/ssn/ammjmsroute/CURRENT/install_data/utils` To encrypt the password, type: **`./encrypt plaintext_password`**

3. Configure AMMJMSROUTE.

   Run the **`configure`** script:

   `cd /usr/ssn/ammjmsroute/CURRENT`

   `./configure`

4. Start AMMJMSROUTE.

```
cd /usr/ssn/ammjmsroute/CURRENT/bin
./init.sh start
```

Next

If you are installing FWU, continue with Installing Firmware Upgrader (FWU) on page 48.

If this is the final application you are installing, you are finished. If so, make sure all of the applications have started and are successfully running. Go to Starting and stopping applications on page 66 for information.

If your applications are running on multiple hosts, make sure you have updated the `client_props.generated` file as described in If installing on multiple hosts on page 17.

10 Installing Firmware Upgrader (FWU)

Firmware Upgrader (FWU) enables you to upgrade the UtilOS firmware or meter firmware on NICs. FWU is an optional installation.

Installing FWU

1. Install and activate FWU.

   `cd /usr/ssn/release/fwu/CURRENT/packages/fwu`

   `./install /usr/ssn --activate`

2. Edit `fwu.properties`.

   `vi /usr/ssn/CONF/CURRENT/fwu.properties`

   Make changes to the properties shown in the following table. Other properties in `/usr/ssn/fwu/CURRENT/etc/masterlist.component` may also be reviewed and if needed, copied into `fwu.properties` with modification; however, it is expected that you will not need to change defaults found in that file with the exceptions of those listed in the table.

Table 6 fwu.properties

Property	Description
`FWU_CELLULAR_ENABLED`	Enables cellular functionality. Default is **false**.
`FWU_SSL_CERT_KEYSTORE`	The FWU SSL keystore. Default value is **`${SHARED_CERT_LOCATION_DIR}/fwu.jks`** There is no reason to change this value unless you change the recommended name for the FWU SSL keystore.
`FWU_SSL_CERT_KEYSTORE_PASSWORD`	The password for SSL certificate. Default is **`U6yQ0VTLoyH2BusDRX4Z4w==`**
`FWU_UI_ENABLE_EXPERT_MODE`	When set to true NIC images with unknown device types are allowed. Default is **false**.

Table 6 fwu.properties (continued)

Property	Description
FWU_SERVICE_RESTART_IN_PROGRESS_UPGRADES_ON_STARTUP	Controls how in-progress upgrades are handled on application startup. When enabled: upgrades that were in-progress when the application shut down are automatically restarted. When disabled: in-progress upgrades are canceled. Restarting and canceling an in-progress upgrade can be slow for large upgrades. Default is **false.**
FWU_HOST	CNAME for FWU server. There is no need to change the default unless you have named the host something other than what is recommended in this document. The default is: **fwu.${SHARED_DOMAIN_NAME}**
FWU_DB_LOGIN	The Oracle user name that FWU will connect to. This user has fewer privileges than the DATABASE_LOGIN_ADMIN. Default is **${SHARED_DB_USER_PFX}_fwu_app**
FWU_DB_PASSWORD	The Oracle password for DATABASE_LOGIN. The encrypted password value must be 40 characters or less. Default is **${SHARED_DB_USER_PASSWORD}**
FWU_DB_LOGIN_OWNER	The Oracle user name that owns the FWU schema. Default is **${SHARED_DB_USER_PFX}_fwu**
FWU_DB_PASSWORD_OWNER	The Oracle password for DATABASE_LOGIN_OWNER Default is **${SHARED_DB_USER_PASSWORD}**
FWU_SSL_HTTP_PORT	Port number for FWU SSL HTTP. The default is **4043**. There is no need to change this unless your firewall administrator tells you to use a different port number.
FWU_DEPLOYMENT_SUMMARY_DNS_AGE_THRESHOLD_DAYS	Use for the deployment summary table shown in the dashboard. Only devices with last update newer than this threshold are included Default is **365**.
FWU_MILLI_AUDIT_RETRY_LIMIT	Number of audit retries allowed for Milli. Default is **1**.
FWU_MILLI_UI_IMAGE_LIST_TIMEOUT_SECONDS	Timeout in seconds for UI Milli image list page. Default is 180.

Table 6 fwu.properties (continued)

Property	Description
FWU_JVM_ARGS	The FWU_JVM_ARGS property has the following required options: **-Xloggc:${INSTALL_BASEDIR}/logs/gc.log** **-XX:+UseConcMarkSweepGC** **-XX:+UseParNewGC** **-XX:+CMSIncrementalMode** **-XX:+UseLargePages** **-XX:+UseMembar** **-XX:+PrintGCDetails** **-XX:+PrintGCTimeStamps** **-XX:-OmitStackTraceInFastThrow**
FWU_JMS_DEVICE_UPDATE_ENABLED	This property is now public. Enables publishing device update messages. For each device being upgraded, a message is published whenever a stage of the upgrade is completed. A final message for that device is published when its upgrade either completes or fails. If enabled, a valid value for FWU_JMS_DEVICE_QUEUE_NAME must be provided. Default is **false**
FWU_JMS_DEVICE_QUEUE_NAME	The JMS queue to publish device update messages to. Default is **/queue/FwuDeviceStatusQueue**
FWU_JMS_SKIP_DUPLICATE_UISTATE_UPDATES_ENABLED	Enables skipping device status updates with the same state and status. Default is **true.**
FWU_JMS_DI_NOTIFICATIONS_ONLY_ENABLED	Enables FWU to send only DI related upgrade messages Default is **true.**
FWU_JMS_UPGRADE_UPDATE_ENABLED	This property is now public. Enables publishing messages when upgrades complete. If enabled, a valid value for FWU_JMS_PROJECT_QUEUE_NAME must be provided. Default is **false**
FWU_JMS_UPGRADE_QUEUE_NAME	The JMS queue where upgrade complete messages are published. Default is **/queue/FwuUpgradeStatusQueue**
FWU_JMS_CACHE_PRODUCERS	Specifies whether to cache JMS MessageProducers per JMS Session instance. Default is **true**
FWU_JMS_SESSION_CACHE_SIZE	Specifies the desired size for the JMS Session cache (per JMS Session type). Default is **1**
FWU_DMS_CAAS_USERNAME	DMS credentials. Default username is **fwu-dms**

Table 6 fwu.properties (continued)

Property	Description
FWU_DMS_CAAS_PASSWORD	**Override required**. DMS password.
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_ENABLED	When true, NICNAC initializes the Cryptkeeper Encryption client (GRPC client) for encryption/decryption/permitting of 500S requests. Default is **true**.
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_AUTHENDPOINT	Cryptkeeper host URL used by NICNAC to call encryption and decryption services. Default is **https://${SHARED_ENCRYPTIONSERVICE_ HOST}:9443/cryptkeeper/auth/accessToken**
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_USERNAME	CAAS username for connecting to Cryptkeeper Default is **fwu-ck**.
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_PASSWORD	CAAS password for connecting to Cryptkeeper Default is **1MA0ECIT4eP/GCaMxAgFh$uXbUnHB/JNLMij9F8mA79g==**
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_PORTNUMBER	Cryptkeeper port number. Default is **${SHARED_ENCRYPTIONSERVICE_PORT}**
FWU_NICNAC_SECURITY_ ENCRYPTIONSERVICE_HOSTNAME	Cryptkeeper host name. Default is **${SHARED_ENCRYPTIONSERVICE_HOST}**
FWU_UI_PROJECT_DEFAULT_PROXIED_ DEVICEFWU_VERIFY_INTERVAL_SECONDS	Default is **180** seconds.
FWU_UI_PROJECT_MAX_METER_VERIFY_ MAX_TRIES	Sets maximum retries. Maximum is 500 retries.
FWU_UI_PROJECT_RESTART_THRESHOLD_ PERCENTAGE	Used in auto restart. Default is **98**.
FWU_UI_PROJECT_FAILURE_THRESHOLD_ MULTIPLIER	Used in auto restart. Default is **3**.
FWU_VERIFY_INTERVAL_SECONDS	Interval seconds. Maximum is 1800 seconds.
FWU_UI_PROJECT_DEFAULT_500S_ VERIFY_MAX_TRIES	Maximum retries for 500S devices. Default is **150**.
FWU_UI_PROJECT_DEFAULT_500S_ VERIFY_INTERVAL_SECONDS	Interval seconds for 500S devices. Default is 3600 seconds.

Table 6 fwu.properties (continued)

Property	Description
FWU_DEVICE_FWU_RUN_BATCH_SIZE_MASTER_METER	Sets batch size for Master meters. Default is **10**.
FWU_DEVICE_FWU_RUN_BATCH_SIZE_500S	Sets batch size for 500S devices. Default is **40**.
FWU_UI_PROJECT_DEFAULT_PROXIED_DEVICEFWU_VERIFY_MAX_TRIES	Default is **50**.
FWU_UI_PATTERN_DATETIME	The date/time format standard date time displays in the UI. Default is **MMM d, yyyy - hh:mm aa** Format for Australia is dd MMMM yyyy - HH:mm
FWU_UI_PATTERN_DATETIME_ALERTS	The date/time format for standard date time displays for alerts on the FWU dashboard. Default is **MMM d, yyyy - hh:mm:ss aa** Format for Australia is dd MMMM yyyy - HH:mm:ss
FWU_UI_PATTERN_DATE	The date format for standard date displays in the UI. Default is **MMM d, yyyy** Format for Australia is dd MMMM yyyy
FWU_SECURITY_SESSION_TIMEOUT_MINUTES	Sets session timeout limit in minutes. Default is **30 minutes**.
FWU_WAIT_TIME_FOR_NIC_TO_BE_READY_AFTER_RESTART	This property should ***only*** be changed for Gen5 Riva Electricity Meters. Time taken for a NIC to be ready after restart. Default is **900 seconds**. For Gen5 Riva Electricity Meters, change the wait time to 30 minutes and restart FWU.
FWU_NICNAC_GATEWAY_ACCOUNT_NAME	**Required for Gateway.** Gateway user name. Default is fwu-gw. This username must exist in CAAS. After the installation is complete, you will follow the steps in Integrate FWU into CAAS for single sign-on. on page 54 to create the user.
FWU_NICNAC_GATEWAY_ACCOUNT_PASSWORD	**Required for Gateway.** Application's password for Gateway. This password must match the encrypted version of the CAAS password. Default is **1MA0ECHBu3AKDd9SmAgFh$NqcBWDN6Had6IZeHoAS2Fg==**
FWU_NICNAC_MAX_SOCKETS	NICNAC socket max count. Default is **5000**.
FWU_NICNAC_START_PORT	NICNAC socket range start. Default is **10000**
FWU_NICNAC_STOP_PORT	NICNAC socket range stop. Default is **65000**.

Table 6 fwu.properties (continued)

Property	Description
FWU_NICNAC_SECURITY_ASSOCATION_TIMEOUT	**If deploying KeySafe, this property must be manually added from /usr/ssn/fwu/CURRENT/etc/masterlist.component and modified as needed:** Time within which a secure association must be completed. Otherwise the association times out. Recommended value is **60** (60 seconds).
FWU_NICNAC_SECURITY_HSM_ENABLED	If deploying KeySafe, this property must be manually added from /usr/ssn/fwu/CURRENT/etc/masterlist.component and modified as needed: HSM users must set this value to **true**. true = Use the HSM as the source for key encryption and certificate authorization. false = Use the keykeep.store file, residing at the path used for the SECURITY_KEYSTORE_DIRECTORY parameter. **Important!** If set to false, all FWU_NICNAC_SECURITY_HSM values are ignored.
FWU_NICNAC_SECURITY_HSM_PKCS11_ENTITY_SLOT	**If deploying KeySafe, this property must be manually added from /usr/ssn/fwu/CURRENT/etc/masterlist.component and modified as needed: :** NM Entity slot number. There is no default here because if you are using an HSM, you must enter the value. Slot from which *non-rate-limited* certificates and keys will be pulled. The NM Entity slot resides on the KeySafe HSM only. You must select a positive slot number (**0**, **1,2,** etc.) to enable it. **Important!** Failover or load balancing should be indicated here. Load-balancing is configured using brackets, failover without. In the following example, HSM 1, slot 1 and HSM 2, slot 1 are co-primary in a load balanced configuration and would fail over in an emergency to the secondary, “hot” HSM 3, slot 1. Example: **[1:1, 2:1],3:1** The HSM TCP/IP addresses should be entered in your cs2_pkcs11.ini file. Refer to *GenX Security Products Installation and Configuration Guide* for more details.
FWU_NICNAC_SECURITY_HSM_PKCS11_ENTITY_PIN	**If deploying KeySafe, this property must be manually added from /usr/ssn/fwu/CURRENT/etc/masterlist.component and modified as needed:** (Required) Encrypted slot user (CKA_CFG_AUTH_USER) PIN for NM Entity slot.

3. Review shared.properties.

   The shared.properties file regenerates every time you install an application. Review all properties and make sure you configure at least the OVERRIDE_REQUIRED properties.

If a property is not identified as OVERRIDE_REQUIRED, you do not have to change it unless you need to, if, for example, your firewall administrator assigns a different port or if you decide to use a different name for a host.

To review and edit `shared.properties`:

```
vi /usr/ssn/CONF/CURRENT/shared.properties
```

As you continue to install more applications, the installation merges more properties into the `shared.properties` file. To see all shared properties available, refer to Shared properties on page 84.

4. Configure FWU

   Run the **`configure`** script after you have saved the properties files.

   ```
   cd /usr/ssn/fwu/CURRENT
   ./configure
   ```

   If you did not modify an override or if any of the prerequisite checks fail, the configure script will fail. If that happens, the installer will provide feedback about what is missing.

5. Preview.

   After all properties are set, run **`/usr/ssn/fwu/CURRENT/bin/preview`** to preview the properties that will be passed on startup and the files they are found in.

6. Load plugins

   All plugins for your deployment must be copied into `/usr/ssn/DATA/dms/plugins`.

   Locate the **dms-plugin** directory generated by the FWU installation and copy the plugin jar files to the DMS plugins location:

   ```
   cd /usr/ssn/fwu/CURRENT/dms-plugin
   cp *.jar /usr/ssn/DATA/dms/plugins
   ```

7. Install routing rules.

   Routing rules specific to this application are generated in the etc directory. Copy them into the `TRAPROUTER_ROUTE_CONFIG_DIR /xmldocs` location specified in the traprouter.properties file in /usr/ssn/CONF/CURRENT. (See the Trap Router section in the *SSC 2.11 Installation Guide* for details.)

   To copy the routing rules file:

   ```
   cd /usr/ssn/fwu/CURRENT/etc
   cp fwu_trap_routing_rules.xml /usr/ssn/DATA/traprouter/xmldocs/
   ```

8. Integrate FWU into CAAS for single sign-on.

   After you have completed the installation, integrate FWU into CAAS. This enables single sign-on and lets you open FWU from a dropdown menu.

Copy `fwu_system_account.xml`:

```
cd /usr/ssn/fwu/CURRENT/etc/
cp fwu_system_account.xml /usr/ssn/DATA/caas/xmldoc
```

Create FWU schemas

After installation and configuration is complete, create the database schema:

1. Execute the schema-creation script:

   ```
   cd /usr/ssn/fwu/CURRENT/database/bin
   ./create-schema.sh
   ```

2. When prompted for the privileged login credentials, enter the Oracle privileged user login and password created as described in The privileged user on page 14.
3. Install the schema:

   ```
   ./fresh-install.sh
   ```

Keystores for FWU

SSL Certificate

FWU requires an SSL keystore named **`fwu.jks`** residing in `/usr/ssn/thirdparty/certs.`

Refer to **SSL Certificate and Keystore Configuration** in the *SSC Installation Guide* for information on generating and installing certificates.

Keykeep.store file

If you are not using a Hardware Security Module (HSM) to securely store credentials required for authentication and authorization, Itron provides a unique keystore called a `keykeep.store` for the applications that require it. This keystore contains Itron-generated private keys required for secure communication between the application server and endpoints (meters, APs, NICs, Relays, and other devices). Installation of the keystore occurs after the applications are installed.

Put the FWU `keykeep.store` file in **`/usr/ssn/DATA/fwu/nicnackeystore.`**

(This directory matches the `NICNAC_SECURITY_KEYSTORE_DIRECTORY` property described in fwu.properties on page 48.) If the directory does not exist, create it.

See the *SSC Installation Guide* for more details about `keykeep.store` files.

If you are using an HSM, make sure you have modified the properties described in fwu.properties on page 48and refer to *GenX Security Products Installation and Configuration Guide* .

Start FWU (as ssn)

You can start FWU now or wait until all applications have been installed. For information about starting and stopping all components, see Starting and stopping applications on page 66.

1. Start the application:

   ```
   cd /usr/ssn/fwu/CURRENT/bin
   ./init.sh start
   ```

2. Verify startup:

   ```
   cd /usr/ssn/fwu/CURRENT/bin
   ./init.sh status
   ```

Next

If this is the final application you are installing, you are finished with the installation. If so, make sure all of the applications have started and are successfully running. Go to Starting and stopping applications on page 66 for information on getting started.

If your applications are running on multiple hosts, make sure you have updated the `client_props.generated` file as described in If installing on multiple hosts on page 17.

If you are installing MPC, continue with Installing Meter Program Configurator (MPC) on page 57.

11 Installing Meter Program Configurator (MPC)

Meter Program Configurator (MPC) enables wireless, remote audits and upgrades of meter programs. MPC is an optional installation. This section contains information on installing and configuring MPC.

Refer to the *Shared Services Components (SSC) 2.11 Installation Guide* for information on how to install SSC components including NA Proxy.

Installing MPC

1. Install and activate the software.

   `cd /usr/ssn/release/mpc/CURRENT/packages/mpc`

   `./install /usr/ssn --activate`

2. Edit mpc.properties:

   `vi /usr/ssn/CONF/CURRENT/mpc.properties`

   Make changes to the following properties. Other properties in `/usr/ssn/mpc/CURRENT/etc/masterlist.component` may also be reviewed and if needed, copied into `mpc.properties` with modification; however, it is expected that you will not need to change defaults found in that file with the exceptions of those listed in the following table.

Table 7 mpc.properties

Property	Description
`MPC_CERT_LOCATION_DIR`	Directory where certs are located. Default is **${SHARED_CERT_LOCATION_DIR}**
`MPC_HOST`	Host name of the machine where MPC is installed. Example: **`mpc.${SHARED_DOMAIN_NAME}`** There should be no need to change this. The variable refers to the property SHARED_DOMAIN_NAME, already defined in the `shared.properties` file.
`MPC_DB_APP_USER`	MPC database application user; the Oracle user name that MPC connects with. The default is **${SHARED_AMM_DB_APP_USER}**, assuming it is the same as the AMM DB app user.
`MPC_DB_APP_PASSWORD`	Password for the database. Default is **${SHARED_AMM_DB_APP_USER_PASSWORD}**

Table 7 mpc.properties (continued)

Property	Description
MPC_DB_USER	The MPC schema user. Default is **MPC_DB_USER=${SHARED_DB_USER_PFX}m** The user name is generated by appending **m** to the SHARED_DB_USER_PFX you set in the shared.properties file. For example, if your SHARED_DB_USER_PFX is **DBuser**, then the MPC_DB_USER will be generated as **DBuserm**
MPC_DB_USER_PASSWORD	Password for the database user. Default is **${SHARED_DB_USER_PASSWORD}**
MPC_NICNAC_GATEWAY_ACCOUNT_PASSWORD	**Required for Gateway.** Application's password for Gateway. This password must match the encrypted version of the CAAS password. Default is **1MA0ECEzUGRt+U/3gAgFh$dl90CAhecu35FqLbCGoTKg==**
MPC_NICNAC_SECURITY_HSM_ENABLED	Enable/disable HSM. Default is **true**.
MPC_NICNAC_SECURITY_HSM_CS2_PKCS11_INI	If deploying KeySafe, this property must be manually added from /usr/ssn/mpc/CURRENT/etc/masterlist.component and modified as needed: Location of CS2 PKCS11 ini file.
MPC_NICNAC_SECURITY_HSM_PKCS11_ENTITY_SLOT	**If deploying KeySafe, this property must be manually added from /usr/ssn/mpc/CURRENT/etc/masterlist.component and modified as needed:** NM Entity slot number. There is no default here because if you are using an HSM, you must enter the value. Slot from which *non-rate-limited* certificates and keys will be pulled. The NM Entity slot resides on the KeySafe HSM only. You must select a positive slot number (**0**, **1,2,** etc.) to enable it. **Important!** Failover or load balancing should be indicated here. Load-balancing is configured using brackets, failover without. In the following example, HSM 1, slot 1 and HSM 2, slot 1 are co-primary in a load balanced configuration and would fail over in an emergency to the secondary, "hot" HSM 3, slot 1. Example **[1:1, 2:1],3:1** The HSM TCP/IP addresses should be entered in your cs2_pkcs11.ini file. Refer to *GenX Security Products Installation and Configuration Guide* for more details.

Table 7 mpc.properties (continued)

Property	Description
MPC_NICNAC_SECURITY_HSM_PKCS11_ENTITY_PIN	**If deploying KeySafe, this property must be manually added from /usr/ssn/mpc/CURRENT/etc/masterlist.component and modified as needed:** (Required) Encrypted slot user (CKA_CFG_AUTH_USER) PIN for NM Entity slot.
MPC_NICNAC_SECURITY_HSM_PKCS11_PERMIT_SLOT	If deploying KeySafe, this property must be manually added from /usr/ssn/mpc/CURRENT/etc/masterlist.component and modified as needed: Required for GMR with Remote Service Management (RSM)/Remote Disconnect (RD) and MPC for non-Street Light application only Configures the COP HSM slot containing *rate-limited* permit key and certificate. **Important!** *Street Light Adapter (SLA) commands do not require permits and therefore GMR with SLA does not connect to COP. This property is valid only for GMR in a [[[Undefined variable UtilityIQ_5_0_Installation.Product]]] environment.* ■ **If COP is not deployed,** you must ***enable*** the Permit slot on the *KeySafe* HSMs. ■ **If COP is deployed, *disable*** the Permit slot on the KeySafe HSMs and make sure to enable it on the COP HSMs. Values: ■ -1 disables the use of the Permit slot. ■ Entry of an HSM number and a slot number for the Permit to enable it. **Important!** Failover or load balancing should be indicated here. Example 1:2, 2:2 Where: 1:2 = HSM 1 and slot 2 2:1 = HSM 2 and slot 2 The HSM TCP/IP addresses should be entered in your cs2_pkcs11.ini file. **Important!** Failover or load balancing should be indicated here. Refer to *GenX Security Products Installation and Configuration Guide* for information.
MPC_NICNAC_SECURITY_HSM_PKCS11_PERMIT_PIN	A NICNAC security property. The encrypted password to use with the COP slot.Required if MPC_NICNAC_SECURITY_HSM_ENABLED is set to true. Default is **EJyreABqwU8=**

Table 7 mpc.properties (continued)

Property	Description
MPC_NICNAC_SECURITY_ENCRYPTIONSERVICE_HOSTNAME	Host name of the Cryptkeeper. Default is **${SHARED_ENCRYPTIONSERVICE_HOST}**
MPC_NICNAC_SECURITY_ENCRYPTIONSERVICE_HTTPPORT	**Cryptkeeper http api service port.** Default is **9443**.
MPC_NICNAC_SECURITY_ENCRYPTIONSERVICE_PASSWORD	Password to connect to Cryptkeeper GRPC services. Default is **1MA0ECGRFWW2bijYYAgFh$fbZp9xPy9686Zlcdp/Jk7g==**
MPC_NICNAC_SECURITY_ENCRYPTIONSERVICE_PORTNUMBER	Cryptkeeper GRPC service port. Default is **${SHARED_ENCRYPTIONSERVICE_PORT}**.
MPC_NICNAC_SECURITY_ENCRYPTIONSERVICE_USERNAME	Username to connect to Cryptkeeper GRPC services. Default is **mpc-ck**.
MPC_SSL_CERT_KEYSTORE	SSL certificate and keystore declarations. Exported for MPCWSRoute. Default is **${MPC_CERT_LOCATION_DIR}/mpc.jks**
MPC_SSL_CERT_KEYSTORE_PASSWORD	SSL certificate keystore password. Exported for MPCWSRoute Default is **U6yQ0VTLoyH2BusDRX4Z4w==**
MPC_COAP_GATEWAY_ACCOUNT_PASSWORD	Password for COAP Gateway account. Default is **1MA0ECKkOMRPlpNyfAgFh$mNKlzcADrZx2lbvMdMQXlw==**
MPC_NICNAC_NUM_WORKERS	Number of NICNAC workers. Default is **20**.
MPC_PROJECT_NEW_DATA_READ_JOB_RETRY_COUNT	Sets number of retry counts for new data read jobs. Default is **3**.
MPC_PROJECT_NEW_DATA_READ_LIMIT	Use it to configure whether or not you want to set limit for number of new data read jobs. Default is **false**.
MPC_PROJECT_NEW_DATA_READ_MAX_THREAD	Required if MPC_PROJECT_NEW_DATA_READ_SPEED_CHECKER_ENABLED is set to true
MPC_PROJECT_NEW_DATA_READ_SPEED_CHECKER_ENABLED	If set to true new data read job on the next batch is not scheduled until the number of devices in the reprogramming queue is zero. Default is **false**.
MPC_SET_LAST_KNOWN_GOOD_IMAGE_AFTER_UPGRADE	Lets you retrieve the last known good image after an upgrade, if set to true. Default is **false**.

Table 7 mpc.properties (continued)

Property	Description
MPC_SYS_ACCOUNT_PASSWORD	MPC system user password. Default is **1MA0ECGRFWW2bijYYAgFh$fbZp9xPy9686Zlcdp/Jk7g==**
MPC_METRICS_EXCLUDE	Leave this blank to disable metric reporting.
MPC_METRICS_INCLUDE	Matches metrics name and tag string of the form -NAME TAG1_KEY=TAG1_VALUE TAG2_KEY=TAG2_VALUETAG3_KEY=TAG3_VALUE . If not specified, all metrics are included.
MPC_METRICS_IGNORETAGS	A comma separated list of tags to ignore when creating metrics. Used to drop tags that cause too many unique metrics to be created.
MPC_METRICS_SPLUNKFILE_ENABLED	Enables/disables generation of the Splunk metrics log. Default is **false**.
MPC_SSL_HTTP_PORT	MPC Port. Default is **5044**.

3. Review shared.properties.

   The `shared.properties` file regenerates every time you install an application. Review all properties and make sure you configure at least the OVERRIDE_REQUIRED properties. If a property is not identified as OVERRIDE_REQUIRED, you do not have to change it unless you need to, if, for example, your firewall administrator assigns a different port or if you decide to use a different name for a host.

   To review and edit `shared.properties`:

   `vi /usr/ssn/CONF/CURRENT/shared.properties`

   As you continue to install more applications, the installation merges more properties into the `shared.properties` file. To see all shared properties available, refer to Shared properties on page 84.

4. Configure MPC.

   Run the **`configure`** script after you have saved the properties files.

   `cd /usr/ssn/mpc/CURRENT`

   `./configure`

   If you did not provide a required value or if any of the prerequisite checks fail, the configure script will fail. If that happens, the installer will provide feedback about what is missing.

5. Preview.

After all properties have been set, optionally run **/usr/ssn/mpc/CURRENT/bin/preview** to preview the properties that are being passed on startup and the files they are found in. Change them if necessary.

6. Install routing rules.

   Routing rules specific to this application are generated in the etc directory. Copy them into the TRAPROUTER_ROUTE_CONFIG_DIR /xmldocs location specified in the traprouter.properties file in /usr/ssn/CONF/CURRENT.

7. To copy the routing rules file:

   cd /usr/ssn/mpc/CURRENT/etc

   cp mpc_trap_routing_rules.xml /usr/ssn/DATA/traprouter/xmldocs/

8. Integrate MPC into CAAS for single sign-on.

   After you have completed the installation, you can integrate MPC into CAAS. This enables single sign-on and lets you open MPC from a dropdown menu.

   Copy mpc_caas_role_priv.xml:

   cp mpc_system_account.xml /usr/ssn/DATA/caas/xmldoc/

   cp mpc_caas_role_priv.xml /usr/ssn/DATA/caas/xmldoc/

If MPC and CAAS are installed on different hosts, do the following:

scp mpc_system_account.xml ssn@<caas_host>:/usr/ssn/DATA/caas/xmldoc/
scp mpc_caas_role_priv.xml ssn@<caas_host>:/usr/ssn/DATA/caas/xmldoc/

Keystores for MPC

SSL certificate

The MPC server requires an SSL keystore named **mpc.jks** residing in /usr/ssn/thirdparty/certs.

Refer to **SSL Certificate and Keystore Configuration** in the *SSC Installation Guide* for information on generating and installing certificates.

Keykeep.store file

If you are not using a Hardware Security Module (HSM) to securely store credentials required for authentication and authorization, Itron provides a unique keystore called a keykeep.store for the applications that require it. This keystore contains Itron-generated private keys required for secure communication between the application server and endpoints (meters, APs, NICs, Relays, and other devices). Installation of the keystore occurs after the applications are installed.

After installation is complete, put the MPC keykeep.store file in /usr/ssn/DATA/mpc/nicnackeystore. (This directory matches the NICNAC_SECURITY_

KEYSTORE_DIRECTORY property in `mpc.properties`.) If the directory does not exist, create it.

See the *SSC 2.9 Installation Guide* for more details about installing `keykeep.store` files.

If you are using an HSM, make sure you have modified the properties described in mpc.properties on page 57 mpc.properties on page 57 and refer to *GenX Security Products Installation and Configuration Guide*.

Create or upgrade MPC schemas

After installation and configuration is complete, create or upgrade the database schema:

```
cd /usr/ssn/mpc/CURRENT/database/bin
```

Create the schema:

```
./fresh-install.sh
```

Or upgrade the schema:

```
./upgrade.sh
```

When prompted for the privileged login credentials, enter the Oracle privileged user login and password created as described in The privileged user on page 14.

Start MPC (as ssn)

You can start MPC now or, if you have been waiting to start all applications, start them in the order shown in Starting and stopping applications on page 66.

1. Start the application:

   ```
   cd /usr/ssn/mpc/CURRENT/bin
   ./init.sh start
   ```

2. Verify startup:

   ```
   cd /usr/ssn/mpc/CURRENT/bin
   ./init.sh status
   ```

Next

Install MPCWSRoute. Proceed with Installing MPCWSRoute on page 64.

12 Installing MPCWSRoute

MPCWSRoute is the web services component of MPC. It is required by MPC and must be installed on the MPC host.

Before you start

Make sure that MPC is installed and configured before you install MPCWSRoute. MPCWSRoute must be installed on the MPC host.

1. Install and activate MPCWSRoute

   `cd /usr/ssn/release/mpcwsroute/CURRENT/packages/mpcwsroute`

   `./install /usr/ssn --activate`

2. Review mpcwsroute.properties

   There is no need to change the default configurations in `mpcwsroute.properties` in `/usr/ssn/CONF/CURRENT/`

   Table 8 MPCWSRoute properties

Property	Description
`MPCWSROUTE_METRICS_EXCLUDE`	Leave this blank to disable metric reporting.
`MPCWSROUTE_METRICS_INCLUDE`	Matches metrics name and tag string of the form -NAME TAG1_KEY=TAG1_VALUE TAG2_KEY=TAG2_VALUETAG3_KEY=TAG3_VALUE . If not specified, all metrics are included.
`MPCWSROUTE_METRICS_IGNORETAGS`	A comma separated list of tags to ignore when creating metrics. Used to drop tags that cause too many unique metrics to be created.
`MPCWSROUTE_METRICS_SPLUNKFILE_ENABLED`	Enables/disables generation of the Splunk metrics log. Default is **false**.

3. Configure MPCWSRoute

   Run the **`configure`** script:

   `cd /usr/ssn/mpcwsroute/CURRENT`

   `./configure`

4. Integrate MPCWSRoute into CAAS for single sign-on.

After you have completed the installation, you can integrate MPCWSRoute into CAAS.

Copy mpcwsroute_caas_role_priv.xml:

```
cp mpcwsroute_system_account.xml /usr/ssn/DATA/caas/xmldoc/
cp mpcwsroute_caas_role_priv.xml /usr/ssn/DATA/caas/xmldoc/
```

5. Start MPCWSRoute

```
cd /usr/ssn/mpcwsroute/CURRENT/bin
./init.sh start
```

6. Preview.

   After all properties are set, optionally run **/usr/ssn/mpcwsroute/CURRENT/bin/preview** to preview the properties that will be passed on startup and the files they are found in. Change them if necessary.

Next

This concludes the installation of the AMM 6.0 product family. Start up all applications as shown in Starting and stopping applications on page 66.

If your applications are running on multiple hosts, make sure you have updated the `client_props.generated` file as described in If installing on multiple hosts on page 17.

A Starting and stopping applications

This section contains start/stop information and recommended order for ALL software applications whether or not they are required for this solution.

> Make sure all DB scripts have run before starting any application.

This chapter contains the recommended start order for all Itron products. **Not all of the applications listed here are included in your installation.**

Starting and stopping applications in `bin`

Most of the applications are started or stopped in the same way, from the component's `bin` directory:

`ssh` to the host on which each application is running.

```
cd /usr/ssn/<component>/CURRENT/bin
./init.sh start|stop
```

For example, to start DMS, type:

```
cd /usr/ssn/dms/CURRENT/bin
./init.sh start
```

To check status after starting or stopping, type:

```
cd /usr/ssn/<component>/CURRENT/bin
./init.sh status
```

Applications that must be started/stopped as Root

Most of the applications start and stop as **`ssn`**; however, some of them require **`sudo`** privileges:

reg

sensoriq 3.x and later

tmb

Start order

Start the applications in the following order:

1. TIBCO (see procedure below)
2. hivemqssncfg
3. reg

4. gateway (see procedure below)
5. gmr
6. mt
7. amm
8. ammwsroute
9. ammjmsroute
10. fwu
11. mpc
12. mpcwsroute
13. dms
14. ztp
15. cryptkeeper
16. CAAS

Always start the main application first before starting JMSROUTE and then WSRoute for apps that have these components like MPC, HCM, SensorIQ.

For example, start MPC before starting MPCJMSRoute and then MPCWSRoute.

GridScape should start last.

...

gridscape

Components that have different start procedures

The following components do not use the start/stop commands in the `bin` directory.

Start TIBCO EMS

TIBCO EMS is normally running continuously. If it is stopped, start it as follows:

```
cd /usr/ssn/thirdparty/tibco/CURRENT/ems/<version_number>/bin
./tibemsd64 -config
/usr/ssn/thirdparty/tibco/CURRENT/tibco/cfgmgmt/ems/data/tibemsd.conf &
```

Where:

version_number is the installed version of TIBCO: (6.1, 8.6.0, or other, depending on what is installed.)

When Starting CAAS

For a first-time installation, start CAAS *before* starting the applications and log in to create users for the applications.

Start Greenplum parallel file distribution server (gpfdist) (for GridScape)

```
cd /usr/ssn/da/CURRENT/bin
./da_gpfdist.sh start
```

Stop order

Stop applications in the opposite order from the start rules:

1. gridscape

   ...

   After gridscape, the stop order does not matter except that the following must be stopped last and in this order:

2. CAAS
3. cryptkeeper
4. dms
5. reg
6. ztp
7. gateway (see procedure below)
8. hivemqssncfg
9. TIBCO EMS (see procedure below)

Components that have different stop procedures

The following components do not use the start/stop commands in the `bin` directory.

When stopping TBR

When shutting down TBR, allow **`init.sh`** a full five minutes for a system with 250,000 devices. Interrupting it prematurely can cause entity cache corruption which will be rebuilt on the next startup.

Stop TIBCO EMS

```
cd /usr/ssn/thirdparty/tibco/CURRENT/ems/<version>/bin
./tibemsadmin ssl://<port>
shutdown
```

Testing startup success

Besides looking at the log files, you can confirm installation success after startup by going to the CAAS host to open any of the applications you have integrated with CAAS. You will

see an indication that the application has started up, in the form of a login screen. The login screen belongs to CAAS.

The CAAS URL is:

https://<*CAAS_CNAME*>:<*port_number*>/caas/

Where *CAAS_CNAME* is the CNAME for the CAAS server as defined in the Worksheet and port_number is the port number for the CAAS server.

https://caas.smartgrid.utility.com:6343/caas/

To log into any application, you will actually log into CAAS, if the CAAS integration was done as described in this document. Use the existing username and password you set when users were created in CAAS previously. From the CAAS UI, you will be able to see the roles and privileges of each application whose .xml file you copied over when doing client integration.

To log into CAAS for the first time immediately after CAAS is installed, work with the person in your organization who is acting as your CAAS administrator, who will set roles and add and manage users. The first person to log into CAAS (the CAAS administrator) logs in as **root** and enters the temporary password **"password**," which then must be changed. After that, the CAAS administrator adds users, each of whom has their own username and password. For more information, see the *CAAS Administrator's Guide*.

Providing URLs to end users

Give end users the URL for the host at https://CNAME:ssl_port/appname. They can reach any of the integrated applications from the CAAS URL or the individual application's URL.

B Upgrading to UtilityIQ 6.0

To upgrade from one version of a product family to the next, refer to the *GenX Compatibility and Requirements Matrix* for information on supported software and to the release notes for the new version.

> If applications are running on separate hosts: Update the `client_props.generated` each time you upgrade a product. See If installing on multiple hosts on page 17 for more details.

General upgrading guidelines for upgrading software to a newer version

1. Obtain the new software files from Itron Networks and store them in `/usr/ssn/sw`. Make sure you are upgrading the newest supported version of the shared services components (SSC package) along with all other components being installed.
2. Read the release notes for each interim version between the software you are upgrading from and the version you are upgrading to, to understand what properties and ports have changed.
3. Shut down each of the components you want to upgrade.

   `cd /usr/ssn/`*`component`*`/CURRENT/bin`

   `./init.sh stop`

   or, for products that require sudo:

   `sudo -E ./init.sh stop`

   See Starting and stopping applications on page 66 for stop order.
4. Set up the staging area for the new software.

   In `/usr/ssn/release/`*`component`*, remove the CURRENT symlink and create new CURRENT symlinks. For example:

   `cd /usr/ssn/release/`*`component`*

   `rm CURRENT`

   `mkdir `*`newversionnumber`*

   `ln -s `*`newversionnumber`* **`CURRENT`**

   where:

- *component* is the name of the directory of the component you are upgrading, such as **caas** or **tbr**
- *newversionnumber* is the release number of the component package.

Example:

```
cd /usr/ssn/release/caas
mv CURRENT PREVIOUS
mkdir 1.13.1b2000408
ln -s 1.13.1b2000408 CURRENT
```

5. Unzip the installation package from the `sw` directory into the `CURRENT` directory:

   ```
   cd /usr/ssn/release/component/CURRENT
   unzip /usr/ssn/sw/1.13.1b2000408.zip
   ```

6. Install and activate new components:

   ```
   cd /usr/ssn/release/component/CURRENT/packages/component
   ./install /usr/ssn --activate
   ```

   For components that require sudo:

   ```
   cd /usr/ssn/release/component/CURRENT/packages/component
   sudo -E ./install /usr/ssn --activate
   ```

7. The **`install`** command updates the properties files in `/usr/ssn/CONF/CURRENT` by merging in the new properties.

   Examine and edit if necessary the *`component`*`.properties`, product properties files, and `shared.properties` files in `/usr/ssn/CONF/CURRENT`.

   Make changes as needed to these files. Refer to the related chapters in this document for details about the properties files.

8. If a new version is available, install the new TIBCO conf files. (For more detail, see Upgrading TIBCO Conf files on page 73.)

   a. Stop TIBCO EMS.

   b. Copy `queues.conf`, `stores.conf`, and `factories.conf` from the new package to `/usr/ssn/thirdparty/tibco/CURRENT/tibco/cfgmgmt/ems/data`

   c. Start TIBCO EMS.

9. Perform CAAS client integration:

   Copy *`<application_name>`*`_caas_role_priv.xml` from `/usr/ssn/`*`<application_name>`*`/CURRENT/etc` to `/usr/ssn/DATA/caas/xmldoc`

10. Copy DMS plugins:

    Locate the **dms-plugin** directory generated by the installation and copy the plugin jar files to the DMS plugins location:

    cd /usr/ssn/<*component*>/CURRENT/dms-plugin

    cp *.jar /usr/ssn/DATA/dms/plugins

11. Configure each application being upgraded:

    cd /usr/ssn/<*component*>/CURRENT

    ./configure

    For components that require sudo:

    cd /usr/ssn/<*component*>/CURRENT

    sudo -E ./configure

    For example, to configure the AMM DB:

    cd /usr/ssn/db/CURRENT

    ./configure

12. If applications are running on separate hosts, merge the contents of all the `client_props.generated` files together and place the merged file into `/usr/ssn/CONF/CURRENT` on each host. See If installing on multiple hosts on page 17 for information on this file.

13. Upgrade the database schema for the applications that require it: CAAS, DLCA, FSU-SAM, FWU, MPC, SensorIQ, and ODS, depending on which of these you have installed.

    cd /usr/ssn/<*component*>/CURRENT/database/bin

    ./upgrade.sh

14. Start each component that you shut down:

    cd /usr/ssn/*component*/CURRENT/bin

    ./init.sh start

For information about starting and stopping all components, see Starting and stopping applications on page 66.

Upgrading AMMJMSRoute

If the value for `AMMJWSROUTE_JAVA_HOME` in `ammjmsroute.properties` is currently `${APP_INSTALLDIR}/thirdparty/java/jdk-1.8.0_161-64`, it should be changed to the new default value of **`${AMMJMSROUTE_DEFAULT_JAVA_HOME}`**. This will allow future upgrades to pick up any version changes automatically.

Remove the other previously public configuration keys from `ammjmsroute.properties`. The application will fail to start if they are not changed, as the keys no longer exist as public or private. The list is:

```
AMMJMSROUTE_MULE_VERBOSE_GC=-verbose:gc
AMMJMSROUTE_MULE_PRINT_GC_DETAILS=-XX:+PrintGCDetails
AMMJMSROUTE_MULE_PRINT_GC_TIMESTAMPS=-XX:+PrintGCTimeStamps
AMMJMSROUTE_MULE_PRINT_GC_DATESTAMPS=-XX:+PrintGCDateStamps
AMMJMSROUTE_MULE_GC_LOGFILE=-Xloggc:${INSTALL_BASEDIR}/logs/gc.log
```

The upgrade instructions are only relevant if upgrading from UtilityIQ 4.13.x or an earlier version.

Upgrading TIBCO Conf files

Always make sure you install the newest TIBCO conf files, available with the shared services release. Refer to SSC release notes to determine if the TIBCO conf file updates affect your applications.

To replace TIBCO conf files:

1. Stop TIBCO EMS:

   ```
   cd /usr/ssn/thirdparty/tibco/CURRENT/ems/8.6/bin
   ./tibemsadmin ssl://7243
   shutdown
   ```

2. Replace TIBCO conf files:

   Unzip the new package and copy all files into `/usr/ssn/thirdparty/tibco/CURRENT/tibco/cfgmgmt/ems/data`

3. Start TIBCOM EMS:

   ```
   cd /usr/ssn/thirdparty/tibco/CURRENT/ems/8.3/bin
   ./tibemsd64 -config
   /usr/ssn/thirdparty/tibco/CURRENT/tibco/cfgmgmt/ems/data/tibemsd.conf &
   ```

About products using ESB server

It is no longer necessary to install a standalone version of Mule or install ESB Server, SSNI Services (ssnservices), or Mule standalone. If you are upgrading one of the applications that used to require ESB Server but that now embeds Mule:

SSNI Services (ssnservices) must be undeployed from the host that ran ESB Server:

```
cd /usr/ssn/ssnservices/CURRENT/bin
./init.sh stop
```

Make sure that the application is no longer listed in `usr/ssn/thirdparty/mule/CURRENT/apps`

Perform a fresh installation on the product using the procedures in this document.

Upgrading FSU-SAM

To upgrade FSU-SAM from 4.11.x or earlier to the latest version of FSU-SAM:

1. Shut down FSU-SAM

   `cd /usr/ssn//CURRENT/bin`

   `./init.sh stop`

2. Make sure you have installed all dependency components, such as the required versions of Oracle, Tomcat, and JDK. Refer to the *Gen™X Compatibility and Requirements Matrix* for information on supported versions.

3. Set up the staging area for the new software.

   In `/usr/ssn/release/sam`, change the CURRENT symlink to PREVIOUS and create a new CURRENT symlink.

   `cd /usr/ssn/release/`*`sam`*

   `mv CURRENT PREVIOUS`

   `mkdir` ***`newversionnumber`***

   `ln -s newversionnumber CURRENT`

   where *newversionnumber* is the release number of the component package; for example, **5.3.0b384697**.

4. Unzip the installation package from the `sw` directory into the `CURRENTdirectory`:

   `cd /usr/ssn/release/`*`component`*`/CURRENT`

   `unzip /usr/ssn/sw/caas-1.13.1b353780.zip`

5. Install and activate the new component:

   `cd /usr/ssn/release/sam/CURRENT/packages/sam`

   `./install /usr/ssn --activate`

6. The **`install`** command updates the properties files in `/usr/ssn/CONF/CURRENT` by merging in the new properties.

   As necessary, update the `sam.properties` file in `/usr/ssn/CONF/CURRENT`.

7. Run the `configure` script after you have saved the properties files.

   `cd /usr/ssn/sam/CURRENT`

   `./configure`

8. Integrate FSU-SAM into CAAS:

```
cd /usr/ssn/sam/CURRENT/etc

cp fsu-sam_caas_role_priv.xml /usr/ssn/caas/CURRENT/xmldoc
```

9. Upgrade the database schema

   ```
   cd /usr/ssn/sam/CURRENT/database/bin/

   ./create-schema.sh

   ./upgrade.sh
   ```

   When prompted, enter the Oracle privileged user login and password created as described in The privileged user on page 14.

10. Start FSU-SAM and install the client software.

Upgrading Trap Router

This section is for upgrading Trap Router from a version earlier than 1.1.3 to version 1.1.3 or later.

Starting with version 1.1.3 in SSC 2.4.7:

- It is no longer necessary to install a standalone version of Mule or install ESB Server for Trap Router, because Trap Router installs its own embedded version of Mule eliminating the need for a Trap Router-specific version of ESB Server, SSNI Services (ssnservices), or Mule.
- There is a new port 5683 for Jolokia.

1. Shut down the version of ESB Server, SSNI Services, and Mule you have running on the Trap Router host.
2. The shutdown should remove the existing version of Trap Router. (Starting with version 1.1.3, it is no longer a requirement to install Trap Router with ESB Server.) After you shut down Trap Router, check that the directory `/usr/ssn/thirdparty/mule/CURRENT/apps/traprouter` no longer exists.
3. In `/usr/ssn/CONF/CURRENT/traprouter.properties`, remove the lines for `TRAPROUTER_ROUTE_CONFIG_DIR` and `TRAPROUTER_MULE_INSTALLDIR` and their values. The new version of Trap Router has defaults that work with the embedded Mule, so you want the new installation to use the new defaults.
4. Copy the contents of /usr/sns/DATA/esbserver/xmldocs to the new default location, `/usr/ssn/DATA/traprouter/xmldocs/`. If it does not exist, create the directory.
5. Install Trap Router according to the procedure included in *SSC Installation Guide*.

C Installation worksheet

To successfully perform an installation or upgrade, keep a spreadsheet that contains all the values that are used repeatedly throughout the process. You should have already started a worksheet based on the information needed for an SSC installation, as described in the *SSC Installation Guide*. Continue to populate the worksheet every time you configure applications or application servers to ensure consistency.

The following table includes some examples of things you will want to track in the worksheet that are specific to an AMM/FWU/MPC installation. Refer to the *SSC Installation Guide* for more information.

Table 9 Installation worksheet

Information needed	Example
appname. This refers to the Itron abbreviations used as part of the CNAME and in naming installation directories and SSL keystores, Use the names shown at right to conform with Itron naming convention. Include them only if you are installing those applications.	**Appname|Product Name|File name** `ammwsroute:` AMMWSRoute (ammwsroute), required for AMM. `db`: Database; a required component for AMM. No CNAME required `fwu`: Firmware Upgrader (FWU), an optional UtilityIQ component `gmr01`: Global Meter Reader (GMR), a required component for AMM **meterplugins**: Meter Plugins, required for AMM. No CNAME required. `mt`: Middle Tier (MT) a required component for AMM `mpc`: Meter Program Configurator (MPC), an optional UtilityIQ component)
CNAMES for all applications being installed. CNAME = *appname*.{SHARED_DOMAIN_NAME} Use the names shown at right to conform with Itron naming convention.	**CNAME convention examples:** fwu.smartgrid.utility.com gmr01.smartgrid.utility.com mt.smartgrid.utility.com mpc.smartgrid.utility.com
SSL certificate keystores. These names are based on the *appnames* listed in this table. Keystores all reside in `/usr/ssn/thirdparty/certs` on their respective servers. Use the names shown at right to conform with Itron naming convention.	These are the names for the SSL keystores required for these products: fwu.jks gmr01.jks mpc.jks

Table 9 Installation worksheet (continued)

Information needed	Example
Keykeep.store locations for file-based keykeep. SSC components do not use keykeeps. If you are using an HSM, these locations will be different. Refer to the *KeySafe and Critical Operations Protector (COP) Installation and Upgrade Guide*.	**FWU**: /usr/ssn/DATA/fwu/nicnackeystore **GMR:** /usr/ssn/DATA/gmr/nicnackeystore **MPC**: /usr/ssn/DATA/mpc/nicnackeystore
Database usernames for Oracle database	By default, your database usernames will be based on the SHARED_DB_USER_PFX property found in the `shared.properties` configuration file. This property indicates the "prefix" used to create all database names for all applications. For example, SHARED_DB_USER_PFX might be **DBuser** This will generates an automated AMM database application user: **DBuserm_app** Refer to the properties files for each application to see how usernames are generated. If upgrading from versions earlier than 4.10: If your earlier database user names have an extension of **_amm**, not **_app**, you will need to override at least some of the names that are generated by editing the `amm.properties` file. You may override the default names if desired. Most applications provide default naming that you will not see unless you go into the `masterlist.component` files in the component's etc directory. If you want to override the database username for any given application, refer to the `masterlist.component` file and copy the relevant properties into the properties files in `/usr/ssn/conf/CURRENT`.
Encrypted database passwords	Passwords are encrypted with the encrypt utility found in the utils directory for each application; for example: `/usr/ssn/`*component*/CURRENT/install_data/utils. **`encrypt`** ***`cleartextpassword`*** where *cleartextpassword* is an unencrypted open-text password.

Table 9 Installation worksheet (continued)

Information needed	Example
Key password when generating private key for SSL certificates Use the password shown at right (literally **changeit**) to conform with Itron naming convention. Although it appears that you are being asked to change the password, this is a standard Tomcat default. If you do choose to create a password other than this one, you must make sure you change it in the Tomcat installation files as well. Itron does not provide instructions for changing the defaults in a Tomcat installation.	**changeit**
Port number for the database (usually 1521) This value is in the `shared.properties` file. Itron recommends that you not change the ports; however, your firewall administrator may wish to make changes. If so, you must be aware of them to edit the `shared.properties` file and document those changes in your Worksheet.	1521
Google Maps Client ID. This is a license ID provided by Google and will be stored in the db.properties file.	Go to https://developers.google.com/maps/documentation/business for more information.
Override required properties in `amm.properties`. See AMM.Properties on page 79 for details.	`AMM_GMR_NODE1_HOST` `AMM_BROADCAST_UDP_MCAST_ADDR`

D AMM.Properties

Whenever you install an AMM application, a file called `/usr/ssn/CONF/CURRENT/amm.properties` is created. The `amm.properties` file contains defaults and override properties that apply to all AMM applications.

In most cases, you need to modify only the properties that are labeled OVERRIDE_REQUIRED. The default property value is anticipated to be correct with no need for modification. If you do need to make a change, copy the property from the following table or `masterlist.shared`, modify the default value, and add it to the application's individual *component*.properties file (for example, `/usr/ssn/CONF/CURRENT/caas.properties` or `/usr/ssn/CONF/CURRENT/mt.properties` or any other component properties file that is generated).

Table 10 amm.properties

Property	Description
AMM_PLUGINS_DIR	Location of Meter Plugins. Default is **${APP_INSTALLDIR}/meterplugins/CURRENT/lib**
AMM_SCHEDULE_BUFFER_MINUTES	Allows for an additional buffer before scheduling system created jobs.
AMM_WEBAPP_SSL_PORT	Port used for secure web services. The default of **3010** is correct unless you are asked by your firewall administrator to change it. Default is **3010**
AMM_WEBAPP_SCP_PASSWORD	**Override required.** MT password for SCP
AMM_WEBAPP_SCP_USER_NAME	MT username for SCP.Default is **ssn**
AMM_WEBAPP_EXPORT_DIRECTORY	MT directory for the export files output by AMM. Default is **${APP_INSTALLDIR}/DATA/mt/export**
AMM_MASTER_APP_USER	Oracle user containing the UtilityIQ schema. Default is **${SHARED_AMM_DB_APP_USER}**
AMM_MASTER_APP_PASSWORD	Encrypted password for user access to the database, taken from the `shared.properties` file. Default is **${SHARED_DB_USER_PASSWORD}**
AMM_SL_ENABLED	Indicates if this AMM instance is used by the Street Light Adapter. Default is **false**

Table 10 amm.properties (continued)

Property	Description
AMM_MASTER_SCHEMA_ORACLE_URL	User interface for AMM. Default is jdbc:oracle:thin:@(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=${SHARED_AMM_DB_HOST})(PORT=${SHARED_AMM_DB_PORT}))(LOAD_BALANCE=yes))(CONNECT_DATA=(SERVICE_NAME=${SHARED_AMM_DB_SERVICE_NAME})(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=5)(DELAY=1))))
AMM_MASTER_APP_USER	**Override required.** AMM database schema user. The SHARED_DB_USER_PFX defined in shared.properties is appended with "m." Default is **${SHARED_DB_USER_PFX}m**
AMM_MASTER_SCHEMA_PASSWORD	**Override required.** AMM database schema password. Default is ${SHARED_DB_USER_PASSWORD}
AMM_DMS_CAAS_USERNAME	Credentials used to access DMS
AMM_DMS_CAAS_PASSWORD	**Override required**. Password for credential used to access DMS.
AMM_ERT_TRAP_PROCESSING_BUFFER_MINUTES	Allow some extra time to receive and process traps before starting data reconciliation.
AMM_ERT_FW_TRAP_RETRY_BUFFER_MINUTES	Allow some time to counter trap retry window in FW before starting data reconciliation
AMM_MASTER_DB_UPDATE_ROLE	AMM database master schema read/write role. The AMM_MASTER_SCHEMA_USER defined above defined in shared.properties is appended with "m." Default is **${AMM_MASTER_SCHEMA_USER}_rw**
AMM_MASTER_SCHEMA_ORACLE_URL	Database access for the AMM master. Default is =jdbc:oracle:thin:@(DESCRIPTION=(ENABLE=BROKEN)(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=${SHARED_AMM_DB_HOST})(PORT=${SHARED_AMM_DB_PORT}))(LOAD_BALANCE=yes))(CONNECT_DATA=(SERVICE_NAME=${SHARED_AMM_DB_SERVICE_NAME})(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=5)(DELAY=1))))
AMM_MASTER_DB_SELECT_ROLE	AMM database master schema read-only role. Default is **${AMM_MASTER_SCHEMA_USER}_role**

Table 10 amm.properties (continued)

Property	Description
AMM_S1_APP_USER	App user for Segment 1. If doing a fresh installation, you do not need to make any changes to this property—it is set to the SHARED_DB_USER_PFX in the shared.properties file, with "s1_app" appended to it to generate the username. It is recommended you leave the value unchanged and allow AMM to auto-generate the DB names. However, if you are upgrading from a previous version and you already have created database user names that are different, you can override the default values of this property.
AMM_S1_APP_PASSWORD	Password for the Segment 1 app user. You do not need to make any changes to this property—it is set to the SHARED_DB_USER_PASSWORD in the shared.properties file. If you do want a different password for this user, change it here.
AMM_S1_SCHEMA_USER	AMM schema username. The SHARED_DB_USER_PFX defined in shared.properties is appended with "s1" Default is **${SHARED_DB_USER_PFX}s1**
AMM_S1_SCHEMA_PASSWORD	AMM schema user's password. Default is **${SHARED_DB_USER_PASSWORD}**
AMM_S1_SCHEMA_ORACLE_URL	Database access for the Segment 1 user. You should not need to make any changes to this property if you follow all the recommendations in this document. Location of segment ID. Default is **${AMM_MASTER_SCHEMA_ORACLE_URL}**
AMM_S1_DB_UPDATE_ROLE	Read/write role for the Segment 1 user. Default is **${SHARED_DB_USER_PFX}s1_rw**
AMM_S1_DB_SELECT_ROLE	Read-only role for the AMM Segment 1 user. Default is **${SHARED_DB_USER_PFX}s1_ro**
AMM_S2_APP_USER	App user for Segment 2. Default is **${SHARED_DB_USER_PFX}s2_app**
AMM_S2_APP_PASSWORD	Password for Segment 2 app user. Default is **${SHARED_DB_USER_PASSWORD**}
AMM_S2_SCHEMA_USER	Schema user for Segment 2. Default is **${SHARED_DB_USER_PFX}s2**
AMM_S2_DB_UPDATE_ROLE	Read/write role for the Segment 2 user. Default is **${SHARED_DB_USER_PFX}s2_rw**

Table 10 amm.properties (continued)

Property	Description
AMM_S2_SCHEMA_ORACLE_URL	URL for the segment 2 database. Default is **${AMM_MASTER_SCHEMA_ORACLE_URL}**
AMM_S2_SCHEMA_PASSWORD	Password for the Segment 2 user. Default is **${SHARED_DB_USER_PASSWORD}**
AMM_S2_DB_SELECT_ROLE	${SHARED_DB_USER_PFX}s2_ro
AMM_GMR_NODE1_SEGMENT_IDS	Node segment ID list handled by GMR 1; for example **1:2:3** means GMR 1 handles segments 1, 2, and 3. 1:3 means GMR 1 handles segments 1 and 3 (not 1-3). If you have more than one GMR, add a new line and value for GMR 2's segment ID list; for example: AMM_GMR_NODE2_SEGMENT_IDS. Default is 1:2
AMM_GMR_NODE1_HOST	**Override required**. GMR host URL. For example, **gmr01.smartgrid.utility.com**. If you have more than one GMR, add a new line for the second; for example: AMM_GMR_NODE2_HOST
AMM_ENABLE_IN_TRANSIT_ENCRYPTION	Enables Oracle data encryption in transit. Default is **true**. The encryption algorithms supported for Oracle in transit encryption. Only required if GMR_ENABLE_IN_TRANSIT_ENCRYPTION = true. AMM_THIN_NET_CHECKSUM_TYPES=SHA256,SHA384,SHA512 The encryption algorithms supported. AMM_THIN_NET_ENCRYPTION_TYPES=AES256
AMM_METRICS_HOST	Leave this blank to disable metric reporting.
AMM_JMS_INTERNAL_SSNEVENTQ_NAME	(Optional, for TBR.) This property corresponds to **/queue/InternalSSNSLEventQ,** an external queue in /usr/ssn/tbr/CURRENT/etc/masterlist.component that prevents TALQ Bridge from accidentally reading contents from an AMM system not being used for Street Light management. This corresponding property in amm.properties can be customized by copying the property from this table or from /usr/ssn/db/CURRENT/etc/masterlist.product and adding the property to amm.properties, setting the value to be the same as the TBR queue.

Table 10 amm.properties (continued)

Property	Description
AMM_JMS_INTERNAL_SSNEXPORTQ_NAME	(Optional, for TBR.) This property corresponds to **/queue/InternalSSNSLExportQ**, an external queue in /usr/ssn/tbr/CURRENT/etc/masterlist.component that prevents TALQ Bridge from accidentally reading contents from an AMM system not being used for Street Light management. This corresponding property in amm.properties can be customized by copying the property from this table or from /usr/ssn/db/CURRENT/etc/masterlist.product and adding the property to amm.properties, setting the value to be the same as the TBR queue
AMM_JMS_INTERNAL_SSNODRQ_NAME	(Optional, for TBR.) This property corresponds to **/queue/InternalSSNSLODRQ,** an external queue in /usr/ssn/tbr/CURRENT/etc/masterlist.component that prevents TALQ Bridge from accidentally reading contents from an AMM system not being used for Street Light management. The corresponding property in amm.properties is AMM_JMS_INTERNAL_SSNODRQ_NAME. This can be customized by adding the property to amm.properties and setting the value to be the same as the TBR queue.
AMM_PLUGINS_DIR	Location of the Meter Plugins. There is no need to change this value. When you install the Meter Plugins as described in Installing Meter Plugins on the GMR Server they will be put into this directory.
AMM_JMS_INTERNAL_SSNEVENTQ_NAME	Add this property to amm.properties and set the value to be the same as that of TBR_TIBCOEMS_TRAP_DEST_NAME in tbr.properties. Default is **/queue/InternalSSNSLEventQ**
AMM_JMS_INTERNAL_SSNEXPORTQ_NAME	Add this property to amm.properties and set the value to be the same as that of TBR_TIBCOEMS_EXPORT_DEST_NAME in tbr.properties. Default is **/queue/InternalSSNSLExportQ**
AMM_JMS_INTERNAL_SSNODRQ_NAME	Add this property to amm.properties and set the value to be the same as that of TBR_TIBCOEMS_METER_READ_DEST_NAME in tbr.properties. Default is **/queue/InternalSSNSLODRQ**
AMM_GDT_TIME	Used to configure the time of the Gas Day Take read. Format must behh:mm. Default is **09:00**
AMM_GDT_TIMEZONE	Used to configure the timezone of the Gas Day Take read. Timezone must be from the list of timezones in the TZ database: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

E Shared properties

Whenever you install an application, changes are merged into `/usr/ssn/CONF/CURRENT/shared.properties` and the file is regenerated.

The following table is a reference to all of the properties that exist or *can* exist in the `shared.properties` file. Not all of these properties apply to every installation. To update shared properties for any given individual installation, review the `shared.properties` file that is generated in `/usr/ssn/CONF/CURRENT` after you have completed the installation and activation.

Modify any property files that are labeled OVERRIDE_REQUIRED or need changing by editing `/usr/ssn/conf/CURRENT/shared.properties`. If a property only need to be changed for a single application, copy the property into the component property file (for example, `/usr/ssn/CONF/CURRENT/caas.properties` or `/usr/ssn/CONF/CURRENT/mt.properties` or any other component properties file that is generated) and modify its value. That property will be overridden only for that application.

In most cases, you need to modify only the properties that are labeled OVERRIDE_ REQUIRED. The default property values are anticipated to be correct with no need for modification.

The `/usr/ssn/conf/CURRENT/shared.properties` file should be kept as a single instance and be made accessible to all hosts rather than keeping a separate version on each application server. Otherwise, you must copy updates to all application servers whenever you make a change.

Properties shown in the shared.properties Table are in alphabetical order. This does not necessarily reflect the order they will appear in your installation's `shared.properties` file.

Table 11 shared.properties

Property	Component affected	Description
SHARED_AMM_DB_APP_USER	AMM	Database application user. The default value is correct if you follow the recommendations in this document. This name is automatically generated by appending **m_app** to the SHARED_DB_USER_PFX you created. For example, if your SHARED_DB_USER_PFX is DBuser, then the app user will be generated as **DBuserm_app**. It is recommended that you accept the naming convention for the DB users as they are generated. An exception would be if you were upgrading from an earlier version of AMM and have existing database schemas. In that case, you can override the naming conventions by manually changing the value of the username or of the suffix. In all cases, whether or not you override the naming system, record the database user names in the worksheet. Default is **${SHARED_DB_USER_PFX}m_app**
SHARED_AMM_DB_APP_USER_PASSWORD	AMM	Encrypted password for the database app user. The default value is correct if this will be the same password as was entered for the SHARED_DB_USER_PASSWORD. If you have a different password for the AMM app user, change this value. The encrypt tool is in /usr/ssn/<*component*>/CURRENT/install_data/utils Default is **${SHARED_DB_USER_PASSWORD}**
SHARED_AMM_DB_HOST	AMI applications that use the Oracle database	**Override required**. Fully qualified Oracle database instance host name for the Oracle database the application is using.
SHARED_AMM_DB_PORT	AMI applications that use the Oracle database	**Override required**. The port number on which the Oracle server is listening for requests.
SHARED_AMM_INTERNAL_WEBAPP_SSL_PORT		Port used for cross-application internal web services. In most cases, this should replace SHARED_AMM_WEBSERVICE_PORT. Default is **3043**.
SHARED_AMM_SEGMENT_DB_PORT		Port for the AMM segment DB Oracle listener. Update if segment schemas are on a separate RDBMS as the master schema. Default is **${SHARED_AMM_DB_PORT}**

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_AMM_DB_SERVICE_NAME	AMI applications that use the Oracle database	**Override required** The Oracle database service name or TNS name registered with the listener.
SHARED_AMM_SEGMENT_DB_SERVICE_NAME	AMI applications that use the Oracle database	Service name for the AMM segment Oracle database. Update if segment schemas are on a separate RDBMS as the master schema. Default is **${SHARED_AMM_DB_SERVICE_NAME}.**
SHARED_AMM_SEGMENT_DB_HOST	AMI applications that use the Oracle database	Host name for the AMM segment Oracle database. Update if segment schemas are on a separate RDBMS as the master schema. Default is **${SHARED_AMM_DB_PORT}**.
SHARED_AMM_WEBAPP_APP_CONTEXT	AMM	AMM web application context. The default is **amm**.
SHARED_AMM_WEBAPP_HOST	AMM, Network Center	MT host CNAME. The MT host should resolve to the shared domain name, which is defined in this file. The default is. **mt.${SHARED_DOMAIN_NAME}** If you are not using AMM or have ssnservices running on its own host with an ssnservices keystore, this property must be copied into ssnservices.proeprties and modified.
SHARED_AMM_WEBSERVICE_PORT	AMM	Port used for secure web services. The default of **3010** is correct unless you are asked by your firewall administrator to change it. Default is **3010**.
SHARED_CAAS_APP_CONTEXT	CAAS	CAAS web application context. The default is **caas**.
SHARED_CAAS_HOST	CAAS	Host name of the machine where CAAS is installed. The default value **caas.${SHARED_DOMAIN_NAME}** is correct. The CAAS host should resolve to the shared domain name defined in this file.
SHARED_CAAS_SSL_PORT	CAAS	CAAS server SSL port. The default value of **6343** is correct unless you are asked by your firewall administrator to change it.

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_CERT_LOCATION_DIR	All applications that require SSL certificates.	Location for all SSL keystores. The default is correct if you follow the recommendations in this document. Default is **${APP_INSTALLDIR}/thirdparty/certs**
SHARED_COUNTRY_CODE	All	Country code used to construct user locale, as defined in ISO 3166-1 alpha-2. If needed, change this to the appropriate two-letter country code. Default is **US**.
SHARED_DB_LANGUAGE	All applications that use the Oracle database	Oracle database value that sets format for language characteristics. Change this only if your DBA requires it. The default is **AMERICAN**.
SHARED_DB_TERRITORY	All applications that use the Oracle database	Oracle database value that sets format for date and number characteristics. Change this only if your DBA requires it. The default is **AMERICA**.
SHARED_DB_USER_PFX	All	**Override required**. A prefix used as part of the default DB user name for all applications. Review
SHARED_DB_USER_PASSWORD	All applications that use the Oracle database	**Override required.** Default database password used if no other is specified. The assumption is that a user will typically use only one password across all the application databases. If you do use more than one password, choose one of them as the main one as the value for this property, in encrypted format. The encrypt tool is in /usr/ssn/*<component>*/CURRENT/install_data/utils
SHARED_DMS_APP_USER	DMS	CAAS user name used by dms-client to connect to the dms-server. Default is =${SHARED_DB_USER_PFX}dms_app
SHARED_DMS_APP_PASSWORD	DMS	Shared DB user password. ${SHARED_DB_USER_PASSWORD}

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_DB_USER_PFX	All applications that use the Oracle database	**Override required**. Basic database user name prefix. This must be a unique string that is not already in use; for example, **SGSDBuser**. A suffix for each application will be added to this name to generate default names for all application database users. To determine the name suffixes for each component or to override the automatic names, refer to the masterlist.component file in the etc directory for a given component.
SHARED_DMS_HTTP_HOST	DMS	DMS CNAME recommended by Itron. The DMS host should resolve to the shared domain name, which is defined in this file. Default is **dms.${SHARED_DOMAIN_NAME}**
SHARED_DMS_HTTP_PORT	DMS	DMS server port. Default is **7080**
SHARED_DMS_HTTP_SSL_PORT	DMS	DMS server SSL port. Default is **7043**
SHARED_DNS_DOMAIN	Registrar	**Override required**. DNS zone for all entries in the reg DNS database. Set to **sg.${SHARED_DOMAIN_NAME}**
SHARED_DNS_HOST	Registrar	The CNAME for DNS. The Registrar host should resolve to the shared domain name, which is defined in this file. Default is **reg01.${SHARED_DOMAIN_NAME}**
SHARED_DNS_PORT	Registrar	DNS server port. The default value is **53** .
SHARED_DNS_REST_PORT	Registrar	DNS server port for REST communication. The default value is **8182**
SHARED_DOMAIN_NAME	All	**Override required**. Domain name for all hosts as defined in the Worksheet. This domain name is used in CNAMEs for all applications. For example, **smartgrid.utility.com** If any host requires a different shared domain name, that name can be manually added to the properties file for that specific application.
SHARED_EMAIL_FROM_ADDRESS	AMM	**Override required**. Address that AMM mail will appear to come from. Change this to an email address within your organization.

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_EMAIL_LOCALE_COUNTRY_CODE	All	Two-letter country code to indicate the country code for the email that originates from the application. Default is **US**. If email originates from a different location, change this to the appropriate Java two-letter language code.
SHARED_EMAIL_LOCALE_LANGUAGE_CODE	AMM	Two-letter language code to indicate the language email will be sent in. Default is English (**EN**). If communications to the user will be in a different language, change this to the appropriate Java two-letter language code.
SHARED_EMAIL_SMTP_SERVER	AMM	**Override required**. Outgoing SMTP email server. Change this to an email server within your organization
SHARED_ENVIRONMENT_TYPE	All applications with a UI	Environment name that will be displayed in the user interface. Default is **Production**.
SHARED_SECONDARY_ENV_LABEL		Defines username for Gateway accounts for secondary environments. This property ensures that customers with an AMM instance using the gateway of another instance of AMM don't use the same account name. Users with multiple secondary environments pulling data from the same primary environment, must ensure that each label is unique. Regex will enforce that, if set, it starts with a non-numeric character and be no more than 8 characters long. For example, "wtr", "wtr01", "sla", "ucp01", "ucp02".
SHARED_ENVIRONMENT_TAG		Used by some SLDP apps as the default value for options that need to uniquely represent an environment. For managed/SaaS custorers: set to an environment's service.
SHARED_ENVIRONMENT_SIZEs	Applications that have been updated to support sizing autoconfiguration	Size of the environment. Options are MICRO|SMALL|MEDIUM|LARGE|XLARGE. (There is no default.) This drives autoconfiguration of sizing properties that previously were set manually. MICRO: fewer than 200K endpoints SMALL: 200K endpoints MEDIUM: 200K-2.5 million endpoints LARGE: 2.5-6 million endpoints XLARGE: greater than 6 million endpoints

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_500S_ENABLED		Required if using 500S devices. If SHARED_500S_ENABLED is **true** TMB_DYNAMIC_SECURE_LISTENER_ENABLE should be set to **true**.
SHARED_GATEWAY_HOST	Any applications using the Gateway	Gateway host. Default is **gateway.${SHARED_DOMAIN_NAME}**
SHARED_GATEWAY_PORT	Any applications using the Gateway	Gateway port. Default is **7881**.
SHARED_HELP_URL	All applications with a UI	Target window that opens when a user clicks the Help link. Default is **https://access.itron.com.** This sends the user to the home page of Itron's customer portal https://access.itron.com, where they can browse for documentation.
SHARED_LANGUAGE_CODE	AMM	ISO 639-1 two-character language code. Default is English (**EN**). If communications to the user will be in a different language, change this to the appropriate two-letter language code. This does not change the language of the user interface.
SHARED_MASTERMETER_ENABLED		Set to true if Master Meter is enabled is the environment. Default is **false**
SHARED_MASTERMETER_PSK		Encryption key for use by DLCA and AMM(MT) for Master Meter. This is required if SHARED_MASTERMETER_ENABLED is set to true
SHARED_MILLI_ENABLED		Set to **true** if Milli is enabled is the environment. Default is **false**.
SHARED_MILLI_REQUEST_DEFAULT_TIMEOUT_SECONDS	Milli devices	Expected timeout for Mill devices in seconds. Default is **3600** (one hour)
SHARED_MQTT_BROKER_SSL_PORT		SMQTT host port.. Default is **8833**.
SHARED_MQTT_BROKER_URI		MQTT host URI. ssl://hivemq.${SHARED_DOMAIN_NAME}:${SHARED_MQTT_ BROKER_SSL_PORT

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_NEC_HOST	HCM	CNAME for NEC. Used by HCM to find NEC. The default value is nec.${SHARED_DOMAIN_NAME} is correct. The NEC host should resolve to the shared domain name, which is defined in this file.
SHARED_NEC_HTTP_PORT	NEC	NEC server HTTP port. The default value is **6980**
SHARED_NEC_HTTPS_PORT	NEC	NEC server HTTPS port. The default value is **6943**
SHARED_NMS_HOST	NC	CNAME for NC. The default value **cepnms.${SHARED_DOMAIN_NAME}** is correct. The NC host should resolve to the shared domain name, which is defined in this file.
SHARED_NMS_SSL_HTTP_PORT	NC	NC server HTTPS port. The default value is **7543.**
SHARED_ORACLE_FAILOVER_DB_HOST	All	Shared Oracle db host
SHARED_ORACLE_FAILOVER_DB_PORT	All	Shared Oracle db port
SHARED_ORACLE_FAILOVER_DB_ SERVICE_NAME	All	Shared Oracle db service name
SHARED_SECONDARY_ENV_LABEL	AMM	Label used to augment the username for Gateway accounts for secondary environments, where AMM is using another instance of Gateway. This label ensures that both Gateway account have unique names.
SHARED_SSL_CIPHER_LIST		Comma-separated list of SSL ciphers for TLS 1.2 supported by the web server.
SHARED_SSL_PROTOCOL_LIST		Comma-separated list of SSL protocols supported by the web server. Supported value is: **TLSv1.2**
SHARED_TIBCOEMS_AUTH_PASSWORD	All applications that use TIBCO EMS	Encrypted version of TIBCO EMS user's password, which was set while installing TIBCO EMS. The encrypt tool is in /usr/ssn/<*component*>/CURRENT/install_data/utils Default is **UH+pA2H/HDA4JbJXYMWwjw==** This must be changed to match the password you set during your TIBCO EMS installation.

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_TIBCOEMS_AUTH_USER	All applications that use TIBCO EMS	TIBCO EMS user, which should be **ssn** as recommended by Itron. Default is **ssn**.
SHARED_TIBCOEMS_HOST	All applications that use TIBCO EMS	**Override required**. CNAME for TIBCO EMS. The TIBCO host should resolve to the shared domain name, which is defined in this file. The default value is **tibco.${SHARED_DOMAIN_NAME}**
SHARED_TIBCOEMS_SSL_PORT	TIBCO EMS	JMS messaging between back-office components; message broker for delivering data to customers. The default value of **7243** is correct unless you are asked by your firewall administrator to change it.
SHARED_TIMEZONE	All	**Override required**. Timezone for your organization's locale. Refer to Time Zone Formats on page 95 for information about other options. US timezones are: **America/Adak** **America/Anchorage** **America/Cayman** **America/Chicago** **America/Denver** **America/Los_Angeles** **America/Martinique** **America/New_York** **America/Phoenix**
SHARED_TOMCAT_INSTALLDIR	All applications that require Tomcat	Location of the shared Tomcat version. The newer versions of the applications now contain a property specifying the Tomcat version and its location. You can symlink your most-used version of Java to CURRENT so that becomes the shared value shown here. The default value is **${APP_ INSTALLDIR}/thirdparty/tomcat/CURRENT**
SHARED_WATER_TIBCOEMS_HOST		Required for dual stack environments. TIBCO messaging server water host. Default is **tibco.${SHARED_DOMAIN_NAME}**

Table 11 shared.properties (continued)

Property	Component affected	Description
SHARED_WATER_TIBCOEMS_SSL_PORT		TIBCO SSL port (water) Default is **7243**
SHARED_WATER_TIBCOEMS_AUTH_USER		TIBCO user (water) Default is **ssn**
SHARED_WATER_TIBCOEMS_AUTH_ PASSWORD		Password to use when authenticating with the TIBCO Messaging server water host).
SHARED_NAPROXY_HOST		NAProxy host. Default is **naproxy.${SHARED_DOMAIN_NAME}**
SHARED_NAPROXY_PORT		NAProxy port. Default is **9880**.
SHARED_ENCRYPTIONSERVICE_HOST		gRPC Encryption Service host and port. Default is **cryptkeeper.${SHARED_DOMAIN_NAME**}
SHARED_ENCRYPTIONSERVICE_PORT		gRPC Encryption Service host and port. Default is **9423**.
SHARED _GRPC_SSL_CIPHER_LIST		
SHARED_MESSAGE_TRACING_ COLLECTORPORT		
SHARED_MESSAGE_TRACING_ COLLECTORURL		

TCP Settings for GMR

This section contains suggested TCP settings at the operating system level when installing a new GMR server.

Table 12 TCP settings for GMR

net.ipv4.conf.all.send_redirects	0
net.ipv4.conf.default.send_redirects	0
net.ipv4.conf.default.accept_redirects	0
net.ipv4.conf.default.secure_redirects	0
net.ipv4.icmp_echo_ignore_broadcasts	1
net.ipv4.tcp_syncookies	1
net.ipv4.conf.all.rp_filter	1
net.ipv4.conf.default.rp_filter	1
net.ipv4.ip_local_port_range	32768 61000 (prevents port conflicts with application)
net.ipv4.tcp_timestamps	0
net.ipv4.tcp_sack	1
net.ipv4.tcp_window_scaling	1
net.ipv4.tcp_keepalive_intvl	1
net.ipv4.tcp_keepalive_probes	200
net.ipv4.tcp_keepalive_time	10 (keepalive time for updates to firewalls)

G Time Zone Formats

This section contains all of the time zone values that can be put into the SHARED_TIMEZONE property in the `shared.properties` file. See Shared properties on page 84 for more information.

America/Adak	Australia/Melbourne	Etc/GMT-7
America/Anchorage	Australia/North	Etc/GMT-8
America/Cayman	Australia/NSW	Etc/GMT-9
America/Chicago	Australia/Perth	Etc/GMT-10
America/Denver	Australia/South	Etc/GMT-11
America/Los_Angeles	Australia/Sydney	Etc/GMT-12
America/Martinique	Australia/Tasmania	Etc/GMT-13
America/New_York	Australia/West	Etc/GMT-14
America/Phoenix	Australia/Yancowinna	Etc/GMT+1
Africa/Johannesburg	Canada/Saskatchewan	Etc/GMT+2
Australia/Victoria	Brazil/AcreBrazil	Etc/GMT+3
Australia/Queensland	Brazil/DeNoronha	Etc/GMT+4
Australia/ACT	Brazil/East	Etc/GMT+5
Australia/Adelaide	Brazil/West	Etc/GMT+6
Australia/Brisbane	Canada/Newfoundland	Etc/GMT+7
Australia/Broken_Hill	GMT	Etc/GMT+8
Australia/Canberra	Etc/GMT-1	Etc/GMT+9
Australia/Darwin	Etc/GMT-2	Etc/GMT+10
Australia/Hobart	Etc/GMT-3	Etc/GMT+11
Australia/LHI	Etc/GMT-4	Etc/GMT+12
Australia/Lindeman	Etc/GMT-5	Pacific/Honolulu
Australia/Lord_Howe	Etc/GMT-6	Portugal