MC-IoT Advanced System Security User Guide

DECEMBER 2019

6802987C70-J

Contact Us

Motorola Solution Support Center

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization’s service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software.
- To confirm troubleshooting results and analysis before taking action.

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response.

However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

- Enter motorolasolutions.com in your browser
- Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
- Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

Copyrights

The Motorola products described in this document might include copyrighted Motorola computer programs. Laws in the United States and other countries preserve for Motorola certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola computer programs contained in the Motorola products described in this document might not be copied or reproduced in any manner without the express written permission of Motorola.

Furthermore, the purchase of Motorola products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Note that certain features, facilities, and capabilities described in this document might not be applicable to or licensed for use on a particular system, or might be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contents

OVERVIEW

Note: Before reading about the MC-IoT Advanced System Security and the secured MC-IoT System Tools Suite (STS), consult the ACE3600 and MC-EDGE documentation to learn about the ACE3600 and MC-EDGE system. For a list of documentation, see *Appendix C: ACE3600/MC-EDGE System Documentation*.

General Security Concept

The purpose of the MC-IoT Advanced System Security is to provide SCADA industrial control systems and other monitoring and control systems with a high level of protection from external and internal cyber threats.

In a secured MC-IoT system, the control processes have a high level of protection from attack, such as attempts to gain unauthorized access, intercept communication, attack data, compromise system integrity. Only authorized users and authorized actions are permitted.

The ACE3600 and MC-EDGE units and software tools include the following enhanced security features:

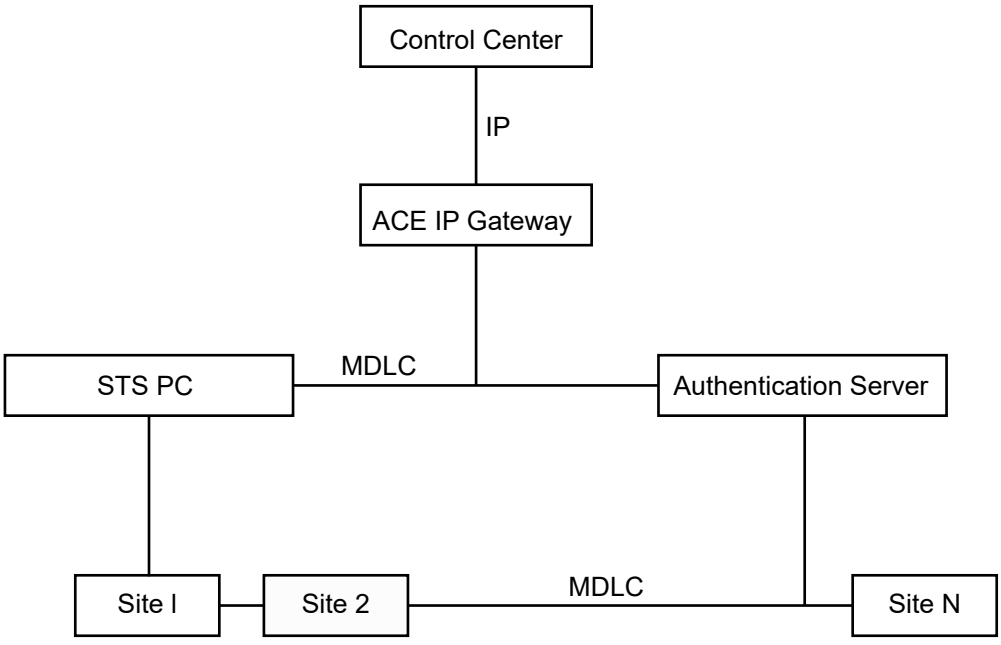
- System-wide security policy enforcement
- User accounts and user authentication
- Roles and role-based permissions
- Field unit authentication
- Communication payload encryption
- Encryption security keys management
- Data file encryption
- Security event logger
- Setup and management tool (STS)
- STS Audit trail
- IP firewall
- Run file whitelisting (ACE3600 only)
- Dedicated security repository
- RTU self test (ACE3600 only)
- Files signature

Using the STS, the system administrator defines the features of the security policy and configures the system accordingly.

MC-IoT Advanced System Security Overview

The MC-IoT secured system includes:

- Secured ACE3600 and MC-EDGE Remote Terminal Units (RTUs) – controller units with enabled security features such as access/interface control, secured communication, secured files, and security-related logs
- Secured ACE IP Gateway and FIU Front-end – communication units with secured access/interface control, secured communication, secured files, and security-related logs
- ACE3600 Authentication Server – an ACE3600 unit responsible for authenticating users in the MC-IoT secured system (in addition to functioning as a standard secured RTU)
- Secured STS – the set of software tools used to configure and manage a secured ACE3600/MC-EDGE system



Administering a secured system requires administering RTUs, Gateways, PCs and users.

Minimum RTU Hardware and Software Requirements

Advanced system security is supported on ACE3640, ACE3680, MC-EDGE and ACE IP Gateway.

Security enabled ACE3600 CPUs must be ordered from the factory.

Existing ACE3600 units cannot be upgraded and do not support the new secured firmware. The ACE3600 firmware version must be ≥ 16.00.

For minimum PC hardware and software requirements, see the *MC-IoT STS User Guide*.

MC-IoT SECURITY CONCEPT

The MC-IoT secured system includes several features. This chapter describes those features briefly.

MC-IoT System Security Policy

The MC-IoT security policy is a set of configurable system-wide security parameters used to enforce the organization's security policy in the MC-IoT system management tools (STS), front-end units and field units. These parameters are defined by the system administrators in the secured STS and applied to all units.

Only one policy can exist in an STS project and it applies to the entire system.

System Security Policy Parameters

The security policy defines the system's security parameters and behavior related to:

- User authentication and user passwords
- MDLC payload encryption
- File encryption in the RTU
- RTU and MDLC driver self test
- Logging of security events
- Whitelisting of files in the RTU (ACE3600 only)
- Message Life Time
- Security files signature hardening

The default values of policy parameters in the STS are configured for maximum protection of your system. It means that user authentication, file encryption, MDLC payload encryption, files signature, and RTU whitelisting are all enabled. For instructions on modifying the policy defaults, see the *Operation* chapter. Some parameters are relevant to the RTU, some are relevant to the STS, and some are relevant to both. For specific details on each security policy parameter, see *Appendix A: Security Policy Parameters*.

IMPORTANT: Once the policy parameters are configured, the policy, users file (required for user authentication, and keys file (required for file encryption and private key signature) must be downloaded to all units in the system.

Downloaded Security Policy

Initially, a unit is unsecured and the policy must be downloaded locally to the unit. Downloading the policy to a unit causes the unit to restart. The policy settings which

relate to MDLC payload encryption and user authentication only take effect once the necessary (and valid) security files (users and roles, keys) have been downloaded to the unit. Other policy settings such as whitelisting, file encryption, security log, and file signature take effect immediately.

If an existing policy is subsequently changed and downloaded, the users and roles, and/or keys files may need to be changed and downloaded again to match the new policy definitions. For example, if the minimum password length in the new policy is longer than in the old policy, the user passwords may need to be replaced. (If the passwords are not replaced, existing user passwords which are shorter than the new length will be rejected upon access attempt and a security event will be logged.)

Sometimes if the policy is changed in the unit, the RTU will continue operating, but will report the conflict between policy and files to the security log. For example, an RTU has a policy to change encryption keys once a month, and the keys in the RTU have duration of one month or less. The policy is then strengthened to require the keys to be changed every day. Until an appropriate keys file is downloaded with keys that change every day, the RTU will continue to operate with the old keys, but will report the conflict to the security log. This way, the RTU will remain secured while using the old keys.

IMPORTANT: If you try to download a users and roles or keys file which conflicts with the policy in the unit, the RTU will reject the file.

A unit, whose policy is configured for user authentication and for MDLC payload encryption, is only considered secured when both user authentication and MDLC payload encryption take effect. Both features will only take effect when both the users file and the keys file have been downloaded. If only MDLC payload encryption is configured, it will only take effect after the keys file is downloaded. If only user authentication is configured, it will only take effect after the users file is downloaded.

Note: If a unit does not have an encryption key downloaded, it will use nonencrypted communication.

Once the system is secured, subsequent changes to the policy, users and keys can be only be downloaded to the units by authorized users.

Security policy can only be downloaded to a unit with secured firmware (V16.0 or higher). The policy version (derived from the STS version) being downloaded must also be higher than the firmware version in the unit. Similarly, when downloading firmware to a secured unit, the firmware version must be lower than the policy version and configuration.

The security policy settings in an RTU can be viewed by administrators using the Software Diagnostics utility. For more information, see the SECPOL device in the *MC-IoT STS Software Diagnostic Output and Error Messages* manual.
Note: During encryption key swap, the key change is only reflected in the security diagnostics after the pre-defined key transmission grace period has elapsed.

Security Policy Impact

The STS GUI reflects the project policy. For example, if MDLC payload encryption is disabled, the menu item used to administer encryption keys is disabled.

The policy dictates the behavior of a system, the behavior of the STS and that of the MDLC communication driver. If a new security file (users, keys, etc.) which conflicts with the policy is downloaded to a unit, the new file is rejected. If a new policy is downloaded which is stricter than the existing keys or users file in the unit, a warning is sent to the security log.

User Authentication

To ensure system integrity, only authenticated users can access any part of the MC-IoT secured system, including the STS, front-end units and RTUs. User access is gained with valid credentials, i.e. a unique user name and password.

The administrator can set the system to work without user authentication. In this case, the unit will use the MDLC password only, in the same manner as in a non-secured system. The STS, however, will still require a user and password to log in.

User Authentication Types

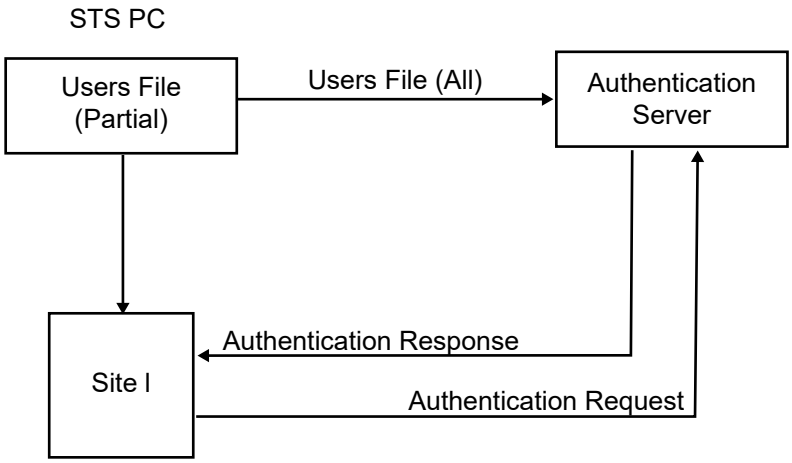
ACE3600 and MC-EDGE support two types of authentication:

- Authentication servers are used to centralize all user authentication.
- User authentication is only performed locally in the units.

In the first type, a dedicated ACE3600 RTU in the system is designated as an authentication server. Up to eight backup authentication servers can also be designated. The users file with all of the user credentials is downloaded to the authentication server. A subset of the users file (local file) is downloaded to each field unit, containing the credentials of the authentication server, of the site itself, and of those users, if any, who were granted local access to that site. (For example, a local user can be defined on each field unit, to enable a technician to communicate directly with the unit, when there is no authentication server or when communication to the server fails.) Note: The users file includes credentials for human users and RTUs.

Each time a field unit receives an access request, it sends an authentication request to the server, which has the most up to date information. Once the user is authenticated, the unit retains the user information in a local cache for a period of time (as determined in the policy). This reduces the number of requests to the server and communication overhead.

In such a centralized system, the system administrator does not need to update all of the field units in the system whenever the user credentials change (only the authentication server and those sites to which the changed users were granted local access.)



IMPORTANT: The time to wait for the authentication server authorization must be configured to ensure that authentication requests can get to the authentication server and back, including link retries.

By default, when the users file is changed in the authentication server, a broadcast is sent to all RTUs to erase the user records in their cache. During the next communication request from a user, the RTUs will authenticate with the server and store the updated information in the cache.

In the second type of authentication, no authentication server is defined. A subset of the users file (local file) is downloaded to each field unit, containing the credentials of the site itself and of those users who were granted local access to that site. User credentials are authenticated locally by the field units for those users which are stored in its local file. In such a decentralized system, the system administrator must update all affected field units in the system when user credentials change. This approach is only practical for a very small system.

Where both authentication server and local files are used, the administrator can determine (in the policy) which source should be checked first for authentication, the authentication server or the local users file. In the event of a conflict, the authentication server is the determining factor. The possible scenarios are as follows:

IF …	AND	THEN …	Note
The authentication server is checked first	The user exists in the authentication server and the password is valid	The access request is approved.	The RTU checks its local users file to make sure that its information is up-to-date. If it is not, a message to that effect is sent to the security log.
	The user does not exist in the authentication server or the password is invalid	The request is rejected.	The local file is not checked.
The local users file is checked first	The user does not exist in the local file	An authentication request to the authentication server.	
	The user does exist in the local file, but the password is not valid	The request is rejected.	
	The user does exist in the local file, and the password is valid	The access request is approved.	

Note: When alternate addresses are assigned to RTUs (All RTU simulation feature), the RTU responds to all site IDs in that defined address range. Permissions to access those additional Site IDs is not granted automatically to users. The administrator must set the proper access rights for this address range. To do so, a "virtual" site must be defined for each "simulated" RTU in the STS system view. Those sites should not have any communication ports (all ports should be set to "Not used") so no additional links are added to the network. These "virtual" sites will appear in the list of sites when configuring users' site access.

User Accounts

User accounts are managed by system administrators.

For each user, the administrator defines the following:

- personal details (first name, last name, etc.),
- a unique user name,
- a user role,

- a valid (initial) password which conforms to strict guidelines,
- the dates during which the password is valid,
- whether the user is enabled or disabled. (A disabled user will be unable to communicate with a secured RTU or open a secured project.)
- whether the users credentials will be downloaded to the authentication server, to the units (all or selected), or to both.
- the list of units (sites) to which the user has access.

User Passwords

The administrator can change user passwords, and enable/disable user access indefinitely or for specific time periods, and for specific field units.

IMPORTANT: It is recommended to change the passwords frequently. The security policy determines the maximum password age.

A valid user password must comply with the following rules:

- 6-30 characters long with no white spaces, (long passwords are recommended)
- at least one character (A-Z, a-z),
- at least one digit (0-9),
- (when changing an existing password) different than your previous X passwords (X is defined in the security policy in the 'Number of old passwords in history list' parameter).

IMPORTANT: Changing the user password in the STS does not change the password in the RTU. It is the responsibility of the authorized user to download the new users file to the relevant RTUs.

When a user password expires, the system locks the (nonadministrator) user for further access. Even if the RTU time is moved back (as a result of day light savings or using the Site Date & Time utility) the user is still locked until an updated users file (with an updated password/duration) is downloaded. As the user password expiration approaches, the STS will display a warning (as per the policy.) If the user logs in with an expired password, the STS displays a prompt to enter a new password.

Users File in the Field Units

When all users have been defined, the users file is downloaded to the authentication server and (a subset of the users file) to all units in the system.

If any change is made to the users file (new password, new user, etc.), it must be downloaded to all relevant units in the system. (The relevant units are marked 'Needs download' automatically in the system view by the STS. The relevant files are marked with a check mark automatically in the Site Download window in the site view.) The users

file is downloaded first to the relevant units, and then to the authentication server. A user can change his/her own password when logged into a secured project (in the STS).

A user account will be locked for a limited period (as configured in the policy) if the user attempts to gain access with an invalid password several times (as configured in the policy.) In this case, only the administrator can unlock the user account. If the user attempts to gain access using an invalid user name, the STS project is locked for a limited period (as configured in the policy.)

User Roles and Permissions

Each user is assigned a role. The default roles in the STS are:

- Administrator
- Technician
- Viewer
- User (default)

Permission to perform certain operations in the system is associated with each role. For the list of standard user roles and permissions, see *Appendix B: User Roles and Permission Groups*. The administrator can change the default permissions of the User role. Because some STS operations have interdependencies, enabling/disabling one permission group to the User role, may cause other, related permission to be enabled/disabled as well. For example, enabling the Site Permissions group, also changes certain permissions in the System Permissions group.

Field Unit Credentials and Authentication

Each RTU in the MC-IoT system has credentials (user name and password of the specific RTU) which are used in RTU-to-RTU communication. These are known as Machine-to-Machine (M2M) credentials. M2M accounts are generated automatically by the STS and M2M credentials are downloaded to the units in the users file.

To ensure system integrity, a field unit receiving a message from another unit, authenticates the M2M credentials of the sending unit.

Unique or Common M2M Credentials

The administrator determines whether each unit uses unique M2M credentials or all the units share one common M2M account name and password.

In a system with common M2M credentials, only one M2M account is generated and communication efficiency is increased (because validation via the authentication server is not required.) If all RTUs share the same common M2M name and password, the M2M account is never locked. However, if an RTU receives an access request with an invalid password, a message is sent to the security log.

IMPORTANT: If a “common” value is used, the user can add up to eight prioritized servers to the system.

In a system with unique M2M credentials, an M2M account is generated for each secured site, and the RTU must authenticate each M2M account. This approach can be used to restrict access to certain sites from other sites.

IMPORTANT: If a “unique” value is used in the M2M mode, no more than two servers can be added to the system.

Note: In order to use Addr. range response for 'All RTU simulation', M2M credentials must be common.

M2M Credentials in the Field Units

The administrator configures whether the M2M account credentials are downloaded to the authentication server, to the units (all or selected), or to both.

The authentication server credentials must be stored locally in all RTUs. This enables units to communicate with the authentication server and authenticate users. Failing to do so prevents RTUs from accessing the authentication server (RTUs will reject replies sent from the authentication server as they do not recognize its credentials.)

M2M accounts cannot be deleted. They are removed from the account repository by the STS when sites are deleted.

The STS automatically configures the default site access of M2M accounts (all units can communicate with each other). Afterwards the administrator can limit M2M site access as appropriate.

Field Unit Passwords

The password for an M2M account is generated by the STS and is not displayed in the GUI. It cannot be edited by the user. The password does not have an expiration date, but can be regenerated by the administrator.

IMPORTANT: If the authentication server M2M password (in a system with unique M2M credentials) needs to be changed, you must first download the updated users file to all the RTUs, and only then download the updated users file to the authentication server itself.

Note: When the users file is changed and downloaded to the units in a system, it can take time to download the updated file to all sites, during which communication problems may occur. This is due to the fact that units with different credentials may not be able to communication with each other.

The M2M passwords of units (in a system with unique M2M credentials) should be changed carefully, as described in the three scenarios below:

- Single authentication server

  After changing the password of an RTU/front end unit in the STS, download the updated users file to the unit itself, to update each unit’s own password that is stored locally. Only then download the updated users file to the authentication server. (If the server is updated first, no user/STS communication will be accepted, as the authentication server will reject that RTU’s user authentication requests due to password mismatch.)

Note: Until the server is updated, no communication from this updated RTU (M2M and users) will be accepted by other RTUs.

- Redundant authentication server

  The process is the same as with a single authentication server, except that the authenticating RTU may access the second server if there is a communication problem with the first server. In the meantime, the updated password is downloaded to all of the RTUs, then to the first server, and then finally to the redundant server. This way, no communication disruptions will occur.

- No authentication server

  If no authentication server is defined in the system, the users file must be updated in all RTUs in the field that store that RTU M2M password locally. M2M communication from that RTU will not be accepted by the other RTUs until they are updated with the users file with the new password.

M2M Site Access

When a human or M2M user is defined in the STS, the administrator configures which sites are accessible via authentication server, and/or which sites are accessible locally. This is done in the STS User Details dialog in the Site Access tab. By default, the STS assigns M2M accounts as follows:

IF …	AND	THEN …	AND
M2M credentials configuration mode is set to Common	An authentication server exists in the project	In the Local Sites panel, all eligible sites are selected and the site tree is disabled.	The Via Authentication server panel is disabled.
	No authentication server exists in the project	In the Local Sites panel, all eligible sites are selected and the site tree is disabled.	The Via Authentication server panel is disabled.
M2M credentials configuration mode is set to Unique*	An authentication server exists in the project	In the Local Sites panel, all authentication server sites and the site which is uses this M2M user for TX are selected.	In the Via Authentication server panel all eligible sites are selected.
	No authentication server exists in the project	In the Local Sites panel, all eligible sites are selected.	The Via Authentication server panel is disabled.

* If the first authentication server is defined or the only authentication server is deleted, the STS will automatically change the configuration of M2M accounts. A message to that effect is displayed.

The M2M credentials of the authentication server itself are also downloaded to all RTUs. This ensures that authentication responses from the authentication server will be accepted by the RTU.

Communication Encryption

The MC-IoT MDLC protocol enables data communications over a wide range of communications media, such as telephone lines, radio, IP networks, cellular networks, etc.

Enhanced MDLC payload encryption seamlessly secures the communication over any communication media. MDLC payload encryption uses an AES 256 blocking CFB128 encryption algorithm (as opposed to the TEA algorithm used in legacy MDLC payload encryption/nonsecured systems.) MDLC payload encryption uses communication-based third party OpenSSL software.

Note: Encrypted MDLC messages are only decrypted in the destination RTU, not in units used to route the message.

IMPORTANT: MDLC payload encryption is not relevant for IP communication between the ACE IP Gateway and the SCADA.

If, for migration purposes, encryption using the TEA algorithm is required for ACE3600 RTUs with firmware V16.00, the secured STS 16.50 must be used and the keys file can be only be downloaded to secured RTUs.

Encryption Key Management

The MC-IoT STS provides efficient key management for a secured project. System administrators can generate, store, and track the encryption keys in the system.

Encryption Key Definition

The administrator defines a set of keys, with an expiration date for each key. (The minimum and maximum numbers of keys are defined in the security policy.) The keys can either be defined manually (based on a key alias, key generation value and a unique initialization vector provided by the user) or generated automatically based on input from the user (i.e. how many keys to create, base string and index for the key alias, and how long each key should be active.) The generated keys are stored (sorted by expiration date) in a keys files. The keys file must then be downloaded to all the units; otherwise the units cannot communicate with each other.

Note: Manual key creation allows organizations to use external key-generating software/ machines to create the keys and then copy them to STS.

IMPORTANT: The key alias is a unique name (string) for each key. While the key value and initialization vector can be hidden from view, the alias is displayed in the keys file. The key alias must be unique.

For each key, an expiration date and time is defined (automatically by the STS or manually by the user), based on the lifespan of a key defined in the policy. The time periods of the keys cannot overlap. After the current key expires, the system starts using the next key in the file. It is recommended to change encryption keys frequently, based on security requirements. Note: Once a key has expired it generally cannot be reused. (There are some exceptions to this rule, e.g. if the clock is moved back for daylight savings, the old key can be used unless it was the last key in the file, and was already extended past the expiration date.

Encryption Key Replacement in the Unit

The encryption mechanism uses the expiration dates to determine when key replacement is necessary. Key replacement in the units is automatic upon the key expiration date, and the next key becomes active. The new key and the previous key are both valid for a pre-defined grace period after key replacement, for both transmit and receive.
Note: The grace period can be set in the keys file by the user. The TX grace period should be a function of the level of clock synchronization in the system and the possible drift between RTU clocks. The RX grace period should be greater than the maximum retry period in the RTU, to enable retry frames to be successfully decrypted and reencrypted when a key is changed during the retry period.

IMPORTANT: Because encryption keys have expiration dates, they are time-dependent, based on GMT. The time zone in the unit must be configured (before downloading the keys) in order for the time/keys to be compatible between the STS (which is hosted by a PC which is configured to support time zone) and the units, and between units in different locations.

When the last key in the file reaches its expiration date, its expiration is extended for another 24 hours, and a message is sent to security log alerting the administrator that new keys must be defined.

Encryption Key Modification

The keys file can be viewed and edited in the STS by the administrator. The key values and initialization vectors are hidden as asterisks by default as a safety feature. The administrator can also choose to display the key values and initialization vectors in ASCII form.

A key which has not become active yet can be modified by the administrator. A key which has not become active yet can be deleted by the administrator, as long as the total (remaining) number of keys is compliant with the security policy. When a key is deleted, the STS will change the expiration dates of the remaining keys to ensure continuous coverage.

The administrator can remove encryptions keys from the keys file. The current, active key can only be erased using Remove All. Erasing the active key causes loss of synchronization between the STS and RTUs, and all units must be erased to establish communication again.

If the administrator chooses to generate keys automatically, all of the existing keys are replaced, except the current active key which is kept maintain communication with the units. If an older keys file has already been downloaded to units in the field, downloading

an updated file can cause loss of synchronization between the STS and those units (after the current key expires.) Therefore the updated keys files must be downloaded while the current key is active.

Encryption Keys File in the Units

Initially, the keys file must be downloaded to the unit locally. Subsequent downloads can be performed locally or remotely via a secured connection. Downloading the keys file to a unit does not cause the unit to restart.

IMPORTANT: Time synchronization is essential for a secured system to operate properly. By default, the site configuration of a secured RTU is configured for time zone to match the STS PC's time zone.

MDLC payload encryption is only in effect if all the encryption/authentication conditions in the policy have been applied to the unit.

Certain encryption key information in an RTU can be viewed by administrators using the Software Diagnostics utility. For more information, see the SECKEYS device in the *MC-IoT STS Software Diagnostic Output and Error Messages* manual.

Encryption Reserved Values in the RTU Database

The RTU database Reserved Values table includes the index of the current active MDLC encryption key index and the number of minutes remaining until the encryption keys are swapped. For more information on the Reserved Values table, see *Appendix D: Security Information in Application Database Tables*.

File Encryption

RTU

Data files (e.g. site configuration, keys, users) which are downloaded can be encrypted in secured field units to protect them from being read in the event of unauthorized access. Files generated by the RTU, the Error Logger and user's logging flash files are not encrypted.

Data file encryption is configured by the administrator in the security policy. File encryption is performed during the download to the RTU's flash, using a unique key. Once the encrypted files are in the unit, access to them must be from a secured STS only.

Note: In the STS Field View utility, RTU files are marked as encrypted or unencrypted.

IMPORTANT: If the encryption in the unit is damaged, the encrypted files stored in the RTU cannot be used and are therefore erased.

All encrypted files from the flash are decrypted before being transmitted over the air (e.g. for upload to the STS.) Therefore, the user must enable MDLC payload encryption which encrypts the transmitted data. The reason for decrypting is that each RTU encrypts the files in its flash with its own encryption key. So the file must be decrypted for transmission and then reencrypted.

STS

In a secured project, the STS manages a secured database. The database is encrypted based on the master password defined during STS installation. (A project created in the secured STS is secured by default.) If the project is not secured, then the STS database is not encrypted.

You can copy/paste the database to another PC if both installation passwords are the same.

File Signature

System users need assurance that they can trust system STS/RTU downloads. A digital signature certificate provides an additional layer of assurance that informs users if the downloaded files are trustworthy and not malicious.

The following sequence provides an overview of the processes behind the generation of a Digital Signature:

1. Before the STS downloads a file to the RTU, it automatically generates longnumber.
2. The generated number is encrypted with the STS Private Key to create a Digital Signature.
3. The file and its Digital Signature are downloaded to the RTU with a file.
4. When the signed file is received by the RTU, It identifies the signature and performs verification actions.
5. The RTU decrypts the file with STS Public Key and compares the received long number with the STS file to verify that the file was not tampered.

Security Log

The secured ACE3600/MC-EDGE field units and STS maintain an encrypted local security log that contains records of access activity and other security-related events. Security events include security warnings, indications of access to the unit, files downloaded, and diagnostics/operations related to the unit, etc.

Events are logged with essential data such as

- event severity type,
- date and time,
- user name and role,
- event description.

When the log file is full, the oldest record is deleted to make room for new records.

Note: In the RTU, the security log is stored in the flash memory and is not erased by RTU restart.

IMPORTANT: The security log in the RTU is only relevant once the policy has been downloaded.

Security Log Record Retrieval

Using the Security tab in the Logger utility, an administrator can:

- Retrieve the records from the security log locally or remotely.
- Clear the security log.
- Save the security log contents in a file (unencrypted) on the STS PC.

For information on retrieving security log information from the RTU using the Logger, see the *Operation* chapter.

The user application in the RTU can also retrieve records from the security log, based on severity (1 = information, 3 = moderate, 5 = high, or 7 = critical.) In the security policy, the administrator configures the severity threshold (e.g. 5) which triggers the application's SecureLogSeverity flag in the Reserved Flags table. The user application can check the SecureLogSeverity flag to see if high severity events have been logged. When the application calls the GetSecLog function, all security log events which are at, or above, the configured high severity threshold level, are retrieved (and cleared) from the security log's high severity queue (in RAM) into the RTU database Reserved Values table.

When high severity events appear in the Reserved Values table, the user application can take appropriate action (e.g. send an alert to the SCADA GUI in the control center.) The control center in turn can display those records, using the STS securelog.txt file which associates message IDs with text.

IMPORTANT: It is recommended to call GetSecLog in each scan to retrieve security log events. This ensures that events are not overwritten, or cleared in the internal high severity queue in RAM (while waiting to be copied to the database) by incoming events.

Other security log flags indicate whether events exist in the security log, whether the security log is almost full, and whether the security log is full. For more information on the Reserved Values and Reserved Flags tables, see *Appendix D: Security Information in Application Database Tables*. For more information on user applications and security, see the *User Application Programming for a Secured System* chapter.

IMPORTANT: It is the responsibility of the user program to retrieve high severity events from the security log and send alerts to the control center.

The severity of each event type is determined in the firmware, however event severities can be tailored per system using a secure logger severity file. See *Changing the Severity of Security Events* in the *Operation* chapter.

Security Log Configuration

Frequently recurring events in the security log can be filtered to prevent the log from filling up. In the security policy, the administrator configures whether to use event filters, after how many occurrences to filter, and after what timeout to stop filtering that event.

Verbose logging is a useful option for technicians diagnosing a problem in the field. Detailed tracer messages are sent by the unit to the security log. This option is disabled by default, so that these tracer type messages do not fill up the security log. The administrator can temporarily turn on verbose logging in the security policy.

Security Event Generation

Security events can be generated by a human user, by an M2M account, or by the RTU itself (e.g. if the RTU self test failed, or if the application tried to do clock synchronization, etc.) In a system without user authentication, N/A is displayed. Note: If there is a discrepancy between the users file in the STS and in the RTU, the user/role is displayed as a numeric value.

Note: When user authentication is disabled, messages to the security log cannot use "username" and "role" in the message. Instead N/A is displayed.

STS Audit Log

The secured MC-IoT STS saves an audit trail of all security-related operations performed during the STS session.

All of these events are stored in a log file for viewing by the system administrator. The events can be stored in an audit log (viewed from the STS), in an event log (viewed from the Windows Event Viewer), or in both logs. The system administrator determines the output type(s) in the policy. The size of the STS audit log is also determined in the policy.

Note: For maximum security, do not configure the STS to store events in a Windows event log where no permissions are enforced.

Note: The audit log is encrypted and can only be read from the STS PC where the project was created, or from another STS which has the same master password.

For more information on the Windows Event Viewer, see Windows help.

For information on viewing the STS audit log, see *Viewing the Audit Log* in the *Operation* chapter.

IP Firewall

Using the IP firewall protects the field units from unauthorized TCP and UDP packet access while permitting legitimate packets to pass through.

The administrator specifies the list of IP addresses to accept, i.e. the list of IP addresses allowed to pass through this firewall. When the firewall is set to Enabled in the site configuration, it will only be active once the list is defined.

For additional protection, the RTU can be configured to prevent changes to the firmware (system file) in the unit and to disable C applications from running in the unit.
Note: In the security policy, the RTU can be configured to block remote download of to the unit.

Note: If debugging a 'C' application is required, temporarily disable the firewall in the site configuration and enable 'C' toolkit debugging in the RTU.

For information on the IP Firewall configuration parameters, see *Appendix A: Site Configuration Parameters* in the *MC-IoT STS User Guide*. For more information on configuring 'C' applications, see the *User Application Programming for a Secured System* section.

RTU Program Whitelisting (ACE3600 Only)

When RTU program whitelisting is enabled in the security policy, a user program (ladder or 'C' application, or third party protocol file such as MODBUS or Allen Bradley) downloaded to a secured RTU from the STS (by an authorized user) is whitelisted by the RTU. The program is added to the RTU's whitelist, along with a time-stamped signature which is used for validation of the executable file.

The RTU will run a program only if it was whitelisted, and has not been modified since it was whitelisted. The RTU will not run a program which is not whitelisted. For example, when the RTU restarts, it validates the program to ensure that it has not been modified.

If the RTU detects tampering of a whitelisted file, an event is logged in the security log. The tampered file is marked suspicious and set aside in the flash. This file remains in the flash until the entire flash is erased during a download (using the Erase all flash before download setting). Use the Field View utility to view the names of files in the flash.

To ensure that your application is not marked as suspicious by the RTU, first enable program whitelisting in the security policy and download the policy to the unit. Only then download the application. (Downloading the application first will cause the file to be considered suspicious. The whitelist in the RTU is dynamic and is updated with each download.

STS Whitelisting

Whitelisting of STS files protects the security files on the STS and PC from unauthorized access. The recommended third party whitelisting software is McAfee® Solidifier (version 5.1).

McAfee® Solidifier should be installed on the PC after a clean Windows installation. Both the change control and run time whitelisting components should be activated. This assures that the Windows files were not tampered with. The STS should be installed immediately after Solidifier for the same reason.

Once the STS is installed, run the C:\STS<version>\Doc\Whitelist\McAfee\whitelist.bat batch file, installed with each version of STS from the McAfee command line utility. This protects the relevant folders of this STS version and allows the STS elements to make changes in the protected folders). Note: Each time a version of the STS is installed, the batch file for that version must be run.

For detailed instructions on whitelisting the STS, see *Hardening the STS PC and the RTU*.

Note: Failure to configure the whitelisting software correctly, may allow unauthorized applications to modify STS files. This can reduce the security level provided by whitelisting software for the STS, and may compromise the security information stored by the STS. It is strongly recommend that whitelisting configuration be done only by a well-trained technician.

ACE3680 Dedicated Security Repository

The ACE 3680 is equipped with an internal dedicated security repository designed to protect the unit and its encryption from tampering. The repository includes the unique system encryption key for that unit. Any attempt to tamper with the unit causes the key in the repository to be erased. As a result, all files in the flash memory which were encrypted with this key are deleted, a tamper message is sent to the Error Logger, and the unit restarts. This means that a unit which has been breached becomes unsecured, and if it was configured for file encryption, all users files are erased.

The security repository is sensitive to:

- extreme changes temperatures (high/low)
- extreme changes voltage/power level (high/low)
- extreme changes in power level in the internal lithium battery
- attempts to physically access or break the components

IMPORTANT: In a system where files in the flash are encrypted, the unit's site configuration is also erased. If this happens, the unit must be reconfigured locally (on site). Therefore care should be taken to maintain proper temperature range and power/battery levels, as described in the unit specifications in the ACE3600 RTU Owner's Manual.

An ACE3680 RTU whose main power switch is off for an extended period may get a tamper event for low battery power when it is first powered up. After startup, a tamper event will be sent, all security files will be erased, and then unit will start up in nonsecured mode. While it is nonsecured, the RTU should be plugged into a power source for a few hours to recharge, during which time diagnostics and logger information can be retrieved. Once the proper power level is attained, redownload the security policy, security files, etc.

The security repository is only enabled when the unit uses the secured system firmware.

Note: The SECPRVD Level 0 diagnostic enables you to read the RTU temperature and the power level of the internal battery on both secured and nonsecured ACE3680 units. In the secured ACE3680, the SELFTST Level 11 diagnostic has an indication if the unit temperature is near the maximum allowed.

Security and Expansion Units

An ACE3600 system with I/O expansion can be secured. All security files (policy, users, permissions, keys, etc.) are downloaded to the main CPU and then daisychained to the expansion unit(s).

When an expansion CPU starts up, it retrieves the security information from the main CPU. If security policy, MDLC payload encryption, and user authentication are enabled in the main CPU, these will be enabled in the expansion CPU(s). These files are retained in the expansion CPU's flash in encrypted format.

All files undergo whitelist validation before being downloaded to the expansion CPU.

The expansion CPU does not have its own security log. Authentication from the STS to the expansion CPU is done in the main CPU, so any security events are logged in the security log in the main CPU.

In a system with I/O expansion and MDLC payload encryption, the encryption key RX and TX grace times should be long enough to allow the new keys file to be downloaded to all expansion units. If the time is too short, the main CPU will move to the new key while the download to expansion units is still in progress, and some of the expansion units will still use the old key.

Security and Redundant Units

If a site with ACE3600 RTU redundancy is designated as the authentication server, only those links which are common to both the primary and secondary CPU can be defined in the STS for the site.

ACE IP Gateway Security

Almost all of the features available in the ACE3600 units are also available in the ACE IP Gateway. There is no access to the security log from the application, because the ACE IP Gateway does not have a user application.

IMPORTANT: Passwords and MDLC payload encryption are relevant only in MDLC communication between the ACE IP Gateway and ACE3600 RTUs. IP communication with the SCADA is not encrypted or password controlled.

MDLC Communication Driver

As of STS V16.50, the MDLC communication driver has been enhanced to support secured communication. The MDLC communication driver can work in either secured or nonsecured mode.

IMPORTANT: An MDLC legacy password must be defined when a project (both secured and nonsecured) is created, or when a legacy STS project is upgraded.

Nonsecured Mode

When invoked from a nonsecured project, the MDLC communication driver is invoked in nonsecured mode. MDLC communication uses the MDLC legacy password which was defined during project creation. All communication operations that are run from the project use this password when in nonsecured mode. When the MDLC driver starts, the user is prompted to confirm the legacy password. If it does not match the password defined during project creation, the communication session cannot be established.

After performing MDLC communication from a nonsecured project (STS ≥V16.50), the MDLC driver remains active even after you close the project.

If you then open another nonsecured project, communication is established only if the MDLC legacy password is the same as in the previous nonsecured project. If the MDLC legacy passwords do not match, then no communication is established and an error is reported. You must stop the active MDLC driver before trying to establish communication from the second project.

However, if you then open a new, secured project, the STS closes the active MDLC driver (a confirmation message is displayed) and a new driver in secured mode is started with the new credentials defined in the project. See *Note:* In earlier versions, the administrator could initiate communication with different units in the same STS project by first stopping the MDLC driver (and entering a different MDLC password when the MDLC driver restarted.) As of V16.50, the STS can only communicate with nonsecured units in the same project if they share a legacy MDLC password. Otherwise, two separate (simultaneous) STS projects must be used and the MDLC driver must be stopped and restarted when initiating communication from one or the other.

Secured Mode below. This new MDLC driver can also serve older versions of the STS and nonsecured projects.

Note: In earlier versions, the administrator could initiate communication with different units in the same STS project by first stopping the MDLC driver (and entering a different MDLC password when the MDLC driver restarted.) As of V16.50, the STS can only communicate with nonsecured units in the same project if they share a legacy MDLC password. Otherwise, two separate (simultaneous) STS projects must be used and the MDLC driver must be stopped and restarted when initiating communication from one or the other.

Secured Mode

When invoked from a secured project, the MDLC communication driver is invoked in secured mode. In secured mode, the MDLC driver supports the following:

- Secured communication from secured STS projects
- Nonsecured communication from both nonsecured and secured STS projects
- Nonsecured communication from legacy STS (< V16.50) projects, or MOSCAD Programming Toolbox

Each communication with an RTU is per channel (by default there are five logical channels.) The various types of communication are supported (one per channel) at the

same time on all projects. For example, you could have a secured project monitoring the application database in secured mode on channel 1, and an unsecured project retrieving Error Logger information from another RTU in nonsecured mode on channel 2.

Each channel has security attributes/credentials that are set in the project. The user can operate several STS projects at the same time, each with different security attributes, e.g. one nonsecured project, one with MDLC payload encryption only, and a third with both MDLC payload encryption and user authentication. The communication for each secured project is in accordance with the policy of that project.

IMPORTANT: In order for the MDLC driver to support simultaneous communication with all of these projects, they must all share the same legacy MDLC password. Otherwise, the MDLC driver must be stopped and restarted when toggling between projects with different legacy passwords.

Self Test

The ACE3600 RTU includes a built-in self test capability which ensures proper operation of the unit and the integrity of the files and code. The RTU self test is enabled by default in the security policy.

Periodic Self Tests

The following functions are tested periodically:

- Security log - Whether the security log in the unit is 100% full.
- Security log- Whether the security log in the unit is 80% full.
- Whitelist - Whether any suspicious files exist on the unit.
- Key repository - Whether the key repository has been tampered with. This test is only relevant in an ACE3680.
- Key repository - Whether the key repository temperature is near the maximum. This test is only relevant in an ACE3680.
- File encryption - Whether the file encryption process in the unit has been tampered with.
- MDLC payload encryption - Whether the MDLC payload encryption process in the unit has been tampered with.
- Encryption algorithm - Whether the encryption algorithm (e.g. AES) in the unit has been tampered with.
- Security keys - Whether all the security keys of a specific type (e.g. for MDLC payload encryption) in the unit have expired.
- Authentication test - Whether the user authentication process has been tampered with.

- Firmware test – Whether the firmware has been tampered with.
- ‘C’ application test – Whether the ‘C’ application has been tampered with.
- Firmware debugger – Whether the firmware debugger is enabled.
- ‘C’ application debugger – Whether the ‘C’ application debugger is enabled.
- Clock run-rate – Whether the RTU clock has been tampered with.

Self Test Diagnostics

If any one of the self test fails, the following message is sent to the security log:

“Security Self-Test failed. Please check the Self-Test diagnostic.”

To check the diagnostic, use the Software Diagnostics (SELFTST device).

The SELFTST device diagnostics also display the frequency of each test, when the last test was run, the maximum time the test took to run, how many times it failed, and the results of the last test.

For more information, see the SELFTST device in the *MC-IoT STS Software Diagnostic Output and Error Messages* manual.

MC-IoT SECURED STS

The MC-IoT STS is delivered with two CDs:

- Secured STS
- Nonsecured STS

The secured STS cannot be installed on the same PC as the nonsecured STS.

IMPORTANT: If the nonsecured STS is installed on the PC, first uninstall it. Then install the secured STS.

Hardware and Software Requirements

The hardware and software requirements for the MC-IoT secured STS PC are the same as those of the nonsecured MC-IoT STS PC. See the *Hardware and Software Requirements* section of the *MC-IoT STS User Guide*.

Installing the Secured MC-IoT STS

The secured MC-IoT STS is installed like any other Windows application. Insert the installation disk in your CD/DVD drive, activate setup.exe, and follow installation messages and instructions. Written instructions can be found on the leaflet attached to the CD.

During installation of the secured STS, a dialog is displayed prompting you to enter a master security password.

On a standalone PC, the master password must comply with the following rules:
- at least 16 characters long,
- at least one lower case character (a-z),
- at least one upper case character (A-Z),• at least one digit (0-9).

On a PC connected to a domain, the rules are generally determined by the requirements of the organization, but cannot be less rigorous than those listed above for a standalone PC.

IMPORANT: Make sure to record/remember the master password in case you need to install a new version of the STS, a new version of Microsoft Windows, or transfer the project to another PC.

IMPORANT: After installing the secured STS, harden the PC as described in the *Hardening the STS PC and the RTU* chapter.

NOTE: Projects created in the secured STS cannot be opened from a nonsecured STS.

Using the Secured STS

The secured STS enables you to perform various security-related configuration and management functions, based on the permissions granted to you. These are in addition to the standard STS tools described in the available in the MC-IoT STS User Guide. For a description of the security operations and the permissions required, see *Appendix B: User Roles and Permission Groups*.

Note: The secured STS can be used to administer nonsecured projects as well.

HARDENING THE STS PC AND THE RTU

For maximal security, use all of the security features described in this manual: MDLC payload encryption, users authentication/passwords, application whitelisting in the RTU, signature, and more.

Both the STS PC and the RTU must be hardened in a secured ACE3600 system.

IMPORTANT: While creating a secured system, unsecured communication is used with the field unit until it starts using encrypted communication. Therefore it is recommended to communicate locally with the unit.

PC Hardening

Procedure 4-1-1 How to Harden the STS PC

To harden the PC, do the following:

1. Install and run updated antivirus software, and make sure the operating system is updated with the latest updates.

2. Install third party whitelisting software that will prevent an unauthorized program from running on the computer. Use the strictest configuration. It is recommended to install a configuration management tool as well.
   Motorola recommends that you use McAfee Solidifier, that you configure it correctly, and set a password for the whitelisting program configuration tool.

3. Activate both the change control and run time whitelisting components of McAfee Solidifier.

4. Install an original copy of the MC-IoT STS (by administrator user only) and update the whitelisting and configuration management program with this installation. During STS installation, you will be prompted to set a password. Keep this password for future STS installations. Failing to give same password in future installations will prevent opening old secured projects.

5. Define all users that need access to the computer (and to the STS) and give each one the minimal permissions required, including 'read only' attribute for file access. STS users should run under User type accounts only.

6. Grant write access to STS folders and files for User type accounts rights to selected Windows users, as needed. Configure each user with the minimal permissions, including changing the PC windows settings.
   Note: If access to legacy STS/ToolBox installations is required for a User type, write permission must likewise be granted access to the folders and files of the legacy STS/ToolBox installations.

7. Until all security features are fully operational (i.e. during migration), be sure to protect STS files and the operating system from unauthorized access.

8. The STS is now ready for setting up a new project.
9. Optional: You may install a disk encryption utility and encrypt the STS project folder.

Whitelisting the STS

Procedure 4-1-2 How to Whitelist the STS

Follow the steps below to whitelist the STS PC.

1. After installing Windows on the STS PC, install McAfee® Solidifier according to the instructions on the Solidifier CD.
   Execute Solidifier and password-protect access to it.
2. Set Solidifier to Update mode.
3. Install the secured MC-IoT STS according to the instructions on the MC-IoT STS CD and activate it.
4. Update Solidifier using the STS whitelisting batch file ([C]:\<STS2250>\Doc\Whitelist\McAfee\Whitelist.bat) which contains the names of the folders where security files are stored, and with information on which files should be write protected.
5. Open the Solidifer command line tool (Run as Administrator).
6. Type in the full pathname of the STS whitelisting batch file name [C]:\<STS2250>\Doc\Whitelist\McAfee\Whitelist.bat and click Enter.
   Result: Solidifier reads the batch file and adds protection commands related to this specific STS.
7. Repeat these steps for each STS PC to be hardened.
8. Set Solidifier to Enabled mode.

Note: If you need to rollback the whitelist configuration, use the Solidifier 'Restore defaults' commands to override the commands added by the batch file.

Setting Security Files Signature Hardening

Procedure 4-1-3 How to Set Security Files Signature Hardening.

Digital signature certificate assures users that their downloaded files can be trusted and do not come from a malicious source.

When a new project is created, a new public key is created and shared with all the components in the system. The public key is used to decrypt downloaded files for signature identification.

Security files signature hardening occurs automatically when files are downloaded in the system and does not require any user action.

However, if the user wants to use other public key, the STS enables to generate or import a key.

CAUTION: If a public key was already downloaded or defined in the system, downloading a new public key may cause damage to the system.

Follow the steps below to generate or import a public key:

1. From the STS menu, select **Security → Keys**.

   Result: the Keys screen is displayed showing the currently used public key.

2. Click the **Import** or **Generate new** button to import or generate a new public key.

   Note: Only keys in PEM format can be used in the system.

3. Close the **Keys** screen by clicking **Close**.

RTU Hardening

To harden the RTU, the administrator must do the following:

Site Configuration (STS)

Procedure 4-1-4 How to Harden the RTU in the Site Configuration

1. Enable and configure the firewall in the site configuration. (For details, see *Appendix A: Site Configuration Parameters* in the *MC-IoT STS User Guide*.)

   - Enable the firewall. (Advanced →Firewall & Hardening)
   - ACE3600: Define the list of IP addresses allowed to pass through this firewall.
   - ACE3600: Specify whether the RTU enables communication from a remote STS (default) or only from the local STS.
   - ACE3600: If debugging a 'C' application is required, temporarily disable the firewall in the site configuration and enable 'C' toolkit debugging in the RTU and (Advanced→ Firewall.) Otherwise, make sure 'C' toolkit debugging is disabled.

2. ACE3600: Block download and execution of 'C' files.
3. ACE3600: Where relevant, block download of remote system software.
4. Set all unused communication ports to Not Used. (Ports)
5. Find solutions for ports which are not MDLC and are not secured.
6. ACE3600: If NTP protocol is not used, disable NTP (**Advanced → NTP)**.
7. Import or generate public signature key or use the default one for downloaded files (**Security → Keys**).

Security Policy Configuration (STS)

Procedure 4-1-5 How to Harden the RTU in the Security Policy

1. Define the maximal strict security policy possible.
2. Create strong (long, complex) passwords and change them frequently.
3. Configure encryption keys to be changed frequently.
4. Configure each STS user with the minimal permissions, and only for those RTUs to which access is required.
5. In the user application, program the units to send important security events from the security log to the control center.
6. Set security files signature hardening. From the STS menu, select **Security → Policy**.

General

Procedure 4-1-6 How to Physically Harden the RTU

1. Secure the sites locally.
2. Where possible, enclose units in a locked case. Equip the case with a tamper switch which, when opened, causes the application to send a tamper message to the control center.

Setting Up a Secured System (Step by Step)

IMPORTANT: You must follow Procedure 4-1-7 carefully, in order to ensure that your system will operate promptly and be secured correctly. Failing to follow this sequence may result in the inability to communicate with the RTUs. For specific instructions for each step, see the *Operation* chapter.

Procedure 4-1-7 How to Set Up a Secured System

1. Create a new secured project in the STS.
2. Design your system, determine who are the users of the system, and designate which site(s) will be used as an MDLC authentication server (if any). (See the *Operation* chapter.)
3. Set the proper policy values. (For a description of the policy parameters, see *Appendix A: Security Policy Parameters*.) For a list of recommended security policy changes, see *RTU Hardening*.
4. Create the new site configuration that includes the correct time zone and firewall settings for each RTU. (For a description of the policy parameters, see *Appendix A: Security Policy Parameters*.) For a list of recommended site configuration changes, see *RTU Hardening*.

5. Use the STS Set Date & Time utility to set the RTUs' date and time to the STS PC time. (See the *Operation* chapter of the *MC-IoT STS User Guide*.)
6. In the STS, create all users accounts that will have access to the system and set the proper roles and access permissions. Make sure that all user accounts have access to the associated sites.
7. Configure the authentication server parameters.
8. Create the file signature encryption keys in the STS.
9. Create the MDLC payload encryption keys in the STS.
10. ACE3600 only: Erase the RTU flash memory by pressing the two pushbuttons during startup.
11. Connect to an RTU locally from the STS PC.
12. Download secured firmware to the unit. (If you prefer to use an IP link for the download, first download the site configuration.)
13. Set the time and date in the unit, including time zone.
14. Download the security policy to the RTU.
15. Download the users file to the RTU.
16. Download the keys file to the RTU.
    After downloading security files, it is recommended to read the security log to make sure that the unit did not identify conflicts between the downloaded file and the policy in the RTU.
17. Download the site configuration to the RTU. If the site configuration was already downloaded above, download it again to have it stored in the RTU in encrypted form.
18. If your region uses daylight savings time, download the application which includes start/end times for daylight savings time. For more information on daylight savings, see the *Clock Functions and Synchronization* section of the *MC-IoT STS Advanced Features* manual, the Time Zone advanced parameters in the *MC-IoT STS User Guide* and the *Daylight Saving Dates Table* section in the *MC-IoT STS User Guide*.
    Note: In order for the application to be whitelisted, it must be downloaded after the security policy.
19. Repeat the downloads to all other RTUs in the system.
20. The RTUs are now secured. It is preferable to download all application files now so they will be whitelisted.

IMPORTANT NOTES:
Downloading the MDLC payload encryption keys and users files is absolutely necessary for the secured configuration to take effect in the RTU. Downloading a policy with MDLC payload encryption and/or user authentication enabled does not

enable those features unless the proper keys/users files are subsequently downloaded.

Securing an existing project does not change the security state of the individual RTUs. As long as the RTUs are not individually secured, they are absolutely not secured. Each RTU needs to be secured in the project and all relevant files must be downloaded to the RTUs.

When downloading keys and users files remotely, the communication channel must be secured.

GUIDELINES FOR SECURING A SYSTEM

The guidelines and notes below have been compiled to guide you in setting up and securing your system properly. For detailed instructions on many of the operations described, see the *Operation* chapter.

Setting Up a Secured System

For a step by step procedure on setting up a secured system, see *Setting Up a Secured System (Step by Step)* in the *Hardening the STS PC and the RTU* chapter. Follow the procedure carefully, in order to ensure that your system will operate promptly and be secured correctly.

PC Hardening at a Glance

For detailed instructions on setting up the STS PC for security, see *PC Hardening* in the *Hardening the STS PC and the RTU* chapter.

When setting up the STS PC, protect STS files and the operating system from unauthorized access until all security features are fully operational (i.e. during migration).

A third party whitelisting tool is highly recommended. Such a tool maintains STS integrity and reduces the risk of external manipulation of STS execution files.

The STS installation must be installed by an administrator, and all STS users should run under User type accounts. Access to the STS' writable area on the PC (i.e. projects folder, etc.) for non-administrators should be limited to selected Windows users. Each user should be configured with minimal permissions, including changing the PC windows settings.

When using the STS under a User type account, legacy STS and MOSCAD Programming ToolBox installations will not work properly unless write permission is given for these users to those STS/ToolBox installations.

Securing an existing project in the STS does not change the security state of the individual RTUs. As long as the RTUs are not individually secured, they are absolutely not secured. Each RTU needs to be secured in the project and all relevant files must be downloaded to the RTUs.

RTU Hardening at a Glance

For detailed instructions on setting up the RTU for security, see the *Hardening the STS PC and the RTU* chapter. When setting up an RTU in your system, you must follow these procedures carefully, in order to ensure that the RTU is secured correctly. Failing to follow the sequence may result in the inability to communicate with the RTU.

The RTU firewall should be active whenever possible. Enable the 'Activate Firewall?' parameter in the site configuration advanced Firewall category.

'C' toolkit debugging is disabled in the site configuration by default. If 'C' toolkit debugging is required, the 'Allow C toolkit debugging' parameter must be set in the site configuration advanced Firewall category. In order to set this parameter, the firewall must first be disabled. After debugging is complete, make sure to enable the firewall and disable 'C' toolkit debugging.
Note: Enabling the firewall automatically disables 'C' toolkit debugging.

It is strongly recommended to send the RTUs high severity events to the SCADA GUI in the control center for monitoring and alarm. For more information, see the *Security Log* section of the *MC-IoT Security Concept* chapter.

IMPORTANT: Downloading the MDLC payload encryption keys and users files is absolutely necessary for the secured configuration to take effect in the RTU. Downloading a policy with MDLC payload encryption and/or user authentication enabled does not enable those features unless the proper keys/users files are subsequently downloaded.

Date & Time

RTU Time Zone

MDLC security features require that the RTU time zone be set in the RTU configuration, and that the RTU date time be set afterward. The STS automatically sets the time zone awareness in secured RTUs.

Daylight Savings

It is very important to assign an application to all RTUs which includes daylight savings start/end dates. If daylight savings is not set, there will be an hour drift between the PC clocks and the RTU clocks, which can be seen, for example, in the in the error logger and security log time display.

Note: Because the ACE IP Gateway does not have a user application, its daylight savings is configured manually, by changing the 'Time zone offset in minutes' parameter appropriately in the advanced site configuration and downloading the site configuration to the ACE IP Gateway.

Changing the PC Time and Date

It is the responsibility of the PC administrator to prevent users from changing the PC date, time and time zone. Changing these values can affect the keys used by the STS and password expiration.

Changing the RTU Time and Date

It is very important to prevent users from setting the RTU with the wrong date and time. This will cause the RTU to use the wrong MDLC encryption key.

Therefore, it is recommended that system administrator give permission for setting the RTU clock only to selected users, who are also responsible for downloading the MDLC encryption keys to the RTU.

Note: If you use nonMDLC clock sync protocols such as NTP, be aware that these are not affected by MDLC payload encryption and are not secured.

Restoring the RTU Time and Date

If an RTU's date and time are reset due to real time clock or battery malfunction (i.e. 1.1.1980), a secured RTU will wake up working with the first key from the MDLC payload encryption key file. This RTU will not be able to communicate with the system's FIU which uses current encryption key.

In order to be notified of such a case, the administrator must dedicate a special FIU that is only loaded with the first MDLC payload encryption key. When the RTU application detects the wrong date (i.e. date <2010), it will communicate with that dedicated FIU. It is the user's responsibility to make sure that this dedicated FIU has only the first key in its file. This can be done by copying the project and modifying the following:

- Set the policy to force the minimum number of MDLC payload encryption keys to 1, with maximum duration.
- Remove all keys but the first one from the MDLC payload encryption key file and change its expiration date to maximum allowed.

This must be done whenever a new MDLC payload encryption key file is updated in the RTUs.

RTU Clock Security Event

If the RTU time is updated by more than an hour, a high severity event is recorded in the security logger. This warning is intended to inform the user of suspicious time setting in the RTU.

RTU Clock Self Test

The RTU has a built in test which verifies that the time in the RTU is continuously advancing. If this test fails, a high severity event is sent to the security logger. The user should investigate the reason for such behavior by analyzing the time set records in the security log.

Users & Permissions

It is the responsibility of the PC administrator to set the proper Windows privileges and file access rights to the STS project, in order to prevent STS file manipulation. It is also advised to keep the STS project in an encrypted volume when it is desirable to hide even the nonsecured part of the STS project.

In a system with an authentication server, when user credentials expire, a user record may still reside in the RTU's credentials cache. This means that the actual "active" period for

the credentials may be extended by the 'Period to keep user records in RTU cache' which is configured in the policy. The actual "active" period for the credentials may also be extended if a new users file is downloaded, but the 'Send broadcast after users file changed in authentication server; parameter in the policy is set to No.

User Authentication Server Tuning

As up to 150000 RTUs can be included in a system, communication bottle neck can occur. A system which experiences a communication bottle neck with the link to the authentication server will display symptoms such as excessive communication delays and retries. To overcome communication delays, up to eight authentication servers can be installed and defined in a system. For details on tuning the authentication server, see the *Troubleshooting* chapter.

Minimizing Secured MDLC Communication Overhead

Secured MDLC communication adds additional security overhead to the MDLC frames. The default system settings are for maximum security, which results in maximum overhead.

In order to better utilize communication channels, some settings may be modified to reduce overhead, but still maintain an acceptable/moderate security level.

The administrator may change the following:

- Reduce the password length for Minisession/Session/Frame-Sequence/Time-sync communication length parameters to 8 bytes (Policy -> User Authentication).
- Extend the period to keep user records in the RTU cache (Policy -> User Authentication).
- Decentralize user control, by either:
  - not defining an authentication server or
  - setting the local RTU users file as the first user authentication source (Policy ->User Authentication)
- Use a common M2M password to reduce communication overhead. Note that this reduces the ability to limit RTU access.

MDLC Payload Encryption

MDLC payload encryption can be set only in a secured RTU, and AES is the optimal encryption algorithm.

For purposes of migration, the TEA algorithm is supported in firmware version 16.00 and STS 16.50. Encryption keys based on the TEA algorithm can be created in secured STS 16.50 and can be downloaded to secured RTUs with firmware V16.00.

IMPORTANT: Until STS 14.50, TEA encryption keys were created using the MOSCAD Programming ToolBox MDLC Encryption Tool, attached to sites using the Add-On manager, and downloaded to MOSCAD legacy units and ACE3600 units with firmware ≤ V15.00. As of STS 15.50, this file type exists in the Downloader, but cannot be downloaded to the unit.)

Encryption Key Management

The RTU time must be set to the correct time before securing it (before enabling encryption).

Motorola recommends that the keys file not be set to have a key swap during the period of moving to/from daylight savings time +/- two hours.

When setting the RTU time zone for the first time (no time zone was set to this RTU before), the RTU time is shifted by the amount of TZ set in configuration. If a key swap time is defined to occur during this interval, the RTU/STS will start using the new key while the STS/RTU is still using the previous key. (e.g. PC time = 13:00+2hTZ=15:00. RTU time was 15:00+0hTZ=15:00 => RTU new time is 15:00+2hTZ=17:00). In this case, make sure a key change is not planned during that period of time, and set the RTU date and time from the STS right after setting the time zone.

Encryption keys for the project should be backed up periodically, as described in *Backing Up the Encryption Keys* in the *Operation* chapter.

Third Party Protocols

Securing MDLC communication does not secure third party protocols. Each protocol has its own level of security (if any.) MODBUS and DNP ports should not be used in the system if they reduce the system's required level of security. Likewise, 'C' toolkit applications which use socket (user protocol over IP) functions should not be used.

Additional Communication Hardening

It is recommended that the user application add and verify timestamps for each frame in all application communication. This increases the protection of the system.

Security Log Events and the Human-Machine Interface

Secure events logged in the RTU security log can be sent to the SCADA GUI. High severity events information is available though the RTU ladder database. It is the user's responsibility to have the ladder program read those values and send them to the GUI. For more information, see *Appendix D: Security Information in Database Tables*.

Unexpected restart events are noted in the security log, but the details of the event are recorded in the Error Logger. It is the operator's responsibility to read the RTU Error Logger whenever a restart event is logged in the security log.

Each time a ladder application is compiled, its hash is calculated and the result is logged in the STS audit log. Each time the application is downloaded to the RTU, its hash is calculated again and logged in the RTU security log as a high severity event, which may be sent to the SCADA GUI if such application is set. The system administrator must verify that the hash logged in the RTU security after download is equivalent to the hash logged by the STS in the audit log after compilation.

RTU Whitelisting

The RTU whitelisting feature is enabled in the policy. Whitelisting of user application files (ladder, 'C' application, third party protocol files) in the RTU is performed at download. Files that were in the RTU before whitelisting was enabled will no longer run after a restart, and will be added to a list of suspicious files. To avoid this, the user is advised to enable the whitelisting feature (ON) when the RTU flash memory is empty of application files.

Note: Whitelisted files are verified when they are first used. MODBUS driver files are used only when a communication port is defined to work with MODBUS and with the matching type/ID. If a MODBUS driver file exists in the RTU but no port is using that driver, the file will not be check by the whitelisting engine.

Note: Use the STS Field View utility or SW Diagnostics (WHITELS device) to view the names of suspicious files in the RTU.

Securing an RTU

It is the administrator's responsibility to secure the RTUs before deploying them in the organization. This action is the first step when deploying a project. For details, see the *Securing a Site* section of the *Operation* chapter.

ACE3600: If the RTU runs firmware < V16.00 (created in STS < V16.50) or is in bootstrap mode, you must first download nonsecured firmware ≥ V16.00 (or higher). For details, see *Migrating a Site* in the *Migrating an ACE3600 System to Security* chapter.

Note: The ACE3600 RTU itself must be security enabled (i.e. it must include a security signature from the factory.)

Unsecuring an RTU

When unsecuring an ACE3600 RTU, fully erase the RTU flash (press both pushbuttons at startup) before downloading the new firmware. This is the safest and recommended method but requires physical access to the RTU.

Unsecuring a site remotely is not recommended since it is a complex task that requires multiple downloads and restarts and could potentially cause a loss of communication with that RTU. For instructions on unsecuring an RTU, see *Unsecuring a Site* in the *Operation* chapter.

Downgrading ACE3600 Firmware to V15.00 or Lower

Note: Downgrading the firmware in the RTU from V16.00 (or higher) to V15.00 (or lower), is a special case of unsecuring the RTU. Here too, downgrading locally is the safest and recommended method but requires physical access to the RTU.

Because in RTUs with firmware ≤V15.00, files are saved in uncompressed format, a two step approach is required. First the RTU is unsecured and the files are erased from the flash. Then it can be downgraded from nonsecured firmware V16.00 to a lower version. When changing the RTU version in the STS to V15.00 or lower, follow the directions in the STS GUI popup message.

Changing the RTU Site ID - Unique M2M Credentials

When the security policy is configured for unique M2M credentials, each RTU has its own user name and password. If you change an RTU's site ID in the STS, this affects these credentials. Therefore, the new user information must be updated in the RTUs. For details, see *Changing the Site ID of a Secured Unit* in the *Operation* chapter.

Backing up your System

It is recommended to save a complete copy of the project as a backup. This copy can be run only on a PC which uses the same master password (defined during installation) as the PC from which the backup was taken. For information, see *Backing up the System* in the *Operation* chapter.

In addition it is recommended to back up encryption keys from the project. This will enable you to decrypt information, even after the current active keys have been swapped. For more information, see *Backing up the Encryption Keys* in the *Operation* chapter.

STS SECURITY OPERATION

General

The procedures described below are specific to a secured MC-IoT system only. For detailed information on the general operations performed in the STS, see the *MC-IoT STS User Guide*.

IMPORTANT NOTES:
Before performing the procedures below, read the *Overview* and *MC-IoT Security Concept* chapters carefully to understand the security concept. Read the *Guidelines for Securing a System* chapter for important guidelines in setting up and securing your system properly. Before upgrading an existing system to secured status, read the *Migrating an ACE3600 System to Security* chapter.

Before setting up any MC-IoT secured system, follow the instructions in the *Hardening the STS PC and the RTU* chapter carefully to prepare the PC and RTU properly.

Note: Security-related changes to the project (policy, users, roles, keys) are saved automatically when the relevant dialog closes. No OK/Cancel confirmation is required.

Building a Secured System

Process 6-1 describes how a secured MC-IoT system is built.

IMPORTANT: Only an administrator can create and modify the security settings in a system.

Process 6-1 Secured System Build Process

1. Create a new secured project in the STS (see Procedure 6-1-1) or open an existing project (see **Procedure 6-1-13**.)
2. Set the security policy parameters. (See Procedure 6-1-2.)
3. Set the encryption keys. (See **Procedure 6-1-3**.)
4. Define the users. (See **Procedure 6-1-4**.)
5. Define the roles. (See **Procedure 6-1-5**.)
6. Set up the site configuration for maximum security. (See *RTU Hardening* in the *Hardening the STS PC and the RTU* chapter.)
7. Define a site as an authentication server, if needed. (See **Procedure 6-1-6**.)
8. Configure and start up secure MDLC communication. (See Procedure 6-1-10.)

9. Download the security settings to the RTUs. (See Procedure 6-1-11.)
10. Download the site configuration to the RTUs. (See the *MC-IoT STS User Guide*.)
11. Perform configuration and management operations on the RTU using MDLC communication.

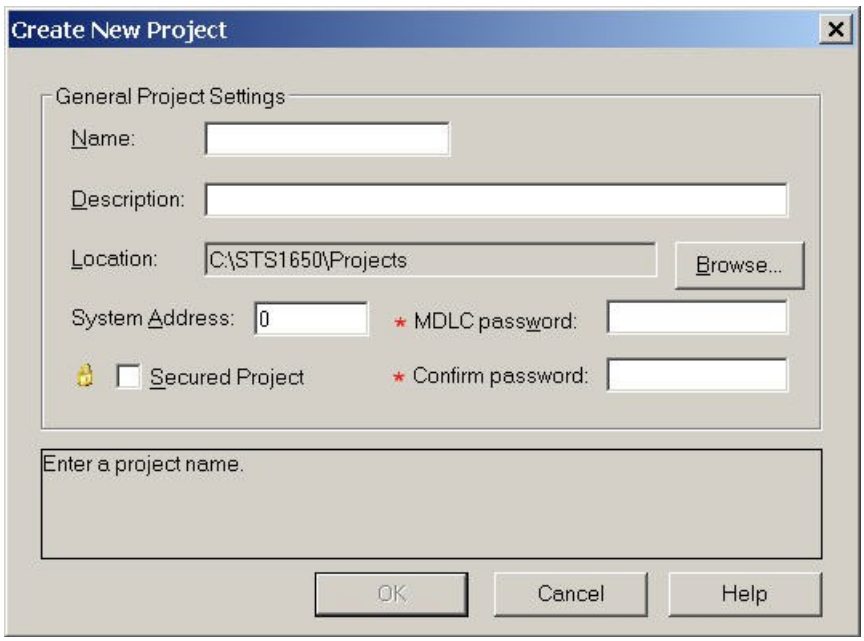
Creating a Project

You can create a secured project or you can create an unsecured project and then secure it afterwards. (See *Securing an Existing Project*.)

Procedure 6-1-1 describes how to create a project in the STS. Each project represents one system.

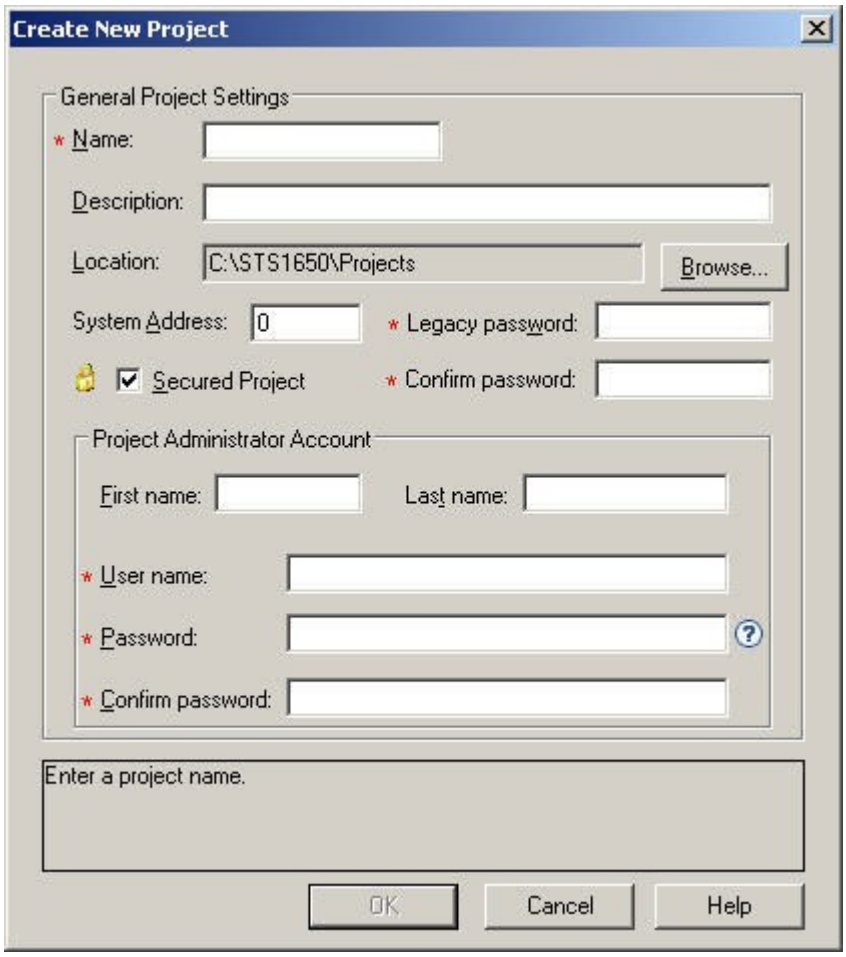
Procedure 6-1-1 How to Create a Secured Project in the STS

1. After starting the STS, click on the New Project button.
   Result: The Create New Project dialog is displayed. Required fields are marked with an asterisk *.



2. Enter the new project name and description, location, and system address (0-65200).
3. Enter and confirm the legacy MDLC password which is used with nonsecured communication (e.g. if the site is nonsecured or if the site is being secured for the first time.)
   Note that the legacy MDLC password is set once during project creation. Afterwards it cannot be changed.

4. Click on Secured Project.
   Result: The Project Administrator Account information is displayed.
   Note: If you do not secure the project, none of the security features will be available. You can secure the project afterwards.



5. Enter the administrator's first name and last name.

6. Enter the administrator's user name.

7. Enter the password and then enter it again to confirm it. (You cannot copy the text from the Password field to paste into the Confirm password field.)

   Note: A valid password must comply with the rules listed in the *User Accounts* section of the *MC-IoT Security Concept* chapter.

8. Click OK to create the new secured project.
   Result: The new project is created in the specified location with the default security policy settings. The system administrator can change these settings.

   Note: When a new project is created, the "Security files signature hardening" is automatically set to enable by default and appears in the policy file.

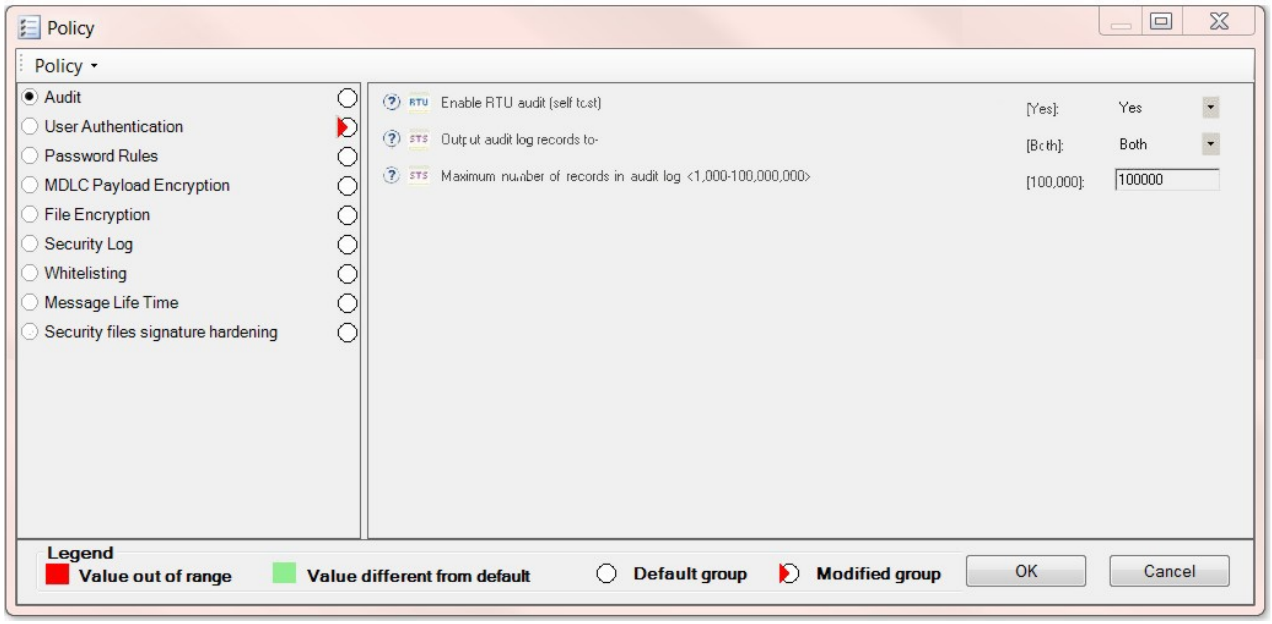
9. Add sites to the project, as described in the *Operation* chapter of the *MC-IoT STS User Guide*.
   Note: By default, a CPU 3680 or CPU 3640 dragged from the inventory is secured. A CPU 3610 dragged from the inventory is unsecured.

Defining the Security Policy

Procedure 6-1-2 describes how to define the security policy for the secured project. For recommended settings, see *Hardening the STS PC and the RTU*.

Procedure 6-1-2 How to Define the Security Policy for the Secured Project

1. To define the security policy for the secured project, select Policy from the Security menu. This command is enabled for administrators only.
   Result: The Policy window is displayed with policy default values.



2. Click on each group in the policy, and configure the parameters for your system. As with the STS advanced site configuration parameters, the color of the policy parameters indicates their status. The color of the policy parameter group reflects change status (white=Default group, red triangle=Modified group). The color of the parameter reflect the value (red=Value Out of Range, green=Value different from default.) For details on each policy parameters and important considerations, see *Appendix A: Security Policy Parameters*.

3. To restore the default policy settings, select Restore default from the Policy menu.

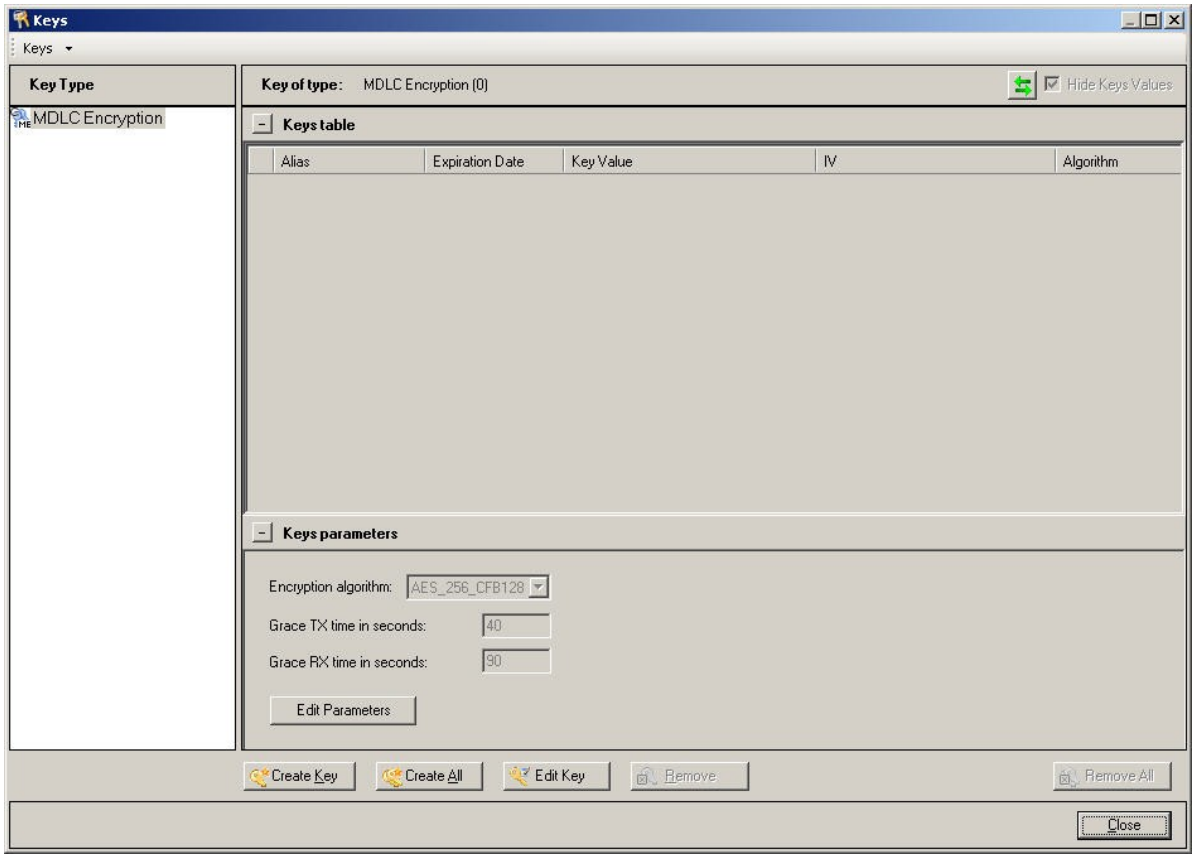
4. Click OK to close the Policy window.
   Result: The Policy window closes and any changes are saved automatically. The settings in the security policy determine the appearance of the GUI, i.e. the availability of certain menu items and fields.

Setting the MDLC Encryption Keys

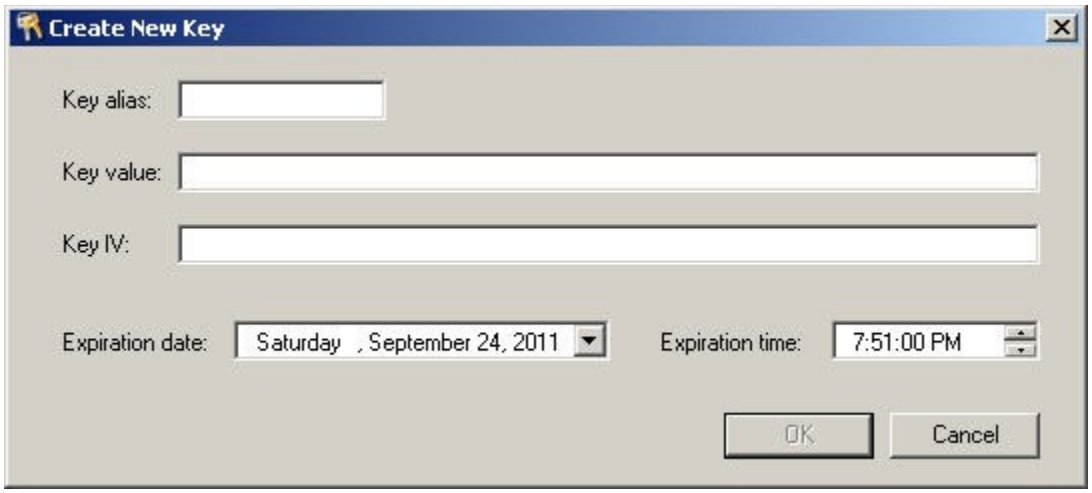
Procedure 6-1-3 describes how to set the encryption keys.

Procedure 6-1-3 How to Set the Encryption Keys

1. To set the encryption keys, select Keys from the Security menu. This command is enabled for administrators only.
   Result: The Keys window is displayed. The key type (e.g. MDLC Encryption) appears in the left pane.



2. To create a key, click on the Create Key button.
   Result: The Create Key dialog is displayed.



3. Enter the Key alias, Key value, and Key IV key information as described in Table 1-1 below. Note that all values must match the settings in the security policy MDLC Payload Encryption group.

4. Enter the expiration date and time which comply with the security policy.

5. Click OK.
   Result: The STS generates a unique, random key to be used for MDLC payload encryption. The parameters of the new key appear in the Keys table.

6. To unhide the key values and key IVs, uncheck the Hide Keys Values field.
   Result: The Key Value and Key IV columns show numeric values instead of asterisks. (Hiding/showing the keys can also be defined in the policy. See the *MDLC Payload Encryption* section of *Appendix A: Security Policy Parameters*

7. If desired, edit the grace TX/RX time. See Table 1-1 below.

To create a set of encryption keys automatically, click on the Create All button.
Result: The Create All Keys Definition dialog is displayed.
Specify the key information per

8. Table 1-2, and click OK.
   Result: A message is displayed asking you to confirm the keys creation which causes all existing keys to be deleted.

9. To remove a key, select the key and click on the Remove button.
   Result: A message is displayed asking you to confirm the key deletion which causes all existing key expiration dates to be updated.
   Click Yes.
   Note: The active key cannot be removed.
   Result: The selected key is removed.
   If removing the key will cause the number of keys in the Keys table to be below the 'Minimum number of MDLC encryption keys' set in the policy, an error message is displayed.

10. To remove all keys, click on the Remove All button.
    Result: A warning message is displayed that removing all keys causes loss of

synchronization between the STS and RTUs, and all units must be erased (on site) to reestablish communication.
Click Yes
Result: All keys in the STS are removed.

11. To refresh the list of keys when the Keys window is open during key swap, click on the Refresh Keys icon. 
Result: The new active key is displayed.

12. To close the Keys window, click on Close.

Table 1-1 Encryption Key Parameters (Manual Creation)

Field	Description
Key alias	Unique key alias
Key value	Unique value used for key generation. Must be 64 hexadecimal characters (for AES).
Key IV	Unique initialization vector used to generate random keys. Must be 32 hexadecimal characters (for AES).
Expiration date	Day and date that the key will expire. Can be selected from the drop-down calendar or components can be modified using the up/down arrow keys.
Expiration time	Time of day that the key will expire.
Encryption algorithm	The encryption algorithm is determined in the Security Policy. Either TEA or AES256 CFB128. IMPORTANT: For purposes of migration, the TEA algorithm is supported in firmware version 16.00 and STS 16.50.
Grace Tx time in seconds	The grace time after the key changes that transmission uses the previous key. After the grace time, transmission uses the current key. This value should be greater than the maximum clock differences between units in the system. This value must also be greater than the maximum retry period in the RTU, to enable retry frames to be successfully decrypted and reencrypted when a key is changed during the Tx retry period. In a system with I/O expansion, the grace time should be long enough to allow the new keys file to be downloaded to all expansion units.

Field	Description
Grace Rx time in seconds	The grace time after the key changes, during which the unit accepts communication based on the previous key or the newly active key. After the grace time, transmission decrypts using the current key only. Note: The grace Rx time should be greater than the grace Tx time. This value should be greater than the maximum clock differences between units in the system. This value must also be greater than the maximum retry period in the RTU, to enable retry frames to be successfully decrypted and reencrypted when a key is changed during the Rx retry period. The grace time should be long enough to allow the message to reach the destination, taking into account routing between several RTUs. In a system with I/O expansion, the grace time should be long enough to allow the new keys file to be downloaded to all expansion units.

Table 1-2 Encryption Key Parameters (Automatic Creation)

Field	Description
Number of keys to create	The number of encryption keys to create. The range is determined by the 'Minimum number of MDLC encryption keys' and 'Maximum number of MDLC encryption keys' parameters in the security policy. By default, the range is between 3 and 12.
Base string for default key alias	The new key aliases will be a combination of this base string and the next parameter, Base index, i.e. <string>_<Base index>, <string>_<Base index+1>, <string>_<Base index+2>, etc. By default, this string is KeyAlias_M/DD.
Base index	A number appended to the previous parameter to form the first new key alias. The number is incremented for each subsequent key alias. By default, this index is 1. (KeyAlias_M/DD_1)

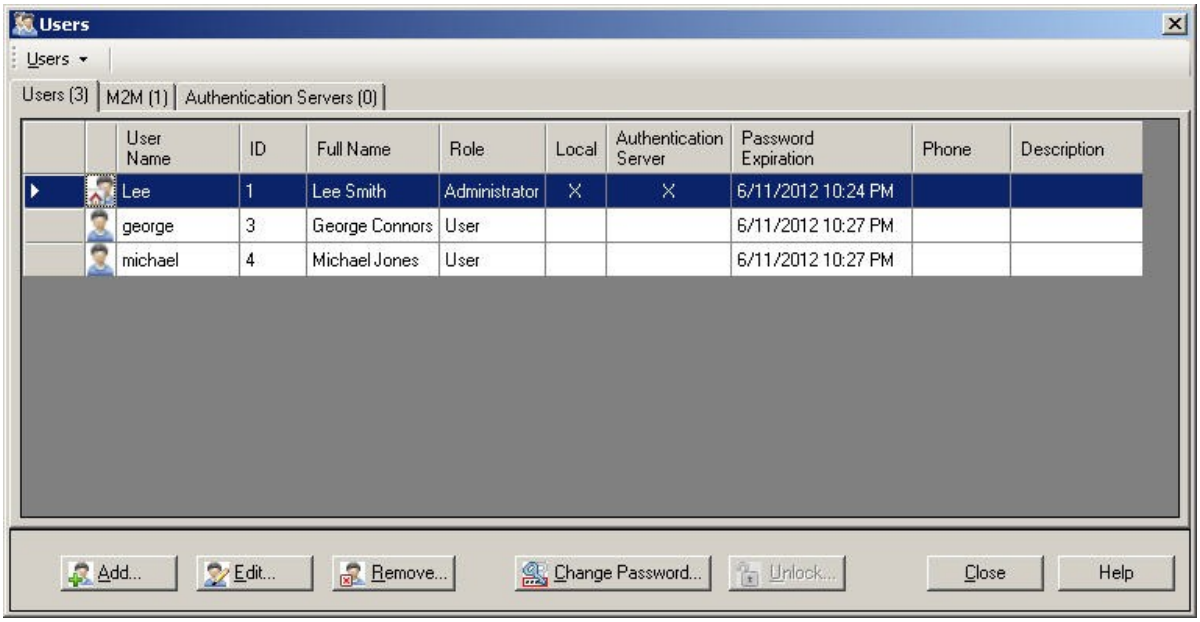
Field	Description
First key expiration date	Day and date that the first key will expire. Can be selected from the drop-down calendar or components can be modified using the up/down arrow keys. The default value is based on the 'Maximum MDLC key duration' setting in the security policy. Once a key has been defined, this field cannot be changed.
Interval time between keys	The number of hours that each subsequent key should be active. The default value is based on the 'Maximum MDLC key duration' setting in the security policy.

Defining the Users

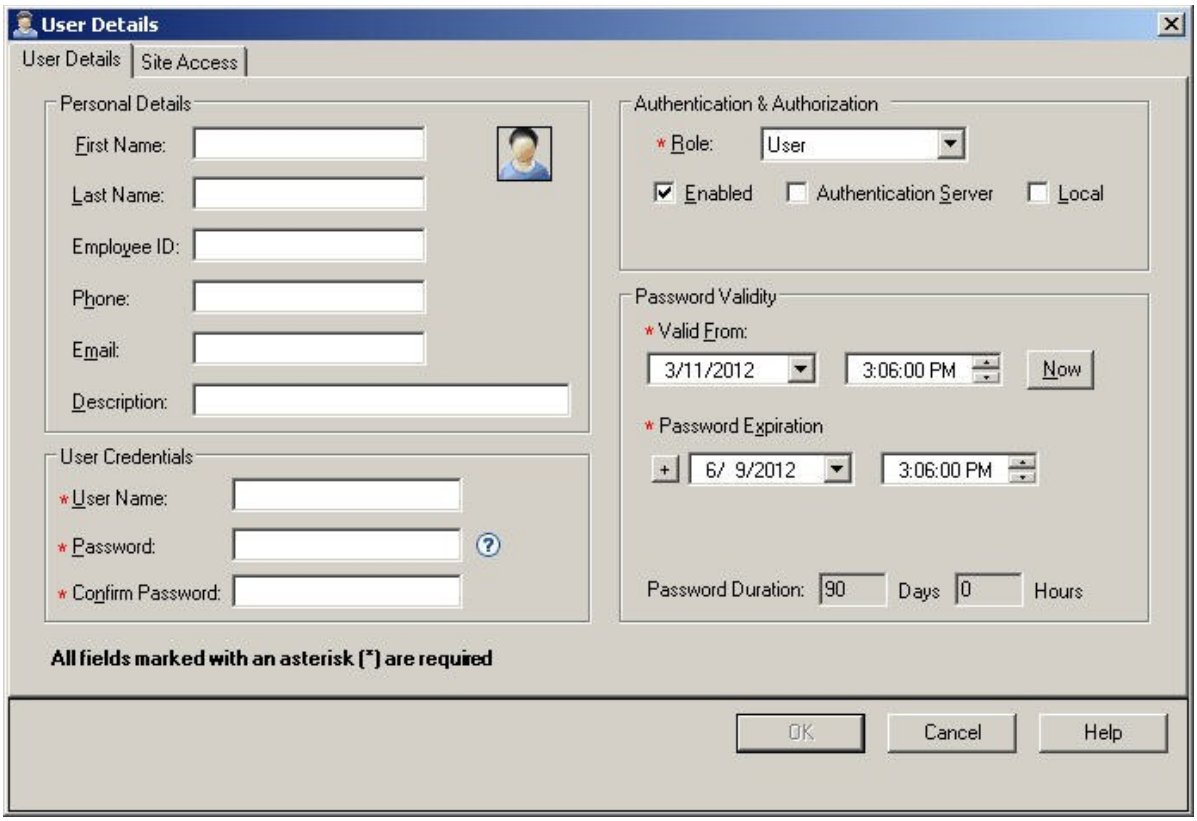
Procedure 6-1-4 describes how to define the users in a system.

Procedure 6-1-4 How to Define the Users in a System

1. To define the users, select Users from the Security menu.
   This command is enabled for administrators only.
   Result: The Users dialog is displayed with the currently configured user(s).



2. To add a human user, click on the Add button.
   Result: The User Details dialog is displayed.



3. Enter the personal details and user credentials (user name and password) of the user. See Table 1-3 for a description of the User Details.
   See the rules for a valid password in *User Accounts* in the *MC-IoT Security Concept* chapter. Click on the icon next to the Password field for the list of valid password rules.
   Confirm the password.

4. Select the user's role from the Role drop-down list.

   To enable the user, click Enabled. A disabled user cannot login to the STS, and once the users file is downloaded to the RTU, cannot access the secured RTU. The disabled user is marked with a slash in the Users dialog.
   IMPORTANT: You cannot disable a user who is the last enabled administrator.

   To restrict site access authentication for this user to the authentication server, click Authentication Server. (The user information will be downloaded to the authentication server.)

   To define the user as a local user of RTUs (where the user credentials will be stored locally in all or selected RTUs), click Local.

5. Specify the password validity date and expiration date:
   To set the Valid From field to the current time and date, click on Now.
   To select a different date, click on the down arrow and click on the desired date.

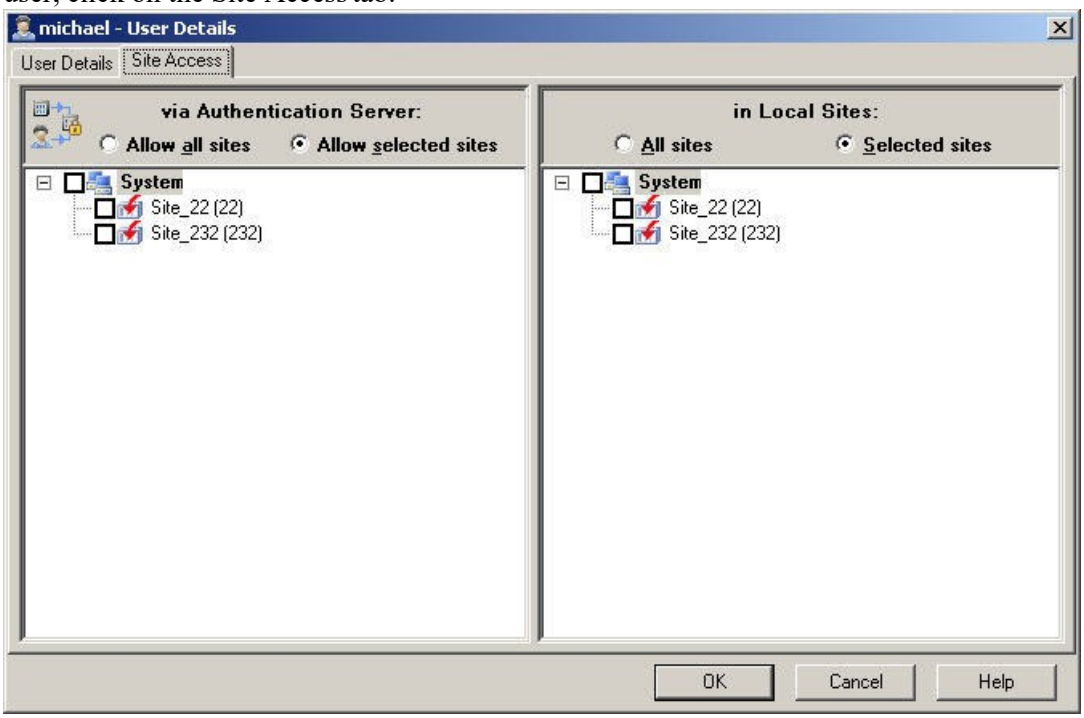
   By default, the Password Expiration is set based on the maximum password age

defined in the security policy.
Expiration can either be specified as a specific date or as a number of hours or days:

To have the password expire on a specific date, click on the down arrow and click on the desired date (per the policy).
Result: The Password Duration field is updated to reflect the selected password duration.

To have the password to expire in a certain number of days, click on the + sign next to the Password Expiration field.
Result: The After field and drop-down list appear.
Select the desired duration in hours or days (per the policy).
Result: The Password Expiration field is updated to reflect the selected period. The Password Duration field is updated to reflect the selected password duration.
Note: An invalid password is marked with a blinking red error icon. Place the mouse over the icon to view the problem (e.g. duration is too long.)

6. By default, the new user has no access to any sites. To define site access for the user, click on the Site Access tab.



Specify whether to allow the user access to all sites or to selected sites when authenticated by the authentication server. (This can be specified even before an authentication server has been defined.) Specify whether to allow the user access to all sites or to selected sites when authenticated by the local site (i.e. as a local user.)
Note: If the Authentication Server field in the User Details tab is not checked, the left panel is disabled. If the Local field in the User Details tab is not checked, the right panel is disabled.

When the All RTU simulation feature is used, access rights must be set for the site IDs in the All RTU simulation address range. Therefore, the administrator must define a "virtual" site in the system for each "simulated" RTU in the address range (with all ports set to "Not used"), and those "virtual" sites will appear in the Site Access tab.
Click OK to close the User Details dialog.

7. To edit a human user, select the user (if there is more than one) and click on the Edit button, or double-click on the user.
   Result: The User Details dialog is displayed.
   Edit the user information as desired.

8. To delete a human user, select the user (if there is more than one) and click on the Remove button.
   Result: A message is displayed asking you to confirm the deletion.
   Click Yes to delete the user, or No to leave the user in the system.
   Note: You cannot delete the currently logged in user.

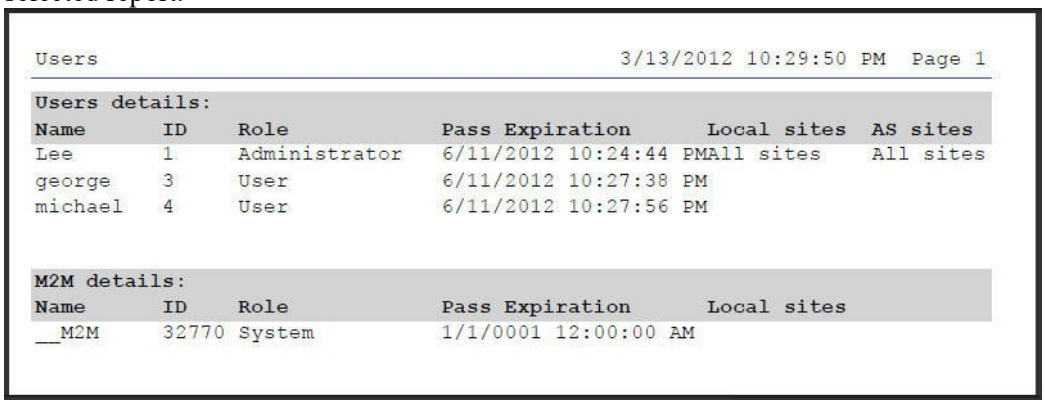
9. To unlock a user who was locked for STS access (due to repeated unsuccessful login attempts), select the user and click on the Unlock button.
   Result: The user is unlocked for STS access.

10. Define authentication servers (up to eight), as defined in **Procedure 6-1-6**, per the policy configuration.

11. To view and edit an M2M (Machine to Machine) user, click on the M2M tab.
    Result: The M2M tab is displayed.
    In a system with common M2M credentials (all RTUs share the same name and password) only one M2M user is displayed. In a system with unique M2M credentials (all RTUs have different names and passwords), all M2M users (one per RTU) are displayed.
    Click on an M2M user and modify the information in the User Details and Site Access tabs, as described in the steps above. Note: Many of the user detail fields are disabled for M2M users.
    See the *Field Unit Credentials and Authentication* section of the *MC-IoT Security Concept* chapter for important information on M2M credentials. See the *M2M Site Access* section of the *MC-IoT Security Concept* chapter for important information on the site access defaults.
    Click OK.
    Note: M2M users cannot be added/removed in the Users dialog.

12. To produce a tabular report of the human and M2M users in the system, click on Print->Table from the Users menu.
    To produce a detailed report of the human and M2M users in the system, click on Print->Details->All properties from the Users menu.
    To produce a brief report of the human and M2M users in the system, click on Print->Details->Essential properties from the Users menu.
    Result: The standard Windows print dialog appears. Click OK to print the

selected report.



Users 3/13/2012 10:29:50 PM Page 1

Users details:

Name	ID	Role	Pass Expiration	Local sites	AS sites
Lee	1	Administrator	6/11/2012 10:24:44 PM	All sites	All sites
george	3	User	6/11/2012 10:27:38 PM		
michael	4	User	6/11/2012 10:27:56 PM		

M2M details:

Name	ID	Role	Pass Expiration	Local sites
__M2M	32770	System	1/1/0001 12:00:00 AM	

13. To close the Users dialog, click on the Close button.
    Result: If no authentication server is defined but there is at least one user configured to be downloaded to the authentication server, a message is displayed asking if you wish to define one.
    Click Yes to go to the Authentication Server tab (see *Defining a Site in a Secured Project*.)

The Procedure 6-for creating a site in a secured project is the same as that of creating a site in a nonsecured project. For more information, see *Defining a Site* in the *MC-IoT STS User Guide*.

When a site is created in a secured project, the site is automatically secured.

New and existing sites must be configured to work properly in a secured system. See specific changes for secured systems in *Appendix A: Site Configuration Parameters* in the *MC-IoT STS User Guide*.

14. Defining an Authentication Server) or No to close the dialog.

15. Once the users in the project are defined and configured, the users file is downloaded (first) to all relevant RTUs and (then) to the authentication server for the changes to take effect. See *Downloading Security Files and Information*.
    Note: Changes to the user names and passwords and roles must be downloaded in order to take effect.

Table 1-3 User Details

Field	Description
First Name	User's first name (optional)
Last Name	User's last name (optional)
Employee ID	Unique (optional)
Phone	User's phone number (optional)
Email	User's email address (optional)
Description	Description of user (optional)

Field	Description
User Name	The name of the user recognized in the system by the STS and the RTUs.
Password	Must conform to valid password rules.
Role	Can be one of: Administrator, Technician, User (default), or Viewer. See *Defining the User Roles and Permissions*.
Enabled	Enables/disables the user from accessing the STS and the RTU.
Authentication Server	Whether the RTUs in the system can authenticate the user's credentials using the authentication server. (The credentials are downloaded to the authentication server.)
Local	Whether the RTUs in the system can authenticate the user's credentials using the local users file, without using the authentication server. (The credentials are to the RTU.)
Password Validity Valid From	Date and time that the password becomes valid. Can be set to today's date and time. Can be selected from the drop-down calendar or components can be modified using the up/down arrow keys. Defaults to today's date.
Password Expiration	Based on the 'Maximum password age' policy parameter and the Valid From field above.
Password Duration	Automatically generated from the previous fields. Reflects the number of days and hours that the password will be valid.

Defining the User Roles and Permissions

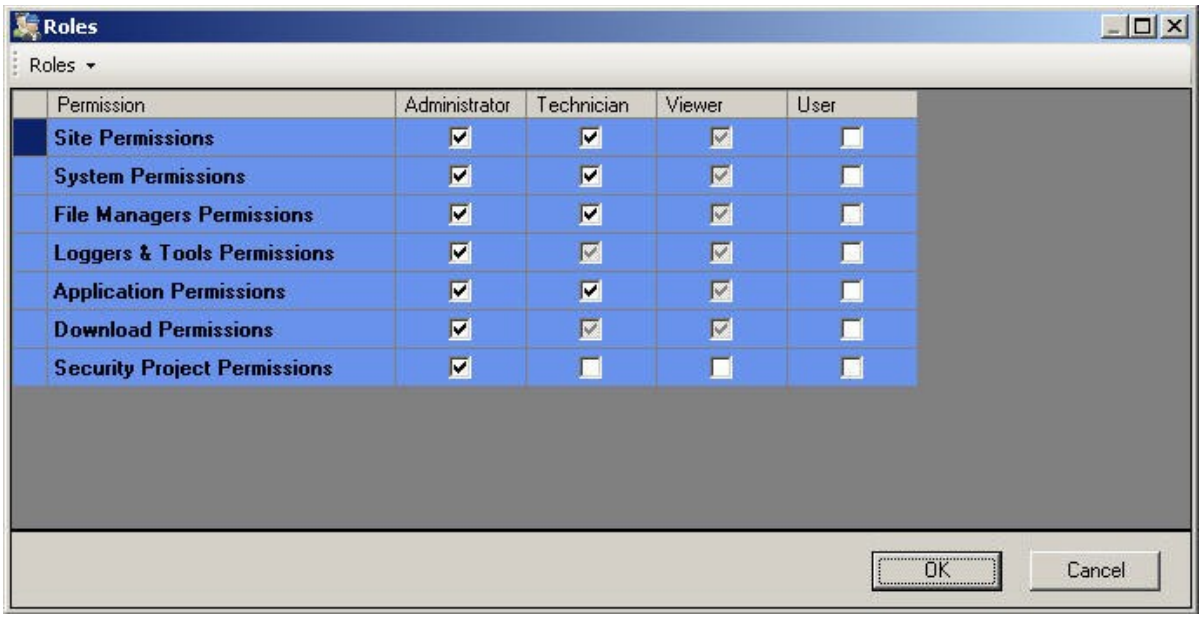
A set of default user roles is defined in a secured system. These roles are used to prevent unauthorized individuals from performing sensitive operations. Each group of permissions includes a number of STS user operations. An authorized administrator can modify the permissions assigned to the "User" role.

For the list of the default user roles and permissions, see *Appendix B: User Roles and Permission Groups*.

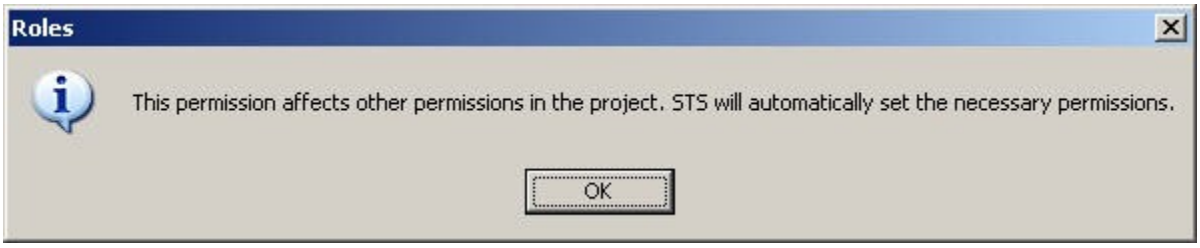
Procedure 6-1-5 describes how to set "User" role and permissions.

Procedure 6-1-5 How to Set User Role Permissions

1. To set the role permissions for the "User" role, select Roles from the Security menu. This command is enabled for administrators only.
   Result: The Roles dialog is displayed.



2. To grant a group of permissions to the User role, click in the checkbox for that permission group. To remove a granted permission group, click again in the checkbox.
   Result: All relevant permissions in the group are changed. If the selected group includes a permission which is related to other permissions, all related permissions are automatically changed by the STS and a message is displayed to that effect. Click OK to close the message.



3. To restore the default roles, select Restore default from the Roles menu.
4. To save the changes to the roles and permissions, click OK.

Defining a Site in a Secured Project

The Procedure 6-for creating a site in a secured project is the same as that of creating a site in a nonsecured project. For more information, see *Defining a Site* in the *MC-IoT STS User Guide*.

When a site is created in a secured project, the site is automatically secured.

New and existing sites must be configured to work properly in a secured system. See specific changes for secured systems in *Appendix A: Site Configuration Parameters* in the *MC-IoT STS User Guide*.

Defining an Authentication Server

In a system with user authentication, the site ID and link ID of the authentication server is downloaded to all RTUs in the project in the users file. The network file includes the path (high speed link) to the authentication server. The authentication server can be any RTU. A second authentication server can be defined for authentication redundancy.

Procedure 6-1-6 describes how to define a site as an authentication server.

Procedure 6-1-6 How to Define an Authentication Server

1. Select Users from the Security menu.
   Result: The Users dialog is displayed.

2. To define an authentication server, click on the Authentication Servers tab. Click on the Add button. Note: This button is disabled if the 'Maximum number of authentication servers' parameter in the policy is set to 0.
   Note: See the *M2M Site Access* section of the *MC-IoT Security Concept* chapter for important information on the site access defaults with authentication servers.
   Result: In a system with unique M2M credentials, a message is displayed warning that adding the first authentication server will automatically change the configuration of Local sites for all M2M users. Click Yes to proceed.
   Result: The New Authentication Server Details dialog is displayed.

   Select the desired Site and Link (preferably a high speed link) from the drop-down lists, and click OK.
   Note: If the authentication server is a redundant CPU, only links that are common to both primary and secondary CPU appear on the list.
   Result: The new authentication server appears in the Authentication Servers tab.
   Note: A list of up to eight prioritized authentication servers can be defined in a system, as specified in the policy in the 'Maximum number of authentication servers' parameter. An authentication server must be defined in order to download users to it.

3. Click on the Users tab. Edit each desired user, using the Site Access tab, to restrict site access to specific sites and the authentication server(s). (See *Defining the Users*.)
   Result: The selected human users will be authenticated on the specified sites using the authentication server.
   Note: The M2M users are automatically assigned authentication via the authentication server.

4. Once the other sites in the project are defined and configured, download the users file with the authentication server ID to all sites. See Downloading Security Files and Information.

5. To edit an authentication server, click on the authentication to be edited, and click on the Edit button.
   Result: The Authentication Server – Details dialog is displayed.

   Change the site or link in the Link drop-down list, and click OK.

6. To delete an authentication server, click on the authentication to be deleted, and click on the Remove button.
   Result: A message is displayed asking you to confirm the removal of the authentication server.
   Click Yes to delete the authentication server.
   Note: The site remains in the project, but it is no longer an authentication server.

7. Click on Close to close the Users dialog.

Adding Authentication Servers to a System

Procedure 6-1-7 How to Add Authentication Servers to a System

1. To enable adding Authentication Servers to a system, from the STS menu, click **Policy**.

   Result: The **Policy** window appears.

2. Set the "Enable selection of Authentication Server per site" option to **Yes**.

3. To Add Authentication servers, from the STS system view, right-click on a site and select **Authentication Server**.

   Result: The **Site Authentication Servers** dialog box appears.

4. Click **Add** to add an Authentication Server. Make sure to set the priority level of the server (0 is the highest and 7 is the lowest priority).

Exporting or Importing Authentication Servers Priority Table

Exporting or importing a priority table of Authentication Servers is used mainly for duplicating priority of Authentication Servers between sites. A table created by the STS

can be exported to a Microsoft Excel file, edited offline, and imported back into the same site or other site.

Procedure 6-1-8 How to Export Authentication Servers Priority Table to a Microsoft Excel file

1. From the STS menu, click **System** and select **Export Site Properties**.

   Result: A dialog box appears.

2. Check the parameters required to be included in the priority table and click **OK**.

Procedure 6-1-9 How to Import Authentication Servers Priority Table to a Site

1. From the STS menu, click System and select "Export Site Properties".

   Result: A dialog box appears.

2. Select a valid Excel file (use the same table format as in the exported file) and click **OK**.

Starting Secured MDLC Communication with the RTU

Communication with the RTU is controlled by the MDLC communication driver, when performing various configuration and management STS operations on the RTU.

By default, communication between a secured STS and a secured site is secured. For detailed information on the MDLC communication driver, see the *MDLC Communication Driver* section of the *MC-IoT Security Concept* chapter. Procedure 6-1-10 describes how to communicate with a secured unit to perform various STS operations.

Note: When migrating a system to secured state, or when changing security features in an existing system, communication-related changes made in the STS (e.g. changing passwords, keys and some policy parameters) are applied immediately to the MDLC driver. This can create a security mismatch between the RTU, which is not yet aware of the change (until the relevant download is performed,) and the STS, which is already using the changed values. For these cases, the STS provides a mechanism which enables you to change the MDLC driver communication settings locally to old settings, for the sake of downloading files to update the RTU. This mechanism is controlled from the gear icon in the Secured field. Initially, when the RTU is not yet secured, communication must be performed on a non-secured channel.

Procedure 6-1-10 How to Communicate with a Secured Site

1. Select the secured STS operation (e.g. download of security policy or security log retrieval) for a secured RTU.

2. In the Connection bar at the top of the window, specify the connection:
   Select Local for a local connection, or select the desired Site ID and Link ID.

   To communicate with a secured site (e.g. to download changed passwords to the authentication server), make sure to the Secured field is set in the Connection bar.

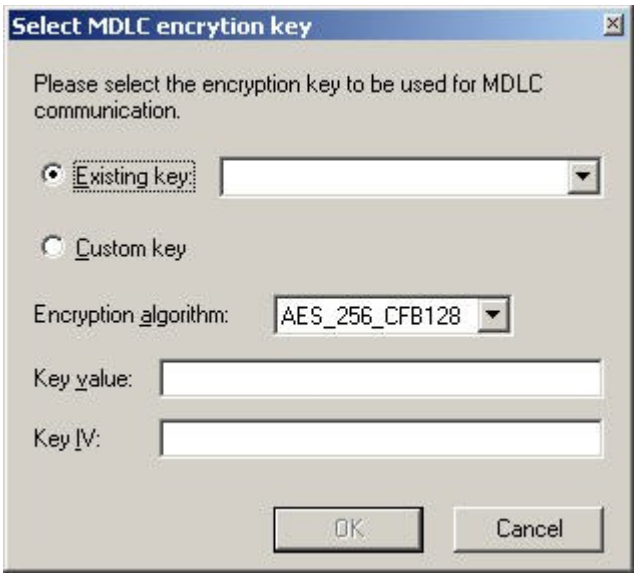
To communicate with an unsecured site (e.g. for the initial download of security files to a new site), unset the Secured field, to use a nonsecured channel in the MDLC driver (using the legacy password defined during project creation). The field will turn pink.

IMPORTANT: Once the site is secured (e.g. initial security information has been downloaded to the site), make sure to set the Secured field in the Connection bar. The field will turn green.

3. To configure MDLC communication with the RTU, click on the gear icon in the Secured field.
Result: The Secured Communication Settings dialog is displayed.

To use the communication settings in the policy, make sure Policy default is checked.
To modify the communication settings to override the policy, uncheck Policy default and configure the settings as desired. See Table 1-4 Secured Communication Settings for a description of the secured communication settings.

To override the encryption key, check Override encryption key.
Result: The Select MDLC encryption key dialog appears.



To use an existing key, select the desired key from the Existing key drop-down list. To create a custom key, check Custom key and enter the desired key information. For more details, see *Setting the MDLC Encryption* Keys.
Click OK to set the key.
Click OK to close the Secured Communication Settings dialog.
Result: The Secured field will turn yellow.

4. Initiate the secured STS operation (e.g. press Download or Start.)
   Result: If your user credentials are valid and no other MDLC driver is running, the MDLC driver is started in secured mode. The driver icon is different than the icon for the MDLC driver in non-secured mode.

   If an MDLC driver in non-secured mode is already running, a message is displayed asking the user to stop that MDLC driver.
   If you stop the driver and confirm this message, the MDLC driver is started in secured mode.
   If you fail to confirm this message, the MDLC driver in non-secured mode continues running and the communication fails.

5. After the STS operation is complete, you may stop the MDLC driver using the Stop Comm Driver command in the Setup menu. Otherwise, leave the MDLC driver for subsequent MDLC communication.
   Note: When the secured STS is closed, the MDLC driver in secured mode remains operative, as it is capable of servicing secured/non-secured STS and even legacy ToolBox versions.

Table 1-4 Secured Communication Settings

Field	Description
Policy default	When checked, MDLC communication uses the settings in the security policy and the most up to date user and key settings. When unchecked, MDLC communication uses the override values in this dialog.
User authentication	When Policy default is unchecked, enables/disables user authentication for this session.
Hash length for session	When Policy default is unchecked, sets the length of the generated hash password (included in each frame) for communication for this session. Note: All communication from the STS is session-based.
Override password	When Policy default is unchecked, overrides the password in the current communication session. Use this option to download a users file in which the password of the current user has been changed, while the unit still recognizes the user's previous password.
Use encryption	When Policy default is unchecked, enables/disables MDLC payload encryption in the current communication session.
Override encryption key	When Policy default is unchecked, overrides the encryption key in the RTU for this session. Used when the STS and RTU are not using the same encryption key (e.g. if the date/time in the RTU and the STS PC are not synchronized, and the active key changes in one and not the other.) In this situation, the STS cannot communicate with the RTU, but it may not be obvious that this is the problem. If you suspect that this is the case, instruct the STS to use a key which is not currently active (select existing key) or is not even defined in the keys file (custom key).
Override encryption key: Existing Key	When overriding the encryption key, enables the user to select an existing encryption key.
Override encryption key: Custom Key	When overriding the encryption key, enables the user to define a custom encryption key.
Encryption algorithm	See Table 1-1.
Key value	See Table 1-1.
Key IV	See Table 1-1.
Define message	When Policy default is unchecked, enables/disables

lifetime	overriding Message Life Time policy parameters.
Message lifetime	When Policy default is unchecked and Define message lifetime is checked, overrides the Message Life Time Window policy parameter.

Downloading Security Files and Information

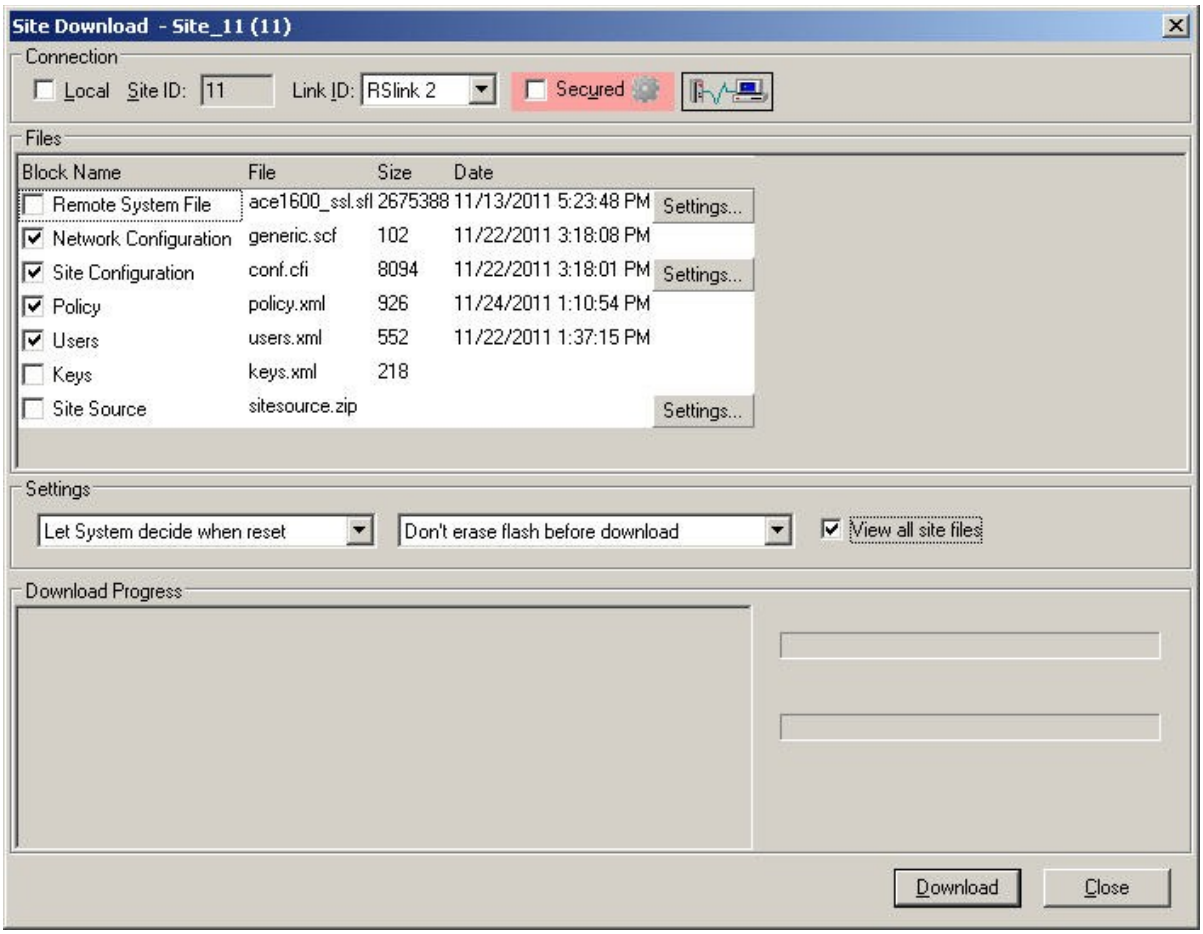
An authorized user can download security files and security related information (policy, users file, and keys file) to a secured site (RTU or authentication server.) Procedure 6-1-11 describes how to download security files and information one or more sites.

Note: When setting up a secured system, an existing nonsecured unit should be erased before downloading security files. See *Securing a Site* below.

Note: Downloading the policy to a unit will cause the unit to restart.

Procedure 6-1-11 How to Download Security Files and Information to a Site

1. To download to a specific site, click on the Download icon in the site view, or select the Download command from the Site menu in the menu bar.
   To download to more than one site, select the Download All Sites command from the System menu in the menu bar.
   Result: If changes were made to the project, you will be prompted to save the project.
   The Site Download window will be displayed with the list of files that can be downloaded. Those files in the list which are marked with a check need to be downloaded.
   Note: The file sizes displayed in the Site Download window are different than those displayed in the Field View. This can be due to file compression, or to the header that is added to the files in the RTU. For site configuration, additional information is added (new site ID) during download. For network configuration, the file sizes differ from site to site, because only relevant communication links are downloaded to each unit.



2. In the Connection bar, specify the connection. For details, see step 3 under Starting Secured MDLC Communication with the RTU.

3. Select the security files to be downloaded to the site (Policy, Users, and/or Keys).

   IMPORTANT NOTES:
   You cannot download the policy to a site if the policy version is lower than the firmware version, or if the firmware is not the secured version. You cannot download firmware to the site if the firmware version is higher than the policy version.

   The users and keys files cannot be downloaded to an RTU before the policy file. The policy is the only security related file which can be downloaded to a non-secured site whose firmware supports security.

   IMPORTANT: The order of downloads is very important. First download the security policy. After the unit resets, you can download the users and then the keys files. Finally, download files such as ladder/'C' application, MODBUS, etc. Note that you cannot download the users and keys files at the same time over unsecured communication. See Securing a Site below.

   Before downloading the users file, you may want to compare the list of users in a site with that of the STS. See Uploading and Comparing Users.

When the users file is downloaded to a site defined as an authentication server, it contains credentials for all users. When the users file is downloaded to a site (local file), it includes
- the site's own (M2M) user name and password
- the authentication server's user name and password
- the user name and password of all users defined as Local for that site

4. In the Downloader Settings section, select the desired settings:
   If you choose to erase the flash, select the flash erase type (the list of flash erase types depends on the state of the unit and the permissions of the user):
   - Erase all flash before download
   - Erase flash and preserve siteConf and policy
   - Erase flash and preserve siteConf and security

5. Click on the Download button to download the file(s).

6. To close the Download window, click on the Close button.

Note: Once security files have been downloaded to a site, they cannot be uploaded to the STS.

Switching Users

Because different users have different roles/permissions, it may be necessary to switch users during an STS session. Procedure 6-1-12 describes how to switch users in the project.

Procedure 6-1-12 How to Switch Users in the Project

1. To switch users, click on the Switch User command in the Security menu, or select Switch User from the Logged in User menu at the bottom of the window.

Result: The Switch Users dialog is displayed.

2. Enter the valid user name and password of the user to switch to.

3. Click OK.
   Result: If the credentials entered are valid, the current user is switched and the new user appears as the Logged in User at the bottom of the window. Otherwise, an error message is displayed.

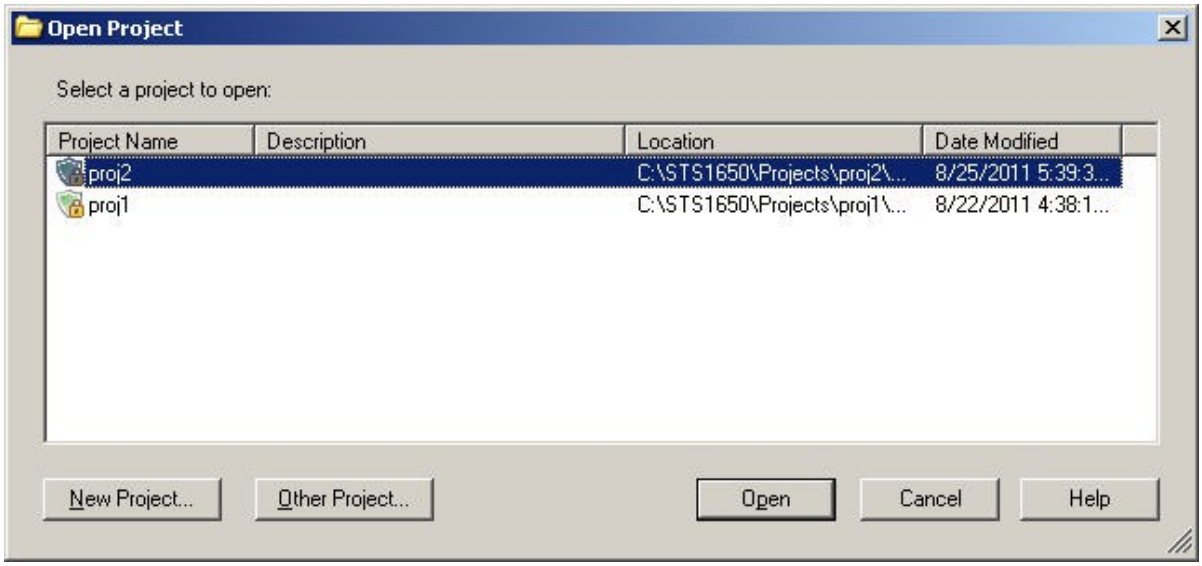
Administering a Secured System

Opening an Existing Project

Procedure 6-1-13 describes how to open an existing project. If the project is not secured, you can secure it after opening it. (See *Securing an Existing Project*.)

Procedure 6-1-13 How to Open an Existing Project

1. After starting the STS, select the Open Project command from the File menu.
   Result: The Open Project dialog is displayed. The icon next to the project name indicates whether the project is secured or not.



2. Click on the desired project name and click on Open, or double-click on the project name.

Result: The Secured Project Login dialog is displayed.

3. Enter a valid User name and Password and click OK.
   Result: The project opens.

   If invalid credentials are entered, an error is displayed.

   If an unknown user name is repeatedly entered (as defined in the security policy in the 'Number of wrong-user-name login attempts before project lock' parameter), the project is locked for a predefined timeout (as defined in the security policy in the 'Lock period after wrong-user-name authentication failure' parameter).

   If an invalid password is repeatedly entered (as defined in the security policy in the 'Number of wrong-password login attempts before user lockout' parameter), the user is locked for a predefined timeout (as defined in the security policy in the 'Lock period after user authentication failure' parameter).

   Note: Administrator credentials will open the project even if it is locked or if the password start time is set to a future time.

4. If the user's (administrator or nonadministrator) password is close to expiration (as defined in the security policy in the 'Password pre expiration alert' parameter), a message is displayed reminding the user to change the password as soon as possible.
   If the (administrator) user logs in and there are user passwords close to expiration, the reminder appears on the dialog which lists all those users whose user passwords are close to expiration.

Changing a User Password

You can change your password while you are logged in to the STS. However, when you change your password, the MDLC driver starts using your new password. Because your user name/current password were not yet downloaded to the RTUs, this may create a conflict. Therefore, the users file must be downloaded again to all relevant RTUs by an administrator. The MDLC driver is automatically updated with the new user name and

password.
Note: If necessary, you can override the password in the Secured Communication Settings. See Starting Secured MDLC Communication with the RTU.

Procedure 6-1-14 describes how to change a user password.

Procedure 6-1-14 How to Change a User Password

1. To change the user password for the current human user, select the Change Password command from the Security menu, (or select Users from the Security menu, and click on the Change Password button in the Users dialog.)
   Result: A message is displayed that the users file will have to be downloaded to all relevant sites. Click Yes to continue (or No to cancel.)
   Result: The Change Password dialog is displayed.

2. Enter the old password. Note: This field does not appear in the Change Password dialog when an administrator is changing a user's password.

3. Enter the new valid password and then enter it again to confirm it. (You cannot copy the text from the Old Password field to paste into the New/Confirm New Password field.) See the rules for a valid password in *User Accounts* in the *MC-IoT Security Concept* chapter.

4. To change the password for another user (permitted for administrators only), Select Users from the Security menu and click on the desired user in the Users dialog.
   Click on the Change Password button.
   Result: The Change Password dialog is displayed.
   Enter the new valid password and then enter it again to confirm it. (You cannot copy the text from the Old Password field to paste into the New/Confirm New Password field.) See the rules for a valid password in *User Accounts* in the *MC-IoT Security Concept* chapter.

5. To change the password for an M2M user (permitted for administrators only), Select Users from the Security menu and click on the desired M2M user in the Users dialog.

Click on the Change Password button.
Result: A message is displayed that the users file will have to be downloaded to all relevant sites. Click Yes to continue (or No/Cancel to cancel.)
In the Secured Project - Password Verification dialog, enter your password. (Your password must be entered again, because this action requires double authentication.)
Result: The password is changed.
IMPORTANT: Downloading the users file with an updated M2M password must be done with care to ensure that communication with units is maintained. See the *Field Unit Passwords* section of the *MC-IoT Security Concept* chapter for important information on the order of downloading.

IMPORTANT: Changing the user password in STS does not change the password in the RTU. It is the administrator's responsibility to download the new users file to the relevant RTUs.

Securing an Existing Project

Procedure 6-1-15 describes how to secure an existing project.

Procedure 6-1-15 How to Secure an Existing Project

1. To secure an unsecured project, open the nonsecured project and select the Secure Project command from the File menu.
   Result: The Secure Project dialog is displayed.

2. Enter the administrator's first name and last name.
3. Enter the user name.
4. Enter your password, confirm it, and click OK.
   Note: You cannot copy the text from the Password field to paste into the Confirm Password field. See the rules for a valid password in *User Accounts* in the *MC-IoT Security Concept* chapter.

Result: A success message is displayed. The administrator has access to all sites in the project.

5. Click OK to close the message window.

6. Once the project is secured, the STS asks if you want to secure all relevant sites (i.e. RTUs with firmware V16.00 or higher.) To have the STS secure the sites for you, click Yes.
   Result: The relevant sites are secured.
   If you click No, you can secure the relevant sites manually. See *Securing a Site*.

Copying a Secured Project

A user with the proper Windows permissions can copy a secured project from one STS PC to another, if the master password defined during STS installation on both PCs is the same.

Securing a Site

The system administrator must secure each site before deploying it in the system.

Before securing the site, the ACE3600 unit should be fully erased (press the two pushbuttons at startup, as described in the *ACE3600 RTU Owner's Manual*).
Note: The RTU itself must be security enabled (i.e. it must include a security signature from the factory.) Legacy units cannot be secured and migrated to a secure system.

Securing an RTU means loading it with firmware that supports security, setting the STS project with all security related values (policy, keys, users, and permissions) and updating RTUs with those files.

Note: If the ACE3600 site runs firmware < V16.00 (created in STS < V16.50) or is in bootstrap mood, you must first download nonsecured firmware ≥ V16.00 (or higher). For details, see the *Migrating an ACE3600 System to Security* chapter.

Procedure 6-1-16 describes how to secure a site in a secured project.

Procedure 6-1-16 How to Secure a Site in a Secured Project

1. To secure an existing unsecured site (ACE3600 with firmware ≥ V16.00), select the Secure command from the Site menu.
   Result: The padlock on the site icon in the Diagram view is enabled.
   IMPORTANT: Securing a site in the STS is only the first step. The site is not actually secured until all the necessary files have been downloaded.

2. Save the project.

3. Define the project's security settings (policy, users, keys, permissions, etc.) See the *Hardening the STS PC and the RTU* and *Guidelines for Securing a System* chapters.

4. Download the necessary files to the site: (See Downloading Security Files and Information)
   a. Connect the STS to the RTU.
   b. Download the site configuration and application (versions must correspond to

the new system software, e.g. STS V16.50 for system V16.00.)
c. ACE3600: After the system restarts, download system software that supports security (≥ V16.00).
d. Download the security policy.
e. Download the users file.
f. Download the keys file.
g. Download the site configuration and application again and any other required files, in order to save them in encrypted form in the RTU.

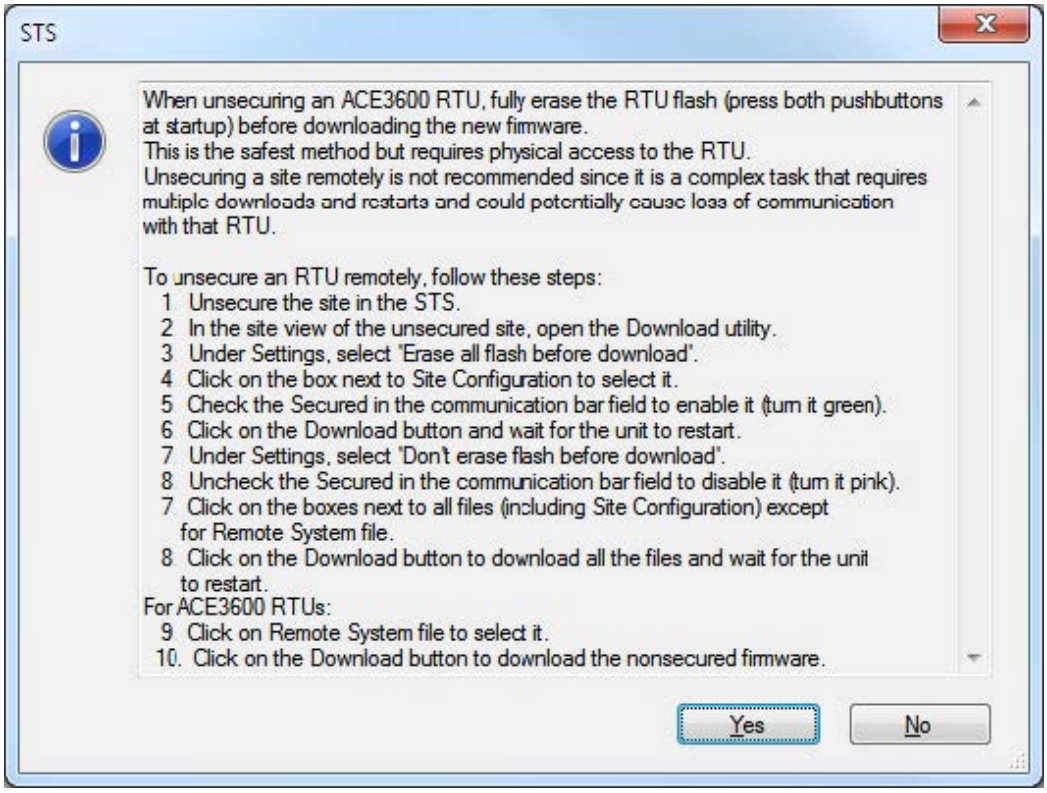
Unsecuring a Site

Procedure 6-1-17 describes how to unsecure an existing site. First the site is unsecured in the STS, and then the corresponding unit is unsecured as well.

IMPORTANT: It is recommended to unsecure a site locally because of potential communication loss with the site.

Procedure 6-1-17 How to Unsecure an Existing Site

1. To unsecure an existing site, select the Unsecure command from the Site menu.
   Result: A message is displayed listing the instructions for unsecuring the corresponding unit.



2. Read the instructions carefully. You can copy the text into a text editor for further reference. Click Yes.
   Result: The padlock on the site icon in the Diagram view is removed. The site is unsecured in the STS.

3. Unsecure the unit according to the instructions.

   Locally (recommended - ACE3600 only):
   a. Connect the STS locally to the unit.
   b. During startup, press both PB1 and PB2 simultaneously to erase all files in the user Flash memory except log files.
   c. Download the non-secured system software.
   d. Download other site files.

   Remotely:
   a. In the site view of the unsecured site, open the Downloader utility.
   b. In the Connection bar, specify the Site ID and Link ID, and check the Secured field to enable it (turn it green).
   c. Under Settings, select 'Erase all flash before download'.
   d. Click on the box next to Site Configuration to select it.
   e. Click on the Download button and wait for the unit to restart.
   f. After the RTU restarts, click on the boxes next to all files (including Site Configuration) except for Remote System file.
   g. In the Connection bar, uncheck the Secured field to disable it (turn it pink).
   h. Click on the Download button to download all the files and wait for the unit to restart.
   i. ACE3600 only: After the RTU restarts, click on Remote System file to select it.
   j. ACE3600 only: Click on the Download button to download the nonsecured firmware.

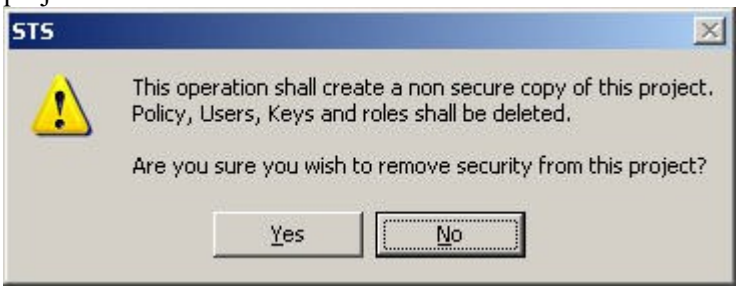
Note: If, after unsecuring the site, you plan to downgrade the ACE3600 RTU to firmware < V16.00, first see *Downgrading Firmware to V15.00 or Lower* in the *Guidelines for Securing a System* chapter.

Unsecuring an Existing Project

Procedure 6-1-18 describes how to unsecure an existing project. Unsecuring a project creates a nonsecured copy of the project, without the security configuration (policy, users, keys, and roles). The secured copy can be saved for later use.

Procedure 6-1-18 How to Unsecure an Existing Project

1. To unsecure a secured project, select the Unsecure Project command from the File menu. This command is enabled for administrators only.
   Result: A prompt is displayed asking you to confirm to copy data from the project.

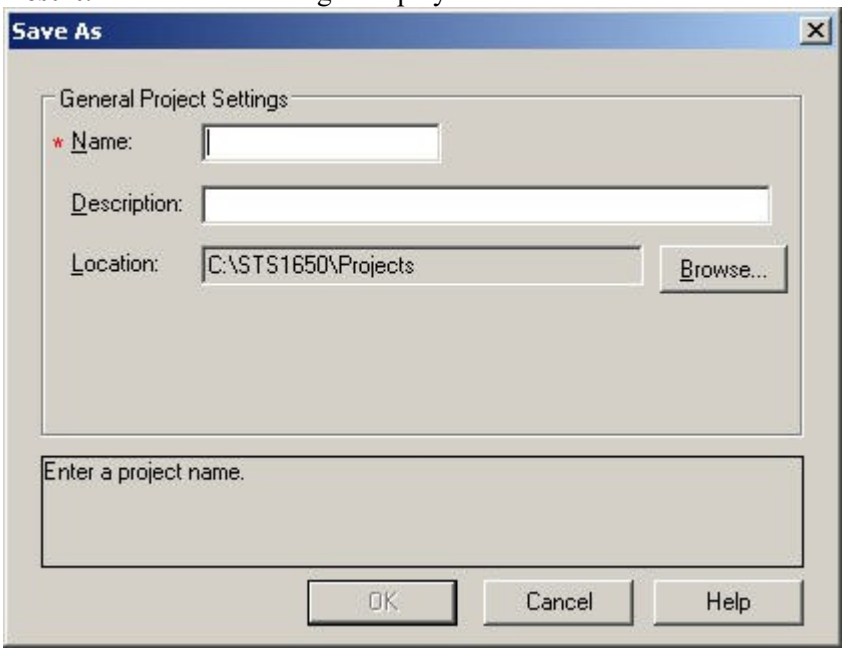


2. Click Yes.

Result: The Secured Project - Save As Dialog is displayed for additional authentication.

Reenter the password and click OK.

3. **Result:** The Save As dialog is displayed.



4. Enter the new project name (e.g. MyProjNonsecure.)

5. Enter the project description (optional).

6. Browse to the desired location to store the project (the default is C:\STS<version>\Projects\), select the location and click OK.

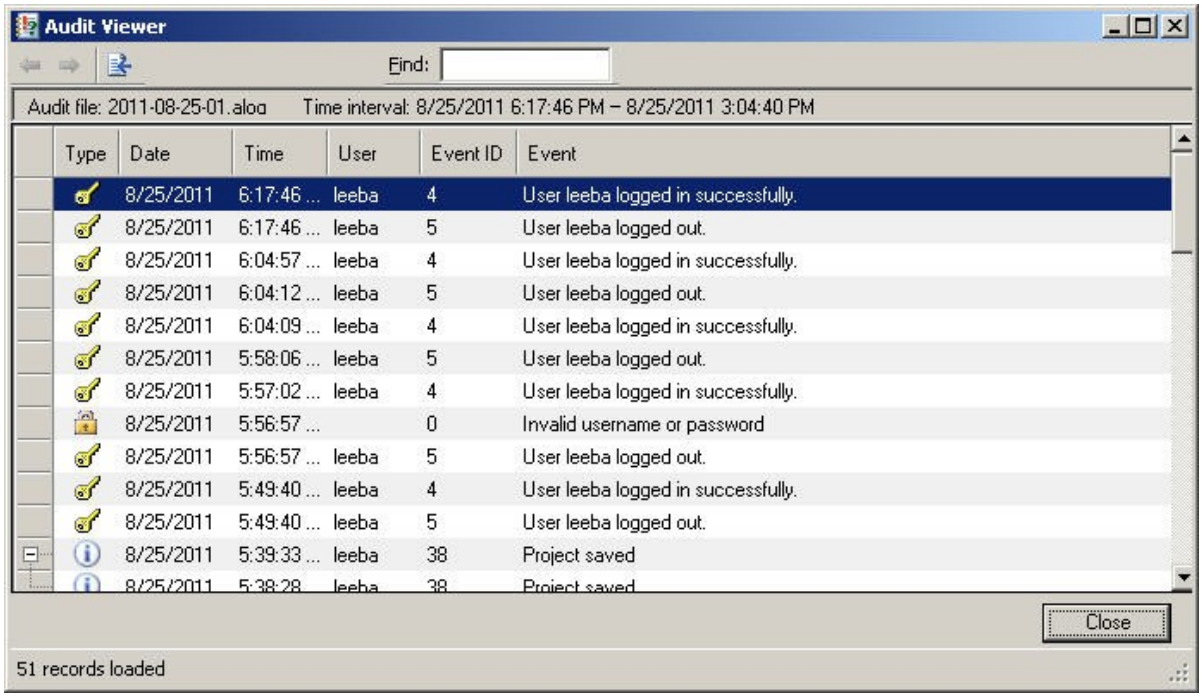
7. Click OK to save the project.
   Result: All security-related files are removed from the new copy of the project. The secured project is closed and the new unsecured project is opened instead. A message is displayed that the new project was successfully unsecured. The RTUs in that project are unsecured.

Viewing the Audit Log

The secure MC-IoT STS saves an audit trail of all security-related operations performed during the STS session. In the security policy, the administrator determines whether this information is saved to an STS event log, to a Windows event log, or to both. Procedure 6-1-19 describes how to view the STS audit event log. For information on viewing the Windows event log with the Windows Event Viewer, see Windows help.

Procedure 6-1-19 How to View the Audit Log in the STS

1. To view the audit log, select the View Audit Log command from the Security menu. This command is enabled for administrators only.
   Result: The Audit Viewer is displayed.



2. To search for a specific event, enter a text string in the Find field.
   Result: The next entry with that string is highlighted.

3. To export the log to a .csv file, click on the Export to File  icon.
   Result: The Save As dialog is displayed.
   Select a location and file name and click Save.
   Result: The audit log .csv file is saved.

4. To see the previous page, click on the Previous icon. To see the next page, click on the Next icon.

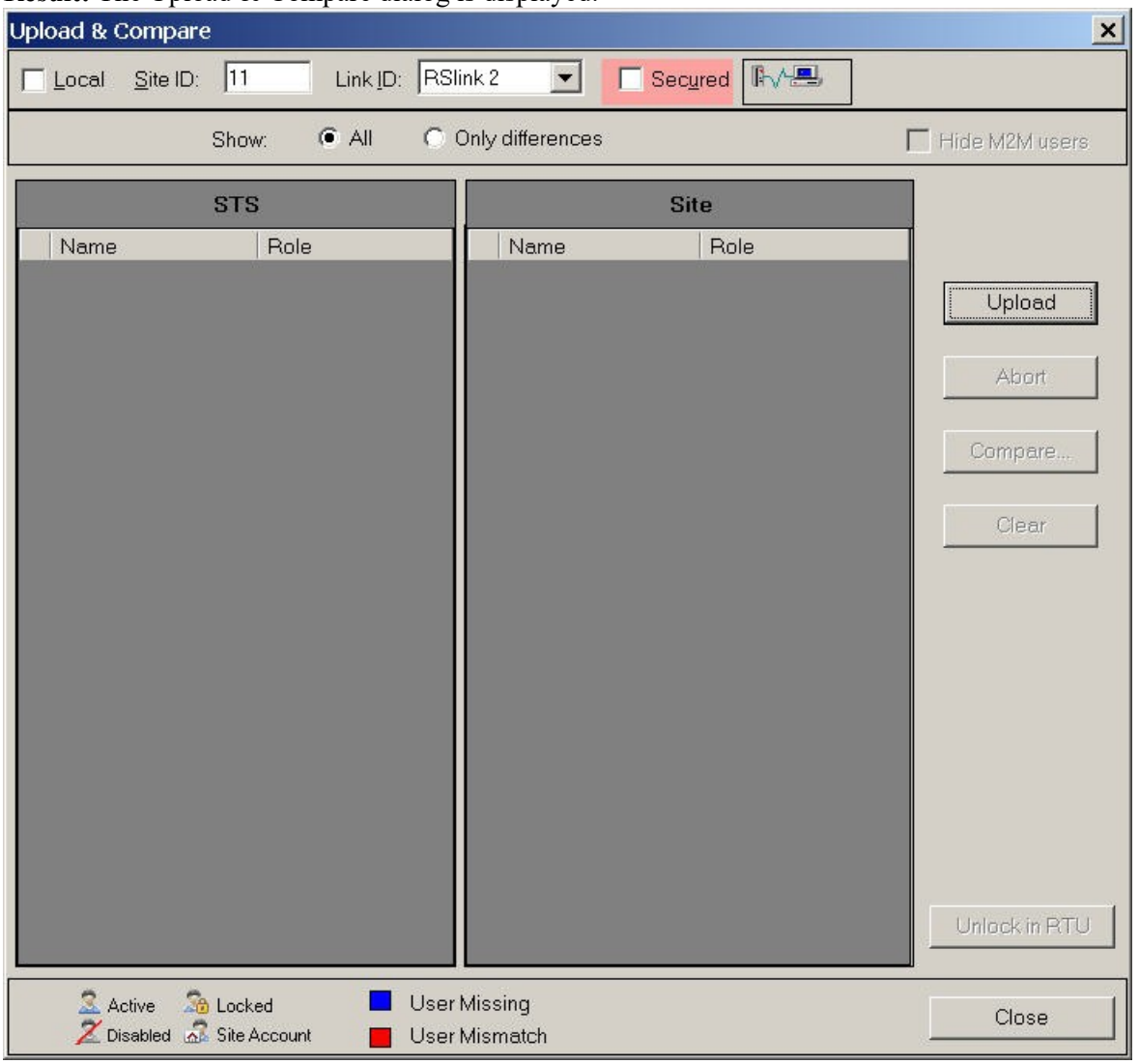
5. To sort the contents of the log by a key field, click on the desired column. Click once to sort in ascending order. Click again to sort in descending order.

Uploading and Comparing Users

Procedure 6-1-20 describes how to upload user data from a site (authentication server or local ACE3600 RTU) and compare it to user information in the STS. This function is useful before downloading the users file to a site.

Procedure 6-1-20 How to Upload and Compare Users

1. From the Users menu in the Users dialog, or from the Site menu, click on the Upload & Compare command from the Users menu.
   Result: The Upload & Compare dialog is displayed.



2. In the Connection bar, specify the connection. See Starting Secured MDLC Communication with the RTU.

3. Click on Upload. To abort the operation, click on Abort.
   Result: The list of users/roles from the STS appears in the left pane. The list of the users/roles from the site appears in the right pane. Users which exist in either the STS or the site (but not both) are marked in blue. Users which exist in both but have different properties are marked in red.

4. To compare details of a specific user, select the user and click Compare.
   Result: For the selected user, the credentials, role, status, and password validity values in both the STS and RTU are displayed.

5. To show all users, in the Show box, select All. To show only users with differences, select Only differences.

6. To hide M2M users, check Hide M2M Users.
   Result: Only human users are displayed.

7. To view the full information for the user, double-click on the desired username.
   Result: The user information is displayed.
   Note: This user information can vary based on user type and site type. For example, password expiration start/end dates are compared for human users but not for M2M users. Or when a nonauthentication server site is compared to the STS, the list of allowed sites to which the user has access via the authentication server is not relevant and therefore not compared.

8. To unlock a locked user in this RTU (i.e. after a number of communication attempts with invalid credentials,) click on the locked user, and then on the Unlock in RTU button.
   Note: This button is only enabled if there is a user who is locked in this RTU.
   Result: The selected user is unlocked in the RTU.

9. To close, click Close.

Viewing all Users Authorized to Work with a Specific Site

Procedure 6-1-21 describes how to view all users authorized to work with a specific secured site.

Procedure 6-1-21 How to View Users in a Secured Site

1. To view the users who are authorized to work with a specific secured site, select Show All Users from the Site menu.
   Result: The list of users with access permission, with their roles, Local status, Authentication server status and password expiration is displayed.

2. To close the dialog, click OK.

Enabling/Disabling a User

Procedure 6-1-22 describes how to enable/disable a user in a project.

Procedure 6-1-22 How to Enable/Disable a User in a Secured Project

1. Select Users from the Security menu.
   Result: The Users dialog is displayed.

2. Select the user to be changed and click on the Edit button.
   Result: The User Details dialog is displayed.

3. To enable the user, check the Enabled field. To disable the user, uncheck the Enabled field.

4. Click OK to close the User Details dialog.

5. Click Close to close the Users dialog.

6. Download the users file to the authentication server for the change to take effect. See Downloading Security Files and Information.
   Result: A disabled user will be unable to communicate with a secured RTU or open a secured project.

Locking/Unlocking the Project

If you need to walk away from the STS during a session, lock the project to prevent unauthorized access. The project also locks automatically after a defined period of inactivity (as defined in the security policy in the 'Number of minutes before project lock' parameter) or after a defined number of invalid user login attempts (as defined in the security policy in the 'Number of wrong-user-name failed login attempts before project lockout' parameter). Unlock the project using valid credentials.

Procedure 6-1-23 describes how to lock and unlock the project.

Procedure 6-1-23 How to Lock and Unlock the Project

1. To lock the project, select the Lock Project command from the Security menu.
   Result: The Secured Project Locked dialog is displayed.

2. To close the STS session, click Close. Note: The Close button is disabled if the project was modified and was not saved yet.
   To go back into the STS session, click Login.

Enter a valid User name and Password and click OK.

3. To unlock a project which was manually or automatically locked, enter valid credentials and click OK.

Unlocking a User

A nonadministrator human user can be locked out of the STS if a number of unsuccessful login attempts are made by the user (as defined in the security policy in the 'Number of incorrect password login attempts before user lockout' parameter. The user can be unlocked by an administrator. Procedure 6-1-24 describes how to unlock a locked user. Note: The user is locked out for a predefined period (as defined in the security policy in the 'Lock period after user authentication failure' parameter) and is automatically unlocked when this period elapses.

Procedure 6-1-24 How to Unlock a Locked User

1. Select Users from the Security menu.
   Result: The Users dialog is displayed.

2. Select the locked user and click on the Unlock button.
   Result: The user is unlocked in the STS.

Note: The administrator can unlock a user who is locked out of an RTU using the Upload and Compare utility. For more information, see *Uploading and Comparing Users*.

Retrieving Security Log Information from a Secured Site

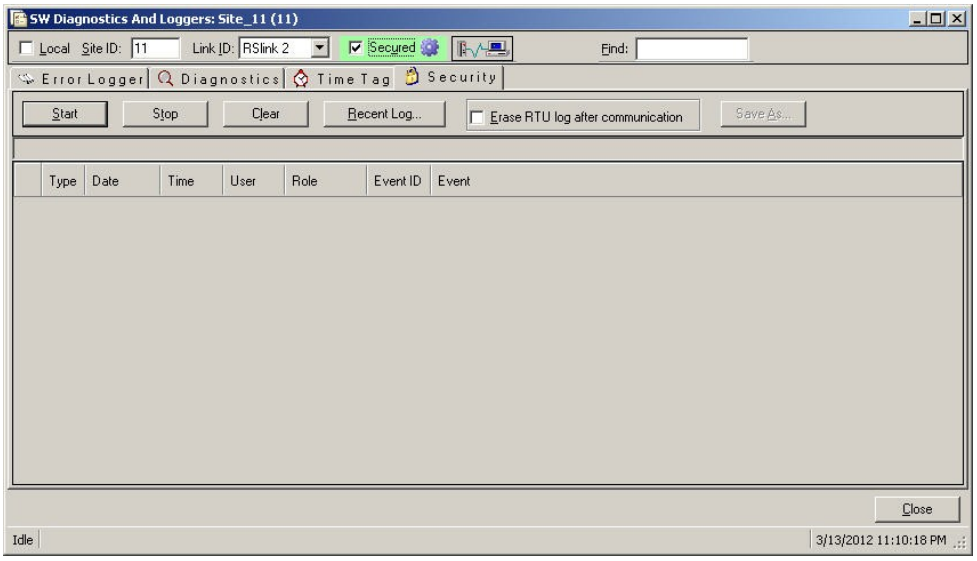
A record of access activity and other security events which occur in the RTU are recorded in the unit's security log. Events are logged with essential data such as user name, role, time and date, description and event severity. For more information on the security log, see the *Security Log* section of the *MC-IoT Security Concept* chapter.

Procedure 6-1-25 describes how to retrieve security log information from the RTU.

Procedure 6-1-25 How to Retrieve Security Log Information from the RTU

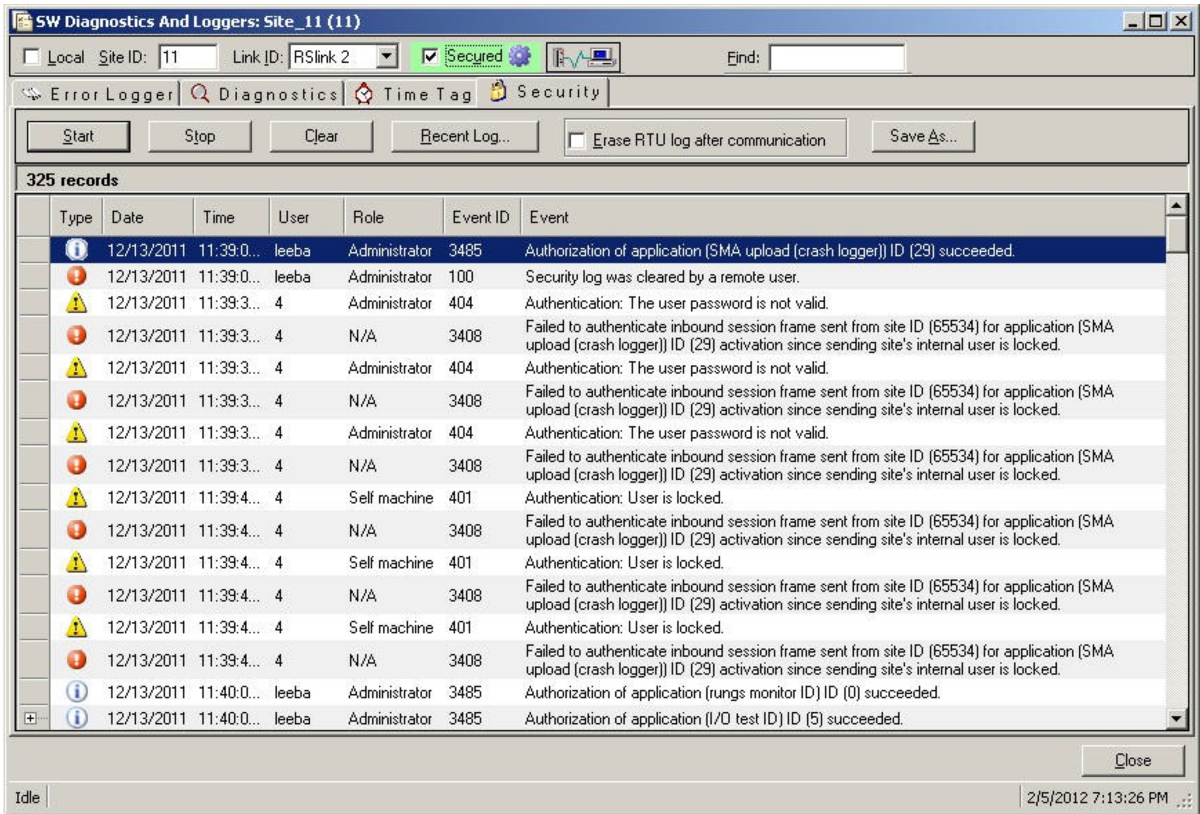
1. To retrieve/view security logger information from the system view, click on a site from the Diagram/Table view and select Logger from the Site menu, or from the site view, click on the Logger icon.
   Result: The Loggers window appears.

2. Click on the Security tab.
   Result: The Security logger appears. (For users without permission to retrieve security log information, the Security tab is not displayed.)



3. In the Connection bar, specify the connection. For details, see Starting Secured MDLC Communication with the RTU. The administrator can retrieve security log events locally or remotely.

4. To use the Start, Stop, Clear, Recent Log, Erase RTU log after communication, Find and Close features, follow the instructions for the Error Logger in the *Operation* chapter of the *MC-IoT STS User Guide*.
   See Table 1-5 for a list of the event fields.



5. To save the contents of the security logger to a .csv file, click on Save As.
   Result: The Save As dialog is displayed.
   Enter a file name.
   Browse to the desired location to store the project (the default is C:\STS<version>\Projects\), select the location and click Save.

6. The contents of the security log's high severity events can be retrieved to the RTU database Reserved Values table, using the GetSecLog function. For more information, see *Appendix D: Security Information in Database Tables*.

Table 1-5 Security Log Event Fields

Field	**Description**
Type	Can be one of: • 1 (information) • 3 (moderate) • 5 (high) • 7 (critical)
Date	The date on which the security event occurred.
Time	The time at which the security event occurred.

Field	Description
User	The name of the user recognized in the system by the STS and the RTUs. Can be the current human user (e.g. Michael), an M2M user (e.g. _M2M_3), or System. In a system without user authentication, N/A is displayed. Note: If there is a discrepancy between the users file in the STS and in the RTU, the user is displayed as a numeric value or with the wrong name.
Role	Can be one of: Administrator, Technician, User (default), or Viewer. See *Defining the User Roles and Permissions*. Note: If there is a discrepancy between the users file in the STS and in the RTU, the role is displayed as a numeric value.
Event ID	Unique ID representing the event.
Event	The description of the event that occurred (e.g. New keys file was downloaded.)

Retrieving the Field View from a Secured Site

The Field View can be used to view the names of files in the flash of a secured unit, when checking for whitelisted files, which were marked as suspicious and set aside.

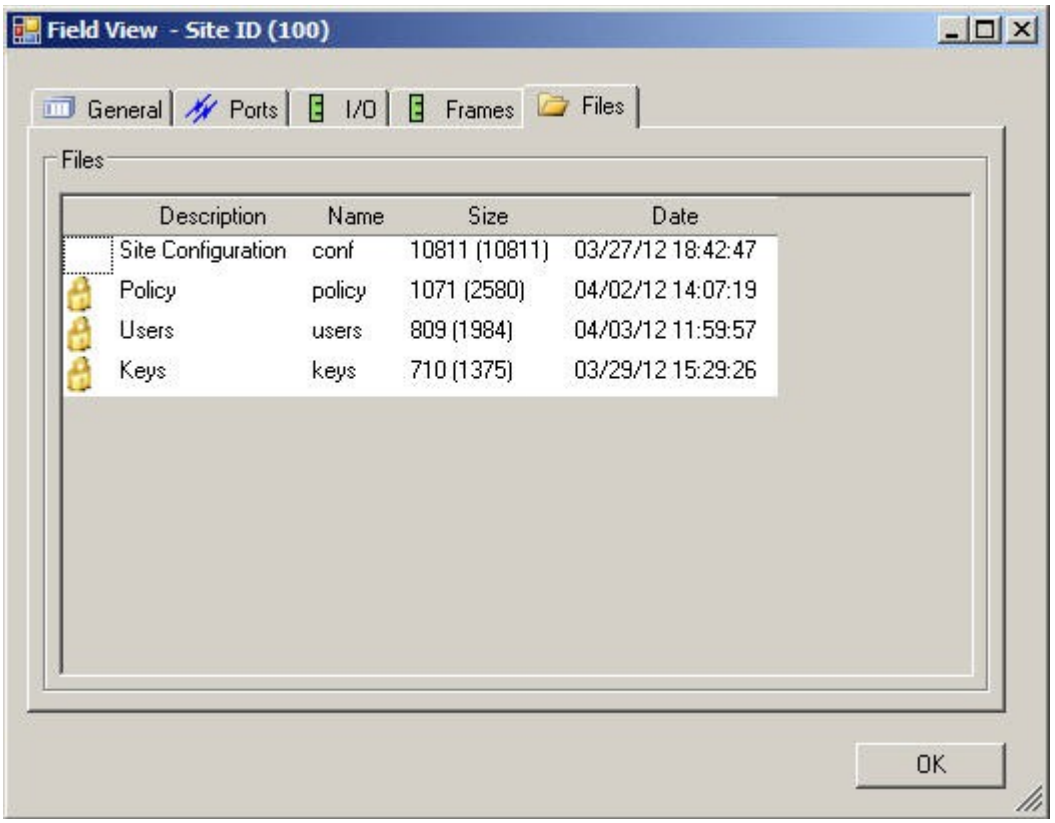
The Unit Type field includes an indication whether the CPU is security-enabled or not.

The Firmware Version field includes an indication whether the firmware is secured or not (with or without SSL.)

The Security field indicates whether the RTU is secured according to the policy (i.e. that all required files were downloaded.)

In the Files tab, RTU files that are encrypted are marked with a lock icon  .

The value in the Size column represents the compressed size of the file, with the uncompressed size added in parenthesis.



Performing Hardware Tests in a Secured System

When performing the CPU test on a site with firmware ≥ V16.00, the Security Enabled parameter will reflect whether security is enabled or disabled in the unit. When performing the CPU test on a site with firmware < V16.00, the Security Enabled parameter is not displayed.

For more information on performing Hardware Tests, see the *MC-IoT STS User Guide*.

Changing the Site ID of a Secured Unit

Changing an RTU's site ID in a secured system is the same as in a nonsecured system. If, however, the security policy is configured for unique M2M credentials, the RTU has its own user name and password. Changing the site ID in the STS, affects these credentials. Procedure 6-1-26 describes how to change the site ID of a secured RTU.

Procedure 6-1-26 How to Change the Site ID of a Secured RTU

1. Change the RTU's site ID in the site view. For more information on changing the site ID, see *Customizing the Configuration of a Site* in the *MC-IoT STS User Guide*.
2. Save the site configuration.
3. Download the site configuration to the RTU. For more information on changing the site ID, see *Downloading to a Site* in the *MC-IoT STS User Guide*.

4. Download the updated users file. For more information on downloading, see *Downloading Security Files and Information*.

5. In a system without authentication servers, download the updated users file to all sites that have this site in their local site access list.

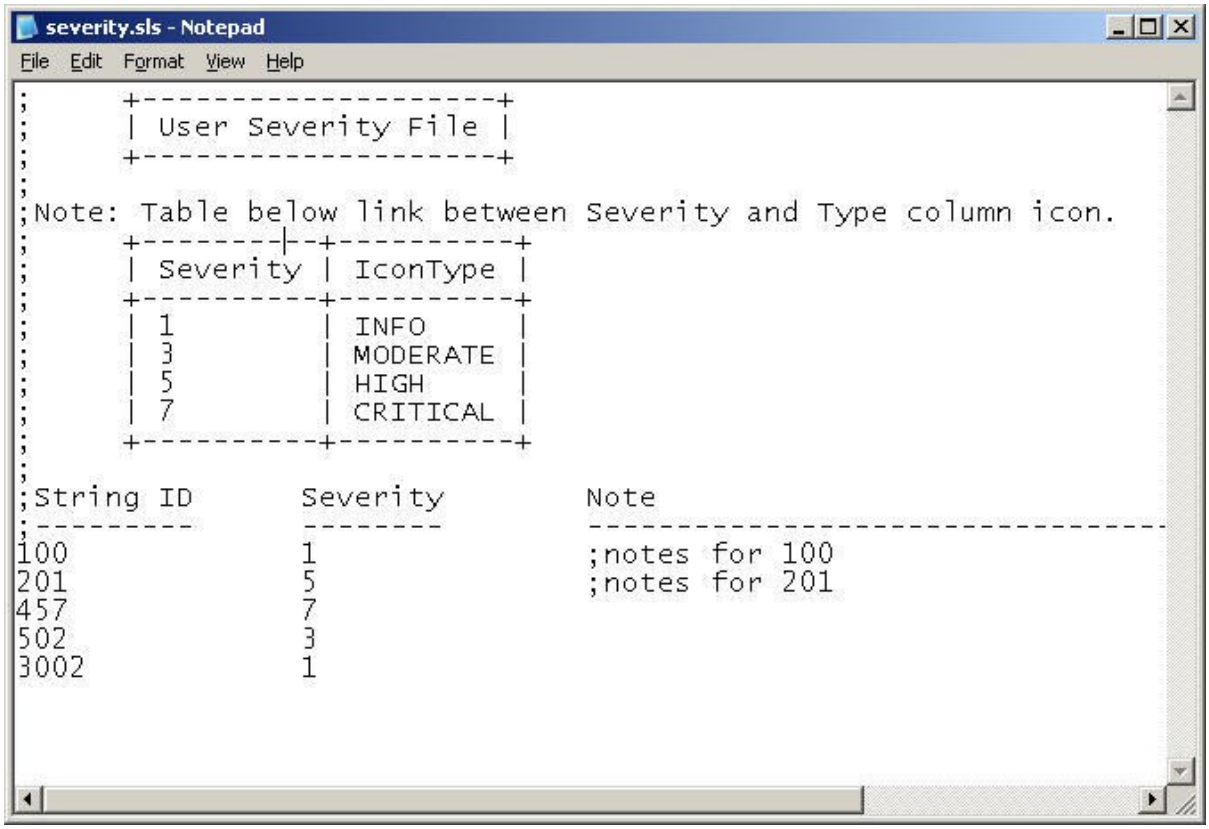
6. In a system which includes an authentication server, the updated users file is downloaded to the authentication server only.

Changing the Severity of Security Events

The severity of security events is hardcoded in the system. If you need to change Procedure 6-1-28 describes how to change the severity of security events in a system.

Procedure 6-1-27 How to Change the Severity of Security Events in a System

1. Using a text editor such as Notepad, create a secure logger severity text file, mapping the String ID of the security events (as defined in C:\STS<version>\Prg\securlog.txt) to a new severity type (1, 3, 5, or 7.)
   Note: It is recommended to document the change with notes in the Note column.



2. Save the file with the .sls extension in C:\STS<version>\config (e.g. severity.sls.)

3. Using the STS Add-On Manager, attach the secure logger severity file to the desired sites. See *Managing Add-On Files* in the *MC-IoT STS User Guide*.

4. Download the secure logger severity (.sls) file to the RTUs.

5. To validate the changes, use the Software Diagnostics (SECLOG device level 2) to retrieve the severity of the security event types from the RTU.

Backing Up the System

Procedure 6-1-28 describes how to back up a system.

Procedure 6-1-28 How to Back Up a System

1. Copy the entire project directory from the STS PC [C:\]STS<version>\Projects.

2. Paste the project directory into another area on the same PC/external media. If desired, copy to another PC.

Note: When running a backed up project, the PC must use the same master password as the password that was defined on the original PC where the project was created.

Backing Up the Encryption Keys

Procedure 6-1-29 describes how to back up the encryption keys for a system.

Procedure 6-1-29 How to Back Up the Encryption Keys for a System

1. In the security policy, allow the encryption keys to be viewed as plain text (Policy -> MDLC payload encryption).

2. Uncheck Hide Keys Values in the Keys dialog.

3. Select all keys and copy them to a text or Excel file as a backup.

Monitoring the Communication Channels in a Secured System

The STS Protocol Analyzer program monitors the data transmitted in the communication channels and enables the user to analyze and view the data.

In a secured system, monitored data is encrypted and must be decrypted using the same key that was active when the data was collected. The key can be copied from the Keys dialog. For this reason, the policy must allow keys to be displayed in plain text.

For more information, see the *Protocol Analyzer* section of the *MC-IoT STS Advanced Features* manual.

IMPORTANT: Protocol analyzer output is written to an output file. When analyzing encrypted communication and providing the key for decryption, the decrypted data is stored in that file. Make sure to erase that file after inspecting its contents or restrict user access to the output folder.

USER APPLICATION PROGRAMMING FOR A SECURED SYSTEM

ACE3600 Ladder Application

For details on creating a ladder user application, see the *Application Programmer* chapter of the *MC-IoT STS User Guide*.

In a secured system, the user application can retrieve the contents of the security log's high severity events to the RTU database Reserved Values table, by calling the GetSecLog function. Based on these values, the user application can take appropriate action (e.g. send an alert to the SCADA GUI in the control center.) For more information, see the *Security Log* section of the *MC-IoT Security Concept* chapter and *Appendix D: Security Information in Database Tables*.

Note: A ladder application which is part of a secured project cannot be opened in a standalone Application Programmer.

'C' Application

For details on creating a 'C' application, see the *'C' Toolkit for ACE3600 RTUs User Guide*.

Before running the 'C' application in the unit, make sure that 'C' applications are enabled in the unit. (The 'Disable C applications in RTU' advanced Firewall parameter must be set to No, and the site configuration must be downloaded.) If a 'C' application is downloaded to a unit in which 'C' applications are disabled, a message is sent to the security log. If the site configuration which disables 'C' applications is downloaded a unit which already has a 'C' application, a message is sent to the security log and to the Error Logger.

Before debugging a 'C' application, enable 'C' toolkit debugging in the RTU (set the 'Allow C toolkit debugging' advanced Firewall parameter to Yes) and temporarily disable the firewall in the site configuration (set the 'Activate Firewall' advanced Firewall parameter to Disable.)

Note: When 'C' toolkit debugging is enabled in the RTU, a high severity message is sent to the security log. When the firewall is disabled, a high severity message is sent to the security log.

MIGRATING AN ACE3600 SYSTEM TO SECURITY

Migration Approach

System migration to security should not impair the current system functionality. Therefore a migration approach is required which suits your system architecture.

Unless the entire system can be migrated at once (unlikely for a large system that is already deployed), divide the system into two, one secured and one nonsecured. Each system requires its own ACE IP Gateway or FIU.

For a star shaped network, each time you secure a unit, connect it to the ACE IP Gateway/FIU of the secured system.

For a peer-to-peer network, identify clusters. Move each cluster from nonsecured to secured and deploy it.

Note: A nonsecured site can route secured frames, and secured sites can route nonsecured frames. That means a node of each type can serve both types of communication.

IMPORTANT: The connection between the ACE IP Gateway and the SCADA is considered a Customer Private Backbone, and from a communication point of view (IP) is nonsecured. It is the customer's responsibility to secure this segment.

Download Order

IMPORTANT: In a deployed system, download of security related information to units must be done in the right order to ensure that continued communication between the STS and the unit.

1. Download the security files to the active authentication server.
2. Start securing units, beginning with the leaves of the hierarchy.
3. Climb up the hierarchy to the nodes, so as not to lose communication with the leaves.

Upgrading Legacy Projects

When a legacy project is to be upgraded to STS ≥ V16.50, an MDLC legacy password must be defined. This password is used by the MDLC communication driver in nonsecured communication.

IMPORTANT: If you plan to communicate from the STS using the same MDLC driver with multiple projects, including secured and nonsecured projects, these projects must all share the same legacy MDLC password.

Migrating a Site

Before migrating a site from a legacy system, make sure that the RTU itself is security enabled (i.e. it must include a security signature from the factory.)

Then make sure that the unit's firmware supports security and that the configuration version is correct, i.e. greater than the firmware version:

To prepare a unit for migration:

1. In the STS, create a site with firmware ≥ V16.00.
2. If you are working in a secured project, unsecure the site (Site->Unsecure).
3. Download the nonsecured firmware to the RTU.
4. After a successful download, secure the site in the STS and download secured firmware to the RTU. See the *Securing a Site* section of the Operation chapter.

Migrating Tips

Before securing a site, make sure that the RTU time is set and that the time zone is configured correctly.

Other useful tips for migrating a system can be found in the *Guidelines for Securing a System* chapter.

Time Synchronization in Mixed Systems

In a secured MC-IoT project, the user can synchronize secured ACE3600/MC-EDGE RTUs, unsecured ACE3600/ACE1000/MC-EDGE RTUs and MOSCAD RTUs. Secured synchronization appends security information to the synchronization request.

Note: Secured MDLC time synchronization requests are sent in 'Legacy sync' time sync method by default. This can be changed in the site configuration to 'Extended sync', if desired.

During migration, when part of the system is secured and part is nonsecured, time synchronization is subject to the following constraints:

- All time synchronization commands must be sent from a secured STS project or from a secured RTU.
- In a mixed system, a secured FIU can synchronize secured and nonsecured RTUs

which are directly connected to it, and secured RTUs which are connected via other secured RTUs.

- All nodes connected to secured RTUs must be secured in order to fully distribute time synchronization commands. (Time synchronization commands forwarded by nonsecured nodes will be rejected by secured sites.)

Note: A mixed system (during migration) cannot be synchronized using an STS version < 16.50 or using MOSCAD Programming ToolBox. Nor can it be synchronized from a nonsecured STS project.

The table below depicts the behavior of RTUs (either secured, nonsecured or with firmware version < V16.00) receiving a time synchronization message in a mixed system. A secured RTU in this context is one where both MDLC payload encryption and user authentication is enabled.

	Nonsecured RTU (or RTU with FW <V16.00) Receives Time Sync	**Secured RTU Receives Time Sync**
Nonsecured RTU (or RTU with FW <V16.00) Initiates Time Sync	Accepts nonsecured time synchronization*.	Rejects nonsecured time synchronization.
Secured RTU/Secured STS Project Initiates Time Sync	Accepts nonsecured time synchronization*.	Accepts secured time synchronization, if security information is successfully validated. (Any transmitting/forwarding nodes must be secured.)

* Time synchronization acceptance is based on the behavior defined in the site configuration. (Advanced ->Time Sync.) For more information, see Time Adjustment and Synchronization in the MC-IoT STS Advanced Features manual and the Time Sync advanced parameters in Appendix A: Site Configuration Parameters in the *MC-IoT STS User Guide*.

Note: Communication via NTP protocol is not secured.

MDLC Encryption Upgrade

To upgrade a distributed system which currently uses the TEA encryption algorithm to the AES encryption algorithm, follow the steps below.

1. Set the MDLC encryption algorithm in the policy to TEA and set the corresponding keys to match those of the MDLC Encryption tool. Make sure that the secured RTUs work with TEA under the secured project and that all RTUs can communicate.
2. Set the MDLC encryption algorithm in the policy to AES.
3. Define new keys.

4. Extend the expiration date on the current active key by a few hours to enable all RTUs to be updated.

5. Download the new policy to the units.

6. Download the new keys file.
   Result: When the current key expires in the unit, all units will transition to AES automatically.

IMPORTANT: For purposes of migration, the TEA algorithm is supported in firmware version 16.00 and STS 16.50.

Expansion CPU Upgrade

When upgrading an ACE3600 system with expansion to security, upgraded expansion CPUs that support security must also be ordered.

Broadcasts during Migration

When using a mixed system (while gradually moving from unsecured to secured), broadcasts will be received by either the secured or the unsecured parts of the networks but not by both. The nonsecured elements cannot receive the secured broadcast and vice versa. Such broadcasts may be listed in the secured sites' security logs as nonencrypted/ nonauthenticated frames.

Firmware Patches during Migration

As of firmware version 16.00, RTU firmware is by default locked to prevent tampering and patches will not load. If you need to run a patch to an RTU, you must disable this feature in the site configuration before upgrading to firmware version 16.00. Failing to do so will cause endless restarts in RTUs after firmware upgrade.

For information on the 'Lock firmware code' advanced IP Firewall configuration parameter, see *Appendix A: Site Configuration Parameters* in the *MC-IoT STS User Guide*.

TROUBLESHOOTING

Communication Issues when Working with a Secured System

If your system is experiencing symptoms such as excessive communication delays and retries, check the following to pinpoint and correct the problem:

- Read the Error Logger to look for events which indicate communication problems.
- Read the Security Log to look for high severity security events. Identify if these relate to authentication or encryption or general communication.
- Check the MFFS SW Diagnostic device (level 0) to make sure that all files were downloaded.
- Check the USRROM SW Diagnostic device (level 100) in the RTUs. Verify that the RTUs have the correct security signature (Security Signature = 1) and firmware (Security Firmware = 1).
- Check the SECMNGR SW Diagnostic device (level 0) in the RTU. Verify that the security features are all enabled (=1).
- Check the SECPOL SW Diagnostic device (level 1) to be sure that the policy in the RTU is the same as the policy in the STS.
- In case of communication failure when NTP is enabled, check the NTP Diagnostic device (level 3) to verify that the RTUs have the correct timezone.
- In case of communication failure between the STS and an RTU, check the C:\STS2250\scratch\mdlcerr.log, if the 'Send an Ack when receiving incompatible MDLC encryption status' parameter is enabled in the policy (STS->Security->Policy->MDLC Payload Encryption).

Tips for Problems in Authentication

Try the following tips if there is no communication with the authentication server, or if the user has no access to the RTU, or if communication is erratic (sometimes working and sometimes not working).

- Make sure that the user has access to the RTU (STS->Security->Users).
- Check if the user's site access is via the authentication server (STS->Security->Users->Site Access).
- Check the ASCLI SW Diagnostic device in the RTU (STS->Logger->Diagnostics) to see if the RTU is sending authentication requests and receiving responses from

the authentication server.

Level 10/11	No of Originate TX Number of authentication requests sent to the authentication server from the RTU.
	No of Answers Receive Number of answers received from the authentication server. The answer can be Approved/Not approved.
	No of received frames as Setcall Number of times the authentication server sent a Setcall to all clients to remove their authentication caches, because a new users file was downloaded to the authentication server.

- Check the ASSER SW Diagnostic device in the authentication server to see if the authentication server is receiving authentication requests and sending responses.

Level 10/11	No of Originate Receive Number of authentication requests received by the authentication server from RTUs.
	No of TX Answers Number of authentication answers (Approved/Not approved) transmitted to the RTU by the authentication server.
	No of Setcall TX This number is incremented after the users file is downloaded to the authentication server. After the download, the authentication server sends a Setcall to all RTUs to delete their caches.

- Check the AUTHSRV SW Diagnostic device in the RTU. Verify that the authentication server is connected to the RTU and that there are users/permissions in the RTU's cache.

Level 0	Users in the cache
Level 1	Permissions in the cache
Level 2	Status of the authentication server
Level 10/11	Statistics

- Check the AUTCORE SW Diagnostic device in the RTU. In the RTU, verify that the users file was downloaded correctly and that the users file is correct in the RTU. Verify that the users file is correct in the authentication server. Check which users were granted/denied access to the RTU.

Level 0	User access information
Level 1	Information from the users file

- Check the NSTOCK SW Diagnostic device (levels 1 and 2) in the RTU. Verify that the RTU has the network connection to reach the authentication server, i.e. the RTU and all forwarding RTUs have links to reach the authentication server and. Also check all link retries.
- Check the IPCNTBL SW Diagnostic device (level 3) in the RTU to see that the RTU has the authentication server's IP address.
- If the problems occur only in a heavily loaded system, try to increase the security policy parameter 'Time to wait for authentication server respond'.

Tips for Problems in Encryption

Try the following tips if encrypted frames are being rejected.

- Check the SECKEYS SW Diagnostic device (level 0) to check the key index and whether the last key has expired.
  Check the SECKEYS SW Diagnostic device (level 1) to check the key expiration date.

Level 0	Key type Key type 0 is the MDLC payload encryption key.
	Num of keys The number of keys in the file.
	Key num The current key index.
	Last key expired Whether the last key expired or not (Y/N).
Level 1	Expiration Date The date that the key expires.

For more detailed information on software diagnostics, see the *MC-IoT STS Software Diagnostic Output and Error Messages* manual.

APPENDIX A: SECURITY POLICY PARAMETERS

The MC-IoT security policy is configured for the system, not individually for each site. A number of parameters and settings are used when configuring the secured MC-IoT policy. The parameters are organized in the following groups:

- Audit
- User Authentication
- Password Rules
- MDLC Payload Encryption
- File Encryption
- Security Log
- Whitelisting
- Message Life Time
- Security Files Signature Hardening

Each policy parameter is related to the STS, to the RTU, or to both, as indicated by the icon to the left of the parameter (

).

The color of the security policy parameters indicates their status. The color of the circle next to each parameter group (category) reflects change status (white=Default group, red triangle=Modified group). Parameters are white for the default value, and green for a value other than the default, and red for a value that is out of range. If you set a parameter to a value that is out of range, a warning message with the recommended range is displayed.

For certain parameters, the range <minimum-maximum> and [default]: values are listed. The default value provided is one of the possible values.

To the left of each parameter is a help icon  . For a tooltip explanation of the parameter, point with the mouse at this icon.

Policy Parameters

Audit

Enable RTU audit (self test) <Yes/No> [Yes]:
Whether to allow the RTU to run self tests on various security related modules.

Output audit log records to [Both]:

The target output file for audit log messages (security-related events at the STS level.) Can be one of:

Event log (Windows)

STS log

Both

Maximum number of records in audit log <1,000-100,000,000> [100,000]:

The maximum number of records in the STS audit log.

User Authentication

Number of minutes before project lock <1-9,999> [10]

The project is locked if inactive for this period. A user password must be entered to open the project.

Number of incorrect password login attempts before user lockout <1-10> [3]

The number of login attempts with the wrong password, after which a human and unique M2M user is locked out of the STS and the RTU. Lockout from the RTU can occur if the user uses the wrong password in the Override password option of the Secured Communication Settings, or if the user's password is changed in the STS but was not downloaded to the RTU yet.

Note: Changed passwords should be downloaded (in the users file) to the relevant RTUs and then to the authentication server as soon as possible. See *Users File in the Field Units* in the *MC-IoT Security Concept* chapter.

Lock period after user authentication failure <1-1,440> (minutes) [15]

The number of minutes to wait before unlocking a known non-administrator user who was locked out of the STS and RTU due to a number of failed login attempts.

Number of wrong-user-name login attempts before project lockout <1-10> [4]

The number login attempts with an invalid user name, after which the STS project is locked.

Lock period after wrong-user-name authentication failure <1-1,440> (minutes) [15]

Once a project has been locked due to repeated login attempts with an invalid user name, it will be unlocked automatically after this number of minutes. Only an administrator can login during this period.

New MDLC user authentication [On]:

Enable MDLC authentication of users. Each user is defined in a users file which is downloaded to an authentication server, to RTUs or to both. Until this file is downloaded, authentication is not activated in the RTU, but the STS uses the credentials in MDLC communication. If no authentication server exists, all the user information is downloaded to a local file in each RTU. If an authentication server exists, each local file will contain at least the user/password of the site itself and of the authentication server.

Note: If user authentication is set to off, the rest of the parameters in this group are disabled.

M2M credentials configuration [Common]:

Whether all M2M communication (RTU to RTU) should use the same user and password (Common) or different users and passwords for each RTU(Unique). If Common, communication efficiency is increased. If Unique, the RTU must authenticate each M2M user individually.

Maximum number of authentication servers [8]

The maximum number of authentication servers that can be configured in the project. If this parameter is set to 0, the Authentication Servers tab in the Users dialog will not appear. The value of this parameter determines how many servers can be added in the Users dialog.

First source for user authentication <Server/Local> [Server]

Where the RTU should go first to authenticate users, either to the authentication server (default) or to the local users file in the RTU. If Server, the RTU will first check its local cache to see if this user was recently authenticated, then it will check the authentication server. If Local, the RTU will first check its local users file. For more information, see the *User Authentication* section of the *MC-IoT Security Concept* chapter.

Number of retries to declare user authentication server unreachable <0-10>

Time to wait for authentication server response <1-10> (seconds)

Period to reestablish communication with unreached authentication server in minutes (0:Disabled), <0-60> (minutes)

Number of retries to declare user authentication server unreachable <1-10> [3]

After this number of failures to communicate with the current authentication server, the RTU will mark it as “failed’ and will target the secondary server (if one is defined). If no secondary server is defined or the secondary server is also ‘failed’, the RTU will try to authenticate using its local file.

Time to wait for authentication server response <1-10> (seconds) [3]

The number of seconds to wait for communication between the RTU and the authentication server to succeed. Make sure that the value is sufficient for the authentication communication to get to the authentication server and back, taking into account the distance from the farthest node to the server, and all link retries. The value must also take into account media channel access delays and speed. If value is too low, the requesting RTU might give up waiting for the authentication response, even though it was actually granted by the server. If the timeout expires, a request retry is sent.

Period to reestablish communication with unreached authentication server <1-60> (minutes) [10]

The number of minutes to wait before retrying communication with a failed authentication server.

Size of queue in receiving RTU awaiting response from authentication server <1-1000> [50]

The number of authentication requests waiting for authentication server response in Minisession type communication.

Send broadcast after users file changed in authentication server [Yes]

If the users file is changed in the authentication server, a broadcast is sent to all RTUs in the system, signaling them to erase the user records in their cache. During the next communication request, the RTUs will authenticate with the server and store the updated information in the cache.

Note: If this parameter is set to No, reduce the Period to keep user records in RTU cache, in order to reduce the time that the cache contains outdated information when changing the users file.

Period to keep user records in RTU cache <10-69,120> (seconds) [180]

The number of seconds to store user authentication records (retrieved from the authentication server) in the RTU cache. Using the cache increases communication efficiency. The user record includes user, password, role, and permissions.

Maximum number of user records to store in RTU cache <0-1,000> [20]

The maximum number of user records in the cache. Once this number of records has been filled, the information of the next authenticated user will overwrite the oldest user record in the cache.

Maximum number of permission records to store in RTU cache <0-100> [10]

The initial size of the RTU's permission cache (in records). Each record includes a set of permissions per role. Once this number of records has been filled, an additional record is added to the cache when a user with a new role attempts to communicate with the RTU.

Password length for Minisession communication. <2-32> (bytes) [16]

Length of password hash (included in each frame) used for Minisession communication. It is recommended to reduce the hash length to 8 for better channel bandwidth.

Password length for Session communication <2-32> (bytes) [16]

Length of password hash (included in each frame) used for Session communication. It is recommended to reduce the hash length to 8 for better channel bandwidth.

Password length for Frame-Sequence communication <2-32> (bytes) [16]

Length of password hash (included in each frame) used for Frame Sequence communication. It is recommended to reduce the hash length to 8 for better channel bandwidth.

Password length for Time Synchronization communication (2-32 bytes) [16]

Length of password hash (included in each frame) used for Time Synchronization messages. It is recommended to reduce the hash length to 8 for better channel bandwidth.

Enable Selection of Authentication Servers per site <Yes>

Selecting Yes enables to link an authentication server(s) to a site.

Password Rules

Minimum password length <6-30> [6]

The minimum number of characters in a password. For valid password requirements, see *Creating a Project* in the *Operation* chapter above.

Maximum password age <60-65,535> (hours) [2,160]

The maximum valid duration of user passwords. After this number of hours, the password must be changed.

Number of old passwords in history list <1-10> [3]

The number of previous user passwords that cannot be reused.

Password pre expiration alert (days) (0:Never) <0-30> (days) [14]

The number of days before password expiration that an expiration alert should be sent. The expiration alert is sent to the security log, and is also displayed when this user or an administrator logs in to the STS.

MDLC Payload Encryption

MDLC payload encryption <On/Off> [On]

Use enhanced MDLC payload communication encryption instead of legacy MDLC encryption. Note: If this parameter is set to Off, the other parameters in this group are disabled, and the Keys command in the Security menu is disabled. If this parameter is set to On, MDLC encryption is only activated once the keys file is created (based on the selected algorithm), and downloaded to the RTUs and all policy requirements are met.

Type of MDLC encryption algorithm <AES/TEA> [AES]

The type of algorithm used for MDLC encryption.
Can be either AES (enhanced) or TEA (legacy). Changing this value deletes all existing encryption keys except the active one.

Minimum number of MDLC encryption keys <1-50> [1]

The minimum number of keys required in the MDLC encryption keys file.

Maximum number of MDLC encryption keys <1-52> [12]

The maximum number of keys that can be defined in the MDLC encryption keys file. This parameter ensures that the system administrator define new encryption keys periodically. When Create All Keys is performed, this number of keys is created automatically by the STS. See *Setting the Encryption Keys* in the *Operation* chapter.

Maximum MDLC key duration <24-1,080> (hours) [720]

The maximum active time in hours for a single MDLC encryption key. This period is also used as the default key duration when creating keys. It is recommended to change encryption keys at least once a month.

Send an Ack when receiving incompatible MDLC encryption status [No]

Whether the receiving RTU should send a reply message to the transmitting RTU when it fails to decrypt the received frame.

Note: If this parameter is set to Yes, the RTU sends an ack for incompatible communication, and the STS displays a message regarding an encryption/decryption problem. If this parameter is set to No, the RTU does not send an ack, and the STS will keep trying until retries are exhausted. There will be no indication that the problem was related to incompatible encryption.

Allow keys to be displayed in plain text <Yes/No> [Yes]

Whether the encryption keys in the Keys dialog can be viewed as plain text.

File Encryption

Encrypt files in RTU FLASH <On/Off> [On]

Whether downloaded files (keys, users, site configuration, application, etc.) should be encrypted in the RTU.

Security Log

Maximum number of records in the security log <200-100,000> [1,000]

Maximum number of events in the RTU security log.
Note: In the ACE3640, this value may not be set to more than 20,000 records, due to flash size which limits the maximum log file size.
Note: MC-EDGE supports only 10000 log records.

High severity threshold level <1, 3, 5, 7> [5]

The value to trigger the application severity flag, values are 1, 3, 5, 7. When a security message arrives with this level or higher, the SecureLogSeverity flag is set in the RTU database Reserved Flags table.

Use event filtering <On/Off> [On]

Enables filtering of security events which repeat themselves consecutively in the RTU.

Start filtering identical events after N occurrences <1-100> [3]

Start filtering events in the RTU after the same event occurs N times.

Identical event filtering timeout <60-2,592,000> [180]

Stop filtering after N seconds from the last identical message.

Support verbose logging <Yes/No> [No]

To reduce the number of messages logged, tracer type messages can be suppressed by setting this parameter to No.

Whitelisting

Use RTU programs whitelisting <On/Off> [On]

Enable RTU whitelisting for user programs.

Disable firmware download to RTUs <Yes/No> [No]

Whether an authorized user can download a system software (firmware) file to the RTU. If this parameter is Yes, download of firmware is only possible in bootstrap mode (locally.)

Message Life Time

Message Life Time Status <On/Off> [On]

If this parameter is set to Off, the other parameters in this group are ignored. If this parameter is set to On, the MDLC frames will include the transmitter UTC time. Setting this parameter to On will be saved only if the MDLC payload encryption is set to On and the Type of MDLC encryption algorithm is set to AES.

Message Life Time Window <1-65535> [60]

The time window (in seconds) in which a received frame can be validated. A receiver validates the frame only if the time difference between the Message Life Time Stamp within the frame and its own UTC time is no more than the time window. This ‘Message Life Time’ functionality implicates that for a system to have a fluent MDLC communication, needs to be fully synchronized from the time respective.

Security Files Signature Hardening

Signature Verification Algorithm <RSA 2048>

RSA2048 is a public-key cryptosystems used for secure signature of transmitted files.

APPENDIX B: USER ROLES AND PERMISSION GROUPS

The following permanent roles exist in an MC-IoT secured system. Each user can be assigned one role:

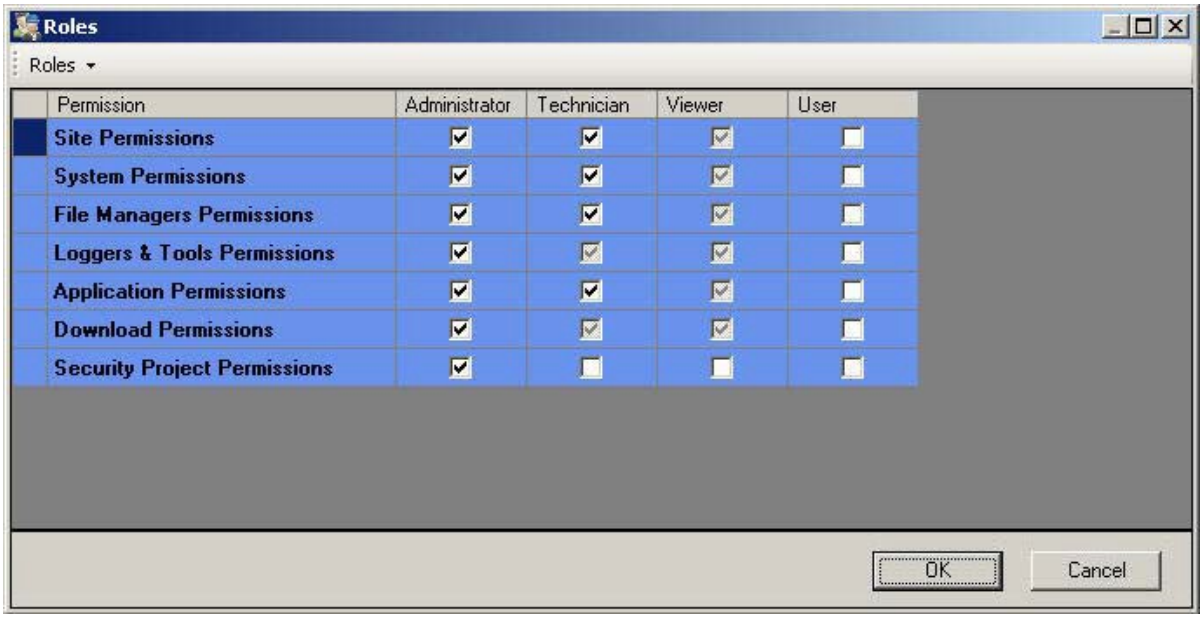
- Administrator
- Technician
- Viewer
- User (can be modified)

A set of permissions is associated with each role. The system administrator can enable or disable certain permissions for the "User" role in the STS.

The permissions are organized into permission groups, although certain operations may require permissions from a different group. The permission groups are shown below. A black ✓ check mark indicates that all permissions in the group are granted. A gray ✓ check mark indicates that not all permissions in the group are granted.

When a permission group is enabled/disabled a set of messages may be displayed, to inform the user of permissions which are being changed.

Note: An operation in one group may require permission for operations in a different group. Those inherited permissions are set automatically when needed. Therefore, it is possible that disabling a permission group will set another group's header to a gray ✓ check, meaning that not all permissions in the group are granted.



The table below lists the permissions within each group.

Note: The details may vary in different releases.

Permissions	Administrator	Technician	Viewer	User
Site Permissions	☑	☑	☑	
View site configuration & Add-Ons	✓	✓	✓	
Modify site configuration & Add-Ons	✓	✓		
View RTU Hardware Test information	✓	✓	✓	
Perform RTU Hardware Test operations	✓	✓		
Change RTU version	✓	✓		
View phonebook	✓	✓	✓	
Modify phonebook	✓	✓		
System Permissions	☑	☑	☑	
Modify (save) secured project	✓	✓		
Field View & Upload site	✓	✓	✓	
View links configuration & cost	✓	✓	✓	
Modify links configuration & cost	✓	✓		
Access dialer	✓	✓	✓	
View system & PRIS address	✓	✓	✓	
Modify system & PRIS address	✓	✓		
Perform time synchronization	✓	✓		
File Managers Permissions	☑	☑	☑	
View network configurations	✓	✓	✓	
Modify & assign network configurations	✓	✓		
View IP conversion tables	✓	✓	✓	
Modify & assign IP conversion tables	✓	✓		
View site tables	✓	✓	✓	
Modify & assign site tables	✓	✓		
Loggers & Tools Permissions	☑	☑	☑	
Read RTU diagnostics	✓	✓	✓	
Read RTU errors	✓	✓	✓	
Erase RTU errors	✓	✓		
Read RTU time tag events	✓	✓	✓	
Erase RTU time tag events	✓	✓		

Permissions	Administrator	Technician	Viewer	User
Upload core dump	✓			
Read RTU date and time	✓	✓	✓	
Set RTU date and time	✓	✓		
Application Permissions	☑	☑	☑	
View applications	✓	✓	✓	
Monitor application data	✓	✓		
Modify monitored application data	✓	✓		
Download Permissions	☑	☑		
Access downloader	✓	✓		
Perform download	✓	✓		
Download policy	✓			
Download keys	✓			
Download users information	✓			
Security Project Permissions	☑			
Unsecure a project	✓			
Secure/Unsecure a site	✓			
View users	✓			
Modify user information	✓			
View security keys	✓			
Modify security keys	✓			
View policy	✓			
Modify policy parameters	✓			
View roles & permissions	✓			
Modify roles & permissions	✓			
Read STS audit log	✓			
Read RTU security log	✓			
Clear RTU security log	✓			
Import security files	✓			
Export secured project	✓			
Encrypt data files	✓			
View/download/decrypt encrypted files	✓			

APPENDIX C: ACE3600/MC-EDGE SYSTEM DOCUMENTATION

The following ACE3600/MC-EDGE system documentation is available to ACE3600/MC-EDGE users:

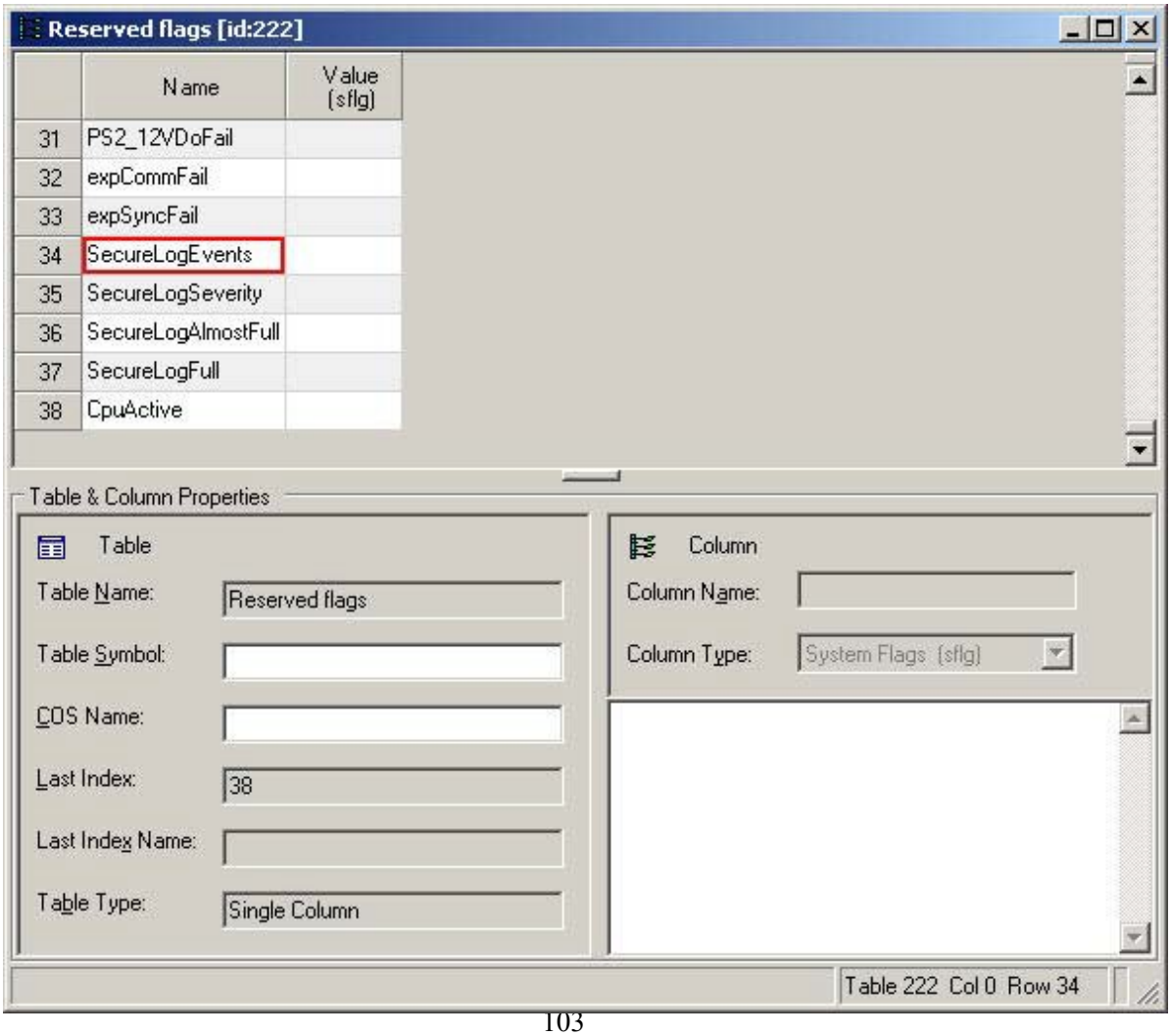
- MC-IoT STS User Guide – in C:\STS<version>\STSManuals after the STS is installed.
- MC-IoT STS Advanced Features Manual – in C:\STS<version>\STSManuals after the STS is installed.
- MC-IoT STS Software Diagnostic Output and Error Messages Manual in C:\STS<version>\STSManuals after the STS is installed.
- MC-IoT STS Third Party Protocols Manual – in C:\STS<version>\STSManuals after the STS is installed.
- ACE3600 C Toolkit User Guide – in C:\cygwin\cross\host\x86-win32\ctkenv\doc after the C Toolkit is installed.
- ACE3600 RTU Owner's Manual – provided with ACE3600 RTUs
- ACE3600 System Planner – available from product support group

APPENDIX D: SECURITY INFORMATION IN APPLICATION DATABASE TABLES

A full description of the ACE3600 database system and constant tables can be found in *Appendix C* of the *MC-IoT STS User Guide*. This appendix describes only the security related elements of the database.

Reserved Flags Table

This system table, shown below, includes variable flags handled by fixed functions in the system. These flags are used for exchanging information between the control program written by the user and the RTU system software, or used by the appropriate rungs when requested through the appropriate functions.



SecureLogEvents: For secured systems only. This flag is set by the system to '1' when there is at least one event in the security log file. It is reset when the file is empty.

The SecureLogEvents variable may be used to inform the control center that there is a security event (SecureLogEvents =1) – as in the *Example Process* below.

SecureLogSeverity: For secured systems only. This flag is set by the system to '1' when there is at least one event in the security log file whose severity is greater than or equal to the predefined 'High severity threshold level' in the policy. It is reset only when the security log is erased.

This variable may be used to inform the control center that the high severity event has occurred (SecureLogSeverity = 1). Note: If the security log is full, older events will be overwritten. Therefore it is possible that the SecureLogSeverity flag is set to 1, but the high severity event itself is no longer there.

SecureLogAlmostFull: For secured systems only. This flag is set by the system to '1' when the security log file is 80% full. It is reset when the number of events in the file falls below this threshold.

This variable may be used to inform the control center that the security log file is almost full (SecureLogAlmostFull = 1).

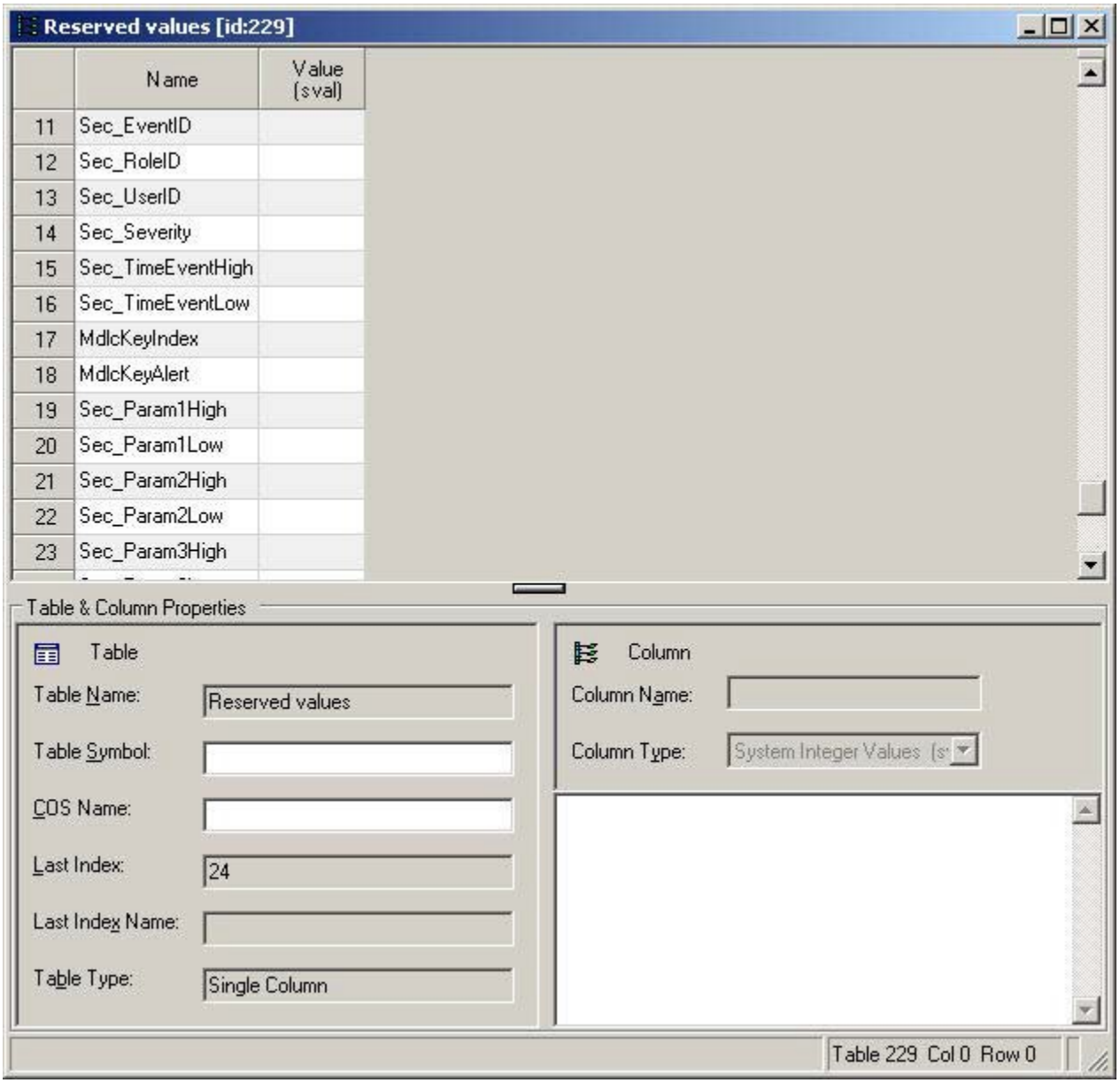
SecureLogFull: For secured systems only. This flag is set by the system to '1' when the security log file is 100% full. It is reset when the number of events in the file falls below this threshold.

This variable may be used to inform the control center that the security log file is full (SecureLogFull = 1) and old messages are being discarded.

These flags will not appear in the Reserved Flags table in a nonsecured system.

Reserved Values Table

This system table includes system values that may be used in the process programming for various purposes.



These security event values are set when the user application calls the GetSecLog ladder function to retrieve the security log events. See the *Example Process* below.

Sec_EventID: For secured systems only. The ID of the retrieved security log event. If '0', then no high severity events exist in the log.

Sec_RoleID: For secured systems only. The user's role ID in the retrieved security log event.

Sec_UserID: For secured systems only. The user's ID in the retrieved security log event.

Sec_Severity: For secured systems only. The severity of the retrieved security log event. Can be one of 1 = information, 3 = moderate, 5 = high, or 7 = critical.

Sec_TimeEventHigh: For secured systems only. The high byte of the date and time of the security log event (day, year).

Sec_TimeEventLow: For secured systems only. The low byte of the date and time of the security log event (milliseconds from the Sec_TimeEventHigh day.)

MdlcKeyIndex: For secured systems only. The active MDLC encryption key index in the list of keys.
Note: At startup, this is set to 0 (= no active key and no encryption) until it gets its actual value. Ignore this value when it is set to 0.

MdlcKeyAlert: For secured systems only. The number of minutes remaining until MDLC payload encryption keys will be swapped. If the value is < 32767, it reflects the actual number of minutes until the key swap. If the value is = 32767 minutes (22.75 days,) the key swap will take place in at least 32767 minutes (could be more.)
Note: At startup, this is set to 0 until it gets its actual value. Ignore this value when it is set to 0.

Sec_Param1High: For secured systems only. The high byte of the first parameter of the security log event text message.

Sec_Param1Low: For secured systems only. The low byte of the first parameter of the security log event text message.

Sec_Param2High: For secured systems only. The high byte of the second parameter of the security log event text message.

Sec_Param2Low: For secured systems only. The low byte of the second parameter of the text messages sent to the security log.

Sec_Param3High: For secured systems only. The high byte of the third parameter of the security log event text message.

Sec_Param3Low: For secured systems only. The low byte of the third parameter of the security log event text message.

Example Process

In the example below, the first rung checks if there are events in the security log. The second rung copies the security event values into parameters and sends a burst with the event.