

SLATE™ SECURITY MANUAL

Best Practices With Respect To Cyber Security
And Network Configuration Safety



Introduction

SLATE provides configurable safety and programmable logic together in one combustion system. The platform is easily customized for almost any requirement or application—offering virtually limitless development opportunities with far less complexity including data integration to building automation systems and remote troubleshooting. The SLATE system is designed to provide great versatility to users, however this versatility also brings with it a necessity to be careful when configuring system for an application.

This security manual is designed to provide best practices with respect to Cyber Security and network configuration safety.

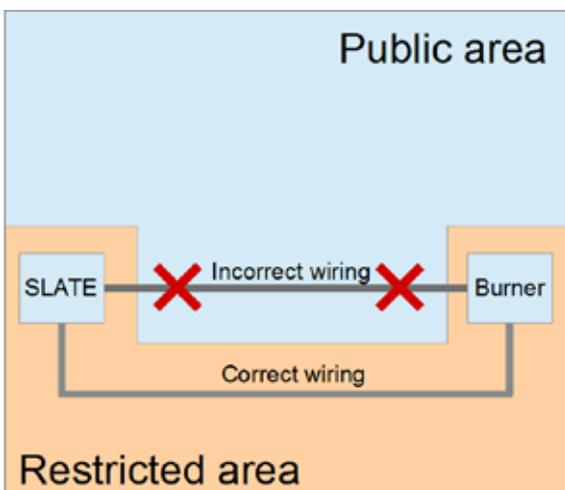
Physical Device Protection

The SLATE Base Module (R8001A1001/U) is designed to provide various security features to avoid being misused remotely. However, it is important to remember that physical security is essential to avoid non-remote threats.

When installing a SLATE device, always select a physical location with limited or even restricted access. It is recommended to lock the device in an enclosed cabinet with access allowed only to approved and trained personnel.

Also, it is strongly advised to keep all the wiring of the device physically secure. An example of correct and incorrect wiring is shown in the figure below.

Caution: When insecurely wired, unauthorized personnel might tamper with wiring of the device other controlled equipment, resulting in questionable behavior. This rule applies to SLATE specific wiring, but also applies to any other controlled equipment.



SLATE Internal Platform Bus

Communication between SLATE modules is essential for system to function in a reliable manner. SLATE modules communicate through the module sub-base (backplane) of the system. It is recommended to avoid connecting any non-SLATE accessories to the module sub-base connectors. Utilizing devices that are not meant to be used with SLATE may break communications between those modules.

Internal vs. External Memory Storage

The SLATE Base Module supports several storage devices for run time and log data

- Internal SLATE Base Module memory
- Internal SD Card
- USB

Internal Base Module Memory

SLATE's Base Module (R8001A1001/U) has approximately 300 MB of internal memory. The memory is physically accessible only if the Base Module is disassembled. This memory includes various log and SLATE AX Too Wire Sheet design information.

It is necessary to understand that any data stored in internal memory is protected against modification as long as the Base Module is physically secure and a strong password for the web interface is in place.

Internal SD Card

The internal SD card can be secured against undetectable tampering by adding a seal on the plastic cover enclosing the card as shown in the figure below.

Network Configuration

For secure device usage keep in mind the following recommendations when installing the device as well as after installation when doing any modifications. Although the system is designed to be secure, it is obvious that remote disturbances can affect performance in an unpredictable way caused by threats that are found after the device release date.

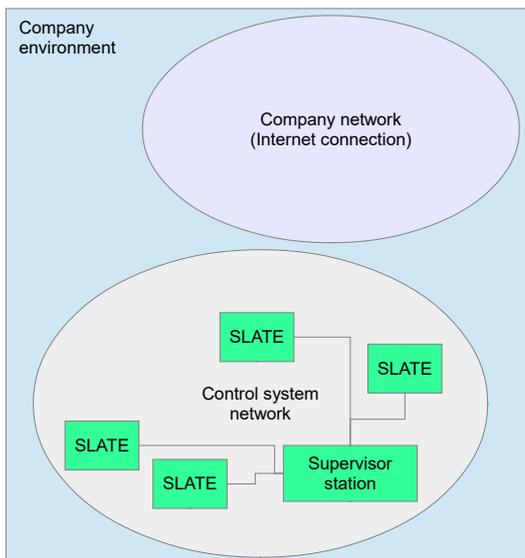
Network Isolation

It is recommended that SLATE be installed on an isolated network. Isolation can be achieved by the following methods:

1. Physical separation of the network
2. Firewall isolation
3. Network Address Translation or (NAT)

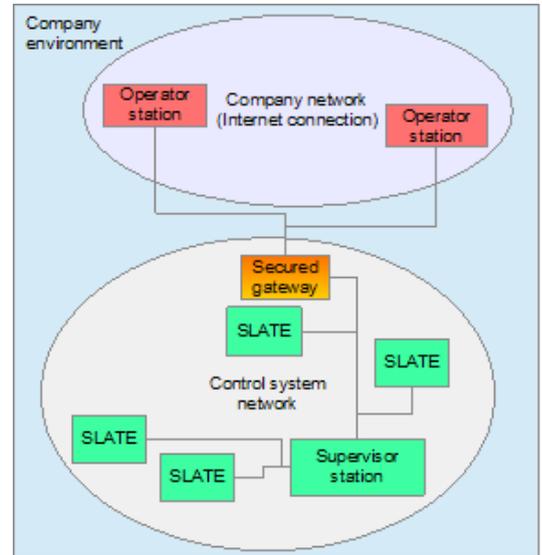
Physical Separation of the Network

The network connection brings the highest level of security since there is no physical connection between SLATE and the outside world. Please be aware that wireless connections are essentially a “physical” connection as well so using any wireless devices as elements of control for the system network can render any security measures challenging.



Firewall Isolation

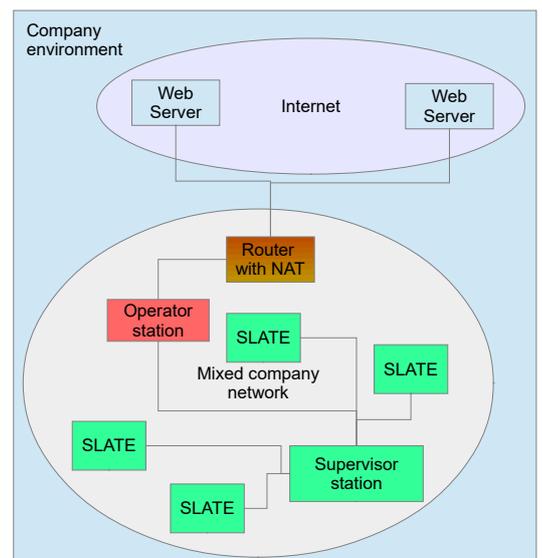
If it is necessary to deploy a connection between the SLATE network and a company’s infrastructure, a recommended solution is to have a properly configured firewall (secured gateway) in place. The role of the gateway is to filter out any traffic from an unknown source and allow only requests coming from reliably identified clients. An example of this type of connection can be observed below:



A possible example of such a secure gateway would be a typical VPN setup with a strictly defined set of approved users.

Network Address Translation

Network Address Translation (NAT) allows partial isolation of outside networks from the SLATE Control System Network. When a NAT is properly configured it should not allow for any connection from an outside system to the SLATE System. Since there are different solutions in the market for configuring networks it is recommended to fully understand the functionality of all system parts and follow recommendations from manufacturers of any network components.



Operator/Supervisor Station Configuration

Since an operator stations can be connected directly to a SLATE device, several steps are recommended before the connection is physically done.

1. Operating system and all other software is kept up to date and configured according to recommendations from the manufacturer. Always use a version of the operating system supported by the vendor. Do not use obsolete operating systems.
2. Antivirus software is installed and run-time protection is enabled.
3. Firewall is installed and enabled
4. Whitelisting is enabled, only explicitly allowed application can execute
5. Always use trustworthy software that is genuine

Web Server Accounts

To keep user data secure there is support for 3 user roles in SLATE. SLATE does not implement typical user accounts with an account for each user. Instead there is an account for each user role.

USER ACCOUNT LEVEL	ALLOWED OPERATIONS
No password	<ul style="list-style-type: none"> • Read any data in system • Modify unprotected registers
Operator	<ul style="list-style-type: none"> • All unrestricted operations • Setup logging features • Export log data • Export/import curve set data (optional) • Modify operator-restricted registers
Installer	<ul style="list-style-type: none"> • All operator-restricted operations • Install configuration packages • Install service packs • Install SSL certificates • Perform safety verification • Modify installer-restricted registers
Designer	<ul style="list-style-type: none"> • All installer-restricted operations • Modify designer-restricted registers

Account Management

Each account role is password protected. When the system is installed, it is strongly recommended to modify passwords for each role (from the default values) to limit system access only to authorized personnel. Passwords must fulfill at least one password strength policy:

1. Password/passphrase of 12 or more characters containing at least one alphabet letter and at least one capital letter
2. Password/passphrase of 8 or more characters containing at least one alphabet letter, one capital letter, one numeric character and one special symbol.

It is recommended to change passwords periodically to lower the chances that a password can be guessed.

Note that a user with higher privileges can change the password for any subsidiary role.

Account Lock

When a user tries to log in with an invalid password more than 10 times in succession, further user account access is denied for 10 minutes. During this time period the account cannot be used and all attempts to log in are automatically rejected (whether or not the correct password is provided).

Remote Identification Number (RIN) The RIN is a random number used to prove physical presence of the user near the unit. This number is random and is generated at the user's request by pressing the "Request RIN" button on a login web page. The RIN is displayed on the system local display (Base Module LCD) and it's value needs to be typed into the RIN field in the logon dialog.

The screenshot shows a login dialog box with the following elements:

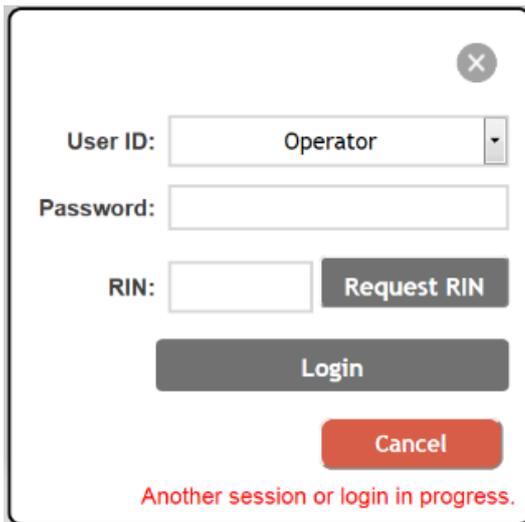
- User ID:** A dropdown menu currently showing 'Operator'.
- Password:** An empty text input field.
- RIN:** An empty text input field next to a 'Request RIN' button.
- Login:** A large grey button.
- Cancel:** A red button.

The screenshot shows the login dialog box after the RIN has been requested. The RIN field now contains a vertical bar, and the 'Request RIN' button has been replaced by a 'Cancel (2:57)' button. The 'Login' and 'Cancel' buttons are still present. A green message at the bottom reads 'RIN was displayed on screen.'

Without a valid RIN it is not possible to login. Please note that each RIN is valid for only 3 minutes, until the "Cancel" button is pressed, or until a successful login occurs. Any of these conditions result in the RIN being invalidated.

Session Concurrency

Only one session can be active at a time. When a user is already logged in, any additional login requests are automatically rejected.



The screenshot shows a login window with a close button (X) in the top right corner. It contains the following elements:

- User ID:** A dropdown menu with "Operator" selected.
- Password:** An empty text input field.
- RIN:** An empty text input field next to a "Request RIN" button.
- A large "Login" button.
- A red "Cancel" button.
- A red error message at the bottom: "Another session or login in progress."

Authenticated Web Server

To assure security of transmitted data via HTTPS protocol using Transport Layer Security (TLS), encryption is used for communication between the user (web browser) and the SLATE Base. This protocol provides integrity check and encryption which protects the data from being tampered with while in transmission or stolen by a possible attacker. It protects user passwords and other confidential data sent into SLATE. E.g. such as register values.

Please note that SLATE supports server authentication only, this means that anyone can connect to its web interface and read data directly from that web interface.

Session Loss

When a new session is opened for an inactive browser window (e.g., operator station suddenly fails), one of the following options can be used to restore access to the unit:

- Use local display (Base module LCD) to terminate the login session by navigating to the Web Interface page and select "Terminate session"
- Wait for the session timeout
- Reboot the unit (cycle power)

Password Reset

If an account password is lost, or is otherwise unknown, e.g., the operator cannot be contacted any more, there are several options to restore access to privileged features of the device:

- If the blocked account is either an Operator or Installer role, the Designer role can always change lesser-privileged passwords.
- If the blocked account is the Designer role, you must contact Honeywell technical support for assistance in resetting the password.

Vendor (Honeywell Technical Support)

Assisted Password Reset

If the Designer account password needs to be reset, a special password reset code needs to be obtained. On the local display (Base module LCD) navigate to Menu->Web Interface->Web password recovery. A password reset code is provided and will be valid for 3 hours. Within this time interval it is necessary to contact technical support and obtain a password reset file corresponding to this code.

Once the password reset is done, the passwords are set to the following default values:

ROLE ACCOUNT	PASSWORD
Operator	SlateOperator
Installer	SlateInstaller
Designer	SlateDesigner

These passwords should all be changed immediately to avoid security risk.

Auditing Guidelines

The SLATE Base Module supports various features allowing identification of problematic situations or unwanted configuration changes in the following areas:

1. Event Log
2. Audit Trail
3. Trend Log
4. Alert Log

Event Log

This feature allows a user to monitor and detect situations which might be important when systems show behavior outside acceptable limits, e.g., random lockouts, faults etc. It is recommended to review the event log content periodically even if no explicit issue is otherwise detected as a form of preventative maintenance, e.g., due to system wearing out.

The Event log is stored in the Base module's internal memory, but it can be archived to an SD card or USB stick at any time. Note that when a system backup to external memory is performed the Event log contents are included in the backup process.

Date	Time	#	Module	Type	Code	Description
2016-12-12	10:19:55am	inf	Base	INFO	10	FBI: Battery is present
2016-12-12	10:19:45am	inf	Base	INFO	4	FBI: Configuration file received
2016-12-12	10:19:45am	inf	Base	INFO	5	Service enabled
2016-12-12	10:19:43am	inf	Base	INFO	25	Kit "Version3 wireconfig swk" successfully installed
2016-12-12	10:19:43am	inf	Base	INFO	5	Service disabled
2016-12-12	10:19:14am	inf	Base	INFO	10	FBI: Battery is present
2016-12-12	10:19:14am	inf	Base	INFO	3	FBI: Module powered up (Power on event: 00000001)
2016-12-12	10:18:14am	inf	Base	INFO	6	Service enabled
2016-12-12	10:18:13am	inf	Base	INFO	6	Module powered up

It is a good idea to activate monitoring for values that are critical for your particular application and review the behavior of these values periodically. It can help to detect long-term changes in the system or process being controlled.

Note: Trend log data is stored on an internal SD card. Please remember to follow recommendations from the "Physical Security" chapter to make this storage secure.

Audit Trail

This feature logs all setting changes to configuration registers. If your system behavior is not correct (but was previously as desired), then it is advised to review the Audit Trail for changes to configuration registers to see if any recent configuration changes may have adversely affected system operation. The Audit Trail is stored in internal device memory and can be saved to external media (USB or SD card) for investigation purpose by pressing the "Save" button.

Date	Time	Source	Register	Value
2016-12-12	10:21:07am	Web	419	6
2016-12-12	10:21:04am	Web	417	3
2016-12-12	10:21:02am	Web	132	15
2016-12-12	10:19:59am	Web	411	6
2016-12-12	10:18:43am	Internal		Kit "Version3 wireconfig swk" installed

Alert Log

This feature allows monitoring of active Alerts in the system. This information is stored in volatile memory so if it is desired to save the current Alert log, it is necessary to save a log snapshot to external storage. Alerts are generally used to assist in troubleshooting or diagnosing the system operation as the messages are often state relevant – e.g., "No Demand Present" for a Burner

Control or "Burner is holding". These messages are active for a period of time as compared to an Event log event which is a one-shot occurrence.

Modbus & BACnet

Modbus and BACnet protocols are each supported in SLATE in two modes: RS-485 and Ethernet, and security of these have to be taken into consideration when designing the system network.

Trend Log

This feature allows run-time monitoring of device behavior. Unlike the Audit Trail and Event Log, this feature is turned off by default and has to be activated explicitly by creating a new trend log. The Trend Log allows monitoring any single numerical value (not just configuration registers but status registers as well) or up to a set of 14 different values. The content of the log is a time correlated report of the selected registers.

Name	Test_Trend_Log_01
Description	The purpose of this trend log is to verify the function of trend log system.
Registers	Reset counter (m1r5200) Watchdog counter (m1r5201) Power-up counter (m1r5202) Brownout counter (m1r5203)
Change snapshot	No
Interval	5 seconds
Enabled	Yes
Size	712.0 KB (326 records)

Although the core of these protocols are different, the security principles used and recommended are the same.

RS-485

Neither protocol standard using the RS-485 physical layer supports any enhanced security features (e.g., additional encryption). This means that security controls need to be fully provided by the user/installer.

RS-485 Physical Security

It is essential to understand that any unauthorized access to physical wiring carrying Modbus/BACnet can allow malicious personnel to modify the communication by intercepting it inserting their own content (Man-in-the-middle) or to sniff data content. Any of these actions could affect behavior of the system in an undesirable way including system malfunction, incorrect behavior of network nodes, etc.

Care must be taken with cable wiring per the Physical protection recommendations to mitigate this security concern.

Ethernet

For Ethernet connections with an insecure protocol enabled (e.g., unencrypted) it is essential to apply special security controls besides those mentioned in the chapter related to Network configuration.

Ethernet Physical Security

When either BACnet or Modbus is enabled, data running on Ethernet line is unencrypted. This means that anyone with the ability to access any network point (e.g., a switch, router, or PC) is able to listen to this communication and possibly create new packets. Such packets have the possibility to disturb or completely inhibit normal system functionality.

Care must be taken with cable wiring and network topology to mitigate these security concerns.

Network Isolation

When an Ethernet network is used for communication between Modbus/BACnet data and also for internet connection, your router/firewall should be configured very carefully to avoid unwanted access from the outside network (internet) into the control network.

Designer Kit

A designer kit file brings configuration data from the SLATE AX Tool into the SLATE Base Module. Because the designer kit carries a complete configuration for a particular system design or set of systems, it is extremely important to only install designer kit files from trustworthy sources.

A designer kit can exist in four types:

1. Standard designer kit
2. Pre-verified designer kit
3. Light designer kit
4. Pre-verified light designer kit

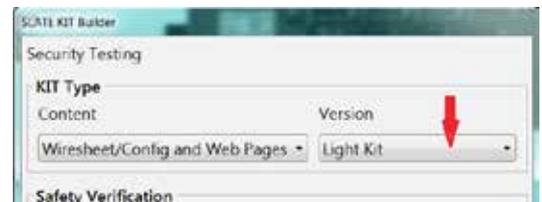
Each of these types have specific concerns for security features, so it is strongly advised to consider which kit type to use prior generating it with the SLATE AX Tool.

Key features of each kit type are listed in following table:

KIT TYPE	HIDDEN CONTENT	BYPASS VERIFICATION	KIT LOCK SUPPORT
Standard	Yes	No	Yes
Pre-verified	Yes	Yes	Yes
Light	No	No	Yes
Light pre-verified	No	Yes	Yes

Hidden Content

This feature is enabled automatically for a Standard kit type. Hiding of content means, that data in the package is obfuscated by a special algorithm which disallows direct reading of the content. Caution: Hiding of content provides a protection against “random readers”. This type of hiding is NOT suitable for IP (intellectual property) protection. If you require real IP protection, please follow the recommendations below. Light kit types do not offer the Hidden content feature, but they provide much better installation performance and are well suited for debugging of web pages or unit configuration. It is, however, generally recommended to use Standard kit types for final designs so that the Hidden content feature is enabled.



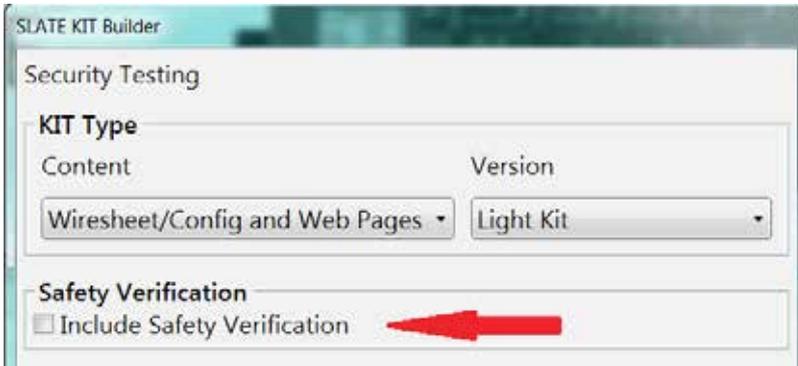
Intellectual Property Protection

1. If real intellectual property protection is required, it is always necessary to understand that data stored in SLATE is protected in a limited way. The reasons are:
 2. Data presented on a web interface is always visible to anyone who has access to the network.
 3. Data stored in registers are able to be read over Ethernet and via Modbus, BACnet, or any other configured interfaces.
 4. A copy of the designer kit is stored on the internal SD card for backup purposes. If it is not possible to protect the unit physically, it is recommended to remove the designer kit copy from the SD card manually after installation. The kit copy is stored on the internal SD card in a folder called “/currentkit/”, and some versions of system also use a folder called “/backupkitdir/”.
5. Always remember that anyone who has access to unit could perform reverse engineering of the kit contents by examining the unit behavior, e.g., simulation of inputs and observing outputs.

Bypass Verification

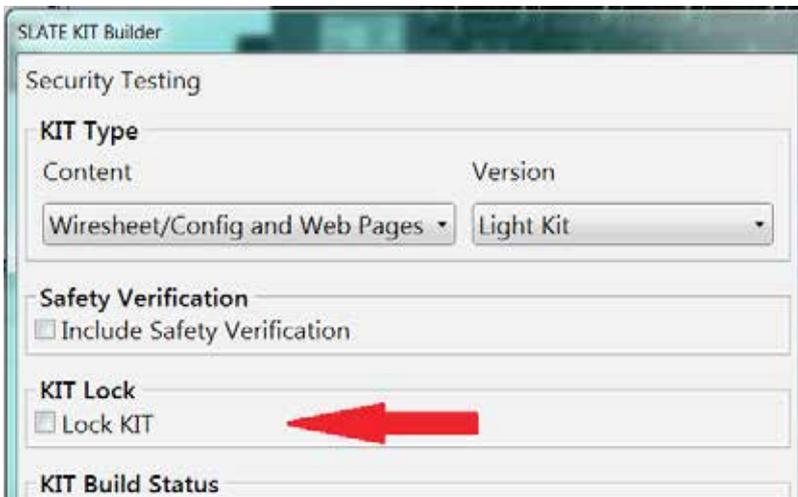
This feature is activated when the “Include Safety Verification” checkbox is checked in the SLATE Kit builder. Using this feature simplifies the configuration process and is suitable for configuration of multiple systems using the same type of application.

Caution: Using this feature is NOT recommended when you are not absolutely sure that configuration carried within the kit is suitable for a particular application.



Kit Lock

Kit Lock is a security feature that allows “binding” of a unit to a particular designer key. Once the kit lock feature is activated and the kit is installed, the SLATE Base Module is immediately bound to that particular designer key. From that moment on the SLATE Base Module rejects any kit installation attempt that does not include a kit that is signed with the same designer key.



CAUTION: Please be aware that once a locked kit is installed, every successive kit installation to the Base module must be locked with the same key. In other words, no unlocked kit or kit with a different key can be installed.

CAUTION: If you lose your designer kit key, it is not possible to re-lock the unit to another key. As result of this, it might be necessary to obtain a new (unlocked) unit from Honeywell to install the new designer kit.

Kit Lock Certificate Handling

To lock the kit a standard x509 PKI certificate is used. The certificate is stored in the SLATE AX Tool installation folder (default path is C:\SlateTools\certificates). As a result of this, anyone who gains access to this folder might be able to create kits with a valid signature.

As a protection against this possibility it is recommended to handle the PC where certificate is stored with care. Special care should be taken when:

1. Computer is shared with other users who are not allowed to create the kit. In such case access to this folder should be limited to only approved users. Alternative and even better suggestion is to delete the certificate from the folder and store it there only when you plan to create a signed kit.
2. Computer is planned to be used no more. In such case it is recommended to uninstall SLATE Tools from the computer and make sure that the folder with certificates is deleted.

Kit Lock Certificate Backup

It is advised to backup the certificate file to some secure location, e.g., removable media, to store in a safe place. For this action (and also restoring certificate) it is possible to use the SLATE AX Tool Certificate Manager – import and export feature (see screenshot below).



Service Pack

The purpose of a service pack is to update the software in the Base module. It can include various types of content, including firmware upgrade files for extension modules and security updates for the system.

A service pack should always be installed when the system is in an idle state because the service pack installation process disables all control mechanisms and the system becomes inaccessible from all interfaces until installation is finished.



CAUTION: Never install a service pack when the controlled application is in a safety critical or unstable state. Although service pack installation cannot disable any safety relevant features of the extension modules, the sudden shutdown of a controlled process might result in damage of your equipment.

Service Pack Installation

A service pack is installed from a USB stick inserted into the Base module. It is essential to place the service pack file in the root directory of your USB stick and the file be named with the extension „.ssp“. An example service pack filename is „Firmware_03.00.13872.ssp“. Make sure that the filename does not contain spaces.

Once loaded into the USB stick and inserted in the Base module, go to the URL https://IP_ADDRESS/spinstall.html (or navigate to the service pack installation page from the Generic Pages), login with proper credentials, and select the desired service pack to install from the „File:“ pull-down. If your file is not listed, press the „Refresh“ button to re-read the service pack list from the USB stick that is plugged into the Base module. The following figure shows this installation page.



Press „ Load service pack from USB“ button to initiate the installation process. Please note that installation cannot be cancelled once started. Never reboot the unit during installation if not prompted to do so.

Service Pack History

It is always possible to list all service packs installed in unit. The list is available via the URL https://IP_ADDRESS/cgi-bin/installedservicepacks.sh.

Service Pack Usage

Each service pack file is protected with a Honeywell unique signature which is validated prior to installation of the service pack. This means that a service pack with a corrupt or invalid signature cannot be installed. However, for security purpose it is not advised to even try installation of a service pack from unknown sources. Also, please be aware that not all service packs are applicable for all systems.

In other words only install service packs that are provided by Honeywell and do so as instructed by Honeywell.

When a service pack should be installed:

1. System suffers from issues explicitly fixed in a particular service pack.
2. System is needed to provide a feature offered by a particular service pack.
3. It is strongly advised by Honeywell to install the service pack since it contains a security-related fix.
4. When installation should be reconsidered:
5. System is stable and does not suffer from any issues.
6. Service pack is not security related.

SLATE AX Tool Application

The SLATE AX Tool is the application used to create the initial configuration file for a SLATE system. Therefore, it is essential that this application is managed and used securely.

Key criteria for application security is to follow these best practices:

1. The PC operating system running the SLATE AX Tool and all other software should be kept up to date and configured according to recommendations from the vendor (e.g., Microsoft). Always use a version of the operating system that is supported by the vendor (and thus receiving security updates). Do not use an obsolete operating system especially when the station is connected to the network.
2. Antivirus and run-time protection is installed and enabled.
3. Firewall is installed and enabled.

4. White-listing is enabled allowing only explicitly listed applications to execute.
5. Use only trusted media such as USB sticks, DVD/CDs, floppy disks, etc.
6. Only authorized personnel should be allowed to access and use the station. Strong passwords are used to protect user accounts.
7. ALWAYS use trustworthy software, never install non-genuine (e.g., cracked) applications.

The SLATE AX Tool application features code signature allowing the end user to verify that application installation is genuine and has not been corrupted.

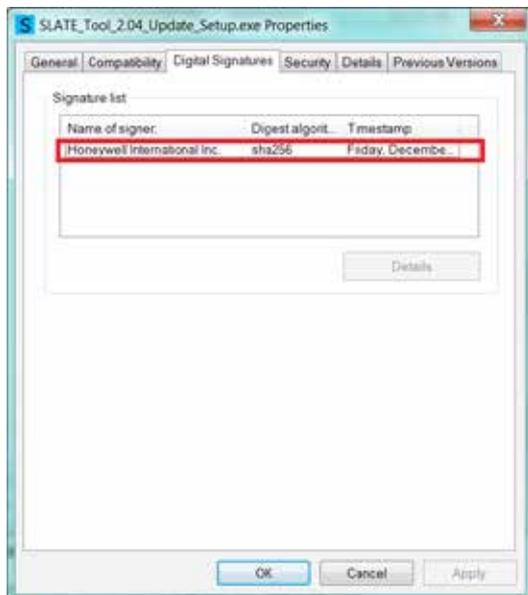
Manual Check of Application/Installer Package Signature

Before starting installation of the SLATE AX Tool, and from time-to-time before using the tool, it is recommended to perform a check of the code signature on the respective file:

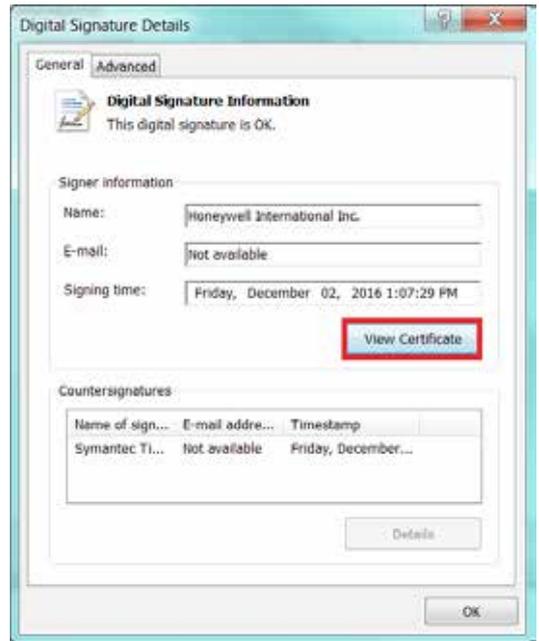
- Installer package file
- Main SLATE AX Tool executable (usually stored in „C:\SlateTools\bin\SLATETool.exe“)

To perform the check:

- Right-click file you wish to validate and open Properties menu.
- Switch to „Digital Signatures “ tab at top row. If tab is NOT present, file is not signed and should not be used. Check if signer is „Honeywell International Inc.“ (see screenshot below).

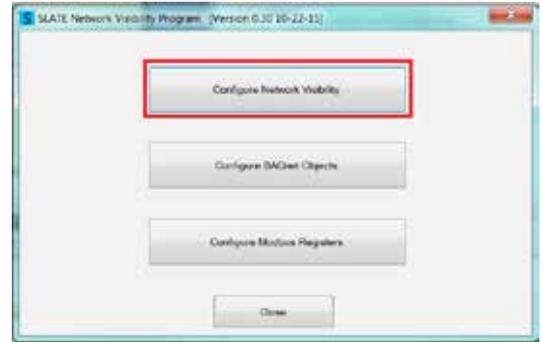


- Click signer name and click „Details“ button. In the opened dialog click „View Certificate“.



- Verify that the certificate is issued by „DigiCert SHA2 Assured ID Code Signing CA“, certification path tab shall look as shown below.





Recommendations and Best Practices

The SLATE system is designed to provide great versatility to users, however this versatility also brings with it a necessity to be careful when configuring system for an application.

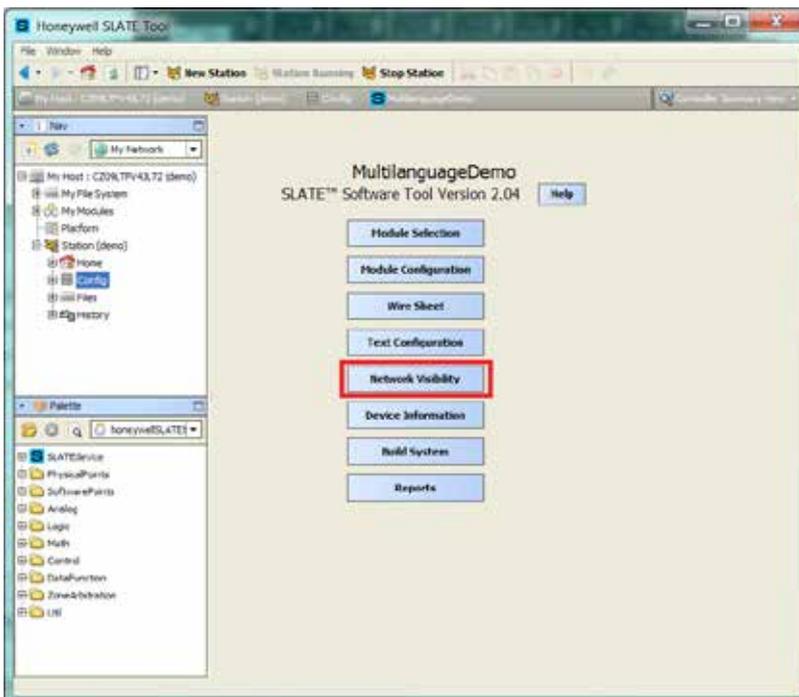
Default register configuration

By default, all registers, except for safety-critical ones, are unprotected. It is strongly recommended to review the register access privileges for all configuration registers and adjust their security levels as appropriate.

In order to perform this task, navigate to Network Visibility in the SLATE Tool and click the Configure Network Visibility button.

For each register select the proper configuration. At a minimum, the following adjustments are recommended:

1. BACnet and Modbus configuration registers are restricted to Operator (m1r100 – m1r118 and m1r139 – m1r141).
2. Ethernet configuration registers (m1r119 – m1r122) are read-only.
3. Login pass code (m1r133) and Login timeout (m1r134) registers are restricted to Operator.
4. Curve set login required register (m1r143) is restricted to Installer.
5. Power cycle command register (m1r416) is restricted to Operator.
6. Date and time configuration registers (m1r123, m1r125, m1r126 and m1r127) are restricted to Operator.



For More Information

The Honeywell Thermal Solutions family of products includes Honeywell Combustion Safety, Honeywell Combustion Service, Eclipse, EXOTHERMICS, HAUCK, Kromschröder and MAXON. To learn more about our products, visit ThermalSolutions.honeywell.com or contact your Honeywell Sales Engineer.

Honeywell Process Solutions

Honeywell Thermal Solutions (HTS)
1250 West Sam Houston Parkway
South Houston, TX 77042

ThermalSolutions.honeywell.com

BR-17-64-US | 09/17
© 2017 Honeywell International Inc.

Honeywell