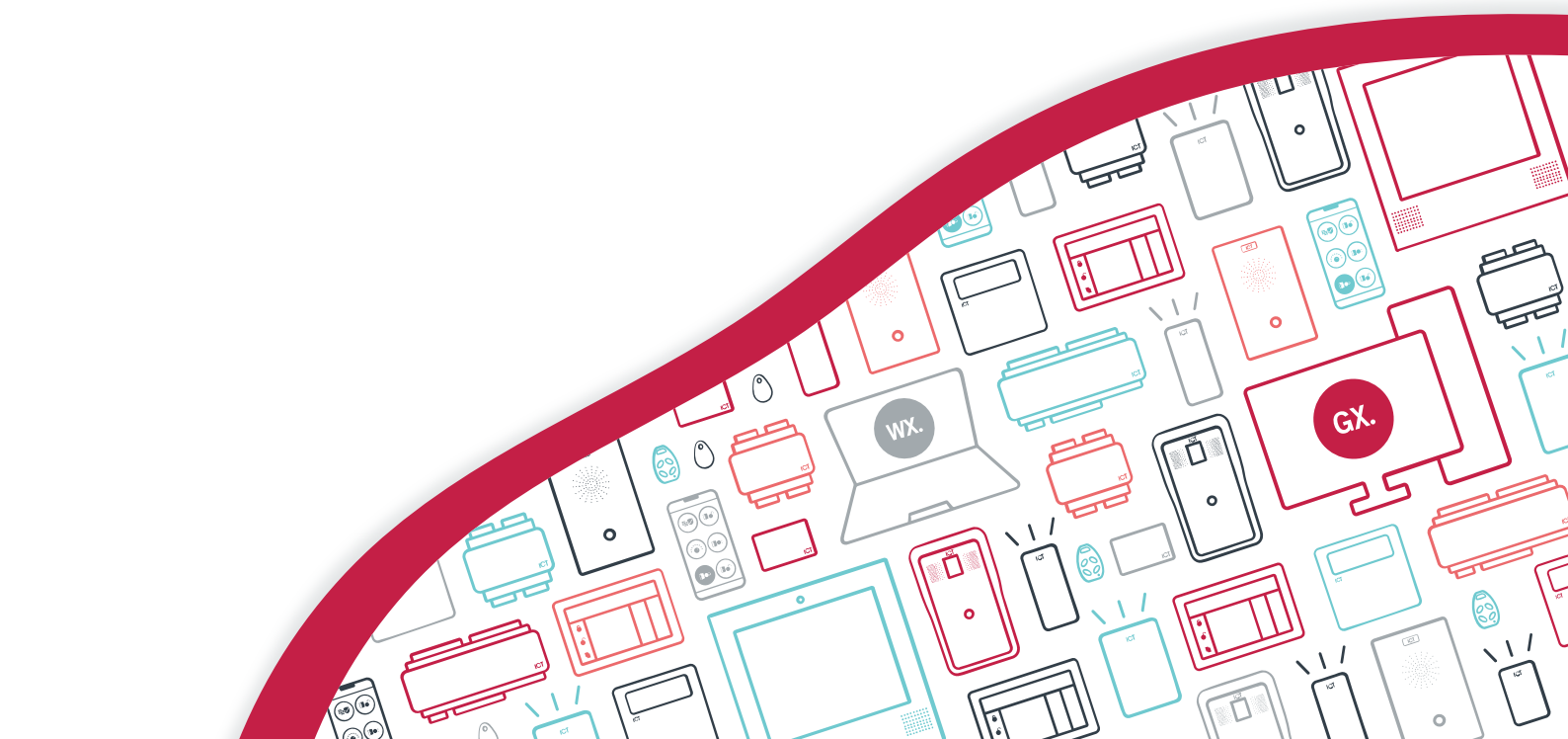
AN-325

Programming Commands in Protege GX and Protege WX

Application Note



Last Published: 26-Apr-24 9:18 AM

Contents

Introduction

As the Protege system is in continuous development, sometimes the Protege GX or Protege WX controller has capabilities which are not yet available in the user interface. However, it is often possible to enable and configure these features by entering programming commands.

This application note contains a list of commands which can be used to program specific features in the controller. This includes some commands which are available in the latest versions of the Protege GX software and/or Protege WX web interface. They are documented here for compatibility with older software versions. If a corresponding UI option is available it is recommended that you use that option instead of the programming command.

Commands related to specific integrations are not included here. These can be found in the relevant application note.

Controller Versions

The controller versions listed below support all of the commands included in this document. Some commands may not be supported in earlier firmware versions. If you have an earlier firmware version, the Protege GX or Protege WX release notes may be able to help you determine whether a command is available in your version.

Controller	Firmware Version
Protege GX Controller	2.08.1360 or higher
Protege WX Controller	4.00.1505 or higher

Using Programming Commands

Programming commands must be entered in the **Commands** field of a specific record in the Protege GX or Protege WX user interface.

It is recommended that you remove any programming commands when the relevant option becomes available in the user interface.

Entering Commands in Protege GX

1. In the Protege GX user interface, navigate to the relevant programming page and select the record that you wish to program.
2. Locate the **Commands** section.
   - For area records this is on the **Configuration** tab (at the bottom of the page).
   - For all other records included in this document this is on the **General** tab.
3. Click on the heading to expand the section.
4. Enter one or more commands in the field. Press enter between each command.

   Ensure that you use the same spacing and capitalization that is used in this document.
5. Click **Save**.
6. If you are editing an expander module, wait for the changes to be downloaded to the controller, then right click on the module record and click **Update Module**.

Entering Commands in Protege WX

1. Log in to Protege WX, navigate to the relevant programming page and select the record that you wish to program.
2. Locate the **Commands** section.
   - For area records this is on the **Configuration** tab (at the bottom of the page).
   - For the controller this is located in **System | Settings | General**.
   - For all other records included in this document this is on the **General** tab.
3. Enter one or more commands in the field. Press enter between each command.

   Ensure that you use the same spacing and capitalization that is used in this document.
4. Click **Save**.
5. If you are editing an expander module, click the **Restart** button.

Commands

Access Levels

Feature	Command	Description
Access Level Door Type	`AllowOverrideDoorType = true`	With this command enabled, users with this access level use alternative credentials to access doors. These alternative credentials must be set in the door type (see page 20). This is equivalent to the **Use access level door Type** option in Protege GX.
Usage Restriction	`LimitUsage = true`	With this command enabled, users can only access doors with this access level a specified number of times. After the usage limit is exceeded they must wait until the reset period has passed before they can use the access level again. This is equivalent to the **Enable usage restriction** option in Protege GX.
	`UsesBeforeDisable = #`	Defines the number of times the user is granted access with this access level. This is equivalent to the **Usage limit** option in Protege GX.
	`UsageResetPeriod = #`	The length of time (in minutes, hours or days) a user will be denied access after reaching the usage limit. Set the units with the command below. This is equivalent to the **Reset period** option in Protege GX.
	`UsageResetType = #`	Sets the unit of time used by the reset period above. The options are: • **M** = Minutes • **H** = Hours • **D** = Days

Analog Expanders

Feature	Command	Description
Pulse Count	`PulseCountCh# = true`	With this command enabled, the analog expander will count pulses on the specified input channel. The count will be recorded in the data value assigned to that channel. • **#** is the analog channel number (1-4). This feature requires analog expander firmware 1.04.005.
	`CountOnRisingEdgeCh# = true`	By default the input channel counts pulses on the falling edge. Enable this command to count pulses on the rising edge. • **#** is the analog channel number (1-4).

Areas

Feature	Command	Description
24HR Arming	`Report24HRArming = true`	With this command enabled, the controller will send a report to the monitoring station when the 24HR portion of the area is armed (enabled). The Contact ID code used is the same as that for arming the main portion of the area.
Auto Rearm	`ReArmLevelTrigger = true`	This command is used in conjunction with the **Disable rearm on schedule** option. Normally this option only suppresses area rearming when the area has been disarmed by the schedule (i.e. not by user, operator, etc.). With this command enabled, the area will not rearm while the schedule is valid, regardless of how the area was disarmed.
	`ReArmAsDeferArea = true`	With this command enabled, automatic area rearming will be deferred for the defined **Defer warning time**, and can be canceled by logging in to the keypad and disarming the area. Canceling a deferred arming will not prevent the area from attempting to arm again after the rearm delay time. To prevent rearming, use **Disable rearm on schedule** and the `ReArmLevelTrigger` command.
Defer Arming	`AskForDeferTime = true`	This command is used in conjunction with the **Defer automatic arming** option. With this command enabled, when the user defers arming at the keypad they can select a number of hours (1-9) to defer arming for.
Force Arming	`UnattendedForceArm = true`	By default, when an area is armed by the **Use unattended brute force arming** feature the area status is set to Armed rather than Force Armed. This can prevent the `EnableForceBypass` and `ForceSendsBypass` commands from working correctly (see page 23). With this command enabled, when the area is brute force armed by an unattended method (e.g. schedule), the status will be set to Force Armed.

Feature	Command	Description
Hold Up Walk Test	`TestOnDisarm = true`	This command enables the area to initiate a hold up walk test when it is disarmed from a keypad. During the test all inputs with the `TestOnDisarm` command enabled (see page 23) must be tested before the area can be fully disarmed. This is equivalent to the **Enable hold up walk test when disarming** option in Protege GX. For more information about this feature, see Application Note 197: Configuring a Hold Up Walk Test in Protege GX.
	`DisarmTestTime = #`	The length of time (in seconds) that will be allowed for the hold up walk test. This is equivalent to the **Maximum test time** option in Protege GX.
	`HUAStartCode = #`	The Contact ID event code that is sent to the monitoring station when the test starts. This is a 3-digit number from 001-999. This is equivalent to the **Contact ID group code for test starting** option in Protege GX.
	`HUAInputCode = #`	The Contact ID event code that is sent to the monitoring station when each input is activated. This is a 3-digit number from 001-999. This is equivalent to the **Contact ID group code for input activation** option in Protege GX.
	`HUAPassCode = #`	The Contact ID event code that is sent to the monitoring station when the test is passed. This is a 3-digit number from 001-999. This is equivalent to the **Contact ID group code for test passed** option in Protege GX.
	`HUACancelCode = #`	The Contact ID event code that is sent to the monitoring station when the test is canceled. This is a 3-digit number from 001-999. This is equivalent to the **Contact ID group code for test canceled** option in Protege GX.
	`HUATestActiveOutput = #`	This output is activated during the hold up walk test, after the first input has been activated. It is deactivated when the test is completed, canceled, or times out. **#** is the output's Database ID. This is equivalent to the **Output to activate during test** option in Protege GX.
	`HUAOutputOnAtStart = true`	With this command enabled, the output above will be activated as soon as the hold up walk test starts, instead of after the first output activation. This also applies to the **Output group to activate during test** (available in Protege GX).

Feature	Command	Description
Remote Area Control	`NoRemoteArm = 1`	When this command is enabled, operators cannot arm the area remotely from the user interface. For more information, see Application Note 326: Disabling Remote Area Arming and Disarming.
	`NoRemoteDisarm = 1`	When this command is enabled, operators cannot disarm the area remotely from the user interface. For more information, see Application Note 326: Disabling Remote Area Arming and Disarming.
	`No24hrRemoteDisarm = 1`	When this command is enabled, operators cannot disarm (disable) the 24HR portion of the area remotely from the user interface. For more information, see Application Note 326: Disabling Remote Area Arming and Disarming.
Remote Notify Delay	`RemoteNotifyDelay = #`	The remote notify delay feature is used to defer reporting to monitoring stations when an alarm is triggered while the area is in entry delay. Essentially this prevents false alarm reporting when a user is temporarily sidetracked off the standard entry route. This is a compliance requirement for BS 8243. • **#** is the delay period in seconds. For more information, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

Feature	Command	Description
User Counting	`CountOnAccess=*[#1,#2,...#16]`	This command can be used alongside the **Enable user counting** option to count the users with specific access levels in the area, and output the number to a data value. • ***** represents the Database ID of the data value which will record the user count. • The **#** values represent the Database IDs of the access levels that will be counted. Up to 16 access levels can be included in each command (comma-separated). Up to four `CountOnAccess` commands can be applied to each area, with each command on a new line. For more information and programming examples, see Application Note 278: Access Level Area Counting in Protege GX.
	`ArmOnCountSched = true`	This command is used in conjunction with the **Arm on user count at 0** option. With this command enabled, when the user count drops to 0 the area will arm only if the **Arm/Disarm schedule** is also invalid.
	`AreaCountOnDoorOpening = true`	When this command is enabled, the user count will only be incremented/decremented if the door is opened after access is granted. If a user gains access but does not open the door, the user count will not be changed. For more information, see Application Note 205: Area Counting.

Controllers

Controller commands are entered in **System | Settings | General** in Protege WX.

Feature	Command	Description
Automation and Control Protocol	`ACPUseDisplayOrder = true`	Normally the ICT Automation and Control Protocol references records in order by Database ID. With this command enabled, records are referenced in order by module address.
Battery Testing	`DisableBattTest = True`	Use this command to disable the regular backup battery test on a PoE (power over ethernet) controller. This ensures that the controller will not periodically drop power draw from the ethernet connection, which may cause a smart ethernet switch to close the controller's ethernet port. Disabling the battery test will prevent the controller from detecting any faults in the backup battery. This command should only be used when the issue stated above is observed on site.
Call to Unlock	`PhoneCallDoor = #`	This command allows the controller to unlock a door when it receives a phone call or text message from specified users. **#** is the Database ID of the default door to unlock. By default, a call or text message from an authorized user will unlock the default door. If the text message contains the Database ID for a different door known to the controller, that door will be unlocked. To use this feature, enter the user's phone number as a card in the format 021:1234567.

Feature	Command	Description
Cross Controller Communications	`LocalIP = *,#`	In some networking scenarios the IP address used by the Protege GX server to communicate with controllers is not the same as the controller's IP address on the internal network used for cross-controller communications. This command provides the IP address which this controller will use to communicate with another controller. Enter one instance of this command for each controller that this controller needs to communicate with. • * is the serial number of the other controller. • # is the internal IP address of the other controller. Do not type a space after the comma, as this will prevent the command from functioning.
	`ICCPort = *`	The default port for cross controller communications is 9470. To change the port, enter this command in the programming for each controller. * is the port to use for communications.
Elevator Integrations	`FloorAccessCheckCar = true`	By default, when a user gains access at an elevator car the controller unlocks all of the floors which they have access to in any access level. With this command enabled, only the floors in the same access level as the elevator car will be unlocked. This command is used with low level elevator integrations.
	`FloorAccessCheckDoor = true`	By default, when a user gains access at the DOP/COP the controller unlocks all of the floors which they have access to in any access level. With this command enabled, only the floors in the same access level as the door record representing the DOP/COP will be unlocked. This command is used with HLI elevator integrations.

Feature	Command	Description
Input Duplexing	`DuplexZones = true`	With this command enabled, the controller can support twice the number of inputs, with open, closed and tamper conditions. The inputs should be wired with a 1K resistor across the first input and a 2K4 resistor across the second input. For more information and wiring instructions, see the relevant controller installation manual.
	`ATZ3RZones = true`	With this command enabled, the controller can support twice the number of inputs with open, closed, tamper and short conditions. The inputs should be wired with a 1K resistor in the circuit, a 1K resistor across the first input and a 2.2K resistor across the second input.
Lockdown	`LockdownDeniesSuperUser = true`	Normally, users with the **User has super rights and can override antipassback** option enabled can unlock doors even when they are locked down. With this command enabled, locked down doors may deny access to super users (following the normal rules for lockdown).
Module Comms	`ReportShortModuleCommFault = true`	With this command enabled, the controller will always open the 'Module Communication Fault' trouble input as soon as it detects a communication failure, without allowing a grace period for the module to come back online. This is equivalent to the **Report short duration module communication failure** option in Protege GX.
	`EnableModuleUDP = true`	With this command enabled, the controller can communicate with remote modules via UDP. Disabled by default.
	`EnableModuleTCP = true`	With this command enabled, the controller can communicate with remote modules via TCP. Disabled by default.
	`EnableTLCDCommsUDP = true`	With this command enabled, the controller can communicate with PRT-TLCD touchscreens over UDP. Disabled by default.
PIN Update	`AutoGenUserPINs = true`	With this command enabled, when a user's PIN expires and they are forced to change it at a keypad, the controller will automatically generate a new 6-digit PIN code. The user can view the number, then press **[ENTER]** to confirm.

Feature	Command	Description
Reporting	`BlindDial = true`	With this command enabled, modem dialing occurs even when no dial tone is detected. This is equivalent to the **Do not wait for dial tone when modem dials out** option in Protege GX and Protege WX.
	`ShowDuplicateIdHealth = true`	With this command enabled, if two users, inputs or areas have the same **Reporting ID** the controller will generate a health status message. Disabled by default.
	`SIAExtendData = true`	SIA reporting over IP using the DC09 protocol supports extended data. This command enables the controller to send the names of any inputs, trouble inputs, users and areas which are included in the report. For more information, see Application Note 317: SIA L2 Reporting in Protege GX andProtege WX.
	`TestReportDayOfWeek = #`	This command configures test reports to occur on a weekly basis. • **#** represents the day of the week, where 1 is Monday and 7 is Sunday. This is equivalent to the **Weekly test report** / **Day of the week** options in Protege GX.
Sequential Access Level Outputs	`CheckSeqAxsLvlOutput = true`	Normally if a user has multiple sequential access levels with associated access level outputs they must activate each output separately as the access level becomes valid. This command allows the outputs from consecutive access levels to be activated automatically as each access level becomes valid. For more information, see Application Note 255: Configuring Sequential Access Level Output Activation.

Feature	Command	Description

Time Drift	`TimeDriftComp = #,*`	Time drift may be experienced by controllers which do not use an SNTP server. With this command, the controller adds a defined number of seconds to its internal clock at the set frequency.
		• **#** is the period of the compensation in days (value from 1 to 31).
		• ***** is the amount of the compensation in seconds (value from -30 to 30).
		For example, if the controller's clock runs 10 seconds slow every 2 days, you would use:
		`TimeDriftComp = 2,10`
		If the controller's clock runs 10 seconds fast every 2 days, you would use:
		`TimeDriftComp = 2,-10`

Troubleshooting	`EnablePing = true`	With this command enabled, you can ping the controller over the onboard ethernet connection. Disabled by default.
UL Compliance	`UL_OPTIONS = true`	With this option enabled, the controller runs in UL compatibility mode. This setting has the following effects: • Adds a 10 second grace period following a failed poll before a module is reported as offline. Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period. • Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual. • Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent. • Limits the **Dial attempts** for reporting services to a maximum of 8. This is equivalent to the **Advance UL operation** option in Protege GX and Protege WX.

Doors

Feature	Command	Description
Access Denied Output	`AccessDeniedOutput = #`	This output is activated for a set time when access is denied at the door. **#** is the output's Database ID.
	`AccessDeniedOutputGroup = #`	This output group is activated for a set time when access is denied at the door. **#** is the output group's Database ID.
	`AccessDeniedTime = #`	Sets the length of time (in seconds) to activate the access denied output or output group for. If this is set to 0, the outputs remain on until they are deactivated.
Door Forced Delay	`DoorForcedStateDelay = #`	Sets the time (in seconds) to delay the door forced processing. With this command in use, when the door is forced open the door forced alarm outputs and trouble input will not be activated until this time has elapsed. For more information, see Application Note 304: Delaying Door Forced Alarms.
Dual Credential	`DualCredPendingTime = #`	Sets the length of time (in seconds) that the door will wait for a second credential to be entered (e.g. when the door type is Card and PIN). The default is 10 seconds.
Function Outputs	`ActivateOnADAF# = true`	When this command is enabled, the function output will only be activated when the door is unlocked by a user with the **User operates extended door access function** option enabled (**Users | Users | Options**). **#** is the number of the function output. Function outputs are currently only available in Protege GX. For more information, see Application Note 336: Programming Function Outputs in Protege GX.
	`RecycleOnADAF# = true`	When this command is enabled along with the preceding command, users with the **User operates extended door access function** option enabled (**Users | Users | Options**) can recycle the function output activation time by entering their credentials again. **#** is the number of the function output. The `RecycleDoorTimeOnAccess` command must also be enabled.
	`DeactivateOnForceF# = true`	When this command is enabled, the function output will be deactivated when the door is forced open. **#** is the number of the function output. The **Deactivate on door open** option (**Programming | Doors | Function outputs**) must also be enabled.

Feature	Command	Description
Invalid Credential Lockout	`LockOutAttempts = #`	Sets the number of invalid authentication attempts that the door will accept before opening the Too Many Attempts trouble input. The default is 3 attempts.
Recycle Lock Time	`RecycleDoorTimeOnAccess = true`	With this command enabled, if a user enters valid credentials while the door is already unlocked the lock activation time will be recycled. This allows users to keep the door unlocked for longer, or reopen an automatic door. For an example of use, see Application Note 260: Usingthe tSec Extra Reader Card Holder.
	`NoAccessEventsIfUnlocked = true`	When the `RecycleDoorTimeOnAccess` command is in use, enable this command to suppress the 'Access Granted' events and reader beeps from subsequent access while the door is already unlocked. For an example of use, see Application Note 260: Using the tSec Extra Reader Card Holder.
Relocking	`RelockOnOpen = true`	With this command enabled, the door will relock when it is opened. If the door is not opened it will still relock after the lock activation time. This is equivalent to the **Relock on door open** option in Protege GX and Protege WX.
Request to Enter	`AlwaysAllowREN = true`	With this command enabled, the door will process the REN (request to enter) input even when the door is open/unlocked. This is similar to the **Always allow REX** option in Protege GX and Protege WX.

Feature	Command	Description
Request to Exit	`AltREX = #`	This input is used as a secondary REX input. When this input is activated the door unlocks for the **REX activation time** instead of the standard lock activation time. **#** is the input's Database ID.
	`BeepOnREX = true`	With this command enabled, the readers associated with the door beep twice when the REX button is pressed. This is equivalent to the **Pulse reader beeper on REX** option in Protege GX and Protege WX.
	`MaintainREX = true`	With this command enabled, the door will remain unlocked as long as the REX button is held down. When REX is released, the door will relock after the REX activation time. This is equivalent to the **Maintain REX** option in Protege GX and Protege WX.
	`REXTime = #`	Sets the length of time (in seconds) that the door will unlock when REX is pressed. This is equivalent to the **REX activation time** option in Protege GX and Protege WX.
Slave Doors	`SlaveREX = true`	By default, slave doors only follow the primary door when it is unlocked by access with a valid credential. With this command enabled, the slave door will also unlock when the primary door is unlocked by REX, REN and operator commands. This command overrides the **Prevent slave unlock on inside area** option. Slave doors can be unlocked by REX, REN and operator commands regardless of area status.
Unlock Schedule	`ScheduleOverridesLatch = true`	With this command enabled, when the unlock schedule becomes invalid the door will automatically lock. In addition, if **Always check unlock schedule** is also enabled, the door cannot be latch unlocked while the schedule is invalid (it will relock immediately). This is equivalent to the **Schedule overrides latch** option in Protege GX.

Door Types

Feature	Command	Description
Access Level Door Types	`OverrideDoorType = #`	This command sets an alternative door type that is used by any users with the `AllowOverrideDoorType` command enabled in their access level (see page 6). **#** is the door type's Database ID. This is equivalent to the **Access level door type** option in Protege GX.
Area Status LEDs	`LED_FUNC[*]=#1,#2,#3,#4,#5,#6,#7`	This command is used to program customized LED patterns to display the status of an area associated with the door. For more information and programming examples, see Application Note 271: Configuring Area Status LED Functions.
Dual Authentication	`CustodyPairEnforced = true`	Normally when dual authentication (dual custody) is in use, only the first user who requests access to a door (normally the dual custody master) has their antipassback and area counting status updated. With this command enabled, the antipassback and area counting status of both users who request access are updated.
Dual Credential Pending LEDs	`DualCredPendingOnColor = #`	When a user enters a credential, the card reader can display a two color LED pattern to notify the user that a second credential is required (e.g. Card and PIN operation). This command defines the first color in the pattern (the 'on' color). For the available LED color codes, see the Appendix (see page 30). This feature is supported by ICT RS-485 readers with RGB LEDs and OSDP readers.
	`DualCredPendingOffColor = #`	This command defines the second color in the dual credential pending pattern (the 'off' color). For the available LED color codes, see the Appendix (see page 30).
	`DualCredPendingOnTime = #`	The time (in seconds) that the first color in the dual credential pending pattern will be displayed.
	`DualCredPendingOffTime = #`	The time (in seconds) that the second color in the dual credential pending pattern will be displayed.

Elevator Cars

Feature	Command	Description
Authentication Mode	`EntryMode = #`	Configures the credentials required to gain access to the elevator car. The options are: • `0` - Card Only (default) • `1` - PIN Only • `2` - Card and PIN • `3` - Card or PIN This is equivalent to the **Authentication mode** option in Protege GX.
	`DualCredPendingTime = #`	When the authentication mode above is set to Card and PIN, this command determines how long (in seconds) the elevator will wait for the second credential. The default time is 10 seconds.
Destination Reporting	`DRIActivatesRelay = true`	In destination reporting integrations, normally when a user badges a card the system waits for an input activation before activating only the floor relay that was selected. With this command enabled, when a user gains access to the elevator car all of the floor relays that they have access to are activated for the **Unlock access time**. If a floor is selected, all relays turn off except for the selected one, which remains on for another **Unlock access time** period. This is required by the security interfaces of some elevator systems.
	`DRMExcludeOpenFloors = true`	In destination reporting integrations, normally when a user selects a floor that is already open the system records access events and status as if the user had unlocked the floor. With this command enabled, no access events or status are recorded for floors that are latched open.
	`DRMAudibleFeedback = true`	With this command enabled, the reader beeper will sound when access is granted or denied after the user selects a floor in a destination reporting integration. This is only supported for Wiegand readers.

Inputs

Feature	Command	Description
Configurable End of Line Resistors	`EOL = Res`	Enables configurable EOL resistor settings on the input. Further commands are used to define up to 3 EOL resistor values, the input states corresponding to different resistance values, and the hysteresis. For more information and programming examples, see Application Note 303: Configuring Input EOL Resistors Using Commands.
Eclipse Keypad Input	`Area#KLESZone = *`	When Eclipse keypads are in use, this command can be used to assign an index that will represent this input on the keypad. When a user attempts to arm an area the keypad will flash its numerical LEDs to indicate which input is preventing the area from arming. The keypad will indicate inputs above 9 by flashing the 0 LED to represent the tens digit. • **#** is the number of an area this input is programmed in (1-4) • ***** is the index that will be displayed on the Eclipse keypad for this input (1-19) This is equivalent to the KLES Input LED 1-4 option in Protege GX and Protege WX.
Input Lockout	`ZoneLockout = true`	With this command enabled, each time this input triggers an alarm a counter is incremented. Once the counter reaches the input lockout count further input activations will not cause alarms. The lockout is reset when the area is disarmed and rearmed again. This is equivalent to the **Enable input lockout** option in Protege GX and Protege WX.
	`ZoneLockoutCount = #`	Sets the number of times that the input can activate the alarm before being locked out. This is equivalent to the **Input lockout count** option in Protege GX and Protege WX,

Input Types

Feature	Command	Description
Force Arming	`EnableForceBypass = true`	With this command enabled, when the area is force armed any open inputs with this input type will be automatically bypassed. The bypass will be removed when the area is disarmed. The **Force input** option must also be enabled in the **Options (1)** tab.
	`ForceSendsBypass = true`	With this command enabled, when the area is force armed any open inputs with this input type will be automatically bypassed. The bypass will be removed when the input is closed. This allows you to send a bypass report for any inputs which have been force armed. The **Force input** option must also be enabled in the **Options (1)** tab. You may also wish to enable the `UnattendedForceArm` command in the area programming (see page 8).
Hold Up Walk Test	`TestOnDisarm = true`	With this command enabled, inputs with this input type must be tested when the area performs a hold up walk test. For more information, see Areas (page 8). This is equivalent to the **Test during hold up walk test** option in Protege GX.
Reporting	`SIACode = #`	This command allows you to report a larger number of unique event types to the monitoring station, using a range of custom event codes. • **#** is the SIA event code (value from 32 to 210). For more information, see Application Note 317: SIA L2 Reporting in Protege GX and Protege WX.

Keypads

Feature	Command	Description
Confidentiality Mode	`ConfidentialMode = true`	When this command is enabled, Protege keypads can enter confidentiality mode, where all lights (power, disarm, arm and LCD backlight) turn off when the keypad is not used for one minute. This occurs only when output 1 on the keypad has been activated. This option is enabled by default on the PRT-KLCD and disabled by default on the PRT-KLCS.
Invalid PIN Lockout	`MaxInvalidPinEntry = #`	The number of times an invalid PIN can be entered before the keypad locks out further attempts. This is equivalent to the **Max invalid PIN entry attempts** option in Protege GX and Protege WX.
	`ENKeypadLockoutTime = #`	The length of time (in seconds) that the keypad will lock out PIN attempts after the maximum number of invalid attempts has been reached. The default is 60 seconds. This is equivalent to the **Lockout keypad time** option in Protege GX and Protege WX.
Offline Menu	`OfflineInputView = true`	With this command enabled, users can view any open inputs in the primary area via the keypad's offline menu. To view open inputs, press **[Menu] [5]** without logging in to the keypad.
	`ClosedInputsInOfflineView = true`	With this command enabled, all inputs in the area can be viewed in the offline menu, regardless of whether they are open or closed. The `OfflineInputView` command must also be included.

Feature	Command	Description
Time and Attendance	`ShowT&ADetail = true`	With this command enabled, whenever a user gains access at the **Door connected to the keypad** the keypad will display the user's name, the current time and the date. This is equivalent to the **Show time and attendance detail** option in Protege GX. See Application Note 177: Time and Attendance on a Protege WX Keypad.
	`T&ADisplayTime = #`	The length of time (in seconds) that the keypad will display the time and attendance details for each user. This is equivalent to the **Length of time to display attendance detail** option in Protege GX.

Outputs

Feature	Command	Description
Custom Reader LED Colors	`LEDColour = #`	This command can be applied to a reader LED output to set the color of the LED. This feature is available for ICT RS-485 readers with RGB LEDs and OSDP readers. This command can be used with the following outputs on a reader expander or controller onboard reader expander: • Output 3 (Port 1 L1) • Output 4 (Port 1 L2) • Output 6 (Port 2 L1) • Output 7 (Port 2 L2) If RS-485 enhanced outputs are enabled (**Enable enhanced smart reader outputs** in **Expanders | Reader expanders | Reader 1/2**), the following outputs should be programmed: • Output 9 (Port 1 Entry L1) • Output 10 (Port 1 Entry L2) • Output 12 (Port 1 Exit L1) • Output 13 (Port 1 Exit L2) • Output 15 (Port 2 Entry L1) • Output 16 (Port 2 Entry L2) • Output 18 (Port 2 Exit L1) • Output 19 (Port 2 Exit L2) **#** represents an LED color code. For the available color codes, see the Appendix (see page 30).

Reader Expanders

Feature	Command	Description
Dual Authentication	`DualAuthOutputR# = *`	This command sets the output that will be activated when the first user enters their credentials at a door that requires dual authentication. • **#** is the reader port (1 or 2) • ***** is the Database ID of the output This is equivalent to the **Reader 1/2 dual authentication pending output** in Protege GX and Protege WX.
	`DualAuthTime = #`	The time (in seconds) that the doors on this reader port will wait for a second credential to be entered. This is equivalent to the **Reader 1/2 dual authentication wait time** in Protege GX and Protege WX.
	`DualAuthOutputEth = #`	This command sets the output that will be activated during the dual authentication process for doors connected to the controller's ethernet port. • **#** is the Database ID of the output
	`DualAuthTimeEth = #`	The time (in seconds) that doors on the controller's ethernet port will wait for a second credential to be entered.
Enhanced RS-485 Outputs	`SmartOutputsR# = true`	This command enables enhanced RS-485 outputs on a reader port. • **#** is the port number (1 or 2). This allows you to use the L1, L2 and BZ outputs as general purpose outputs when the readers are connected in RS-485 configuration. This is equivalent to the **Enable enhanced smart reader outputs** option in Protege GX and Protege WX. For more information on this feature, see Application Note 295: Enhanced Smart Reader Outputs in Protege GX or Application Note 324: Enhanced Smart Reader Outputs in Protege WX.

Feature	Command	Description
Smart Readers	`SmartReaderPortOffset = true`	This command allows multiple smart readers to be connected to the controller's ethernet port. With this command enabled, the controller listens for each smart reader over a different TCP/IP port. The port of each smart reader is equal to the **Ethernet port** of the controller's onboard reader expander plus the **Configured address** of the smart reader. For more information, see Application Note 276: Configuring Credential Types in Protege GX or Application Note 219: Configuring Credential Types in Protege WX.
Wiegand Readers	`DualLEDMode = true`	With this command enabled, both reader ports will support card readers wired in dual LED Wiegand configuration. This is disabled by default.

Trouble Inputs

Feature	Command	Description
Alarm/Restore Speeds (Debounce)	`AlarmSpeed = #`	When an alarm speed is configured, the trouble input must be open for this length of time before it is registered as open. This is equivalent to the **Alarm input speed** in the input programming. **#** is a time in milliseconds. The available times are 10, 50, 100, 250, 500, 1000, 2000, 3000, 4000, 5000, 10000, 30000, 60000, 120000, 600000, 1800000 and 3600000. If an invalid value is entered, it is automatically matched to the closest valid value. See Application Note 305: Trouble Input Alarm and Restore Speeds.
	`RestoreSpeed = #`	When a restore speed is configured, the trouble input must be closed for this length of time before it is registered as closed. This is equivalent to the **Restore input speed** in the input programming. **#** is a time in milliseconds. The available times are 10, 50, 100, 250, 500, 1000, 2000, 3000, 4000, 5000, 10000, 30000, 60000, 120000, 600000, 1800000 and 3600000. If an invalid value is entered, it is automatically matched to the closest valid value. See Application Note 305: Trouble Input Alarm and Restore Speeds.

Appendix: LED Color Codes

The following color codes are available for commands that control the reader LEDs.

RGB color display requires ICT or OSDP readers with RGB LEDs, connected in RS-485 configuration. To determine whether RGB colors are supported, see Application Note 270: Identifying the Hardware on a tSec Reader.

Number (#)	Color	RS-485	OSDP
0	Off	✓	✓
1	Red	✓	✓
2	Amber	✓	✓
3	Orange	✓	✗
4	Yellow	✓	✗
5	Lime	✓	✗
6	Green	✓	✓
7	Mint	✓	✗
8	Turquoise	✓	✗
9	Cyan	✓	✗
10	Sky Blue	✓	✗
11	Cobalt	✓	✗
12	Blue	✓	✓
13	Violet	✓	✗
14	Purple	✓	✓
15	Magenta	✓	✗
16	Crimson	✓	✗

This table applies to configuration commands programmed in Protege GX. TLVs programmed directly on the card readers do not include the 'off' index (0), so the color numbers are Red=0 through to Crimson=15.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.