



AN-326

Disabling Remote Area Arming and Disarming

Application Note



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2021. All rights reserved.

Last Published: 14-Sep-21 1:47 PM

Contents

Introduction	4
Prerequisites	4
Configuration	5
Operation	5

Introduction

In Protege GX and Protege WX it is possible to independently disable remote arming and disarming functionality on an individual area basis. This ensures that the area cannot be armed via the user interface, web client or any other remote means, and can only be armed and disarmed using a local keypad.

This feature supports ULC Standard S302, which limits arming and disarming of a Security Level 3 or Level 4 Area to only the local system keypad(s).

These protection requirements are applicable for safes, ATMs, CDUs, CRUs, night depositories and vaults.

Prerequisites

The following controllers support this feature:

Controller	Firmware Version
PRT-CTRL-DIN	2.08.1141 or higher
PRT-CTRL-DIN-1D	
PRT-WX-DIN	4.00.593 or higher
PRT-WX-DIN-1D	

Configuration

To disable remote area arming and disarming, add the appropriate command(s) to the programming of each required area.

1. Navigate to **Programming | Areas** and select the area to be configured.
2. Add the following commands in the **Commands** section as required:
 - Add the command **NoRemoteArm = true** to disable remote arming.
 - Add the command **NoRemoteDisarm = true** to disable remote disarming.
 - Add the command **No24hrRemoteDisarm = true** to disable remote 24hr disarming.
3. **Save** your configuration, and repeat for all required areas.

Operation

1. When one or more of these commands are added to the area programming, the following manual commands are disabled in the Protege GX client software, Protege GX web client and Protege WX user interface:

Programming Command	Disabled Manual Commands
NoRemoteArm	<ul style="list-style-type: none">• Arm• Force arm• Arm stay• Arm instant• Force arm instant• Arm 24 hrs• Walk test enable• Walk test disable
NoRemoteDisarm	<ul style="list-style-type: none">• Disarm• Disarm 24 hrs• Silence alarm• Walk test enable• Walk test disable
No24hrRemoteDisarm	<ul style="list-style-type: none">• Disarm 24 hrs

2. Disabling a remote area function does not prevent remote arming/disarming functionality via:

- Automation and control service
- Area control programmable functions
- Card readers

To disable arming/disarming at the card reader, ensure that the **Reader 1/2 arming mode** and **Disarm area for door on access** options are disabled in **Expanders | Reader expanders | Reader 1/2**.

3. To validate that this feature has been programmed correctly:
 - Log in to Protege GX, the Protege GX web client, or Protege WX as an operator with permission to control areas.
 - From a monitoring page, right click on the programmed area (Protege GX) or click the **[+]** button beside the area (Protege WX / web client).
 - Select one of the area arming or disarming functions which should be disabled by this command, as

determined by the table above.

- If this command has been programmed correctly, the area should fail to arm/disarm.

There are no additional events to indicate that an operator has attempted to perform a remote area function that has been disabled.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2021. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.