Integriti Intruder/Access Systems
APPLICATION NOTE

Active User Rotation Module
(AURM)

Contents

Introduction

This document provides information about the Integriti/Infiniti Active User Rotation Module (AURM) feature. Check for the latest version via the 'Installer Downloads' menu on the Inner Range website. https://www.innerrange.com//login?service=https://www.innerrange.com/login

The AURM feature allows systems to support numbers of Users far in excess of what the Controller can store locally by dynamically updating the local database from the software database when a credential unknown to the Controller is presented in the system.

Further Information can be found in the Integriti Programming Reference Manual available via the web link shown above.

Requirements

To take advantage of Active User Rotation, the following criteria must be met:
• Integriti Software Active User Rotation Module license. (P/N: 996956)
• Integriti or Infiniti controller(s)
• Connected Integriti or Infiniti Software.
• AURM configuration enabled.
• If the Integriti Controller firmware is a version prior to V20, a Controller Smart Card Level 4 Expansion licence is also required.

Active User Rotation Module

Overview

The Active User Rotation Module (AURM) feature has been designed to accommodate configurations consisting of one or many Integriti or Infiniti controllers that require more users than can fit in an Integriti/Infiniti controller's on-board database. The on-board database can accommodate up to 100,000 User records.

It works by only keeping a subset of the user programming in each controller and querying a connected software instance when an unknown credential is presented at a reader.

In this model, a user's programming will only get into a controller in one of two ways;
   1. The user has the "AURM permanent" programming option enabled.
   2. The user has presented their credential at a reader associated with that controller.

When a user presents their card/credential to a reader, the controller will search its own memory for the user record. If the user's record exists locally then the controller will grant access as per its programmed configuration. If the user does not exist then the controller will send a request to a connected Integriti or Infiniti software. The software will then search for this card/credential within its own database and update the controller with the user's record if found. If all of the user records in the controller are already full, the controller will remove the user record that has been inactive the longest to make space for the new record.

For a user who's programming is not yet in the controller, the transaction time of presenting a card to a reader and getting their information into the controller will vary depending on the latency of the network link to the software. The total time taken is approximately 3 seconds from when the card is presented, to when the user is granted or denied access.

When the AURM feature is implemented, users can no longer be deleted via the LCD Terminal regardless of the sync mode setting. It is recommended to disable the ability to edit programming from an LCD Terminal in systems utilizing the AURM feature.

PIN access.

AURM does not query the software for an unknown PIN.
This means for 'PIN only' access to succeed the user must already be in the controller's programming via one of the two methods outlined above.

AURM Permanent programming.

The "AURM permanent" programming option in a user record indicates that this user's programming should always be retained in the controller/s.
This is useful to retain important users in the controller/s so they can always be available even if the controller is not connected to the software.
e.g. System integrators/installers and personnel who perform roles such as on-site security, management, supervision, OH & S, site maintenance, etc.

This programming option should also be used for when a user has PIN access, but not card access on the site.

Administrators should be careful to only use this programming judiciously, as enabling this option for all users will exhaust the user programming space in the controller's memory.

Configuring Active User Rotation

Before starting, please ensure you are using a controller with firmware version 18.1.0 or above. To check the firmware version log onto the terminal and navigate to **[Menu], [1], [9]**.
In this menu, the down arrow **[V]** key can be used to obtain the controller serial number and IP address if required.

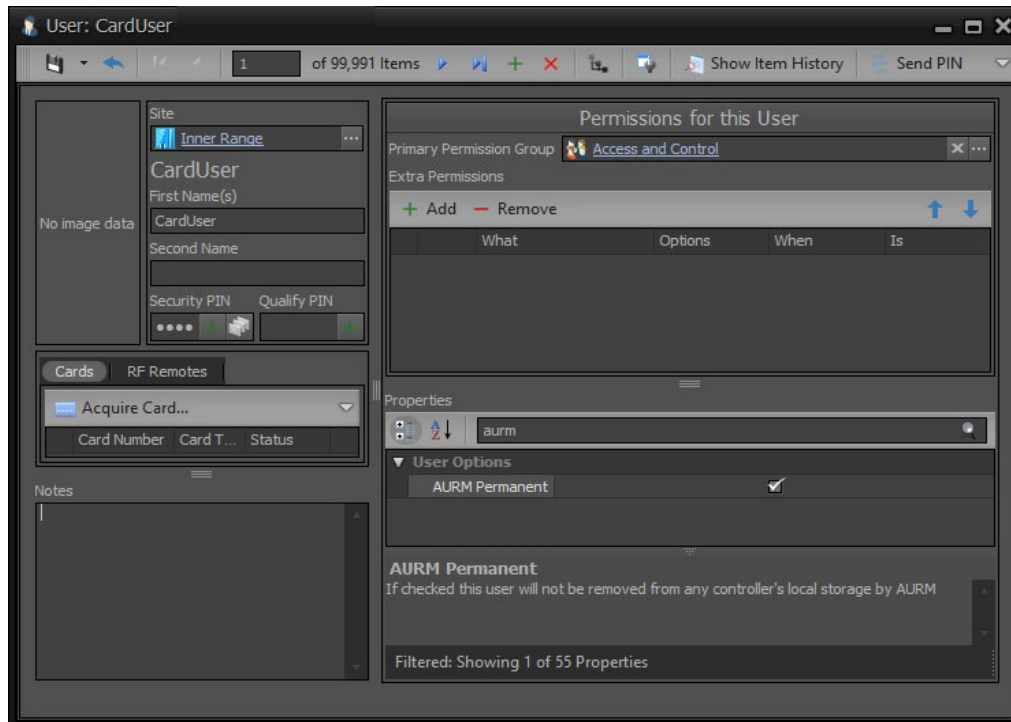Configuring the Integriti controller:

1) Ensure the controller (ISC or IAC) has V18.1.0 or later firmware installed AND a default is performed after that firmware is installed. If this is an upgrade to an existing controller, backup the Controller database first.

2) Configure AURM in the controller.
   a   Login to the terminal connected to the controller.
   b   Press; **[Menu], [7], [2], [0], [1]** – Press **[OK]** until you get to these options **..U.GAEL**
   c   User the right arrow key **[>]** and the **[9]** key to place a **"Y"** under the **"A"** to **Enable AURM**, then press **[OK]** to save and **[END]** to exit.

   Note that the "Ask PC" option in the settings for each Reader now only applies to the 'Operator Challenge' feature and is not required for AURM operation.

3) Configure AURM in the Integriti software.
   a   Edit the controller's programming to configure AURM as shown below and save the change.
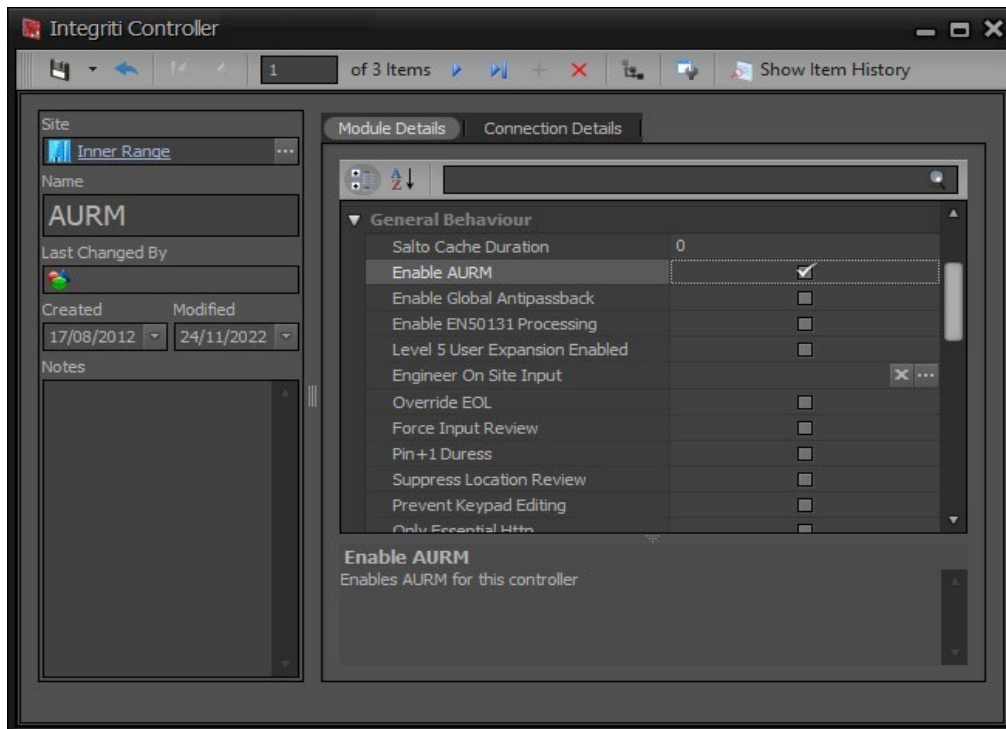
4) If not already done, enable the "AURM Permanent" option in the user programming for each user whose records are to be permanently retained in the controller/s.

5) Connect or enrol the controller to the software.

Note: The "Enable AURM" option MUST BE set via the Terminal as described in step 2 PRIOR to syncing the controller from the Integriti software.

Integriti Review

Below are typical review events for user access when using AURM.

Access granted to a valid user not previously in the Controller: *See note below		
31/08/2023 4:56:42 PM	Site 1 ISC	IR SIFER Site (56): Site =00001001(dec) Card = 00115751(dec) Issue = 00000(dec) at <I01:Rdr01> Card 115751
31/08/2023 4:56:42 PM	Site 1 ISC	Declan McManus Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Request [Card 115751]
31/08/2023 4:56:42 PM	Site 1 ISC	Declan McManus Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Response [Card 115751]
31/08/2023 4:56:42 PM	Site 1 ISC	Declan McManus location changed to Office Area
31/08/2023 4:56:42 PM	Site 1 ISC	Office Area Number of Users = 00000004 increased by Declan McManus
31/08/2023 4:56:42 PM	Site 1 ISC	Declan McManus Card Access at <I01:Rdr01> into Staff Entry Door [Card 115751]

Access denied to a valid user with no permissions, not previously in the Controller:		
31/08/2023 4:59:14 PM	Site 1 ISC	IR SIFER Site (56): Site =00001001(dec) Card = 00115752(dec) Issue = 00000(dec) at <I01:Rdr01> Card 115752
31/08/2023 4:59:14 PM	Site 1 ISC	Peter Ponsil Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Request [Card 115752]
31/08/2023 4:59:14 PM	Site 1 ISC	Peter Ponsil Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Response [Card 115752]
31/08/2023 4:59:14 PM	Site 1 ISC	Peter Ponsil Card Access at <I01:Rdr01> into Staff Entry Door Denied - Door Denied [Card 115752]

Access denied to an invalid card. (i.e. A Card not in the Software):		
31/08/2023 5:00:17 PM	Site 1 ISC	IR SIFER Site (56): Site =00001001(dec) Card = 00115753(dec) Issue = 00000(dec) at <I01:Rdr01>
31/08/2023 5:00:17 PM	Site 1 ISC	Unknown User Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Request
31/08/2023 5:00:17 PM	Site 1 ISC	Unknown User Card Access at <I01:Rdr01> into Staff Entry Door Denied - Unknown Card

Access request timed out for a valid user not previously in the Controller. (e.g. Controller is offline from the Software): †See note below		
31/08/2023 5:01:34 PM	Site 1 ISC	IR SIFER Site (56): Site =00001001(dec) Card = 00115754(dec) Issue = 00000(dec) at <I01:Rdr01> Card 115754
31/08/2023 5:01:34 PM	Site 1 ISC	Reg Dwight Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Request [Card 115754]
31/08/2023 5:01:39 PM	Site 1 ISC	Reg Dwight Card Access at <I01:Rdr01> into Staff Entry Door Denied - Software Auth. Timeout [Card 115754]

AURM Licence not enabled in the Integriti Software:		
31/08/2023 3:42:57 PM	Site 1 ISC	IR SIFER Site (56): Site =00001001(dec) Card = 00115755(dec) Issue = 00000(dec) at <I01:Rdr01> Card 115755
31/08/2023 3:42:57 PM	Site 1 ISC	Unknown User Card Access at <I01:Rdr01> into Staff Entry Door - Software Auth. Request [Unassigned Card, Card 115755]
31/08/2023 3:42:58 PM	Site 1 ISC	AURM command not processed. Reason: Not Licensed
31/08/2023 3:43:02 PM	Site 1 ISC	Unknown User Card Access at <I01:Rdr01> into Staff Entry Door Denied - Software Auth. Timeout [Unassigned Card, Card 115755]

Notes:
* Area events are only generated when an Area is assigned inside &/or outside the Door.
† These review events were uploaded to the software and the user name added in the software review after connection was reestablished.

Disclaimer:

1. The manufacturer and/or its agents take no responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from the correct or incorrect use of the system or its peripherals. The purchaser assumes all responsibility in the use of the system and its peripherals.
2. While every effort has been made to ensure the accuracy of this manual, the manufacturer assumes no responsibility or liability for any errors or omissions. Due to ongoing development, product specifications and the contents of this manual are subject to change without notice.

Please send any comments or suggestions regarding this manual to publications@innerrange.com