Integrated Control Technology

ArmorIP

Release Notes | Version 3.0.16.0

Last Published: 25-May-23 01:04 PM

Contents

Introduction

This document provides information on the new features, enhancements and resolved issues released with:

- ArmorIP version 3.0.16.0

This document contains all changes from the previously released version 3.0.14.5.

Upgrading ArmorIP

To upgrade ArmorIP, simply run the new installer and follow the prompts to install the new software version.

> If you have edited the config file for the service (ArmorIPCommService.exe.config), we recommend that you make a copy of this file before you upgrade the software to ensure that the settings are not overwritten. This file can be found in: C:\Program Files (x86)\Integrated Control Technology\ArmorIP3\Services

Upgrading to Version 3.0.16.0

There are some additional actions required when upgrading ArmorIP from a version lower than 3.0.16.0 to this version or higher.

1. This ArmorIP version requires Microsoft OBDC Driver 11 for SQL Server installed before the upgrade. You can download the driver from the Microsoft website.
2. In this version, some options that were previously configured in the config file are now available in the software UI (see page 6). If you have previously configured any of these settings in the config file you will need to configure them again in **System | Settings | Automation Software** after upgrading.
3. This version encrypts operator passwords in the database. Each operator's password will be encrypted the first time that operator logs in after the upgrade or when the password is changed. It is recommended that all operators on the system log in shortly after the upgrade.

Editing the ArmorIP Config File

Some new features in ArmorIP are not yet available in the user interface. However, you can still enable and configure these features by editing the config file for the service.

To configure settings in the config file:

1. Stop the ArmorIP services under **System | Settings | Service Control**.
2. In the File Explorer, navigate to the ArmorIP installation directory.
   By default this is C:\Program Files (x86)\Integrated Control Technology\ArmorIP3
3. Open the Services folder.
4. Open the **ArmorIPCommService.exe.config**.

   > Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

5. Locate the `<customAppSettings>` node as follows:

```
<customAppSettingsGroup>
  <customAppSettings>
    <add key="DebugEnabled" value="true"/>
  </customAppSettings>
</customAppSettingsGroup>
```

6. Enter the new settings within the **`<customAppSettings>`** node. For example:

```
<customAppSettingsGroup>
  <customAppSettings>
    <add key="DebugEnabled" value="true"/>
    <add key="CSVPollAny" value="true" />
  </customAppSettings>
</customAppSettingsGroup>
```

7. Save the config file.

8. Start the ArmorIP services.

ArmorIP Version 3.0.16.0

Feature Enhancements (3.0.16.0)

The following enhancements have been made to existing features in this release.

User Interface

- Added the license expiry date to **System | License | General**, allowing operators to see when they need to renew their license.
- Added a Poll Status indicator to the dashboard.

Automation Settings

- Added the following options under **System | Settings | Automation Software**:
  - Stop Receiver Service During Automation Software Failure
  - Max Poll Count
  - Max Retry Count
  - Require Ack Response For Ademco Okay
  - Enable Purge
  - Purge from Before (Days)

  If you have previously configured any of these options in the config file you will need to set them again in the user interface.
- Added the ability to append the channel and port to incoming messages to override the default automation settings if required. To enable this option, add the following line to the config file:
  ```
  <add key="AppendChannel" value="true" />
  ```

For more information, see Editing the ArmorIP Config File (page 4).

CSV Channels

- CSV accounts will now be automatically added when messages are received by the system with no password specified. This reduces the amount of administration required for onboarding new accounts.
- Optionally, the system can automatically add a CSV account when a message is received with a password. To enable this, add the following line to the config file:
  ```
  <add key="CSVAddWithPassword" value="true" />
  ```
- The poll event used by CSV reporting can differ by manufacturer. To enable the system to support multiple different poll events, add the following line to the config file:
  ```
  <add key="CSVPollEvent" value="181xxx, 181yyy" />
  ```
  The value is a comma-separated list of event codes which will be treated as poll events by ArmorIP. Each must include 18 (CID code), 1 (new event), then the three digit event code.
- Added an option to reset the poll timeout for the account on every event. This is because some systems will send standard messages instead of a normal poll. To enable this setting, add the following line to the config file:
  ```
  <add key="CSVPollAny" value="true" />
  ```
- Added an option to pass CSV polls through to the automation software. To enable this option, add the following line to the config file:
  ```
  <add key="CSVPollSend" value="true" />
  ```

For more information, see Editing the ArmorIP Config File (page 4).

Issues Resolved (3.0.16.0)

The following issues were resolved with this release.

- Resolved an issue where a "page not found" message was displayed when an operator clicked the Export button.
- Fixed an issue where system information was visible to guard users on the homepage.
- Resolved an issue where some automation messages would be sent in XML format regardless of which format was selected.
- Resolved an issue which caused ArmorIP to stop responding on a regular basis.
- Resolved an issue where ArmorIP could not accept multiple CSV-IP messages per connection.
- Fixed the text for some CID messages.
- Resolved an issue where CSV-IP checksums were not handled correctly.
- Resolved an issue where it was possible to create an operator with no username or password.
- Resolved an issue where ArmorIP with CSV-IP enabled would stop responding when it received invalid data .
- Resolved an issue where operator passwords were visible in the ArmorIP UI.
- Resolved an issue where operator passwords were stored in plain text in the database.

  > After the software is upgraded, passwords will remain in plain text initially. The password will be encrypted when the operator logs in for the first time after the software upgrade, or if the operator's password is changed.

- Resolved an issue with the Surgard format where the CID identification number was set to 0, while some automation software expected it to be 5. This has been corrected and will not affect existing installations.

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

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.