

Technical Reference

Testing Products Before AWID Issues RMA

Change History

Version	Date	Author	Comments
1.0	01 December 2011	L. Hickcox	First release.

It may not be easy to know what part of an access control system is causing a problem that seems to be a “bad” reader or a “bad” credential (card or tag). AWID’s goals through Technical Support are --

- (a) to prevent returning a reader or a credential that is actually working well when the customer requests a Return Material Authorization (RMA),*
- (b) to help our customers identify the actual source of trouble, and*
- (c) to assist the customer’s technical people to prevent further problems with installed products.*

We offer the following suggestions in this spirit.

Identify the Products

Try to find the model number of readers, and the part number of cards.

On **readers**, look at the labels on the back surface for model number, serial number, revision (“Rev. _”) letter, and firmware (“F/W: _”) version. The host system’s set-up programming screen may have a reader type selected.

On **credentials**, look for the part number printed on the tag (if it is printed).

Note: AWID has some **cards** that look identical but use different card technologies or protocols, and therefore they use different reader models. It is *very* important to know the exact part number of cards.

For **all products**, look for product identification in the customer’s purchase order, the supplier’s or AWID’s sales order, the packing list for the shipment, the label on the carton or bag in which AWID shipped the products, and the programming of the access control system (see the host system’s set-up screen for the reader type). In addition, AWID’s product sheets, installation instructions and manuals may give the necessary information.

Identify the Codes

Readers are simple – AWID’s readers have no programming for the codes that are used in the system. The readers are “transparent” to the code in credentials that are read on the readers. If the credential is valid for use with an AWID reader, the reader will capture the identifying code from the credential and transmit it by the interface into the system’s controller.

Cards generally have the full code information (format, facility code, and identification number) printed on the cards in small black type. The visible printed code is the same as the internal programmed code. The ID numbers are sequential.

Vehicle tags have peelable paper labels with printed code. The labels must be peeled off before adhesive tags are used.

Other sources of the code data are the customer’s purchase order, the supplier’s or AWID’s sales order, the packing list for the shipment, the label on the carton or bag in which AWID shipped the products, the programming of the access control system (see the host system’s set-up screen for the code format, or the users database screens, or a displayed or printed database report, sorted by card numbers), and handwritten lists of assignment of the credentials to employees, student or residents. Do not rely on the credentials’ supplier to have the code records.

Note: The code data are not included in AWID’s part numbers for credentials. The code data must be written out in the description for these products. Every order requires --

- (1)** Code format (most commonly the industry-standard “26-bit-STD”),
- (2)** Facility code or site code that applies to all credentials in this line of the order, and
- (3)** Starting number for the sequential range of ID numbers (also called PINs).

Most code formats do not include data fields for issue numbers, priority numbers, group numbers, or company numbers.

Readers

All of AWID's **proximity** (LF), **dual-frequency** (HF+LF), and **UA-612** (UHF) readers are self-testing. The reader should be disconnected and physically removed from its mounting for the basic isolation tests. If a compatible credential is presented to an AWID reader, it beeps and the red LED changes color to amber for one-half second, then returns to red for standby. This sequence indicates that the reader is functioning normally, and that the credential's code would be communicated to the controller. There will be one beep and one LED color change for each presentation of the credential to the reader.

The UHF **long-range** readers require the test unit from the Installation Kit for this same kind of testing, to show simply if the reader is able to read a tag and to transmit the tag's code to the system. There will be a continuing sequence of beeps and LED color changes as long as the credential is present in the reader's RF field.

Credentials

For **proximity**, **dual-frequency**, and **UA-612** readers: The self-testing readers (above) indicate if a credential is functional. First, identify a reader (same technology – same frequency) that the credential type being tested is known to work on. Then, present the credential being tested to the reader. If the reader beeps and its LED changes color briefly, that credential is functioning normally. There will be one beep and one LED color change for each presentation of the credential to the reader.

For UHF **long-range** readers: Clip the Installation Kit's test unit to the reader's wires. If the tag or card causes the test unit to beep and its LED to change color, this credential is normal. There will be a continuing sequence of beeps and LED color changes as long as the credential is present in the reader's RF field.

The most common cause of failure of ISO-type **graphics-quality cards** is improper punching of a slot for clip-strap at the edge of the cards. The person who punches the slots must refer to the instruction sheet that AWID folds and inserts inside the cover for each shipment of these cards. The card "Type" pictured on the instructions sheet *must* match the small Reference Mark that is printed at one corner of the cards. Failure to punch slots in the correct location (center of one edge of the card, at the correct inset from the edge of the card) will damage the card's antenna. Use a *good* slot-punch!

Only graphics cards may have slots or holes punched in them (in the allowed locations).

Wrong settings of the photo ID **badge printer** with graphics cards may also damage the cards. The printer should be tested, using blank cards of the same material, for correct card thickness, temperature, pressure, and rate of card feed.

To protect credentials -- They must not be subjected to bending or mechanical force that creases or deforms the material. Credentials except adhesive vehicle tags must not be left on a car's dashboard in direct sunlight on a hot day. Credentials with slots or holes must not be twisted hard on a key ring, to prevent breaking the credential at the slot or hole.

Reference

Technical Reference "Basic Isolation Tests"

This memo shows the very simple tests that let the technician use the reader as a self-testing tool to verify performance of proximity and dual-frequency readers and of their credentials. **Supplies** for basic isolation tests: the reader, a well-charged back-up battery, a DC voltmeter, a compatible credential, clip leads, and masking tape.

Instructions "LR-2000KIT Quick Installation Guide"

These instructions show how to use the test unit of the Installation Kit, to show that the UHF long-range readers are reading tags.

Technical Reference "Matching Technologies"

This is a list of every AWID reader model. Under each reader model there is a list of the credentials (cards and tags) that work with that reader model.