Advanced Card Systems Limited

Scripting Tool Manual

ACR122 NFC Reader

Advanced Card Systems Limited

## ACR122 NFC Reader

Table of Contents

1.0 Overview

The ACR122 Scripting Tool is a tool designed to work with ACR122 and this manual will help the user understand how to use this scripting tool.

The application detects the card reader that is currently connected to the computer. In the "Readers" box, it will show "CCID USB Reader" in Inserted Status – this is the ACR122 USB Device. You can click on the "Refresh" button to find the reader if there is no smart card reader detected.

Choose the smart card reader in the list of Smart Card Readers then click on "Connect" to establish connection to the card. Once successful connection has been established, it will be shown in the "Output" box

Note that this Scripting Tool will work with sending and receiving data to and from the card. However, the user will not be able to control the ACR122 Device Peripherals (LED and Buzzer). It is possible though to use the ACR122 Card Tool to control the user peripherals. To use and send APDU commands, please refer to the ACR122 API for more information.
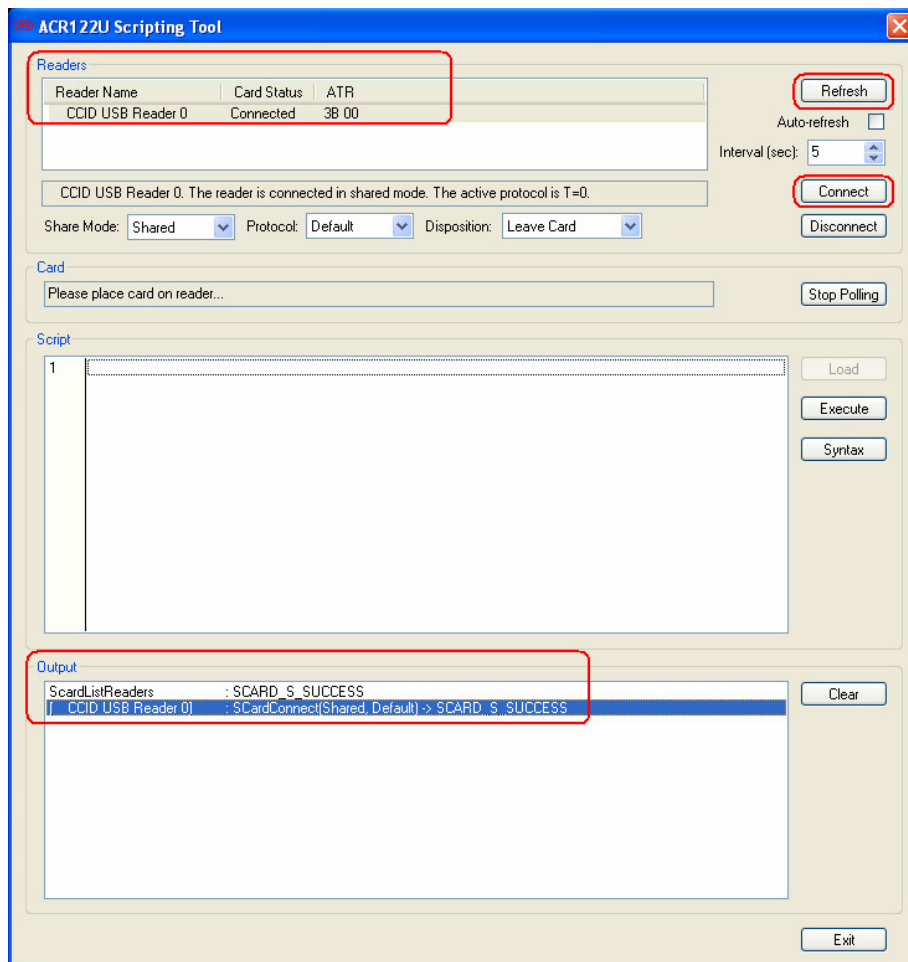
2.0 Polling for Contactless Tags

Click on the "Start Polling" button to start polling for contactless tags. After clicking on this button, it will change to "Stop Polling" then the type of card will be shown in the "Card box" as shown in the screenshot below:
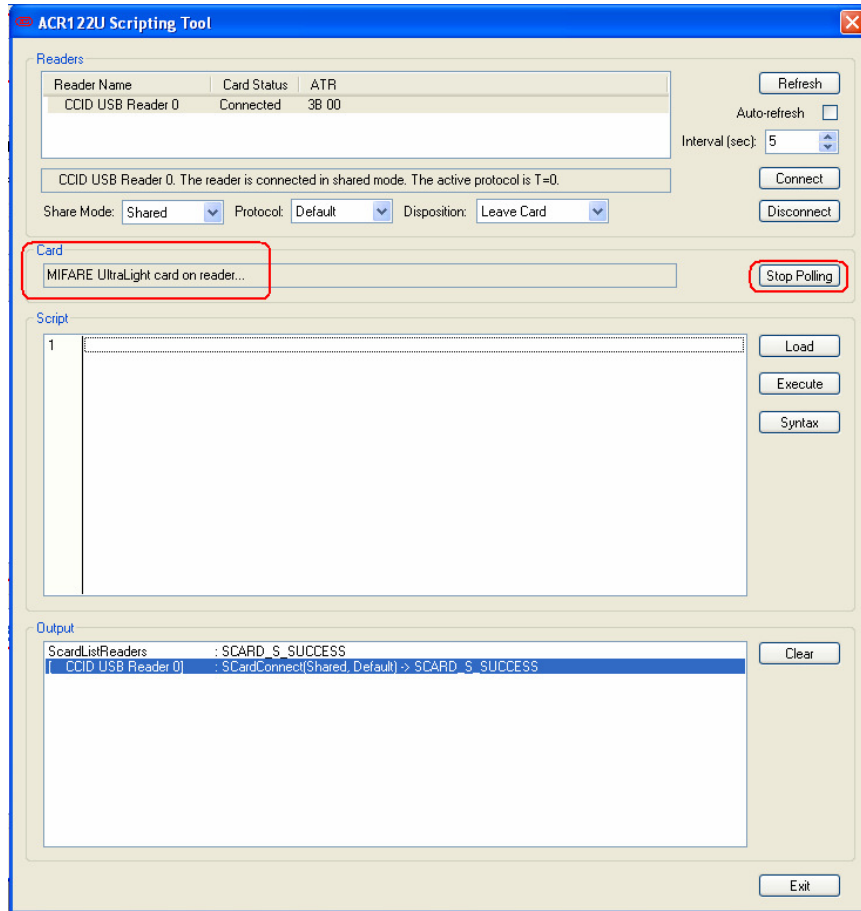
3.0   Scripting

To manually input commands in the Script box, simply click on the first line in the script box, then you can start typing the commands. Here are some simple guidelines on how to input the commands:

1. To create or add a new line, press Enter.
2. When you use ";" the succeeding characters will be treated as a comment.
3. For Direct Transmit (see API for more details) the format used is:
   Direct Transmit Command (Status Code)
   Example for Topaz Cards:
   > FF 00 00 00 05 D4 40 01 01 08 (6106)
4. For Get Response (see API for more details) the format used is:
   Get Response Command [Length of Response] (Status Code)
   > *The Length of Response is in the format of [xx xx … xx] and the number of 'xx' should be excluding the 2 status bytes
   Example:
   > FF C0 00 00 06 [xx xx xx xx] (9000)
   > FF C0 00 00 05 [xx xx xx] (9000)
   > FF C0 00 00 10 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)
   Note: The Status Code 9000 means that the operation is successful.

Remark: Please refer to the ACR122 API for more details on the commands. You can also check the Appendix for Sample Scripts.

Click on the "Syntax" button to check if there are syntax errors
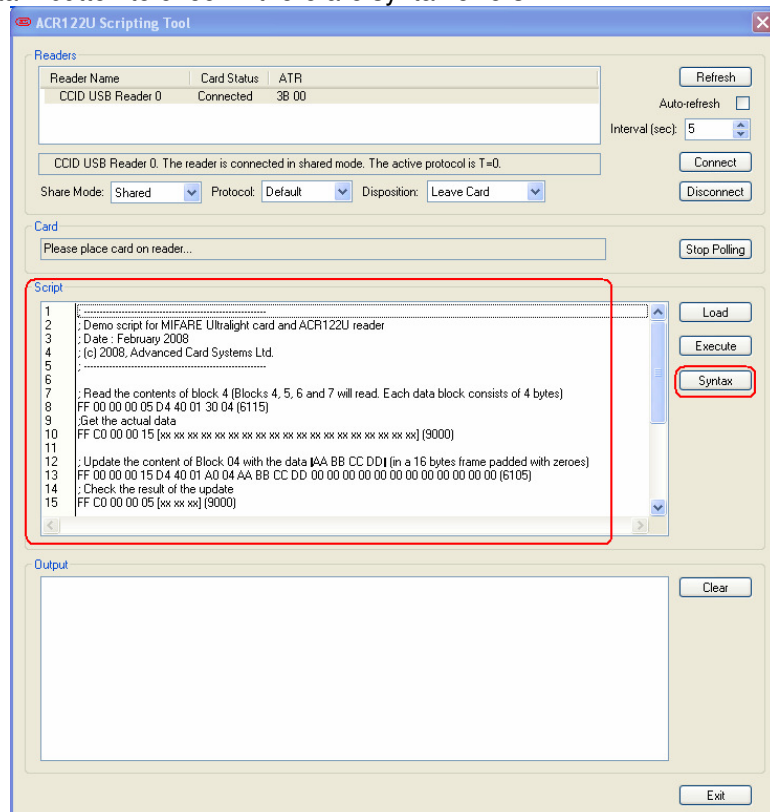

If there are no syntax errors, you can then click on the "Execute" button to execute the script. The output logs can be seen in the output box. A pop-up box will appear if there is an error. You can click the OK button when this error message is shown and correct the error. For example: "Line [N], the returned status is different than the expected status" is shown.

The application will inform you if the script has been successfully executed afterwards, you can then check the output box for the results.
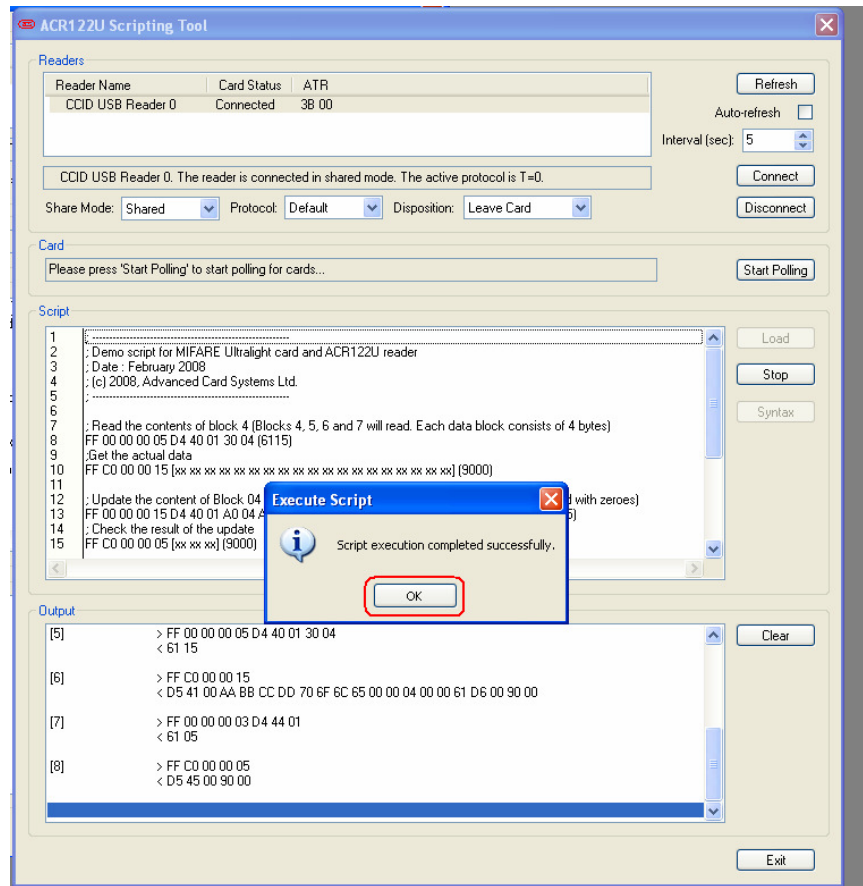
Since the Direct Transmit and Get Response APDU come in pair so the Output box is usually made up of the following:

[1]   > Direct Transmit
        < Status Code Returned by the reader (see the API for more details on the meaning of the status codes)

[2]   < Get Response
        > Response. Data returned.

Please refer to the ACR122 API for more details on the card commands and the response returned. Furthermore, there are sample scripts provided for JCOP cards, Mifare Ultralight and Topaz tags. Once the card has been placed on the reader, you can click on the "Load" button to load and run the sample scripts provided.

Appendix 1: MiFare Cards (Classic: 1K/4K)

Steps:
1. Get UID
2. Authenticate block
3. Read Block
4. Update Block
5. Read Block
6. Halt Polling (optional)

Get UID
1. Issue Polling Command. Direct Transmit: FF 00 00 00 09 D4 60 01 01 20 23 11 04 10
2. Status Code: 61 10
3. Get Response (to get the UID) FF C0 00 00 10
4. Response: D5 61 01 10 09 01 00 02 18 04 D4 D4 BE E1 90 00
   Where, 01 = One Tag is found
           10 = Tag Type = MIFARE
           09 = The Tag Info has 9 bytes in length
            Target number = 01
           SENS_RES = 00 02; SEL_RES = 18 (MIFARE 4K)
           Length of the UID = 4; UID = D4 D4 BE E1 (this changes with each card)
           Operation Finished = 90 00

For this example, we authenticate Block 04.
1. Direct Transmit: FF 00 00 00 0F D4 40 01 60 04 FF FF FF FF FF FF D4 D4 BE E1
2. Where: Block 04, KEY = FF FF FF FF FF FF, UID = D4 D4 BE E1
3. Status Code: 61 05
4. Get Response: FF C0 00 00 05
5. D5 41 [00] 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
Operation finished: 90 00

Read the contents of Block 04
1. Direct Transmit: FF 00 00 00 05 D4 40 01 30 04
2. Status Code: 61 15
3. Get Response: FF C0 00 00 15
4. Response: D5 41 [00] 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
   Block Data = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

Update the contents of Block 04:
1. Direct Transmit:
   FF 00 00 00 15 D4 40 01 A0 04 0A 0B 0C 0D 0E 0F 1A 1B 1C 1D 1E 1F 2A 2B 2C 2D
2. Status Code: 61 05
3. Get Response: FF C0 00 00 05
4. Response: D5 41 [00] 90 00

Read the contents of Block 04
1. Direct Transmit: FF 00 00 00 05 D4 40 01 30 04
2. Status Code: 61 15
3. Get Response: FF C0 00 00 15
4. Response: D5 41 [00] 0A 0B 0C 0D 0E 0F 1A 1B 1C 1D 1E 1F 2A 2B 2C 2D 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
   Block Data = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
Operation finished: 90 00

Halt Polling
1. Direct Transmit: FF 00 00 00 03 D4 44 01
2. Status Code: 61 05
3. Get Response: FF C0 00 00 05
4. Response: D5 45 [00] 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
Operation finished: 90 00

Sample Script for the MiFare Classic Card described in the previous section

Step 1: Get the UID
;GET UID first
;command 1. polling command.
FF 00 00 00 09 D4 60 01 01 20 23 11 04 10 (6110)

;command 2. get response.
FF C0 00 00 10 [xx xx xx xx xx xx xx xx xx xx **xx xx xx xx**] (9000)

Step2: Input the acquired UID then run the script below:

;command 1. authenticate Block 04
FF 00 00 00 0F D4 40 01 60 04 FF FF FF FF FF FF **D4 D4 BE E1** (6105)

;command 2. get response.
FF C0 00 00 05 [xx xx xx] (9000)

;command 3. Read the contents of Block 04
FF 00 00 00 05 D4 40 01 30 04 (6115)

;command 4. get response.
FF C0 00 00 15 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

;command 5. Update the contents of Block 04
FF 00 00 00 15 D4 40 01 A0 04 0A 0B 0C 0D 0E 0F 1A 1B 1C 1D 1E 1F 2A 2B 2C 2D (6105)

;command 6. get response.
FF C0 00 00 05 [xx xx xx] (9000)

;command 7. Read the contents of Block 04
FF 00 00 00 05 D4 40 01 30 04 (6115)

;command 8. get response.
FF C0 00 00 15 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

; command 9. halt polling.
FF 00 00 00 03 D4 44 01 (6105)

;command 10. get response.
FF C0 00 00 05 [xx xx xx] (9000)

Appendix 2: MiFare Ultralight

Steps:
1. Get UID
2. Read Page
3. Update Page
4. Read Page
5. Halt Polling (optional)

Get UID
1. Issue Polling Command. Direct Transmit: FF 00 00 00 09 D4 60 01 01 20 23 11 04 10
2. Status Code: 61 13
3. Get Response (to get the UID) FF C0 00 00 13
4. Response: D5 61 01 10 0C 01 00 44 00 07 04 C8 A0 01 F4 02 80 90 00
            where,   01 = One Tag is found
                   10 = Tag Type = MIFARE
                      0C = The Tag Info has C bytes in length
                      Target number = 01
                      SENS_RES = 00 44; SEL_RES = 00 (Ultralight)
                      Length of the UID = 7; UID = 04 C8 A0 01 F4 02 80
                      Operation Finished = 90 00

Read the contents of Page 04
1. Direct Transmit FF 00 00 00 05 D4 40 01 30 04
2. Status Code: 61 15
3. Get Response: FF C0 00 00 15
4. Response: D5 41 [00] 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
   Block Data = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16

Update the contents of Block 04:
1. Direct Transmit:
           FF 00 00 00 09 D4 40 01 A2 04 AA BB CC DD
2. Status Code: 61 05
3. Get Response: FF C0 00 00 05
4. Response: D5 41 [00] 90 00

Read the contents of Block 04
1. Direct Transmit: FF 00 00 00 05 D4 40 01 30 04
2. Status Code: 61 15
3. Get Response: FF C0 00 00 15
4. Response: D5 41 [00] AA BB CC DD 0E 0F 1A 1B 1C 1D 1E 1F 2A 2B 2C 2D 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
   Block Data = AA BB CC DD 0E 0F 1A 1B 1C 1D 1E 1F 2A 2B 2C 2D. Note that only Page 4 is updated
   Operation finished: 90 00

Halt Polling
1. Direct Transmit: FF 00 00 00 03 D4 44 01
2. Status Code: 61 05
3. Get Response: FF C0 00 00 05
4. Response: D5 45 [00] 90 00
   Where: error code [XX] and [00] = Valid, other = Error and
   Operation finished: 90 00

Sample Script for Mifare Ultralight described in the previous section

```
;GET UID
;command 1. polling command.
FF 00 00 00 09 D4 60 01 01 20 23 11 04 10 (6113)

;command 2. get response.
FF C0 00 00 13 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

;command 3: Read Page 4
FF 00 00 00 05 D4 40 01 30 04 (6115)

;command 4. get response.
FF C0 00 00 15 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

;command 5. Update page 04
FF 00 00 00 09 D4 40 01 A2 04 AA BB CC DD (6105)

;command 6. get response.
FF C0 00 00 05 [xx xx xx] (9000)

; command 7. read page 4 again.
FF 00 00 00 05 D4 40 01 30 04 (6115)

; command 8. get response.
FF C0 00 00 15 [xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

; command 9. halt polling.
FF 00 00 00 03 D4 44 01 (6105)

; get response.
FF C0 00 00 05 [xx xx xx] (9000)
```

Appendix 3: Topaz Cards

Steps:
1. Get UID
2. Read Memory Address
3. Update Memory Address
4. Read Memory Address
5. Halt Polling (optional)

Get UID
1. Issue Polling Command. Direct Transmit: FF 00 00 00 09 D4 60 01 01 20 23 11 04 10
2. Status Code: 61 0E
3. Get Response (to get the UID) FF C0 00 00 0E
4. Response: D5 61 01 04 07 01 0C 00 **EF 64 3C 00** 90 00
   Where, 01 = One Tag is found
          10 = Tag Type = MIFARE
          09 = The Tag Info has 9 bytes in length
          Target number = 01
          SENS_RES = 00 02; SEL_RES = 18 (MIFARE 4K)
          Length of the UID = 4; **UID = EF 64 3C 00**
          Operation Finished = 90 00

Read the contents of Memory Address **08**
1. Direct Transmit: FF 00 00 00 05 D4 40 01 **01 08**
2. Status Code: 61 06
3. Get Response: FF C0 00 00 06
4. Response: D5 41 [00] **18** 90 00
   Where: Error Code = [00] (no error), otherwise, error (see error code for more details)
             Response Data = **18**

Update the memory address **10** (Block 1: Byte-0) with the data AC
1. Direct Transmit: FF 00 00 00 06 D4 40 01 **53 10 AC**
2. Status Code: 61 06
3. Get Response: FF C0 00 00 06
4. Response: D5 41 [00] **AC** 90 00
   Where: Error Code = [00] (no error), otherwise, error (see error code for more details)
             Response Data = **AC**

Halt Polling
1. Direct Transmit: FF 00 00 00 03 D4 44 01
2. Status Code: 61 05
3. Get Response: FF C0 00 00 05
4. Response: D5 45 [00] 90 00
   Where: Error code [XX] and [00] = Valid, other = Error and
             Operation finished: 90 00

Sample Script for Topaz described in the previous section

```
;GET UID
;command 1. polling command.
FF 00 00 00 09 D4 60 01 01 20 23 11 04 10 (610E)

;command 2. get response.
FF C0 00 00 0E [xx xx xx xx xx xx xx xx xx xx xx xx] (9000)

; command 3. read Memory Address
FF 00 00 00 05 D4 40 01 01 08 (6106)

;command 4. get response
FF C0 00 00 06 [xx xx xx xx] (9000)

; command 5. Update Memory Address
FF 00 00 00 06 D4 40 01 53 08 AA (6106)

; command 6. get response
FF C0 00 00 06 [xx xx xx xx] (9000)

;command 7. Read Memory Address
FF 00 00 00 05 D4 40 01 01 08 (6106)

; command 8. get response
FF C0 00 00 06 [xx xx xx xx] (9000)

; command 9. halt polling
FF 00 00 00 03 D4 44 01 (6105)

; command 10. get response.
FF C0 00 00 05 [xx xx xx] (9000)
```