NCompuing RX-RDP

Firmware version 1.9.0

RELEASE NOTES

March 29, 2019

NComputing

1875 SOUTH GRANT STREET | SUITE 570 | SAN MATEO | CALIFORNIA 94402

PRODUCT RELEASE NOTES: NCOMPUTING RX-RDP FIRMWARE, VERSION 1.9.0

Product: NComputing RX-RDP firmware

Version: 1.9.0

Device configuration version: 13

Supported hardware:

- NComputing RX-RDP thin clients

Supported virtual desktop environments:

- Microsoft Remote Desktop Services:
    - Microsoft Windows Server systems:
        - Windows Server 2008 R2
        - Windows Server 2012 R2
        - Windows Server Multipoint Server 2012
        - Windows Server 2016
        - Windows Server 2016 (Multipoint Services)
        - Windows Server 2019
    - Microsoft Windows desktop systems:
        - Windows 7
        - Windows 8.1
        - Windows 10
- NComputing VERDE VDI 8.2.1 or higher version

Supported device management systems:

- NComputing PMC 1.1, PMC 1.5, PMC 2.0

Contained NComputing Pi Zero SDA firmware:

- 0.9.8

This document contains important information. Please read the entire document to ensure that your deployment process goes smoothly.

ABOUT THE PRODUCT:

NComputing RX-RDP devices are thin client devices supporting connections to Microsoft Remote Desktop Services deployments and Microsoft Windows desktop systems with the Remote Desktop feature enabled, as well as to NComputing VERDE VDI systems.

ABOUT THIS RELEASE:

1.9.0 is an RX-RDP firmware release which replaces the 1.6.1 firmware. The 1.9.0 firmware introduces numerous new product features as well as fixes for multiple issues affecting previous firmware versions.

NEW FEATURES AND IMPROVEMENTS:

Following are the new product features introduced in RX-RDP firmware version 1.9.0:

- Support for RemoteApp and Desktop connections.
- Support for native (functional) redirection of printers in RDP sessions.
- Support for VNC screen shadowing.
- Ability to setup a desktop wallpaper.
- Enhanced single- and multi-touch screen support.
- Calibration tool for touch screen monitors.
- Enhanced vCAST Web Streaming with Vimeo support.
- Enhanced vCAST VLC Media Streaming with NComputing SDA support.
- PMC connection status display.

Other improvements introduced in firmware version 1.9.0:

- Ability to select screen saver action.
- Lock-up of the ‘Domain’ field on the logon screen if a domain name is pre-configured in Kiosk Mode settings.
- Additional splash screen at the early stage of device boot-up process.
- Ability to configure ‘Custom RDP parameters’ for RDP connections in VERDE VDI Client mode.
- Improved behavior of the logon screen in VERDE VDI Client mode when the ‘Allow using custom VERDE Connection Brokers’ option is enabled.
- Cosmetic changes and spelling improvements in the GUI.

ISSUES FIXED IN THIS VERSION:

The following RX-RDP firmware issues have been fixed in version 1.9.0:

- RXRDP-282 – GUI termination due to receiving the SIGUSR1 signal just after boot.
- RXRDP-173 – Enabling RemoteFX while vCAST is being used causes artifacts in RDP sessions.

KNOWN ISSUES:

Following are the known RX-RDP firmware issues still existing in version 1.9.0:

- RXRDP-276 – Inability to use VNC if it was turned on at the same time when reconfiguring screen resolution.
  Workaround: The issue will not happen when screen resolution change and enabling VNC will be performed separately.
- RXRDP-273 – RemoteApp: All icons presented by task-switcher are identical.
- RXRDP-264 – RemoteApp: If user tries to launch an application that was unpublished after being enumerated on device, no message is displayed.
  Workaround: Clicking the 'Refresh' button re-enumerates the published RemoteApp applications and desktops.
- RXRDP-261 – Artifacts on the screen when dragging RemoteApp windows.
- RXRDP-259 – Mouse pointer shape does not change when working with RemoteApp programs.
- RXRDP-162 – Booting issue: In some rare cases after powering on the RX-RDP device does not display GUI - only black screen with mouse pointer.
  Workaround: Rebooting the device resolves the issue.
- RXRDP-146 - Generic USB redirection doesn't work for printers in RDP sessions.
  Workaround: The upcoming NComputing SuperRDP software installed on the Remote Desktop Session Host resolves the issue.
- RXRDP-131 – vCAST Web streaming does not work on Windows 10 when USB headset was connected before starting Chrome browser.
- RXRDP-127 – VERDE VDI Client mode: Webcam does not work.
- RXRDP-68 – RDP Client: Kiosk mode application auto-start does not work in RDP sessions.
  Workaround: Please see the additional note below.
- RXRDP-44 – RDP Client: File copy process may get stuck for long time at 0% when copying larger files (several dozen kB) to redirected FAT32 USB drives.

FIRMWARE UPDATE INSTRUCTIONS:

The firmware update could take anywhere between 5-10 minutes. Please do not turn off your device during this time. Once the firmware update is complete, the device will reboot automatically.

- **Updating firmware from an FTP or web server**

  The device firmware can be updated manually from the Setup GUI with a firmware update package uploaded to an FTP or web server:

  - Upload the ‘rx-rdp-1.9.0.upd’ firmware update package file into your FTP or web server.
  - On the RX-RDP device open the Setup GUI and go to the ‘Support’ section.
  - Enter the FTP or HTTP URL of the firmware update package and click the ‘Update’ button.
  - Alternatively, user can use the following NComputing’s web URL to download and install this version of firmware directly to the RX-RDP device: http://firmware.ncomputing.com/RX-RDP/rx-rdp-1.9.0.upd

  Once the device finishes downloading the firmware update package the firmware update process will start and will take a few minutes. The process should not be interrupted. Especially when the process reaches 76% the progress bar will stop moving for a longer while. This is normal and the update will continue once the background tasks are completed. Firmware update will end with a device reboot.

- **Updating firmware from PMC**

  The device firmware can be updated from supported version of PMC. Follow the below steps to perform the firmware update on remote RX-RDP devices:

  - Logon to PMC as a user with administrative privileges, open the Menu, go to ‘Administration > Files’.
  - Select ‘Firmware Image’ as file type.
  - Click the ‘Choose file’ button and select the ‘rx-rdp-1.9.0.upd’ file.
  - Click the ‘Upload file’ button to upload the firmware package.
  - Open the Menu, go to ‘Device Management > Firmware Updates’.
  - Select the ‘rx-rdp-1.9.0.upd’ firmware package.
  - Select the device group.
  - Select the devices which should receive the firmware update.
  - Schedule the update date and time, or opt to update now.
  - Click the ‘Apply’ button.

  If ‘Update now’ was chosen then within 30 seconds the device will receive a request to initiate the firmware update. For remote devices the process can be followed by observing the Audit Events log on Dashboard. The firmware update process will take a few minutes and should not be interrupted. Especially when the process reaches 76% the progress bar will stop moving for a longer while. This is normal and the update will continue once the background tasks are completed. Firmware update will end with a device reboot.

ADDITIONAL NOTES:

- **Managing the RX-RDP devices from PMC 2.0**

  Each RX-RDP device comes with a perpetual license of PMC software and first-year complimentary software maintenance update (AMP for RX-RDP).

  After the first-year complimentary AMP for RX-RDP has expired then the RX-RDP device can only receive firmware updates from PMC. Furthermore, extended AMP for RX-RDP licenses must be purchased and allocated to each RX-RDP device to allow PMC to push firmware update.

- **Managing the RX-RDP devices with 1.9.0 firmware from PMC 1.1 and 1.5**

  The RX-RDP 1.9.0 firmware uses version 13 of the device configuration. To be able to manage the RX-RDP devices running firmware using this configuration version a set of schema files describing this configuration version must be uploaded to PMC 1.1 and 1.5. Without that PMC 1.1 and 1.5 will only be able to show the device on the device list, but will not allow editing the device (or device profile) settings for configuration version 13.

  Follow the below steps to upload to PMC the schema files for RX-RDP configuration version 13:

  - Logon to PMC as a user with administrative privileges, open the Menu, go to 'Administration > Device Configurations'.
  - Click the 'Choose file' button and select the ZIP file (for PMC 1.1) or PCU file (for PMC 1.5) containing the version 13 schema files.
  - Click the 'Upload file' button to upload the schema files.

  After completing the above actions PMC 1.1 and 1.5 will become fully able to manage the RX-RDP devices running firmware using the configuration version 13 (e.g. the 1.9.0 firmware).

- **PMC server auto-discovery**

  To automate the PMC server discovery the DHCP option 207 can be used. This DHCP option should provide a string value containing the URL in form of 'https://<PMC_address>', like: 'https://pmc.company.local', or: 'https://192.168.10.12'.

- **RDP Client connection configuration**

  The RX300 firmware version 3.4.0 introduces support for RemoteApp and Desktop Connections. The parameters necessary for the RDP Client connection are different depending on the RemoteApp support being enabled or not.

  - RemoteApp and Desktop Connections not enabled: The RDP Client connects directly to specified Remote Desktop Session Host.
  - RemoteApp and Desktop Connections enabled: The RDP Client first communicates with the specified Remote Desktop Web Access server (which cooperates with Remote Desktop Connection Broker; both must exist in the RDS deployment). The Remote Desktop Web Access server URL must be specified in RDP Client connection configuration. This URL can be in simplified or full form, e.g.
    - 192.168.50.7 – will be expanded to: https://192.168.50.7/RDweb

        - rdwa – will be expanded to: https://rdwa/RDWeb
        - rdwa.company.local – will be expanded to: https://rdwa.company.local/RDWeb
        - https://rdwa.company.local/RDWeb - will be used as is.

- **Using custom parameters for RDP connections**

  The 1.9.0 firmware allows specifying custom parameters for RDP connections. Please refer to FreeRDP documentation (https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface) for the information about supported parameters. If multiple custom parameters must be specified then they should be separated by the ";" (semicolon) character.

- **Enabling fonts smoothing (ClearType) in RDP connections in VERDE VDI Client mode**

  The font smoothing in VERDE VDI RDP sessions can be enabled by adding the following parameter to 'Custom RDP parameters' of VERDE VDI connection settings:

  +fonts

  Note: Fonts smoothing is enabled by default in RDP Client mode connections.

- **Displaying window contents while dragging in RDP connections in VERDE VDI Client mode**

  The 'Show window contents while dragging' function can be enabled in the VERDE VDI RDP sessions by adding the following parameter to 'Custom RDP parameters' of VERDE VDI connection settings:

  +window-drag

  Note: In RDP Client mode connections the window contents will be always displayed while dragging.

- **vCAST support in RDP sessions**

  Support for vCAST Web Streaming and vCAST VLC Media Streaming in RDP sessions started from RX-RDP devices requires installation of the NComputing SuperRDP software on the Remote Desktop machine.

- **Supported Secondary Display Adapters**

  This firmware supports following Secondary Display Adapter (SDA) options:

    - **NComputing Raspberry Pi Zero (Pi0) SDA**

      Secondary Display Adapters based on Raspberry Pi Zero are supported.

    - **DisplayLink SDA**

      Secondary Display Adapters based on DisplayLink DL-1x0 and DL-1x5 chipsets are supported. DisplayLink adapters with following USB vendor ID and product ID (VID:PID) are supported:

        - 17e9:0290
        - 17e9:0351
        - 17e9:030b
        - 17e9:0377
        - 17e9:0378
        - 17e9:0379

        - 17e9:037a
        - 17e9:037b
        - 17e9:037c
        - 17e9:037d
        - 17e9:410a
        - 17e9:430a
        - 17e9:4312

    Device must be rebooted to become properly configured after physically connecting or disconnecting any DisplayLink adapter. Hot-plugging the DisplayLink adapters is not supported.

    - **NComputing N-series SDA**
      Secondary Display Adapters based on SMSC/Microchip UFX6000 chip, previously offered by NComputing for the N-series devices, are supported and can be used to extend the full-screen UXP and RDP desktop sessions.

- **Secondary Display Adapters limitations**

  The Secondary Display Adapters are mainly purposed to allow desktop extension in full-screen vSpace (UXP) and RDP desktop sessions. Certain limitations apply to different scenarios as listed in the following table:

Scenario	Desktop extension to:		
	Pi0 SDA	DisplayLink SDA	N-series SDA
Local device GUI	Not supported	Supported	Not supported
VERDE VDI, UXP session	Supported	Not supported	Supported
VERDE VDI, RDP session	Supported	Supported	Supported
RDP full-screen desktop session	Supported	Supported	Supported
RDP RemoteApp application session	Not supported	Supported	Not supported

- **vCAST limitations**
  The vCAST Web Streaming and vCAST Media Streaming technologies require the client device to use optimized (hardware-accelerated) display drawing to work properly. As not every Secondary Display Adapter is technically capable to offer the necessary drawing method following limitations apply to vCAST:

Scenario	vCAST on:			
	Primary display	Pi0 SDA	DisplayLink SDA	N-series SDA
VERDE VDI, UXP session	Supported	Supported	N/A	Not supported
VERDE VDI,	Supported	Supported	Not	Not

RDP session			supported	supported
RDP full-screen desktop session	Supported	Supported	Not supported	Not supported
RDP RemoteApp application session	Not supported	Not supported	Not supported	Not supported

N/A – not applicable

Note: For vCAST support in RDP sessions the SuperRDP software must be installed on the remote machine.

The vCAST Media Streaming technology can only offload to the client device H.264-encoded media contents. For other formats the VLC player needs to have the 'Windows GDI' video output selected under Video output settings.

- **VNC screen shadowing limitations**

  The VNC screen shadowing feature is mainly purposed for remote viewing and controlling the local device GUI. When the device is running a terminal session some limitations apply and the screen shadowing might end-up with a black screen being displayed in VNC viewer application. This happens because of the optimized (hardware-accelerated) display drawing methods used in some scenarios. The display data bypasses the traditional frame buffer then and can't be shadowed with VNC.

Scenario	Primary screen shadowing	Secondary screen shadowing
Local device GUI, no SDA connected	Supported	N/A
Local device GUI, Pi0 SDA connected	Supported	N/A
Local device GUI, DisplayLink SDA connected	Supported	Supported
Local device GUI, N-series SDA connected	Supported	N/A
VERDE VDI (UXP) session, no SDA connected	Not supported	N/A
VERDE VDI (UXP) session, Pi0 SDA connected	Not supported	Not supported
VERDE VDI (UXP) session, DisplayLink SDA connected	Not supported	N/A
VERDE VDI (UXP) session, N-series SDA connected	Not supported	Not supported
RDP full-screen desktop session, no SDA connected	Not supported	N/A
RDP full-screen desktop session, Pi0 SDA connected	Not supported	Not supported

Scenario	Primary screen shadowing	Secondary screen shadowing
RDP full-screen desktop session, DisplayLink SDA connected	Supported	Supported
RDP full-screen desktop session, N-series SDA connected	Not supported	Not supported
RDP RemoteApp application session, no SDA connected	Supported	N/A
RDP RemoteApp application session, Pi0 SDA connected	Supported	N/A
RDP RemoteApp application session, DisplayLink SDA connected	Supported	Supported
RDP RemoteApp application session, N-series SDA connected	Supported	N/A

N/A – not applicable

- **Server CPU load in RDP sessions with RemoteFX enabled**

  Enabling the RemoteFX feature for Remote Desktop connections greatly improves user experience by providing very good GUI performance. This is thanks to optimized algorithms used to encode the areas of the session screen which contain dynamically changing contents (like videos or animations). Ideally the screen encoding on the server side should be accelerated by supported graphics cards. Leveraging server CPUs for RemoteFX screen encoding can cause high load and effectively limit the per-server user density.

- **Kiosk mode application auto-start**

  Latest versions of Windows operating systems favor RemoteApp publishing (which is supported in the 1.9.0 firmware) and do not allow launching applications with program paths specified on the client side. This functionality can be re-enabled by modifying the Windows registry:

  Registry key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\TSAppAllowList
  Registry value: REG_DWORD fDisabledAllowList
  Registry value data: 1

  Registry key: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server
  Registry value: REG_DWORD HonorLegacySettings
  Registry value data: 1

- **Generic USB redirection of peripheral devices in RDP sessions on Windows Server 2016/2019 and Windows 10**

  In Windows Server 2016/2019 and Windows 10 the 'Do not allow supported Plug and Play device redirection' Group Policy setting is enabled by default (when not configured), which prevents the Generic USB redirection of the peripheral devices to the above mentioned operating systems. This Group Policy setting can be found under 'Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection'. To be able to use the Generic USB redirection of RX-RDP peripheral devices in Remote Desktop sessions running on operating systems mentioned in this note this policy must be explicitly disabled. In Windows Server 2012 R2, Windows 8.1 and older Windows server and desktop operating systems the Remote Desktop Services by default allows the redirection of supported plug and play devices, thus the ‘Do not allow supported Plug and Play device redirection’ Group Policy setting does not need to be altered.

- **Native (functional) redirection of printers in RDP sessions**

  Following are the topics to consider when planning to use the native/functional redirection of printers in RDP sessions:

  - Locally connected USB printers and network printers supporting the JetDirect protocol (also known as RAW or AppSocket) can be used with native redirection.
  - Low-cost GDI printers should be avoided, as they may not work properly. More advanced printers understanding the PCL, PostScript, and/or other high-level page description languages are advisable and should work.
  - Functional redirection of printers requires the installation of appropriate Windows printer driver on the remote machine running the RDP session. The literally spelled name of the Windows printer driver must be entered in the ‘Windows printer driver name’ when adding a printer for native redirection.
  - The ‘Windows printer driver name’ often matches the ‘USB printer identification’ string obtained from the USB printer during the detection process, but this is not a general rule. For some USB printers the ‘Windows printer driver name’ automatically populated when detecting the printer will have to be edited to match the real name of the Windows printer driver installed on the remote server.
  - The ‘class 3’ drivers for Windows x64 architecture should be selected for installation. ‘Class 4’ drivers are known to cause issues with functional redirection of printers.
  - The list of Windows printer drivers installed on a Windows machine (with the information about class and architecture) can be obtained with the following command executed in Command Prompt:

    ```
    wmic /NameSpace:\\Root\CIMV2 path Win32_PrinterDriver GET Name
    ```

- **Native (functional) redirection of smart card readers in RDP and UXP sessions**

  Functional redirection of smart card readers leverages the PC/SC daemon and smart card reader drives embedded in the device firmware. Drivers for following smart card readers are present in the firmware and the following readers should work:

  Readers supported by the ACS driver:

  - ACS ACR32 ICC Reader
  - ACS ACR3201 ICC Reader
  - ACS ACR33U-A1 3SAM ICC Reader
  - ACS ACR33U-A2 3SAM ICC Reader
  - ACS ACR33U-A3 3SAM ICC Reader
  - ACS ACR33U 4SAM ICC Reader
  - ACS ACR38U-CCID

- ACS ACR3801
- ACS ACR39U ICC Reader
- ACS ACR39K ICC Reader
- ACS ACR39T ICC Reader
- ACS ACR39F ICC Reader
- ACS ACR39U ID1 Card Reader
- ACS ACR39U-SAM ICC Reader
- ACS ACR3901 ICC Reader
- ACS ACR83U
- ACS ACR85 PINPad Reader
- ACS ACR88U
- ACS ACR89 ICC Reader
- ACS ACR89 Dual Reader
- ACS ACR89 FP Reader
- ACS ACR100 ICC Reader
- ACS ACR101 ICC Reader
- ACS ACR102 ICC Reader
- ACS ACR122U
- ACS ACR1222 1SAM PICC Reader
- ACS ACR1222 1SAM Dual Reader
- ACS ACR1222 Dual Reader
- ACS ACR1222 1SAM PICC Reader
- ACS ACR1222 3S PICC Reader
- ACS ACR123 3S Reader
- ACS ACR123 PICC Reader
- ACS ACR123US_BL
- ACS ACR125 nPA plus
- ACS ACR1251 1S CL Reader
- ACS ACR1251 CL Reader
- ACS ACR122U
- ACS ACR1251U-C Smart Card Reader
- ACS ACR1251U-C Smart Card Reader
- ACS ACR1251K Dual Reader
- ACS ACR1251 1S Dual Reader
- ACS ACR1251 Reader
- ACS ACR1251 CL Reader
- ACS ACR1252 1S CL Reader
- ACS ACR1252 CL Reader
- ACS ACR1252 USB FW_Upgrade v100
- ACS ACR1252U BADANAMU MAGIC READER
- ACS ACR1252IMP 1S CL Reader
- ACS ACR1255U-J1 PICC Reader
- ACS ACR1256U PICC Reader
- ACS ACR1261 1S Dual Reader
- ACS ACR1261 CL Reader
- ACS ACR128U
- ACS ACR1281 1S Dual Reader
- ACS ACR1281 CL Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 PICC Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 PICC Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 2S CL Reader
- ACS ACR1281 1S PICC Reader
- ACS ACR1281U-K PICC Reader
- ACS ACR1281U-K Dual Reader
- ACS ACR1281U-K 1S Dual Reader
- ACS ACR1281U-K 4S Dual Reader

- ACS ACR1283 4S CL Reader
- ACS ACR1283 CL Reader
- ACS ACR1283U FW Upgrade
- ACS ACR1311 PICC Reader
- ACS AET62 PICC Reader
- ACS AET62 1SAM PICC Reader
- ACS AET65 ICC Reader
- ACS AMR220 Reader
- ACS APG8201
- ACS APG8201-B2
- ACS APG8201Z
- ACS APG8201Z
- ACS CryptoMate64
- ACS CryptoMate (T1)
- ACS CryptoMate (T2)
- ACS ACR38U
- ACS ACR38U-SAM
- ACS AET65 1SAM ICC Reader
- ACS CryptoMate
- IRIS SCR21U

CCID-compliant readers:

- Access IS ePassport Reader
- Access IS NFC Smart Module
- ACS ACR 38U-CCID
- ACS ACR101 ICC Reader
- ACS ACR122U PICC Interface
- ACS ACR1251 Dual Reader
- ACS ACR1252 Dual Reader
- ACS ACR1255U-J1
- ACS ACR3901U ICC Reader
- ACS ACR39U ICC Reader
- ACS APG8201 PINhandy 1
- ACS APG8201 USB Reader
- ACS CryptoMate (T2)
- ACS CryptoMate64
- ActivCard ActivCard USB Reader V2
- ActivIdentity Activkey_Sim
- ActivIdentity USB Reader V3
- AK910 CKey
- AK910 IDONE
- Aktiv Co., ProgramPark Rutoken Magistra
- Aktiv PINPad Ex
- Aktiv PINPad In
- Aktiv Rutoken ECP
- Aktiv Rutoken lite
- Aktiv Rutoken PINPad 2
- Aladdin R.D. JaCarta
- Aladdin R.D. JaCarta Flash
- Aladdin R.D. JaCarta LT
- Aladdin R.D. JaCarta U2F (JC602)
- Aladdin R.D. JCR-770
- Aladdin R.D. JC-WebPass (JC600)
- Alcor Micro AU9520
- Alcor Micro AU9522
- Alcor Micro AU9560
- ANCUD CCID USB Reader & RNG
- appidkey GmbH ID100L-USB-SC-Reader
- appidkey GmbH ID50 -USB

- appidkey GmbH ID60-USB
- ASK-RFID CPL108
- Athena ASE IIIe
- Athena ASEDrive IIIe Combo Bio PIV
- Athena ASEDrive IIIe KB
- Athena ASEDrive IIIe KB Bio PIV
- Athena IDProtect Flash
- Athena IDProtect Key v2
- ATMEL AT90SCR050
- ATMEL AT90SCR100
- ATMEL AT91SC192192CT-USB ICCD reader
- ATMEL AT91SO CCID Smart Card Reader
- ATMEL AT98SC032CT-USB
- ATMEL VaultIC420 Smart Object
- ATMEL VaultIC440
- ATMEL VaultIC460
- Avtor SC Reader 371
- Avtor SecureToken
- Axalto Reflex USB v3
- BIFIT iBank2Key
- BIFIT iToken
- BIFIT USB-Token iBank2key
- Bit4id CKey4
- Bit4id cryptokey
- Bit4id Digital DNA Key
- Bit4id iAM
- Bit4id miniLector
- Bit4id miniLector-s
- Bit4id tokenME FIPS v3
- BLUTRONICS BLUDRIVE II CCID
- Broadcom Corp 5880
- C3PO KBR36
- C3PO LTC31 v2
- C3PO LTC32
- C3PO LTC36
- C3PO LTC3x USB
- C3PO TLTC2USB
- CASTLES EZCCID Smart Card Reader
- CCB eSafeLD
- charismathics plug'n'crypt CCID token
- Cherry GmbH SmartBoard XX1X
- Cherry GmbH SmartBoard XX33
- Cherry GmbH SmartBoard XX44
- Cherry GmbH SmartTerminal ST-1275
- Cherry GmbH SmartTerminal ST-2xxx
- Cherry GmbH SmartTerminal XX1X
- Cherry GmbH SmartTerminal XX44
- Cherry KC 1000 SC
- Cherry KC 1000 SC Z
- Cherry KC 1000 SC/DI
- Cherry KC 1000 SC/DI Z
- Cherry Smart Card Reader USB
- Cherry Smartcard Keyboard G87-1xx44
- Cherry SmartTerminal XX44
- Cherry TC 1300
- Chicony HP USB Smartcard CCID Keyboard JP
- Chicony HP USB Smartcard CCID Keyboard KR
- Chicony USB Smart Card Keyboard
- COVADIS ALYA

- COVADIS Auriga
- COVADIS VEGA-ALPHA
- Dell Dell Smart Card Reader Keyboard
- Dell keyboard SK-3106
- DUALi DE-620 Combi
- DUALi DRAGON NFC READER
- eID_R6 001 X8
- Elatec TWN4 SmartCard NFC
- Elatec TWN4/B1.06/CPF3.05/S1SC1.32/P (Beta 3)
- ESMART Token GOST
- Eutron Card Reader
- Eutron CryptoIdentity CCID
- Eutron Digipass 860
- Eutron Smart Pocket
- Feitian 502-CL
- Feitian bR301
- Feitian bR500
- Feitian eJAVA Token
- Feitian ePass2003
- FEITIAN iR301
- Feitian R502
- Feitian SCR301
- Feitian Technologies FT SCR310
- Feitian VR504 VHBR Contactless & Contact Card Reader
- Free Software Initiative of Japan Gnuk
- FT CCID
- FT CCID KB
- FT ePass2003Auto
- FT U2F CCID
- FT U2F CCID KB
- Fujitsu Siemens Computers SmartCard Keyboard USB 2A
- Fujitsu Siemens Computers SmartCard USB 2A
- Fujitsu Smartcard Reader D323
- FujitsuTechnologySolutions GmbH Keyboard KB100 SCR
- FujitsuTechnologySolutions GmbH Keyboard KB100 SCR eSIG
- FujitsuTechnologySolutions GmbH Smartcard Keyboard G87-914x
- FujitsuTechnologySolutions GmbH SmartCase KB SCR eSIG
- GEMALTO CT1100
- Gemalto EZIO CB+
- Gemalto Ezio Shield
- Gemalto Ezio Shield Branch Reader
- Gemalto Ezio Shield Secure Channel
- Gemalto Gem e-Seal Pro USB Token
- Gemalto GemCore SIM Pro Smart Card Reader
- Gemalto GemPC Express
- Gemalto Gemplus USB SmartCard Reader 433-Swap
- Gemalto Hybrid Smartcard Reader
- Gemalto IDBridge K3000
- Gemalto PC Twin Reader
- Gemalto PDT
- Gemalto Prox Dual USB PC Link Reader
- Gemalto Prox SU USB PC LinkReader
- Gemalto SA .NET Dual
- Gemalto Smart Enterprise Guardian Secure USB Device
- Gemalto USB GemPCPinpad SmartCard Reader
- Gemalto USB Shell Token V2
- Gemplus GemCore POS Pro Smart Card Reader
- Generic MultiCard Device
- Generic Smart Card Reader Interface

- Generic USB Smart Card Reader
- Generic USB2.0-CRW
- German Privacy Foundation Crypto Stick v1.2
- Giesecke & Devrient GmbH Star Sign Card Token 350 (ICCD)
- Giesecke & Devrient GmbH Star Sign Card Token 550 (ICCD)
- Giesecke & Devrient GmbH StarSign Crypto USB Token
- Giesecke & Devrient GmbH StarSign CUT S
- GIS Ltd SmartMouse USB
- GoldKey Security PIV Token
- HDZB uKeyCI800-K18
- Hewlett Packard HP USB Smartcard CCID Keyboard
- Hewlett Packard MFP Smart Card Reader
- Hewlett-Packard Company HP USB CCID Smartcard Keyboard
- Hewlett-Packard Company HP USB Smart Card Keyboard
- Hewlett-Packard HP lt4112 Gobi 4G Module
- HID Global OMNIKEY 3x21 Smart Card Reader
- HID Global OMNIKEY 5022 Smart Card Reader
- HID Global OMNIKEY 5122 Dual
- HID Global OMNIKEY 5122 Smartcard Reader
- HID Global OMNIKEY 5422 Smartcard Reader
- HID Global OMNIKEY 6121 Smart Card Reader
- HID Global veriCLASS Reader
- HID OMNIKEY 5025-CL
- HID OMNIKEY 5127 CK
- HID OMNIKEY 5326 DFR
- HID OMNIKEY 5427 CK
- Hitachi, Ltd. Hitachi Biometric Reader
- Hitachi, Ltd. Hitachi Portable Biometric Reader
- id3 Semiconductors CL1356A_HID
- id3 Semiconductors CL1356T
- Identiv @MAXX ID-1 Smart Card Reader
- Identiv @MAXX Light2 token
- Identiv CLOUD 2980 F Smart Card Reader
- Identiv SCR3500 A Contact Reader
- Identiv SCR3500 B Contact Reader
- Identiv SCR35xx USB Smart Card Reader
- Identiv uTrust 2900 R Smart Card Reader
- Identiv uTrust 2910 R Smart Card Reader
- Identiv uTrust 2910 R Taglio SC Reader
- Identiv uTrust 3512 SAM slot Token
- Identiv uTrust 3522 embd SE RFID Token
- Identiv uTrust 3700 F CL Reader
- Identiv uTrust 3701 F CL Reader
- Identiv uTrust 4701 F Dual Interface Reader
- Identive CLOUD 2700 F Smart Card Reader
- Identive CLOUD 2700 R Smart Card Reader
- Identive CLOUD 4000 F DTC
- Identive CLOUD 4500 F Dual Interface Reader
- Identive CLOUD 4510 F Contactless + SAM Reader
- Identive SCT3522CC token
- Identive Technologies Multi-ISO HF Reader - USB
- IID AT90S064 CCID READER
- IIT E.Key Almaz-1C
- IIT E.Key Crystal-1
- InfoThink IT-102MU Reader
- INGENICO Leo
- Ingenico WITEO USB Smart Card Reader
- Inside Secure AT90SCR050
- Inside Secure AT90SCR100

- Inside Secure AT90SCR200
- INSIDE Secure VaultIC 405 Smart Object
- Inside Secure VaultIC 420 Smart Object
- Inside Secure VaultIC 440 Smart Object
- INSIDE Secure VaultIC 441 Smart Object
- Inside Secure VaultIC 460 Smart Object
- IonIDe Smartcard Reader
- KACST HSID Reader
- KACST HSID Reader Dual Storage
- KACST HSID Reader Single Storage
- Kapsch TrafficCom USB SAM reader
- KEBTechnology KONA USB SmartCard
- Kingtrust Multi-Reader
- KOBIL EMV CAP - SecOVID Reader III
- KOBIL KAAN Advanced
- KOBIL KAAN Base
- KOBIL KAAN SIM III
- KOBIL Systems IDToken
- KOBIL Systems mIDentity 4smart
- KOBIL Systems mIDentity 4smart AES
- KOBIL Systems mIDentity fullsize
- KOBIL Systems mIDentity fullsize AES
- KOBIL Systems mIDentity M
- KOBIL Systems mIDentity visual
- KOBIL Systems mIDentity XL
- KOBIL Systems Smart Token
- KRONEGGER Micro Core Platform
- KRONEGGER NFC blue Reader Platform
- Ledger Nano S
- Lenovo Integrated Smart Card Reader
- Lenovo Lenovo USB Smartcard Keyboard
- Liteon HP SC Keyboard - Apollo (Liteon)
- Liteon HP SC Keyboard - Apollo JP (Liteon)
- Liteon HP SC Keyboard - Apollo KR (Liteon)
- Macally NFC CCID eNetPad
- mCore SCard-Reader
- Microchip SEC1110
- Microchip SEC1210
- MK Technology KeyPass S1
- Morpho MSO1350 Fingerprint Sensor & SmartCard Reader
- Morpho MSO350/MSO351 Fingerprint Sensor & SmartCard Reader
- MSI StarReader SMART
- MYSMART MySMART PAD V2.0
- Neowave Weneo
- Nitrokey Nitrokey HSM
- Nitrokey Nitrokey Pro
- Nitrokey Nitrokey Start
- Nitrokey Nitrokey Storage
- NTT Communications Corp. SCR3310-NTTCom USB SmartCard Reader
- NXP Pegoda 2 N
- NXP PR533
- O2 Micro Oz776
- OBERTHUR TECHNOLOGIES ID-ONE TOKEN SLIM v2
- OCS ID-One Cosmo Card USB Smart Chip Device
- OMNIKEY 5421
- OMNIKEY 6321 CLi USB
- OMNIKEY AG 3121 USB
- OMNIKEY AG 6121 USB mobile
- OMNIKEY AG CardMan 3121

- OMNIKEY AG CardMan 3621
- OMNIKEY AG CardMan 3821
- OMNIKEY AG CardMan 5121
- OMNIKEY AG CardMan 5125
- OMNIKEY AG CardMan 6121
- OMNIKEY AG Smart Card Reader
- OMNIKEY CardMan 1021
- OMNIKEY CardMan 4321
- OMNIKEY CardMan 5321
- Panasonic Panasonic USB Smart Card Reader 7A-Smart
- Philips Semiconductors JCOP41V221
- Philips Semiconductors SmartMX Sample
- PIVKey T800
- Planeta RC700-NFC CCID
- Precise Biometrics Precise 200 MC
- Precise Biometrics Precise 250 MC
- Precise Biometrics Sense MC
- Raritan D2CIM-DVUSB VM/CCID
- Regula RFID Reader
- REINER SCT cyberJack go
- REINER SCT cyberJack one
- REINER SCT cyberJack RFID basis
- REINER SCT cyberJack RFID standard
- REINER SCT tanJack Bluetooth
- Rocketek RT-SCR1
- RSA RSA SecurID (R) Authenticator
- SafeNet eToken 5100
- SafeNet eToken 5300
- SafeNet eToken 7300
- SafeTech SafeTouch
- SAFETRUST SABRE SCR
- SchlumbergerSema SchlumbergerSema Cyberflex Access
- SCM Microsystems Inc. HP USB Smartcard Reader
- SCM Microsystems Inc. SCL010 Contactless Reader
- SCM Microsystems Inc. SCL01x Contactless Reader
- SCM Microsystems Inc. SCR 331
- SCM Microsystems Inc. SCR 3310
- SCM Microsystems Inc. SCR 3311
- SCM Microsystems Inc. SCR 331-DI
- SCM Microsystems Inc. SCR 335
- SCM Microsystems Inc. SCR 355
- SCM Microsystems Inc. SCR3310 USB Smart Card Reader
- SCM Microsystems Inc. SCR331-DI USB Smart Card Reader
- SCM Microsystems Inc. SCR3320 - Smart Card Reader
- SCM Microsystems Inc. SCR3340 - ExpressCard54 Smart Card Reader
- SCM Microsystems Inc. SCR33x USB Smart Card Reader
- SCM Microsystems Inc. SDI010 Smart Card Reader
- SCM Microsystems Inc. SDI011 Contactless Reader
- SCM Microsystems Inc. SPR 532
- Secure Device Solutions DOMINO-Key TWIN
- SecuTech SecuTech Token
- Sitecom Sitecom USB simcard reader MD-010
- Softforum Co., Ltd XecureHSM
- SpringCard CrazyWriter
- SpringCard CSB6 Basic
- SpringCard CSB6 Secure
- SpringCard CSB6 Ultimate
- SpringCard EasyFinger Standard
- SpringCard EasyFinger Ultimate

- SpringCard H512 Series
- SpringCard H663 Series
- SpringCard NFC'Roll
- SpringCard Prox'N'Roll
- Spyrus Inc PocketVault P-3X
- SYNNIX STD200
- Teridian Semiconductors TSC12xxFV.09
- THRC Smart Card Reader
- THURSBY SOFTWARE TSS-PK1
- TianYu CCID Key TianYu CCID SmartKey
- Tianyu Smart Card Reader
- Todos Argos Mini II
- Todos CX00
- ubisys 13.56MHz RFID (CCID)
- udea MILKO V1.
- Unicept GmbH AirID USB
- Unicept GmbH AirID USB Dongle
- Validy TokenA sl vt
- VASCO DIGIPASS 870
- VASCO DIGIPASS 875
- VASCO DIGIPASS 920
- VASCO DIGIPASS KEY 101
- VASCO DIGIPASS KEY 200
- VASCO DIGIPASS KEY 202
- VASCO DIGIPASS KEY 860
- VASCO DP855
- VASCO DP865
- VASCO DP905v1.1
- Verisign Secure Storage Token
- Verisign Secure Token
- VMware Virtual USB CCID
- WatchCNPC USB CCID Key
- Watchdata USB Key
- Watchdata W5181
- Winbond CCID SmartCard Controller
- XIRING Leo v2
- XIRING MyLeo
- XIRING XI-SIGN USB V2
- Yubico Yubikey 4 CCID
- Yubico Yubikey 4 OTP+CCID
- Yubico Yubikey 4 OTP+U2F+CCID
- Yubico Yubikey 4 U2F+CCID
- Yubico Yubikey NEO CCID
- Yubico Yubikey NEO OTP+CCID
- Yubico Yubikey NEO OTP+U2F+CCID
- Yubico Yubikey NEO U2F+CCID

CONTACTING TECHNICAL SUPPORT AND ADDITIONAL RESOURCES

- Visit the NComputing Knowledge Base at http://kb.ncomputing.com/ for more information, guides, and walkthroughs.
- To request Technical Support, please visit the NComputing Support page at http://www.ncomputing.com/support/overview.

Disclaimer

Information contained in this document may have been obtained from internal testing or from a third party. This information is for informational purposes only. Information may be changed or updated without notice. NComputing reserves the right to make improvements and/or changes in the products, programs and/or specifications described herein anytime without notice.

All NComputing software is subject to NComputing intellectual property rights and may be used only in conjunction with Genuine NComputing hardware and in accordance to the NComputing End User Licensing Agreement and Terms of Use.

www.ncomputing.com