Proxmark Card Lab User Guide

Version 0.1.9 beta | West Coast Security

Purpose

Proxmark Card Lab is a standalone WCS desktop tool for authorized security technicians and engineers working with unknown client access credentials. It helps identify card technology, summarize scan sessions, preserve multi-technology and multi-format scan candidates, capture decoded values, compare Match Code Lab values, save client/site reader-format profiles, flash the Proxmark3 reader, run targeted LF/HF lab workflows, store encrypted card records, move approved cards into a Clone Vault, clone supported LF HID cards, emulate supported LF HID raw credentials, run guarded advanced Proxmark commands, check for updates, and export lab findings. The app runs as a 2-day demo or with a signed WCS license.

Local Paths

Installed binaries: C:\Program Files\WCS\Proxmark Card Lab
Writable app state: %ProgramData%\WCS\Proxmark Card Lab
License file: %ProgramData%\WCS\Proxmark Card Lab\license.key
Encrypted card list: %ProgramData%\WCS\Proxmark Card Lab\card-list.json.enc
Encrypted client/site profiles: %ProgramData%\WCS\Proxmark Card Lab\site-profiles.json.enc
Exports: %USERPROFILE%\Documents\WCS\Proxmark Card Lab\Exports

Licensing

Proxmark Card Lab allows a 2-day demo period on first run. After the demo expires, scanning, flashing, encoding, cloning, emulation, advanced commands, and export require a signed WCS license. Use Help > Register / License to copy the machine ID, open or copy a license request email to TechServices@wcsecurity.com, import the returned license file, or paste and apply the license key. Request name, request email, and company / organization are required before a request can be generated. The request includes the WCS license portal reference, product ID ProxmarkCardLab, company, machine ID, computer name, Windows user/domain, local IP addresses, public IP/location lookup, app version, and demo status. Use Help > Check for Updates to manually check for a newer release; automatic startup checks can be enabled or disabled from the Help menu and stay quiet unless a newer version is available. When an update is available, the app opens the WCS product page or controlled trial/request flow rather than downloading an installer directly.

Device Workflow

Connect the Proxmark3 reader, select the detected COM port, confirm the bundled Proxmark3 root path, flash firmware when the reader firmware is missing or stale, then run Identify Unknown, LF Scan, HF Scan, or Scan All. Scan All continues through LF and HF discovery. Identify Unknown creates a scan-session summary with candidate counts, likely primary format, alternate warnings, and recommended next step.

Card Records

Successful scans can be added to the card list. By default, Auto-add scans and Add Latest add likely primary candidates only. Verified HID H10301 results are labeled as primary; Indala, Tecom, and similar interpretations from the same HID bitstream are kept as low-confidence Verify Format First alternates. Use Include alternates or Add All Candidates when a lab review needs every Proxmark interpretation side by side. Scan History is the evidence log; Clone Vault is the deliberate later-use list. Clone Selected and Emulate Selected are enabled only for vaulted LF HID records with usable raw HID data and prompt for confirmation before running. The Proxmark Output pane can be resized with the divider under the Card List or hidden from the Card List toolbar.

HF Read Profiles

The HF profile buttons run targeted Proxmark command sequences for common unknown-card families. MIFARE Classic 1K runs ISO 14443-A selection, Classic information, and a default-key survey. DESFire runs ISO 14443-A selection plus DESFire information and application enumeration. iCLASS runs iCLASS information and reader output. NTAG / MIFARE Ultralight, ISO 14443-A/B, and ISO 15693 profiles focus on card identity, manufacturer, UID/CSN, configuration, and protocol details. These workflows are read/identify profiles; full HF dumping, cloning, or emulation can require customer authorization, keys, secure-card behavior, or card-family-specific validation.

Match Code Lab And Site Profiles

The Match Code Lab panel shows tested H10301 match-code data where facility code and card number support it, deterministic UID/raw reference conversions, and clearly labeled helper values for candidate Wiegand layouts and HF UID comparisons. Each row includes a status such as Verified H10301, Reference, Velocity helper, Reader helper, or Experimental. The Reader / Site Profile area saves client/site reader assumptions, Velocity format notes, expected facility code, card-number ranges, and comments. Saved profiles are encrypted under ProgramData and appear in the Site Profiles tab.

Encoder Formats

The encoder dropdown includes known credential families seen in Proxmark scan output. HID H10301, AWID 26-bit, Indala, and Kantech ioProx have one-click write commands in this beta. Other entries, including Identiv FIDO / U2F and additional LF candidate formats, are included for scan recognition and card-list storage until a validated write workflow is added.

Advanced Commands

The Advanced panel runs a single confirmed Proxmark client command for authorized engineering workflows. Use it for supported client commands that are not yet represented as one-click buttons, then review and store the raw output with the card record when useful.

Clone And Emulate

Stored LF HID credentials can be loaded, cloned, or emulated later from the card list. Cloning and emulation ask for direct Yes/No confirmation after the action is clicked. HF cards can often be identified from a scan, but full HF cloning or emulation can require card-family-specific dumps, keys, or secure-element behavior.

Export

Use Export Excel to write the card list to an .xlsx workbook. The export includes a structured card list worksheet, a raw-output worksheet, and a Match Code Lab worksheet for engineering review. Use Export PDF to create a concise client/engineering report with scan-session summaries and selected credential details. Exports work from saved card-list data even when the Proxmark reader is not currently attached.

Handling

Credential data is sensitive customer security information. Store exports only in approved WCS/client project locations and remove lab copies when they are no longer needed.