credenti
A Tecnics Company

Supported Cards and Readers for TecTANGO

Credenti supports a wide variety of low frequency (125 kHz) and high frequency (13.56 MHz) cards and readers for logical access as well as physical access without the need to issue new badges to the employees.

The following is a non-exhaustive list of cards supported by Credenti.

- Sentry Biometric Card Biometric Credential w/HID Prox (125 kHz) + UHF
- Sentry Biometric Card Biometric Credential w/HID iCLASS (13.56 MHz) + UHF
- Sentry Biometric Card Biometric Credential w/HID SEOS (13.56 MHz) + UHF
- HID 125kHz PROX and PROX II
- HID iCLASS card & fob
- HID iCLASS SE
- HID MIFARE Classic
- HID MIFARE DESFire
- HID iCLASS Seos
- HID Crescendo
- AWID
- CASI-RUSCO
- Indala
- Legic

The following is a non-exhaustive list of readers supported by Credenti.

- Embedded readers in rugged laptops: Dell, Getac,Panasonic
- Android/iOS devices with NFC capability (recommended with Sentry Biometric Card)
- rfIDEAS pcProx(now called WAVE ID)
- rfIDEAS WAVE ID Plus Mini
- rfIDEAS WAVE ID Nano
- HID Omnikey 5022
- HID Omnikey 5023
- HID Omnikey 5427 CK Gen 2
- HID Omnikey 5422
- HID Omnikey 5025 CL
- ACS ACR Series
- Identiv uTrust

The following is a list of biometric readers supported by Credenti.

- HID DigitalPersona 4500 Fingerprint Reader
- HID DigitalPersona 5300 Fingerprint Reader
- HID EikonTouch TC510 Fingerprint Reader

If your card type is not listed here, please contact our sales team at sales@credenti.com for personalized assistance and to explore compatibility options.

WHY CHOOSE CREDENTI

Securing ones identity is fundamental to implementing a zero trust strategy and to fulfill user-to-application access requirements. Companies have adopted the zero trust security model since decentralized business models and IT systems have made it significantly more complicated to ensure proper access controls are in place across multiple networks and physical locations. Zero trust networking solutions like Credenti, a Tecnics Company allows companies to continuously monitor network activity and user behavior to adapt authentication requirements on an individual basis.