Ethernet Card Reader Whitepaper
Table of contents

Roots .................................................................................................................................................. 3
Equitrac’s first RFID readers ........................................................................................................... 3
Early external readers ....................................................................................................................... 4
Medusa readers ................................................................................................................................. 5
Feature additions ............................................................................................................................... 6
Gen 2 USB readers ............................................................................................................................. 7

The Ethernet Reader ......................................................................................................................... 9
Introduction ......................................................................................................................................... 9
Advantages ......................................................................................................................................... 9
Connections ....................................................................................................................................... 10
Addressing ......................................................................................................................................... 11
Communications ............................................................................................................................... 11
Discovery ........................................................................................................................................... 12
Identification ...................................................................................................................................... 12
Encryption .......................................................................................................................................... 13
Certificates and lock down ................................................................................................................ 14
High availability ................................................................................................................................. 14
Connection and discovery issues ....................................................................................................... 15
Factory reset ...................................................................................................................................... 15
Maintenance mode ........................................................................................................................... 16
LED indications ................................................................................................................................. 17
Configuration and maintenance ......................................................................................................... 20
Roots

Equitrac’s first RFID readers
The first Radio Frequency Identification (RFID) card readers from Equitrac were internal to the PageCounter: Mifare, Legic, or HID Proximity reader hardware was added to the terminal endcaps as orderable options.

To preserve the PageCounter’s serial port for the fax option, these internal readers were connected to the track 2 magnetic swipe head interface. This restricted the data returned by a reader to numeric values only, either a decimal conversion of a card’s Unique ID (UID) with the Mifare and Legic hardware, or a 16 digit octal representation of the raw card data with HID Proximity.

The Mifare and Legic readers were based on the Baltech ID-engine product, customized to fit the PageCounter housing. To access card data from encrypted memory locations in Mifare or LEGIC cards, the readers could be customized by presenting special ConfCards created for Equitrac by Baltech. This feature was frequently put to use in Europe where such card systems are common.

The HID Proximity reader was built from HID Corporation’s eProx Multi-Chip Module, which connects directly to a magnetic swipe card interface and cannot be customized. The HID decoding feature in the Equitrac software was added as a workaround to this limitation.

The PageCounter Mifare reader was Equitrac’s first multi-card reader, returning UIDs from any card system built on ISO 14443 or ISO 15693 standards, including HID iClass cards.
Early external readers

Posh Magswipe Reader
Equitrac’s first external reader was a track 2 magnetic swipe card reader for use with the Xerox Secure Access (XSA) Authentication Device. Custom designed for Equitrac by Posh Manufacturing, it attached to the XSA device with an 8-pin mini-DIN connector. The pinout of this connector is proprietary to Equitrac.

Access45 Readers
External RFID card readers were also required for use with the XSA devices. Baltech produced these for Equitrac in the familiar Mifare, Legic, and HID flavors, based on their ID-engine compatible Access45 platform. The convention of returning unique IDs in decimal and raw HID Prox data in octal was preserved for compatibility in mixed fleets, where XSA devices and PageCounters were installed side by side.

Role Expansion
Support for the mini-DIN readers was added to the Equitrac Print & Copy Control client on Ricoh multi-function printers by use of a special SDIO card, power supply, and Y cable. The Equitrac TouchPoint Console also launched with a mini-DIN connector to support the external card reader hardware.
Medusa readers
Demand for readers that could be used on any Multi-Function Printer (MFP) resulted in Baltech’s development of a new ID-engine compatible platform called Medusa.

Each flavor of Medusa reader could be manufactured with one of three different cables: Mini-DIN for legacy devices, EPA for Fuji-Xerox MFPs, and USB for other MFP brands. Baltech also created a magnetic swipe reader in the Medusa line that added support for cards with data on tracks 1, 3, or the Japanese JIS-II track, in addition to classic track 2 support. The Posh and Access45 readers were retired, quietly replaced by their Medusa counterparts.

Licensing for embedded clients was originally tied directly to the reader hardware, with software code recognizing Medusa USB readers by their Vendor and Product IDs. Since XSA had different licensing terms, a second set of USB readers were produced exclusively for the Xerox channel which were identical but for their USB Product IDs.

Requests for compatibility with additional 125 kHz card systems resulted in the later development of the Medusa Indala reader, with support for cards built from Indala, Hitag, or EM-Marin RFID chips. This expanded the number of external reader part numbers to 20.
Feature additions

Keyboard emulation was added to the Medusa USB readers as a configurable option, to support Sharp MFPs whose environment did not allow embedded code to communicate directly with a reader in its native protocol. New generations of Mifare card and exposure to additional 125 kHz card systems also required updated firmware and configuration options.

These feature additions complicated maintenance, as dependencies were created between multiple configurations and firmware versions. Baltech created the Equitrac Reader Maintainer tool (RMT) to simplify maintenance by allowing users to select from a list of stock solutions. Each stock solution ensures that the correct combination of firmware and configuration is used for a particular application. The RMT also provides facilities to load custom firmware and configuration files, test reader configurations, identify cards, and restore readers to the factory default behavior.

The RMT works directly with USB readers, while the Equitrac Reader Adapter Box is required to work with PageCounter Internal, mini-DIN, or EPA readers.

The Equitrac Reader Adaptor Box connects PageCounter Internal, mini-DIN, and EPA readers to the RMT.
Gen 2 USB readers
As large customers grew by acquisition they required card readers that could simultaneously support a mix of technologies, to work with the various access control systems used in their facilities.

Baltech’s ID-Engine compatible Shark-M platform incorporates both 125 kHz and 13.56 MHz chipsets into a single reader. Launched by Nuance as the Equitrac ID Card Reader with Multi-Card capability, a new housing was used to differentiate it from previous reader generations.

The ID Card Reader line also launched with two cost-reduced models for sale at lower price points. The Mifare (gen 2) reader contains only the 13.56 MHz components, while the HID/Indala (gen 2) reader has just the 125 kHz parts. These readers obsoleted the legacy Medusa Mifare, HID, and Indala USB readers.
The iClass reader
Although full support for HID iClass cards (access to the encrypted card number) was a design feature of the Shark-M platform, the required decryption chip proved too expensive to include in every reader. Support was dropped for the ID Card Reader launch, and released later as the Multi + iClass model. This premium reader also includes a SAM socket for the insertion of a customer-sourced Secure Access Module (SAM), to enable the use of high security card systems with proprietary encryption keys or algorithms.

The Legic (gen 2) reader
The most recent addition to the ID Card Reader line is the Legic (gen 2) reader, produced in response to obsolescence of the LEGIC chipset used in legacy models. To ensure continued production of the Medusa mini-DIN and EPA Legic readers, a stockpile of original chips was procured and all USB Legic sales migrated to the Legic (gen 2) reader.

The Legic (gen 2) version of the Equitrac ID Card Reader was the first to launch with Nuance branding.
The Ethernet Reader

Introduction
Job release on single function printers was traditionally performed with costly reader plus terminal solutions. The Nuance Ethernet Card Reader, built on the Baltech Shark-E platform, directly connects to Ethernet networks to lower the purchase and support costs associated with single function print release.

Advantages
The Ethernet Card Reader offers many advantages when compared to both traditional and competing Ethernet card reader solutions:

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower cost</td>
<td>Every intelligent electronic device is its own micro computer system.</td>
</tr>
<tr>
<td></td>
<td>With the Ethernet Card Reader there is just one such system per installed location, rather than the two required in separate reader + converter solutions.</td>
</tr>
<tr>
<td>High security</td>
<td>Card numbers and access details are never sent in the clear.</td>
</tr>
<tr>
<td></td>
<td>PKI encryption ensures the highest level of data secrecy and tampering protection.</td>
</tr>
<tr>
<td>High availability</td>
<td>Configuring a secondary server provides fail-over in the event of communications link or equipment problems.</td>
</tr>
<tr>
<td>Common configuration</td>
<td>The Ethernet Card Reader uses the same configuration system as the ID Card Reader line (gen 2 USB).</td>
</tr>
<tr>
<td>Central management</td>
<td>Nuance system software can push configuration and firmware updates out to all Ethernet Card Readers simultaneously.</td>
</tr>
<tr>
<td>Power over Ethernet</td>
<td>Readers can be powered either by an AC adaptor or with Power over Ethernet.</td>
</tr>
</tbody>
</table>
Connections
As with Nuance terminal products, the Ethernet Card Reader has two ports which connect to an internal unmanaged network switch, so that both printer and reader can be serviced from a single network drop.

The Network port also supports Power over Ethernet (PoE), so that no AC adapter or additional outlet is required when PoE is available. This is attractive in markets where power outlets are not provided in pairs; and power bars and taps are either considered too costly or prohibited by safety regulations.
Addressing

By default the Ethernet Card Reader uses the Dynamic Host Configuration Protocol (DHCP) to obtain an Internet Protocol version 4 (IPv4) address.

The reader’s DHCP Request and Discovery packets include the Vendor Class Identifier (Option 60) string “Baltech Proxreader”. Customer IT departments may use this string to specifically recognize card readers and assign them an address from a certain pool, open the necessary firewall ports, and so on.

Each reader can be assigned a static IP address during configuration if required, disabling further use of DHCP.

Communications

All communications with the Ethernet Card Reader take place over a single TCP/IP connection using the Baltech Reader Protocol (BRP). Originally developed as a serial protocol for RS232 connections, BRP has been extended to RS485, USB, and Ethernet use cases. The commands, data, and packet structure are always the same; but the packets themselves can be wrapped in HID Feature Reports on USB (BRP-over-HID), or pushed through a TCP connection on Ethernet networks (BRP-over-TCP).

“Hosts open port 2939 on the reader during discovery and configuration.”

A BRP-over-TCP connection can be established by either the reader or its host. The host can be a server running the Nuance Device Control Service, or a PC running the Nuance Reader Maintainer software. When discovering and configuring an out-of-the-box reader, the host initiates a TCP connection from an ephemeral port (a random port number in a non-reserved range) to port 2939 on the reader. The host closes this connection once the reader is configured.

“Readers open port 5420 on the server to report activity.”

Each reader’s configuration contains the IP address and port of at least one server running the Nuance Device Control Service (DCS). The reader uses this information to open a server connection from an ephemeral port in response to trigger events. A trigger can be a card presentation, link status change, printer IP detection, reader reboot, or session key expiration. Once the trigger event is reported and serviced, the DCS closes the connection to conserve resources.

If the DCS is set up to communicate on a port other than 5420, then the reader configuration must be updated accordingly to ensure proper operation of the system.
Discovery
There are three methods of discovering an Ethernet Card Reader: UDP Introspection, IP range scanning, and the Service Location Protocol.

UDP Introspection is the method used to discover a single Ethernet Card Reader connected to a specific print device. When the server sends a specially formatted UDP packet to port 2939 on the printer, the card reader can hear it as long as that printer is connected to the reader’s Printer port. From this packet the reader learns the IP address of both printer and server, and the server port to contact for further configuration. In Equitrac 5.6, this process is initiated by right-clicking on a specific print device in System Manager and selecting Discover Nuance Card Reader.

For discovery of multiple card readers the server can perform an IP range scan. The user enters the first and last IP address of a range, and the server attempts to establish a BRP-over-TCP connection to every address within it. Devices that respond correctly (and are not already in the system database) are presented to the user for import.

The Service Location Protocol (SLP) can also be used for discovery, with each reader implementing the Service Agent (SA) function. While SLP has a reputation for generating excessive multicast traffic as each SA attempts to locate a Directory Agent (DA) to register with, the Ethernet Card Reader uses a passive implementation to avoid this. Readers will only speak when spoken to. Requests must be directed to “service:x-proxreader” in the “BALTECH” scope in order to receive a response. The URL in the Service Reply takes the form “service:x-proxreader://IP_Address:Port”, informing the requester of both the IP address and port necessary to initiate a BRP-over-TCP connection.

Only the Nuance Reader Maintainer uses SLP discovery to find and select readers for maintenance; the Nuance Device Control Service makes no use of SLP in relation to the Ethernet Card Reader.

Identification

“Hosts identify an Ethernet Card Reader by its serial number.”

Although the Ethernet Card Reader requests its last known IP address from DHCP following a reboot or power cycle, the DHCP service may be unwilling or unable to honor this request. Since a fixed IP address cannot be guaranteed, a host will always identify an Ethernet Card Reader by serial number rather than IP address.
Encryption
Card IDs, firmware, and reader configurations (which may contain information about how IDs are stored on a card) are never transmitted in the clear with the Ethernet Card Reader.

While the Baltech Reader Protocol (BRP) has always had a symmetric encryption option using stored Advanced Encryption System (AES) keys, the ease of eavesdropping on Ethernet networks demanded a higher level of security.

“The use of PKI is mandatory on the Ethernet Card Reader.”
Public Key Infrastructure (PKI) encryption is mandatory on the Ethernet Card Reader. A cryptographically random session key is established by the Elliptic Curve Diffie-Hellman (ECDH) algorithm, using Public Key Infrastructure X.509 (PKIX) certificates verified by the Elliptic Curve Digital Signature Algorithm (ECDSA). This session key is then used to encrypt further communications with AES. While these methods are commonly associated with the Secure Sockets Layer and Transport Layer Security protocols used on the internet (collectively known as SSL), they were directly included in BRP-over-TCP rather than layering BRP on top of standard SSL. This created an implementation more suitable to the storage limitations of the reader’s embedded processor, while maintaining identical security. The AES key strength is 128 bits, with an ECC-P256 key curve used for ECDH / ECDSA. These strengths are fixed in the code and cannot be adjusted.

PKI revolves around asymmetric encryption using public/private key pairs, where a message encrypted by a freely shared public key can only be decrypted by a secret private key known to the receiver. When each end of a communications channel has its own public/private pair, mutual authentication can be performed to ensure that both ends are trusted parties, and a shared session key created for faster symmetric encryption of additional messages. The algorithm used to create the session key ensures it is known only to the end parties, and cannot be deduced by an eavesdropper or man-in-the-middle attacker. Stored public/private pairs are used for authentication, with the session key created from randomly generated pairs that are signed and verified by the stored keys. This ensures forward secrecy: future compromise of the stored keys cannot compromise past session keys, even if an attacker interfered in the original communications.

“Initial creation of the session key takes 20 seconds.”
Mutual authentication and creation of the session key takes approximately 20 seconds due to the complexity of the math involved. As this key is stored only in the reader’s dynamic memory and never in Flash or EEPROM, a new session key must be created after every reboot or power cycle. Session keys are also time limited to a duration set by the server during authentication. To avoid the inconvenience of the delay, the Nuance Device Control Service (DCS) sets each session key to expire at approximately 2:00 a.m. local time. Card readers automatically connect to DCS to establish a new session key once their old key has expired.
Certificates and lock down

Every Ethernet Card Reader and Nuance system server has its own unique public/private key pair. Public keys are stored in X.509 certificates, which are exchanged and examined during mutual authentication. This process allows servers to verify that connecting devices are legitimate card readers, and for each reader to verify that its server is a legitimate host.

“Readers are locked to their host system by the system certificate.”

When connecting to an out-of-the-box card reader, a factory certificate is used for authentication, with a system certificate created and written to the reader as it’s configured. An Ethernet Card Reader becomes locked to the system once the system certificate is in place. Connections established with the factory certificate can no longer issue secured commands or request sensitive data. This prevents unauthorized access to readers in the field, even in the event that a malicious third party gains knowledge of the factory certificate.

When using SSL communications on the internet, certificate chains must be traceable to a trusted root certificate from a known third-party Certificate Authority (CA). Since none of the communications between an Ethernet Card Reader and its host system involve the use of a web browser or other public tools, such traceability is unnecessary. The CA for the system is a component of the Nuance software itself, with a self-signed root certificate generated automatically during installation. In high availability systems, intermediate certificates for distributed components are automatically created and signed by the root as necessary. These system certificates are neither manageable nor accessible to a Nuance system administrator.

High availability

The Ethernet Card Reader contains configuration settings for both a primary and secondary server. Following a reboot or power cycle, the reader connects to the primary server by default. If that connection cannot be opened successfully, the secondary server is contacted. Two attempts are made to each server (four total, alternating between servers) before the reader will show a Host Connection Failed indication (3 red blinks) on its LED, with alternating attempts continued until reconnection is achieved.

When a transaction with a server is complete, the server closes the connection to conserve resources. When reconnecting in response to a trigger (card presentation, link status change, printer IP detection, session key expiration, or power cycle), the reader always starts with the last server to which it has communicated successfully, regardless of the primary or secondary designation.

“The reader is unaware that a server is down until after a trigger event has occurred.”

Since connections are not left open, the reader is unaware of whether or not the Nuance Device Control Service (DCS) is available until after it has attempted to connect in response to a trigger. If a communications link or DCS goes down, there will be no indication of trouble on the reader’s LED until after a trigger event has occurred, and initial connection attempts (two per server) have failed.
Connection and discovery issues
The Ethernet Card Reader supports only one connection at a time. This can be the cause of discovery and connection issues when maintaining a reader which has already been configured.

If the reader has an active session with a server, or is attempting to open one in response to a trigger, it will deny all connection attempts from other hosts and services. The same happens if a PC running the Nuance Reader Maintainer (NRM) has an Ethernet Card Reader selected, leaving a connection to that reader open. The affected reader will be invisible to any Nuance system performing a discovery operation, and although other NRM instances will be able to discover the reader via the Service Location Protocol (SLP), attempts to select it will fail.

In normal operation all communications take place between a reader and just one server at a time, so this will not be an issue. It can cause frustration in a demo environment however, or when redeploying a previously configured reader to a new system. If the issue persists it can be resolved by placing the reader into Maintenance Mode and performing a Factory Reset, erasing the stored configuration and any stale server settings.

Another issue exists exclusively with the Nuance Reader Maintainer and its reliance on IP multicast packets for SLP discovery. These packets may not always be forwarded by the switches in the local network. Managed switches may be configured to block multicast traffic, or the IGMP snooping function which alerts them to forward multicast packets can be disabled or have an associated timeout. Power cycling the card reader sends a new IGMP request that can restore multicast forwarding to make it discoverable again. If that fails, a PC running the NRM can be connected directly to the card reader’s Printer port to bypass any restrictions of the local network environment.

Factory reset
The Factory Reset command deletes the system certificate to unlock the reader, and reverts all reader settings to their default values.

This Factory Reset behavior is identical, whether you use the reset to factory defaults operation in the Nuance system or you use the Restore Reader function of the Nuance Reader Maintainer (NRM).

The Factory Reset command does not affect the firmware image stored within a reader. An Ethernet Card Reader whose firmware has been upgraded will remain upgraded after the Factory Reset is performed.

The Restore Reader function of the NRM also provides an option to write a known/good firmware and default configuration after sending the reset. This is useful to ensure that all restored readers deployed to a new system start with a common base. The firmware and configuration files used for this operation are built into the NRM, being the best available at the time of its release.
Maintenance mode
An Ethernet Card Reader which has been locked to a system or configured with invalid network settings can be reset by placing it into Maintenance Mode.

Maintenance Mode is entered by physically reconfiguring the reader so that only the Power and Printer port connections are used:

Once in Maintenance Mode, the LED repeatedly blinks red-green-off and the reader operates with the following temporary settings:

- The Static IP is disabled
- DHCP addressing is enabled
- Link Local addressing is enabled
- Configured server IP and port settings are ignored
- A Factory Reset command is accepted on connections secured with the factory certificate

When working in a network environment without DHCP, Link Local addressing allows for a point-to-point connection between the reader’s Printer port and a PC running the Nuance Reader Maintainer (NRM) software. To obtain a link local IP address, the PC must be set to use DHCP and then given 2 minutes to timeout after the link with the reader is established. An alternative method to avoid the timeout is to set the PC with the static IP address 169.254.1.1 and subnet mask 255.255.0.0 before connecting it to the reader. The reader chooses a non-conflicting address in the 169.254.x.x range, allowing for discovery, selection, and Factory Reset by the NRM.
LED indications
The Ethernet Card Reader’s RJ45 jacks have no link or status LEDs of their own, so the reader LED indicates both network and system status.

As a result of this dual role, the reader’s LED displays two distinct sets of indications:

– Online, when the LED is controlled by a Nuance system
– Offline, when communications with the host system have not, or cannot, occur

“Online and offline indications are visually distinct from each other.”

Online indications use either a solid color or continuously flash the LED with 50/50 duty cycle (equal amounts of time spent on and off).

Offline indications use a series of brief flashes (blinks) of the LED, followed by 2 seconds with the LED off before the blinks repeat.

When a reader is powered on, the LED is never off for more than 2 seconds.

Power on lamp/beeper test
At power up, an Ethernet Card Reader’s beeper sounds briefly and both the red and green elements of its LED light up, causing it to appear orange. The LED remains orange for several seconds, after which it presents an Online or Offline indication appropriate to its current state.

Link change indication
When an Ethernet Card Reader detects a change in link status (cable connected or disconnected) on either of its ports, the LED turns solid orange for several seconds, after which it presents the appropriate Online or Offline indication for its new state.
Online indications
An Ethernet Card Reader is Online once communications have been established with a Nuance system, which assumes control of its LED.

<table>
<thead>
<tr>
<th>Indication</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid red</td>
<td>Idle</td>
<td>No user logged in, reader is waiting for card presentation.</td>
</tr>
<tr>
<td>Slow flashing red</td>
<td>Not ready</td>
<td>A system problem has occurred. (Misconfiguration, no printer association, etc.)</td>
</tr>
<tr>
<td>Solid green</td>
<td>Session active</td>
<td>A user is logged in to perform a task.</td>
</tr>
<tr>
<td>Slow flashing green</td>
<td>Authenticating card</td>
<td>The system is looking up the user.</td>
</tr>
<tr>
<td>Fast flashing red</td>
<td>Unknown user</td>
<td>Presented card did not match any user record.</td>
</tr>
<tr>
<td>Fast flashing green</td>
<td>No print jobs</td>
<td>The user has no print jobs to release.</td>
</tr>
<tr>
<td>Alternating red/green</td>
<td>Insufficient funds</td>
<td>User account balance too low to perform job release.</td>
</tr>
</tbody>
</table>

Slow flashes have a 1 second period (LED on 500 ms, off 500 ms) while fast flashes have an 0.4 second period (LED on 200 ms, off 200 ms).

The availability of a specific indications and the length of time spent in each depends on the type and configuration of Nuance system to which the reader is connected.
Offline indications
An Ethernet Card Reader is Offline when communications with the host system are either impossible or have not yet occurred. Offline indications use a series of brief flashes (blinks) of the LED, followed by 2 seconds with the LED off before the blinks repeat.

“End users are not expected to be familiar with the Offline indications.”

In a support case users will be asked to report the color and number of blinks from which next steps can be determined. Red blinks indicate a hard failure requiring intervention, green that the reader is waiting on an external resource in order to transition online.

<table>
<thead>
<tr>
<th>Indication</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 green blink</td>
<td>Network linked</td>
<td>The Network port has an Ethernet link, but the reader has not yet obtained a valid IP address.</td>
</tr>
<tr>
<td>2 green blinks</td>
<td>Searching for host</td>
<td>The reader has a valid IP and is attempting to connect to a host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the reader has not yet been configured, it is also attempting to discover a host by performing UDP introspection.</td>
</tr>
<tr>
<td>1 red blink</td>
<td>No links</td>
<td>Cables may be disconnected at one end or the other, or the local network may be down.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If there is no issue with cabling, it could be that the reader is configured with a rate and duplex setting incompatible with the local network.</td>
</tr>
<tr>
<td>2 red blinks</td>
<td>UDP connect failed</td>
<td>Attempts to connect to the server identified by UDP introspection have failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required TCP ports may be blocked by the firewall settings of the server or other intermediate networking gear.</td>
</tr>
<tr>
<td>3 red blinks</td>
<td>Host connect failed</td>
<td>Attempts to connect to configured host servers have failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>There is either a problem with the network, or the system has changed and the reader configuration must be updated to match.</td>
</tr>
<tr>
<td>4 red blinks</td>
<td>IP address conflict</td>
<td>Another device on the network is using the same IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT must identify conflicting devices, then one or the other should be reconfigured and the reader subsequently rebooted.</td>
</tr>
<tr>
<td>Red blink, green blink</td>
<td>Maintenance mode</td>
<td>There is a network link on the Printer port only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If unintentional, the local network could be down or the reader is configured with an incompatible rate and duplex setting.</td>
</tr>
</tbody>
</table>
Configuration and maintenance

The Ethernet Card Reader uses the same configuration system as all previous card readers from Baltech. Nuance staff and select third parties can use ConfigEditor software to create custom configurations for use with both legacy USB card readers and Ethernet Card Readers alike.

The Nuance Reader Maintainer software can be used with gen 2 USB and Ethernet card readers for card testing and configuration upload, and comes with a number of stock solutions for common usage scenarios. In particular, it is often advantageous to configure Multi-Card readers to work only with the specific access card technology used at the customer site, to the exclusion of all other technologies. This prevents spam reads from unrelated tap-and-pay card systems that users may carry alongside their site access cards within a purse or wallet.

A significant new feature of the Ethernet Card Reader is that a configuration or firmware file can be pushed to multiple readers simultaneously from within the Nuance system software. The stock solutions included in the Nuance Reader Maintainer are also distributed as a zipped collection of individual configuration files for use with this feature.

About Nuance Communications, Inc.

Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.