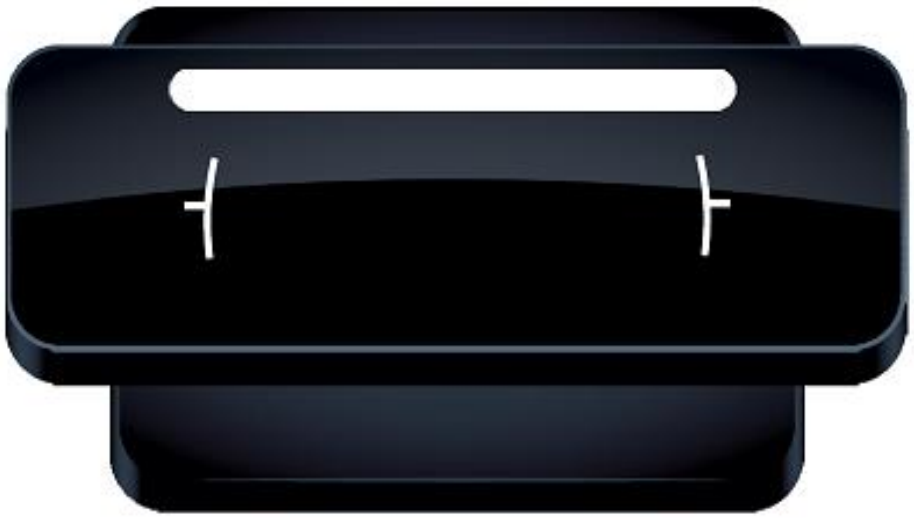
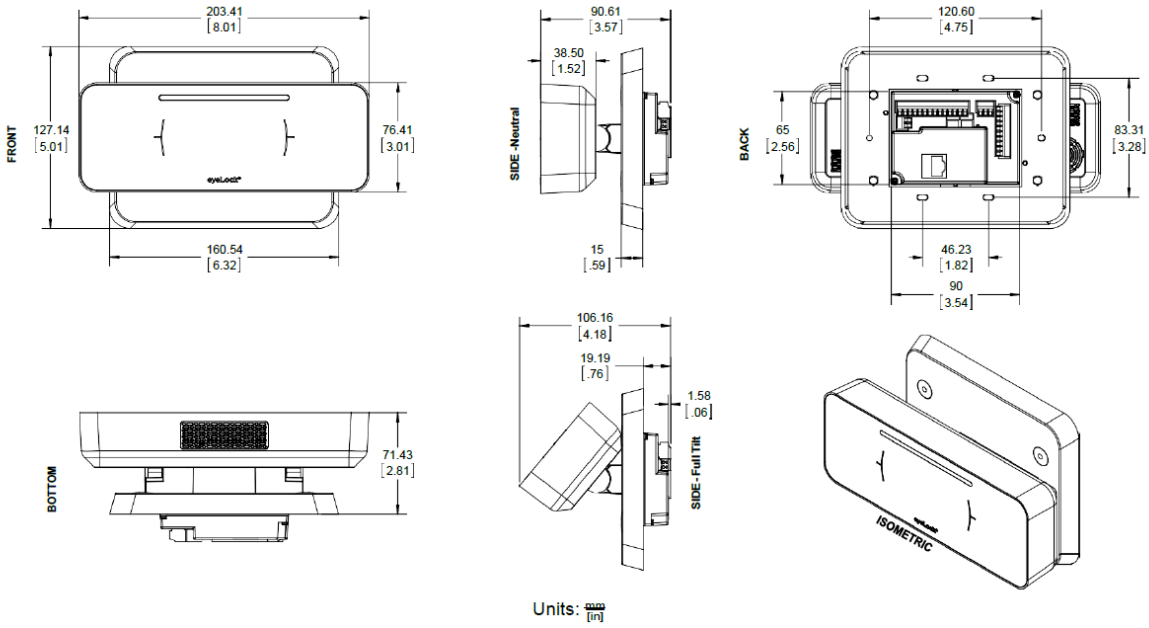
ETE NANO NXT



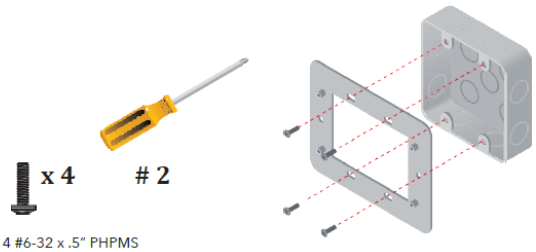
Eter Biometric Technologies Srl
Via Enrico Mattei 21 41043 Casinalbo (MO) - Italy Tel +39 059 7874620 Fax +39 059 7874622 Web www.eter.it

Dimensioni



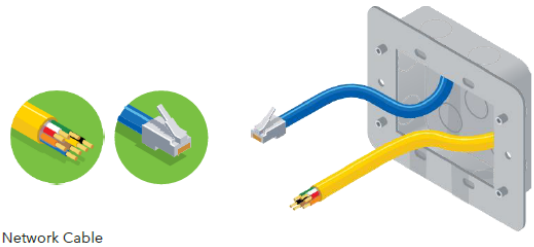
Installazione HARDWARE

1 Montare il pannello sul muro



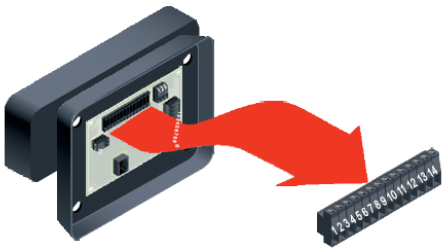
4 #6-32 x .5" PHPMS
No. 2 Phillips Screwdriver

2 Fare passare i cavi dall'apposita uscita

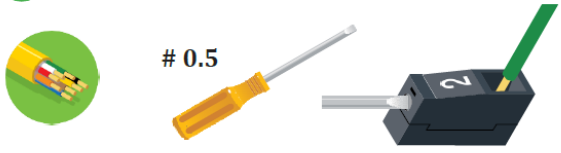


Network Cable
ACS Cable (8 or 6 conductor)

3 Rimuovere il connettore

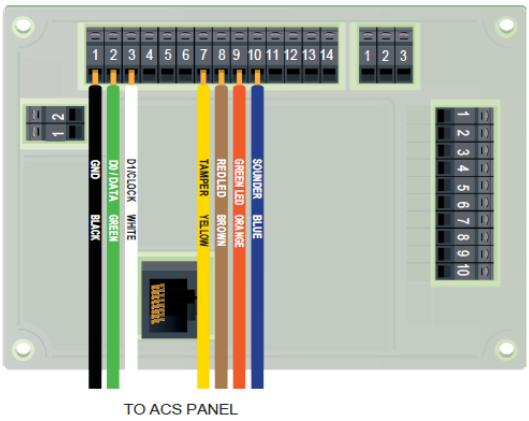


4 Effettuare i collegamenti

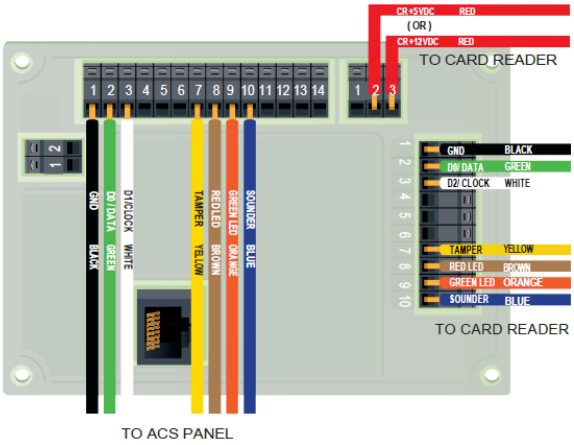


Eter Biometric Technologies Srl
Via Enrico Mattei 21 41043 Casinalbo (MO) - Italy Tel +39 059 7874620 Fax +39 059 7874622 Web www.eter.it

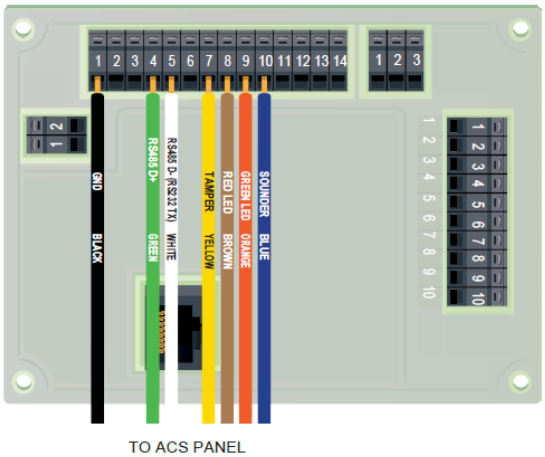
Wiegand fattore singolo



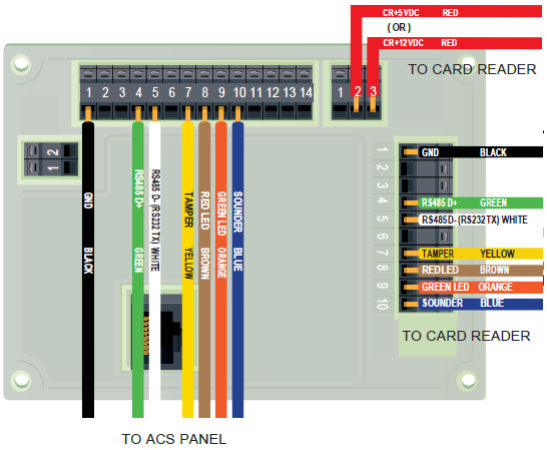
Wiegand doppio fattore



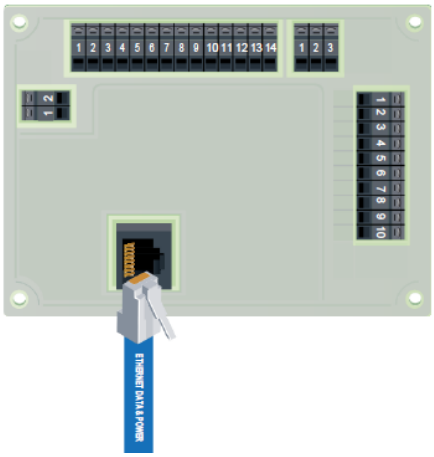
OSDP Fattore singolo

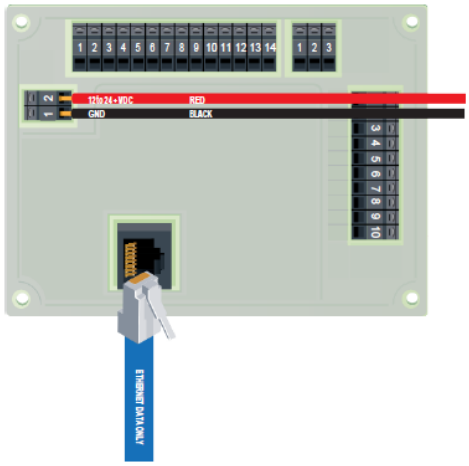


OSDP Fattore doppio



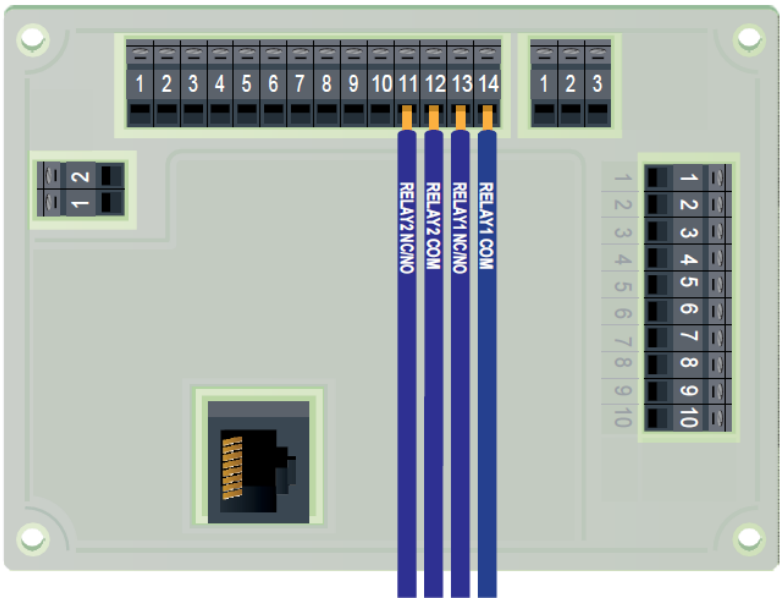
ALIMENTAZIONE:



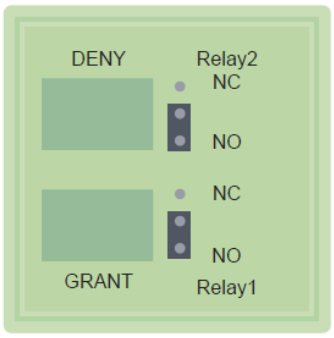


Si può alimentare solo in POE.

RELAY



JUMPERS



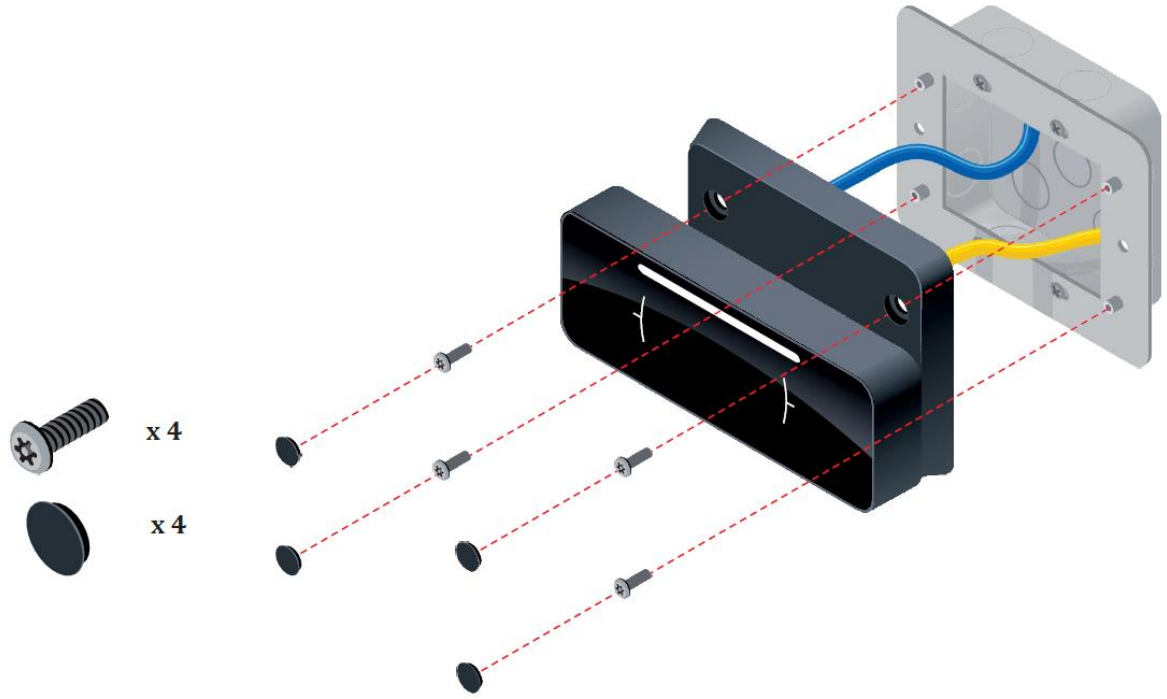
RELAY1: viene attivato quando l'autenticazione ha esito positivo. (CONCEDERE)

RELAY2: viene attivato quando l'autenticazione non riesce. (NEGARE)

RELAY2: (Modalità non coercizione) viene attivato quando l'autenticazione non riesce. (NEGARE)

RELAY2: (Modalità coercizione) si attiva quando viene rilevata una coercizione tramite l'immissione del PIN.

INSTALLAZIONE FINALE



INSTALLAZIONE DEL SOFTWARE DI GESTIONE

1. Aprire un browser Web e accedere a http://help.eyelock.com/.
2. Crea un account e accedi al sito per accedere al software.
3. Una volta effettuato l'accesso al sito, accedere a EyeLock Identity Suite.
4. Scaricare e rivedere il manuale utente EIS.
5. Scarica il software EIS e segui il Manuale utente EIS per installarlo.

Utilizzare l'accesso basato sul Web al dispositivo tramite l'applicazione Webconfig per eseguire la configurazione iniziale da un PC di configurazione. Il PC di configurazione deve essere impostato affinché DHCP acceda a Webconfig.

Collega il nano NXT e il PC alla rete. Il nano NXT indicherà che sta avviando la sequenza di avvio facendo lampeggiare rapidamente il LED rosso, verde, quindi blu. Il LED si illuminerà quindi di giallo per indicare che la sequenza di avvio è in corso. Infine, il LED si illuminerà di bianco quando il dispositivo è pronto per l'uso.

Luce Gialla **Luce Bianca**

La luce Gialla indica che la sequenza di avvio è in corso.

Attendere che il LED del dispositivo sia bianco prima di iniziare.

Quando il nano NXT è inizialmente connesso alla rete, il nano NXT tenterà di ottenere un indirizzo IP tramite DHCP. Se non è possibile ottenere un indirizzo IP tramite DHCP entro 60 secondi, il nano NXT utilizzerà per impostazione predefinita un indirizzo IP fisso noto (169.254.1.1) e una maschera di sottorete (255.255.0.0).

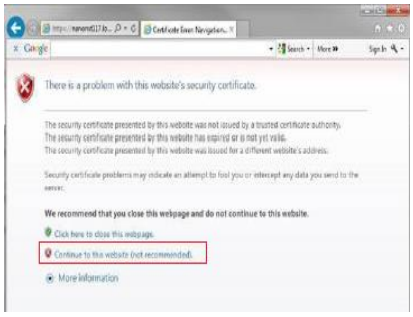
Quando il PC è connesso alla rete, tenterà anche di ottenere un indirizzo IP tramite DHCP. Se non è possibile ottenere un indirizzo IP, utilizza APIPA (Indirizzamento IP privato automatico) per configurarsi automaticamente con un indirizzo IP e una maschera di sottorete. L'intervallo di indirizzi IP è compreso tra 169.254.0.1 e 169.254.255.254, un intervallo in grado di comunicare con il nano NXT.

Attendi almeno 60 secondi per consentire al nano NXT di unirsi alla rete.

AVVISO CRITTOGRAFIA SSL IN WEB CONFIG

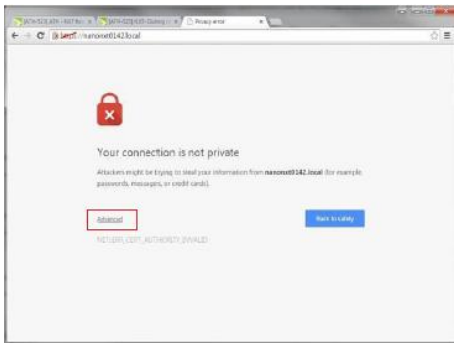
La crittografia SSL viene fornita come mezzo per proteggere la comunicazione delle impostazioni da Webconfig a nano NXT. Al primo caricamento del browser Webconfig, il browser genererà un avviso di certificato. È sicuro procedere se ricevi uno degli avvisi illustrati di seguito. Si prega di vedere quanto segue per le istruzioni su come procedere nei browser supportati.

EXPLORER



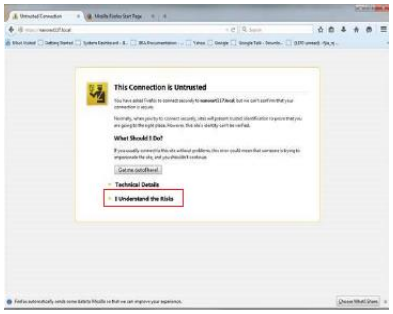
Per procedere con il certificato esistente, fare clic su "Continua con questo sito Web (non consigliato)".

CHROME



Per procedere con il certificato esistente, fai clic su "Avanzate" (nella foto sopra). Quindi fare clic su "Procedi a nanonxt0000.local (non sicuro)" (non mostrato).

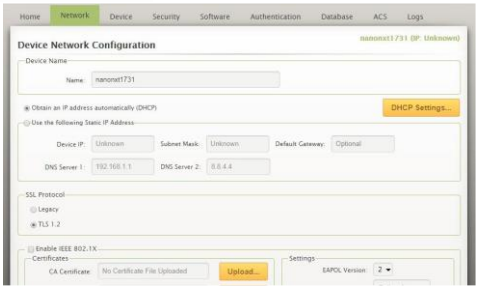
FIREFOX



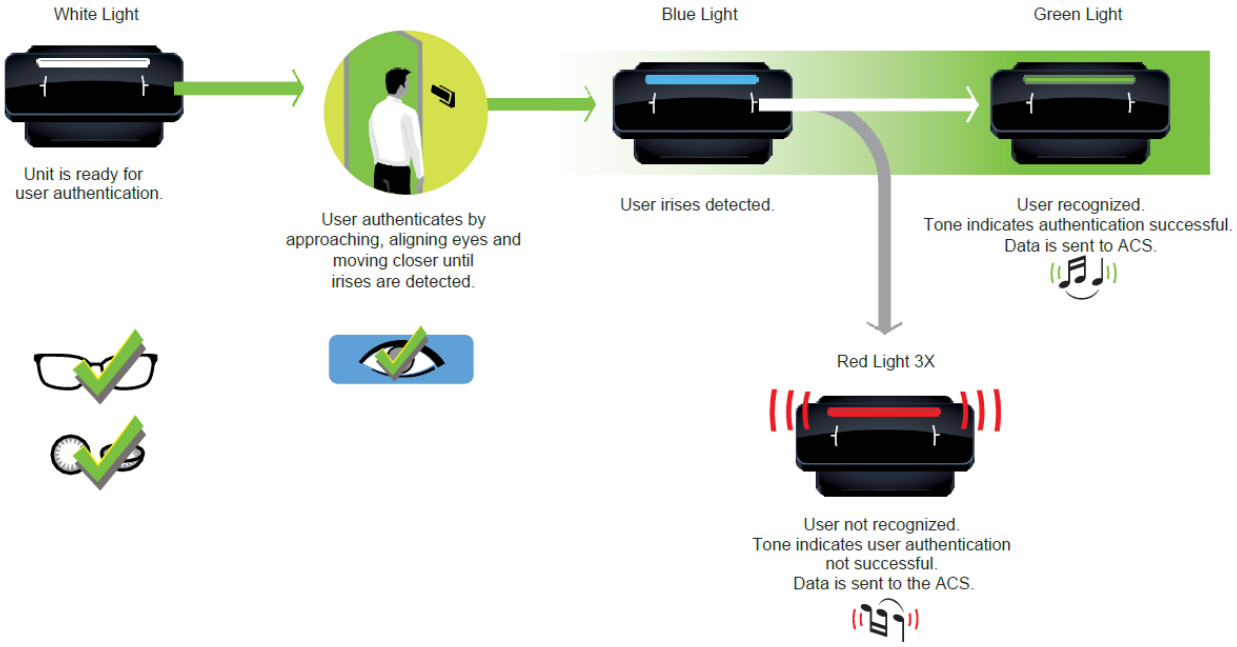
In order to proceed with the existing certificate, please click **'I Understand the Risks'** (pictured above). Then click **'Confirm Security Exception'** (not shown).

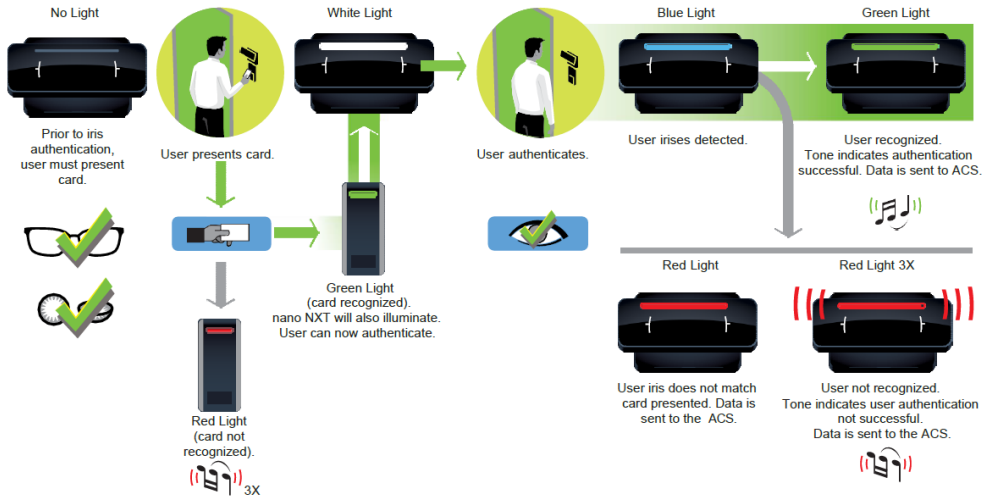
CONFIGURAZIONE INIZIALE DEL DISPOSITIVO IN WEB CONFIG

ACCEDERE
Immettere il nome di accesso e la password, quindi fare clic su ACCESSO. Gli installatori devono accedere utilizzando il nome e la password predefiniti.
Il nome di accesso predefinito è programma di installazione. La password predefinita è installatore.
Gli amministratori hanno privilegi di modifica della configurazione limitati in Webconfig.
Il nome dell'amministratore è admin. La password dell'amministratore è admin.

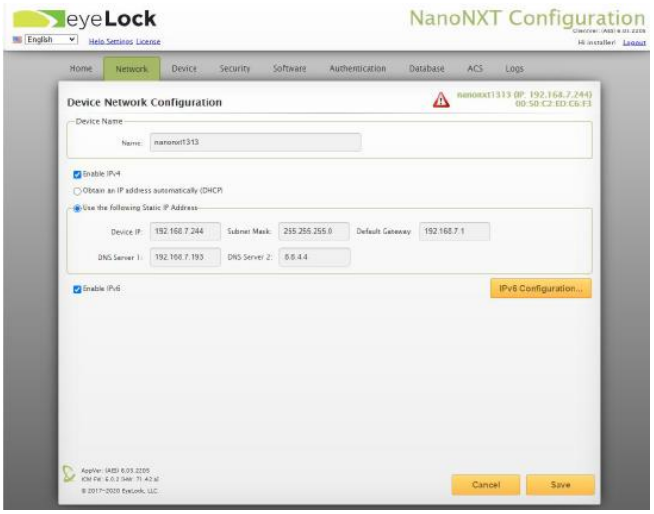


CONFIGURAZIONE DELLA RETE DEL DISPOSITIVO.
Fare clic sulla scheda RETE. Se si utilizza un indirizzo IP dinamico, vengono visualizzati l'indirizzo IP corrente, la rete di trasmissione, la sottorete e il gateway.
Se si utilizza un indirizzo IP statico, selezionare UTILIZZA IL SEGUENTE INDIRIZZO IP STATICO per inserire l'IP statico.

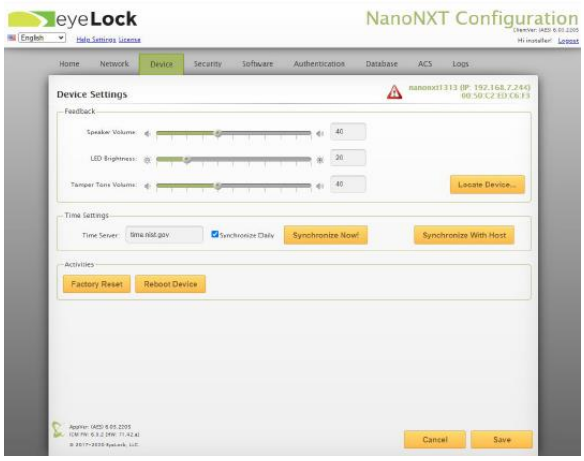




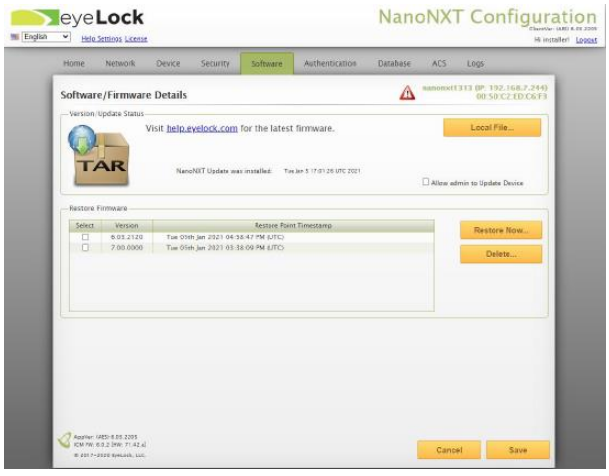
HOME
Fare clic sulla scheda HOME per INFORMAZIONI NANO NXT.
Fare riferimento a questa scheda per informazioni su firmware, date e orari di aggiornamento precedenti, versioni software, informazioni sul database, ecc.



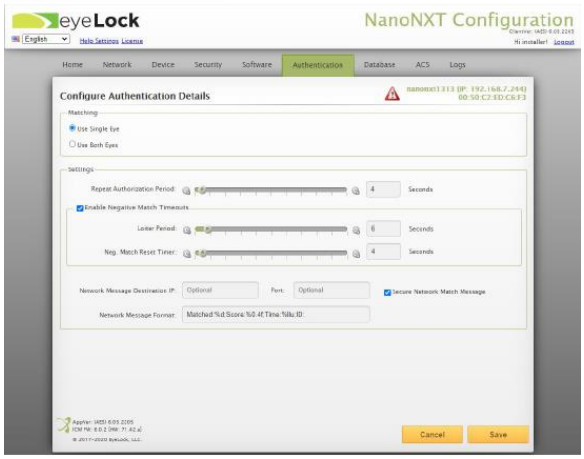
CONFIGURAZIONE DELLA RETE DEL DISPOSITIVO
Fare clic sulla scheda RETE. Se si utilizza un indirizzo IP dinamico, vengono visualizzati l'indirizzo IP corrente, la rete di trasmissione, la sottorete e il gateway.
Se si utilizza un indirizzo IP statico, selezionare UTILIZZA IL SEGUENTE INDIRIZZO IP STATICO per inserire l'IP statico.



IMPOSTAZIONI DEL DISPOSITIVO
Regola le impostazioni del FEEDBACK facendo clic e trascinando i cursori. Fare clic su Localizza dispositivo per attivare un LED lampeggiante. Selezionare un URL visibile al dispositivo per il time server. Fai clic su Sincronizza ora per sincronizzare data e ora.

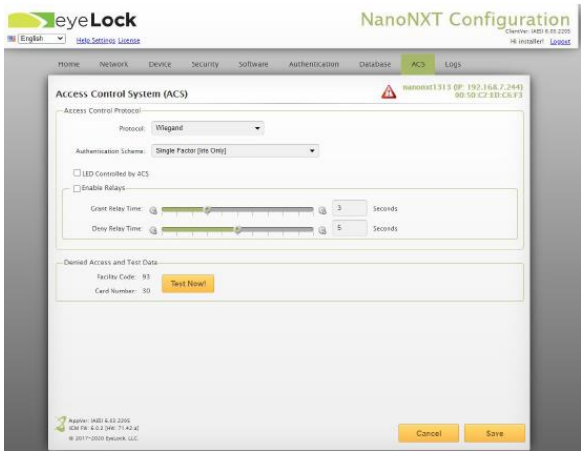


DETTAGLI SOFTWARE
Verificare la versione corrente del firmware del dispositivo ed eseguire l'aggiornamento del firmware da un file *.TAR memorizzato localmente.
Gli aggiornamenti software non cancelleranno il database utente.

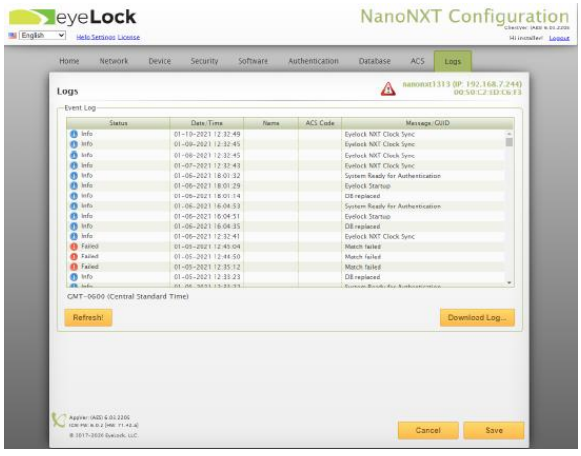


IMPOSTAZIONI DI AUTENTICAZIONE
Le impostazioni predefinite devono essere modificate solo se indicato dall'amministratore di rete/sicurezza.

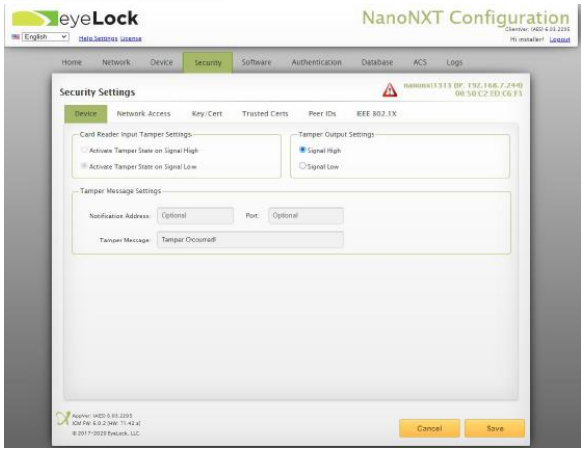
CONFIGURAZIONE DEL DATABASE
Configurazione per database / Network Matcher / Modelli portabili.



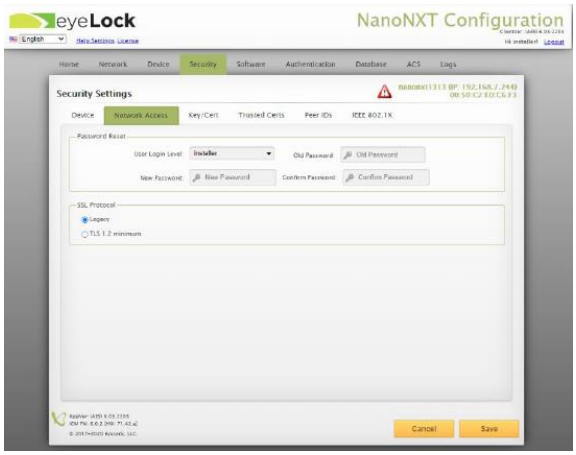
IMPOSTAZIONI DEL SISTEMA DI CONTROLLO ACCESSI
Selezione di Wiegand, OSDP, F2F o PAC dall'elenco a discesa Protocollo. Selezione dell'autenticazione a fattore singolo, doppio oa tre fattori [Iris, Card e PIN].



LOG
Visualizza i registri del dispositivo in ordine cronologico.
Il registro di sistema mostra fino alle ultime 5.000 azioni eseguite sul dispositivo. Per salvare il registro come file di testo, fare clic su Scarica registro.

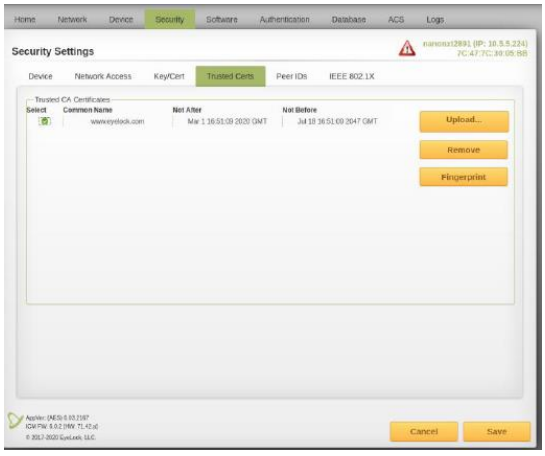


IMPOSTAZIONI DI SICUREZZA
Le impostazioni antimanomissione, la gestione delle chiavi e le password non devono essere modificate a meno che non siano state specificate dall'amministratore di rete/sicurezza.
Lo stato di manomissione attivo su segnale basso è selezionato per impostazione predefinita.



ACCESSO ALLA RETE
Selezionare la crittografia del traffico di rete – SSL (Legacy) / TLS. Si consiglia TLS.

CHIAVE / CERT
Impostare il modello di crittografia del traffico di rete del dispositivo. Usa chiave predefinita è per la chiave di crittografia configurata in fabbrica. Facendo clic su Usa chiave personalizzata inizierà il processo che consentirà all'utente di creare una chiave di crittografia univoca personalizzata per ciascun dispositivo. Usa chiave personalizzata Chiave e certificato personalizzati serve a stabilire una comunicazione sicura in stile PKI tra il dispositivo e il server EIS.

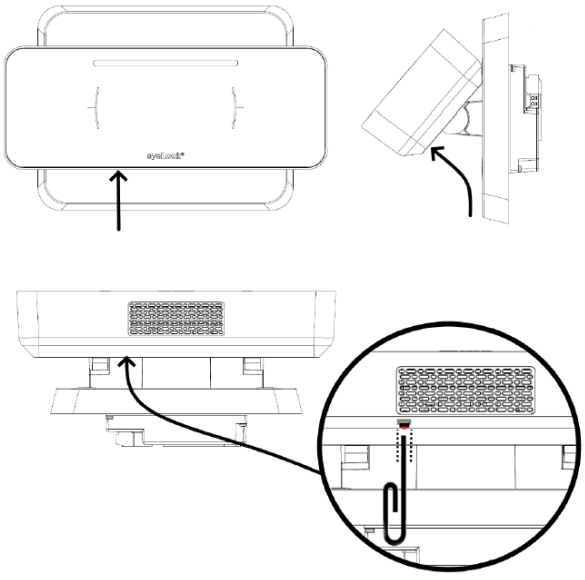


CERTIFICATO AFFIDABILE
Visualizza e gestisci i certificati di sicurezza utilizzati per crittografare il traffico di rete.

ID coetanei
Necessario per EyeLock Device PKI. Questo menu consente la configurazione degli ID Peer per gli host autorizzati a gestire il dispositivo.

802.1 X
Abilita IEEE 802.1X per utilizzare questo tipo di crittografia. Carica il certificato dell'autorità di certificazione (CA), il certificato del cliente e la chiave privata del cliente.

SOFT REBOOT



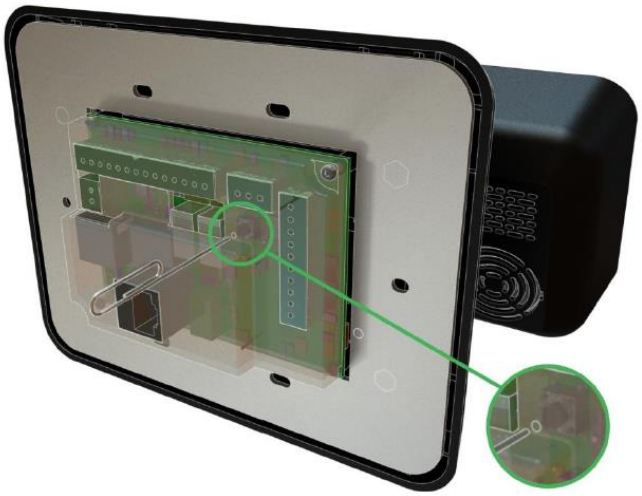
Per riavviare il dispositivo nano NXT, scollegalo e ricollegalo alla fonte di alimentazione. Se la fonte di alimentazione non è facilmente accessibile, eseguire il riavvio graduale.

Per riavviare il nano NXT, utilizzare una graffetta THIN e premere il pulsante situato nella parte posteriore del dispositivo come mostrato in figura. Il dispositivo si riavvierà senza perdere alcuna impostazione o eliminare il database.

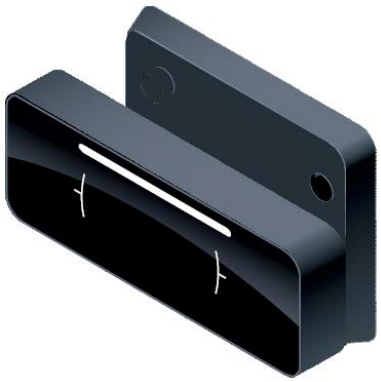
RIPRISTINO A IMPOSTAZIONI DI FABBRICA

Per ripristinare le impostazioni di fabbrica del nano NXT, tieni premuto il pulsante di ripristino sul retro del dispositivo per 10 secondi. Il dispositivo tornerà alle impostazioni di fabbrica iniziali e il database verrà cancellato. QUESTO NON PUÒ ESSERE DIMENTICATO.

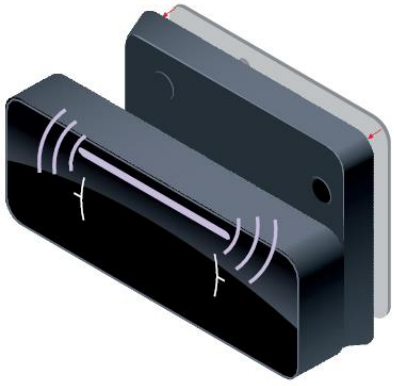
Il dispositivo può essere ripristinato tramite Webconfig. Facendo clic su RIPRISTINO DI FABBRICA nella pagina Webconfig → Dispositivo, il dispositivo ripristinerà le impostazioni di fabbrica ed eliminerà il database.



TAMPER



Il nano NXT è programmato per avvisare gli utenti in caso di manomissione. Si verifica una manomissione quando si tenta di rimuovere un dispositivo installato. L'avviso di manomissione si attiva non appena l'unità viene separata dalla piastra posteriore.



Quando il nano NXT è separato dalla piastra posteriore, l'uscita TAMPER fa suonare un allarme, accompagnato dal LED che mostra una luce viola fissa. Per fermare l'allarme e il LED, riattaccare l'unità alla piastra posteriore.

Webconfig può essere utilizzato per configurare le impostazioni del segnale di manomissione sia per il lettore di schede (solo doppia autenticazione) che per nano NXT. Per i lettori di tessere in cui la condizione di tamper per il lettore di tessere collegato è attiva su segnale basso, selezionare ATTIVA STATO TAMPER SU SEGNALE BASSO e fare clic su SALVA. Per i lettori di tessere in cui la condizione di tamper per il lettore di tessere collegato è attiva su segnale alto, selezionare ATTIVA STATO TAMPER SU SEGNALE ALTO e fare clic su SALVA. Il segnale varia in base al produttore. nano NXT è in grado di emettere SEGNALE ALTO o SEGNALE BASSO per adattarsi alle impostazioni previste dal sistema di controllo accessi.
Scegliere l'impostazione prevista dal sistema di controllo accessi e fare clic su SALVA.