# Aegis™ Secure Key 3


## Manuale dell'utente

# Indice

**(Revisione 02-19)**

# Importante

NON PREMERE ALCUN TASTO MENTRE LA CHIAVE USB AEGIS SECURE VIENE INSERITA NELLA PORTA USB DI UN COMPUTER. La pressione esercitata può danneggiare la porta USB causandone il malfunzionamento. Inserire tutti i PIN e le combinazioni di tasti PRIMA di inserire in una porta USB.

# Batteria

La chiave USB Aegis Secure è dotata di una batteria ricaricabile interna con circuito di caricamento smart. Per sicurezza, ciascuna chiave è confezionata con una carica parziale. Prima del primo utilizzo si raccomanda di collegare la chiave USB Aegis Secure a una porta USB per 80 minuti per caricare completamente la batteria. La batteria si caricherà automaticamente quando viene collegata a una porta USB. In Modalità bloccata, la spia LED **ROSSA** si spegne e si accende per indicare che il circuito di caricamento smart è attivo. Se la batteria è completamente scarica, la chiave USB Aegis Secure entrerà in Modalità auto-diagnostica al collegamento a una porta USB.


**Nota: Il Configuratore Aegis può essere utilizzato per configurare diversi prodotti Aegis Secure simultaneamente SOLTANTO se sul retro del dispositivo è presente il logo "Configurabile". In caso di utilizzo del Configuratore per impostare un prodotto Aegis Secure, NON eseguire i passaggi di seguito: il Configuratore Aegis è in grado di riconoscere soltanto i prodotti Aegis Secure in modalità Out-of-Box.**

# Aegis Keypad Panel


1 **UNLOCK** button

2 **LOCK** button

3 **LED** Indicator lights

**Ogni prodotto Aegis Secure è fornito senza PIN (Personal Identification Number) predefinito. Prima del primo utilizzo è necessario creare un PIN amministratore da 7-16 cifre. (Per i dispositivi non-FIPS è necessario creare un PIN da 6-16 cifre.) Il PIN amministratore può essere utilizzato per passare alla modalità amministratore in qualsiasi dispositivo o per accedere ai dati del prodotto Aegis Secure.**

# Modalità “Out-of- Box”

Ogni prodotto Aegis Secure è fornito senza PIN (Personal Identification Number) predefinito. Prima del primo utilizzo è necessario creare un PIN amministratore da 7-16 cifre. (Per i dispositivi non-FIPS è necessario creare un PIN da 6-16 cifre.) Il PIN amministratore può essere utilizzato per passare alla modalità amministratore in qualsiasi dispositivo o per accedere ai dati del prodotto Aegis Secure.

1. Premere 🔓 + 9 per avviare la Modalità registrazione.
2. Inserire una combinazione da 7-16 cifre per il PIN amministratore (vedi i requisiti PIN a pag. 4) e premere il tasto 🔓. *
3. Reinserire lo stesso PIN e premere 🔓 di nuovo.
4. Il prodotto Aegis Secure è ora in Modalità amministratore, dalla quale è possibile avviare le diverse funzioni. (ad es., aggiungere un utente).

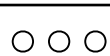
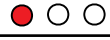
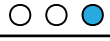
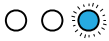
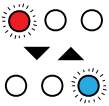
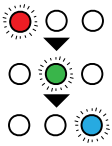
* **La spia LED VERDE lampeggerà se il PIN viene accettato; se il PIN NON viene accettato, la spia LED ROSSA lampeggerà—inserire un codice PIN valido due volte per completare la procedura di Registrazione amministratore. (vedi modalità LED a pag. 6).**

**Requisiti PIN**

I PIN devono contenere un minimo di sette caratteri e un massimo di sedici. Un PIN non può contenere numeri in sequenza (ad es., 01234567, 9876543) e non può contenere lo stesso numero ripetuto (ad es., 1111111, 2222222). *

***In sequenza, 0 ricorre prima di 1, NON dopo di 9.**

# GLI STATI DEI LED E IL LORO SIGNIFICATO

| | | |
|---|---|---|
|  | LED **ROSSA** che lampeggia lentamente | Batteria in caricamento (se collegata a una porta USB) |
|  | Nessuna spia LED | Il dispositivo è bloccato, l'interruttore è spento, il dispositivo è scollegato |
|  | **ROSSO** lampeggiante | Errore/immissione tasto errata; Modalità Non Disponibile; Modifica PIN utente |
|  | **ROSSO** fisso | Bloccato/stato di stand-by; In attesa di inserimento PIN |
|  | **VERDE** lampeggiante | Immissione tasto accettata |
|  | **BLU** fisso / **VERDE** lampeggiante | In attesa di creazione nuovo PIN Utente o Amministratore |
|  | **BLU** fisso | Modalità Amministratore |
|  | **VERDE** fisso | Il dispositivo è sbloccato |
|  | **BLU** lampeggiante lento | Il dispositivo è sbloccato in Modalità Superamento Blocco |
|  | **VERDE** fisso / **ROSSO** lampeggiante lento | Il dispositivo è sbloccato in Modalità Sola Lettura |
|  | IN ALTERNANZA **ROSSO** / **BLU** | Indica una modalità inserita che può causare l'eliminazione di un Utente o dei dati sul disco (a seconda della modalità scelta).<br><br>Anche utilizzata nell'impostazione Blocco automatico |
|  | Un secondo di luce **ROSSA** seguito da un secondo di luce **VERDE** seguito da un secondo di luce **BLU** | Modalità test automatico (eseguita automaticamente durante l'avvio), garantisce che tutti i componenti siano pronti e funzionanti |
|  | Tre secondi di **ROSSO** / **VERDE** fisso | Durante la procedura di ripristino indica il ripristino corretto dei parametri di sicurezza crittografica |

# Modalità Amministratore

Per accedere ai controlli delle funzioni l'operatore deve accedere prima alla Modalità amministratore, dalla quale è possibile gestire le diverse funzioni premendo la rispettiva combinazione di tasti (vedi Guida rapida a pag. 24). In modalità amministratore, i dati del prodotto Aegis Secure NON saranno accessibili. Dopo trenta secondi di inattività o premendo il tasto 🔒 il prodotto Aegis Secure tornerà alla Modalità bloccata. Eseguire i passaggi di seguito per tornare alla Modalità amministratore.

1. Premere e tenere premuto 🔓 + 0 per cinque secondi finché la spia LED **ROSSA** non lampeggia una volta al secondo.
2. Reinserire il PIN amministratore e premere 🔓.
3. Il prodotto Aegis Secure è ora in Modalità amministratore.
4. Per uscire dalla Modalità amministratore attendere trenta secondi di inattività o premere il tasto 🔒.

# Modificare il PIN amministratore

1. Accedere alla Modalità amministratore.
2. Premere (🔓 + 9) per avviare la Modalità registrazione.
3. Inserire una nuova combinazione da 7-16 cifre per il PIN amministratore e premere il tasto 🔓.
4. Reinserire lo stesso PIN e premere 🔓 di nuovo.

# Modalità Bloccata

Per sbloccare un dispositivo bloccato premere il tasto 🔒. Se l'operazione è riuscita la spia LED **ROSSA** si illuminerà fissa. I prodotti Aegis Secure NON verranno riconosciuti da alcun sistema operativo in modalità bloccata.*

* *Nel caso in cui vengano scritti dati sul prodotto Aegis Secure, la modalità bloccata verrà rinviata fino al completamento dell'operazione.*

# Modalità Sbloccata

1. Il prodotto Aegis Secure è ora in Modalità bloccata.
2. Per le chiavi USB Aegis Secure, inserire un PIN e premere il tasto 🔓. Collegare la chiave a una porta USB entro trenta secondi o il prodotto Aegis Secure tornerà in Modalità bloccata. Per tutti gli altri.

# PIN utente

***Nota: Questa pagina è relativa SOLTANTO al PIN utente, non leggere se si intende utilizzare il PIN amministratore per accedere ai dati del prodotto Aegis Secure.***

*La maggior parte dei prodotti Aegis Secure aderiscono allo standard FIPS 140-2; i modelli non-FIPS e FIPS Livello 2 consentono un massimo di un amministratore e quattro utenti; i modelli FIPS Livello 3 consentono soltanto un amministratore e un utente. Aggiungere un PIN utente è un modo ideale per condividere in modo sicuro il prodotto Aegis Secure o configurarlo per l'utilizzo in situazioni in cui l'operatore NON necessiti delle funzionalità amministratore. Il PIN utente non ha diritti di amministratore, tuttavia l'operatore può comunque accedere ai dati, modificare il PIN utente e abilitare la modalità sola lettura.*

Esistono due modi per configurare il PIN utente:

**A.) PIN GENERATO DALL'AMMINISTRATORE**

1. Accedere alla Modalità amministratore.
2. Premere i tasti 🔓+1 insieme per avviare la Modalità registrazione.
3. Inserire una combinazione da 7-16 cifre per il PIN utente e premere il tasto 🔓 (da 6-16 cifre per i modelli non FIPS.)
4. Reinserire lo stesso PIN e premere il tasto 🔓 di nuovo.

**B.) MODALITÀ REGISTRAZIONE FORZATA DELL'UTENTE**

**Avvertenza di sicurezza per la modalità di registrazione forzata dell'utente:**

**Una volta in Modalità registrazione forzata dell'utente, il prodotto Aegis Secure appare in Modalità "Out-of-Box" ma è in Modalità registrazione. Pertanto, NON caricare dati sensibili sul prodotto Aegis Secure se si sta per avviare la Registrazione forzata dell'utente.**

1. Accedere alla Modalità amministratore.
2. Premere 0 + 1 insieme per passare alla Modalità registrazione forzata dell'utente.
3. Premere il tasto 🔒.
4. Premere 🔓+1 per avviare la Modalità registrazione.
5. Inserire una combinazione da 7-16 cifre per il PIN utente e premere il tasto 🔓.
6. Reinserire lo stesso PIN e premere 🔓 di nuovo.

# Modificare il PIN Utente

1. Accedere alla Modalità sbloccata con il PIN utente.
2. Premere e tenere premuti i tasti 🔓 + 1 insieme per cinque secondi.
3. Inserire il PIN utente attuale per avviare la Modalità registrazione.
4. Inserire una nuova combinazione da 7-16 cifre per il PIN utente e premere il tasto 🔓.
5. Reinserire lo stesso PIN e premere il tasto 🔓 di nuovo.

# PIN di Ripristino Monouso

In caso di smarrimento del PIN, i PIN di ripristino monouso creano uno stato di Registrazione forzata dell'utente in cui è possibile creare un nuovo PIN utente senza eliminare i dati del dispositivo. È possibile registrare fino a quattro PIN di ripristino monouso nella modalità amministratore del dispositivo. Una volta implementato, un PIN di ripristino non potrà più essere utilizzato.

**NOTA IMPORTANTE:** I PIN di ripristino devono essere usati esclusivamente in caso di recupero di PIN smarriti. Se si sospetta che un PIN sia compromesso o sia stato rubato, eseguire la **Eliminazione/modifica del PIN utente** o il procedimento di **Ripristino completo**.

**Nota: I PIN di ripristino NON accederanno alla Modalità sbloccata ma metteranno il prodotto Aegis Secure in modalità Registrazione forzata dell'utente, dalla quale l'operatore potrà creare un nuovo PIN utente.**

1. Accedere alla Modalità amministratore.
2. Premere il tasto 🔓 + 8 per avviare la Modalità registrazione.
3. Inserire una combinazione da 7-16 cifre per il PIN di ripristino e premere il tasto 🔓.
4. Reinserire lo stesso PIN e premere il tasto 🔓 di nuovo.
5. Per aggiungere più PIN di ripristino ripetere i passaggi 2-4.

# Uso di un PIN di ripristino monouso

1. Premere e tenere premuti i tasti 🔓 + 7 insieme per cinque secondi.
2. Inserire un PIN di ripristino e premere il tasto 🔓 per avviare la Modalità registrazione.
3. Inserire una combinazione da 7-16 cifre per il PIN utente e premere il tasto 🔓.
4. Reinserire lo stesso PIN e premere il tasto 🔓 di nuovo.

# PIN auto- distruggente

I prodotti Aegis Secure possono impostare un PIN auto- distruggente che può essere utilizzato come misura finale per evitare la compromissione dei dati. Per impostazione predefinita, i PIN auto-distruggenti sono disabilitati. Se inserito in Modalità bloccata, il PIN auto- distruggente eliminerà tutti i PIN e tutti i dati, eseguirà una cripto-cancellazione, genererà un nuovo codice di cifratura, imposterà il PIN auto-distruggente come nuovo PIN amministratore e tenterà di accedere alla Modalità sbloccata, tuttavia il dispositivo dovrà essere inizializzato e formattato prima dell'uso. (Vedi Inizializzazione e formattazione, pag. 17).

1. Accedere alla Modalità amministratore.
2. Premere i tasti (7-4) insieme per attivare il PIN auto-distruggente. *

(I seguenti passaggi possono essere completati in Modalità amministratore o in Modalità sbloccata)

3. Premere e tenere premuti 🔓 + 3 insieme per avviare la Modalità registrazione PIN auto-distruggente.
4. Inserire una combinazione da 7-16 cifre per il PIN auto-distruggente e premere il tasto 🔓.
5. Reinserire lo stesso PIN e premere il tasto 🔓 di nuovo.
6. Il PIN auto-distruggente è ora attivo.

**UTILIZZARE CON CAUTELA**

*Disabilitare il PIN auto-distruggente dopo averne creato uno eliminerà tale PIN auto-distruggente creato.

NOTA: Dopo l'avvio di una sequenza di autodistruzione, è necessario eseguire un Ripristino utente per creare un nuovo PIN auto-distruggente.

# Eliminazione PIN

La procedura di Eliminazione PIN eliminerà tutti i PIN di ripristino, il PIN auto-distruggente e il PIN utente.

1. Accedere alla Modalità amministratore.
2. Premere i tasti (7+8) insieme per cinque secondi per avviare la modalità Eliminazione PIN.
3. Premere ancora insieme i tasti (7 + 8) per cinque secondi.

# Modalità sola lettura o lettura/scrittura

La Modalità sola lettura è particolarmente utile per prevenire la penetrazione di virus in caso di accesso ai dati da postazioni pubbliche, ed è una funzione importante per le applicazioni forensi che richiedono che i dati vengano preservati in modo inalterato. L'abilitazione corretta della Modalità di sola lettura è indicata da una spia LED **VERDE** singola che lampeggia in alternanza con una spia LED **VERDE** e **ROSSA**.

## Per abilitare la Modalità sola lettura dalla Modalità amministratore:

1. Accedere alla Modalità amministratore.
2. Premere i tasti 7 (r) + 6 (o) insieme per cinque secondi per avviare la Modalità sola lettura.
3. Per abilitare la Modalità lettura/scrittura premere e tenere premuti i tasti 7 (r) + 9 (w) insieme per cinque secondi.*

## Per abilitare la Modalità sola lettura dalla Modalità bloccata (utente):

1. Riattivare il dispositivo premendo il tasto 🔓 o 🔒 se già sbloccato.
2. Premere e tenere premuti i tasti 7 (r) + 6 (o) insieme per cinque secondi per avviare la Modalità sola lettura. Tre spie LED **VERDI** lampeggeranno rapidamente seguite da una spia LED **ROSSA** fissa che indica l'attivazione della modalità. Mentre la spia LED **ROSSA** è illuminata, inserire il PIN utente e premere [Sblocca]. La mancata autenticazione prima dell'attivazione della spia LED **ROSSA** disattiverà la variazione di modalità in sola lettura.
3. Per abilitare la Modalità lettura/scrittura premere e tenere premuti i tasti 7 (r) + 9 (w) insieme per cinque secondi. Dopo i tre lampeggiamenti rapidi in **VERDE** e mentre la spia LED **ROSSA** è illuminata, inserire il PIN utente e premere 🔓. La mancata autenticazione prima dell'attivazione della spia LED **ROSSA** disattiverà la variazione di modalità in lettura/scrittura.

* La Modalità lettura/scrittura attivata dalla Modalità amministratore avrà priorità globale su una Modalità sola lettura impostata dalla Modalità bloccata. Se la Modalità sola lettura è attivata in Modalità amministratore, la Modalità amministratore sarà il SOLO modo per abilitare la Modalità lettura/scrittura.

# Modalità blocco automatico imprevisto

I prodotti Apricorn Secure possono essere impostati affinché entrino in Modalità bloccata dopo un periodo predeterminato di inattività come protezione contro gli accessi non autorizzati se lasciati incustoditi in Modalità sbloccata. Per impostazione predefinita la funzionalità Blocco automatico incustodito è disabilitata. La funzionalità Blocco automatico incustodito può essere impostata per cinque, dieci o venti minuti di inattività.

1. Accedere alla Modalità amministratore.
2. Premere 🔓 + 6 per avviare la Modalità blocco automatico incustodito. *
3. Premere uno dei numeri di seguito: 0 = OFF
   1 = Cinque minuti
   2 = Dieci minuti
   3 = Venti minuti

***La Modalità blocco automatico incustodito ignorerà la Modalità superamento blocco.**

# Modalità superamento blocco

Taluni casi d'utilizzo prevedono che il prodotto Aegis Secure rimanga in Modalità sbloccata; nel corso di un riavvio, durante il passaggio a una macchina virtuale o altre situazioni che, in circostanze normali, farebbero entrare il prodotto Aegis Secure in Modalità bloccata. Per gestire queste situazioni, la Modalità superamento blocco (segnalata da spie LED lampeggianti intermittenti **VERDE** e **BLU**/**VERDE**) abiliterà la Modalità sbloccata tramite una ri-numerazione delle porte USB finché non viene interrotta l'alimentazione USB. In Modalità superamento blocco, il prodotto Aegis Secure può essere spostato da un computer all'altro purché rimanga collegato a una sorgente di alimentazione USB, ad es. un hub alimentato o un cavo a Y. A causa della sua vulnerabilità, Apricorn raccomanda caldamente di utilizzare la Modalità superamento blocco SOLO in circostanze in cui il prodotto Aegis Secure possa essere messo in sicurezza fisicamente (ad es., stanza server chiusa a chiave) o monitorato a vista.

1. Accedere alla Modalità amministratore.
2. Premere 7 + 1 insieme per abilitare la Modalità superamento blocco. *
3. Premere 7 + 0 insieme per abilitare la Modalità superamento blocco. **

***La Modalità blocco automatico incustodito ignorerà la Modalità superamento blocco**

****Riportare sempre la Modalità superamento blocco del prodotto Aegis Secure su OFF in caso di ritorno al funzionamento normale.**

# Modalità lampeggiamento LED

Genera un effetto lampeggiante nelle spie LED alla pressione dei tasti.

1. Accedere alla Modalità amministratore.
2. Premere (0 + 3) insieme per abilitare la Modalità lampeggiamento LED.
3. Premere (0 + 4) insieme per disabilitare la Modalità lampeggiamento LED.

# Lunghezza minima PIN

La lunghezza minima PIN impostata è pari a 7 caratteri, tuttavia, per garantire una maggiore sicurezza, è possibile implementare requisiti minimi per il PIN fino a 16 caratteri.

1. Accedere alla Modalità amministratore.
2. Premere i tasti 🔓 + 4, la spia LED ROSSA lampeggerà una volta al secondo.
3. Premere due cifre per la lunghezza minima del PIN (ad es.,: 08 = 8 caratteri, 11 = 11 caratteri, ecc.)

# Modalità brute-force

Un attacco brute-force è un metodo di violazione di uno schema di protezione dei dati crittografati che prevede l'esecuzione sistematica di un numero astronomico di possibilità di decifrazione. Il protocollo AES 256 garantisce una migliore protezione dei dati presenti sul prodotto Aegis Secure contro gli attacchi brute-force per ottenere i PIN. Di norma i PIN sono l'anello più debole di qualsiasi piano di protezione dati, e pertanto i PIN sono sostanzialmente tutto ciò che un attacco brute- force ha necessità di decifrare.

Per impostazione predefinita, il numero di tentativi brute-force per l'inserimento dei PIN è dieci. (ovvero, sono disponibili dieci tentativi di inserimento del PIN prima che venga avviata la Modalità brute-force, e dieci ulteriori tentativi di inserimento del PIN dopo il codice "LastTry", per un totale di 20 tentativi). Una volta che tutti i tentativi di inserimento PIN brute-force sono stati utilizzati, il prodotto Aegis Secure dovrà essere ripristinato, inizializzato e formattato prima dell'uso.

1. La spia LED **ROSSA** lampeggerà un numero di volte pari ai tentativi di inserimento PIN falliti a partire dal terzo fino al decimo (e finale) tentativo prima che la modalità brute-force venga inizializzata.
2. Il decimo tentativo di inserimento PIN non riuscito causerà il blocco del tastierino, non sarà possibile accedere a nessuna funzione e la spia LED **ROSSA** lampeggerà al ritmo di tre lampeggiamenti al secondo.
3. Il prodotto Aegis Secure consentirà ulteriori dieci tentativi di inserimento PIN prima che il prodotto Aegis Secure elimini tutti i dati. Per ottenere questi dieci tentativi extra, premere i tasti 🔓 + 5 insieme, le spie LED **ROSSA** e **VERDE** lampeggeranno in modo alternato.
4. Inserire il codice "LastTry" (5278879) e premere il tasto 🔓 per consentire dieci tentativi aggiuntivi. *

***L'attivazione della Modalità sbloccata riporterà il contatore della Modalità brute-force a zero.***

Il numero di tentativi di inserimento PIN prima che la Modalità brute-force elimini tutti i dati può essere impostata fra due e dieci. Impostando i tentativi PIN al minimo di due consentirà un totale di quattro tentativi (due prima del codice "LastTry" e due dopo).

Per modificare il numero di tentativi brute-force:

1. Accedere alla Modalità amministratore.
2. Premere e tenere premuti 🔓 + 5 insieme per tre secondi. La spia LED ROSSA lampeggerà due volte.
3. Premere due cifre per impostare il numero di tentativi di inserimento PIN in Modalità brute-force.

# Ripristino completo

In determinate circostanze (PIN dimenticato, redistribuzione dei dispositivi, ritorno alle impostazioni predefinite di fabbrica) potrebbe essere necessario un Ripristino completo. Il Ripristino completo eliminerà tutti i PIN e i dati, eseguirà una cripto-cancellazione, genererà un nuovo codice di cifratura e riporterà tutte le impostazioni ai valori di fabbrica predefiniti.

1. Premere e tenere premuto 🔒 + 🔓 + 2 insieme per cinque secondi per avviare il Ripristino completo.
2. Le spie LED indicheranno la Modalità di ripristino crittografico.
3. Una volta che il prodotto Aegis Secure è entrato in Modalità "Out-of-Box", il ripristino è completo.

# Inizializzazione e formattazione

Il Ripristino completo eliminerà tutti i PIN, i dati e le impostazioni di partizione; eseguirà una cripto- cancellazione, genererà un nuovo codice di cifratura e riporterà tutte le impostazioni ai valori di fabbrica predefiniti, richiedendo l'esecuzione di inizializzazione e formattazione.

**A.) Windows 7, 8, e 10**

1. Creare il PIN amministratore.
2. Accedere alla Modalità sbloccata con il PIN amministratore.
3. Windows 7 e precedenti: Dal menu Start fare clic con il tasto destro su "Il mio computer" e selezionare "Gestisci".

a. Nel pannello più a sinistra di "Gestione computer", selezionare "Gestione disco".

**Windows 8, 8.1, o 10: Fare clic con il tasto destro su "Start" e selezionare "Gestione disco".**

4. In "Gestione disco" il prodotto Aegis Secure apparirà come "Non inizializzato" e "Non allocato". Fare clic con il tasto destro sulla casella "Non inizializzato" e selezionare "Inizializza disco".
5. Fare clic su "Ok" nella finestra pop-up che si aprirà.
6. Fare clic con il tasto destro sulla casella "Non allocato" e selezionare "Nuovo volume semplice".
7. Seguire le indicazioni della "Procedura guidata nuovo volume semplice", selezionare il disco, il file system, l'etichetta del volume e fare clic su "Termina".

**B.) macOS**

1. Creare il PIN amministratore.
2. Accedere alla Modalità sbloccata con il PIN amministratore.
3. Fare clic su "Ignora" nella finestra pop-up che si aprirà.
4. Aprire l'app "Utilità disco".
5. Selezionare il dispositivo "Apricorn" dall'elenco di dispositivi "Esterni".
6. Fare clic sul tasto "Cancella".
7. Seguire le istruzioni per selezionare nome, formato, schema e fare clic su "Cancella".

**C.) Linux**

1. Creare il PIN amministratore.
2. Accedere alla Modalità sbloccata con il PINamministratore.
3. Aprire l'applicazione "Dischi".
4. Selezionare il dispositivo "Apricorn" dal pannellosinistro.
5. Fare clic sull'icona in "Volumi" e selezionare "Altre opzioni di partizione".
6. Selezionare "Formatta partizione..."
7. Seguire le istruzioni per selezionare nome,formato e fare clic su "Formatta".

# La Modalità diagnostica

a Modalità diagnostica è in grado di verificare il funzionamento corretto del tastierino e identificare i problemi. La Modalità diagnostica NON consente l'accesso ai dati né alla modalità amministratore.

1. Dalla Modalità bloccata premere 🔒 + 1, rilasciare, quindi tenere premuto il tasto (0) per cinque secondi.
2. La spia LED **BLU** lampeggerà diverse volte per indicare il numero delle revisioni minori e maggiori. Il punto decimale verrà rappresentato da un lampeggiamento singolo della spia LED **ROSSA.** Al termine, la spia LED **BLU** si illuminerà fissa. (ad es., la versione 7.8 sarà indicata da sette lampeggiamenti LED **BLU**, un lampeggiamento LED **ROSSO**, otto lampeggiamenti LED **BLU** e un lampeggiamento LED **ROSSO** .
3. Per testare la funzionalità del tastierino premere ogni tasto, il numero di tasti premuti verrà indicato da alcuni lampeggiamenti LED **ROSSI**. (Esempio: Tasto 1 = un lampeggiamento, tasto 2 = due lampeggiamenti ... Tasto 0 = dieci lampeggiamenti, tasto 🔒 = undici lampeggiamenti, tasto 🔓 = dodici lampeggiamenti).
4. Per uscire dalla Modalità diagnostica attendere 12-20 secondi di inattività, tenere premuto il tasto 🔒 per tre secondi o scollegare il dispositivo dalla porta USB/sorgente di alimentazione.

**Modalità auto-diagnostica:**

Nel corso dell'accensione ogni prodotto Aegis Secure eseguirà un'auto-diagnosi dell'algoritmo di cifratura e dei componenti hardware fondamentali, indicata da tre lampeggiamenti LED, uno **ROSSO**, uno **VERDE**, uno **BLU**. Se la spia LED **ROSSA** lampeggia in modo continuo prima dell'ingresso in modalità Standby, provare una porta USB diversa. Se la spia LED **ROSSA** continua a lampeggiare come indicato sopra e non riesce ad accedere alla Modalità sbloccata da una porta USB diversa, ciò significa che un componente critico è guasto e che pertanto il prodotto Aegis Secure non può più funzionare.

Se la spia LED **ROSSA** lampeggia tre volte in due secondi in Modalità sbloccata, ciò significa che si è verificato un guasto che NON arresterà immediatamente il prodotto Aegis Secure e non ne comprometterà la sicurezza. Le funzionalità di amministrazione potrebbero invece essere limitate, e questa modalità rappresenta un avvertimento che invita a sostituire il prodotto Aegis Secure al più presto possibile.

Se qualcuna di queste condizioni si verifica, rimuovere dalla porta USB, attendere che il prodotto Aegis Secure entri in modalità Standby e riprovare. Entrambi gli eventi saranno estremamente rari, tuttavia se il prodotto Aegis Secure non è in grado di ripristinare le normali indicazioni LED, deve essere sostituito il prima possibile.

# Ibernazione, uscita o sospensione

Prima di eseguire qualsiasi ibernazione, uscita o sospensione su un prodotto Aegis Secure o sul sistema operativo host si raccomanda di salvare e chiudere tutti i file. Da "Esplora risorse" o "Gestione disco" selezionare il simbolo "Espelli" o "Rimozione sicura hardware" per rimuovere il prodotto Aegis Secure dal sistema. Si raccomanda di portare il prodotto Aegis Secure in Modalità bloccata prima di qualsiasi operazione di ibernazione, uscita o sospensione.

Per garantire l'integrità dei dati il prodotto Aegis Secure deve trovarsi in Modalità bloccata se lasciato incustodito in aree pubbliche.

# Risoluzione dei problemi

**D: Che cosa succede se il PIN utente viene smarrito o dimenticato?**

R: Se è stato creato un PIN di ripristino l'operatore può usarlo per creare un nuovo PIN utente. In caso contrario è possibile utilizzare un PIN utente per creare un PIN di ripristino.

**D: Che cosa succede se il PIN amministratore viene smarrito o dimenticato?**

R: Non vi è modo di recuperare un prodotto Aegis Secure se il PIN amministratore viene smarrito o dimenticato, sarà necessario un Ripristino completo

**D: Perché il sistema operativo non ha riconosciuto il prodotto Aegis Secure dopo un Ripristino completo?**

R: Il prodotto Aegis Secure deve essere inizializzato e formattato. (Vedi Inizializzazione e formattazione, pag. 16)

**D: I prodotti Aegis Secure possono essere usati senza un PIN?**

R: I prodotti Aegis Secure non possono essere usati senza un PIN.

**D: Quale algoritmo di cifratura è utilizzato in questo prodotto?**

R: I prodotti Aegis Secure utilizzano l'algoritmo AES 256-bit.

**D: Perché il prodotto Aegis Secure non riesce ad eseguire inizializzazione e formattazione?**

R: Windows richiede i privilegi di Amministratore per accedere allo strumento Gestione disco.

**D: La spia LED ROSSA lampeggia in ROSSO e il tastierino non risponde, perché?**

R: Il prodotto Aegis Secure ha registrato 10 tentativi di inserimento PIN errati ed è entrato in modalità brute-force. (vedi modalità LED a pag. 14)

**D: Il prodotto Aegis Secure sembra caldo al tatto, è normale?**

R: Sì. I prodotti Aegis Secure utilizzano il raffreddamento passivo per dissipare il calore.

**D: C'è un modo per recuperare i dati in caso di PIN dimenticato?**

R: Senza un PIN di ripristino o un PIN amministratore non è possibile recuperare i dati, tuttavia il prodotto Aegis Secure può essere ripristinato in Modalità "Out-of-Box".

**D: Perché la spia LED indica un errore quando cerco di cambiare un PIN?**

R: I requisiti PIN per i prodotti Aegis Secure devono soddisfare un livello di sicurezza minimo. Esistono diverse combinazioni NON consentite, ad esempio se includono numeri ripetuti o in sequenza; inoltre, il PIN deve contenere un minimo di sette cifre e un massimo di sedici.

# Guida rapida

### Modalità Bloccata

- Premere i tasti (7 + 6) insieme per cinque secondi = Modalità sola lettura
- Premere e tenere premuti i tasti (7 + 9) insieme per cinque secondi = Modalità lettura/ scrittura
- Premere 🔒 + 1 insieme, quindi tenere premuto (0) per cinque secondi = Modalità diagnostica

### Modalità utente

- Premere 🔓 + 1 insieme = Modifica PIN utente
- Premere 🔓 + 3 insieme = Modalità registrazione PIN auto-distruggente

### Modalità Amministratore

- Premere e tenere premuti 🔓 + 0 insieme per cinque secondi = Modalità amministratore
- Premere 🔓 + 1 insieme = Registrazione PIN utente
- Premere 🔓 + 3 insieme = Modalità registrazione PIN auto-distruggente
- Premere 🔓+ 4 = Modalità lunghezza minima PIN
- Premere 🔓 + 5 insieme = Modalità tentativi PIN brute-force
- Premere 🔓 + 6 = la Modalità blocco automatico incustodito
- Premere 🔓 + 7 insieme = Registrazione PIN utente monouso
- Premere 🔓 + 8 insieme = Utilizzo PIN ripristino monouso
- Premere 🔓 + 9 = Modalità modifica PIN amministratore
- Premere 7 + 1 insieme = Abilita superamento blocco
- Premere 7 + 0 insieme = Disabilita superamento blocco
- Premere 7 + 4 insieme = Attivazione PIN auto-distruggente
- Premere 7 + 6 insieme = Abilita Modalità sola lettura
- Premere 7 + 9 insieme = Disabilita Modalità sola lettura
- Premere 0 + 1 insieme = Abilita Modalità registrazione forzata utente
- Premere 0 + 3 insieme = Abilita Modalità lampeggiamento LED
- Premere 0 + 4 insieme = Disabilita Modalità lampeggiamento LED
- Premere e tenere premuti i tasti 7 + 8 insieme per cinque secondi = eliminazione PINs utente, auto-distruggente, e ripristino

# Assistenza tecnica

1. Sito Web Apricorn: **https://www.apricorn.com**
2. Scriveteci via email a **support@apricorn.com**
3. Contattate l'assistenza tecnica Apricorn al numero

**1-800-458-5448** dalle 8:00 alle 17:00 PST, da lunedì a venerdì.

# Informazioni di garanzia

**Garanzia limitata Apricorn:**
Apricorn offre una garanzia limitata di tre anni sulla chiave Aegis Secure e i tastierini Aegis. Apricorn offre una garanzia limitata di tre anni sul tastierino Aegis DT e Aegis DT FIPS. Il periodo di garanzia ha inizio dalla data di acquisto presso Apricorn o un rivenditore autorizzato.

**Dichiarazione di responsabilità e termini della garanzia:**
LA GARANZIA HA INIZIO DALLA DATA DI ACQUISTO E DEVE ESSERE VERIFICATA A FRONTE DI SCONTRINO DI VENDITA O FATTURA INDICANTE LA DATA DI ACQUISTO DEL PRODOTTO.

APRICORN, SENZA COSTI AGGIUNTIVI, PROVVEDERÀ A RIPARARE O SOSTITUIRE LE PARTI DIFETTOSE CON PARTI NUOVE O RICONDIZIONATE PARI AL NUOVO. TUTTE LE PARTI CAMBIATE E TUTTI I PRODOTTI SOSTITUITI AI SENSI DELLA PRESENTE GARANZIA DIVENTERANNO PROPRIETÀ DI APRICORN.

LA PRESENTE GARANZIA NON SI APPLICA A PRODOTTI NON ACQUISTATI DIRETTAMENTE PRESSO APRICORN O SUOI RIVENDITORI AUTORIZZATI NÉ A PRODOTTI DANNEGGIATI O RESI DIFETTOSI DALL'UTENTE: 1. IN CONSEGUENZA DI INCIDENTI, ABUSI, NEGLIGENZA, USO ERRATO O GUASTI E/O IMPOSSIBILITÀ DI RISPETTARE LE ISTRUZIONI SCRITTE FORNITE IN QUESTA GUIDA DI ISTRUZIONI: 2. CON L'USO DI PARTI NON PRODOTTE O VENDUTE DA APRICORN; 3. CON LA MODIFICA DEL PRODOTTO; OPPURE 4. IN CONSEGUENZA DI MANUTENZIONE, ALTERAZIONE O RIPARAZIONE DA PERSONE DIVERSE DA APRICORN. QUESTA GARANZIA NON COPRIRE USO E USURA NORMALI.

NESSUN'ALTRA GARANZIA, IMPLICITA O ESPLICITA, INCLUSE GARANZIE DI COMMERCIABILITÀ O IDONEITÀ A DETERMINATI SCOPI, VIENE O VERRÀ FORNITA DA O PER CONTO DI APRICORN O TRAMITE RICORSO ALLE LEGGI IN VIGORE IN RELAZIONE AL PRODOTTO O ALLA SUA INSTALLAZIONE, USO, SOSTITUZIONE O RIPARAZIONE.

APRICORN NON È DA RITENERSI RESPONSABILE, IN VIRTÙ DELLA PRESENTE GARANZIA O ALTRIMENTI, PER QUALSIASI DANNO ACCIDENTALE, SPECIALE O CONSEQUENZIALE INCLUSE PERDITE DI DATI CAUSATE DALL'USO DEL PRODOTTO, INDIPENDENTEMENTE DAL FATTO CHE APRICORN VENGA INFORMATA O MENO IN TAL SENSO.

APRICORN


12191 Kirkham Road,
Poway, CA, U.S.A. 92064
1-858-513-2000 www.apricorn.com