Aegis™ Secure Key 3z

Benutzer-handbuch

Inhaltsverzeichnis

(Überarbeitet 02-19)

Wichtig

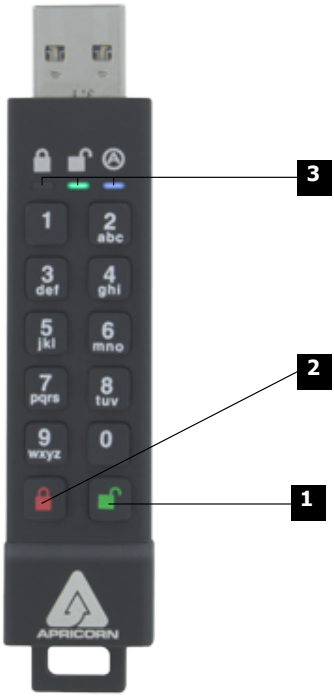
BETÄTIGEN SIE KEINE SCHALTFLÄCHEN, WÄHREND DER AEGIS SECURE KEY IN EINEM COMPUTER-USB-PORT STECKT. Der Abwärtsdruck kann den USB-Port beschädigen, wodurch er defekt werden kann. Geben Sie alle PINs und Schaltflächenkombinationen ein, BEVOR Sie das Gerät in einen USB-Port stecken.

Akku

Der Aegis Secure Key hat einen internen Akku mit Smart-Lademöglichkeit. Aus Sicherheitsgründen sind alle teilweise aufgeladen. Es wird empfohlen, vor dem ersten Gebrauch den Aegis Secure Key 80 Minuten lang in einem USB-Port vollständig zu laden. Der Akku lädt automatisch, wenn er mit einem USB-Port verbunden wird. Im gesperrten Modus wird die ROTE LED stärker und schwächer und zeigt an, dass das Smart-Charging aktiv ist. Falls der Akku vollständig leer ist, geht der Aegis Secure Key durch den Selbstdiagnose-Modus, wenn er mit einem USB-Port verbunden wird.

Hinweis: Der Aegis Configurator kann verwendet werden, um mehrere Aegis Secure-Produkte gleichzeitig zu konfigurieren, aber NUR, falls auf der Rückseite des Geräts das Logo „Configurable“ zu sehen ist. Falls Sie den Configurator verwenden, um Ihre Aegis Secure-Produkte einzurichten, führen Sie KEINEN der unten stehenden Schritte durch; der Aegis Configurator kann nur Aegis Secure-Produkte im Out-of-Box-Modus erkennen.

Aegis Padlock Keypad Panel



1	**UNLOCK** button
2	**LOCK** button
3	**LED** Indicator lights

Jedes Aegis Secure-Produkt wird ohne eine vorher festgelegte Persönliche Identifikationsnummer (PIN) geliefert. Vor dem ersten Gebrauch muss eine sieben- bis sechzehnstellige Admin-PIN eingerichtet werden. (Bei Nicht-FIPS-Geräten muss die PIN sechs bis sechzehn Stellen haben.) Die Admin-PIN kann verwendet werden, um Funktionen aus dem Admin-Modus aus zu aktivieren sowie um auf die Aegis Secure-Produktdaten zuzugreifen.

Out-of-Box-Modus

Jedes Aegis Secure-Produkt wird ohne eine vorher festgelegte Persönliche Identifikationsnummer (PIN) geliefert. Vor dem ersten Gebrauch muss eine sieben- bis sechzehnstellige Admin-PIN eingerichtet werden. (Bei Nicht-FIPS-Geräten muss die PIN sechs bis sechzehn Stellen haben.) Die Admin-PIN kann verwendet werden, um Funktionen aus dem Admin- Modus aus zu aktivieren sowie um auf die Aegis Secure- Produktdaten zuzugreifen.

1. Drücken Sie 🔓 + 9 gleichzeitig, um den Eintragungsmodus zu starten.
2. Geben Sie eine sieben- bis sechzehnstellige Kombination für die Admin-PIN ein (siehe PIN- Anforderungen auf Seite 4) und drücken Sie die Schaltfläche 🔓.*
3. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.
4. Das Aegis Secure-Produkt ist jetzt im Admin- Modus, wo die Funktionen aktiviert werden können (z. B. Hinzufügen eines Benutzers).

* **GRÜNE LED blinkt, wenn die PIN akzeptiert wurde; Falls die PIN nicht akzeptiert wurde, blinkt die ROTE LED. Geben Sie zweimal eine gültige PIN ein, um den Admin-Eintragungsprozess abzuschließen (siehe LED-Modi auf Seite 6).**

PIN-ANFORDERUNGEN

PINs müssen mindestens aus sieben und maximal aus sechzehn Zeichen bestehen. Eine PIN darf nicht nur aus sequenziellen Zahlen (z. B. 01234567, 9876543) und nicht nur aus derselben Zahl bestehen (z. B. 1111111, 2222222).*

***Sequenziell, 0 kommt vor 1, NICHT nach 9.**

LED-ZUSTÄNDE UND IHRE BEDEUTUNGEN

	Langsam erlöschende **ROT** LED	Akku lädt (bei Anschluss an den USB-Port)
	Keine LEDs	Gerät ist gesperrt, Leistungsschalter ausgeschaltet, Stecker ausgesteckt
	Blinkendes **ROT**	Fehler / falsche Schaltflächeneingabe; Modus nicht verfügbar; Änderung Benutzer-PIN
	Permanentes **ROT**	Gesperrt / Standby-Modus; PIN-Eingabe wird erwartet
	Blinkendes **GRÜN**	Schaltflächeneingabe akzeptiert
	Permanentes **BLAU** / Blinkendes **GRÜN**	Warten auf Erstellung eines neuen Benutzers oder Admin-PIN
	Permanentes **BLAU**	Admin-Modus
	Permanentes **GRÜN**	Gerät ist entsperrt
	Langsam blinkendes **BLAU**	Gerät ist entsperrt im Lock-Override-Modus
	Permanentes **GRÜN** Langsam blinkendes **ROT**	Gerät ist entsperrt im Nur-Lesen-Modus
	ABWECHSELND **ROT** / **BLAU**	Zeigt an, dass ein Modus eingegeben wurde, der zur Löschung eines Benutzers oder der Daten auf der Festplatte führen kann (abhängig vom ausgewählten Modus)
	Eine Sekunde **ROT**, dann eine Sekunde **GRÜN** und dann eine Sekunde **BLAU**	Selbsttest-Modus (automatische Aktivierung beim Start des Geräts) stellt sicher, dass alle Komponenten bereit sind und ordnungsgemäß funktionieren
	Drei Sekunden Permanentes **ROT** / **GRÜN**	Zeigt beim Reset-Prozess das erfolgreiche Zurücksetzen der kryptografischen Sicherheits-parameter an

Admin-Modus

Um auf Funktionssteuerungen zuzugreifen, muss der Bediener zuerst den Admin-Modus aktivieren, wo jede Funktion mit der jeweiligen Kombination ausgelöst werden kann (siehe Kurzanleitung auf Seite 24). Im Admin-Modus sind die Daten auf dem Aegis Secure- Produkt NICHT zugänglich. Bei dreißig Sekunden Inaktivität oder bei Betätigung der Schaltfläche 🔒 wird das Aegis Secure-Produkt zurück in den gesperrten Modus geschaltet. Führen Sie unten stehende Schritte aus, um erneut in den Admin-Modus zu gelangen.

1. Halten Sie 🔓 + 0 gleichzeitig fünf Sekunden lang gedrückt, bis die **ROTE** LED einmal pro Sekunde blinkt.
2. Geben Sie die Admin-PIN ein und drücken Sie die Schaltfläche 🔓.
3. Das Aegis Secure-Produkt ist jetzt im Admin- Modus.
4. Um den Admin-Modus zu verlassen, warten Sie entweder 30 Sekunden Inaktivität ab oder drücken Sie die Schaltfläche 🔒.

Ändern der Admin- PIN

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie 🔓 + 9 gleichzeitig, um den Eintragungsmodus zu starten.
3. Geben Sie eine neue sieben- bis sechzehnstellige Kombination für die Admin-PIN ein und drücken Sie die Schaltfläche 🔓.
4. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.

Gesperrter Modus

Um ein entsperrtes Gerät zu sperren, drücken Sie einfach auf die Schaltfläche 🔒. Falls es erfolgreich ist, leuchtet die **ROTE** LED durchgehend auf. Aegis Secure-Produkte werden von Betriebssystemen im gesperrten Modus NICHT erkannt.*

* *Falls immer noch Daten auf das Aegis Secure-Produkt geschrieben werden, wird der gesperrte Modus verzögert, bis der Betrieb abgeschlossen ist.*

Entsperrter Modus

1. Stellen Sie sicher, dass das Aegis Secure-Produkt im gesperrten Modus ist.
2. Geben Sie für Aegis Secure Keys eine PIN ein und drücken Sie die Schaltfläch 🔓. Stecken Sie es innerhalb von dreißig Sekunden in einen USB-Port, ansonsten geht das Aegis Secure-Produkt zurück in den gesperrten Modus. Für alle anderen Apricorn Secure Devices: Stecken Sie sie in einen USB-Port und in eine externe Stromversorgung (falls zutreffend), geben Sie eine PIN ein und drücken Sie die Schaltfläche 🔓.

Benutzer-PIN

Hinweis: Diese Seite bezieht sich NUR auf die Benutzer-PIN. Falls die Admin-PIN für den Zugriff auf die Daten des Aegis Secure-Produkts verwendet wird, ignorieren Sie diese Seite.

Die meisten Aegis Secure-Produkte erfüllen den FIPS 140-2-Standard. Nicht-FIPS- und FIPS-Level-2-Modelle ermöglichen einen Admin und vier Benutzer; FIPS-Level-3-Modelle ermöglichen nur einen Admin und einen Benutzer. Das Hinzufügen einer Benutzer-PIN ist eine perfekte Möglichkeit, um das Aegis Secure-Produkt sicher zu teilen oder für den Einsatz bereitzustellen, wenn der Bediener KEINEN Zugriff auf Admin-Funktionen benötigt. Die Benutzer-PIN hat keine Admin-Rechte, aber der Bediener hat trotzdem Zugriff auf die Daten, kann die Benutzer-PIN ändern und den Nur-Lesen-Modus aktivieren.

Es gibt zwei Möglichkeiten, die Benutzer-PIN zu erstellen:

A.) VOM ADMIN GENERIERTE PIN

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie 🔓 + 1 gleichzeitig, um den Eintragungsmodus zu starten.
3. Geben Sie eine sieben- bis sechzehnstellige Kombination (bei Nicht-FIPS-Modellen sechs- bis sechzehnstellig) für die Benutzer-PIN ein und drücken Sie die Schaltfläche 🔓.
4. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.

B.) VOM BENUTZER ERZWUNGENER EINTRAGUNGSMODUS

Sicherheitswarnung für eine vom Benutzer erzwungene Eintragung:

Sobald das Aegis Secure-Produkt im vom Benutzer erzwungenen Eintragungsmodus ist, scheint es im Out-of-Box-Modus zu sein, ist jedoch tatsächlich im Eintragungsmodus. Laden Sie deshalb KEINE sensiblen Daten auf das Aegis Secure-Produkt, wenn der vom Benutzer erzwungene Eintragungsmodus aktiv ist.

1. Starten Sie den entsperrten Modus mit der Benutzer-PIN.
2. Halten Sie die Schaltflächen 🔓+1 gleichzeitig fünf Sekunden lang gedrückt.
3. Drücken Sie die Schaltfläche 🔒.
4. Drücken Sie 🔓+1 gleichzeitig, um den Eintragungsmodus zu starten.
5. Geben Sie eine neue sieben- bis sechzehnstellige Kombination für die Benutzer-PIN ein und drücken Sie die Schaltfläche 🔓.
6. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.

Ändern der Benutzer-PIN

1. Starten Sie den entsperrten Modus mit der Benutzer-PIN.
2. Halten Sie die Schaltflächen 🔓 + 1 gleichzeitig fünf Sekunden lang gedrückt.
3. Geben Sie die aktuelle Benutzer-PIN ein, um den Eintragungsmodus zu starten.
4. Geben Sie eine neue sieben- bis sechzehnstellige Kombination für die Benutzer-PIN ein und drücken Sie die Schaltfläche 🔓.
5. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.

Einmal-Wiederherstellungs-PIN

Im Falle einer vergessenen Benutzer-PIN schaffen Einmal-Wiederherstellungs-PINs einen vom Benutzer erzwungenen Eintragungsmodus, indem eine neue Benutzer-PIN erstellt werden kann, ohne die Daten des Geräts zu löschen. Im Admin-Modus des Geräts können bis zu vier Einmal-Wiederherstellungs-PINs eingetragen werden. Sobald eine Wiederherstellungs-PIN verwendet wurde, kann sie nicht erneut eingesetzt werden.

WICHTIGER HINWEIS: Wiederherstellungs-PINs werden nur im Falle von vergessenen Benutzer-PINs eingesetzt. Falls eine **Benutzer-PIN** gefährdet oder gestohlen wurde, führen Sie stattdessen Benutzer-PIN **löschen/ändern** oder **Durchführen des vollständigen Zurücksetzens** durch.

Hinweis: Wiederherstellungs-PINs greifen NICHT auf den entsperren Modus zu, sondern bringen das Aegis Secure-Produkt in den vom Benutzer erzwungenen Eintragungsmodus, in dem der Bediener eine neue Benutzer-PIN erstellen kann.

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie 🔓 + 8 gleichzeitig, um den Eintragungsmodus zu starten.
3. Geben Sie eine sieben- bis sechzehnstellige Kombination für die Wiederherstellungs-PIN ein und drücken Sie die Schaltfläche 🔓.
4. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.
5. Um mehr Wiederherstellungs-PINs hinzuzufügen, wiederholen Sie die Schritte 2 bis 4.

Verwenden einer Einmal Wiederherstellungs PIN

1. Halten Sie die Schaltflächen 🔓 + 7 gleichzeitig fünf Sekunden lang gedrückt.
2. Geben Sie eine Wiederherstellungs-PIN ein und drücken Sie die Schaltfläche 🔓, um den Eintragungsmodus zu aktivieren.
3. Geben Sie eine sieben- bis sechzehnstellige Kombination für die Benutzer-PIN ein und drücken Sie die Schaltfläche 🔓.
4. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.

Selbstzerstörende PIN

Apricorn Secure Products können eine selbstzerstörende PIN erstellen, die als endgültige Maßnahme eingesetzt werden kann, um eine Datenkompromittierung zu verhindern. Standardmäßig ist die selbstzerstörende PIN deaktiviert. Vom gesperrten Modus aus löscht die selbstzerstörende PIN alle PINs, alle Daten, führt einen Crypto Erase durch, generiert einen neuen Verschlüsselungsschlüssel, legt die selbstzerstörende PIN als neue Admin-PIN fest und scheint den entsperrten Modus ganz normal zu aktivieren, muss jedoch vor dem Gebrauch initialisiert und formatiert werden (siehe Initialisieren und Formatieren auf Seite 17).

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie die Schaltflächen 7 und 4 gleichzeitig, um die selbstzerstörende PIN zu aktivieren.*

(Die folgenden Schritte können entweder im Admin- oder im entsperrten Modus durchgeführt werden)

3. Halten Sie 🔓 + 3 gleichzeitig gedrückt, um den Eintragungsmodus für die selbstzerstörende PIN zu starten.
4. Geben Sie eine sieben- bis sechzehnstellige Kombination für die selbstzerstörende PIN ein und drücken Sie die Schaltfläche 🔓.
5. Geben Sie die gleiche PIN erneut ein und drücken Sie die Schaltfläche 🔓.
6. Die selbstzerstörende PIN ist jetzt aktiv.
   MIT VORSICHT VERWENDEN

*Das Deaktivieren der selbstzerstörenden PIN nach der Einrichtung löscht diese selbstzerstörende PIN.

HINWEIS: Nach dem Starten einer selbstzerstörenden Sequenz muss ein Benutzer-Reset durchgeführt werden, um eine neue selbstzerstörende PIN zu erstellen.

PINs löschen

Das Löschen von PINs löscht alle Wiederherstellungs-PINs, die selbstzerstörende PIN und die Benutzer-PIN.

1. Aktivieren Sie den Admin-Modus.
2. Halten Sie die Schaltflächen 7 und 8 fünf Sekunden lang gedrückt, um den Modus zum Löschen der PINs zu starten.
3. Halten Sie die Schaltflächen 7 und 8 erneut fünf Sekunden lang gedrückt.

Nur-Lesen-Modus/Lesen-Schreiben-Modus

Der Nur-Lesen-Modus ist besonders nützlich, um eine Virusinfiltration zu verhindern, wenn auf Daten öffentlich zugegriffen wird. Er ist eine wichtige Funktion für forensische Anwendungen, bei denen Daten in einem ungeänderten Status erhalten werden müssen. Eine erfolgreiche Aktivierung des Nur-Lesen-Modus wird durch einmaliges Blinken der **GRÜNEN** LED angezeigt, die abwechselnd mit einer einmal blinkenden **GRÜNEN** und **ROTEN** LED aufblinkt.

Aktivieren des Nur-Lesen-Modus vom Admin-Modus aus:

1. Aktivieren Sie den Admin-Modus.
2. Halten Sie 7 (r) und 6 (o) gleichzeitig fünf Sekunden lang gedrückt, um den Nur-Lesen-Modus zu starten.
3. Um den Lesen-Schreiben-Modus zu aktivieren, halten Sie 7 (r) und 9 (w) gleichzeitig fünf Sekunden lang gedrückt.*

Aktivieren des Nur-Lesen-Modus vom gesperrten (Benutzer-) Modus aus:

1. Wecken Sie das Gerät entweder auf, indem Sie auf die Schaltfläche 🔓 oder 🔒 drücken, je nachdem, ob das Gerät bereits gesperrt ist oder nicht.
2. Halten Sie die Schaltflächen 7 (r) und 6 (o) fünf Sekunden lang gedrückt, um den Nur-Lesen-Modus zu starten. Die **GRÜNE** LED blinkt dreimal schnell auf, danach leuchtet die **ROTE** LED durchgehend auf, um zu zeigen, dass der Nur-Lesen-Modus aktiv ist. Während die **ROTE** LED aufleuchtet, geben Sie die BENUTZER-PIN ein und drücken Sie [Entsperren]. Wenn die Authentifizierung nicht erfolgt, bevor die **ROTE** LED erlischt, wird der Nur-Lesen-Modus abgebrochen.
3. Halten Sie die Schaltflächen 7 (r) und 9 (w) fünf Sekunden lang gedrückt, um den Lesen-Schreiben-Modus zu starten. Die **GRÜNE** LED blinkt dreimal schnell auf, danach leuchtet die **ROTE** LED durchgehend auf. Geben Sie die BENUTZER-PIN ein und drücken Sie 🔓. Wenn die **Authentifizierung** nicht erfolgt, bevor die **ROTE** LED erlischt, wird der Lesen-Schreiben-Modus abgebrochen.

* Lesen-Schreiben-Modus, aktiviert vom Admin-Modus aus, überschreibt global einen Nur-Lesen-Modus, der aus dem gesperrten Modus aus aktiviert wurde. Falls Nur-Lesen im Admin-Modus aktiviert ist, ist der Admin-Modus der EINZIGE Weg, den Lesen-Schreiben-Modus zu aktivieren.

Unbeaufsichtigter Auto-Sperrmodus

Apricorn Secure Products können nach einer vorher festgelegten Zeit der Inaktivität in den gesperrten Modus gebracht werden, um vor unautorisiertem Zugriff zu schützen, falls sie im entsperren Modus unbeaufsichtigt gelassen werden. Standardmäßig ist die Funktion Unbeaufsichtigte Auto-Sperre deaktiviert. Die Unbeaufsichtigte Auto-Sperre kann auf fünf, zehn oder zwanzig Minuten Inaktivität festgelegt werden.

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie 🔓 + 6 gleichzeitig, um den Unbeaufsichtigten Auto-Sperrmodus auszulösen.*
3. Drücken Sie eine der unten stehenden Zahlen:

    0 = AUS

    1 = Fünf Minuten

    2 = Zehn Minuten

    3 = Zwanzig Minuten

***Der unbeaufsichtigte Auto-Sperrmodus ignoriert den Lock-Override-Modus.**

Lock-Override-Modus

Bestimmte Anwendungsfälle involvieren, dass das Aegis Secure-Produkt im entsperren Modus bleibt; während eines Reboots, bei Passieren einer virtuellen Maschine oder einer ähnlichen Situation, die unter normalen Umständen dazu führen würde, dass das Aegis Secure-Produkt in den gesperrten Modus übergeht. Um diese Situationen zu berücksichtigen, ermöglicht der Lock-Override-Modus (angezeigt durch abwechselnd blinkende **GRÜNE** und **BLAUE** / **GRÜNE** LEDs) den entsperrten Modus durch eine Re-Enumeration des USB-Ports ermöglichen, bis die USB-Stromversorgung unterbrochen wird. Im Lock-Override-Modus ist das Aegis Secure-Produkt anfällig, von einem Computer zu einem anderen bewegt zu werden, vorausgesetzt, dass es mit der USB-Stromversorgung verbunden bleibt (z. B. einem mit Strom versorgten Hub oder einem Y-Kabel). Aufgrund dieser Anfälligkeit empfiehlt Apricorn besonders, dass der Lock-Override-Modus NUR in Fällen eingesetzt wird, in denen das Aegis Secure-Produkt physisch gesichert (z. B. geschlossener Serverraum) oder visuell überwacht werden kann.

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie gleichzeitig auf (7 und 1), um den Lock-Override-Modus zu aktivieren.*
3. Drücken Sie gleichzeitig auf (7 und 0), um den Lock-Override-Modus zu deaktivieren.**

***Der unbeaufsichtigte Auto-Sperrmodus ignoriert den Lock-Override-Modus.**

****Schalten Sie den Lock-Override-Modus des Aegis Secure-Produkts immer auf OFF (AUS), wenn Sie zum Normalbetrieb zurückkehren.**

LED-Flickermodus

Sorgt für einen Flickereffekt der LED-Leuchten, der positive Schaltflächenbetätigungen zeigt.

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie gleichzeitig auf (0 und 3), um den LED-Flickermodus zu aktivieren.
3. Drücken Sie gleichzeitig auf (0 und 4), um den LED-Flickermodus zu deaktivieren.

Mindestlänge PIN

Die Standard-Mindestlänge für PINs ist 7. Für eine höhere Sicherheit können jedoch längere PINs mit bis zu sechzehn Stellen eingesetzt werden.

1. Aktivieren Sie den Admin-Modus.
2. Drücken Sie 🔓 + 4. Die **ROTE** LED blinkt einmal pro Sekunde.
3. Drücken Sie zwei Ziffern für die Mindestlänge der PIN; (z. B. 08 = 8 Zeichen; 11 = 11 Zeichen usw.)

Brute-Force-Modus

Ein Brute-Force-Angriff ist eine Möglichkeit, ein kryptografisches Datenverteidigungsschema zu verletzen, indem systematisch eine astronomische Anzahl an Entschlüsselungsmöglichkeiten durchgeführt wird. Mithilfe von AES 256 werden die auf einem Aegis Secure-Produkt gespeicherten Daten mehr als nur gut vor Brute-Force-Angriffen geschützt, die darauf abzielen, Zugriff auf die PINs zu erhalten. PINs sind üblicherweise sie schwächsten Verbindungen eines jeden Datenschutzplans, und deshalb sind PINs im Wesentlichen das einzige, was Brute-Force-Angriffe entschlüsseln müssen.

Standardmäßig ist die Anzahl an Brute-Force-Modus PIN-Versuchen zehn. (Das heißt, es gibt zehn PIN-Versuche, bis der Brute-Force-Modus aktiviert wird, und zehn zusätzliche PIN-Versuche nach dem „Letzter Versuch"-Code, für insgesamt 20 PIN-Versuche.) Sobald alle Brute-Force-Modus-PINs verwendet wurden, muss das Aegis Secure-Produkt vor dem Gebrauch zurückgesetzt, initialisiert und formatiert werden.

1. Die **ROTE** LED blinkt die Anzahl der fehlgeschlagenen PIN-Versuche nach dem dritten bis hin zum zehnten (und letzten) PIN-Versuch, bevor der Brute-Force-Modus aktiviert wird.
2. Der zehnte nicht erfolgreiche PIN-Versuch führt dazu, dass das Keyboard nicht mehr reagiert, keine Funktionen mehr zugänglich sind und die **ROTE** LED in einer Geschwindigkeit von drei Blinkzeichen pro Sekunde aufblinkt.
3. Das Aegis Secure-Produkt ermöglicht bis zu zehn zusätzliche PIN-Versuche, bevor das Aegis Secure-Produkt alle Daten löscht. Um diese zehn zusätzlichen PIN-Versuche zu erhalten, drücken Sie gleichzeitig auf 🔓 + 5. Die **ROTE** und die **GRÜNE** LED leuchten abwechselnd auf.
4. Geben Sie den „Letzter Versuch"-Code (5278879) ein und drücken Sie die Schaltfläche 🔓, wodurch zehn zusätzliche Versuche erlaubt werden.*

Das Aktivieren des entsperrten Modus bringt den Brute-Force-Modus-Zähler auf Null.

Die Anzahl der PIN-Versuche, bevor der Brute-Force-Modus alle Daten löscht, kann zwischen zwei und zehn festgelegt werden. Das Einstellen von PIN-Versuchen auf das Minimum von zwei führt zu insgesamt vier Versuchen (zwei vor dem „Letzter Versuch"-Code und zwei danach.)

So wird die Anzahl der Brute-Force-Versuche geändert:

1. Aktivieren Sie den Admin-Modus.
2. Halten Sie die Schaltflächen 🔓 + 5 drei Sekunden lang gedrückt. Die **ROTE** LED blinkt doppelt.
3. Drücken Sie zwei Ziffern für die Anzahl der Brute-Force-Modus-PIN-Versuche.

Vollständiges Zurücksetzen

Es kann Umstände geben (vergessene PIN, Umstrukturierung, Zurücksetzen auf die Werkseinstellungen), die ein vollständiges Zurücksetzen erfordern. Das vollständige Zurücksetzen löscht alle PINs, alle Daten, führt einen Crypto Erase durch, generiert einen neuen Verschlüsselungsschlüssel und setzt alle Einstellungen auf den Werksmodus zurück.

1. Halten Sie 🔒 + 🔓 + 2 zehn Sekunden lang gedrückt, um das vollständige Zurücksetzen zu starten.
2. Die LEDs zeigen den kryptografischen Reset-Modus.
3. Sobald das Aegis Secure-Produkt den Out-of-Box-Modus startet, ist das Zurücksetzen abgeschlossen.

Initialisieren und Formatieren

Bei einem vollständigen Zurücksetzen werden alle PINs, Daten und Partitionseinstellungen gelöscht, einen Crypto Erase durchgeführt, ein neuer Verschlüsselungsschlüssel generiert und alle Einstellungen auf den Werksmodus zurückgesetzt, wodurch eine Initialisierung und Formatierung erforderlich werden.

A.) Windows 7, 8, und 10

1. Erstellen Sie die Admin-PIN.
2. Starten Sie den entsperrten Modus mit der Admin-PIN.
3. Windows 7 und früher: Rechtsklick auf „Mein Computer“ im Startmenü, dann „Verwalten“.

a. Wählen Sie im linken Fenster „Computerverwaltung“ „Disk-Management“.

Windows 8, 8.1 oder 10: Rechtsklick auf „Start“ und dann „Disk-Management“.

4. Im „Disk-Management“ erscheint das Aegis Secure-Produkt „Nicht initialisiert“ oder „Nicht zugewiesen“. Machen Sie einen Rechtsklick auf das Kästchen „Nicht initialisiert“ und wählen Sie „Disk initialisieren“.
5. Klicken Sie im sich öffnenden Fenster auf „OK“.
6. Machen Sie einen Rechtsklick auf das Kästchen „Nicht zugewiesen“ und wählen Sie „Neues einfaches Volumen“.
7. Folgen Sie den Anweisungen des „Assistenten für neues einfaches Volumen“, wählen Sie den Laufwerksbuchstaben, das Dateisystem, das Volumenlabel und klicken Sie dann auf „Abschließen“.

B.) MacOS

1. Erstellen Sie die Admin-PIN.
2. Starten Sie den entsperrten Modus mit der Admin-PIN.
3. Klicken Sie im sich öffnenden Fenster auf „Ignorieren“.
4. Öffnen Sie die App „Disk Utility“.
5. Wählen Sie das Gerät „Apricorn“ aus der Liste der „externen“ Geräte.
6. Klicken Sie auf die Schaltfläche „Löschen“.
7. Folgen Sie der Aufforderung, einen Namen, ein Format sowie ein Schema auszuwählen und klicken Sie auf „Löschen“.

C.) Linux

1. Erstellen Sie die Admin-PIN.
2. Starten Sie den entsperrten Modus mit der Admin-PIN.
3. Öffnen Sie die Anwendung „Disks“.
4. Wählen Sie das Gerät „Apricorn“ aus dem linken Fenster.
5. Klicken Sie auf das Symbol unter „Volumen“ für „Zusätzliche Partitionsoptionen“.
6. Wählen Sie „Partition formatieren“.
7. Folgen Sie der Aufforderung, einen Namen und ein Format auszuwählen und klicken Sie auf „Formatieren“.

Diagnose-Modus

Der Diagnose-Modus kann eine ordnungsgemäße Keypad-Funktion verifizieren und Fehlersuchen durchführen. Der Diagnose-Modus ermöglicht KEINEN Zugriff auf Daten oder Admin-Funktionen.

1. Drücken Sie aus dem gesperrten Modus aus 🔒 + 1 gleichzeitig, lassen Sie los und halten Sie dann die Schaltfläche (0) fünf Sekunden lang.
2. Die **BLAUE** LED blinkt mehrere Male, um die Anzahl der großen und kleinen Revisionen anzuzeigen. Der Dezimalpunkt wird von einem einmaligen Blinken der **ROTEN** LED dargestellt. Nach Abschluss leuchtet die **BLAUE** LED durchgehend auf. (Version 7.8 wäre z. B. siebenmaliges Aufleuchten der **BLAUEN** LED, einmaliges Aufleuchten der **ROTEN** LED, achtmaliges Aufleuchten der **BLAUEN** LED und einmaliges Aufleuchten der **ROTEN** LED.)
3. Um die Funktionalität des Keypads zu testen, drücken Sie jede Schaltfläche. Die Nummer der betätigten Schaltfläche wird durch Aufblinken der **ROTEN** LED angezeigt. (Beispiel: 1 Schaltfläche = einmaliges Blinken, 2 Schaltfläche = zweimaliges Blinken, ... 0 Schaltfläche = zehnmaliges Blinken, 🔒 Schaltfläche = elfmaliges Blinken, 🔓 Schaltfläche = zwölfmaliges Blinken.)
4. Um den Diagnose-Modus zu verlassen, warten Sie entweder zwölf bis zwanzig Sekunden Inaktivität ab, halten Sie die Schaltfläche 🔒 drei Sekunden lang gedrückt oder trennen Sie das Gerät vom USB-Port/der Stromversorgung.

Selbstdiagnose-Modus:

Beim Einschalten führen Aegis Secure-Produkte eine Selbstdiagnose des Verschlüsselungsalgorithmus und der kritischen Hardwarebestandteile durch, die durch drei aufblinkende LEDs angezeigt werden, einer **ROTEN**, einer **GRÜNEN** und einer **BLAUEN**. Falls die **ROTE** LED durchgehend blinkt, bevor der Standby-Modus aktiviert wird, probieren Sie einen anderen USB-Port. Falls die **ROTE** LED ständig wie oben erklärt blinkt und der entsperrte Modus in einem anderen USB-Port nicht aktiviert werden kann, hat eine kritische Komponente versagt und das Aegis Secure-Produkt funktioniert nicht länger.

Falls die **ROTE** LED im entsperrten Modus dreimal in zwei Sekunden blinkt, ist ein Fehler aufgetreten, der das Aegis Secure-Produkt NICHT sofort vom Funktionieren abhält, und auch die Sicherheit nicht beeinflusst. Admin-Funktionen können eingeschränkt sein. Dieser Modus ist eine Warnung, dass das Aegis Secure-Produkt bald ersetzt werden muss.

Falls eine dieser Situationen auftritt, entfernen Sie den USB-Port und bringen Sie das Aegis Secure-Produkt in den Standby-Modus. Versuchen Sie es dann erneut. Beide Diagnose-Fehler sind sehr selten, aber falls das Aegis Secure-Produkt nicht zu den normalen LED-Anzeigen zurückkehrt, muss es so bald wie möglich ersetzt werden.

Ruhezustand, Ausloggen oder Außerkraftsetzen

Stellen Sie sicher, dass alle Dateien auf dem Aegis Secure-Produkt vor dem Ruhezustand, Außerkraftsetzen oder Ausloggen vom Host-Betriebssystem gespeichert und geschlossen sind. Wählen Sie über „Dateiexplorer“ oder „Disk-Management“ das Symbol „Auswerfen“ oder „Hardware sicher entfernen“, um das Aegis Secure-Produkt vom System zu entfernen. Es wird empfohlen, das Aegis Secure-Produkt in den gesperrten Modus zu versetzen, bevor es in den Ruhezustand versetzt, aus dem System ausgeloggt oder außer Kraft gesetzt wird.

Um Datenintegrität sicherzustellen, muss das Aegis Secure-Produkt im gesperrten Modus sein, wenn es in einem öffentlichen Bereich unbeaufsichtigt verwendet wird.

Fehlersuche

F: Was passiert, wenn die Benutzer-PIN verloren oder vergessen wird?

A: Falls eine Wiederherstellungs-PIN erstellt wurde, kann der Bediener diese verwenden, um eine neue Benutzer-PIN zu erstellen. Ansonsten kann die Admin-PIN verwendet werden, um eine Wiederherstellungs-PIN zu erstellen.

F: Was passiert, wenn die Admin-PIN verloren oder vergessen wird?

A: Wenn die Admin-PIN verloren oder vergessen wurde, gibt es keine Möglichkeit, ein Aegis Secure-Produkt wiederherzustellen. In diesem Fall ist ein vollständiges Zurücksetzen erforderlich.

F: Warum hat das Betriebssystem das Aegis Secure-Produkt nach dem vollständigen Zurücksetzen nicht erkannt?

A: Das Aegis Secure-Produkt muss initialisiert und formatiert werden (siehe Initialisieren und Formatieren auf Seite 16).

F: Können Aegis Secure-Produkte ohne PIN verwendet werden?

A: Aegis Secure-Produkte können nicht ohne PIN verwendet werden.

F: Welcher Verschlüsselungsalgorithmus wird für dieses Produkt verwendet?

A: Aegis Secure-Produkte verwenden den AES 256-bit-Algorithmus.

F: Warum lässt sich das Aegis Secure-Produkt nicht initialisieren und formatieren?

A: Windows erfordert Admin-Rechte, um auf das Disk-Management zugreifen zu können.

F: Die ROTE LED blinkt ROT und das Keypad antwortet nicht, warum?

A: Das Aegis Secure-Produkt hat 10 falsche PIN-Versuche verhindert und ist jetzt im Brute-Force-Modus (siehe Brute-Force-Modus auf Seite 14).

F: Das Aegis Secure-Produkt ist bei Berührung warm, ist das normal?

A: Ja. Aegis Secure-Produkte nutzen eine passive Kühlung, um die Wärme zu verteilen.

F: Gibt es eine Möglichkeit, Daten wiederherzustellen, falls PINs vergessen wurden?

A: Ohne eine Wiederherstellungs-PIN oder Admin-PIN können Daten nicht wiederhergestellt werden. Das Aegis Secure-Produkt kann jedoch in den Out-of-Box-Modus zurückgesetzt werden.

F: Warum zeigt die LED einen Fehler an, wenn versucht wird, eine PIN zu ändern?

A: PIN-Anforderungen für Aegis Secure-Produkte müssen ein Mindestsicherheitsniveau erfüllen. Es gibt mehrere Kombinationen, die NICHT erlaubt sind, wie z. B. sich wiederholende Zahlen oder sequenzielle Zahlen. Die PIN muss zudem aus mindestens sieben und maximal sechzehn Zeichen bestehen.

Kurzanleitung

Gesperrter Modus

- Schaltflächen (7 und 6) fünf Sekunden lang gedrückt halten = Nur-Lesen-Modus
- Schaltflächen (7 und 9) fünf Sekunden lang gedrückt halten = Lesen-Schreiben-Modus
- Schaltflächen 🔒 + 1 gleichzeitig drücken, dann (0) fünf Sekunden lang gedrückt halten = Diagnose-Modus

Benutzermodus

- 🔓 + 1 gleichzeitig drücken = Benutzer-PIN ändern
- 🔓 + 3 gleichzeitig drücken = Eintragungsmodus selbstzerstörende PIN

Admin-Modus

- 🔓 + 0 fünf Sekunden lang gleichzeitig gedrückt halten = Admin-Modus
- 🔓 + 1 gleichzeitig drücken = Benutzer-PIN Eintragung
- 🔓 + 3 gleichzeitig drücken = Eintragungsmodus selbstzerstörende PIN
- 🔓 + 4 drücken = Mindestlänge PIN Modus
- 🔓 + 5 drücken = Brute-Force-Modus PIN-Versuche
- 🔓 + 6 drücken = Unbeaufsichtigter Auto-Sperrmodus
- 🔓 + 7 drücken = Eintragung Einmal-Wiederherstellungs-PIN
- 🔓 + 8 drücken = Einsatz Einmal-Wiederherstellungs-PIN
- 🔓 + 9 drücken = Modus Admin-PIN ändern
- 7 + 1 zusammen drücken = Lock-Override aktivieren
- 7 + 0 zusammen drücken = Lock-Override deaktivieren
- 7 + 4 zusammen drücken = Selbstzerstörende PIN auslösen
- 7 + 6 zusammen drücken = Nur-Lesen-Modus aktivieren
- 7 + 9 zusammen drücken = Lesen-Schreiben-Modus aktivieren
- 0 + 1 zusammen drücken = Vom Benutzer erzwungenen Eintragungsmodus auslösen
- 0 + 3 zusammen drücken = LED-Flickermodus aktivieren
- 0 + 4 zusammen drücken = LED-Flickermodus deaktivieren
- 7 + 8 zusammen fünf Sekunden lang gedrückt halten = Benutzer, Selbstzerstörende, Wiederherstellungs PINs löschen

Technischer Support

1. Apricorn-Website: **https://www.apricorn.com**
2. Schreiben Sie uns eine E-Mail an **support@apricorn.com**
3. Rufen Sie den Apricorn Kundendienst unter **1-800-458-5448**

von Montag bis Freitag, 8:00 Uhr bis 17:00 Uhr (PST) an.

Garantieinformationen

Apricorn Eingeschränkte Gewährleistung:
Apricorn bietet eine auf drei Jahre begrenzte Gewährleistung auf Aegis Secure Keys und Aegis Padlock Produkte. Apricorn bietet eine auf ein Jahr begrenzte Gewährleistung auf Aegis Padlock DT und Aegis Padlock DT FIPS. Der Gewährleistungszeitraum gilt ab dem Kaufdatum, entweder direkt von Apricorn oder von einem autorisierten Händler.

Haftungsausschluss und Garantiebedingungen:
DIE GEWÄHRLEISTUNG GILT AB DEM TAG DES KAUFES UND MUSS MIT DEM KAUFSBELEG ODER DER RECHNUNG, DIE DAS DATUM DES PRODUKTKAUFS ZEIGT, VERIFIZIERT WERDEN.

APRICORN WIRD OHNE ZUSÄTZLICHE KOSTEN DEFEKTE TEILE REPARIEREN ODER MIT NEUEN TEILEN ODER WARTBAREN, BEREITS VERWENDETEN TEILEN ERSETZEN, DIE IN DER LEISTUNG WIE NEU SIND. ALLE AUSGEWECHSELTEN TEILE UND PRODUKTE UNTER DIESER GEWÄHRLEISTUNG WERDEN EIGENTUM VON APRICORN.

DIESE GEWÄHRLEISTUNG GILT NICHT FÜR PRODUKTE, DIE NICHT DIREKT VON APRICORN ODER EINEN AUTORISIERTEN HÄNDLER GEKAUFT WURDEN, ODER FÜR PRODUKTE, DIE BESCHÄDIGT ODER MANGELHAFT SIND: 1. AUFGRUND EINES UNFALLS, FEHLGEBRAUCHS, VERNACHLÄSSIGUNG, MISSBRAUCHS ODER FEHLER UND/ODER DER UNFÄHIGKEIT, DIE SCHRIFTLICHEN ANWEISUNGEN IN DIESER ANLEITUNG ZU BEFOLGEN; 2. DURCH DEN EINSATZ VON TEILEN, DIE NICHT VON APRICORN HERGESTELLT ODER VERKAUFT WURDEN; 3. DURCH ÄNDERUNG DES PRODUKTS; ODER 4. AUFGRUND VON WARTUNGSARBEITEN, ÄNDERUNGEN ODER REPARATUREN VON ANDEREN AUSSER APRICORN, UND WIRD DADURCH UNGÜLTIG. DIESE GEWÄHRLEISTUNG UMFASST NICHT NORMALEN VERSCHLEISS UND ABNUTZUNGEN.

KEINE WEITERE GEWÄHRLEISTUNG, AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIESSLICH GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, WURDE ODER WIRD GEMACHT DURCH ODER IM NAMEN VON APRICORN ODER KRAFT GESETZES IN BEZUG AUF DAS PRODUKT ODER DIE INSTALLATION, DEN GEBRAUCH, DIE BEDIENUNG, DEN ERSATZ ODER DIE REPARATUR.

APRICORN IST NICHT HAFTBAR FÜR DIESE GEWÄHRLEISTUNG ODER FÜR ZUFÄLLIGE, BESONDERE ODER FOLGESCHÄDEN, EINSCHLIESSLICH DATENVERLUST DURCH DEN GEBRAUCH ODER BETRIEB DES PRODUKTS, UNABHÄNGIG DAVON, OB APRICORN VON DER MÖGLICHKEIT DIESER SCHÄDEN WEISS ODER NICHT.

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