

# Secure Lock Manager Easy Quick Start Guide

This product includes "Secure Lock Manager Easy", Buffalo's encryption software for storage devices.

## About Secure Lock Manager Easy

Secure Lock Manager Easy allows you to encrypt and password-protect your Buffalo storage device. Provision for auto-authentication is available in the software. Encryption is disabled by default.



## Before Using This Software

Please read the following notes before you use Secure Lock Manager Easy.

- Keep your password secure.
- Without your password, you will not be able to access the hard drive or change settings. If you forget your password, you must reset your drive to the factory defaults.
- Windows 7/ Vista/ XP/ 2000/ Windows Server 2003/Sever 2003 R2/ Windows Server 2008/ Server 2008 R2 are supported.
- The list of compatible operating systems is for Secure Lock Manager Easy only. To find out which operating systems your product works with, consult its documentation.
- To use Secure Lock Manager Easy on a Windows Server 2003 and Server 2003 R2 PC, log in with an administrator account.

## Installation

Secure Lock Manager Easy can be installed from DriveNavigator. Use the following procedure to install it.

- 1** Connect the drive to your computer.
- 2** Right-click on [Utility\_HD-\*\*\*\*] () in My Computer, and select [Open].  
(\*\*\*\* is the part number of your DriveStation/MiniStation.)
- 3** Double click [DriveNavi.exe] ().  
DriveNavigator will launch.  
\* if "A program needs your permission to continue" is displayed, click [Continue].
- 4** Click [Options].
- 5** Click [Install Secure Lock Manager Easy].

Follow the instructions displayed on the screen to install the software.

# Launching Secure Lock Manager Easy

To launch Secure Lock Manager Easy,

## 1 Connect the drive to your computer.

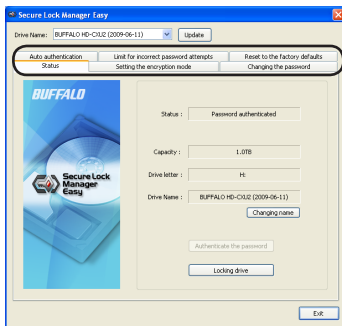
If the password authentication screen is displayed, enter your password.

**Note:** If you forget your password and reset the unit to the factory defaults, close the screen.

## 2 Click [Start] - [(All) Programs] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

# Secure Lock Manager Tabs

Clicking on tabs in Secure Lock Manager Easy allows you to configure the following settings.

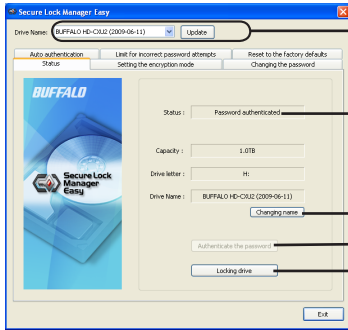


Click an item you want to configure.

- Status (page 3)  
Check the status of the drive.
- Encryption mode (page 3)  
Enable/Disable encryption.
- Password (page 3)  
Change the password.
- Auto authentication (page 4)  
Automatically enters the password when the drive is connected to a computer.
- Limit for incorrect password attempts (page 4)  
Set the behavior of the unit when you enter an wrong password.
- Reset to factory defaults (page 5)  
Delete all settings and data on the hard drive, resetting it to the factory defaults.

## • Status

Check the status of the drive.



Select the product you want to configure.

Display the current status of the drive.

- Standard
- Password not authenticated yet
- Password authenticated

Enter a name (30 characters or less).

\* This name is displayed only by Secure Lock Manager Easy.

Enter your password to authenticate it.

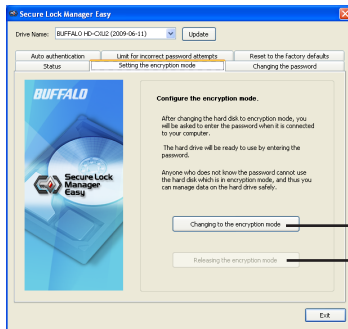
\* If the encryption mode is released, it is not effective even though you click it.

Lock the drive. Authentication will be

needed again for further access to the drive.

## • Encryption mode

Enable/Disable encryption.

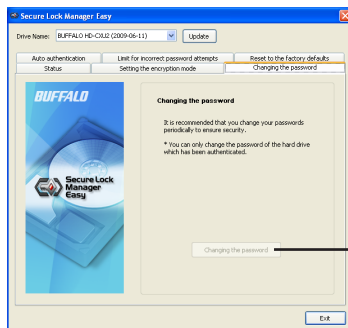


Enable Encryption. You will have to enter a password to access the drive, or set up auto-authentication.

Disable encryption mode. Anyone can access the drive without authenticating.

## • Password

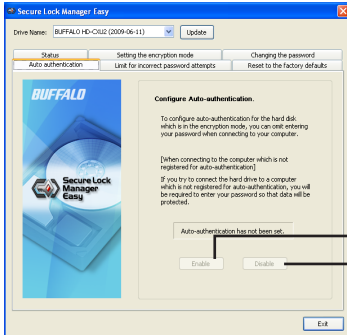
Change the password.



Change the password. To change the password, encryption must be enabled and you must have entered the old password.

- Auto authentication

Set the method to enter a password for the drive. Your password can be entered automatically (auto-authentication). This setting can be used for one unit per computer.



Enable Auto authentication.

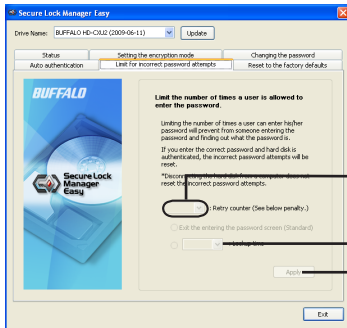
Disable Auto authentication.

**Note:** Each computer that uses auto-authentication needs to install the software and enable this setting. On a single computer, each user needs to enable auto-authentication to use it.

**Warning:** Auto-authentication is not recommended if you share your computer with multiple users. Data can be viewed, deleted or edited by other users since data on the hard drive can be accessible just like standard hard drives.

- Limiting incorrect password attempts

Set the behavior of the unit when you enter a wrong password.



Select for incorrect password attempts from [3], [5] and [10].

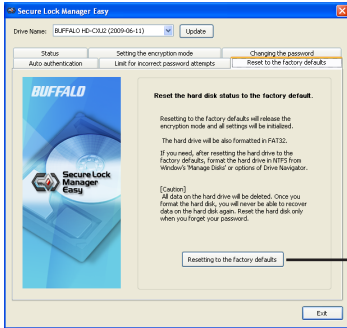
Select the behavior when reaching the limit of the incorrect password attempts.

Apply a setting.

The behavior when reaching the limit of the incorrect password attempts	
Exiting the entering the password screen (Default value)	The screen to enter the password will close. To authenticate the password, you need to open the screen to enter the password again.
Cannot authenticate during **	Select the target term from [5 minutes], [10 minutes], [30 minutes] and [1 hour], which will refuse authentication attempts. Authentication cannot be done until the time has passed.

- **Resetting to the factory defaults**

Delete settings of the drive and data on the hard drive, and reset it to the factory defaults.

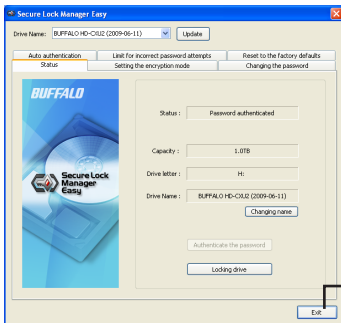


Reset to the factory defaults. Delete the password and all data that have been saved.

\* The hard drive is formatted in FAT32 and the encryption mode will be released.

## Exiting Secure Lock Manager Easy

To exit Secure Lock Manager Easy, click [Exit] at the bottom right of the screen.



Click [Exit].

## To uninstall

You can uninstall Secure Lock Manager Easy when you no longer need it. To uninstall it, click [Start] - [(All) Programs] - [BUFFALO] - [Secure Lock Manager Easy] - [Uninstall]. Then follow the instructions on the screen.

# Secure Lock Manager Easy Erste Schritte

Zu diesem Produkt gehört [Secure Lock Manager Easy], die Verschlüsselungssoftware von Buffalo für Speichermedien.

## Info über Secure Lock Manager Easy

Mit Secure Lock Manager Easy können Sie Ihr Speichermedium von Buffalo mit einem Passwort schützen und Daten verschlüsseln. Die Software bietet eine automatische Authentifizierung. Die Verschlüsselung ist standardmäßig deaktiviert.



## Vor der Verwendung dieser Software

Lesen Sie vor der Verwendung von Secure Lock Manager Easy bitte die folgenden Hinweise.

- Bewahren Sie Ihr Passwort sicher auf.
- Ohne Ihr Passwort ist der Zugriff auf das Laufwerk nicht möglich und die Einstellungen können nicht geändert werden. Haben Sie Ihr Passwort vergessen, müssen Sie das Laufwerk auf die werkseitigen Standardeinstellungen zurücksetzen.
- Windows 7/Vista/XP/2000/Windows Server 2003/Sever 2003 R2/Windows Server 2008/Server 2008 R2 werden unterstützt.
- Die Liste der kompatiblen Betriebssysteme gilt nur für Secure Lock Manager Easy. Wenn Sie erfahren möchten, welche Betriebssysteme Sie für Ihr Produkt verwenden können, sehen Sie in der zugehörigen Produktdokumentation nach.
- Wenn Sie Secure Lock Manager Easy auf einem PC unter Windows Server 2003 und Server 2003 R2 verwenden möchten, melden Sie sich mit einem Administratorkonto an.

## Installation

Secure Lock Manager Easy kann vom DriveNavigator aus installiert werden. Führen Sie Installation anhand der folgenden Schritte durch.

- 1** Schließen Sie das Laufwerk an Ihren Computer an.
  - 2** Klicken Sie mit der rechten Maustaste unter Arbeitsplatz auf [Utility\_HD-\*\*\*\*]  und wählen Sie [Öffnen].  
  
(\*\*\*\* ist die Teilenummer Ihrer DriveStation/MiniStation.)
  - 3** Doppelklicken Sie auf [DriveNavi.exe] .
- Der DriveNavigator startet.
- \* Wird in Windows Vista die Meldung [Zur Fortsetzung des Programms ist Ihre Zustimmung erforderlich] angezeigt, klicken Sie auf [Weiter].
- 4** Klicken Sie auf [Optionen].
  - 5** Klicken Sie auf [Secure Lock Manager Easy installieren].

Befolgen Sie die angezeigten Anweisungen, um die Software zu installieren.

# Starten des Secure Lock Manager Easy

Um den Secure Lock Manager Easy zu starten:

## 1 Schließen Sie das Laufwerk an Ihren Computer an.

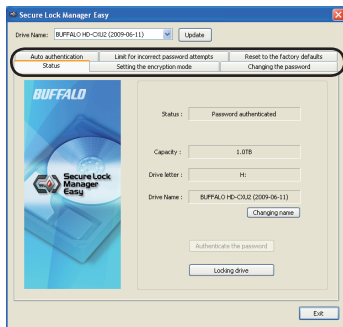
Wird der Bildschirm zur Passwort-Authentifizierung angezeigt, geben Sie Ihr Passwort ein.

**Hinweis:** Haben Sie Ihr Passwort vergessen und setzen Sie das Gerät auf die werkseitigen Standardeinstellungen zurück, schließen Sie den Bildschirm.

## 2 Klicken Sie auf [Start] - [(Alle) Programme] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

# Registerkarten des Secure Lock Manager

Wenn Sie die Registerkarte des Secure Lock Manager Easy anklicken, können Sie die Einstellungen konfigurieren.

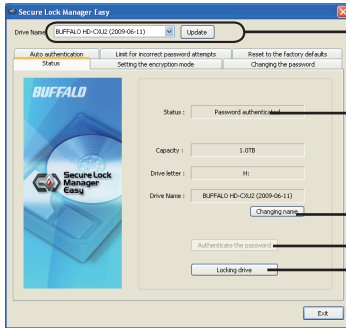


Klicken Sie das Element an, das Sie konfigurieren möchten.

- Status (Status) (Seite 3)  
Prüfung des Laufwerkstatus.
- Encryption mode (Verschlüsselungsmodus) (Seite 3)  
Aktivierung/Deaktivierung der Verschlüsselung.
- Password (Passwort) (Seite 3)  
Änderung des Passworts.
- Auto authentication (Automatische Authentifizierung) (Seite 4)  
Automatische Eingabe des Passworts beim Anschließen des Laufwerks an einen Computer.
- Limit for incorrect password attempts (Begrenzung der Eingabeversuche bei inkorrektem Passwort) (Seite 4)  
Einstellen des Geräteverhaltens bei Eingabe eines falschen Passworts.
- Reset to factory defaults (Rücksetzung auf werkseitige Standardeinstellungen) (Seite 5)  
Löschen aller Einstellungen und Daten auf der Festplatte, so dass sie auf die werkseitigen Standardeinstellungen zurückgesetzt werden.

## • Status (Status)

Prüfung des Laufwerkstatus.



Klicken Sie das Produkt an, das Sie konfigurieren möchten.

Zeigt den aktuellen Status des Laufwerks an.

- Standard
- Passwort noch nicht authentifiziert
- Passwort authentifiziert

Geben Sie einen Namen ein (max. 30 Zeichen).

\* Dieser Name wird nur vom Secure Lock Manager Easy angezeigt.

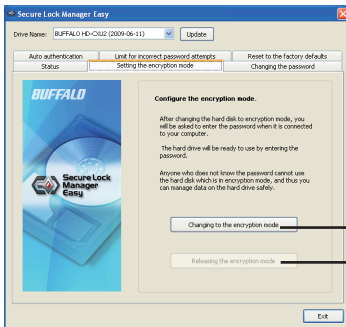
Geben Sie Ihr Passwort zur Authentifizierung ein.

\* Der Verschlüsselungsmodus ist bei Freigabe trotz Anklicken nicht gültig.

Sperren des Laufwerks. Um wieder auf das Laufwerk zugreifen zu können, ist erneut eine Authentifizierung erforderlich.

## • Encryption mode (Verschlüsselungsmodus)

Aktivierung/Deaktivierung der Verschlüsselung.



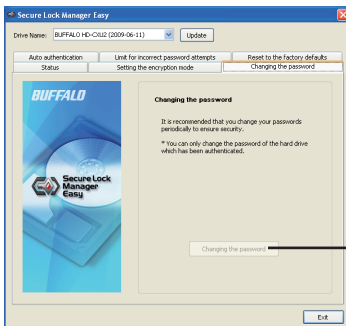
Aktivierung der Verschlüsselung. Sie

müssen ein Passwort eingeben, um auf das Laufwerk zugreifen zu können oder die automatische Authentifizierung einrichten.

Deaktivierung des Verschlüsselungsmodus. Der Zugriff auf das Laufwerk ist für jeden ohne Authentifizierung möglich.

## • Password (Passwort)

Änderung des Passworts.

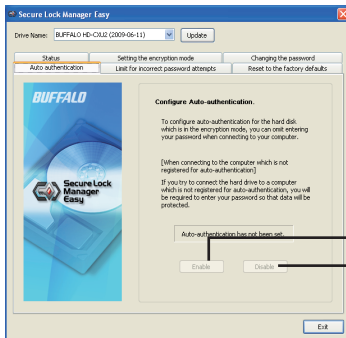


Änderung des Passworts. Damit das Passwort geändert werden kann, muss die Verschlüsselung aktiviert und das alte Passwort eingegeben worden sein.



- **Auto authentication (Automatische Authentifizierung)**

Auswahl der Methode für die Passworteingabe des Laufwerks. Ihr Passwort kann automatisch eingegeben werden (automatische Authentifizierung). Diese Einstellung kann für ein Gerät pro Computer verwendet werden.



Aktivierung der automatische Authentifizierung.

Deaktivierung der automatische Authentifizierung.

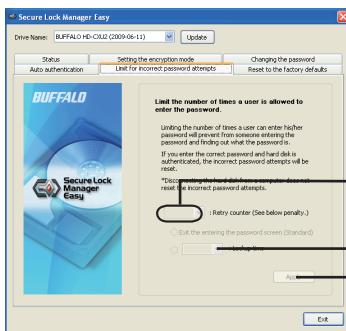
**Hinweis:** Auf jedem Computer, auf dem die automatische Authentifizierung verwendet wird, muss die Software installiert und diese Einstellung aktiviert sein. Bei einem Einzelcomputer muss die automatische Authentifizierung von jedem Benutzer für die Verwendung aktiviert werden.

**Warnung:** Die automatische Authentifizierung wird nicht empfohlen, wenn mehrere Personen einen Computer gemeinsam nutzen. Daten können von anderen Benutzern angezeigt, gelöscht oder bearbeitet werden, da der Zugriff auf Daten der Festplatte wie bei herkömmlichen Festplatten möglich ist.

- **Limiting incorrect password attempts**

(Begrenzung der Eingabeversuche bei inkorrektem Passwort)

Einstellen des Geräteverhaltens bei Eingabe eines falschen Passworts.



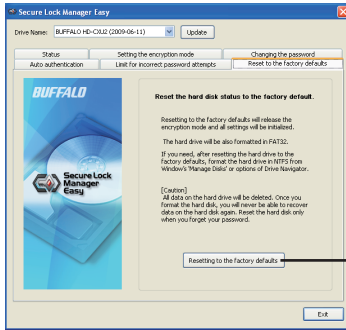
Einstellung der maximalen Eingabeversuche bei inkorrektem Passwort: [3], [5] und [10].

Auswahl des Verhaltens bei Erreichen der maximalen Passwort-Eingabeversuche.

Übernehmen einer Einstellung.

Verhalten bei Erreichen der maximalen Passwort-Eingabeversuche	
Schließen des Bildschirms für die Passworteingabe (Standardwert)	Der Bildschirm für die Eingabe des Passworts wird geschlossen. Um das Passwort zu authentifizieren, muss der Bildschirm für die Passworteingabe geöffnet werden.
Keine Authentifizierung möglich für **	Wählen Sie eine Option aus [5 Minuten], [10 Minuten], [30 Minuten] und [1 Stunde] aus, in der keine Authentifizierung möglich ist. Die Authentifizierung ist erst nach Ablauf dieses Zeitraums wieder möglich.

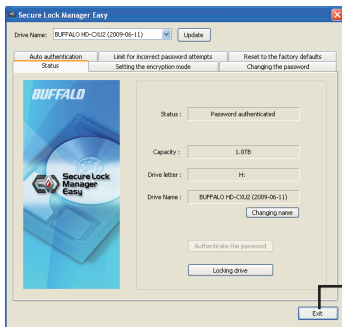
- Resetting to the factory defaults (Rücksetzung auf die werkseitigen Standardeinstellungen)  
Löschen der Einstellungen und Daten auf der Festplatte und Rücksetzung auf die werkseitigen Standardeinstellungen.



Rücksetzung auf die werkseitigen Standardeinstellungen. Löschen des Passworts und aller gespeicherten Daten.  
\* Die Festplatte wird mit FAT32 formatiert und der Verschlüsselungsmodus wird freigegeben.

## Beenden des Secure Lock Manager Easy

Um den Secure Lock Manager Easy zu beenden, klicken Sie unten rechts auf dem Bildschirm auf [Exit] (Beenden).



Klicken Sie auf [Exit] (Beenden).

## Deinstallation

Sie können den Secure Lock Manager Easy deinstallieren, wenn Sie ihn nicht mehr benötigen. Um das Programm zu deinstallieren, klicken Sie auf [Start] - [(Alle) Programme] - [BUFFALO] - [Secure Lock Manager Easy] - [Deinstallieren]. Befolgen Sie anschließend die angezeigten Anweisungen.

# Secure Lock Manager Easy Guía de inicio rápido

Este producto incluye [Secure Lock Manager Easy], el software de cifrado de Buffalo para los dispositivos de almacenamiento.

## Acerca de Secure Lock Manager Easy

Secure Lock Manager Easy le permite cifrar y proteger con contraseña su dispositivo de almacenamiento Buffalo. En el software se dispone de la disposición para la autenticación automática. El cifrado está desactivado por defecto.


## Antes de usar este software

Lea las siguientes notas antes de usar Secure Lock Manager Easy.

- Mantenga segura la contraseña.
- Sin la contraseña, no podrá acceder al disco duro ni cambiar la configuración. Si olvida la contraseña, debe restablecer la unidad a los predeterminados de fábrica.
- Compatible con Windows 7/ Vista/ XP/ 2000/ Windows Server 2003/Server 2003 R2/ Windows Server 2008/ Server 2008 R2.
- La lista de sistemas operativos compatibles se refiere a Secure Lock Manager Easy únicamente. Para averiguar con qué sistemas operativos es compatible su producto, consulte la documentación.
- Para utilizar Secure Lock Manager Easy en PC con Windows Server 2003 y Server 2003 R2, inicie sesión con una cuenta de administrador.

## Instalación

Secure Lock Manager Easy se puede instalar desde DriveNavigator. Utilice el siguiente procedimiento para instalarlo.

- 1 Conecte la unidad al ordenador.
- 2 Haga clic con el botón derecho del ratón en [Utility\_HD-\*\*\*\*]  en Mi PC y seleccione [Abrir].

(\*\*\*\* es el número de pieza de su DriveStation/MiniStation).

- 3 Haga doble clic en [DriveNavi.exe] .

Se iniciará DriveNavigator.

\* Si se muestra [Un programa necesita su autorización para continuar] en Windows Vista, haga clic en [Continuar].

- 4 Haga clic en [Opciones].

- 5 Haga clic en [Instalar Secure Lock Manager Easy].

Siga las instrucciones mostradas en la pantalla para instalar el software.

# Iniciando el Secure Lock Manager Easy

Para iniciar el Secure Lock Manager Easy,

## 1 Conecte la unidad al ordenador.

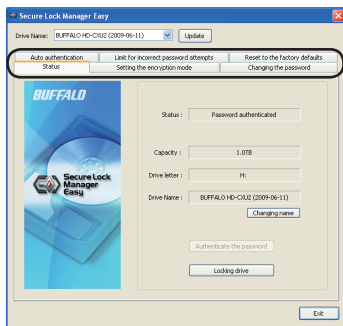
Si se muestra la pantalla de autenticación por contraseña, introduzca la contraseña.

**Nota:** Si olvida la contraseña y restablece la unidad a los predeterminados de fábrica, cierre la pantalla.

## 2 Haga clic en [Inicio] - [(Todos) Programas] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

## Pestañas Secure Lock Manager

Al hacer clic en las pestañas en Secure Lock Manager Easy puede configurar los siguientes ajustes.

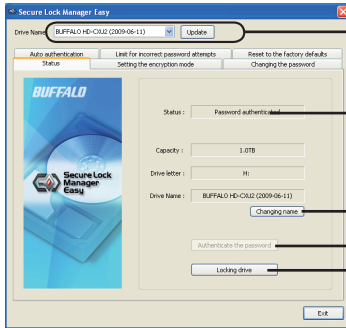


Haga clic en un elemento que desee configurar.

- Status (Estado) (página 3)  
Comprueba el estado de la unidad.
- Encryption mode (Modo de cifrado) (página 3)  
Activa/Desactiva el cifrado.
- Password (Contraseña) (página 3)  
Cambia la contraseña.
- Auto authentication (Autenticación automática) (página 4)  
Introduce automáticamente la contraseña cuando la unidad está conectada a un ordenador.
- Limit for incorrect password attempts (Límite de intentos de contraseña incorrectos) (página 4)  
Ajusta el comportamiento de la unidad cuando introduce una contraseña incorrecta.
- Reset to factory defaults (Restablecer a predeterminados de fábrica) (página 5)  
Elimina todos los ajustes y datos del disco duro, restableciéndolos a los predeterminados de fábrica.

## • Status (Estado)

Comprueba el estado de la unidad.



Seleccione el producto que desee configurar.

Muestra el estado actual de la unidad.

- Standard (Estándar)
- Contraseña no autenticada todavía
- Contraseña autenticada

Introduzca un nombre (30 caracteres o menos).

\* Este nombres sólo es mostrado por Secure Lock Manager Easy.

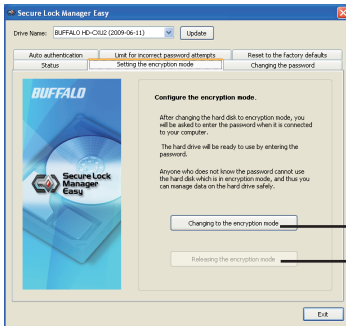
Introduzca su contraseña para autenticarla.

\* Si se activa el modo de cifrado, no es efectivo aunque haga clic en él.

Bloquee la unidad. La autenticación será necesaria otra vez para acceder de nuevo a la unidad.

## • Encryption mode (Modo de cifrado)

Activa/Desactiva el cifrado.

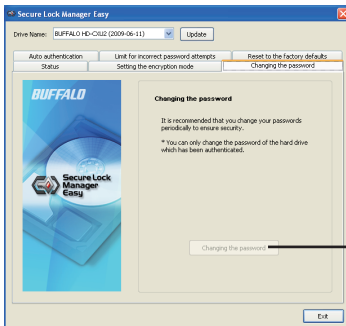


Activar el cifrado. Tendrá que introducir una contraseña para acceder al disco o establecer la autenticación automática.

Desactiva el modo de cifrado. Cualquiera puede acceder a la unidad sin autenticación.

## • Password (Contraseña)

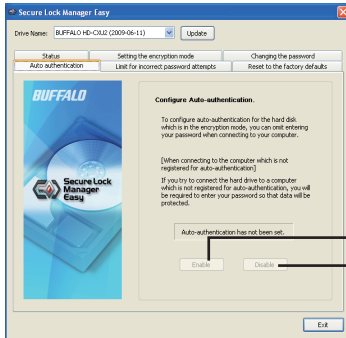
Cambia la contraseña.



Cambia la contraseña. Para cambiar la contraseña, se debe activar el cifrado y debe haber introducido la antigua contraseña.

- **Auto authentication (Autenticación automática)**

Establece el método para introducir una contraseña para la unidad. Su contraseña puede ser introducida automáticamente (autenticación automática). Este ajuste se puede usar para una unidad por ordenador.



Activar la autenticación automática.

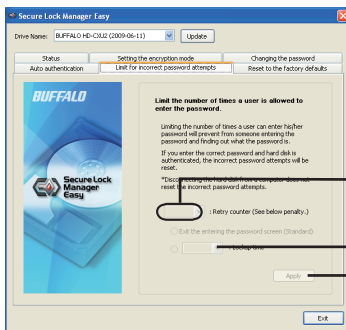
Desactivar la autenticación automática.

**Nota:** En cada ordenador que utilice la autenticación automática se necesita instalar el software y activar este ajuste. En un solo ordenador, cada usuario necesita activar la autenticación automática para usarla.

**Advertencia:** No se recomienda la autenticación automática si comparte el ordenador con múltiples usuarios. Los datos pueden ser visualizados, eliminados o editados por otros usuarios ya que se puede acceder a los datos del disco duro como en los discos duros estándar.

- **Limiting incorrect password attempts (Limite de intentos de contraseña incorrectos)**

Ajusta el comportamiento de la unidad cuando introduce una contraseña incorrecta.



Seleccione los intentos de contraseña incorrectos entre [3], [5] y [10].

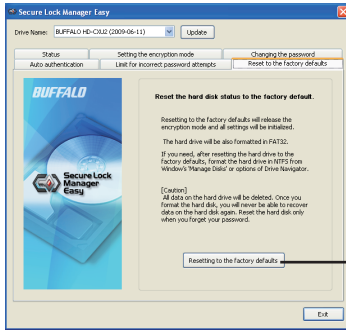
Seleccione el comportamiento cuando se alcanza el límite de intentos de contraseña incorrectos.

Aplicar un ajuste.

El comportamiento cuando se alcanza el límite de intentos de contraseña incorrectos	
Salir de la pantalla de introducción de contraseña (Valor predeterminado)	La pantalla para introducir la contraseña se cerrará. Para autenticar la contraseña, es necesario abrir la pantalla para introducir la contraseña de nuevo.
No se puede autenticar durante **	Seleccione el plazo objetivo de [5 minutos], [10 minutos], [30 minutos] y [1 hora], que rechazará los intentos de autenticación. La autenticación no se puede terminar hasta que el tiempo haya pasado.

- **Resetting to the factory defaults (Restablecer a los predeterminados de fábrica)**

Elimina los ajustes de la unidad y los datos del disco duro, restableciéndolos a los predeterminados de fábrica.

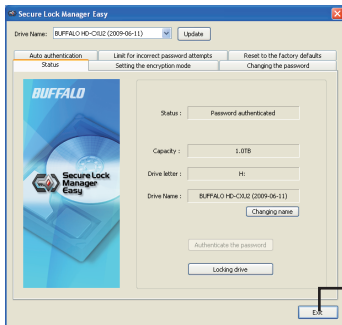


Restablecer a los predeterminados de fábrica. Elimina la contraseña y todos los datos que se hayan guardado.

\* El disco duro se formatea en FAT32 y el modo de cifrado se activa.

## Salir de Secure Lock Manager Easy

Para salir de Secure Lock Manager Easy, haga clic en [Exit] (Salir) en el lado inferior derecho de la pantalla.



Haga clic en [Exit] (Salir).

## Para desinstalar

Puede desinstalar Secure Lock Manager Easy cuando ya no lo necesite. Para desinstalarlo, haga clic en [Inicio] - [(Todos) Programas] - [BUFFALO] - [Secure Lock Manager Easy] - [Desinstalar]. A continuación, siga las instrucciones de la pantalla.

# Secure Lock Manager Easy Guide de démarrage rapide

Ce produit intègre le logiciel de cryptage [ Secure Lock Manager Easy ] de Buffalo pour les périphériques de stockage.

## À propos de Secure Lock Manager Easy

Secure Lock Manager Easy vous permet de crypter et de protéger par un mot de passe votre périphérique de stockage Buffalo. Les dispositions pour l'authentification automatique sont disponibles dans le logiciel. Le cryptage est désactivé par défaut.



## Avant d'utiliser ce logiciel

Veillez lire les remarques suivantes avant d'utiliser Secure Lock Manager Easy.

- Conservez votre mot de passe dans un endroit sûr.
- Sans votre mot de passe, vous ne pourrez pas accéder au disque dur ou modifier les paramètres. Si vous oubliez votre mot de passe, vous devrez réinitialiser votre lecteur aux valeurs d'usine par défaut.
- Windows 7/Vista/XP/2000/Windows Server 2003/Server 2003 R2/Windows Server 2008/Server 2008 R2 sont pris en charge.
- La liste des systèmes d'exploitation compatibles ne concerne que le produit Secure Lock Manager Easy. Pour savoir avec quels systèmes d'exploitation votre produit est compatible, consultez sa documentation.
- Pour utiliser le Secure Lock Manager Easy sur un ordinateur Windows Server 2003 ou Server 2003 R2, connectez-vous avec un compte d'administrateur.

## Installation

Secure Lock Manager Easy peut être installé à partir de DriveNavigator. Pour l'installer, utilisez la procédure suivante :

- 1 Connectez le lecteur à votre ordinateur.
- 2 Cliquez avec le bouton droit de la souris sur [ Utility\_HD-\*\*\*\* ] () dans Poste de travail et sélectionnez [ Ouvrir ].  
(\*\*\*\* correspond au numéro de référence de votre DriveStation/MiniStation.)
- 3 Double-cliquez sur [ DriveNavi.exe ] ().  
DriveNavigator démarre.  
\* Si le message [ Un programme nécessite votre autorisation pour continuer ] s'affiche dans Windows Vista, cliquez sur [ Continuer ].
- 4 Cliquez sur [ Options ].
- 5 Cliquez sur [ Installer Secure Lock Manager Easy ].

Suivez les instructions affichées à l'écran pour installer le logiciel.



# Lancement de Secure Lock Manager Easy

Pour lancer Secure Lock Manager Easy,

## 1 Connectez le lecteur à votre ordinateur.

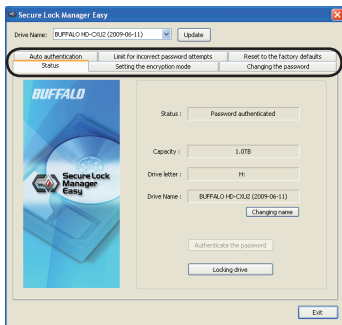
Si l'écran d'authentification par un mot de passe s'affiche, saisissez votre mot de passe.

**Remarque :** Si vous oubliez votre mot de passe et réinitialisez l'appareil aux valeurs d'usine par défaut, fermez l'écran.

## 2 Cliquez sur [ Démarrer ] - [ (Tous les) Programmes ] - [ BUFFALO ] - [ Secure Lock Manager Easy ] - [ Secure Lock Manager Easy ].

# Onglets de Secure Lock Manager

En cliquant sur les onglets de Secure Lock Manager Easy, vous pouvez configurer les paramètres ci-dessous.

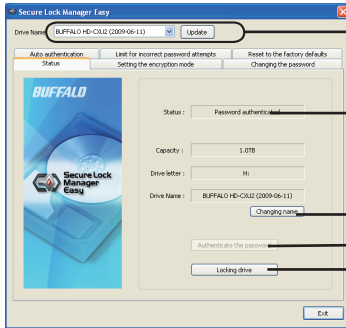


Cliquez sur un élément que vous voulez configurer.

- Status (État) (page 3)  
Vérifiez l'état du lecteur.
- Encryption mode (Mode cryptage) (page 3)  
Activez/désactivez le cryptage.
- Password (Mot de passe) (page 3)  
Changez le mot de passe.
- Auto authentication (Authentification automatique) (page 4)  
Entre automatiquement le mot de passe lorsque le lecteur est connecté à un ordinateur.
- Limit for incorrect password attempts (Limite du nombre de tentatives avec un mot de passe incorrect) (page 4)  
Définissez le comportement de l'appareil lorsque vous saisissez un mot de passe incorrect.
- Reset to factory defaults (Réinitialiser aux valeurs d'usine par défaut) (page 5)  
Supprimez tous les paramètres et données sur le disque dur en le réinitialisant aux valeurs d'usine par défaut.

## • Status (État)

Vérifiez l'état du lecteur.



Sélectionnez le produit que vous voulez configurer.

Affichez l'état actuel du lecteur.

- Standard
- Mot de passe non encore authentifié.
- Mot de passe authentifié

Entrez un nom (30 caractères au maximum).  
\* Ce nom n'est affiché que par Secure Lock Manager Easy.

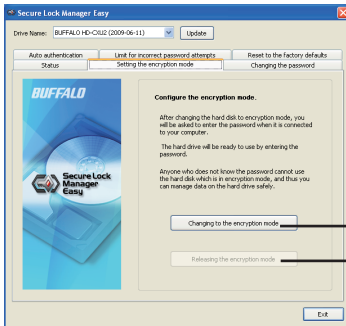
Saisissez votre mot de passe pour l'authentifier.

\* Si le mode de cryptage n'est pas activé, cela n'a aucun effet même si vous cliquez dessus.

Verrouillez le lecteur. L'authentification sera de nouveau nécessaire pour accéder ultérieurement au lecteur.

## • Encryption mode (Mode cryptage)

Activez/désactivez le cryptage.

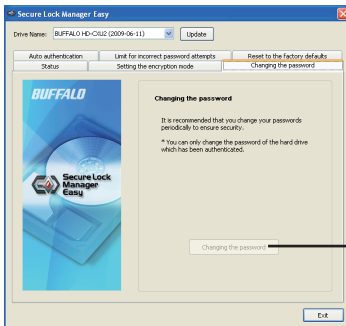


Activez le cryptage. Vous devrez entrer un mot de passe pour accéder au lecteur ou pour définir l'authentification automatique.

Désactivez le mode de cryptage. Tout le monde peut accéder au lecteur sans authentification.

## • Password (Mot de passe)

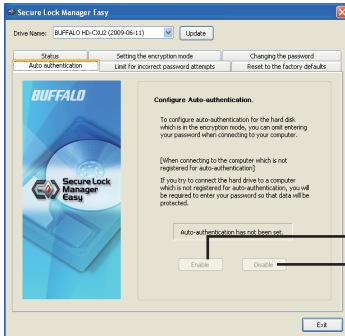
Changez le mot de passe.



Changez le mot de passe. Pour changer le mot de passe, il faut que le cryptage soit activé et que vous ayez saisi l'ancien mot de passe.

- **Auto authentication (Authentification automatique)**

Définissez la méthode pour saisir un mot de passe pour le lecteur. Votre mot de passe peut être saisi automatiquement (authentification automatique). Ce réglage peut être utilisé pour une seule unité par ordinateur.



Activez l'authentification automatique.

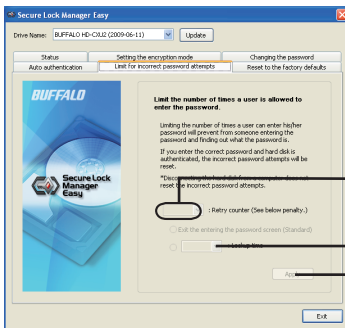
Désactivez l'authentification automatique.

**Remarque :** Il faut que le logiciel soit installé sur chaque ordinateur utilisant l'authentification automatique et que ce réglage soit activé. Sur un ordinateur unique, chaque utilisateur doit activer l'authentification automatique pour pouvoir l'utiliser.

**Avertissement :** L'authentification automatique n'est pas recommandée si vous partagez votre ordinateur avec plusieurs utilisateurs. Les données peuvent être affichées, supprimées ou modifiées par les autres utilisateurs puisque les données qui se trouvent sur le disque dur sont accessibles de la même manière que pour des disques durs standards.

- **Limiting incorrect password attempts (Limitation du nombre de tentatives avec un mot de passe incorrect)**

Définissez le comportement de l'appareil lorsque vous saisissez un mot de passe incorrect.



Sélectionnez le nombre de tentatives avec un mot de passe incorrect, [ 3 ], [ 5 ] ou [ 10 ].

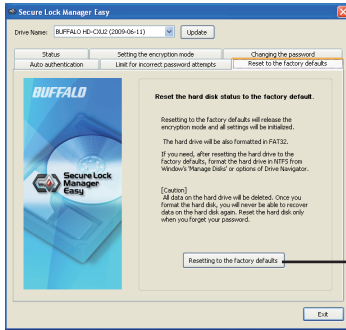
Sélectionnez le comportement lorsque la limite de tentatives avec un mot de passe incorrect est atteinte.

Appliquez un réglage.

Comportement lorsque la limite de tentatives avec un mot de passe incorrect est atteinte	
Sortie de l'écran de saisie du mot de passe (valeur par défaut)	L'écran de saisie du mot de passe se ferme. Pour authentifier le mot de passe, vous devez ouvrir l'écran pour ressaisir le mot de passe.
Authentification impossible pendant **	Sélectionnez la durée voulue, [ 5 minutes ], [ 10 minutes ], [ 30 minutes ] ou [ 1 heure ], pendant laquelle les tentatives d'authentification seront refusées. L'authentification ne sera possible qu'après l'expiration de ce délai.

- Resetting to the factory defaults (Réinitialisation aux valeurs d'usine par défaut)

Supprimez les paramètres du lecteur et les données sur le disque dur et réinitialisez-le aux valeurs d'usine par défaut.

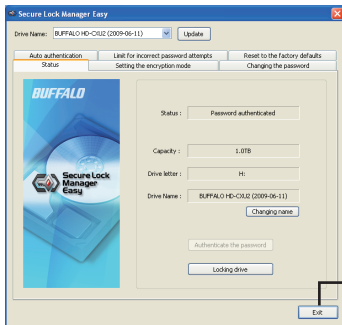


Réinitialisez les valeurs d'usine par défaut. Supprimez le mot de passe et toutes les données qui ont été enregistrées.

\* Le disque dur est formaté selon le système de fichiers FAT32 et le mode cryptage sera désactivé.

## Sortie de Secure Lock Manager Easy

Pour sortir de Secure Lock Manager Easy, cliquez sur le bouton [ Exit ] (Quitter) en bas à droite de l'écran.



Cliquez sur [ Exit ] (Quitter).

## Désinstallation

Vous pouvez désinstaller Secure Lock Manager Easy lorsque vous n'en avez plus besoin. Pour le désinstaller, cliquez sur [ Démarrer ] - [ (Tous les) Programmes ] - [ BUFFALO ] - [ Secure Lock Manager Easy ] - [ Désinstaller ]. Suivez ensuite les instructions à l'écran.

# Guida rapida all'avvio di Secure Lock Manager Easy

Questo prodotto include [Secure Lock Manager Easy], il software di crittografia di Buffalo per le periferiche di memorizzazione.

## Informazioni su Secure Lock Manager Easy

Secure Lock Manager Easy consente di crittografare e proteggere mediante password la periferica di memorizzazione Buffalo. Nel software sono disponibili sistemi per l'autenticazione automatica. La crittografia è disabilitata per impostazione predefinita.



## Prima di utilizzare il software

Leggere le seguenti note prima di utilizzare Secure Lock Manager Easy.

- Conservare la password al sicuro.
- Senza la password, non sarà possibile accedere all'unità disco rigido né modificare le impostazioni. Se la password viene dimenticata, sarà necessario reimpostare l'unità ai valori predefiniti di fabbrica.
- Windows 7/Vista/XP/2000/Windows Server 2003/Server 2003 R2/Windows Server 2008/Server 2008 R2 sono supportati.
- L'elenco di sistemi operativi compatibili è valido solo per SecureLockManager Easy. Per scoprire quali sono i sistemi operativi con cui funziona il vostro prodotto, consultate la sua documentazione.
- Per usare SecureLockManager Easy su un PC Windows Server 2003 e Server 2003 R2, accedere con un account di amministratore.

## Installazione

Secure Lock Manager Easy può essere installato da DriveNavigator. Attenersi alla seguente procedura per l'installazione.

- 1 Collegare l'unità al computer.
- 2 Fare clic con il pulsante destro del mouse su [Utility\_HD-\*\*\*\*]  in Risorse del computer, quindi selezionare [Apri].  
(\*\*\*\* indica il numero di codice del dispositivo DriveStation/MiniStation in uso.)
- 3 Fare doppio clic su [DriveNavi.exe] .  
Viene avviato DriveNavigator.  
\* Se in Windows Vista viene visualizzato il messaggio [Per continuare è necessaria l'autorizzazione dell'utente], fare clic su [Continua].
- 4 Fare clic su [Options].
- 5 Fare clic su [Install Secure Lock Manager Easy].

Attenersi alle istruzioni visualizzate per installare il software.

# Avvio di Secure Lock Manager Easy

Per avviare Secure Lock Manager Easy:

## 1 Collegare l'unità al computer.

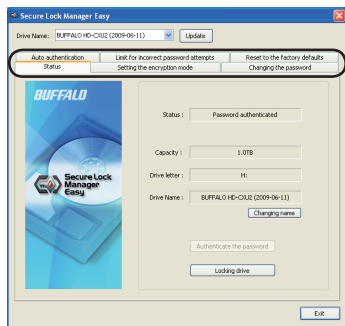
Se viene visualizzata la schermata di autenticazione mediante password, immettere la password.

**Nota:** se la password viene dimenticata, sarà necessario reimpostare l'unità ai valori predefiniti di fabbrica; in questo caso, chiudere la schermata.

## 2 Fare clic su [Start] - [Tutti i programmi] o [Programmi] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

# Schede di Secure Lock Manager

Le schede di Secure Lock Manager Easy consentono di configurare le seguenti impostazioni.

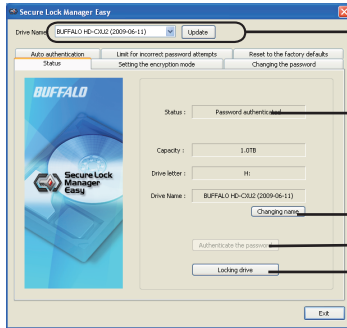


Fare clic su un elemento da configurare.

- Status (Stato) (pagina 3)  
Per controllare lo stato dell'unità.
- Encryption mode (Modalità di crittografia) (pagina 3)  
Per abilitare/disabilitare la crittografia.
- Password (pagina 3)  
Per cambiare la password.
- Auto authentication (Autenticazione automatica) (pagina 4)  
Per immettere automaticamente la password quando l'unità viene collegata a un computer.
- Limit for incorrect password attempts (Limite tentativi password non corretti) (pagina 4)  
Per impostare il comportamento dell'unità in caso di immissione di una password errata.
- Reset to factory defaults (Ripristina i valori predefiniti di fabbrica) (pagina 5)  
Per eliminare tutte le impostazioni e i dati sull'unità disco rigido, ripristinando i valori predefiniti di fabbrica.

## • Status (Stato)

Per controllare lo stato dell'unità.



Selezionare il prodotto da configurare.

Visualizza lo stato corrente dell'unità.

- Standard
- Password non ancora autenticata
- Password autenticata

Immettere un nome (massimo 30 caratteri).

\* Il nome viene visualizzato solo da Secure Lock Manager Easy.

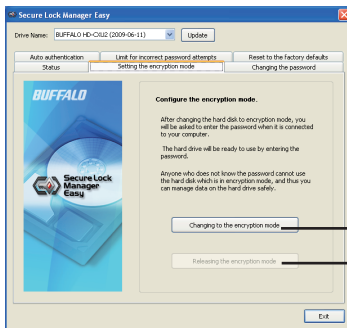
Immettere la password per autenticarla.

\* Se la modalità di crittografia non è abilitata, l'impostazione non ha effetto.

Per bloccare l'unità. Sarà nuovamente necessaria l'autenticazione per accedere all'unità.

## • Encryption mode (Modalità di crittografia)

Per abilitare/disabilitare la crittografia.

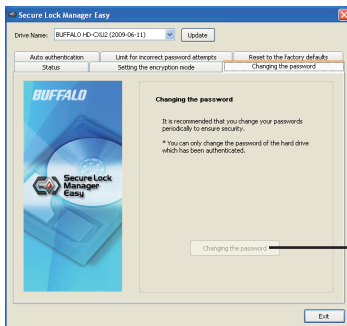


Per abilitare la crittografia. È necessario immettere una password per accedere all'unità oppure configurare l'autenticazione automatica.

Per disabilitare la modalità di crittografia. Chiunque può accedere all'unità senza autenticazione.

## • Password

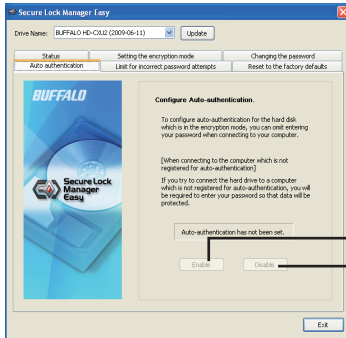
Per cambiare la password.



Per cambiare la password. La crittografia deve essere abilitata ed è necessario immettere la password precedente.

- **Auto authentication (Autenticazione automatica)**

Consente di impostare il metodo di immissione di una password per l'unità. La password può essere immessa automaticamente (autenticazione automatica). Questa impostazione può essere utilizzata per una sola unità per computer.



Per abilitare l'autenticazione automatica.

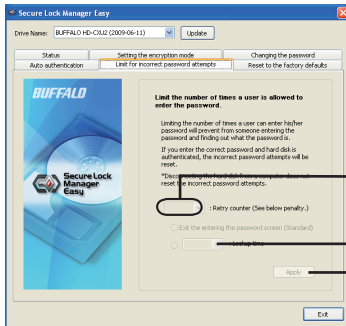
Per disabilitare l'autenticazione automatica.

**Nota:** su ogni computer che utilizza l'autenticazione automatica deve essere installato il software e l'impostazione deve essere abilitata. Su un singolo computer, ogni utente deve abilitare l'autenticazione automatica per utilizzarla.

**Avvertenza:** l'autenticazione automatica non è consigliata se il computer è condiviso con altri utenti. Tali utenti possono visualizzare, eliminare o modificare i dati sull'unità disco rigido, che diventano accessibili come nelle classiche unità disco rigido.

- **Limiting incorrect password attempts (Limite tentativi password non corretti)**

Per impostare il comportamento dell'unità in caso di immissione di una password errata.



Scegliere il numero di tentativi password non corretti tra [3], [5] e [10].

Selezionare il comportamento da tenere al raggiungimento del limite per i tentativi password non corretti.

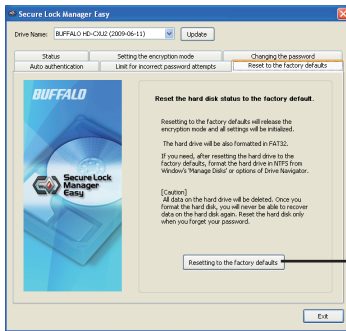
Per applicare un'impostazione.

Comportamento al raggiungimento del limite per i tentativi password non corretti	
Uscita dalla schermata di immissione password (valore predefinito)	La schermata per immettere la password si chiude. Per autenticare la password, aprire nuovamente la schermata per immettere la password.
Impossibile eseguire l'autenticazione durante **	Selezionare il tempo di destinazione, tra [5 minuti], [10 minuti], [30 minuti] e [1 ora], per cui verranno rifiutati i tentativi di autenticazione. L'autenticazione non potrà essere eseguita fino allo scadere del tempo impostato.



- **Resetting to the factory defaults (Ripristino dei valori predefiniti di fabbrica)**

Per eliminare le impostazioni dell'unità e i dati sull'unità disco rigido, ripristinando i valori predefiniti di fabbrica.

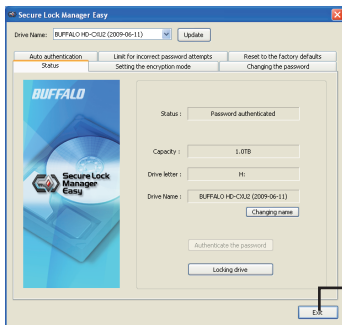


Consente il ripristino dei valori predefiniti di fabbrica. Vengono eliminati la password e tutti i dati salvati.

\* L'unità disco rigido è formattata in FAT32 e la modalità di crittografia verrà disabilitata.

## Chiusura di Secure Lock Manager Easy

Per uscire da Secure Lock Manager Easy, fare clic su [Exit] (Esci) nell'angolo inferiore destro della schermata.



Fare clic su [Exit] (Esci).

## Disinstallazione

È possibile disinstallare Secure Lock Manager Easy quando non è più necessario. Per la disinstallazione, fare clic su [Start] - [Tutti i programmi] o [Programmi] - [BUFFALO] - [Secure Lock Manager Easy] - [Uninstall]. Attenersi quindi alle istruzioni sullo schermo.

## Руководство по быстрому запуску программного обеспечения Secure Lock Manager Easy

Данная продукция содержит [Secure Lock Manager Easy], программное обеспечение кодирования, разработанное компанией Buffalo для запоминающих устройств.

### О программе Secure Lock Manager Easy

Программа Secure Lock Manager Easy предоставляет Вам возможность кодирования и защиты с помощью пароля Вашего запоминающее устройство Buffalo. В этом программном обеспечении доступна возможность автоматического определения подлинности. По умолчанию кодирование отключено.



### Перед использованием этого программного обеспечения

Перед использованием программы Secure Lock Manager Easy, пожалуйста, прочитайте следующие замечания.

- Надежно храните Ваш пароль.
- Без Вашего пароля Вы не сможете получать доступ к накопителю на жестких дисках или изменять установки. Если Вы забудете Ваш пароль, Вам потребуется вернуть Ваш накопитель на жестких дисках к заводским установкам по умолчанию.
- Поддерживаются операционные системы Windows 7 / Vista / XP / 2000, Windows Server 2003 / Sever 2003 R2 / Server 2008 / Server 2008 R2.
- Список совместимых операционных систем только для программного обеспечения Lock Manager Easy. Чтобы узнать, с какими операционными системами работает ваш продукт, обратитесь к сопроводительной документации.
- Чтобы воспользоваться программным обеспечением Secure Lock Manager Easy для работы на компьютере с ОС Windows Server 2003 и Server 2003 R2, войдите в систему как администратор.

### Установка

Программу Secure Lock Manager Easy можно установить из программного обеспечения управления DriveNavigator. Для его установки используйте следующую процедуру.

- 1 Подсоедините накопитель к Вашему компьютеру.
- 2 Выполните правый щелчок по [Utility\_HD-\*\*\*\*]  в Мой компьютер и выберите [Открыть].  
(\*\*\*\* является номером компонента Вашего устройства DriveStation/MiniStation.)
- 3 Дважды щелкните по [DriveNavi.exe] .  
Загрузится программное обеспечение управления DriveNavigator.  
\* Если для Windows Vista отображается сообщение [Для продолжения программы требуется Ваше разрешение], щелкните [Продолжить].
- 4 Щелкните [Дополнительное].
- 5 Щелкните [Установите программу Secure Lock Manager Easy].

Для установки программного обеспечения следуйте инструкциям, отображаемым на экране.

# Запуск программы Secure Lock Manager Easy

Для запуска программы Secure Lock Manager Easy,

## 1 Подсоедините накопитель к Вашему компьютеру.

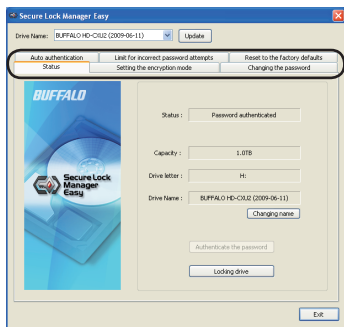
Если отображается экран определения подлинности пароля, введите Ваш пароль.

**Замечание:** Если Вы забыли Ваш пароль и возвращаете Ваш накопитель на жестких дисках к заводским установкам по умолчанию, закройте экран.

## 2 Щелкните [Пуск] - [(Все) Программы] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

# Ярлыки программы Secure Lock Manager Easy

Щелчок по ярлыкам программы Secure Lock Manager Easy дает Вам возможность сконфигурировать следующие установки.

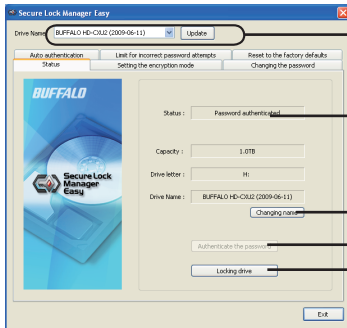


Щелкните по пункту, который Вы хотите сконфигурировать.

- Status (Состояние) (стр. 3)  
Проверка состояния накопителя.
- Encryption mode (Режим кодирования) (стр. 3)  
Включение/отключение кодирования.
- Password (Пароль) (стр. 3)  
Изменение пароля.
- Auto authentication (Автоматическое определение подлинности) (стр. 4)  
Автоматический ввод пароля при подсоединении накопителя к компьютеру.
- Limit for incorrect password attempts (Ограничение для попыток неправильного ввода пароля) (стр. 4)  
Установка поведения устройства в случае ввода Вами неправильного пароля.
- Reset to factory defaults (Возврат к заводским установкам по умолчанию) (стр. 5)  
Удаление всех установок и данных на накопителе на жестком диске путем возврата его к заводским установкам по умолчанию.

## • Status (Состояние)

Проверка состояния накопителя.



Выбор устройства, которое Вы хотите сконфигурировать.

Отображение текущего состояния накопителя.

- Стандартное
- Подлинность пароля еще не определена
- Подлинность пароля определена

Введите имя (не более 30 символов).

\* Это имя отображается только программой Secure Lock Manager Easy.

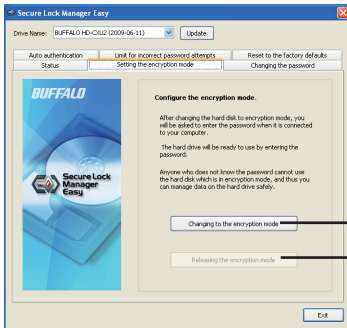
Введите Ваш пароль для определения его подлинности.

\* Если режим кодирования отменен, не работает даже в случае щелчка по этому пункту.

Блокировка накопителя. Для дальнейшего доступа к накопителю потребуется еще одно определение подлинности.

## • Encryption mode (Режим кодирования)

Включение/отключение кодирования.

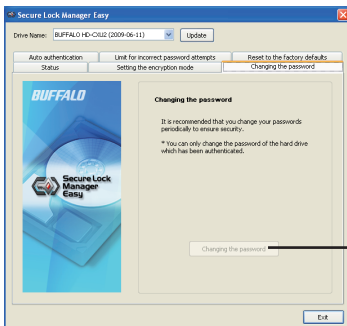


Включение кодирования. Вам будет необходимо ввести пароль для получения доступа к накопителю или для настройки автоматического определения подлинности.

Режим кодирования отключен. Любой пользователь может получить доступ к накопителю без определения подлинности.

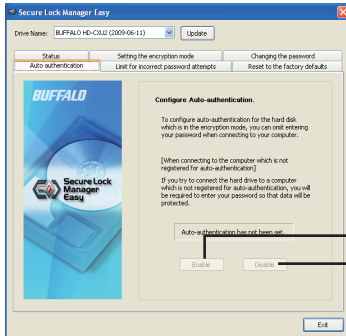
## • Password (Пароль)

Изменение пароля.



Изменение пароля. Чтобы изменить пароль, должно быть включено кодирование, и Вам потребуется ввести старый пароль.

- **Auto authentication (Автоматическое определение подлинности)**  
 Автоматический способ ввода пароля для накопителя. Ваш пароль может вводиться автоматически (автоматическое определение подлинности). Эту установку можно использовать только для одного устройства на компьютер.



Включение автоматического определения подлинности.

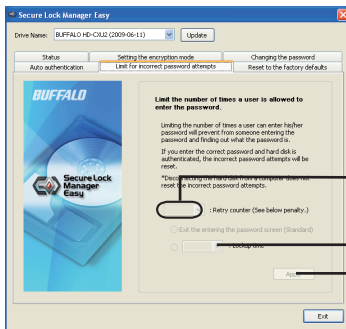
Отмена автоматического определения подлинности.

**Замечание:** На каждом компьютере, который использует автоматическое определение подлинности, необходимо установить программное обеспечение и включить такую установку. На одном компьютере каждый пользователь должен включить автоматическое определение подлинности, чтобы использовать такую функцию.

**Предупреждение:** Автоматическое определение подлинности не рекомендуется в случае использования Вашего компьютера несколькими пользователями. Другие пользователи смогут просматривать, удалять и редактировать данные, поскольку к доступу к накопителю на жестких дисках может быть осуществлен также, как и к обычным накопителям на жестких дисках.

- **Limiting incorrect password attempts (Ограничение попыток неправильного ввода пароля)**

Установка поведения устройства в случае ввода Вами неправильного пароля.



Выбор количества попыток неправильного ввода пароля из значений [3], [5] и [-10].

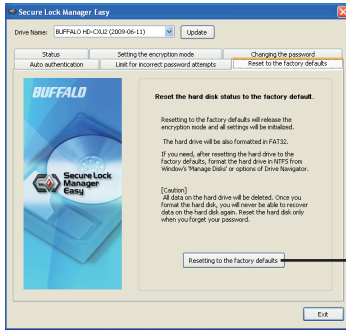
Выбор поведения при достижении предела попыток неправильного ввода пароля.

Применение установки.

Поведение при достижении предела попыток неправильного ввода пароля	
Выход из экрана ввода пароля (Значение по умолчанию)	Экран ввода пароля будет закрыт. Для определения подлинности пароля Вам потребуется открыть экран для ввода пароля еще раз.
Определение подлинности невозможно в течение **	Выберите нужный промежуток времени из значений [5 минут], [10 минут], [30 минут] и [1 час], в течение которого попытки определения подлинности отклоняются. Определение подлинности невозможно до истечения этого времени.

- **Resetting to the factory defaults (Возврат к заводским установкам по умолчанию)**

Удаление установок накопителя и данных на накопителе на жестком диске и его возврат к заводским установкам по умолчанию.

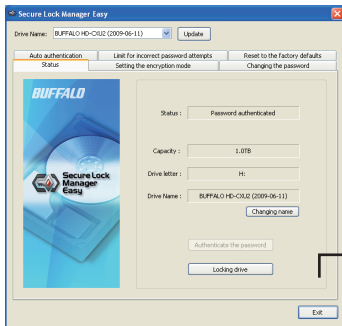


Возврат к заводским установкам по умолчанию. Удаление пароля и всех сохраненных данных.

\* Накопитель на жестких дисках форматируется в системе FAT32, и режим кодирования отменяется.

## Выход из программы Secure Lock Manager Easy

Для выхода из программы Secure Lock Manager Easy щелкните [Exit] (Выйти) в нижней правой части экрана.



Щелкните [Exit] (Выйти).

## Для удаления

Вы можете удалить программу Secure Lock Manager Easy, если она больше Вам не требуется. Для ее удаления щелкните [Пуск] - [(Все) Программы] - [BUFFALO] - [Secure Lock Manager Easy] - [Удаление]. Затем следуйте инструкциям на экране.

# Secure Lock Manager Easy 快速入门指南

本产品包括[Secure Lock Manager Easy].Buffalo 用于存储设备的加密软件。

## 关于 Secure Lock Manager Easy

Secure Lock Manager Easy 用于加密和密码保护 Buffalo 存储设备。软件中提供了自动验证功能。默认情况下禁用加密。


## 使用本软件之前

在使用 Secure Lock Manager Easy 之前，请阅读以下注意事项。

- 保管您的密码安全。
- 没有密码，您将无法存取硬盘或更改设定。如果您忘记密码，必须将硬盘重设为出厂默认设定。
- 支持 Windows 7 / Vista / XP / 2000 / Windows Server 2003 / Sever 2003 R2 / Windows Server 2008 / Server 2008 R2。
- 此处兼容操作系统列表仅适用于 Secure Lock Manager Easy。若要找出可与您产品配合使用的操作系统，请参阅产品文档。
- 若要在运行 Windows Server 2003 和 Server 2003 R2 的 PC 上使用 Secure Lock Manager Easy，请使用管理员帐户登录。

## 安装

Secure Lock Manager Easy 可从 DriveNavigator 安装。请使用以下过程进行安装。

- 1** 连接硬盘到计算机。
- 2** 在[我的电脑]中右键单击[Utility\_HD - \*\*\*\*]()，然后选择[打开]。  
(\*\*\*\* 是 DriveStation / MiniStation 的部件编号。)
- 3** 双击[DriveNavi.exe]()。  
DriveNavigator 将启动。  
\* 如果 Windows Vista 显示[程序需要您的许可才能继续]，单击[继续]。
- 4** 单击[选项]。
- 5** 单击[安装 Secure Lock Manager Easy]。

按照画面上显示的指示安装软件。

# 启动 Secure Lock Manager Easy

要启动 Secure Lock Manager Easy,

## 1 连接硬盘到计算机。

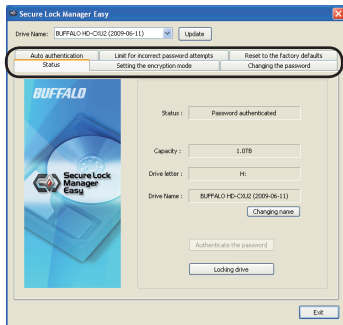
如果显示密码验证画面, 输入密码。

**注意:** 如果您忘记密码并将硬盘重设为出厂默认设定, 请关闭画面。

## 2 单击[开始] - [(所有)程序] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy]。

# Secure Lock Manager 选项卡

单击 Secure Lock Manager Easy 中的选项卡可配置下列设定。



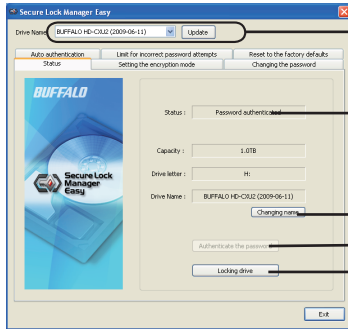
单击您要设置的项目。

- Status (状态)(第3页)  
检查硬盘的状态。
- Encryption mode (加密模式)(第3页)  
启用 / 禁用加密。
- Password (密码)(第3页)  
更改密码。
- Auto authentication (自动验证)(第4页)  
当硬盘连接计算机时自动输入密码。
- Limit for incorrect password attempts (密码输入不正确次数限制)(第4页)  
设置当输入错误密码时设备的动作。
- Reset to factory defaults (重设为出厂默认设定)(第5页)  
删除硬盘上所有设定和数据, 将其重设为出厂默认设定。



## • Status (状态)

检查硬盘的状态。



选择您要设置的产品。

显示硬盘的当前状态。

- 标准
- 尚未验证密码
- 已验证密码

输入名称 (30个字符或以下)。

\* 此名称仅在 Secure Lock Manager Easy 中显示。

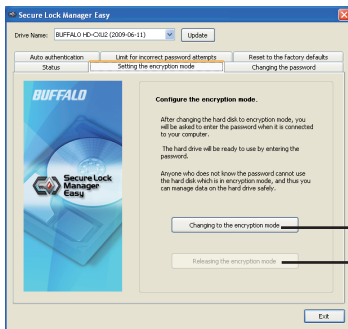
输入密码以进行验证。

\* 如果加密模式解除, 即使单击它也无效。

锁定硬盘。接下来存取硬盘将再次需要验证。

## • Encryption mode (加密模式)

启用 / 禁用加密。

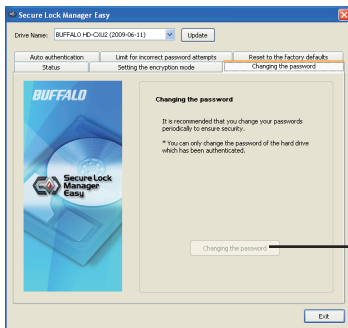


启用加密。您将需要输入密码才能存取硬盘或设置自动验证。

禁用加密模式。任何人不用验证就可存取硬盘。

## • Password (密码)

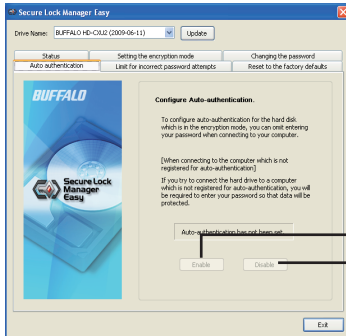
更改密码。



更改密码。要更改密码, 必须启用加密并且输入旧的密码。

## • Auto authentication (自动验证)

设置输入硬盘密码的方法。您的密码可自动输入(自动验证)。此设定可用于每台计算机的一个设备。



启用自动验证。

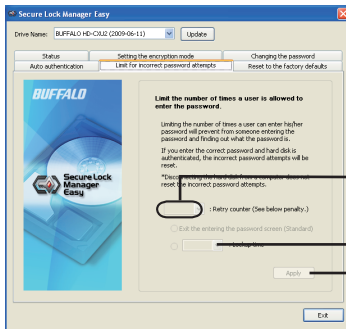
禁用自动验证。

**注意：**使用自动验证的每台计算机都需要安装本软件并启用此设定。在单台计算机上，每个用户需要启用自动验证才能使用。

**警告：**如果您与多个用户共享计算机，则不推荐使用自动验证。否则其他用户就可以查看、删除或编辑数据，因为硬盘上的数据可象标准硬盘那样被存取。

## • Limiting incorrect password attempts (限制密码输入不正确次数)

设置当输入错误密码时设备的动作。



从[3]、[5]和[10]选择密码输入不正确次数。

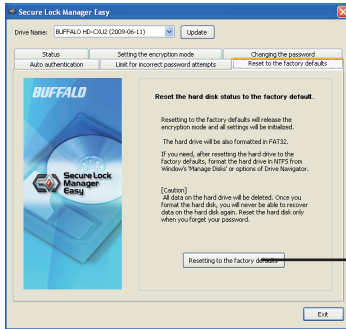
选择当达到不正确密码输入次数限制时的动作。

应用设定。

当达到不正确密码输入次数限制时的动作	
退出输入密码画面 (默认值)	密码输入画面将关闭。要验证密码，您需要打开画面并重新输入密码。
在 ** 期间不能验证	从[5 分钟]、[10 分钟]、[30 分钟]和[1 小时] 选择目标时间，在此期间将拒绝验证尝试。经过这些时间后才可进行验证。

## • [Resetting to factory defaults](重设为出厂默认设定)

删除硬盘设定和硬盘上的数据，并将其重设为出厂默认设定。

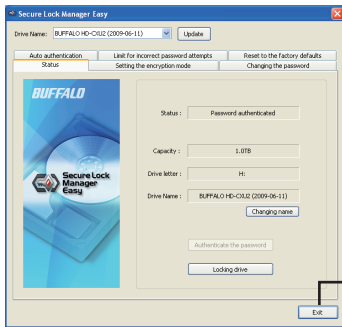


重设为出厂默认设定。删除保存的密码和所有数据。

\* 硬盘用 FAT32 格式化，加密模式将解除。

## 退出 Secure Lock Manager Easy

要退出 Secure Lock Manager Easy,单击画面右下方的[Exit](退出)。



单击[Exit](退出)。

## 要卸载

不再需要时，您可以卸载 Secure Lock Manager Easy。要卸载它，单击[开始] - [(所有)程序] - [BUFFALO] - [Secure Lock Manager Easy] - [卸载]。然后按画面上的指示进行操作。

# Secure Lock Manager Easy 快速使用指南

此產品包含 Buffalo 為儲存裝置開發的加密軟體[Secure Lock Manager Easy]。

## 關於 Secure Lock Manager Easy

Secure Lock Manager Easy 可讓您將 Buffalo 儲存裝置加密並使用密碼保護。  
此軟體也提供自動驗證功能。預設值為停用加密功能。

## 使用此軟體之前

在您使用 Secure Lock Manager Easy 之前請先閱讀下列注意事項。

- 請妥善保護您的密碼。
- 若沒有密碼，您將無法存取硬碟或變更設定。若您忘記密碼，您必須將磁碟重設為出廠預設值。
- 支援 Windows 7/Vista/XP/2000/Windows Server 2003/Sever 2003 R2/Windows Server 2008/Server 2008 R2。
- 該相容作業系統清單僅適用於 Secure Lock Manager Easy。請參閱您的產品文件，以找出可與您產品搭配使用的作業系統。
- 若要在執行 Windows Server 2003 和 Server 2003 R2 的電腦上使用 Secure Lock Manager Easy，您需要使用管理員帳戶登入。

## 安裝

您可從 DriveNavigator 安裝 Secure Lock Manager Easy。請透過下面的程序安裝。

- 1** 將磁碟連接至電腦。
- 2** 在[我的電腦]中的[Utility\_HD-\*\*\*\*]上按一下右鍵，()，然後選擇[開啟]。  
(\*\*\*\* 為 DriveStation/MiniStation 的零件編號。)
- 3** 按兩下[DriveNavi.exe] ()。  
便會載入 DriveNavigator。  
\* 若在 Windows Vista 中顯示[此程式需要您的允許才能執行]，請按一下[繼續]。
- 4** 按一下[選項]。
- 5** 按一下[安裝 Secure Lock Manager Easy]。

依照畫面上顯示的指示安裝軟體。

# 載入 Secure Lock Manager Easy

若要載入 Secure Lock Manager Easy，

## 1 將磁碟連接至電腦。

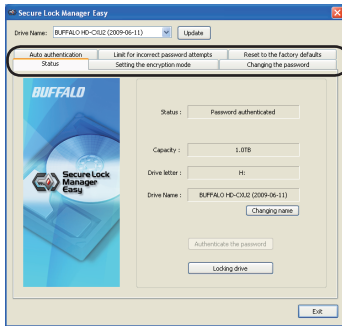
若有顯示密碼驗證畫面，請輸入您的密碼。

註：若您忘記密碼並將裝置重設為出廠預設值，請關閉畫面。

## 2 按一下[開始] - [所有程式 (程式集)] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy]。

# Secure Lock Manager 標籤

按一下 Secure Lock Manager Easy 中的標籤可讓您設定下列設定。

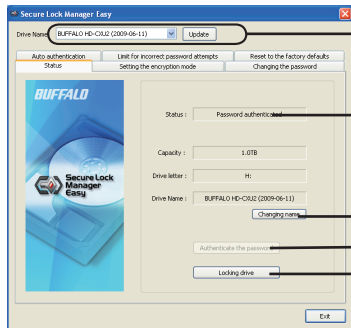


按一下您想要設定的項目。

- Status (狀態) (第3頁)  
檢查磁碟狀態。
- Encryption mode (加密模式) (第3頁)  
啟用/停用加密功能。
- Password (密碼) (第3頁)  
變更密碼。
- Auto authentication (自動驗證) (第4頁)  
在磁碟連接至電腦時自動輸入密碼。
- Limit for incorrect password attempts (密碼輸入錯誤的次數限制) (第4頁)  
設定密碼輸入錯誤時裝置的反應。
- Reset to factory defaults (重設為出廠預設值) (第5頁)  
刪除硬碟上的所有設定與資料，並將之重設為出廠預設值。

## • Status (狀態)

檢查磁碟狀態。



選擇您想要設定的產品。

顯示磁碟目前的狀態。

- 標準
- 尚未驗證密碼
- 已經驗證密碼

輸入名稱 (30 個以下的字元)。

\* 此名稱只會在 Secure Lock Manager Easy 中顯示。

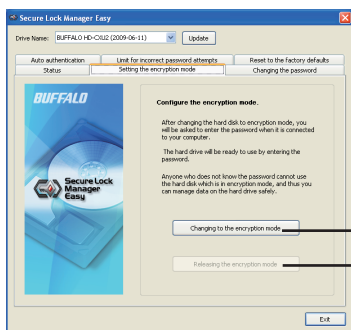
輸入您的密碼以驗證密碼。

\* 若已經釋放加密模式，即使按一下此按鍵也沒有作用。

鎖住磁碟。若要再次存取磁碟，便會再度執行驗證作業。

## • Encryption mode (加密模式)

啟用/停用加密功能。

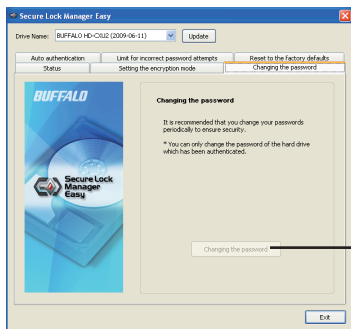


啟用加密功能。您必須輸入密碼來存取磁碟，或設定自動驗證。

停用加密模式。任何人都不需要驗證即可存取磁碟。

## • Password (密碼)

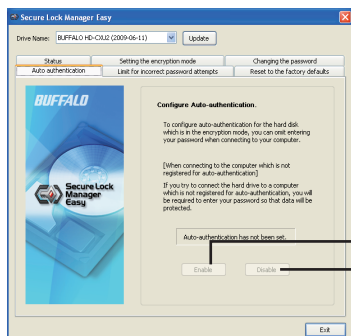
變更密碼。



變更密碼。若要變更密碼，便必須啟用加密功能，並且您必須輸入舊的密碼。

## ▪ Auto authentication (自動驗證)

設定輸入磁碟密碼的方式。您可以讓軟體自動輸入密碼(自動驗證)。每部電腦的其中一部裝置可使用此設定。



啟用自動驗證。

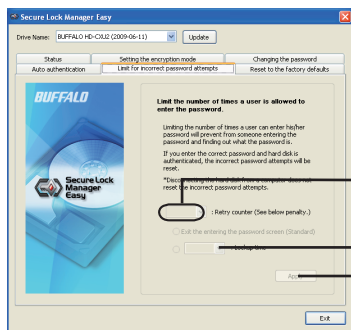
停用自動驗證。

**註：**每部使用自動驗證功能的電腦皆必須安裝此軟體並啟用此設定。在單一電腦上，每個使用者皆必須啟用自動驗證以使用該功能。

**警告：**若您與多個使用者共用您的電腦，不建議您使用自動驗證。資料可能會被其他使用者檢視、刪除或編輯，因為他們可像存取標準硬碟一樣存取硬碟上的資料。

## ▪ Limiting incorrect password attempts (密碼輸入錯誤的次數限制)

設定裝置在您輸入錯誤密碼時的反應。



從 [3]、[5] 及 [10] 中選擇允許密碼輸入錯誤的次數限制。

選擇達到密碼輸入錯誤次數限制時的反應。

套用設定。

### 達到密碼輸入錯誤次數限制時的反應

退出密碼輸入畫面  
(預設值)

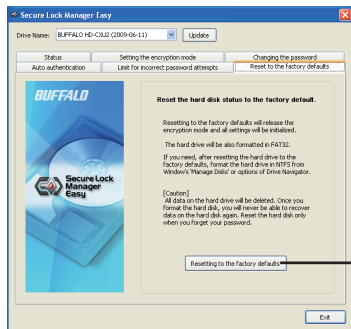
密碼輸入畫面將會關閉。若要驗證密碼，您必須開啟畫面再度輸入密碼。

在 \*\* 時無法驗證

從 [5 分鐘]、[10 分鐘]、[30 分鐘] 及 [1 小時] 中選擇拒絕嘗試驗證的目標時限。超過時間限制之後仍然無法完成驗證。

## ▪ Resetting to the factory defaults (重設為出廠預設值)

刪除硬碟的設定和硬碟上的資料，並將之重設為出廠預設值。

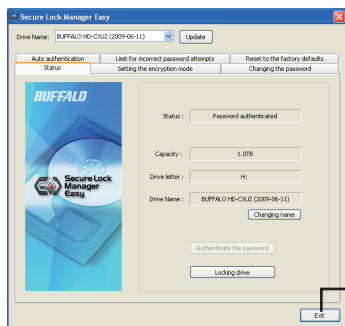


重設為出廠預設值。刪除密碼及已經儲存的所有資料。

\* 會以 FAT32 檔案系統將硬碟格式化，並釋放所有加密模式。

## 結束 Secure Lock Manager Easy

若要結束 Secure Lock Manager Easy，請按一下畫面右下方的[Exit] (結束)。



按一下[Exit] (結束)。

## 解除安裝

您可以在不需要 Secure Lock Manager Easy 的時候將它解除安裝。若要將它解除安裝，請按一下[開始]-[所有程式 (程式集)]-[BUFFALO]-[Secure Lock Manager Easy]-[解除安裝]。



# SecureLock Manager Easy の使いかた

本書は、本製品の暗号化機能管理ソフトウェア「SecureLock Manager Easy」について説明します。

## SecureLock Manager Easy とは

本製品の暗号化設定を行うソフトウェアです。このソフトウェアを使用すれば、パスワードを設定したり、暗号化モードの変更やパスワードの変更、自動認証などを設定することができます。

## お使いになる前に

SecureLock Manager Easy をお使いになる前に、以下のことをご確認ください。

● **パスワードは厳重に管理してください。**

パスワードを忘れた場合、本製品の設定、認証が行えず、保存したデータは一切取り出せません。パスワードを忘れた場合は、本製品を出荷時の状態に戻してください。

● SecureLock Manager Easy は、Windows 7/Vista/XP/2000/Server 2008 R2/Server 2008/Server 2003 R2/Server 2003 に対応しています。


※ 上記は、SecureLock Manager Easy の対応 OS です。製品によっては対応 OS が異なることがありますので、製品の対応 OS にも適応したパソコンでお使いください。

※ Windows Server 2003 R2/Server 2003 の場合、コンピューターの管理者 (Administrator) 権限を持つユーザーでログインしないとお使いいただけません。

## インストール

SecureLock Manager Easy は、ドライブナビゲータ (本製品に収録されている「DriveNavi.exe」をダブルクリックしたときに表示されるメニュー) からインストールできます。以下の手順でインストールしてください。

**1 本製品をパソコンに接続します。**

**2 コンピュータ (マイコンピュータ) にある「Utility\_HD-xxxx」(xxxx は製品名) (  ) を右クリックし、[開く] を選択します。**

**3 「DriveNavi.exe」(  ) をダブルクリックします。**

ドライブナビゲーターが起動します。

※ 「次のプログラムにこのコンピュータへの変更を許可しますか？」や「プログラムを続行するにはあなたの許可が必要です」と表示されたら、[はい]または[続行]をクリックしてください。

**4 [オプション] をクリックします。**

**5 [SecureLock Manager Easy のインストール] をクリックします。**


以降は、画面の指示に従ってインストールしてください。

# SecureLock Manager Easy を起動する

SecureLock Manager Easy は、以下の手順で起動してください。

## 1 本製品をパソコンに接続します。

パスワード認証の画面が表示された場合は、パスワードを入力します。

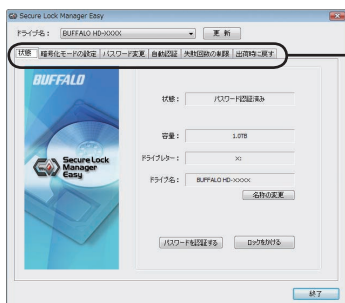
 パスワードを忘れて出荷時の状態に戻す場合は、画面を閉じてください。

## 2 [スタート] – [(すべての) プログラム] – [BUFFALO] – [SecureLock Manager Easy] – [SecureLock Manager Easy] をクリックします。

SecureLock Manager Easy が起動します。

# SecureLock Manager Easy の項目説明

SecureLock Manager Easy の画面上的タブをクリックすることにより、以下の設定を行えます。

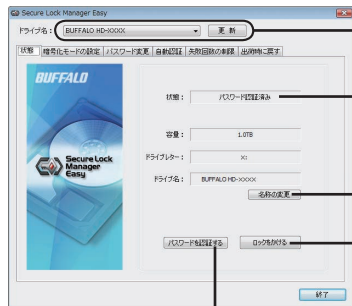


設定する項目をクリックします。

- **状態 (P3)**  
本製品の状態を確認できます。
- **暗号化モードの設定 (P3)**  
暗号化機能の有効 / 無効を設定できます。
- **パスワード変更 (P4)**  
登録済みのパスワードを変更できます。
- **自動認証 (P4)**  
パソコンへの接続時にパスワード入力が省略できます。
- **失敗回数の制限 (P5)**  
パスワード入力に失敗した場合の動作を設定します。
- **出荷時に戻す (P5)**  
本製品の設定やデータを削除し、出荷時の状態に戻します。

## ■状態

本製品の状態を確認できます。



設定する本製品を選択します。

本製品の状態を表示します。

名称を変更します。半角 30 文字以内で入力してください。  
※この名称は SecureLock Manager Easy でのみ表示されます。

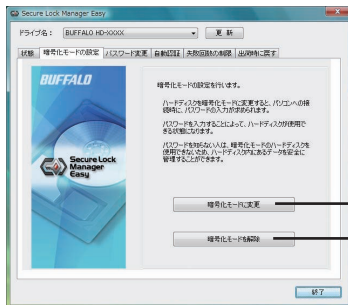
本製品をロックします。  
※パスワード認証前の状態にします。

パスワードを入力して認証します。  
※暗号化モードを解除した場合は、使用しません。

状態	
通常	本製品にアクセスできます。
パスワード認証前	パスワードを入力するまで、本製品にアクセスできません。
パスワード認証済み	本製品にアクセスできます。

## ■暗号化モードの設定

暗号化機能の有効 / 無効を設定できます。

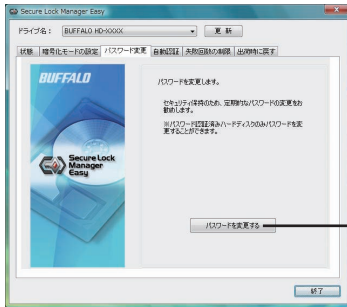


暗号化モードに変更します。通常モードの本製品に対し、パスワードを設定します。パスワード認証に成功しないと、本製品を使用できません。

暗号化モードを解除します。通常のドライブとして、使用可能です。  
※第三者にデータを取り出される恐れがあります。

## ■パスワード変更

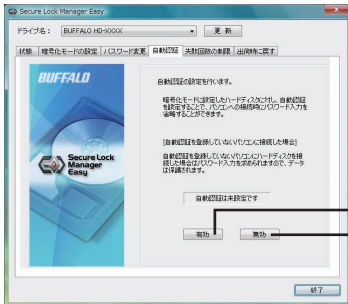
登録済みのパスワードを変更できます。



パスワードを変更します。  
※通常モード、パスワード認証前は設定できません。

## ■自動認証

本製品のパスワード入力方法を設定します。パスワードを自動で入力（自動認証）することができます。お使いのパソコン1台ごとと製品ごとに設定を行います。



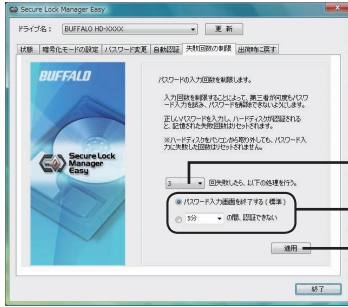
自動認証を有効にします。パスワード入力が省略できます。  
※パスワード入力が省略できるのは、本機能を有効にしたパソコンのみです。  
※他のユーザーでログオンした場合も、パスワード入力を省略します。

自動認証を無効にします。

**△注意** お使いのパソコンを複数のユーザーで使用されている場合は、自動認証を有効にする設定はお勧めできません。ハードディスク内のデータが通常のハードディスクと同じように見えるため、他の人に閲覧、削除、編集される可能性があります。

## ■失敗回数の制限

パスワード入力に失敗した場合の動作を設定します。



パスワード入力の失敗回数を「3回」「5回」「10回」から選択します。

失敗回数に達した場合の動作を選択します。

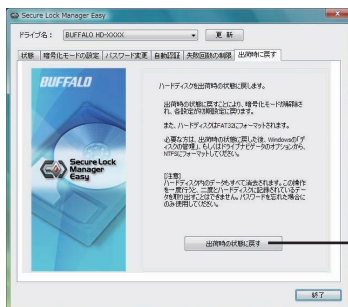
設定を適用します。

### 失敗回数に達した場合の動作

パスワード入力画面を終了する(初期値)	パスワード入力画面が終了します。認証するには、改めてパスワード入力画面を起動してください。
XXの間、認証できない	XXは「5分」「10分」「30分」「1時間」のいずれかを選択します。設定した時間が経過するまで、認証できません。

## ■出荷時に戻す

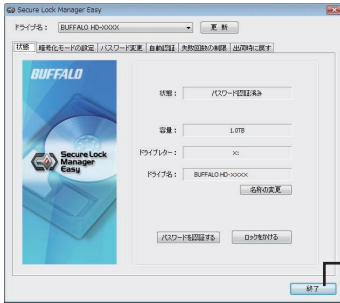
本製品の設定やデータを削除し、出荷時の状態に戻します。



出荷時の状態に戻します。パスワードや記録済みの全データを削除します。  
※FAT32でフォーマットし、暗号化モードは解除されます。

## SecureLock Manager Easy を終了する

SecureLock Manager Easy を終了するときは、画面右下の [終了] をクリックしてください。



[終了] をクリックします。

## アンインストールするときは

SecureLock Manager Easy が不要になった場合は、アンインストールできます。アンインストールするときは、[スタート] - [(すべての) プログラム] - [BUFFALO] - [SecureLock Manager Easy] - [アンインストール] をクリックし、画面の指示に従ってください。

# Secure Lock Manager Easy 퀵스타트 가이드

본 제품에는 Buffalo의 저장 장치용 암호화 소프트웨어, [Secure Lock Manager Easy] 가 포함되어 있습니다.

## Secure Lock Manager Easy에 대하여

Secure Lock Manager Easy 를 통해 Buffalo 저장 장치를 암호화하고 암호를 보호할 수 있습니다. 자동 인증 준비는 소프트웨어에서 사용할 수 있습니다. 암호화는 기본적으로 해제되어 있습니다.


## 이 소프트웨어를 사용하기 전에

Secure Lock Manager Easy 를 사용하기 전에 다음 주의사항을 확인하시기 바랍니다.

- 암호를 안전하게 보관하십시오.
- 암호가 없이 하드 드라이브에 액세스하거나 설정을 변경할 수 없습니다. 암호를 분실한 경우 드라이브를 공장 출하시 기본값으로 재설정해야 합니다.
- Windows 7/Vista/XP/2000/Windows Server 2003/Sever 2003 R2/Windows Server 2008/Server 2008 R2 를 지원합니다.
- 이 호환 운영 체제 목록은 Secure Lock Manager Easy에만 해당됩니다. 사용 제품과 호환되는 운영 체제 목록은 설명서를 참조하십시오.
- Windows Server 2003 과 Server 2003 R2 PC에서 Secure Lock Manager Easy 를 사용하려면 관리자 계정으로 로그인 하십시오.

## 설치

Secure Lock Manager Easy 는 DriveNavigator 에서 설치할 수 있습니다. 다음 절차에 따라 설치하십시오.

- 1 드라이브를 컴퓨터에 연결합니다.
- 2 내 컴퓨터에서 [Utility\_HD-\*\*\*\*]  를 마우스 오른쪽 단추로 클릭하고 [열기]를 선택합니다.  
(\*\*\*\*는 DriveStation/MiniStation 의 부품 번호입니다.)
- 3 [DriveNavi.exe]  을 두 번 클릭합니다.  
DriveNavigator 가 시작됩니다.  
\* [계속하려면 프로그램에서 사용자 권한을 요구합니다] 라는 메시지가 Windows Vista 에서 표시되면, [계속]을 클릭하십시오.
- 4 [옵션] 을 클릭합니다.
- 5 [Secure Lock Manager Easy 설치] 를 클릭합니다.

화면에 표시된 설명을 따라 소프트웨어를 설치합니다.

# Secure Lock Manager Easy 시작하기

Secure Lock Manager Easy 를 시작하려면,

**1** 드라이브를 컴퓨터에 연결합니다.

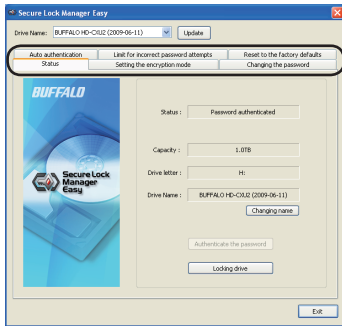
암호 인증 화면이 표시되면 암호를 입력합니다.

**참고:** 암호를 분실한 경우 유닛을 공장 출하시 기본값으로 재설정하고 화면을 닫습니다.

**2** [시작] - [(모든) 프로그램] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy] 을 클릭합니다.

## Secure Lock Manager 탭

Secure Lock Manager Easy 의 탭을 클릭하여 다음 설정을 구성할 수 있습니다.



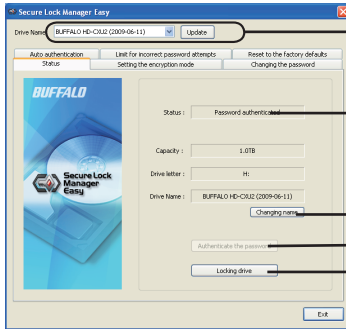
구성할 항목을 클릭합니다.

- **Status (상태)** (3페이지)  
드라이브 상태를 확인합니다.
- **Encryption mode (암호화 모드)** (3페이지)  
암호화를 사용/해제합니다.
- **Password (암호)** (3페이지)  
암호를 변경합니다.
- **Auto authentication (자동 인증)** (4페이지)  
드라이브가 컴퓨터에 연결되면 암호를 자동으로 입력합니다.
- **Limit for incorrect password attempts (정확하지 않은 암호 시도에 대한 제한)** (4페이지)  
정확하지 않은 암호를 입력했을 때 유닛의 동작을 설정합니다.
- **Reset to factory defaults (공장 출하시 기본값으로 재설정)** (5페이지)  
공장 출하시 기본값으로 재설정하여 하드 드라이브의 모든 설정과 데이터를 삭제합니다.



## • Status (상태)

드라이브 상태를 확인합니다.



구성하려는 제품을 선택합니다.

드라이브의 현재 상태를 표시합니다.

- 표준
- 암호가 아직 인증되지 않음
- 암호 인증됨

이름(30자 이하)을 입력합니다.

\* 이 이름은 Secure Lock Manager Easy 에 의해서만 표시됩니다.

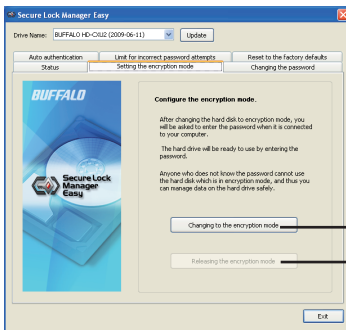
암호를 입력하여 인증합니다.

\* 암호화 모드를 해제한 경우 클릭을 하더라도 응답하지 않습니다.

드라이브를 잠급니다. 나중에 드라이브에 액세스하려면 다시 인증을 받아야 합니다.

## • Encryption mode (암호화 모드)

암호화를 사용/해제합니다.

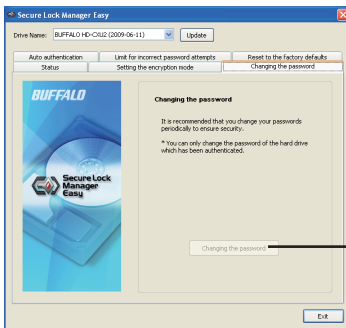


암호화를 사용합니다. 드라이브에 액세스하거나 자동 인증을 설정하려면 암호를 입력해야 합니다.

암호화 모드를 해제합니다. 인증 없이 누구나 드라이브에 액세스할 수 있습니다.

## • Password (암호)

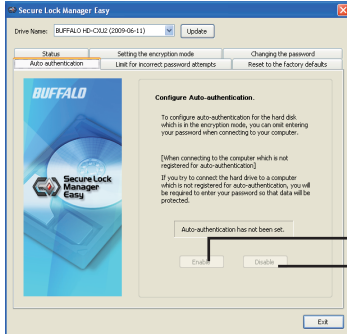
암호를 변경합니다.



암호를 변경합니다. 암호를 변경하려면 암호화를 사용할 수 있어야 하고 이전 암호를 입력하여야 합니다.

## • Auto authentication (자동 인증)

드라이브 암호를 입력할 방법을 설정합니다. 암호를 자동으로 입력할 수 있습니다(자동 인증). 이 설정은 컴퓨터 한 대당 하나의 유닛에 사용할 수 있습니다.



자동 인증을 사용합니다.

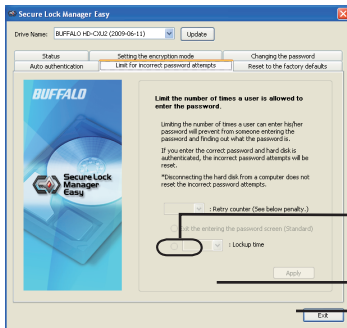
자동 인증을 해제합니다.

**참고:** 자동 인증을 사용하는 각 컴퓨터는 소프트웨어를 설치해야 하고 이 설정을 사용할 수 있어야 합니다. 단일 컴퓨터에서 사용하려면 각 사용자가 자동 인증을 사용할 수 있어야 합니다.

**경고:** 컴퓨터를 여러 사용자와 함께 공유하는 경우 자동 인증을 사용하지 않는 것이 좋습니다. 하드 드라이브의 데이터는 표준 하드 드라이브처럼 액세스할 수 있으므로 다른 사용자가 데이터를 보거나, 삭제하거나 편집할 수 있습니다.

## • Limiting incorrect password attempts (정확하지 않은 암호 시도 제한)

정확하지 않은 암호를 입력했을 때 유닛의 동작을 설정합니다.



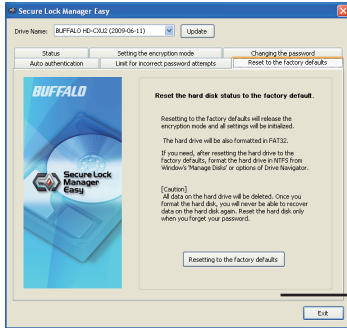
정확하지 않은 암호 시도를 [3], [5] 및 [10] 중에서 선택합니다.

정확하지 않은 암호 시도 한계에 도달했을 때의 동작을 선택합니다.

설정을 적용합니다.

정확하지 않은 암호 시도 한계에 도달했을 때의 동작	
암호 입력 화면 끝내기 (기본 값)	암호를 입력할 화면이 닫힙니다. 암호를 인증하려면 화면을 열고 암호를 다시 입력해야 합니다.
** 동안 인증할 수 없음	목표 시간을 [5분], [10분], [30분] 및 [1시간] 중 선택하여 인증 시도를 거부합니다. 시간이 지날 때까지 인증을 완료할 수 없습니다.

- **Resetting to the factory defaults (공장 출하시 기본값으로 재설정하기)**  
하드 드라이브의 설정과 데이터를 삭제하고 공장 출하시 기본값으로 재설정합니다.

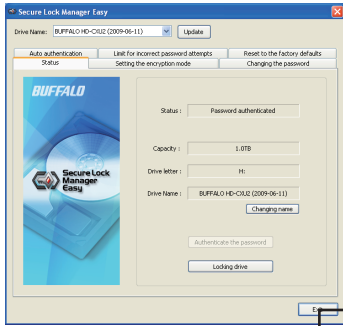


공장 출하시 기본값으로 재설정합니다.  
저장되어 있는 암호와 모든 데이터를 삭제합니다.

\* 하드 드라이브는 FAT32로 포맷되어 있고 암호화 모드가 해제됩니다.

## Secure Lock Manager Easy 끝내기

Secure Lock Manager Easy 를 끝내려면, 화면 하단 오른쪽에 있는 [Exit] (끝내기)를 클릭합니다.



[Exit] (끝내기)를 클릭합니다.

## 제거하려면

더 이상 필요하지 않을 경우 Secure Lock Manager Easy를 제거할 수 있습니다. 제거하려면 [시작] - [(모든) 프로그램] - [BUFFALO] - [Secure Lock Manager Easy] - [제거] 를 클릭합니다. 그런 다음 화면의 지시사항을 따릅니다.

## คู่มือการเริ่มต้นใช้งาน Secure Lock Manager Easy ฉบับย่อ

ผลิตภัณฑ์นี้มาพร้อมกับ [Secure Lock Manager Easy" ซึ่งเป็นซอฟต์แวร์การเข้ารหัสสำหรับอุปกรณ์เก็บข้อมูล ของ Buffalo

### เกี่ยวกับ Secure Lock Manager Easy

Secure Lock Manager Easy ช่วยให้คุณสามารถเข้ารหัสและใช้รหัสผ่านเพื่อป้องกันอุปกรณ์เก็บข้อมูล Buffalo ของคุณได้ ซอฟต์แวร์นี้มีการเตรียมใช้งานสำหรับการรับรองความถูกต้องอัตโนมัติ การเข้ารหัสจะปิดใช้งานตาม ค่าเริ่มต้น



### ก่อนใช้ซอฟต์แวร์นี้

โปรดอ่านหมายเหตุต่อไปนี้ก่อนใช้ Secure Lock Manager Easy

- เก็บรักษารหัสผ่านของคุณให้ปลอดภัย
- ถ้าไม่มีรหัสผ่าน คุณจะไม่สามารถเข้าใช้งานฮาร์ดไดรฟ์หรือเปลี่ยนการตั้งค่าได้
- ถ้าคุณลืมรหัสผ่าน คุณต้องตั้งค่าไดรฟ์ของคุณใหม่ให้เป็นค่าเริ่มต้นจากโรงงาน
- ต้องใช้ระบบ Windows 7/Vista/XP/2000/Windows Server 2003/Server 2003 R2/Windows Server 2008/Server 2008 R2
- รายการระบบปฏิบัติการที่รองรับเฉพาะสำหรับ Secure Lock Manager Easy ดูระบบปฏิบัติการที่สามารถใช้งานร่วมกับผลิตภัณฑ์ของคุณได้จากเอกสารกำกับ
- ใช้ Secure Lock Manager Easy กับ Windows Server 2003 และ Server 2003 R2 PC ได้โดยล็อกอินเข้าในบัญชีผู้ดูแลระบบ

### การติดตั้ง

คุณสามารถติดตั้ง Secure Lock Manager Easy ได้จาก DriveNavigator โดยทำตามขั้นตอนการติดตั้งต่อไปนี้

- 1 เชื่อมต่อไดรฟ์เข้ากับคอมพิวเตอร์ของคุณ
- 2 คลิกขวาที่ [Utility\_HD-\*\*\*\*]  ใน คอมพิวเตอร์ของฉัน แล้วเลือก [เปิด] (\*\*\*\* คือหมายเลขอุปกรณ์ของ DriveStation/MiniStation ของคุณ)
- 3 คลิกสองครั้งที่ [DriveNavi.exe]   
DriveNavigator จะเปิดขึ้นมา  
\*ถ้า Windows Vista แสดงข้อความว่า [โปรแกรมต้องการสิทธิ์ของคุณเพื่อดำเนินการต่อ] ให้คลิก [ดำเนินการต่อ]
- 4 คลิก [ตัวเลือก]
- 5 คลิก [ติดตั้ง Secure Lock Manager Easy]

ทำตามคำแนะนำที่ปรากฏบนหน้าจอเพื่อติดตั้งซอฟต์แวร์

# การเปิดใช้ซอฟต์แวร์ Secure Lock Manager Easy

เมื่อต้องการเปิดใช้ซอฟต์แวร์ Secure Lock Manager Easy

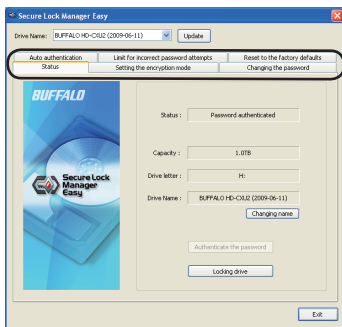
## 1 ให้เชื่อมต่อไดรฟ์เข้ากับคอมพิวเตอร์ของคุณ

ถ้าหน้าจอการรับรองความถูกต้องของรหัสผ่านแสดงขึ้น ให้ใส่รหัสผ่านของคุณ  
หมายเหตุ: ถ้าคุณลืมรหัสผ่านและตั้งค่าอุปกรณ์ใหม่ให้เป็นค่าเริ่มต้นจากโรงงาน ให้ปิดหน้าจอ

## 2 คลิก [เริ่ม] - [โปรแกรม (ทั้งหมด)] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy]

# แท็บ Secure Lock Manager

เมื่อคลิกที่แท็บใน Secure Lock Manager Easy คุณจะสามารกำหนดค่าต่างๆ ดังต่อไปนี้

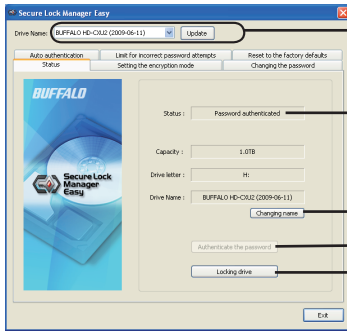


คลิกรายการที่คุณต้องการกำหนดค่า

- Status (สถานะ) (หน้า 3)  
ตรวจสอบสถานะของไดรฟ์
- Encryption mode (โหมดการเข้ารหัส) (หน้า 3)  
เปิดใช้งาน/ปิดใช้งานการเข้ารหัส
- Password (รหัสผ่าน) (หน้า 3)  
เปลี่ยนรหัสผ่าน
- Auto authentication (การรับรองความถูกต้องอัตโนมัติ) (หน้า 4)  
จะใส่รหัสผ่านให้โดยอัตโนมัติเมื่อเชื่อมต่อไดรฟ์เข้ากับคอมพิวเตอร์
- Limit for incorrect password attempts (จำกัดจำนวนครั้งของความพยายามในการใส่รหัสผ่านไม่ถูกต้อง) (หน้า 4)  
ตั้งค่าลักษณะการทำงานของอุปกรณ์เมื่อคุณใส่รหัสผ่านไม่ถูกต้อง
- Reset to factory defaults (ตั้งค่าใหม่ให้เป็นค่าเริ่มต้นจากโรงงาน) (หน้า 5)  
ลบการตั้งค่าและข้อมูลทั้งหมดบนฮาร์ดไดรฟ์ แล้วตั้งค่าใหม่ให้เป็นค่าเริ่มต้นจากโรงงาน

● Status (สถานะ)

ตรวจสอบสถานะของไดรฟ์



เลือกผลิตภัณฑ์ที่คุณต้องการกำหนดค่า

แสดงสถานะปัจจุบันของไดรฟ์

- มาตรฐาน
- ยังไม่ได้รับรองความถูกต้องของรหัสผ่าน
- รับรองความถูกต้องของรหัสผ่านแล้ว

ใส่ชื่อ (ไม่เกิน 30 อักขระ)

\* ชื่อนี้จะแสดงโดย Secure Lock Manager Easy เท่านั้น

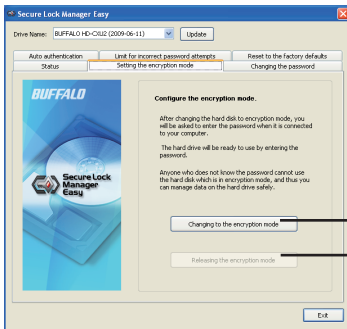
ใส่รหัสผ่านของคุณเพื่อรับรองความถูกต้อง

\* ถ้าโหมดการเข้ารหัสถูกปลดออกใหม่ตอนนี้จะไม่ทำงานแม้ว่าคุณจะคลิกที่ปุ่ม

ล็อกไดรฟ์ จะต้องรับรองความถูกต้องอีกครั้งเพื่อ เขาใช้ไดรฟ์ต่อไป

● Encryption mode (โหมดการเข้ารหัส)

เปิดใช้งาน/ปิดใช้งานการเข้ารหัส



เปิดใช้งานการเข้ารหัส

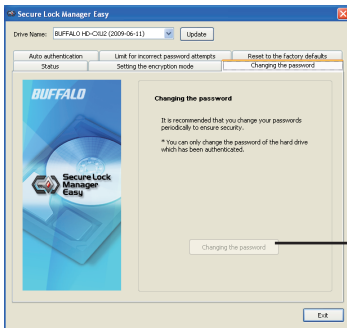
คุณจะต้องใส่รหัสผ่านเพื่อเข้าใช้งานไดรฟ์หรือตั้งค่าการรับรองความถูกต้องอัตโนมัติ

ปิดใช้งานโหมดการเข้ารหัส

ผู้ใช้ทุกคนสามารถเขาใช้ไดรฟ์ได้โดยไม่ต้องผ่านการรับรองความถูกต้อง

● Password (รหัสผ่าน)

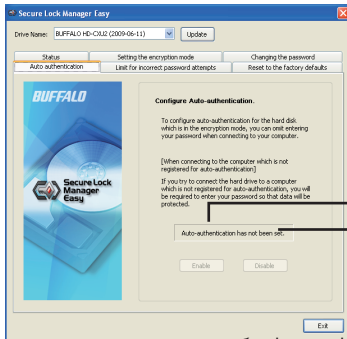
เปลี่ยนรหัสผ่าน



เปลี่ยนรหัสผ่าน

เมื่อต้องการเปลี่ยนรหัสผ่านคุณต้องเปิดใช้งานการเข้ารหัสและใส่รหัสผ่านเดิม

- Auto authentication (การรับรองความถูกต้องอัตโนมัติ)  
ตั้งควาวิธีการใส่รหัสผ่านสำหรับไดรฟ์ คุณสามารถใส่รหัสผ่านของคุณโดยอัตโนมัติได้ (การรับรองความถูกต้องอัตโนมัติ) การตั้งค่านี้ใช้ได้กับอุปกรณ์หนึ่งตัวต่อคอมพิวเตอร์หนึ่งเครื่องเท่านั้น



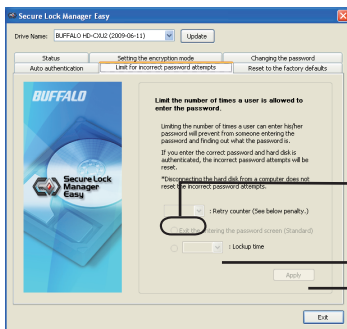
เปิดใช้งานการรับรองความถูกต้องอัตโนมัติ

ปิดใช้งานการรับรองความถูกต้องอัตโนมัติ

**หมายเหตุ:** คอมพิวเตอร์แต่ละเครื่องที่ใช้การรับรองความถูกต้องอัตโนมัติต้องติดตั้งซอฟต์แวร์และเปิดใช้งาน การตั้งค่านี้ บนคอมพิวเตอร์แต่ละเครื่อง ผู้ใช้แต่ละคนต้องเปิดใช้งานการรับรองความถูกต้อง อัตโนมัติก่อนใช้งาน

**คำเตือน:** ไม่แนะนำให้ใช้การรับรองความถูกต้องอัตโนมัติถ้าคุณใช้คอมพิวเตอร์ของคุณร่วมกับผู้ใช้หลายคน ซึ่งผู้ใช้อื่นๆ สามารถดู ลับ หรือแก้ไขข้อมูลได้ เนื่องจากผู้ใช้สามารถเข้าถึงข้อมูลบนฮาร์ดไดรฟ์ได้เช่นเดียวกับฮาร์ดไดรฟ์มาตรฐานทั่วไป

- Limit for incorrect password attempts (จำกัดจำนวนครั้งของความพยายามใน การใส่รหัสผ่านไม่ถูกต้อง)  
ตั้งคาลักษณะการทำงานของอุปกรณ์เมื่อคุณใส่รหัสผ่านไม่ถูกต้อง



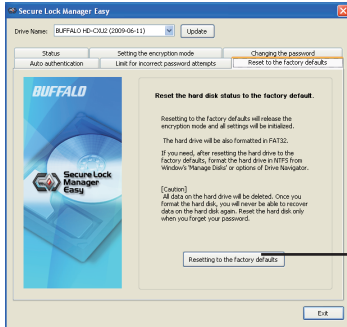
เลือกจำนวนครั้งของความพยายามในการใส่รหัสผ่านไม่ถูกต้อง ตั้งแต่ "3" "5" และ "10"

เลือกลักษณะการทำงานเมื่อใส่รหัสผ่านไม่ถูกต้อง ครบตามจำนวนครั้งที่จำกัด

นำการตั้งค่าไปใช้

ลักษณะการทำงานเมื่อใส่รหัสผ่านไม่ถูกต้องครบตามจำนวนครั้งที่จำกัด	
การออกจากหน้าจอการใส่รหัสผ่าน (ค่าเริ่มต้น)	หน้าจอการใส่รหัสผ่านจะปิด เมื่อต้องการรับรองความถูกต้องของ รหัสผ่าน คุณต้องเปิดหน้าจอการใส่รหัสผ่านอีกครั้ง
ไม่สามารถรับรองความถูกต้อง ในระหว่าง **	เลือกระยะเวลาเป้าหมายที่จะปฏิเสธความพยายามในการรับรอง ความถูกต้อง ตั้งแต่ [5 นาที] [10 นาที] [30 นาที] และ [1 ชั่วโมง] โดยจะไม่สามารถรับรองความถูกต้องไดจนกว่าจะครบกำหนดเวลา

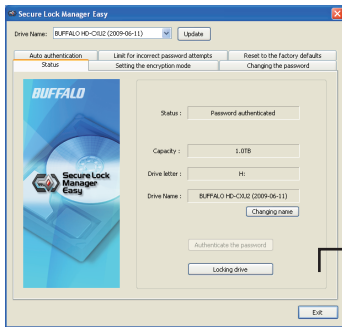
- Reset to factory defaults (การตั้งค่าใหม่ให้เป็นค่าเริ่มต้นจากโรงงาน) ลบการตั้งค่าของไดรฟ์และข้อมูลบนฮาร์ดไดรฟ์ แล้วตั้งค่าใหม่เป็นค่าเริ่มต้นจากโรงงาน



การตั้งค่าใหม่เป็นค่าเริ่มต้นจากโรงงาน  
ลบรหัสผ่านและข้อมูลทั้งหมดที่บันทึกไว้  
\* ฮาร์ดไดรฟ์จะถูกฟอร์แมตเป็น FAT32  
และโหมดการเข้ารหัสจะถูกปลดออก

## การออกจาก Secure Lock Manager Easy

เมื่อต้องการออกจาก Secure Lock Manager Easy ให้คลิก [Exit (ออก)] ที่ด้านล่างขวาของหน้าจอ



คลิก [Exit (ออก)]

## การถอนการติดตั้ง

คุณสามารถถอนการติดตั้ง Secure Lock Manager Easy ได้เมื่อคุณไม่ต้องการใช้โปรแกรมนี้อีกต่อไป เมื่อต้องการถอนการติดตั้ง ให้คลิก [เริ่ม] - [โปรแกรม (ทั้งหมด)] - [BUFFALO] - [Secure Lock Manager Easy] - [ถอนการติดตั้ง] จากนั้นทำตามคำแนะนำบนหน้าจอ



# دليل البدء السريع لبرنامج Secure Lock Manager Easy

يتضمن هذا المنتج برنامج التشفير [Secure Lock Manager Easy] المخصص لأجهزة التخزين، من إنتاج شركة Buffalo.

## حول برنامج Secure Lock Manager Easy

يتيح لك برنامج Secure Lock Manager Easy إمكانية تشفير جهاز تخزين Buffalo لديك، وحمايته باستخدام كلمة المرور. وتتوفر وظيفة المصادقة المتلقائية في البرنامج، علمًا بأن التشفير معطل افتراضيًا.

## قبل استخدام هذا البرنامج

يرجى قراءة الملاحظات التالية قبل استخدام برنامج Secure Lock Manager Easy.

- حافظ على أمان كلمة المرور.
- بدون كلمة المرور، لن تتمكن من الوصول إلى محرك القرص الثابت، أو تغيير الإعدادات. فإذا نسيت كلمة المرور، يجب عليك إعادة تعيين محرك الأقراص على افتراضيات المصنع.
- يتم دعم Windows 7/Vista/XP/2000/ Windows Server 2003/Server 2003 R2/Windows Server 2008/ Server 2008 R2.
- قائمة أنظمة التشغيل المتوافقة مخصصة لبرنامج Secure Lock Manager Easy فقط. ولكي تتعرف على أنظمة التشغيل التي يعمل معها المنتج الموجود لديك، راجع المستندات الخاصة به.
- لكي تستخدم برنامج Secure Lock Manager Easy على كمبيوتر Windows Server و Server 2003 R2، قم بالتسجيل باستخدام حساب المسؤول.

## التثبيت

يمكن تثبيت برنامج Secure Lock Manager Easy بواسطة معالج DriveNavigator. لإجراء التثبيت، اتبع الإجراء التالي.

١ قم بتوصيل محرك الأقراص بجهاز الكمبيوتر.

٢ انقر بزر الماوس الأيمن فوق [Utility\_HD-\*\*\*\*] (🗑️) في [جهاز الكمبيوتر]، ثم حدد [فتح].

(\*\*\*\* عبارة عن رقم الجزء لمحرك الأقراص DriveStation/MiniStation).

٣ انقر نقرًا مزدوجًا فوق [DriveNavi.exe] (🗑️).

سيتم بدء تشغيل معالج DriveNavigator.

\* إذا ظهرت لك الرسالة [يحتاج البرنامج إلى إذن للمتابعة] على نظام التشغيل Windows Vista، فانقر فوق [متابعة].

٤ انقر فوق [خيارات].

٥ انقر فوق [تثبيت برنامج Secure Lock Manager Easy].

اتبع التعليمات المعروضة على الشاشة لتثبيت البرنامج.

# بدء تشغيل برنامج Secure Lock Manager Easy

لبداء تشغيل برنامج Secure Lock Manager Easy.

١ قم بتوصيل محرك الأقراص بجهاز الكمبيوتر.

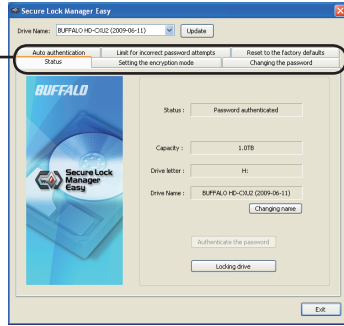
إذا تم عرض شاشة مصادقة كلمة المرور، فأدخل كلمة المرور.  
ملاحظة: إذا نسيت كلمة المرور وأعدت تعيين الوحدة على افتراضيات المصنع، فأغلق الشاشة.

٢ انقر فوق [ابدأ] - [كافة البرامج] - [BUFFALO] - [Secure Lock Manager Easy] - [Secure Lock Manager Easy].

## علامات تبويب برنامج Secure Lock Manager Easy

يتيح لك النقر فوق علامات التبويب الموجودة في برنامج Secure Lock Manager Easy إمكانية تكوين الإعدادات التالية.

انقر فوق العنصر الذي ترغب في تكوينه.



- Status (الحالة) (صفحة ٣)  
التحقق من حالة محرك الأقراص.
- Encryption mode (وضع التشفير) (صفحة ٣)  
تمكين/تعطيل التشفير.
- Password (كلمة المرور) (صفحة ٣)  
تغيير كلمة المرور.
- Auto authentication (المصادقة التلقائية) (صفحة ٤)  
إدخال كلمة المرور تلقائيًا عند توصيل محرك الأقراص بجهاز كمبيوتر.
- Limit for incorrect password attempts (الحد المسموح به لمحاولات إدخال كلمات مرور غير صحيحة) (صفحة ٤)  
ضبط سلوك الوحدة عند إدخال كلمة مرور خاطئة.
- Reset to factory defaults (إعادة التعيين على افتراضيات المصنع) (صفحة ٥)  
حذف جميع الإعدادات والبيانات الموجودة على محرك القرص الثابت، وإعادة التعيين على افتراضيات المصنع.

## • Status (الحالة)

تتيح علامة التنويب هذه التحقق من حالة محرك الأقراص.

عرض الحالة الحالية لمحرك الأقراص.

- قياسي
- لم تتم مصادقة كلمة المرور حتى الآن
- تمت مصادقة كلمة المرور

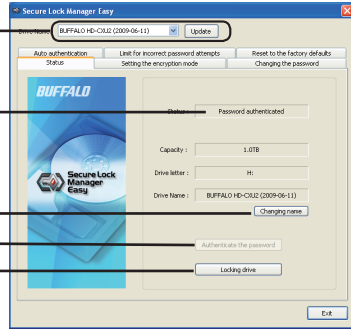
أدخل اسماً (٣٠ حرفاً أو أقل).

\* يتم عرض هذا الاسم من خلال برنامج Secure Lock Manager Easy فقط.

أدخل كلمة المرور لمصادقتها.

\* إذا تم تحرير وضع التشفير، فلن يعمل حتى لو قمت بالنقر فوقه.

قم بفتح محرك الأقراص. ستحتاج إلى إجراء المصادقة من جديد؛ للوصول إلى محرك الأقراص مرة أخرى.

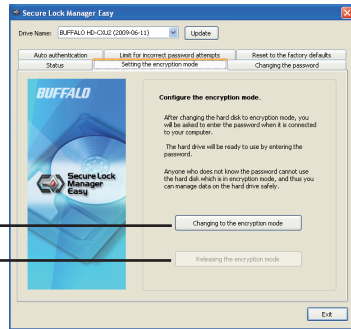


## • Encryption mode (وضع التشفير)

تتيح علامة التنويب هذه تمكين/تعطيل التشفير.

قم بتمكين التشفير. سبتعين عليك إدخال كلمة مرور للوصول إلى محرك الأقراص، أو إعداد المصادقة التلقائية.

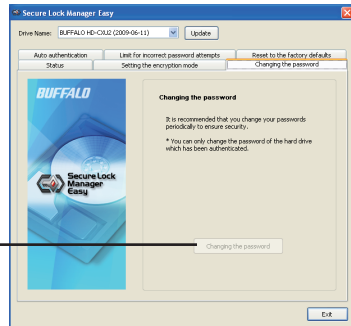
قم بتعطيل وضع التشفير. يستطيع أي شخص الوصول إلى محرك الأقراص دون إجراء مصادقة.



## • Password (كلمة المرور)

تتيح علامة التنويب هذه تغيير كلمة المرور.

تغيير كلمة المرور. لتغيير كلمة المرور، يجب تمكين التشفير، وإدخال كلمة المرور القديمة.

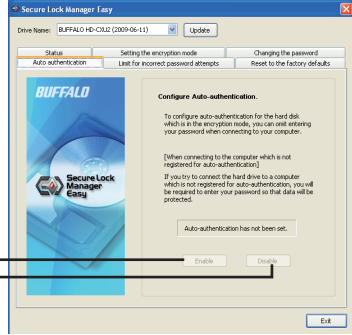


## • Auto authentication (المصادقة التلقائية)

تتيح علامة التويب هذه تعيين نمط إدخال كلمة مرور لمحرك الأقراص. ويمكن إدخال كلمة المرور تلقائياً (المصادقة التلقائية)، علماً بأنه يمكن استخدام هذه الإعداد لوحدة واحدة لكل جهاز كمبيوتر.

تمكين المصادقة التلقائية.

تعطيل المصادقة التلقائية.



**ملاحظة:** يحتاج كل جهاز كمبيوتر يستخدم المصادقة التلقائية إلى تثبيت البرنامج، وتمكين هذا الإعداد. ويحتاج كل مستخدم من

مجموعه مستخدمي مشتركين في جهاز كمبيوتر واحد إلى تمكين المصادقة التلقائية لاستخدامها.

**تحذير:** لا يوصى باستخدام المصادقة التلقائية، إذا كنت تشارك جهاز الكمبيوتر مع عدة مستخدمين. ويعزى ذلك إلى إمكانية الوصول

إلى البيانات الموجودة على محرك القرص الثابت، مثله في ذلك مثل محركات الأقراص الثابتة القياسية؛ ومن ثم قد يقوم

مستخدمون آخرون بعرض البيانات، أو حذفها، أو تحريرها.

## • Limiting incorrect password attempts (الحد المسموح به لمحاولات إدخال كلمات

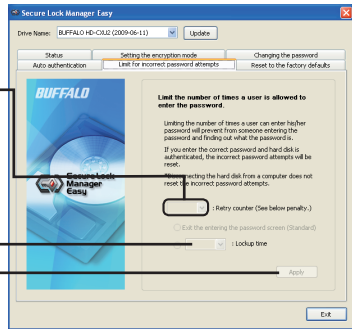
مرور غير صحيحة)

تتيح علامة التويب هذه ضبط سلوك الوحدة عند إدخال كلمة مرور خاطئة.

حدد عدد محاولات إدخال كلمات مرور غير صحيحة  
من بين [٣]، و[٥]، و[١٠].

حدد السلوك المتبع عند بلوغ الحد المسموح به  
لمحاولات إدخال كلمات مرور غير صحيحة.

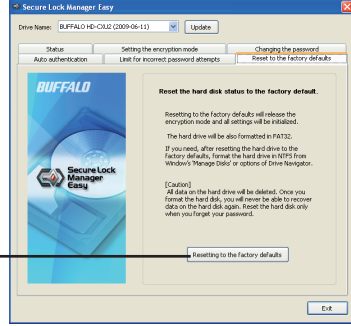
قم بتطبيق الإعداد.



السلوك المتبع عند بلوغ الحد المسموح به لمحاولات إدخال كلمات مرور غير صحيحة	الخروج من شاشة إدخال كلمة المرور (القيمة الافتراضية)
سيتم إغلاق شاشة إدخال كلمة المرور. ولمصادقة كلمة المرور، تحتاج إلى فتح الشاشة لإدخال كلمة المرور مرة أخرى.	
حدد المدة الزمنية المستهدفة من بين [٥ دقائق]، و[١٠ دقائق]، و[٣٠ دقيقة]، و[ساعة]، والتي سترفض خلالها محاولات المصادقة. ويتعذر إجراء المصادقة حتى انقضاء المدة الزمنية المحددة.	تعذرت المصادقة أثناء **

## • Resetting to the factory defaults (إعادة التعيين على افتراضيات المصنع)

تتيح علامة التويب هذه حذف جميع إعدادات محرك الأقراص، والبيانات الموجودة على محرك القرص الثابت، ثم إعادة تعيين الوحدة على افتراضيات المصنع.

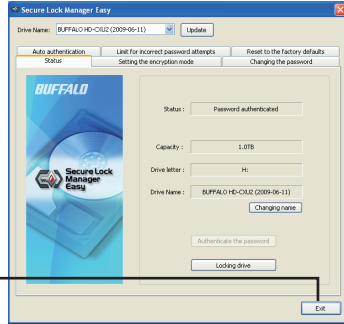


إعادة التعيين على افتراضيات المصنع وحذف كلمة المرور وجمع البيانات المحفوظة.

\* محرك القرص الثابت مهيأ بتنسيق FAT32؛ ولذا سيتم تحرير وضع التشفير.

## إنهاء برنامج Secure Lock Manager Easy

لإنهاء برنامج Secure Lock Manager Easy، انقر فوق [Exit] (إنهاء) على الجانب الأيمن للجزء السفلي من الشاشة.



انقر فوق [Exit] (إنهاء).

## لإزالة التثبيت

يمكنك إزالة تثبيت برنامج Secure Lock Manager Easy عند عدم الحاجة إليه. لإزالة تثبيت البرنامج، انقر فوق [إبدأ] - [كافة] البرامج - [Secure Lock Manager Easy] - [BUFFALO] - [إزالة التثبيت]. ثم اتبع التعليمات المعروضة على الشاشة.