# Installation und Konfiguration des Netzwerkhardlocks

# Inhalt

Systemvoraussetzungen	. 1
Unterstützte Betriebssysteme	. 1
Benötigte Hardware-Schnittstellen	. 1
Virtualisierung des Hardlock-Servers	. 2
Installation und Konfiguration	. 2
Grundsätzliches Vorgehen	. 2
Herunterladen der benötigten Software	. 2
Installation des Hardlocktreibers	. 3
Installation des Aladdin Monitor	. 4
Installation des Hardlock-Server-Dienstes	. 5
Registrierung des Hardlocks beim Hardlock-Server-Dienst	. 9
Konfiguration der Firewall	. 9
VPN-Betrieb und beschleunigte Hardlock-Suche	12

# Systemvoraussetzungen

## Unterstützte Betriebssysteme

Der Hardlock kann prinzipiell auf allen aktuellen Windows-Betriebssystemen betrieben werden, wobei es keine Rolle spielt, ob es sich um ein Server- oder Client-Betriebssystem handelt. Die Mindestvoraussetzungen sind wie folgt:

- Client-Systeme: Windows 7 SP1 oder neuer
- Server-Systeme: Windows Server 2008 oder neuer

#### Benötigte Hardware-Schnittstellen

Als Hardlock werden ausschließlich USB-Dongles verwendet. Der gewünschte Rechner muss also über eine USB-Schnittstelle verfügen.

Alternativ kann der Hardlock auch an einem sogenannten "USB Device Server", der USB-Geräte transparent über das Netzwerk bereitstellen kann, betrieben werden.

Die physikalischen Abmessungen des Dongles selbst sind wie folgt:

- Die bis 2014 ausgelieferte Version (oberes Bild):
   Länge: 5 cm, Breite: 1,5 cm Höhe: 0,8 cm
- Die aktuell ausgelieferte Version (unteres Bild): Länge: 4 cm, Breite: 1,6 cm Höhe: 0,8 cm



## Virtualisierung des Hardlock-Servers

Falls der Hardlock-Server-Dienst in einer virtuellen Maschine betrieben werden soll, gibt es zwei Möglichkeiten zur Umsetzung:

- Die Virtualisierungssoftware unterstützt das Durchreichen von USB-Ports an die virtuelle Maschine (z.B. Oracle VM VirtualBox oder VMware Workstation, nicht jedoch z.B. Microsoft Hyper-V)
- Verwendung eines USB Device Server, an den man den Dongle ansteckt und sich dann mit einer mitgelieferten Software damit verbindet, als würde er lokal am Rechner stecken.

Ansonsten gelten dieselben Voraussetzungen wie für einen physikalischen Rechner.

# Installation und Konfiguration

#### Grundsätzliches Vorgehen

Die folgenden Schritte sind für die Installation und Konfiguration des Netzwerkhardlocks erforderlich:

- Herunterladen der benötigten Software
- Installation des Hardlocktreibers
- Installation des Aladdin Monitor
- Installation des Hardlock-Server-Dienstes
- Registrierung des Hardlocks beim Hardlock-Server-Dienst
- Konfiguration der Firewall (falls vorhanden)
- Einstellungen für den VPN-Betrieb (falls benötigt)

#### Herunterladen der benötigten Software

Auf unserer Homepage unter <u>https://www.rehm.de/downloads</u> steht Ihnen die benötigte Software zum Download zur Verfügung. Hier laden Sie sich die gelb markierten Dateien "Aladdin Hardlocktreiber (Kommandozeilenversion)" ("haspdinst.exe") und "Aladdin Monitor" ("aksmon32\_setup.exe") herunter:

	Fernwartung (TeamViewer) Programm zur Durchführung einer Fernwartungssitzung (TeamViewer)
	EXE-Datei , 23 MB
	Online-Präsentation (TeamViewer) Programm zur Durchführung einer Online-Vorführung (TeamViewer)
	EXE-Datei , 15 MB
	Komplett-Paket für die Installation unserer Programme Enthält sämtliche benötigte Software und Treiber für den Betrieb der Rehm-Programme. Ihre lizenzierten Programme werden während der Installation nach Eingabe Ihrer Zugangsdaten direkt von unserem Server heruntergeladen. Bitte verwenden Sie diese Datei für die Installation unserer Software auf einem neuen Rechner.
	EXE-Datei , 108 MB
	Software-Installationsanleitung Ausführliche Beschreibung des Vorgehens zur Installation unserer Software auf Ihrem PC
	PDF-Datei , 616 KB
	Netzwerkhardlock-Installationsanleitung Ausführliche Beschreibung des Vorgehens zur Installation des Netzwerkhardlocks auf Ihrem Server, sowie des Zugriffs von den Arbeitsplätzen
	PDF-Datei , 859 KB
۵	Aladdin Hardlocktreiber (Kommandozeilenversion) Aktueller Hardlocktreiber für Einzelplatz- und Netzwerkhardlocks (Kommandozeilenversion). Wichtig: Installation mit den Parametern "/i /ld"
	EXE-Datei , 25 MB
	Aladdin Monitor Netzwerkhardlock-Verwaltungswerkzeug für die Einrichtung des Netzwerkhardlocks, sowie die Anzeige und Freigabe aktiver Lizenzen
	EXE-Datei , 2 MB
	Microsoft Access Database Engine 2010 x64 64-Bit-Datenbanktreiber (benötigt für FLUSS-2D, GraPS und HYKAS)
	Programm zur Verwaltung einer vorhandenen Rehm-Installation sowie Ihrer Lizenzen auf Ihrem PC. Für eine Neuinstallation verwenden Sie bitte das "Komplett-Paket für die Installation unserer Programme" weiter oben.
-	

# Installation des Hardlocktreibers

Öffnen Sie eine Kommandozeile, wechseln Sie in den Download-Ordner und starten Sie die Datei "haspdinst.exe" mit den Parametern "/i /ld" auf dem Server und warten Sie, bis die Installation abgeschlossen ist:





Nach der Installation und dem Anstecken des Hardlocks sollte hinten am USB-Hardlock eine rote LED leuchten. Ist dies der Fall, war die Installation des Hardlocks erfolgreich.

#### Installation des Aladdin Monitor

Die Hardlockverwaltung erfolgt über ein Programm namens "Aladdin Monitor". Starten Sie das Programm "aksmon32\_setup.exe". Beachten Sie, dass dieses Setup sowohl auf 32-Bit- als auch auf 64-Bit-Betriebssystemen verwendet wird.

🕑 Will	lkommen X	Ø	Lizenz-Vereinbarung	x
₩ Wire supplied Wire supplied Wir	Allkommen im Installationsprogramm für Aladdin fonitor 1.4.2. Disess Programm installiert Aladdin fonitor 1.4.2. auf Ihrem Computer. en nachdrücklich, vor Ausführen disess programms alle Windows-Programme zu beenden. en klicken, um die Installation zu beenden und alle togramme zu schließen. Auf Weiter klicken, um mit tionsprogramm beginnen. i: Dieses Programm ist unheberrechtlich sowie ationale Verträge geschützt. sige Vervielfältigung oder Verbreitung dieses ob ganz oder auszugsweise, kann schwere zivil- hliche Konsequerzen nach sich ziehen und wird Ausschöpfung der Rechtsmittel geahndet.		ALADDIN KNOWLEDGE SYSTEMS LTD. Aladdim Monitor LICENSE AGREEMENT IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE DOWNLDADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF THE Aladdim Monitor including any retvisions, controctions, modifications, enhancements, updates and/or upgrades thereto (hereinater Gottware] SUPPLIE BY ALADDIN KNOWLEDGE SYSTEMS LTD. or any of its affiliates (either of them referred to as JALADDINI)ARE AND SHALL BE, SUBJECT TO THE TERMS AND CONDITIONS SET FORTH IN THIS AGREEMENT. BY DOWNLOADING THE SOFTWARE (as defined hereunder)AND/OR BY INSTALLING THE SOFTWARE (b) AGREEING TO BE BOUND BY ITS TERMS AND CONDITIONS.	<
	Weiter> Abbrechen		< <u>Z</u> urück <u>W</u> eiter> Abbreche	n



Nach erfolgreicher Installation finden Sie im Startmenü unter "Alle Programme / Aladdin / Monitor" eine neue Verknüpfung namens "AKS Monitor":



## Installation des Hardlock-Server-Dienstes

Starten Sie den eben installierten AKS Monitor **mit Administratorrechten**. Falls Sie möchten, können Sie die Sprache von Englisch auf Deutsch umstellen. Dazu gehen Sie auf "File / Settings" und stellen unter "Language" von "English" auf "German". Nach einem entsprechenden Hinweis können Sie den AKS Monitor schließen und neu starten.



Im Normalfall sollte unter "HL-Server" noch kein Eintrag sichtbar sein. Falls doch, dann ist in Ihrem Netzwerk offensichtlich schon ein anderer Aladdin-Hardlock-Server vorhanden. Diesen können sie ggf. einfach ignorieren.

Wählen Sie unter "Dienste" den Punkt "HL-Server-Dienst installieren":



Sie erhalten eine Bestätigungsmeldung erhalten:

Aladdin Monitor
Der Hardlock-Dienst wurde auf dem lokalen Rechner installiert. ACHTUNG: Die Datei HLS32SVC.EXE wurde in Ihr Systemverzeichis kopiert und wird in Zukunft von dort gestartet. Um den Server zu starten, wählen Sie "HL- Server-Dienst starten" aus dem Dienste-Menu. Kopieren Sie Lizenzdateien (*.ALF) in das Systemverzeichnis oder benutzen Sie die Environment-Variable HL_LICENSEDIR.
ОК

Interessant für uns ist nur der erste Satz, der besagt, dass der Dienst erfolgreich installiert wurde. Der Rest der Meldung, der die Lizenzdateien betrifft, ist für uns nicht relevant.

Schließen Sie die Meldung mit "Ok". Wählen Sie dann wiederum unter "Dienste" den Punkt "HL-Server-Dienst starten":

	Dienste	Ansicht	Hilf	e
	Hardlock		×	HL-Server-Dienst starten
ľ	HA	SP	►	HL-Server-Dienst anhalten

Nach dem Start sollte unter dem Eintrag "HL-Server" in der Baumnavigation jetzt Ihr Servername mit dem Zusatz "(Lokal)" erscheinen:



Zum Abschluss der Dienstinstallation sollten Sie noch prüfen, ob der Hardlock-Server-Dienst für den automatischen Start konfiguriert ist. Dazu öffnen Sie "Dienste" unter "Systemsteuerung / Verwaltung". Dort sollte jetzt ein Eintrag "HL-Server" zu finden sein:

🎑 Gruppenrichtlinienclient	Von dem Dien	Wird au	Automatisch (Start durch Au	Lokales System
🍓 Hilfsprogramm für spezielle	Ermöglicht Ad		Manuell	Lokales System
🔍 HL-Server		Wird au	Automatisch	Lokales System
🌼 Hyper-V-Datenaustauschdi	Stellt einen M		Manuell (Start durch Auslöser)	Lokales System
鵒 Hyper-V-Dienst für Zeitsync	Synchronisiert		Manuell (Start durch Auslöser)	Lokaler Dienst

Sollte hier unter "Starttyp" nicht "Automatisch" (bzw. im Falle eines virtuellen Servers mit Hardlock an einem USB Device Server "Automatisch (Verzögerter Start)") stehen, klicken Sie mit der rechten Maustaste auf den Eintrag "HL-Server" und wählen Sie "Eigenschaften":

🧠 Hilfsprogramm für spezielle.	Ermöglicht Ad
🔅 HL-Server	Starten
🔍 Hyper-V-Datenaustauschc	Beenden
🧠 Hyper-V-Dienst für Zeitsyr	beenden
🥋 Hyper-V-Dienst zum Heru	Anhalten
鵒 Hyper-V-Remotedesktopv	Fortsetzen
🔍 Hyper-V-Taktdienst	Neu starten
🔍 Hyper-V-Volumeschatten	Alle Aufgaben
🔍 IKE- und AuthlP IPsec-Sch	, inc , largabert
鵒 Infrastrukturdienst für Hin	Aktualisieren
🎑 Integritätsschlüssel- und Z	Eigenschaften
🎑 Intelligenter Hintergrundü	Hilfe
🔍 IP-Hilfsdienst	rime

Ändern Sie den "Starttyp" auf "Automatisch" (bzw. im Falle eines virtuellen Servers mit Hardlock an einem USB Device Server "Automatisch (Verzögerter Start)") und bestätigen Sie mit "Ok":

Pfad zur EXE-Datei: C:\Windows\system32\HLS32SVC.EXE					
Starttyp:	Automatisch	~			
	Automatisch (Verzögerter Start)				
Unterstützung bein	Automatisch Manuell				
Dienststatus:	Deaktiviert vvira ausgerunn				

#### Registrierung des Hardlocks beim Hardlock-Server-Dienst

Um Ihren Rehm-Hardlock beim Hardlock-Server-Dienst anzumelden, wählen Sie Ihren lokalen Server unter "HL-Server" aus:

8		Aladdin Monitor	_ 🗆 X
Datei Dienste Ansicht Hilfe			A
\$   <b>\$ \$</b>   <b>\$</b> \$			Aladdin
Aladdin Netzwerk			
HL-Server	Hardlock Se	ver	
HASP License Manager	Name	WIN2012-HS	
	Version	4.60	□ <u>I</u> PX
	IP	192.168.2.21	✓ NetBIOS
	IPX		
	OS/Treiberversion	n WIN32 / DRV 3.83 / API 3.88 / HLVDD.DLL 2.21	
	Moduladresse	Max. Logins Aktuell Spitzenwert	
	<u>M</u> oduladresse	29809 <u>H</u> inzufügen	<u>E</u> ntfernen
	Statistiken —		
	TOD ND	Empfangen Gesendet Fehler	
	NetBIOS		
	1		NUM

Stellen Sie sicher, dass der Hardlock am Rechner angesteckt bzw. der Rechner mit dem Hardlock am USB Device Server verbunden ist und die LED am Hardlock rot leuchtet. Tragen Sie unter "Moduladresse" den Wert "23645" ein und klicken Sie auf "Hinzufügen". Ein Eintrag in der Tabelle sollte erscheinen:

Moduladresse	Max. Logins	Aktuell	Spitzenwert	
23645	250	0	0	
1				
<u>M</u> oduladresse	23645 📑	(Hinzufügen)	<u>E</u> ntfern	ien

Der Hardlock ist jetzt betriebsbereit.

#### Konfiguration der Firewall

Falls Sie auf dem Rechner, auf dem der HL-Server-Dienst läuft, eine Firewall betreiben, so muss diese noch so konfiguriert werden, dass Client-Anfragen auch zum HL-Server-Dienst gelangen. Je nach Firewall-Produkt ist die Konfiguration unterschiedlich, das Vorgehen wird hier am Beispiel der Windows-Firewall auf einem Windows Server 2012 demonstriert, sollte bei anderen Produkten aber ähnlich vonstattengehen.

Starten Sie "Windows-Firewall mit erweiterter Sicherheit" und wechseln Sie zu "Eingehende Regeln":

		Windows-Firewall mit erweiterter Sicherheit							
D	atei Aktion Ansicht ?								
4	• 🔿 🙍 🖬 🗟 🔽								
	Windows-Firewall mit erweitert	Eingehende Regeln					A	ktionen	
	Eingehende Regeln	Name	Gruppe 📩	Profil	Aktiviert	Aktion ^	E	ingehende Regeln	•
	Kasgehende Regeln	Sentinel License Manager		Alle	Ja	Zulassen	ulassen 🔐 Neue Regel	Neue Regel	
	Verbindungssicherneitsrege	Anmeldedienst (NP eingehend)	Anmeldedienst	Alle	Nein	Zulassen			
۲ V	o dei wachung	Ø Autorisierung f ür den Anmeldedienst (RP	Anmeldedienst	Alle	Nein	Zulassen	י	Nach Profil filtern	'
		BranchCache - Gehosteter Cacheserver (	BranchCache - Gehosteter C	Alle	Nein	7ulassen	2	Nach Status filtern	<u> </u>

Klicken Sie auf "Neue Regel". Als "Regeltyp" wählen Sie "Port" und klicken Sie auf "Weiter":

<i></i>	Assistent für neue eingehende Regel								
Regeltyp Wählen Sie den Typ der zu erstellenden Firewallregel aus.									
Schritte: Regeltyp Protokolle und Ports Aktion Profil Name	Welchen Regeltyp möchten Sie erstellen?         Programm         Regel, die die Verbindungen für ein Programm steuert.         Port         Regel, die die Verbindungen für einen TCP- oder UDP-Port steuert.         Vordefiniert:         Anmeldedienst         Regel, die die Verbindungen für einen Windows-Vorgang steuert.         Benutzerdefiniert         Benutzerdefiniert Regel								
	< Zurück Weiter > Abbrechen								

Wählen Sie "UDP" und "Bestimmte lokale Ports", dort tragen Sie "3047" ein und klicken auf "Weiter":



Wählen Sie "Verbindung zulassen" und klicken Sie auf "Weiter":



Wählen Sie das für Ihre Konfiguration passende Firewall-Profil. Im Zweifel lassen Sie einfach alle drei Häkchen aktiviert:



Geben Sie einen passenden Namen und optional eine Beschreibung ein und klicken Sie auf "Weiter":

Name:	
Aladdin HL-Server-Dienst	
Beschreibung (optional):	
Aladdin Hardlock-Server-Dienst, der den Hardlock für die Rehm-Programme über das Netzwerk zur Verfügung stellt.	

Die neue Regel sollte jetzt in der Tabelle der eingehenden Regeln zu sehen sein:

t	Eingehende Regeln							
Ш	Name	Gruppe 📩	Profil	Aktiviert	Aktion			
	Aladdin HL-Server-Dienst		Alle	Ja	Zulassen			
e	Sentinel License Manager		Δlle	la	Zulassen			

## VPN-Betrieb und beschleunigte Hardlock-Suche

Der Betrieb unserer Programme in VPN-Umgebungen, beispielsweise für die Arbeit aus dem Home-Office, wird immer häufiger umgesetzt. Für solche Umgebungen muss in der Regel durch eine zusätzliche Einstellung dem Hardlocktreiber mitgeteilt werden, auf welchem Server sich der Hardlock befindet. Diese Einstellung wird über eine System-Umgebungsvariable gesteuert.

Auch in Umgebungen, in denen kein VPN-Betrieb berücksichtigt werden muss, kann diese Einstellung die Kommunikation mit dem Hardlock-Server stabilisieren und beschleunigen.

Öffnen Sie dazu am Client in der Systemsteuerung den Eintrag "System" und klicken Sie auf "Erweiterte Systemeinstellungen":

	System – 🗆			
( → ↑ I → Systemsteue	rung → System und Sicherheit	▶ System	✓ ♂ Systemsteuerung durchsuchen 𝒫	
Datei Bearbeiten Ansicht Extras	?		🔲 👗 🔓 📋 🗙 🖌 🖃 谷	
Startseite der Systemsteuerung	Basisinformationen übe	r den Computer anzeigen	0	
🛞 Geräte-Manager	Windows-Edition			
🌍 Remoteeinstellungen	Windows 8.1 Enterprise			
😌 Computerschutz	© 2013 Microsoft Corporati	on. Alle Rechte vorbehalten.		
🛞 Erweiterte Systemeinstellungen				
System				
	Prozessor:	Intel(R) Core(TM) i7 CPU 870 @ 2.93GHz 2.93 GHz	z	
	Installierter Arbeitsspeicher (RAM):	16,0 GB		
	Systemtyp:	64-Bit-Betriebssystem, x64-basierter Prozessor		
	Stift- und Toucheingabe:	Für diesen Bildschirm ist keine Stift- oder Toucheingabe	e verfügbar.	
	Einstellungen für Computernan	nen, Domäne und Arbeitsgruppe		

Hier klicken Sie auf "Umgebungsvariablen":

12

Systemeigenschaften					
Computername	Hardware	Erweitert	Computerschutz	Remote	
Sie müssen als durchführen z	s Administrat u können.	or angemel	det sein, um diese	Änderungen	
Visuelle Effel Speicher	cte, Prozess	orzeitplanur	ng, Speichemutzun	ig und virtueller	
				Einstellungen	
Benutzerprof	le				
Desktopeins	tellungen be	züglich der	Anmeldung		
				Einstellungen	
Starten und	Niederherste	ellen			
Systemstart,	Systemfehle	r und Debu	ginformationen		
				Einstellungen	
			Umg	ebungsvariablen	
		C	)K Abbree	<b>chen</b> Überneh	men

Klicken Sie unter "Systemvariablen" auf "Neu":

omputername	Hardware	Erweitert	Computerschutz	Remote			
		maebun	asvariablen		×		
Ungebungsvariablen							
Benutzerva	Benutzervariahlen für Schneider						
Variable		Wort					
				0			
MOZ_PLU	JGIN_P	C: Program	Files (X86) (Foxit Si EILE %\AppData\L	ottware (			
TMP		%USERPROFILE% (AppData (Local \Temp					
			, rec to the bear of the	ocar (remp			
		Neu	Bearbeiten	Löscher	n		
Systemvari	ablen						
Systemvari Variable	ablen	Wert			^		
Systemvari Variable CM2013D	ablen DIR	Wert C:\Program	Files (x86)\Commo	n Files\A	^		
Systemvari Variable CM2013D ComSpec	ablen DIR	Wert C:\Program C:\WINDOW	Files (x86)\Commo /S\system32\cmd.4	n Files\A	^		
Systemvari Variable CM2013D ComSpec FP_NO_H	DIR HOST_C	Wert C:\Program C:\WINDOW NO	Files (x86)\Commo /S\system32\cmd.{	n Files\A exe	^		
Systemvari Variable CM2013D ComSpec FP_NO_H ILBDIR	ablen DIR HOST_C	Wert C:\Program C:\WINDOW NO C:\Program	Files (x86)\Commo /S\system32\cmd.( Files (x86)\Commo	n Files\A exe n Files\A	<b>^</b>		
Systemvari Variable CM2013D ComSpec FP_NO_H ILBDIR	ablen DIR HOST_C I	Wert C:\Program C:\WINDOW NO C:\Program	Files (x86)\Commo /S\system32\cmd.« Files (x86)\Commo Bearbeiten	n Files \A exe n Files \A	^		
Systemvari Variable CM2013D ComSpec FP_NO_H ILBDIR	ablen DIR HOST_C	Wert C:\Program C:\WINDOW NO C:\Program Neu	Files (x86)\Commo /S\system32\cmd.e Files (x86)\Commo Bearbeiten	n Files\A exe n Files\A Löscher	^ ~		

Fügen Sie eine Variable mit dem Namen "HLS\_IPADDR" ein. Als Wert tragen Sie die IP-Adresse des Rechners ein, auf dem der HL-Server-Dienst läuft (hier z.B. "192.168.2.21") ein. Alternativ können Sie auch den Rechnernamen angeben (z.B. "APPSERVER-BUERO").

Neue Systemvariable					
Name der Variablen: Wert der Variablen:	HLS_IPADDR				
	OK Abbrechen				

Die neue Variable sollte jetzt in der Tabelle "Systemvariablen" sichtbar sein:

Systemvariablen		
Variable	Wert	^
FP_NO_HOST_CHECK	NO	
HLS_IPADDR	192.168.2.21	
NUMBER_OF_PROCESSORS	12	

Bestätigen Sie mit "Ok". Der Client sucht den Hardlock ab sofort nur noch am eben eingestellten Server, falls kein lokaler Hardlock gefunden wird.

Dieser Vorgang muss selbstverständlich auf jedem Client, der den Netzwerkhardlock ansprechen soll, durchgeführt werden.