

rmDATA Schutzsystem

Sentinel HASP

Copyright rmDATA, 2021

Alle Rechte vorbehalten



rmDATA GmbH (Österreich)
Industriestraße 6
7423 Pinkafeld
Tel: +43 3357 43333

rmDATA GmbH (Deutschland)
Merzbrück 212
52146 Würselen
Tel: +49 2405 4066917

rmDATA AG (Schweiz)
Tägerhardring 8
5436 Würenlos
Tel: +41 41 51121 31

office@rmdatagroup.com www.rmdatagroup.com

Inhaltsverzeichnis

Einleitung	4
Voraussetzungen	4
Änderungen zum bisherigen Schutzsystem	4
Erstinstallation einer neuen Lizenz	6
Erstinstallation eines Softlock	6
Erstinstallation von lokalen Hardlock (Dongle)	7
Erstinstallation von Netzwerklizenzen	8
Manuelle Installation des HASP Treibers	9
Ändern von Lizenzen	10
Ändern eines lokalen Soft- oder Hardlock	10
Ändern eines Netzwerk Hardlock	10
Deaktivieren eines Softlock	10
Der rmDATA Lizenzmanager (RUS)	12
Softlock-Erstinstallation mit c2v-Datei	12
Lizenzupdate mit c2v-Datei	13
v2c-Datei einlesen	16
Transfer License	18
Das Admin Control Center (ACC)	19
Konfiguration des Lizenzservers	20
Verwendeter Port / Firewall Konfigurationen	20
Zugriff von Clients auf den Lizenzserver erlauben	21
Zugriff von Clients auf das Admin Control Center erlauben	22
Auffinden des Lizenzservers	22
Klarnamen für products und features	23
ACC Einstellungen auf andere Rechner verteilen	24

Einleitung

rmDATA Produkte benötigen für ihren Einsatz eine gültige Lizenz. Beim HASP Schutzsystem haben Sie die Wahl zwischen folgenden Lösungen:

- **Lokaler Softlock:** Die Lizenz wird direkt für Ihren Rechner ausgestellt und auf Ihrem Rechner gespeichert. Sie kann vom Anwender nicht auf andere Rechner übertragen werden.
- **Lokaler Hardlock:** Die Lizenz befindet sich auf einem Dongle, den Sie an der USB-Schnittstelle Ihres Rechners anstecken. Sie können den Dongle jederzeit umstecken, und die Lizenz so abwechselnd auf verschiedenen Rechnern einsetzen.
- **Netzwerk Hardlock:** Die Lizenzen befinden sich auf einem Dongle, der an einem beliebigen Rechner (meist einem Server) angeschlossen wird. Alle Rechner im Netzwerk können die Lizenzen abwechselnd nutzen.

Diese Lizenzen können auch frei kombiniert werden.

Im Folgenden finden Sie die Anleitung, wie Sie Lizenzen auf Ihrem Rechner aktivieren und verwalten.

Voraussetzungen

Produktversionen:

Das HASP Schutzsystem wurde in allen rmDATA Produktversionen ab dem Jahr 2012 integriert

Ab 2016 wird nur noch das HASP Schutzsystem unterstützt, der Betrieb mit dem alten Schutzsystem (Sentinel SuperPro) ist seitdem nicht mehr möglich.

Netzwerk:

Beim Netzwerkschutz läuft die Kommunikation zwischen Client und Server(n) über den TCP bzw. UDP Port 1947. Dieser darf daher von Firewalls bzw. Proxy-Servern nicht blockiert werden, und er darf auch nicht von anderen Anwendungen belegt sein.

USB-Dongle:

Der Dongle muss an eine USB-Schnittstelle des jeweiligen Rechners (Lokaler Dongle am Einzelplatzrechner, bzw. Serverdongle am Lizenzserver) angesteckt werden.

Bei virtuellen Rechnern muss für den Zugriff auf einen USB-Dongle die USB-Schnittstelle vom Hostrechner oder einem USB-Device-Server an die VM weitergereicht werden.

Fernzugriff über RDP / Terminal Server:

Wenn rmDATA Produkte auf einem fernen Rechner über RDP ausgeführt werden sollen (zB Terminal Server, Citrix, Remote Desktop) ist dafür eine spezielle Netzwerklizenz erforderlich – bitte wenden Sie sich dafür an rmDATA.

Änderungen zum bisherigen Schutzsystem

Das neue Schutzsystem auf Basis Sentinel HASP ist leistungsfähiger und gleichzeitig komfortabler als das bisher bei rmDATA verwendete System auf Basis von Sentinel SuperPro:

- Es werden keine Lizenzdateien (rm2.ini, rm2.1, ..., rmLock.ini, rm2f.000) mehr verwendet. Die Lizenzinformationen sind vollständig im Hard- bzw. der Softlock im Rechner gespeichert.

Anmerkungen:

- o Bei der Installation von rmDATA-Programmen über den alten Installationsassistenten (IASist.exe) wird auch keine Lizenzdatei mehr installiert. Die Lizenzverwaltung dort betrifft nur das alte Schutzsystem!
- o Beim Umstieg vom alten Schutzsystem müssen die alten Lizenzdateien vom Rechner gelöscht werden, da es zu starken Performance Einbußen kommen kann, wenn der zugehörige alte Dongle bzw. Lizenzserver nicht mehr in Betrieb ist.
- Die Umgebungsvariable RMD-USER wird nicht mehr verwendet.
- Für Einzelplatzlizenzen kommen nun oft auch Softlocks zum Einsatz, ohne einen Dongle (ähnlich zB den von Autodesk bekannten Lizenzen)
- Auf Wunsch kann aber auch weiterhin ein Hardlock (mit einem Dongle) verwendet werden, z.B. wenn die Lizenz abwechselnd auf verschiedenen Rechnern verwendet werden soll.
- Mehrere Dongles können nun zugleich an einem Rechner angesteckt werden. Es stehen dann alle Lizenzen der Dongles auf dem Rechner gemeinsam zur Verfügung.
- Der Dongle Treiber wird über die Windows Updates automatisch installiert.
- Für Netzwerklizenzen ist kein laufendes Programm (rmSrvLck.exe) mehr notwendig. Die Funktionalität ist vollständig in den Dongle Treiber integriert, die Konfiguration erfolgt über den Webbrowser.

Beim Umstieg vom alten Schutzsystem sollte rmSrvLck deaktiviert, und vom Rechner gelöscht werden.

- Netzwerklizenzen müssen im Allgemeinen nicht konfiguriert werden, weder am Server noch am Client.
Sobald der Netzwerk-Dongle an einem beliebigen Rechner angesteckt ist, können die darauf enthaltenen Lizenzen sofort auf allen Rechnern im lokalen Netzwerk (LAN) verwendet werden.
- Es wird nur noch ein einziger Port für die Kommunikation zwischen Client und Server verwendet. ICMP Echo Pakete (Ping) werden nicht mehr benutzt.
- Der Lizenzstatus (wer verwendet welche Lizenz) kann von jedem Arbeitsplatz-Rechner aus abgefragt werden, sofern der Administrator dies erlaubt hat
(siehe Kapitel „Zugriff von Clients auf das Admin Control Center erlauben“)

Erstinstallation einer neuen Lizenz

Erstinstallation eines Softlock

Die benötigten Treiber und Hilfsprogramme werden mit dem Setup des jeweiligen rmDATA-Programmes automatisch mitinstalliert.

Die Softlock-Lizenz muss nur noch aktiviert werden:

1. Generieren Sie eine c2v-Datei mit der ein neuer Softlock Key angelegt wird, und senden Sie diese Datei an rmDATA
Siehe Kapitel „Softlock-Erstinstallation mit c2v-Datei“
2. Sie erhalten von rmDATA eine v2c-Datei mit der Freischaltung retour. Lesen Sie diese ein, dadurch wird ein neuer SL-Key angelegt.
Siehe Kapitel „v2c-Datei einlesen“

Die rmDATA Produkte sind damit bereit für den Einsatz.

Hinweise:

- Sie können den Softlock nur auf diesem Rechner nutzen.
Die Übertragung auf andere Rechner durch den Anwender ist nicht möglich!
- Auf demselben Rechner können auch zusätzlich ein oder mehrere Hardlocks (Dongles) angesteckt werden.
Es werden dann alle Lizenzen gemeinsam verwendet
- Eine im Netzwerk vorhandene Netzwerklizenz wird automatisch mitverwendet, wenn ein Programm aufgerufen wird, das durch die lokale Lizenz nicht freigeschalten ist.
- Einzelplatzlizenzen (egal ob Soft- oder Hardlock) können nicht auf Terminalservern oder über Remote Desktop betrieben werden!
Dazu ist eine spezielle Netzwerklizenz erforderlich.

Erstinstallation von lokalen Hardlock (Dongle)

Sie erhalten Sie von rmDATA einen grünen Dongle:



HASP Einzelplatz-Dongle

1. Stecken Sie den Dongle an einer USB-Schnittstelle Ihres Rechners an.
2. Die benötigten Treiber werden mit dem Setup des jeweiligen rmDATA-Programmes automatisch mitinstalliert. Sollte der Dongle schon zuvor angesteckt werden, wird der benötigte Treiber automatisch über die Windows-Update Funktion des Betriebssystems heruntergeladen und installiert.
3. Die rmDATA-Produkte stehen sofort zur Verwendung bereit.

Hinweise:

- Sie können den Dongle auch auf anderen Rechnern anstecken, und so abwechselnd auf verschiedenen Rechnern nutzen.
- Auf demselben Rechner kann zusätzlich auch eine Softlock Lizenz installiert sein. Auch mehrere HASP Dongle zugleich können angesteckt werden. Es werden dann alle Lizenzen gemeinsam verwendet.
- Eine im Netzwerk vorhandene Netzwerklizenz wird automatisch mitverwendet, wenn ein Programm aufgerufen wird, das durch die lokale Lizenz nicht freigeschaltet ist.
- Einzelplatzlizenzen (egal ob Soft- oder Hardlock) können nicht auf Terminalservern oder über Remote Desktop betrieben werden! Dazu ist eine spezielle Netzwerklizenz erforderlich.

Erstinstallation von Netzwerklizenzen

Sie erhalten von rmDATA einen roten Netzwerk Dongle:



HASP Netzwerk-Dongle

1. Stecken Sie den Dongle an einer USB-Schnittstelle des Servers an.

Ein dezidiert Server ist nicht zwingend notwendig, der Netzwerkdongle kann auch an einem beliebigen Rechner angeschlossen werden, der dann aber immer in Betrieb bleiben sollte.

2. Bei der ersten Verwendung auf dem Rechner wird der benötigte Treiber automatisch über die Windows-Update Funktion des Betriebssystems heruntergeladen und installiert.
Sollte die Windows Update Funktion deaktiviert sein, kann der Treiber auch manuell installiert werden.
3. Die rmDATA-Produkte stehen sofort zur Verwendung bereit.

Hinweise:

- Sie können den Dongle auch auf anderen Rechnern anstecken, wenn am Server Wartungsarbeiten anfallen. Normalerweise wird er von den anderen Rechnern automatisch gefunden (siehe Kapitel „Auffinden des Lizenzservers“)
- Beachten Sie die Kapitel über die Konfigurationsmöglichkeiten im Admin Control Centers (siehe Kapitel „Das Admin Control Center“)
- Für den Betrieb auf Terminalservern oder über Remote Desktop ist eine spezielle Netzwerklizenz erforderlich. Bitte wenden Sie sich dazu an rmDATA.

Manuelle Installation des HASP Treibers

Der Sentinel HASP Treiber wird mit den rmDATA Anwendungsprogrammen automatisch mitinstalliert, bzw. beim Anstecken eines Dongles - auch ohne installierte rmDATA-Programme - automatisch über die Windows-Update Funktion des Betriebssystems heruntergeladen und installiert.

Er kann aber auch manuell installiert werden, was z.B. notwendig sein kann

- wenn ein Netzwerk Dongle auf einem Rechner mit deaktivierten Windows-Update und ohne rmDATA Programmen verwendet werden soll.
- oder auch wenn bei der ursprünglichen Installation des Dongles Fehler aufgetreten sind, und dadurch das Admin Control Center nicht funktioniert.

Das Setup für den Treiber kann aus dem rmDATA Kundenportal heruntergeladen werden, unter „Downloads – Allgemein“: <https://portal.rmdatagroup.com/>

Das Treibersetup besteht aus drei Dateien:

```
rmDATA_LicenseInstaller.exe  
rmDATA_LicenseInstaller_installieren.bat  
rmDATA_LicenseInstaller_entfernen.bat
```

Für die Installation eines Softlock sowie zum Ändern eines Hardlock wird außerdem noch die Datei „rmDATA_Lizenzmanager.exe“ benötigt.

Für die Installation rufen Sie die „rmDATA_LicenseInstaller_installieren.bat“ auf, für die vollständige Deinstallation die „rmDATA_LicenseInstaller_entfernen.bat“. Dadurch wird die „rmDATA_LicenseInstaller.exe“ mit den jeweils benötigten Parametern gestartet, und danach zur Kontrolle das Admin Control Center aufgerufen.

Achtung:

Für Windows 10 ab Version 2004 (April 2020) wird der HASP Treiber v7.100 oder neuer benötigt. Mit älteren HASP-Versionen kann es in dieser Windows Version zu Abstürzen (Bluescreens) kommen!

Im Kundenportal finden Sie immer den aktuellen Treiber, und auch in unseren Programmsetups ist der zur Freigabe aktuelle HASP Treiber enthalten.

Ändern von Lizenzen

Die Änderung von Lizenzen (Hinzufügen oder Löschen von Features/Modulen, ändern der max. Benutzeranzahl, etc.) erfolgt über den rmDATA Lizenzmanager.

Ändern eines lokalen Soft- oder Hardlock

Das Ändern von Lizenzen (z.B. um neue Programmfeatures freizuschalten) erfolgt genauso wie die Installation eines Softlock:

1. Generieren Sie eine c2v-Datei und senden Sie diese an rmDATA
Siehe Kapitel „Lizenzupdate mit c2v-Datei“
2. Sie erhalten von rmDATA eine v2c-Datei mit der Freischaltung retour. Lesen Sie diese in den SL-Key ein.
Siehe Kapitel „v2c-Datei einlesen“

Die Änderungen werden damit auf Ihrem Soft- bzw. Hardlock gespeichert. Die rmDATA Produkte sind bereit für ihren Einsatz.

Ändern eines Netzwerk Hardlock

Um Änderungen am Netzwerk-Hardlock (roter Dongle) vornehmen zu können, muss das Dienstprogramm „Lizenzmanager“ („rmDATA_Lizenzmanager.exe“) installiert sein.

- Wenn auf dem Lizenzserver auch rmDATA-Programme installiert sind, wurde dieses Dienstprogramm bereits mitinstalliert.
- Ist es auf dem Server nicht installiert, können Sie es im rmDATA Kundenportal herunterladen, oder von einem beliebigen Client kopieren, auf dem rmDATA Programme installiert wurden.
Siehe Kapitel „Manuelle Installation des HASP Treibers“
- Alternativ kann der Dongle auch temporär auf einem beliebigen Arbeitsplatz angesteckt werden, auf dem rmDATA-Software installiert ist.

Die Änderungen selbst erfolgen dann genauso wie im vorigen Kapitel „Ändern eines lokalen Soft- oder Hardlock“

Deaktivieren eines Softlock

Wenn der Softlock eines Rechners entfernt werden soll (z.B. weil diese Lizenz auf einem anderen Rechner neu freigeschalten werden soll), gehen Sie wie folgt vor:

1. Generieren Sie eine c2v-Datei und senden Sie diese an rmDATA
Siehe Kapitel „Lizenzupdate mit c2v-Datei“
2. Sie erhalten von rmDATA eine v2c-Datei zur Deaktivierung der Lizenz retour. Lesen Sie diese in den SL-Key ein.
Siehe Kapitel „v2c-Datei einlesen“
3. Nach dem Einspielen der Lizenz-Deaktivierung werden die geänderten Lizenzinformationen vom Lizenzmanager automatisch erneut gespeichert, wiederum als c2v-Datei.

4. Senden Sie diese Datei als Bestätigung der Deaktivierung per E-Mail an rmDATA
office@rmdatagroup.com

Damit wurde die Lizenz vom Rechner entfernt, und kann auf einem anderen Rechner neu aktiviert werden.

Der rmDATA Lizenzmanager (RUS)

Mit dem Lizenzmanager können Lizenzen (Keys) aktualisiert werden.

Der Lizenzmanager kann im Windows-Startmenü aufgerufen werden, alternativ können Sie den „rmDATA_Lizenzmanager.exe“ auch aus dem Programmordner heraus starten:

C:\Program Files (x86)\rmDATA\Administration\rmDATA_Lizenzmanager.exe
oder
C:\Program Files\rmDATA\Administration\rmDATA_Lizenzmanager.exe

Sie können die *.exe von dort auch auf einen anderen Rechner kopieren, zB einen Server.

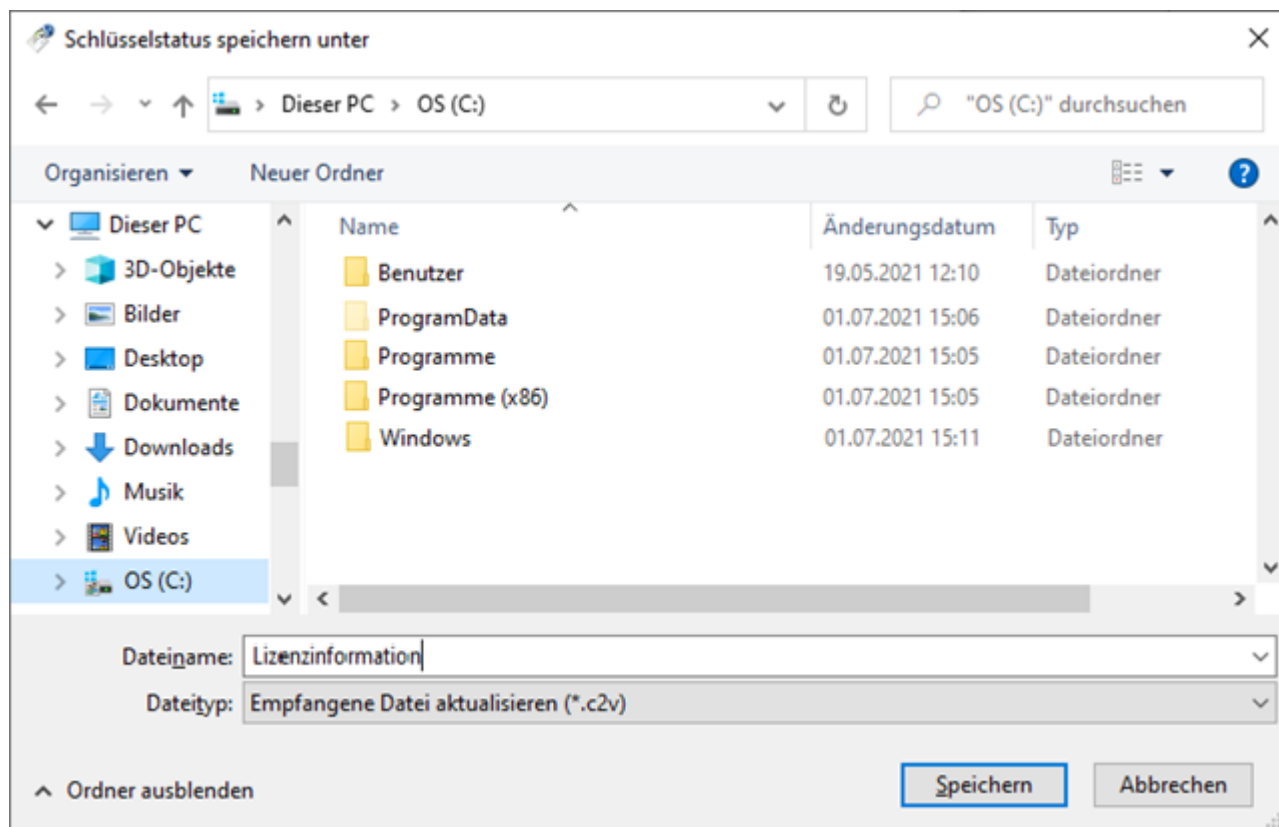
Softlock-Erstinstallation mit c2v-Datei

In der ersten Karteikarte "Statusinformationen abrufen" können die notwendigen Informationen zum Anlegen eines neuen Softlock in eine *.c2v Datei („Customer to Vendor“) exportiert werden:

1. Starten Sie das Programm „Lizenzmanager“



2. Stellen Sie sicher, dass die Option „Installation eines neuen Schutz-Keys“ ausgewählt ist
3. Klicken Sie auf [Informationen abrufen]
4. Speichern Sie die Lizenzinformationen als c2v-Datei unter einem beliebigen Namen, z.B. „Lizenzinformation.c2v“ in ein beliebiges Verzeichnis Ihres Rechners:



5. Senden Sie diese Datei per E-Mail an rmDATA
office@rmdatagroup.com

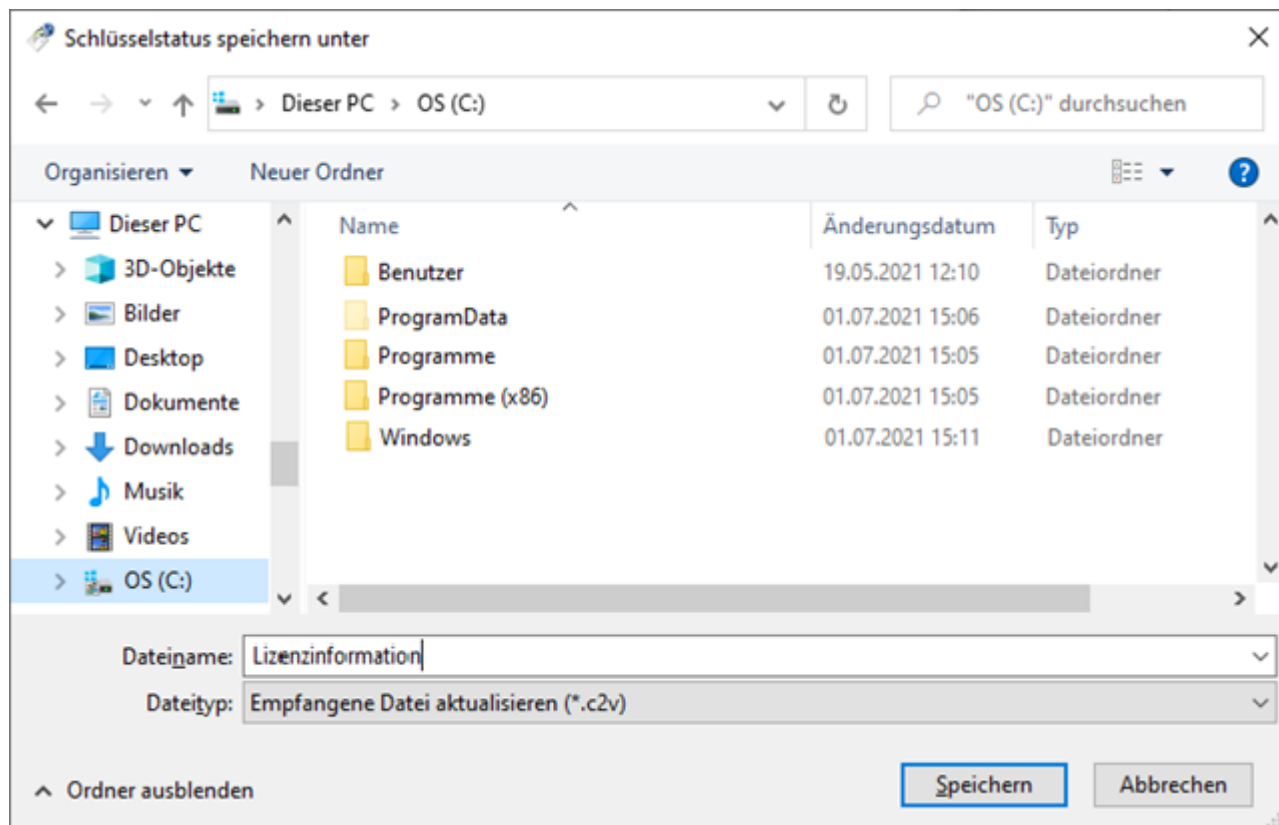
Lizenzupdate mit c2v-Datei

In der ersten Karteikarte "Collect Status Information" kann der aktuelle Inhalt eines Key (Soft- oder Hard-lock) in eine *.c2v Datei („Customer to Vendor“) exportiert werden

1. Starten Sie das Programm „Lizenzmanager“:



2. Stellen Sie sicher, dass die Option „Vorhandenen Schutz-Key aktualisieren“ ausgewählt ist (die Key's werden mit in der Regel den Programmsetups mitinstalliert - die Installation eines neuen Key's ist nur in Ausnahmefällen notwendig)
3. Klicken Sie auf [Informationen abrufen]
4. Speichern Sie die Lizenzinformationen als c2v-Datei unter einem beliebigen Namen, z.B. „Lizenzinformation.c2v“ in ein beliebiges Verzeichnis Ihres Rechners:



5. Sollten mehrere Lizenzkey's (Hardlocks und/oder Softlocks) auf dem Rechner vorhanden sein, erscheint ein Fenster in dem die gewünschte Lizenz ausgewählt werden muss. Hier z.B. hat der Rechner einen Hardlock (ein Dongle, aufgelistet als „HL“) und zwei Softlocks (ein neuerer „SL-Adminmode“, und ein älterer „SL-Legacy“):



6. Senden Sie diese Datei per E-Mail an rmDATA
office@rmdatagroup.com

Anmerkung:

Bei bestimmten Keys (nicht bei allen) kann die c2v-Datei alternativ auch aus dem [Admin Control Center](#) heraus erzeugt werden.

Dazu rufen Sie das ACC im Webbrowser auf (<http://localhost:1947>), wechseln zum Menüpunkt „Sentinel Keys“, und klicken beim gewünschten Key auf die Schaltfläche [C2V]:

Location	Vendor	Key ID	Key Type	Configuration	Version	Sessions	Actions
Local	rmDATA (106205)	1069684140418832634	HASP SL Legacy		8.11		Products Features Sessions C2V
Local	rmDATA (106205)	1030507504857309066	HASP SL AdminMode		8.11		Products Features Sessions Certificates

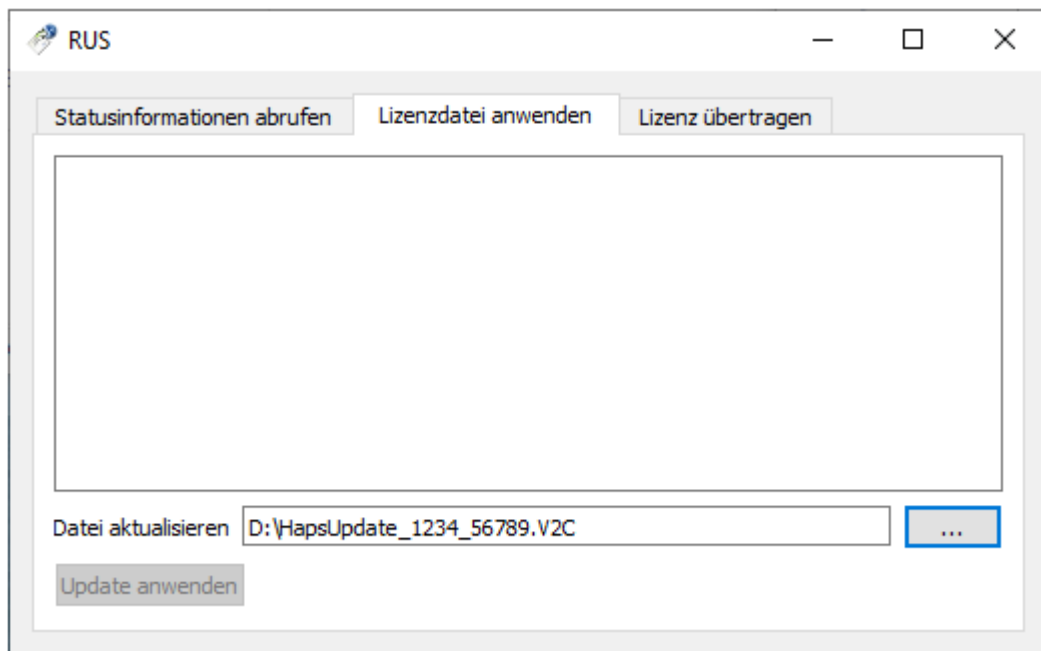
v2c-Datei einlesen

In der zweiten Karteikarte „Lizenzdatei anwenden“ kann ein von rmDATA generiertes Lizenzupdate (*.v2c Datei, „Vendor to Customer“) eingelesen, und auf den dazu passenden Key geschrieben werden

1. Sie erhalten von rmDATA eine v2c-Datei z.B. „HaspUpdate_1234_467890123.v2c“) retour
2. Starten Sie den Lizenzmanager erneut

Wechseln Sie in die Registerkarte „Lizenzdatei anwenden“

3. Wählen Sie die mit dem Button [...] die v2c-Datei aus, die Sie von rmDATA erhalten haben.



4. Klicken Sie auf [Update anwenden]

Die Änderungen werden damit auf Ihrem Soft- bzw. Hardlock gespeichert. Die rmDATA Produkte sind damit bereit für ihren Einsatz.

Die v2c Datei wird danach nicht mehr benötigt, und kann gelöscht werden (sie kann nur ein einziges Mal eingelesen werden, und nur auf dem Rechner mit dem dazu passenden Key)

Anmerkung:

Alternativ kann die v2c-Datei auch im [Admin Control Center](#) eingelesen werden.

Dazu rufen Sie das ACC im Webbrowser auf (<http://localhost:1947>), wechseln zum Menüpunkt „Aktualisieren/Einbinden“, wählen mit [Datei wählen...] die v2c-Datei aus, und klicken auf die Schaltfläche [Datei hinzufügen]:



Transfer License

Diese Funktion ist für rmDATA Lizenzen derzeit nicht möglich!

RUS

Statusinformationen abrufenLizenzdatei anwendenLizenz übertragen

Um eine Lizenz von einem Computer auf einen anderen zu übertragen (rehosten), müssen Sie das RUS-Programm auf beiden Computern ausführen. Wählen Sie auf jedem Computer die Registerkarte **Lizenz übertragen**, und führen Sie die entsprechenden Schritte aus.

Informationen zum Empfänger-Computer sammeln

Schritt 1: Rufen Sie auf dem Computer, auf den Sie die Lizenz übertragen möchten (der Empfänger-Computer) Informationen zu diesem Computer ab, und speichern Sie sie.

Empfängerinformationen speichern in

Informationen abrufen und speichern

Lizenzübertragungsdatei generieren

Schritt 2: Wählen Sie auf dem Computer, auf dem sich die Lizenz aktuell befindet (der Quell-Computer), die zu übertragende Lizenz, lesen Sie die Datei mit den Empfängerinformationen, und generieren Sie Lizenzübertragungsdatei.

Key-Typ	Key-ID	Produkte
---------	--------	----------

Datei mit den Empfängerinformationen

Die Lizenzübertragungsdatei generieren

Lizenzübertragungsdatei generieren

Das Admin Control Center (ACC)

Mit dem Admin Control Center haben Sie direkt auf Ihrem Rechner einen Überblick über alle verfügbaren Lizenzen im ganzen Netzwerk.

Die am lokalen Rechner installierten Lizenzen sind hier als Location „Local“ aufgelistet.

1. Öffnen Sie einen Internetbrowser (Internet Explorer, Firefox, ...)
2. Geben Sie die Seite <http://localhost:1947> ein
3. Das Sentinel Admin Control Center wird geöffnet

Standort	Vendor	Key-ID	Key-Typ	Konfiguration	Version	Sitzungen	Aktionen
Lokal	rmDATA (106205)		HASP SL Legacy		8.11		Produkte Features Sitzungen C2V
Lokal	rmDATA (106205)		HASP SL AdminMode		8.11		Produkte Features Sitzungen Zertifikate
	rmDATA (106205)		HASP HL Net 50		3.25	32	Öffnen Netz-Features

© 2021 Thales Group. All Rights Reserved. [English](#) [Deutsch](#) [Español](#) [Français](#) [Italiano](#) [日本語](#) [Русский](#) [中文](#) Laufzeit-Installationsprogramm 8.21.116380.1

4. Im Menü links wechseln Sie zwischen den verschiedenen Menüpunkten

- **Sentinel-Keys**

Überblick über alle Lizenzschlüssel, die im Netzwerk vorhanden sind (Lizenzserver, aber auch Einzelplatzlizenzen).

die verschiedenen Lizenzarten werden mit einem entsprechenden Icon gekennzeichnet:

Admin Mode Softlock (ab 2017):

Legacy Softlock (bis 2017):

Einzelplatz Hardlock: oder

Netzwerk Hardlock:

Durch Klick auf den Rechnernamen (in der Spalte „Location“) kann auf das HASP Admin Control Center eines anderen Rechners (z.B. Ihren Lizenzserver) gewechselt werden, sofern der Zugriff auf das ACC dieses Rechners erlaubt wurde.

Weiters können in der Spalte „Actions“ direkt auf die [Produkte], [Features] und [Sitzungen] des jeweiligen Keys zugegriffen werden, bei Netzlizenzen auf die [Netz-Features]. Außerdem kann man die LED eines Harlocks blinken lassen um diesen schneller lokalisieren zu können [Blink on], und bei Softlocks eine C2V Datei schreiben [C2V].

- **Produkte**

Überblick über alle Produkte, die Sie auf dem ausgewählten Rechner nutzen können. Die Produkte, die direkt am lokalen Rechner lizenziert sind, werden dabei mit der Location

„Local“ aufgelistet.

Anmerkung:

Die „Products“ sind nur Gruppierungen von Features – Relevant für die Lizenzierung sind die „Features“.

Mit Klick auf [Features] sehen Sie alle verfügbaren Features zu diesem Produkt.

- **Features**
Überblick über alle Features (Module), die Sie auf dem ausgewählten Rechner nutzen können.
 - **Sitzungen**
Übersicht über die aktuell genutzten Lizenzen des ausgewählten Rechners.
Sollte ein Fehler aufgetreten sein, beenden Sie mit [Disconnect] die betroffene Sitzung. Damit steht die Lizenz wieder frei zur Verfügung.
- Achtung:** Rufen Sie [Disconnect] nie auf, wenn noch in der aktuellen Sitzung gearbeitet wird. Das jeweilige rmDATA Produkt wird dadurch auf dem betroffenen Rechner sofort beendet.
- **Zugriffsprotokoll**
zeigt das Protokoll der Zugriffe
 - **Konfiguration**
hier können diverse Einstellungen des ACC geändert werden
 - **Diagnose**
zeigt Diagnoseinformationen an
 - **Spracheinstellungen** (in der Fußzeile)
hier kann die Sprache umgeschaltet werden

Hinweis:

- Wenn das Admin Control Center auf dem lokalen Rechner nicht angezeigt wird, ist der HASP Treiber nicht oder nicht korrekt installiert.
Bitte installieren Sie den Treiber nochmals manuell

Konfiguration des Lizenzservers

Die nächsten Kapitel beschreiben einige öfters benötigte Einstellungen im Admin Control Center.

Diese Punkte sind hauptsächlich für den Netzwerkschutz wichtig, sind aber zum Teil auch bei lokalen Lizenzen verwendbar, z.B. um Informationen abzufragen.

Verwendeter Port / Firewall Konfigurationen

Die gesamte Kommunikation zwischen Client und Server läuft über die Protokolle TCP und UDP auf Port 1947.

Der Port darf nicht von einer Firewall blockiert werden, und er darf auch von anderen Diensten nicht verwendet werden.

Hinweis:

Der Port 1947 wurde bei der [Internet Assigned Numbers Authority \(IANA\)](https://www.iana.org/) registriert.
Er sollte daher auch nicht von anderen Diensten verwendet werden.

Zugriff von Clients auf den Lizenzserver erlauben

Im Admin Control Center des Lizenzservers (der Rechner, auf dem der Netzwerk-Dongle angesteckt ist) muss unter “Konfiguration – Zugriff von Remote-Clients” der Zugriff erlaubt sein.
Hier können auch erweiterte Einschränkungen (z.B. Ausschluss bestimmter Clients) konfiguriert werden:

The screenshot shows the 'Sentinel Admin Control Center' interface. The left sidebar contains navigation links: Sentinel-Keys, Produkte, Features, Sitzungen, Aktualisieren/ Einbinden, Zugriffsprotokoll, Konfiguration (highlighted), and Diagnose. The main content area is titled 'Konfiguration' with a hostname of 'martins-10'. It features a tabbed interface with the following tabs: Grundeinstellungen, Benutzer, Zugriff auf Remote License Manager, Zugriff von Remote-Clients (active), Client-Identitäten, Auslagerbare Lizenzen, and Netzwerk. Under the 'Zugriff von Remote-Clients' tab, the 'Zugriff von Remote-Clients zulassen' section has three radio button options: 'Niemand', 'Nur identifizierbare Clients. Auf Nicht-Cloud-Lizenzen kann nicht zugegriffen werden.', and 'Cloud-Lizenzen erfordern Identität. Auf alle anderen Lizenzen kann durch alle Clients zugegriffen werden.' The third option is selected. Below this, a red-bordered box highlights the text: 'Auf alle Lizenzen kann ohne Identität zugegriffen werden'. A red warning note states: 'Hinweis: Unabhängig von der ausgewählten Option können Remote-Computer, die eine Client-Identität verwenden, nicht auf Lizenzen außerhalb der Cloud zugreifen.' Below this are input fields for 'Öffentliche Adresse für Zugriff mit Identität und ACC', 'Vertrauenswürdige IP-Adresse', and 'Öffentlicher Port für Zugriff mit Identität'. There are also checkboxes for 'Abhören nach Clients auch an Port 80' and radio buttons for 'Klartext' (selected) and 'Mit dem mit der Sentinel AdminAPI zur Verfügung gestellten Speicher-Key'. A large text area for 'Zugriffseinschränkungen' is present, with a button 'Letzten Client-Zugriff anzeigen' below it. At the bottom are buttons for 'Übernehmen', 'Abbrechen', and 'Einstellungen'. A footer note explains the evaluation order of the restrictions.

Im Admin Control Center der Clients muss unter “Konfiguration – Zugriff auf Remote License Manager” die Checkbox “Zugriff auf Remote Lizenzen” angehakt sein:

The screenshot shows the 'Sentinel Admin Control Center' interface for a client. The left sidebar is identical to the previous screenshot, with 'Konfiguration' highlighted. The main content area is titled 'Konfiguration' with a hostname of 'martins-10'. The tabs are: Grundeinstellungen, Benutzer, Zugriff auf Remote License Manager (active), Zugriff von Remote-Clients, Client-Identitäten, Auslagerbare Lizenzen, and Netzwerk. Under the 'Zugriff auf Remote License Manager' tab, the 'Zugriff auf Remote-Lizenzen zulassen' checkbox is checked. Below it, the 'Broadcast-Suche nach Remote-Lizenzen' checkbox is also checked, and the 'Offensive Suche nach Remote-Lizenzen' checkbox is unchecked. The 'Suchparameter für Remote-Lizenzen' section contains a text area with the following content: 'Name_meines_Lizenzservers', 'oder', and 'IP-Adresse_meines_Lizenzservers'. At the bottom are buttons for 'Übernehmen', 'Abbrechen', and 'Einstellungen'.

Beide Einstellungen sind nach der Installation per Default aktiviert. Sie sollten normalerweise nicht deaktiviert werden.

Zugriff von Clients auf das Admin Control Center erlauben

Um Clients den Zugriff auf das Admin Control Center des Servers zu erlauben (z.B. um den Clients zu erlauben festzustellen wer eine bestimmte Lizenz belegt hat) muss unter "Konfiguration – Grundeinstellungen" die Checkbox "Remote-Zugriff auf ACC zulassen" auf „HTTP" gestellt werden. Dies ist per Default nicht erlaubt.

Wird der Zugriff auf das ACC erlaubt sollte gleichzeitig auch ein Passwort für die Konfigurationsseiten vergeben werden, um zu verhindern, dass Anwender versehentlich Konfigurationsänderungen am Lizenzserver vornehmen:

Hinweis:

Notieren Sie das Passwort, und verwahren Sie es an einem sicheren Ort.
Wir haben keine Möglichkeit, ein verlorenes Passwort zurückzusetzen!

Auffinden des Lizenzservers

Auf den Clients kann unter "Konfiguration – Zugriff auf Remote License Manager" eingestellt werden, wie sie den Lizenzserver suchen sollen.

Normalerweise geschieht dies automatisch über Network Broadcast – die Option „Broadcast Suche“ ist per Default immer aktiviert.

Wenn Sie Ihr Netzwerk in mehrere Subnetze strukturiert haben, oder VPN-Verbindungen nutzen, werden die Broadcast-Pakete möglicherweise von den Routern ausgefiltert.

In solchen Fällen muss der zu verwendende Lizenzserver manuell angegeben werden, im Feld „Suchparameter“, mit der IP-Adresse oder dem Rechnernamen.

Die Option „Offensive Suche“ wird normalerweise nicht benötigt.

Sentinel Admin Control Center

Konfiguration Hostname: martins-10

Grundeinstellungen Benutzer Zugriff auf Remote License Manager Zugriff von Remote-Clients Client-Identitäten Auslagerbare Lizenzen Netzwerk

Zugriff auf Remote-Lizenzen zulassen ☒ Möglicherweise gibt es einige Minuten Verzögerung, bevor Ihre Änderungen in Kraft treten.

Broadcast-Suche nach Remote-Lizenzen ☒

Offensive Suche nach Remote-Lizenzen ☐

Suchparameter für Remote-Lizenzen

Name_meines_Lizenzservers
oder
IP-Adresse_meines_Lizenzservers

Einstellungen

Übernehmen Abbrechen

Klarnamen für products und features

Im Admin Control Center werden Produkte und Features normalerweise nur über deren Nummer angezeigt.

Um die Listen lesbarer zu gestalten, können Sie von rmDATA eine Übersetzungstabelle anfordern („106205.xml“), die im Admin Control Center eingelesen wird (Menüpunkt „Aktualisieren/Einbinden“):

Sentinel Admin Control Center

Lizenz aktualisieren/einbinden Hostname: martins-10

Datei wählen: 106205.xml Datei wählen... ?

Dateiformat: V2C-, V2CP-, H2R-, R2H-, H2H- oder ID-Datei

Datei hinzufügen Abbrechen

Danach werden Produkte und Features mit lesbaren Klarnamen angezeigt:

Sentinel Admin Control Center			
Verfügbare Features Hostname: martins-10			
Sentinel-Keys			
Produkte			
Features			
Sitzungen			
Aktualisieren/ Einbinden			
Zugriffsprotokoll			
Vendor	Key-ID	Produkt	Feature
rmDATA	1276749475	621 Alle Produkte - HL NET 06-2021	1300 rmGEO.DXF-Schnittstelle
rmDATA	1276749475	621 Alle Produkte - HL NET 06-2021	1240 rmGEO.Messdatenschnittstelle.GEOMAX
rmDATA	1276749475	621 Alle Produkte - HL NET 06-2021	1235 rmGEO.Messdatenschnittstelle.TRIMBLE.SC

ACC Einstellungen auf andere Rechner verteilen

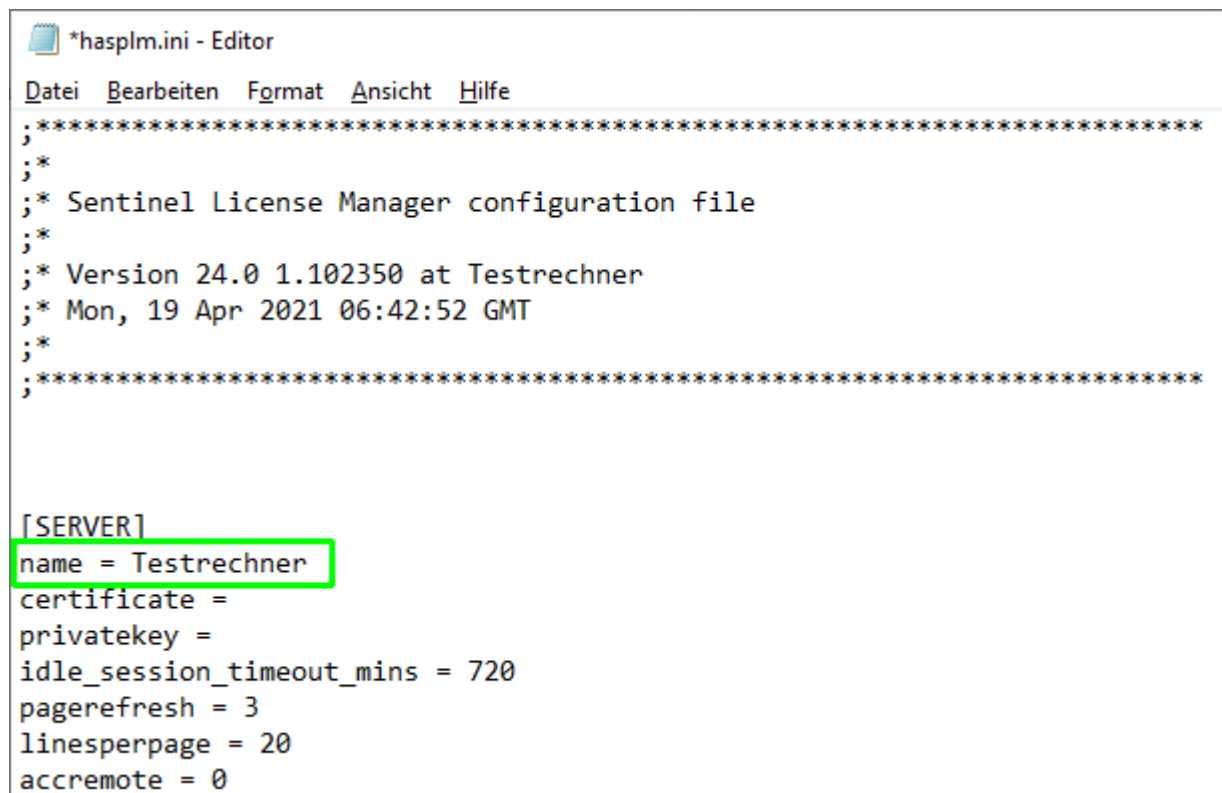
Die Einstellungen des Admin Control Centers werden auf dem jeweiligen Rechner in der Datei "C:\Program Files (x86)\Common Files\Aladdin Shared\HASP\hasplm.ini" gespeichert.

Diese Datei kann auf andere Rechner verteilt werden, was vor allem für die Clienteneinstellungen sinnvoll sein kann (z.B. wenn der Name des Lizenzservers explizit festgelegt wurde)

Achtung:

In der Datei ist der Hostname des ursprünglichen Rechners (der Eintrag „name =...“ in der Sektion [SERVER]) enthalten.

Dieser Eintrag muss vor dem Kopieren auf einen anderen Rechner aus der Datei gelöscht, oder auf den jeweiligen Rechnernamen abgeändert werden:



```
*hasplm.ini - Editor
Datei Bearbeiten Format Ansicht Hilfe
;*****
;*
;* Sentinel License Manager configuration file
;*
;* Version 24.0 1.102350 at Testrechner
;* Mon, 19 Apr 2021 06:42:52 GMT
;*
;*****

[SERVER]
name = Testrechner
certificate =
privatekey =
idle_session_timeout_mins = 720
pagerefresh = 3
linesperpage = 20
accremote = 0
```