SecuLution Application Whitelisting Installationsanleitung

de en it es fr

Index

Kurzanleitung

Video

Begleitend zu dieser Installationsanleitung finden Sie eine Video-Playlist.

Erstinstallation SecuLution

- SecuLution Appliance installieren
  - 16 GB RAM, 12 CPUs, NIC: VMXNET3, MAC statisch
- AdminWizard installieren und Grundkonfiguration durchführen
  - IP der Appliance (DHCP) auf der Konsole der Appliance ablesen
  - Login Default-Passwort: “password”
  - IP der Appliance (temporär DHCP) auf korrekte statische IP ändern (im AdminWizard unter “SecuLution Appliance” -> “IP Konfiguration”, wir empfehlen hier einen DNS-Server zu verwenden, der nicht mit dem Agent abgesichert werden wird, wie z.B. das GW)
  - Login Passwort ändern (“SecuLution Appliance”-“Login Passwort”)
  - Lern-Benutzer im AD anlegen
  - AD Replikation (Menü “Extra”)
  - Lern-Benutzer konfigurieren (Tab “Lern-Quellen”-“Lern-Benutzer”)
- Client Konfiguration einrichten (empfohlene Default Werte)
  - Standard Nachrichten: “Dieses Programm wurde nicht als vertrauenswürdig eingestuft und kann daher nicht gestartet werden. Wenden Sie sich an die EDV Abteilung, falls Sie das Programm beruflich benötigen.”
  - Sprache: Deutsch
  - USB Whitelisting: nach Wahl

    - Deaktivierungspasswort: setzen (hier ein neues Passwort verwenden, das man zur Not weitergeben kann)
    - Deaktivierungsmeldung: an
    - DLL Prüfung: RunDLL
    - Signaturprüfung: an
    - Java Prüfung: an
    - Agent Symbol verbergen: aus
    - Offline Modus: “Keine Passwortüberprüfung, alles wird erlaubt” für die ersten 4 Wochen nach Installation, danach “Passwort” oder “Challenge Response”
    - Performance Cache: 900s
- Musterrechner Import (Tab ”Import-Quellen”-”Importieren dieses Rechners als Musterrechner”)
- SecuLution Appliance reboot (Tab “SecuLution Appliance” / Neustarten, triggert sofortige Erstellung der für Agent-Installationen benötigten offline-db)
- Agent Verteilung einrichten
    - Tab “Client-Management”-”RCM” Einrichtung
    - Clients zur Verteilung des Agents markieren
- Signaturherausgeber hinzufügen (signierte Files per Drag’nDrop hinzufügen, “Signatur zur Whitelist hinzufügen”)
- Automatismus hinzufügen
- Agent Verteilung initialisieren und abwarten (z.B. 2 Wochen; der initiale Lernmodus ist noch an; die Whitelist wird alle noch unbekannten Hashes lernen)
- Lernmodus abschalten und *gelernte* Hashes gegen die TLDB prüfen
- Hashes mit TL<4 manuell prüfen

Begriffe

SecuLution Appliance

In diesem Dokument bezeichnet “SecuLution Server Appliance” die SecuLution Server Datenbank, Ihre VM, die die Whitelist enthält.

Agent / Client

In diesem Dokument bezeichnet “Agent” die SecuLution Agent Software, die auf jedem Computer, der mit SecuLution geschützt werden soll, installiert werden muss. Es können so viele Agenten installiert werden, wie Lizenzen erworben wurden. Da sich der Agent mit der SecuLution Server Appliance verbindet, ist er in diesem Sinne auch ein Client. Der Agent ist kompatibel mit allen Windows Versionen ab Windows XP SP3 auf allen x86 und x64 Architekturen (nicht ARM).

AdminWizard

In diesem Dokument bezeichnet der Begriff “AdminWizard” die SecuLution Management GUI Software, mit der Administratoren die Konfiguration von SecuLution verwalten.

Allgemeines

Geräte

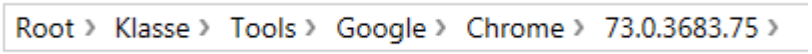
SecuLution kann alle USB-Geräte anhand ihrer Hersteller- und Produkt-ID (VIDPID) erkennen und verwalten. Ein unbekanntes Gerät wird nicht zugelassen, egal welcher Geräteklasse es entspricht, dies gilt also z.B. auch für Tastaturen. Ist die Unterscheidung der Geräte nach Seriennummer konfiguriert, so gilt dies nur für USB-Massenspeichergeräte. Nicht-Massenspeichergeräte werden trotz der Einstellung “Unterscheidung nach Seriennummer” nur über die VIDPID verwaltet.
USB-Geräte werden in der TLDB nicht verwaltet, daher muss zur Vermeidung von gesperrten USB-Tastaturen und USB-Mäusen bei eingeschalteter USB-Geräteprüfung eine Agent-Installation im Lernmodus erfolgen.

AD Objekte

Regeln können sich auf Active Directory (AD) Objekte beziehen. Um diese aus dem AD zu replizieren, klicken Sie auf Menü Extras / Active Directory Objekte aktualisieren.
Ihr Active Directory (AD) enthält Informationen über Sicherheitsgruppen, Computer und Benutzer, die von SecuLution als Referenzobjekte für individuelle Richtlinien verwendet werden können. Nach Abschluss der Replikation können Aktionen, die sich auf Hashes beziehen, nun nicht nur auf IP-Adressen, sondern auch auf AD-Objekte vom Typ Benutzer, Computer oder Gruppe bezogen werden. Die AD-Objekte werden in der Whitelist gespeichert. Dieser Vorgang kann automatisch über den Automatismus durchgeführt werden.

Klassifizierungen

Zur besseren Verwaltung können Hashes mit einer Klassifizierung versehen werden. Dabei handelt es sich um einen Freitext, der keinen Einfluss darauf hat, ob ein Hash zugelassen oder abgelehnt wird, sondern nur zur besseren Strukturierung und Übersichtlichkeit für den Administrator zur Verfügung steht. Das Semikolon im Freitext definiert eine Trennung der Ebenen. Wir empfehlen Klassifizierungen wie `Musterrechner;WINDOWS10;PC123` oder `Tools;Hersteller;Produkt;Version`



Signaturen

SecuLution kann unbekannte Software automatisch zur Whitelist hinzufügen, wenn diese elektronisch signiert ist (Authenticode). Dazu kann der Administrator Signaturen von Herstellern, deren Software er automatisch vertrauen möchte, per Drag’nDrop einer signierten Datei im AdminWizard hinzufügen. (Checkbox “Signatur-Hersteller hinzufügen”).

TrustLevel Datenbank Service (TLDB)

SecuLution betreibt einen redundanten Cluster einer Cloud-basierten Datenbank mit Hashes vertrauenswürdiger Software in deutschen Rechenzentren. Wie vertrauenswürdig ein Hash ist, bewertet SecuLution mit sogenannten TrustLevels. Die TrustLevel-Datenbank wird ausschließlich von Mitarbeitern der SecuLution GmbH gepflegt und liefert bei über 99% der Anfragen einen guten TrustLevel. Unter dem Reiter “Lernquellen” kann ein minimaler TrustLevel-Schwellenwert festgelegt werden. Ist ein Hash in der lokalen Whitelist nicht bekannt, wird er in der TrustLevel-Datenbank abgefragt. Ist der TrustLevel des Hashes in der TrustLevel Datenbank mindestens so hoch wie der eingestellte Schwellenwert, wird der Hash automatisch der Whitelist als erlaubt hinzugefügt. Auf diese Weise lernt Ihr SecuLution System automatisch vertrauenswürdige Software, ohne dass ein Administrator manuell eingreifen muss.

TrustLevel in der lokalen Whitelist

In der lokalen Whitelist ist der TrustLevel eine Metainformation, die an einen Hash angehängt werden kann. Der TrustLevel hat keinen Einfluss auf die Zulässigkeit einer Software.

TrustLevel in der SecuLution TrustLevel-Datenbank (TLDB)

Die im SecuLution TrustLevel Datenbank Service verwendeten TrustLevel werden wie folgt vergeben:

TrustLevel 0
: Es liegen Indikatoren vor, die auf eine potenzielle Schadhaftigkeit dieser Software hinweisen.

TrustLevel 1-2
: Es liegen Indikatoren vor, die darauf hinweisen, dass diese Software im geschäftlichen Umfeld ungeeignet ist (z. B. Signatur revoked).

TrustLevel 3
: Die Software ist entweder unbekannt, völlig neu oder es liegen ebenso viele Indikatoren für eine positive wie eine negative Einstufung der Software vor.

TrustLevel 4-10
: Es liegen Indikatoren vor, die auf eine erwünschte und vertrauenswürdige Software hinweisen. Je höher der Wert, umso stärker sind die Indikatoren

Detaillierte Beschreibung der Installation

Syslog Server

Ihre Appliance kann Log-Meldungen an einen externen Syslog Server senden. Der Syslog-Server selbst (der Server, der Syslog-Meldungen empfängt und speichert) ist nicht Bestandteil von SecuLution. Es stehen jedoch verschiedene kommerzielle und freie Produkte zur Verfügung. Jede Linux-Distribution enthält einen Syslog-Server. Um Ihnen bei Supportanfragen helfen zu können, sind Syslogs zwingend erforderlich.

Regeln in der Firewall oder Proxy, Zugriff auf die TrustLevel Service Datenbank, Ports, Zertifikate

Die Kommunikation der SecuLution Komponenten erfolgt über TLS-gesicherte Verbindungen mit gegenseitiger Zertifikatsprüfung und Certificate Pinning. Dies bedeutet insbesondere, dass die TLS-Verbindung zwischen den SecuLution Komponenten nicht unterbrochen werden darf. Gegebenenfalls muss in Ihrer Firewall und/oder Ihrem (transparenten) Proxy eine Ausnahme für den Zugriff auf Port 443 (HTTPS) eingerichtet werden, damit die SecuLution Appliance und der AdminWizard ungefiltert auf die SecuLution Appliance und die TrustLevel Service Datenbank zugreifen können. Proxies werden nicht unterstützt.

Datenverkehr der SecuLution Appliance

Die SecuLution Appliance benötigt ungefilterten Zugriff auf Port 443 der folgenden Hosts:

- tldb2.seculution.com
- tldb3.seculution.com
- *.seculution.com (für die Zukunft, falls einstellbar)

Mehrere SecuLution Appliances eines MultiServer SecuLution Appliance Clusters kommunizieren untereinander über Port 1404.
Die SecuLution Appliance kommuniziert mit den von Ihnen konfigurierten DNS-, NTP- und Syslog-Servern über die Standard-Ports dieser Dienste.
Jede SecuLution Appliance muss jeden der oben genannten Kommunikationspartner über ICMP erreichen können.

Datenverkehr des AdminWizards

Computer mit installiertem AdminWizard benötigen ungefilterten Zugriff auf Port 443 der folgenden Hosts:

- cdn.seculution.com
- tldb2.seculution.com
- tldb3.seculution.com
- *.seculution.com (für die Zukunft, falls einstellbar)

Datenverkehr für Client Computer mit Agent

Der SecuLution Agent benötigt ungefilterten Zugriff auf Port 443 Ihrer SecuLution Appliance. Für den Download von Updates benötigen Client-Computer, die aktuell keinen Zugriff auf das AD haben (z.B. Home-Office Systeme), Zugriff auf das Cloudflare-CDN unter der Domain *.`r2.dev`.

Datenverkehr zwischen AdminWizard und SecuLution Appliance

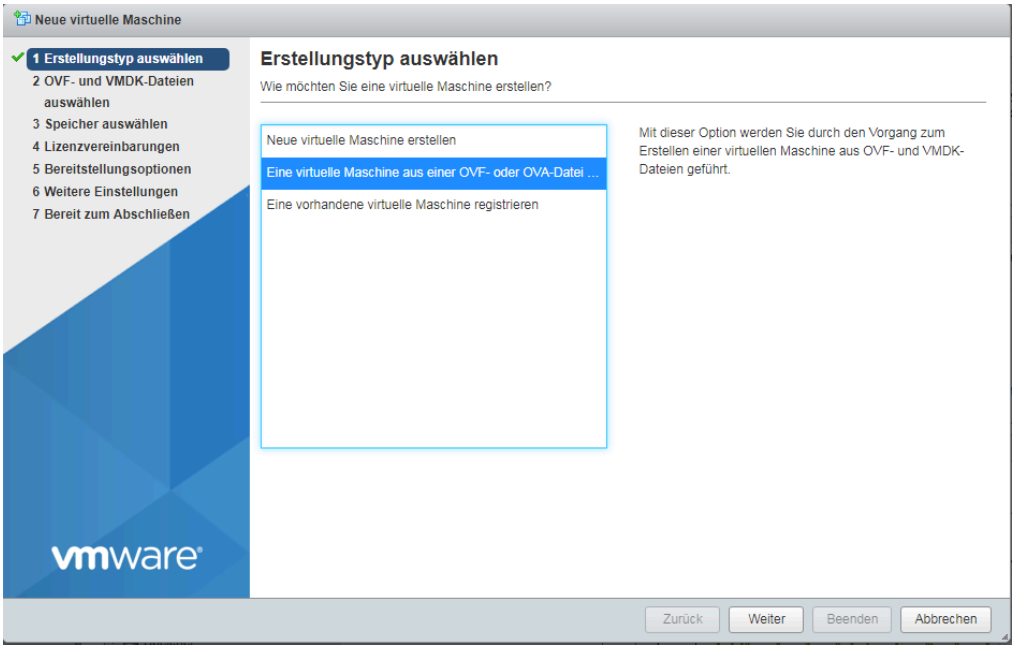
Computer mit installiertem AdminWizard benötigen ungefilterten Zugriff auf folgende Ports der SecuLution Appliance

- 443
- 8191
- 8192
- 8193
- 11310

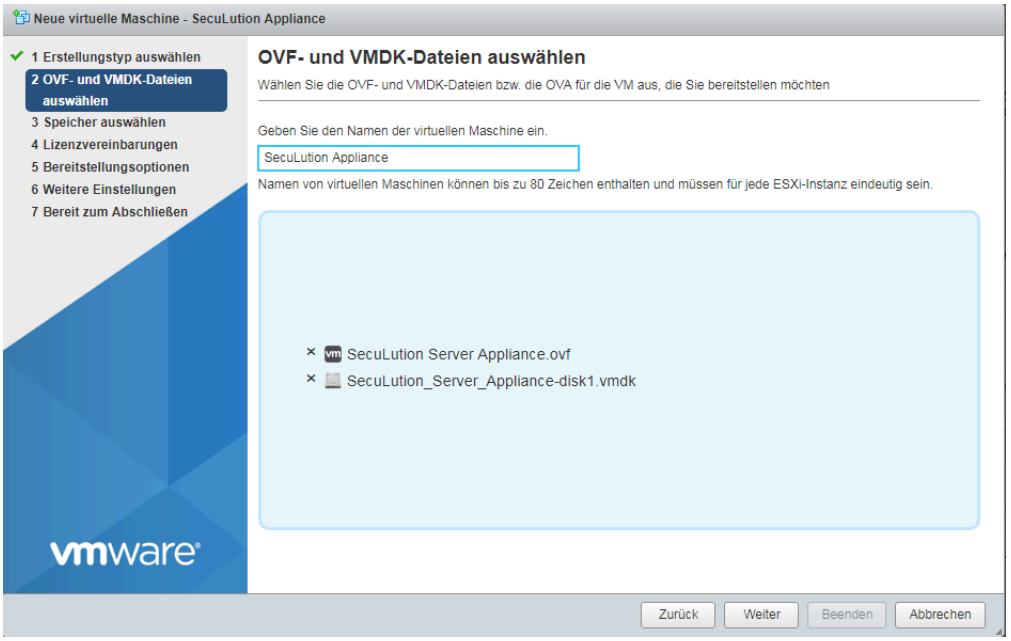
SecuLution Appliance installieren

Installation der SecuLution Appliance am Beispiel der VMware Web Konsole

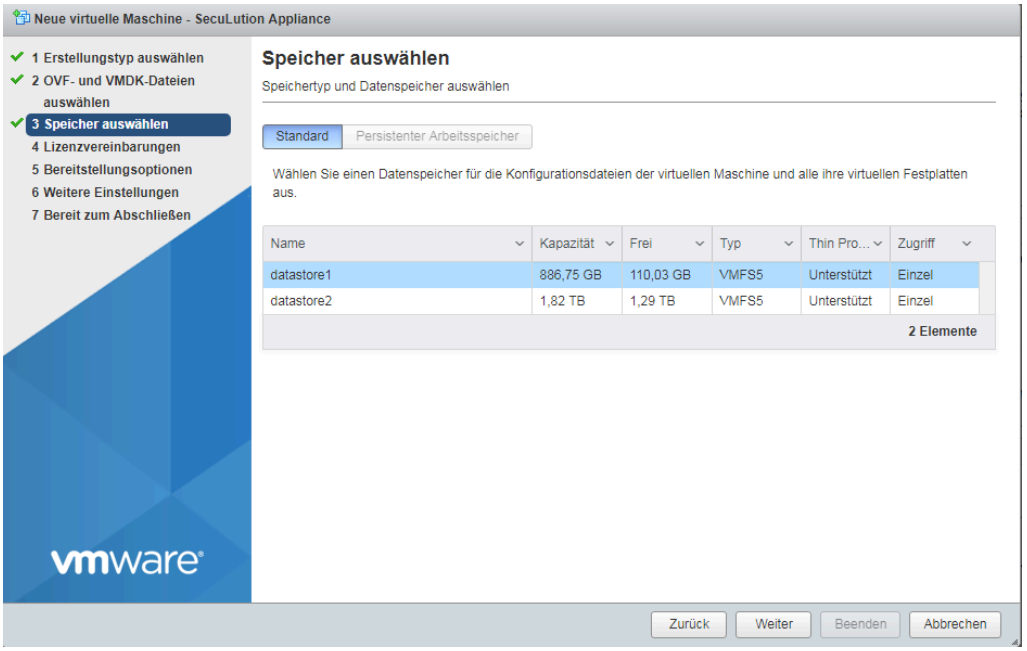
Wählen Sie in der VMware Web Konsole “Neue Virtuelle Maschine” und wählen Sie “aus OVF”:



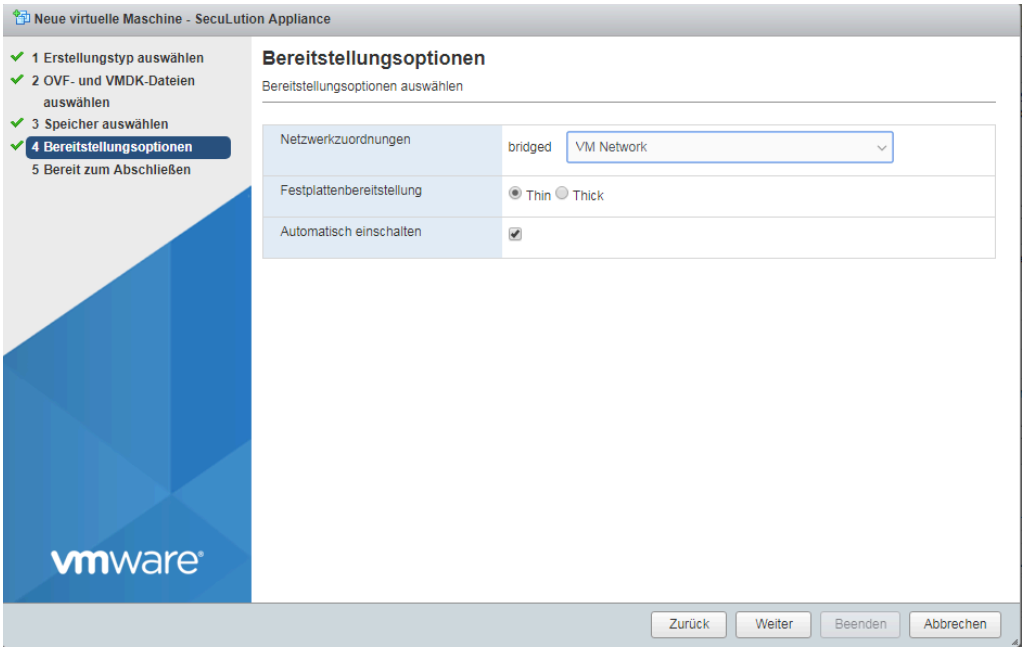
Vergeben Sie einen Namen und fügen Sie die .ovf und die .vmdk Datei dem Import hinzu.



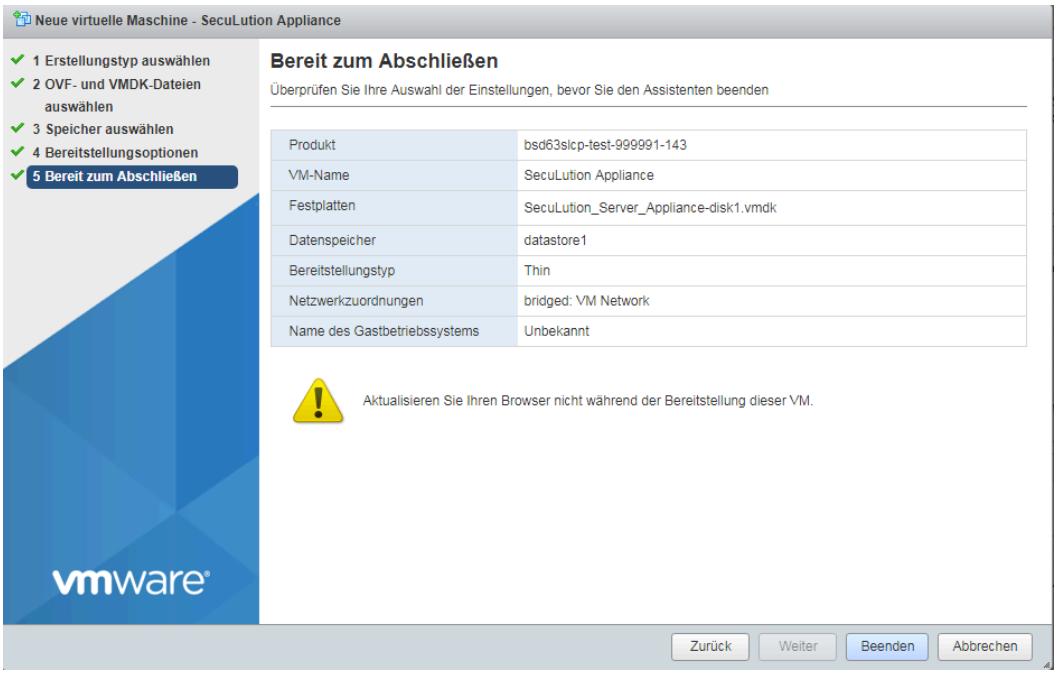
Geben Sie den Speicherort für die SecuLution Appliance an. Es werden 16 GB im Datastore benötigt.



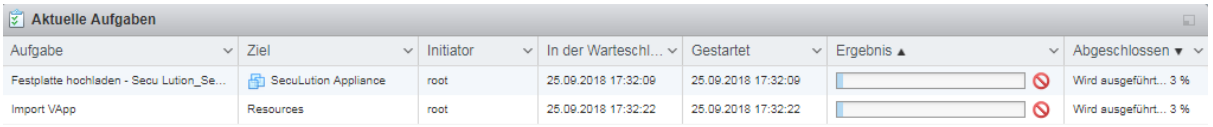
Legen Sie die Netzwerkzuordnung fest:



Schließen Sie die Installation ab.



Die VM wird importiert.



Installation der SecuLution Appliance mit ovftool

Alternativ zur Web Konsole kann die OVA in VMWare ESXi auch mit ovftool importiert werden.
Syntax (alles in einer Zeile):

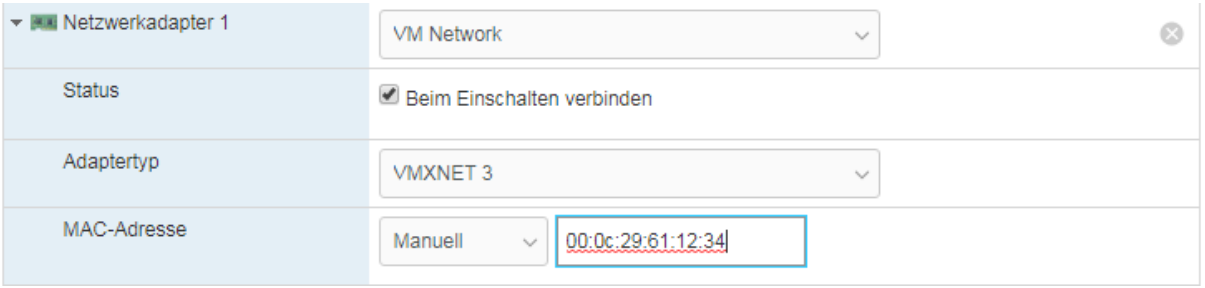
```
ovftool.exe --acceptAllEulas --name=SecuLution
--datastore=<Speicherort> "<Pfad_zur_OVA_Datei>"
vi://root:<esxi-root-passwort>@<esxi-IP-Adresse>
```

Beispiel (alles in einer Zeile):

```
ovftool.exe --acceptAllEulas --name=SecuLution
--datastore=datastore1 "c:\temp\SecuLution_Appliance_std.ova"
vi://root:password@192.168.111.111
```

Einstellungen der Netzwerkkarte

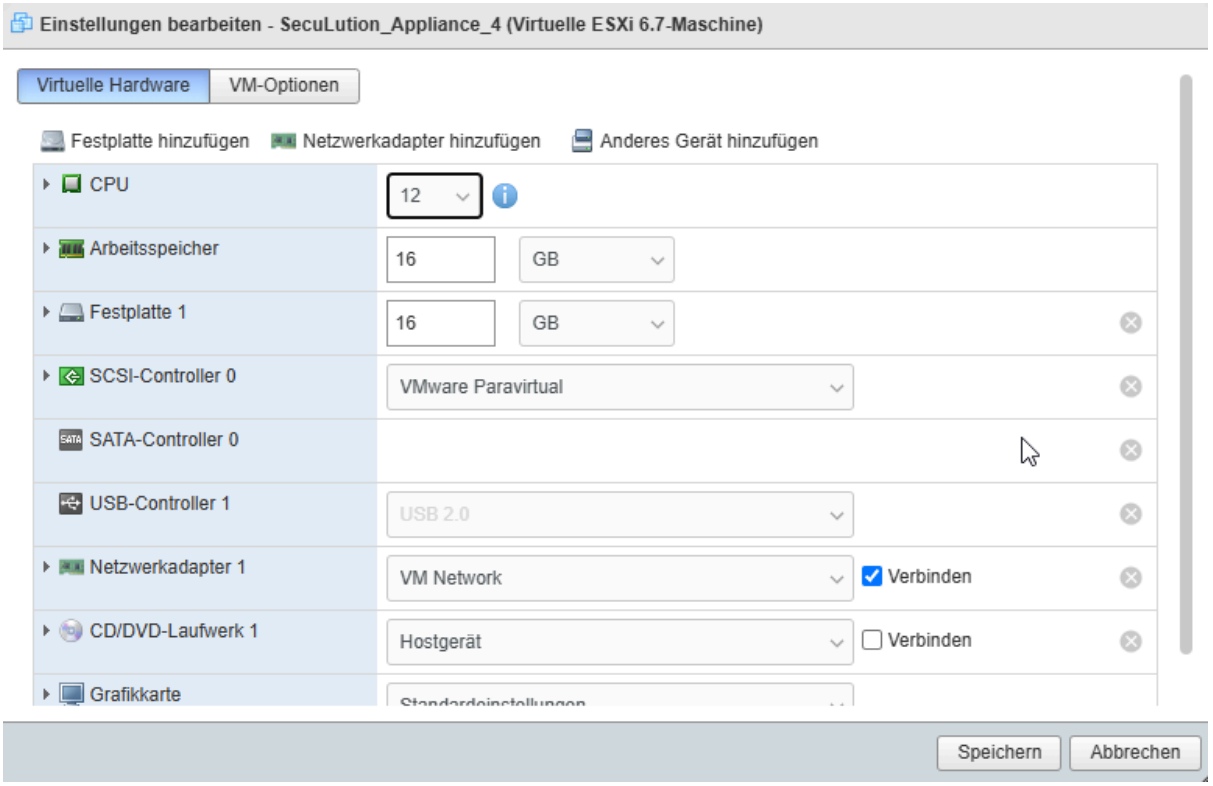
Editieren Sie die Einstellungen der Netzwerkkarte in Adaptertyp VMXNET3, wählen Sie das passende VLAN und stellen Sie eine zufällige statische MAC Adresse ein.



The MAC address range is `00:50:56:00:00:00-00:50:56:3F:FF:FF`.

Ressourcen: RAM und CPU

Wir empfehlen die Konfiguration von 16 GB RAM und 12 Prozessorkernen. Siehe: Anmerkungen zum Ressourcenbedarf .



Anmerkungen zum Ressourcenbedarf der SecuLution Appliance

nachträgliche RAM-Änderung erfordert neue Initialisierung der DB

Die SecuLution Appliance ermittelt beim ersten Start die verfügbaren RAM-Ressourcen und konfiguriert die Datenbank entsprechend. Eine nachträgliche Änderung des RAM-Speichers erfordert daher eine Neuinstallation der Datenbank, die über die Konsole beim Booten durchgeführt werden kann (“Reset to factory settings”).

RAM: Minimal 8, besser 16 GB

In der Regel benötigt die SecuLution Appliance nur 2-3 GB RAM. Einige Aktionen, die der Administrator im SecuLution AdminWizard durchführt, laufen deutlich schneller, wenn die SecuLution Appliance kurzzeitig auf mehr Arbeitsspeicher zurückgreifen kann. Es ist daher kein Nachteil, der VM 8 GB RAM oder mehr zur Verfügung zu stellen, damit dieser Speicher bei Bedarf kurzfristig verfügbar ist.

CPUs: Empfohlen: 12

Auch wenn die SecuLution Appliance technisch minimal mit 4 CPUs lauffähig ist, profitiert die Performance der SecuLution Appliance erheblich von der Zuweisung weiterer CPUs. Insbesondere profitieren nicht nur Operationen im SecuLution AdminWizard, sondern alle Aufgaben des Betriebssystems von zusätzlichen CPU-Ressourcen.

Die Datenbank der Appliance kann bei internen Reorganisationsaufgaben kurzfristig alle verfügbaren CPUs (bis maximal 8) voll auslasten. Dies kann dazu führen, dass dem Betriebssystem bei weniger als 9 verfügbaren CPUs nicht mehr genügend CPU-Leistung für seine eigenen Aufgaben zur Verfügung steht.

In der Praxis hat sich eine Zuweisung von 12 CPUs als optimal erwiesen, da in diesem Fall 4 CPUs für die Aufgaben des Betriebssystems reserviert bleiben, während die Datenbank bis zu 8 CPUs nutzen kann.

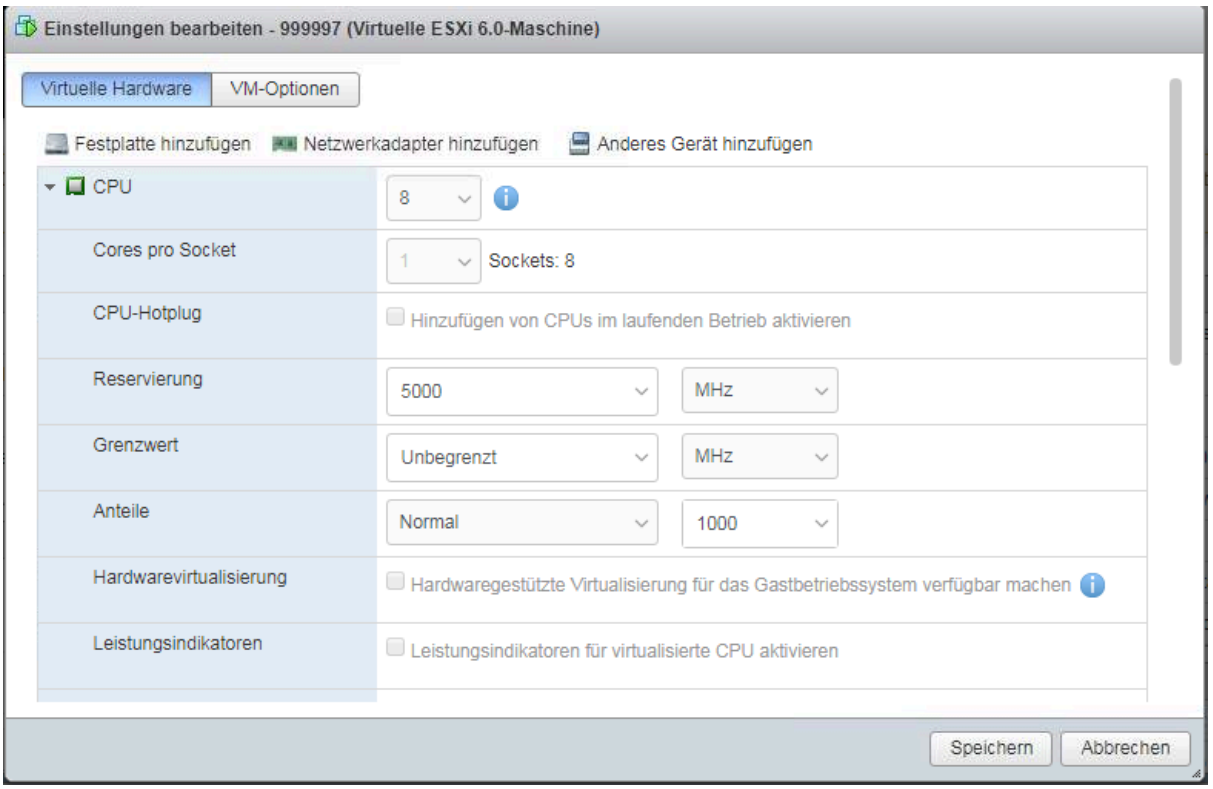
Obwohl es technisch möglich ist, nur 4 oder 8 CPUs zuzuweisen, wird dies nicht empfohlen, da es zu Leistungseinbußen kommen kann. Für andere virtuelle Maschinen (VMs) auf demselben Hypervisor-Host hat die Zuweisung von 12 CPUs an die SecuLution Appliance keine Nachteile. Die Appliance belegt nur dann CPUs, wenn tatsächlich rechenintensive Aufgaben ausgeführt werden, wie z.B. Operationen im AdminWizard GUI oder andere systeminterne Prozesse.

BIOS Clock in UTC

Ab Version 4.x der Appliance ist es möglich, die BIOS Zeit in localtime zu pflegen.

Ressourcen Reservierung

Für einen stabilen Betrieb der VM ist es wichtig, dass die SecuLution Appliance auch bei hoher Last auf dem Hypervisor (z.B. beim Backup der VM) genügend Ressourcen zur Verfügung hat, um ihre Arbeit ungehindert ausführen zu können. In den meisten Fällen reicht hierfür die Reservierung von CPU-Ressourcen (Reservierung von 5000 MHz) aus.



OVA importieren oder konvertieren

Sie erhalten die SecuLution Appliance als OVA. Diese kann in alle gängige Virtualisierungsumgebungen importiert werden.

Falls Ihre ESXi Version nicht zur OVA passt (zu alt, zu neu), um die Hardware-Version der OVA oder .vmdk zu unterstützen, führen Sie eine Hardware-Konvertierung durch.

Hinweise zu bestimmten Hypervisoren:

- QEMU - Prozessor-Typ auf “Host” stellen
- Proxmox Install script

Allgemeine Hinweise für andere Hypervisoren:

- OVA mittels 7zip entpacken
- neue VM auf Hypervisor anlegen (Ressourcen), keine Festplatte anlegen
- entpackte .vmdk in Ordner der zuvor angelegten VM hochladen / kopieren
- Der VM das .vmdk als vorhandene Festplatte hinzufügen

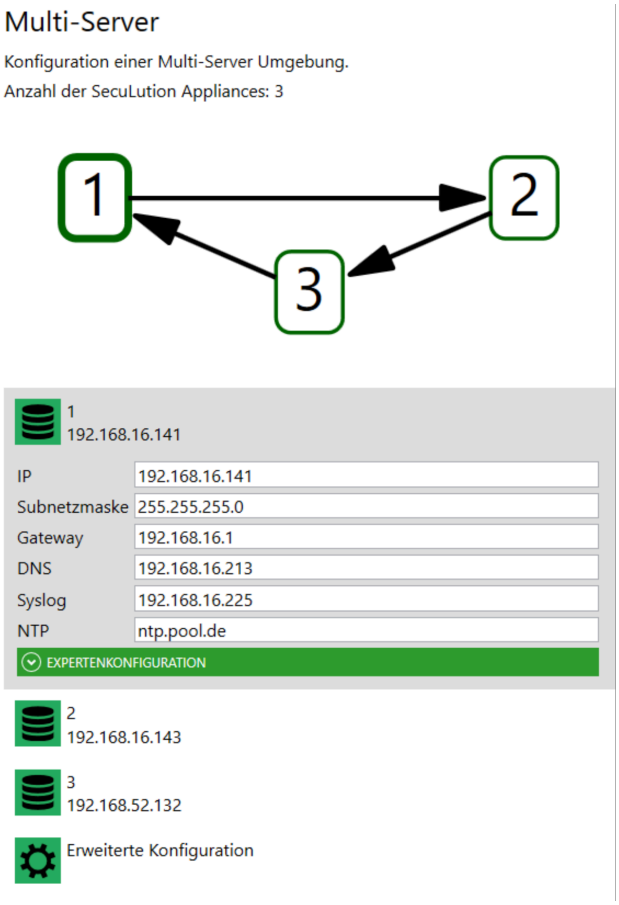
IP Konfiguration einer oder mehrerer SecuLution Appliances

Ab Version 4.0.21 fragt die SecuLution Server Appliance beim ersten Start nach der Installation einen DHCP-Server nach einer (temporären) IP-Adresse. Falls Sie keinen DHCP-Server im Netzwerksegment der SecuLution Server Appliance betreiben, kann beim Booten eine temporäre IP-Adresse manuell in der Konsole eingegeben werden. Bei einer

temporären Änderung der IP in der Konsole gilt die IP-Konfiguration nur für diesen einen Bootvorgang, d.h. nach jedem Reboot wird die IP wieder auf die fest konfigurierte IP zurückgesetzt.
Eine dauerhafte Änderung der Konfiguration muss dann über den AdminWizard unter “SecuLution Appliance” -> IP -> Konfiguration vorgenommen werden.

Ab der Appliance Version 4.0.22 unterstützt SecuLution den Betrieb mehrerer, paralleler SecuLution Server Appliances. Die SecuLution Appliances arbeiten dann als Cluster mit automatischer Lastverteilung, Synchronisation und Redundanz (Ausfallsicherheit).

1. Bringen Sie zunächst nur die erste SecuLution Server Appliance in Betrieb.
2. Verbinden Sie den AdminWizard mit der ersten Appliance und führen in der GUI des AdminWizards unter “SecuLution Appliance” die IP Konfiguration für den oder die weiteren SecuLution Server Appliances durch:



3. Nehmen Sie nun, falls lizenziert, weitere SecuLution Server Appliances in Betrieb, indem Sie jeweils dasselbe OVA Image importieren, das Sie für die Inbetriebnahme der ersten SecuLution Server Appliance verwendet haben. Beim Start muss jeder weiteren SecuLution Server Appliance mitgeteilt werden, unter welcher IP-Adresse die erste SecuLution Appliance zu erreichen ist. Hierzu wählen Sie auf der Konsole das Boot-Menü aus und geben unter “multi-server setup” die IP-Adresse der bereits in Betrieb befindlichen ersten SecuLution Server Appliance an. Jede zusätzliche SecuLution Server Appliance wird nun automatisch und selbstständig folgende

Schritte durchführen:

a. per DHCP eine IP-V4 Adresse beziehen
b. die über das Boot-Menü angegebene IP-Adresse der ersten SecuLution Server Appliance kontaktieren und die IP-Konfiguration aller Server herunterladen
c. die IP-Adresse der zweiten SecuLution Server Appliance anpingen, um zu prüfen, ob die IP-Adresse der zweiten SecuLution Server Appliance frei ist (Ping ist nicht erfolgreich, folglich ist die zweite SecuLution Server Appliance noch nicht in Betrieb)
d. die IP-Konfiguration für die SecuLution Server Appliance aus Schritt b in der Appliance hinterlegen
e. rebooten
f. mit der ermittelten IP-Adresse in Betrieb gehen
g. die Datenbank mit den bestehenden SecuLution Server Appliances synchronisieren

4. Nehmen Sie ggf. weitere SecuLution Appliances wie in Schritt 3 beschrieben in Betrieb
5. ggf. kann nach Abschluss der Installation aller Instanzen des SecuLution Server Appliance Clusters ein Reboot der SecuLution Server Appliance notwendig sein, da die ersten SecuLution Server Appliances beim Boot die nachträglich in Betrieb genommenen SecuLution Server Appliance noch nicht erreichen konnte
6. Die SecuLution Server Appliance des Clusters booten mit leerer Datenbank (Whitelist) und daher im Lernmodus. Es werden in dieser Zeit also keine Programme verweigert. Spielen Sie eine ggf. vorhandene Datensicherung der bisherigen Appliance ein und schalten Sie den Lernmodus ab.

Grundkonfiguration

Führen Sie folgende Schritte bei der Erstinstallation von SecuLution durch

Installation des AdminWizards

Das Setup Programm des AdminWizards ist personalisiert und enthält bereits die Zertifikate für den Zugriff auf die SecuLution Appliance. Nach der Installation geben Sie die IP Ihrer SecuLution Appliance ein und loggen Sie sich mit dem Default-Passwort “password” ein.

Voraussetzungen des AdminWizards:

- .NET Framework 4.5.2 (evtl. auch die benötigten Komponenten innerhalb der Features aufführen)
- VC-redist_2017
- RSAT Tools (nur bei einmaliger Ersteinrichtung des RCM)
- Als Domänen-Admin Starten (nur bei einmaliger Ersteinrichtung des RCM)

Vor der erstmaligen Installation eines Agents

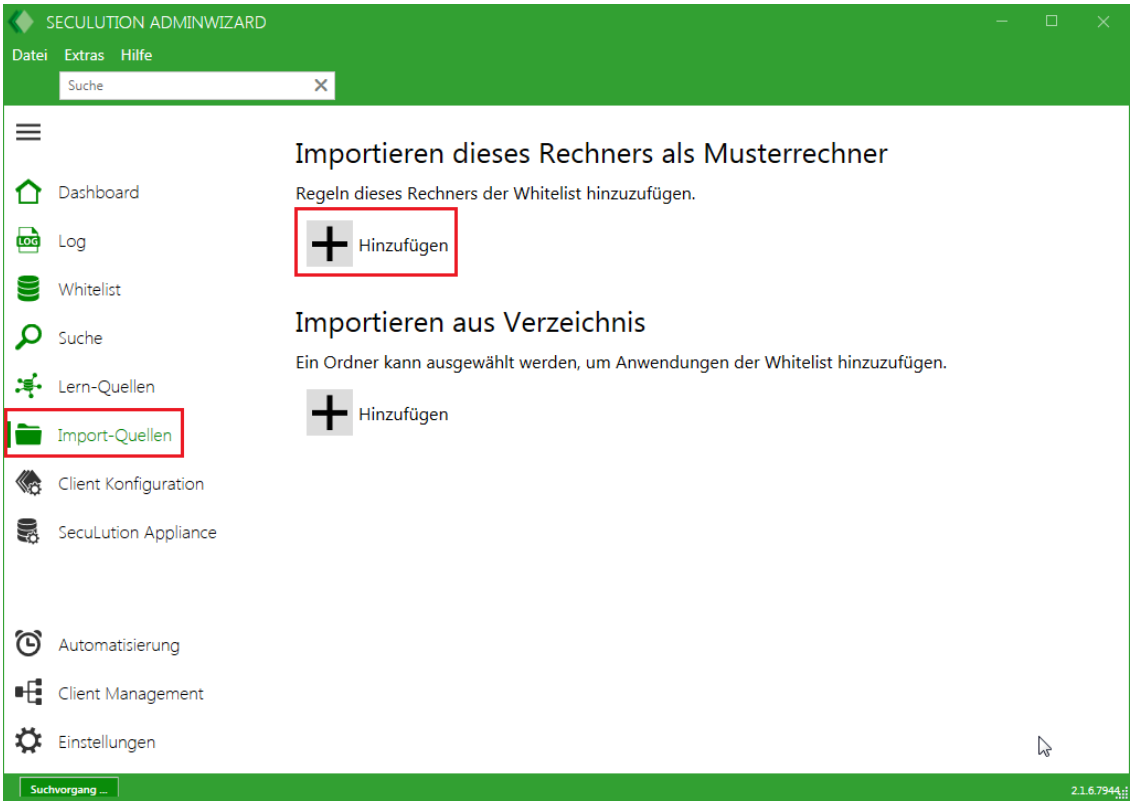
Bevor Sie einen SecuLution Agent zum ersten Mal installieren, sollten Sie auf dem Computer, auf dem Sie den Agent zum ersten Mal installieren, einen Musterrechner Import durchführen, damit die auf diesem Computer verwendete Software in der Whitelist erlaubt ist. Aktivieren Sie anschließend einen Lernmodus, damit auch Geräte und Software erfasst werden, die im Musterrechner Import nicht hinzugefügt werden konnten.

Musterrechner Import

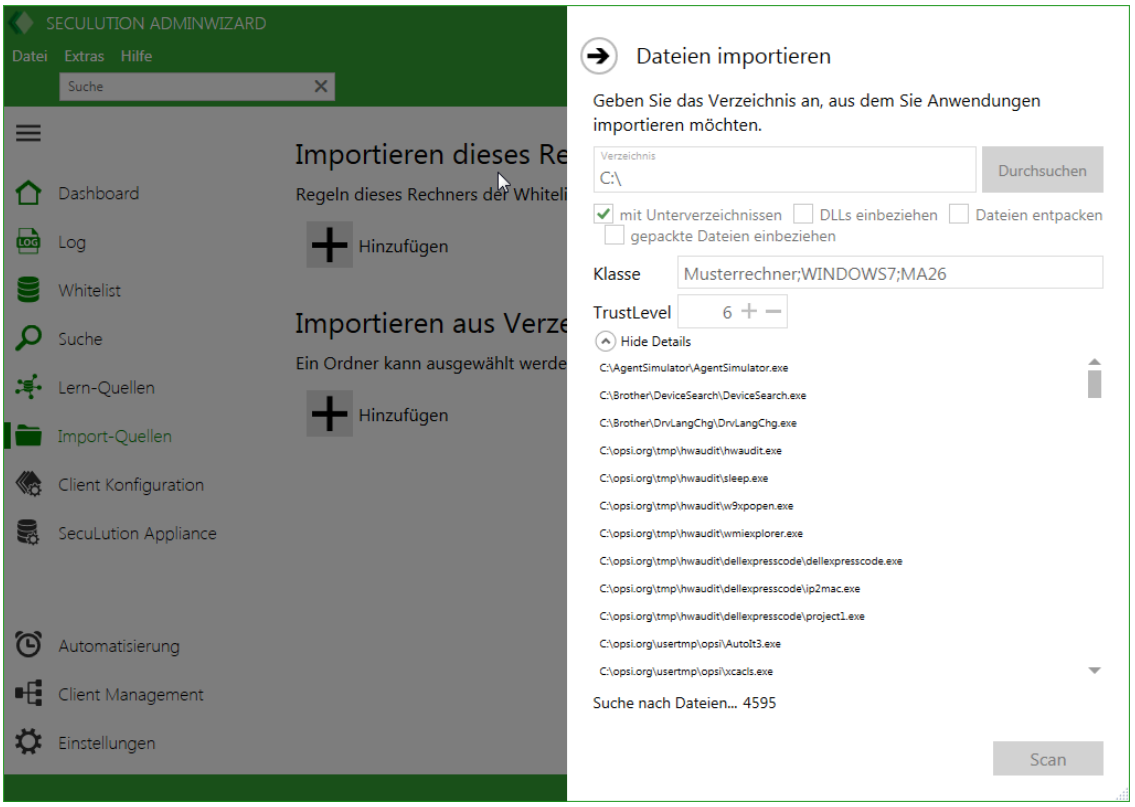
Setzen Sie Computer auf, auf denen nur vertrauenswürdige Software installiert ist (Musterrechner)
Erstellen Sie eine Liste der Betriebssysteme (OS), mit denen Ihre Benutzer arbeiten und die Sie später mit SecuLution sichern werden.

Erstellen Sie für jedes OS auf der Liste einen "Musterrechner", auf dem Sie nur garantiert vertrauenswürdige Datenquellen installieren. Je mehr garantiert saubere Software Sie auf diese Weise auf den Musterrechnern installieren, desto weniger Arbeit haben Sie später bei der Überprüfung der Abweichungen. Beachten Sie hierzu auch die FAQ.

Importieren Sie Software von vertrauenswürdigen Computern
Der einfachste Weg, um vertrauenswürdige Hashes von einem Musterrechner zu importieren, ist, den AdminWizard auf dem Musterrechner zu installieren und alle Dateien aus „C:\“ zu importieren. Hierzu wählen Sie im Tab “Import-Quellen” “Importieren dieses Rechners als Musterrechner” den +-Button “Hinzufügen”. Beachten Sie die FAQ hierzu.



Der AdminWizard wird nun die C:\ Partition des PCs scannen und alles in einer vorgegebenen Klasse in Ihre Whitelist importieren.



Lernmodus einschalten

Stellen Sie sicher, dass ein Lernmodus für eine ausreichende Dauer eingeschaltet ist (Tab “Lern-Quellen” - “Lern-Modi”).

Lern-Benutzer anlegen

Legen Sie einen Lern-Benutzer Account in Ihrem AD an.

AD Replikation

Führen Sie eine AD Replikation durch (Menü “Extras / Aktualisiere Active Directory Objekte”)

Lern-Benutzer einstellen

Wählen Sie den zuvor im AD angelegten Lern Benutzer Account als Lern-Benutzer aus (Tab “Lern-Quellen” “Lern-Benutzer”).

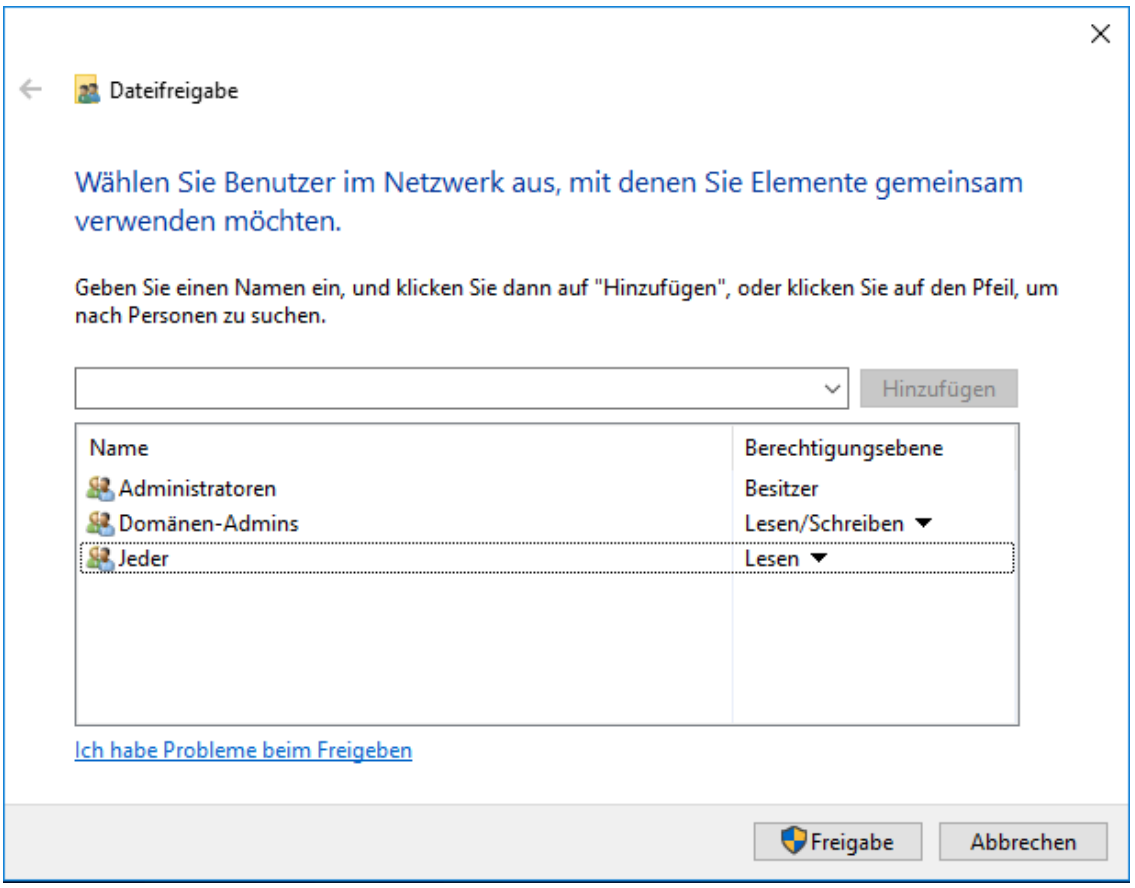
Einrichtung der Agent-Softwareverteilung

Wählen Sie das Tab “Client-Management” und klicken Sie ganz oben auf “RCM Status”. Der AdminWizard führt Sie durch die Einrichtung der Softwareverteilung.
Sie benötigen:

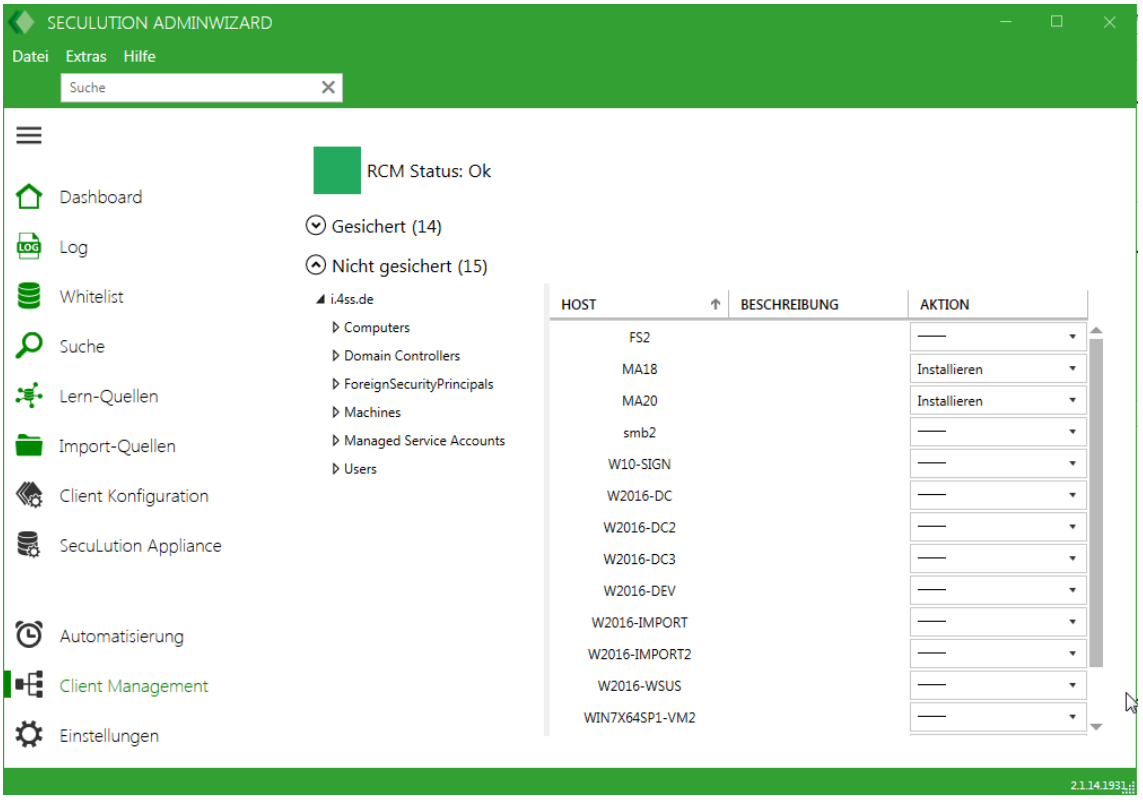
- die RSAT Tools müssen installiert und aktiviert sein
    - bis Windows 10 1809 als Installationspaket
    - ab Windows 10 1809 über die Aktivierung der Windows Features
- einen Domain-Admin Account
- einen UNC Pfad auf einem File-Server in Ihrem AD, auf dem die Agent Installationsdateien abgelegt werden

Die benötigten Freigabeeinstellungen und Berechtigungen für den RCM Freigabepfad:

- Domänen-Admins: Vollzugriff
- Jeder: Lesen / Ausführen



Wählen Sie dann unter den Computern “nicht gesichert” mit gedrückter UMSCHALT-Taste (Shift/Großschreibung) die Computer aus, auf denen Sie den SecuLution Agent installieren wollen:



Die Agent-Verteilung erfolgt automatisch beim Start des Rechners, sobald Windows die Gruppenrichtlinie auf den Computern anwendet.

Hashes zur Whitelist hinzufügen

In SecuLution wird alles verweigert, was nicht explizit erlaubt ist. Um Hashes von Software oder Geräten zur Whitelist hinzuzufügen, bietet der AdminWizard verschiedene Methoden zum Lernen und Importieren von vertrauenswürdigen Hashes an:

Hashes Lernen

“Lernen” ist das automatische Hinzufügen einen Hashes zur Whitelist ausgelöst durch eine Anfrage durch einen Agent.

Lernmodi

Um neue Hashes zu Ihrer Whitelist hinzuzufügen, können Sie einen automatischen Lernmodus verwenden.

Der Lernmodus ist eine Konfigurationsoption, die die SecuLution Appliance anweist, Hashes, die noch nicht in der Whitelist enthalten sind, zu lernen, anstatt sie abzulehnen. Beim Lernen wird ein Hash für den anfragenden Agenten zugelassen und der Whitelist hinzugefügt. Eine Überprüfung der Vertrauenswürdigkeit des Hashes findet nicht statt. Diese kann zu einem späteren Zeitpunkt nachgeholt werden. Es sind mehrere Lernmodi von verschiedenen Quellen möglich.

Während des Lernmodus lernt die SecuLution Appliance nur neue unbekannte Hashes, die von einem Agenten geprüft wurden. Hashes, die sich bereits in der Whitelist befinden, werden nicht gelernt, da sie bereits bekannt sind. Dies ist unabhängig davon, ob es für den Hash tatsächlich eine „Erlauben“-Aktion gibt. Somit ist es auch tatsächlich möglich, Hashes während des Lernmodus abzulehnen.

Lern-Benutzer (Permanent learn-user PLU)

Der "Lern-Benutzer” ermöglicht neue Software zum Regelsatz hinzuzufügen, indem das hinzuzufügende Programm mit den Berechtigungen eines dafür ausgesuchten Benutzeraccounts durchgeführt wird. (Rechtsklick auf die Software, "als anderer Benutzer ausführen"). Legen Sie eine neue globale Sicherheitsgruppe in Ihrem Active Directory an und nennen Sie diese z. B. "SecuLutionLernuser". Legen Sie einen oder mehrere neue Benutzeraccounts an, die später zur Installation neuer Software verwendet werden. Fügen Sie diese Accounts der Gruppe Administratoren und der zuvor angelegten Gruppe als Mitglieder hinzu. Nach einer AD Replikation wird dieser Account im AdminWizard unter Lern-Quellen -> Lern-Benutzer zur Auswahl zur Verfügung stehen.

TrustLevel Service (TLDB)

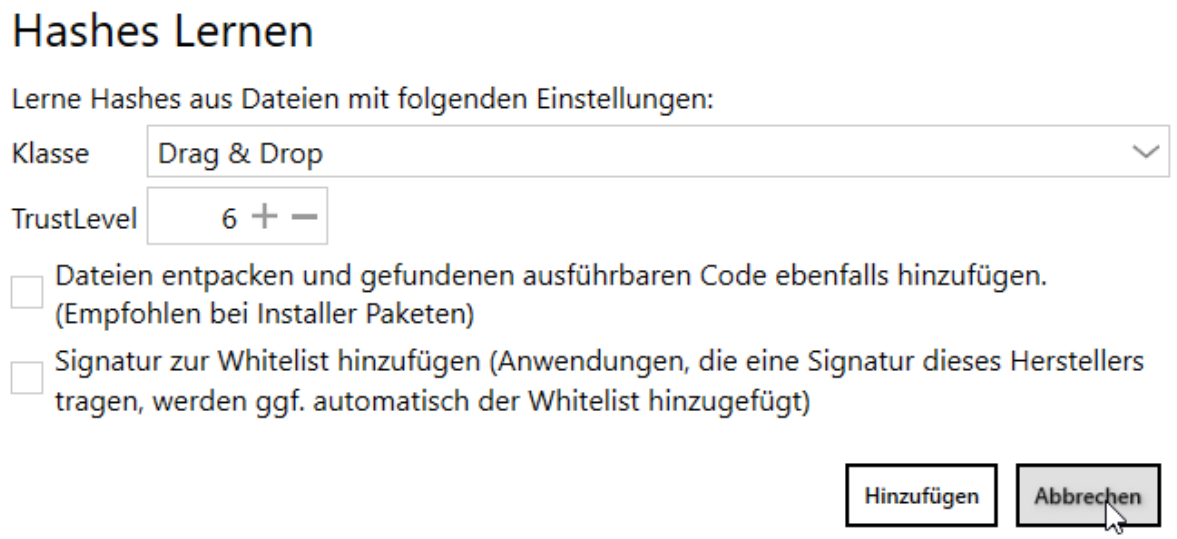
Siehe TrustLevel Datenbank (TLDB)
Über die Funktion “Ausnahmen hinzufügen” kann eine Liste von Dateinamen definiert werden, die explizit vom TLDB basierten Lernvorgang ausgenommen werden. Beispiel:
`*powershell*`
Bitte beachten Sie, dass die Ausnahmeerkennung ausschließlich auf den Dateinamen abzielt. Es ist wichtig zu berücksichtigen, dass der Dateiname der auszuführenden Datei leicht geändert werden kann. Dies hat zur Folge, dass diese Konfiguration in der Praxis leicht umgangen werden kann. Es sei jedoch darauf hingewiesen, dass dies keine Sicherheitsbedenken aufwirft, da die TLDB ohnehin nur Programme erlernt, die als vertrauenswürdig gelten.

Vertrauenswürdige Signaturen

Siehe Signaturen

Drag-and-drop

Sowohl Dateien als auch ganze Verzeichnisse können per Drag-and-drop in den AdminWizard gezogen werden:



Hashes Importieren

Importieren ist das (automatische) Hinzufügen von Hashes zur Whitelist aus Dateien, die der Administrator als vertrauenswürdig einstuft. Beachten Sie die FAQ hierzu.

Musterrechner Import

Durch einen Musterrechner Import werden alle Dateien dieses Computers in die Whitelist aufgenommen und als vertrauenswürdig eingestuft. Beachten Sie die FAQ hierzu.

Importieren aus Verzeichnissen

Durch Importieren aus Verzeichnissen können Updates oder Programmpakete manuell und automatisiert in die Whitelist übernommen werden. Beachten Sie die FAQ hierzu.

Log

Alarm in Regel umwandeln

Wird einmal ein Programm verweigert, kann der Administrator - nachdem er sich von der Vertrauenswürdigkeit der Software überzeugt hat - die Software mit Rechtsklick -> “Regel zur Whitelist hinzufügen” der Whitelist hinzufügen. Eine Mehrfachauswahl ist möglich.

Aufgaben automatisieren

Tab “Automatisierung” - SecuLution kann sich wiederholende Aufgaben automatisiert durchführen. Zur Einrichtung muss der AdminWizard mit einem Administrator-Account gestartet werden.

Datensicherung

Das Erstellen einer Datensicherung und das Wiederherstellen mit der Option, alle Daten in der DB mit den Daten aus der Datensicherung zu ersetzen, setzt die Informationen über die verwendeten Lizenzen zurück.

Whitelist bereinigen

Schalten Sie die automatische Bereinigung der Whitelist ein.

Active Directory Replikation

SecuLution repliziert die Informationen über Benutzer, Gruppen und Computer aus Ihrem AD.

WSUS Import

Vom Importieren von WSUS Updates wird seit Windows 10 Version 1809 abgeraten. WSUS Updates sind über den TLDB Service verfügbar.

Import aus Verzeichnissen

Der Import von Dateien aus Verzeichnissen kann automatisiert werden.

Durch Anlegen einer Datei `dateiname.importignore` kann eine einzelne Datei vom Import ausgenommen werden.
Durch Anlegen einer Datei `.SecuLutionImportIgnore.txt` in einem Unterverzeichnis des zu importierenden Verzeichnisses kann das gesamte Unterverzeichnis vom Import ausgenommen werden.

Maximales Dateialter (Monat)
Die Einstellung "Maximales Dateialter (Monate)" definiert den Zeitraum, für den der AdminWizard Dateien untersucht.

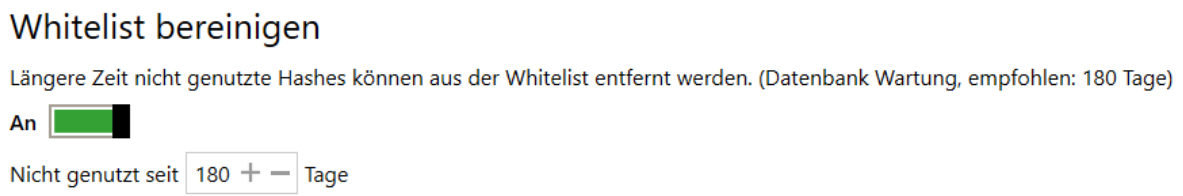
Beispiel:
Ein Wert von "0" (oder leer) bedeutet: ab sofort werden täglich alle Dateien importiert, unabhängig von ihrem Alter.

Ein Wert von "3" bedeutet: einmalig alle Dateien importieren, die innerhalb der letzten 3 Monate in diesem Verzeichnis abgelegt wurden und zusätzlich ab jetzt täglich alle Dateien, die seit der letzten Ausführung der Automatisierung neu sind.

Empfohlene Einstellungen

Whitelist bereinigen

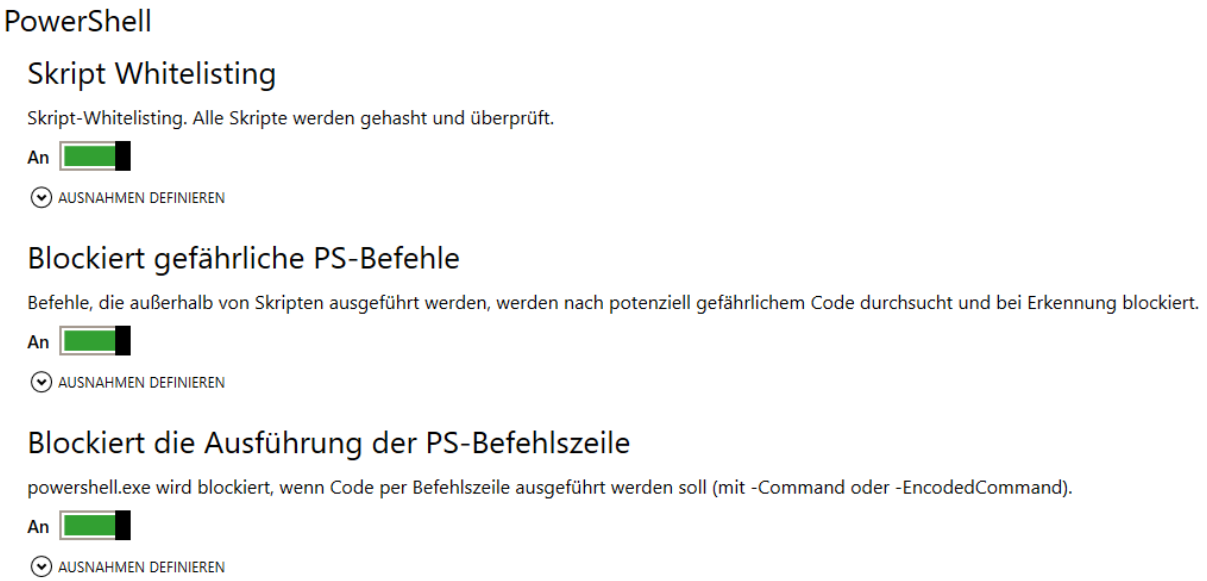
Keine Datenbank kann endlos Daten hinzufügen, daher empfehlen wir eine automatische Bereinigung der Datenbank um unbenutzte Hashes (empfohlen: 180 Tage):



PowerShell

SecuLution behandelt PowerShell Scripte (.ps1) wie ausführbare Programme, die zur Ausführung in der Whitelist als vertrauenswürdig eingestuft sein müssen (Voraussetzungen: AdminWizard => 2.0.54, Agent => 2.0.98, Appliance => 2.0.36). Auch sicherheitskritische PowerShell Befehlszeilen-Aufrufe und Befehle werden blockiert. Wir empfehlen, die Default-Einstellungen (alle Funktionen aktiv) unter “Client Konfiguration -> PowerShell Skript

Whitelisting” beizubehalten. Ausnahmen können sowohl für einzelne Programme konfiguriert werden, als auch für Computer (siehe Screenshot hier unter “AUSNAHMEN DEFINIEREN”)



Die in älteren Versionen von SecuLution empfohlenen Einschränkungen der Ausführung von PowerShell sind nicht mehr notwendig.

Auf Windows Server Versionen ist die PowerShell Prüfung erst ab Windows Server 2019 möglich, da ältere Windows Server Versionen die zur Restriktion benötigte Schnittstelle noch nicht bereitstellen.

Agent Verhalten im Offline Modus

Der Agent kommuniziert mit der SecuLution Appliance, solange diese erreichbar ist. Falls die SecuLution Appliance nicht erreichbar ist, verwendet der Agent eine lokale Kopie der Whitelist.

Für den Fall, dass der SecuLution Agent offline ist (SecuLution Appliance nicht erreichbar), und ein Hash verwendet werden soll, der nicht in der lokalen Whitelist auf dem Computer bekannt ist, wird die Konfigurationseinstellung "offline mode" verwendet.

Die folgenden Optionen stehen zur Verfügung:

- "Passwort":
  Der Benutzer erhält die Möglichkeit, ein Passwort einzugeben. Falls das korrekt ist, wird der Hash erlaubt und sowohl in den lokalen "Offline Cache" als auch in einen "Delta Cache" eingetragen.
- "Passwort nicht abfragen, alles erlauben":
  Der Agent wird keine Hashes blocken. Unbekannte Hashes werden aber dennoch sowohl in den lokalen "Offline Cache" als auch in einen "Delta Cache" eingetragen.
- "Challenge Response Verfahren":
  Der Benutzer wird aufgefordert, eine Zahlenkombination (Response) zu einer

angegebenen Zahlenkombination (Challenge) einzugeben. Der Benutzer kann diese Autorisierung z. B. telefonisch vom Administrator erbitten.

Wir empfehlen während der ersten 4 Wochen nach Installation von SecuLution die Einstellung "Passwort nicht abfragen, alles erlauben" zu wählen, danach "Challenge Response Verfahren" oder “Passwort”.

Support / Troubleshooting

Sollten Sie Hilfe bei der Benutzung von SecuLution benötigen, stehen wir Ihnen gern zur Verfügung.

FAQ

Bei technischen Fragen prüfen Sie bitte, ob wir diese bereits in unseren Support-FAQ beantwortet haben.

Welche Version?

Bitte arbeiten Sie immer mit den aktuellsten Versionen aller SecuLution-Komponenten. Wählen Sie dazu im AdminWizard den Menüpunkt “Hilfe / Auf neue Versionen prüfen”. Achten Sie auch darauf, dass auf den Client-Rechnern immer die aktuellste Version des Agenten installiert ist. Achten Sie insbesondere darauf, dass alle Installationen des AdminWizards die gleiche, aktuelle Version haben.

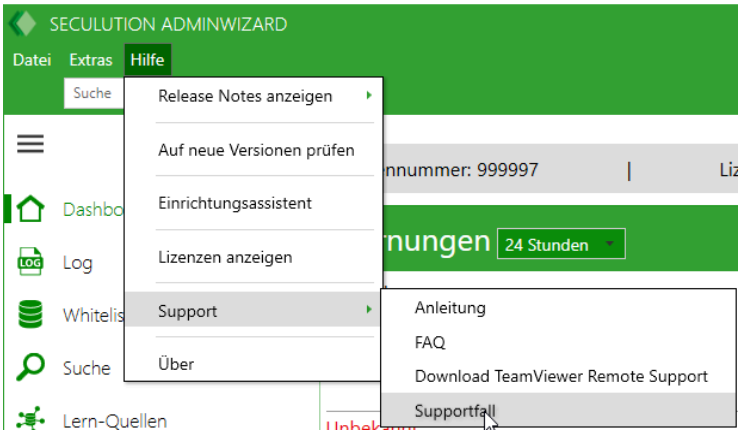
Kontaktaufnahme mit dem Support

Was braucht der SecuLution Support, um Ihnen helfen zu können?

Bitte prüfen Sie, ob Ihre Frage bereits in den FAQ beantwortet wird, bevor Sie ein neues Ticket erstellen.

Bei allen Problemen

Um ein neues Ticket zu eröffnen, wählen Sie im AdminWizard den Menüpunkt Hilfe / Support / Supportfall. Das SecuLution Ticketsystem im AdminWizard sammelt automatisch einige relevante Logs, anonymisiert diese DSGVO-konform und stellt sie dem Support zur Verfügung.



Achten Sie beim Ausfüllen der Felder auf eine aussagekräftige Beschreibung des Problems. Seien Sie bei der Fehlerbeschreibung möglichst detailliert: Was ist passiert und was hätte stattdessen passieren sollen? Fügen Sie einen Screenshot bei. Wenn möglich, geben Sie die Uhrzeit, den Computernamen und den Hash des Vorfalls an. Wenn Sie Schlussfolgerungen ziehen (z.B. “XY funktioniert nicht”), beschreiben Sie bitte auch, wie Sie zu dieser Annahme gekommen sind.

Bei AdminWizard-Problemen

Bevor Sie den Menüpunkt "Supportfall" aufrufen, stellen Sie bitte das Logging auf “Debug” (AdminWizard: Einstellungen -> LogLevel -> Debug), starten Sie den AdminWizard neu und reproduzieren Sie das Problem erneut. Stellen Sie sicher, dass Sie den AdminWizard als der Benutzer gestartet haben, unter dem das Problem aufgetreten ist.

Bei Agent-Problemen

Bitte fügen Sie dem Ticket zusätzlich alle Dateien aus `%programdata%\SecuLution\Agent` an.

Bei Appliance-Problemen

Bitte fügen Sie dem Ticket zusätzlich die Syslog Dateien an.

Bei RCM Problemen (Agent Verteilung)

Bitte fügen Sie dem Ticket zusätzlich alle Dateien aus `%programdata%\SecuLution\RCM` an.

Bei Automatisierungs-Problemen

1. AdminWizard als derjenige Benutzer starten, der auch die geplante Aufgabe für die Automatisierung startet
2. das Logging der Automatisierung einschalten (AdminWizard: Automatisierung -> Logs der Automatisierung -> an und Level “Debug”)
3. das Problem reproduzieren
4. im AdminWizard (gestartet als derjenige Benutzer, unter dem das Problem aufgetreten ist) den Supportfall eröffnen

Rohdaten statt nur Screenshots

Daten (Hashes), die durch Kopieren und Einfügen ermittelt werden sollen, bitte *NICHT nur als Screenshot* einreichen, sondern immer auch über die Zwischenablage (z.B. im AdminWizard Maus über Text halten, dann CTRL-C) in ein Textdokument einfügen (E-Mail oder readme.txt erzeugen), damit die Daten elektronisch auswertbar sind.

Große Datenmengen

Für große Datenmengen empfehlen wir, diese mit einem Passwort gesicherten ZIP zu packen und über einen Versender wie https://send.firefox.com, https://www.transfernow.net, https://www.transferxl.com oder Ähnlichen zu versenden. Den erzeugten Download-Link senden Sie uns bitte mit zugehöriger Ticket-Nummer im Betreff an support@seculution.com.

An wen wenden?

Direktkunden der SecuLution GmbH

Verwenden Sie die Funktion “Supportfall” im AdminWizard, so wird mit dem Button “ZIP hochladen zu SecuLution” automatisch ein Ticket eröffnet. Möchten Sie manuell ein Ticket eröffnen, senden Sie Ihre Anfrage an support@seculution.com
In dringenden Fällen können Sie unseren Support auch telefonisch unter +49 2922 9589210 erreichen.

Kunden von Vertriebspartnern der SecuLution GmbH

Wenden Sie sich an Ihren Vertriebspartner.

Links zu diesem Dokument

Diese Anleitung ist als Google Gocs Dokument und als html-Export verfügbar.