Allegro Packets
Network Multimeter

Installation Guide

Allegro Network Multimeter Virtual Edition

1. Wichtige Information vor der Installation 2

2. Systemanforderung 2

2.1 Hypervisor 2

2.2 Systemanforderungen der Virtual Machine: 2

3. Installation 2

3.1 VM-Image Download 2

3.2 OVF-Bereitstellung für VMware ESXi 3

3.3 OVF-Bereitstellung für VirtualBox 5

4. USB-Lizenz-Dongle installieren 7

4.1 VMware ESXi 7

4.2 VirtualBox 8

5. Die Virtual Machine anschalten 8

6. Lizenz 9

7. Pcap-Verarbeitung 10

8. Speicher für den Paket-Ringpuffer einrichten 11

8.1 VMware ESXi 11

8.2 VirtualBox 11

9. Weiterführende Konfiguration 12

9.1 Konfiguration der Verwaltungsschnittstelle 12

9.2 Zurücksetzen der Konfiguration und Firmware-Aktualisierung 12

9.3 Benachrichtigung über Firmware-Update 12

9.4 Zurücksetzen auf Werkeinstellung 13

10. Bedienungsanleitung 13

1. Wichtige Information vor der Installation

Die Allegro Virtual Edition ist für zwei Anwendungsfälle ausgelegt: Sie kann Pcaps unbegrenzter Größe forensisch untersuchen oder den Live-Verkehr von virtuellen Maschinen über einen virtuellen Mirror-Port oder ERSPAN analysieren.

Beachten Sie bitte, dass ein aktivierter Ringpuffer die IO-Performance für alle VMs verschlechtern kann. Es wird empfohlen, eine oder mehrere dedizierte HDDs oder SSDs für den Ringpuffer zu verwenden, um Nebenwirkungen auf andere VMs zu vermeiden.

2. Systemanforderung

2.1 Hypervisor

Die Allegro Virtual Edition unterstützt alle Virtualization Hypervisors, die 64bit x86 Linux Virtualization unterstützen. Allegro Packets hat die Lösung getestet auf:

- VMware ESXi 6.7.0 oder neuere Versionen
- VMware workstation (Windows, Linux)
- VMware Fusion (Mac)
- VirtualBox (Windows, Linux, Mac)
- KVM (Linux)

Dieser Installation Guide konzentriert sich auf VMware ESXi.

2.2 Systemanforderungen der Virtual Machine:

- x86 64bit Intel/AMD CPU mit SSE4.2-Unterstützung (seit 2011)
- 4 CPU-Kerne
- mindestens 2 GB RAM für die In-Memory-DB; je mehr, desto besser
- 20 GB freier Festplattenspeicher

3. Installation

3.1 VM-Image Download

Laden Sie das neueste VM-Image als Zip-Datei herunter:

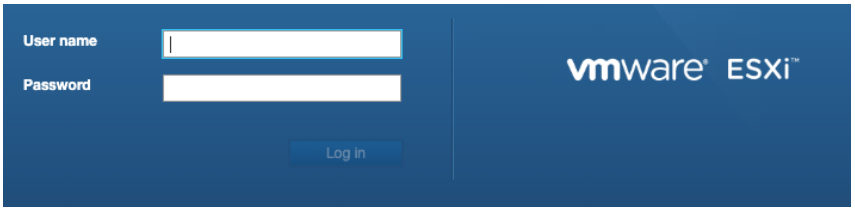
https://support.allegro-packets.com/multimeter/vm-images/

Bitte kontaktieren Sie allegro-packets.com/support oder Ihren Reseller für das Passwort zum Allegro Virtual Edition Installation-Zip-Archiv.

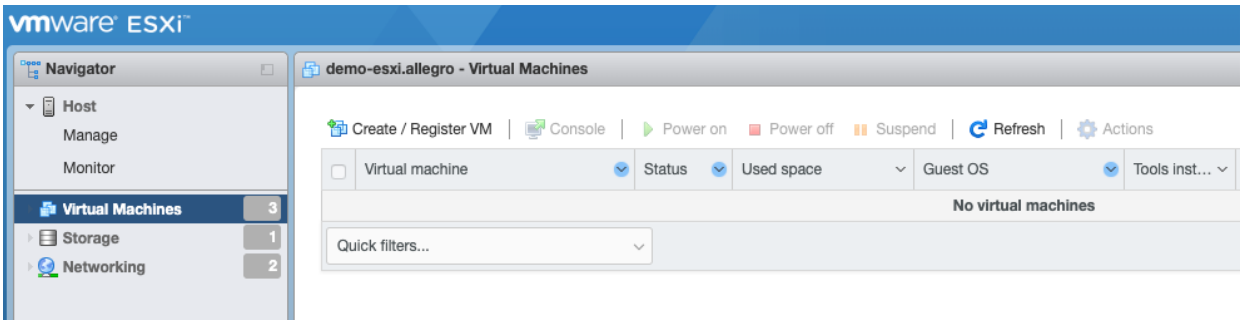
Entpacken Sie das Zip-Archiv. Es sollte folgende Dateien enthalten: "allegro-multimeter.ovf", "allegro-multimeter.vmdk" und "allegro-multimeter-virtualbox.ovf".

3.2 OVF-Bereitstellung für VMware ESXi

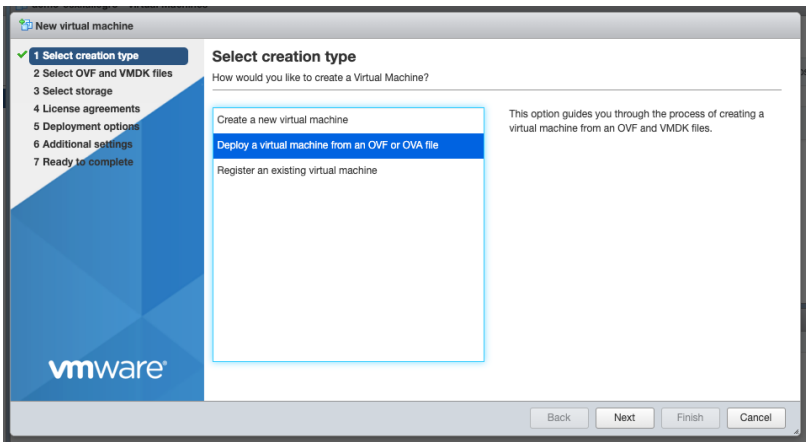
Melden Sie sich bei VMware ESXi an.



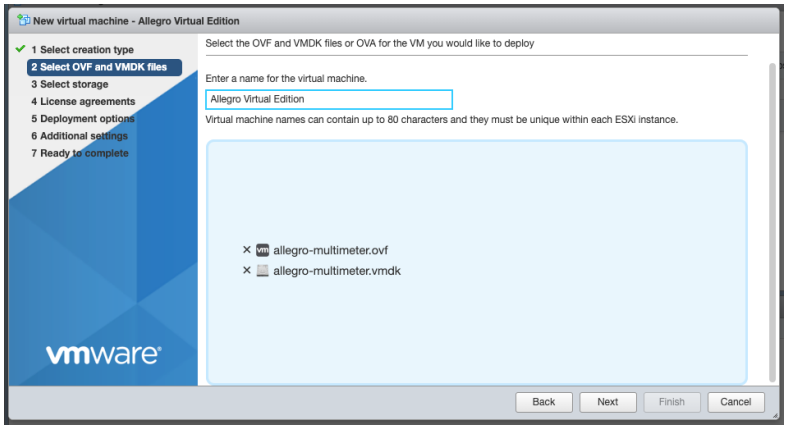
Sobald Sie sich angemeldet haben, navigieren Sie zu "Virtual Machines".



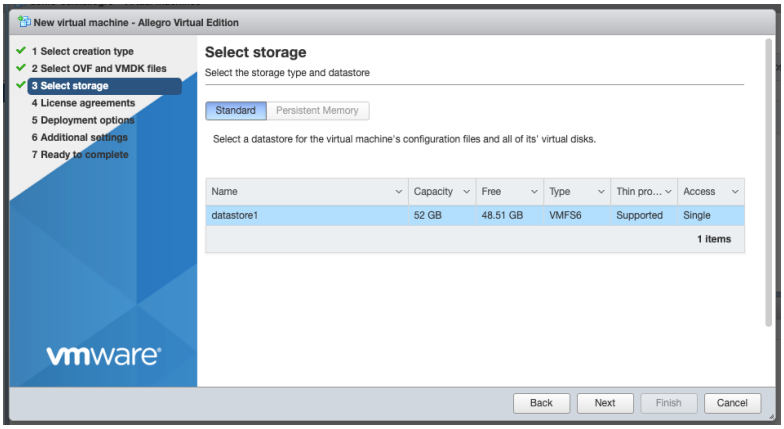
Erstellen Sie eine neue VM mit "Create VM / Register VM" und wählen Sie die Option "Deploy a virtual machine from an OVF or OVA file".



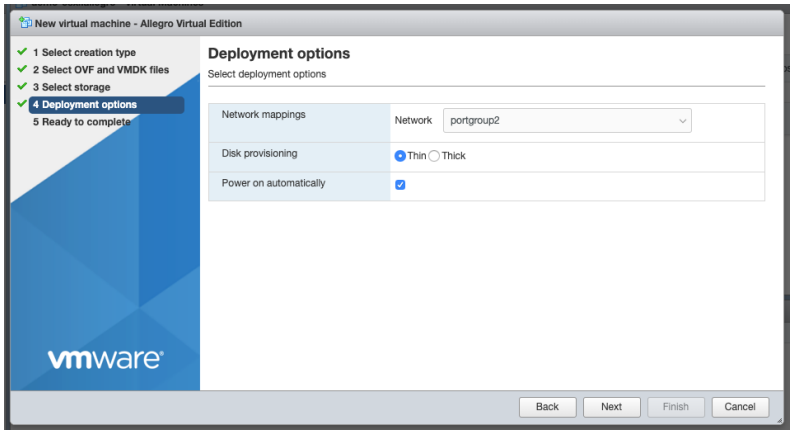
Drücken Sie "Next". Geben Sie nun einen Namen für die Allegro Virtual Edition ein und ziehen Sie die zwei Dateien in das Fenster. Drücken Sie anschließend auf "Next".



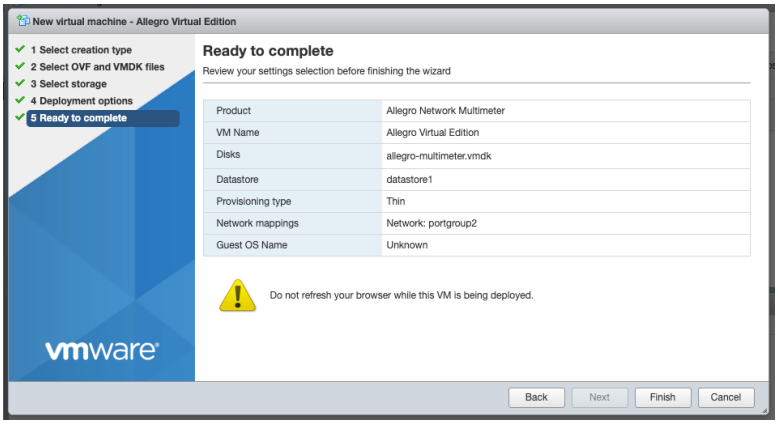
Wählen Sie Ihren Datenspeicher für das Allegro Network Multimeter. Dieser Speicher wird als Boot-Partition und zur Speicherung der Konfiguration der Allegro Virtual Edition verwendet und benötigt keine Hochgeschwindigkeitsfestplatte. Es wird nicht für den Paket-Ringspeicher benutzt.



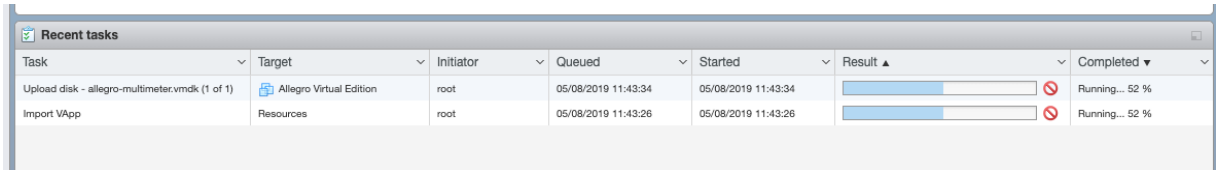
Mit den Bereitstellungsoptionen können Sie die Netzwerkzuordnung für den MGT-Port und die Festplatten-Provisionierung auswählen.



Bitte überprüfen Sie alle Optionen in der nächsten Dialogbox und drücken Sie auf "Finish", wenn alles in Ordnung ist.

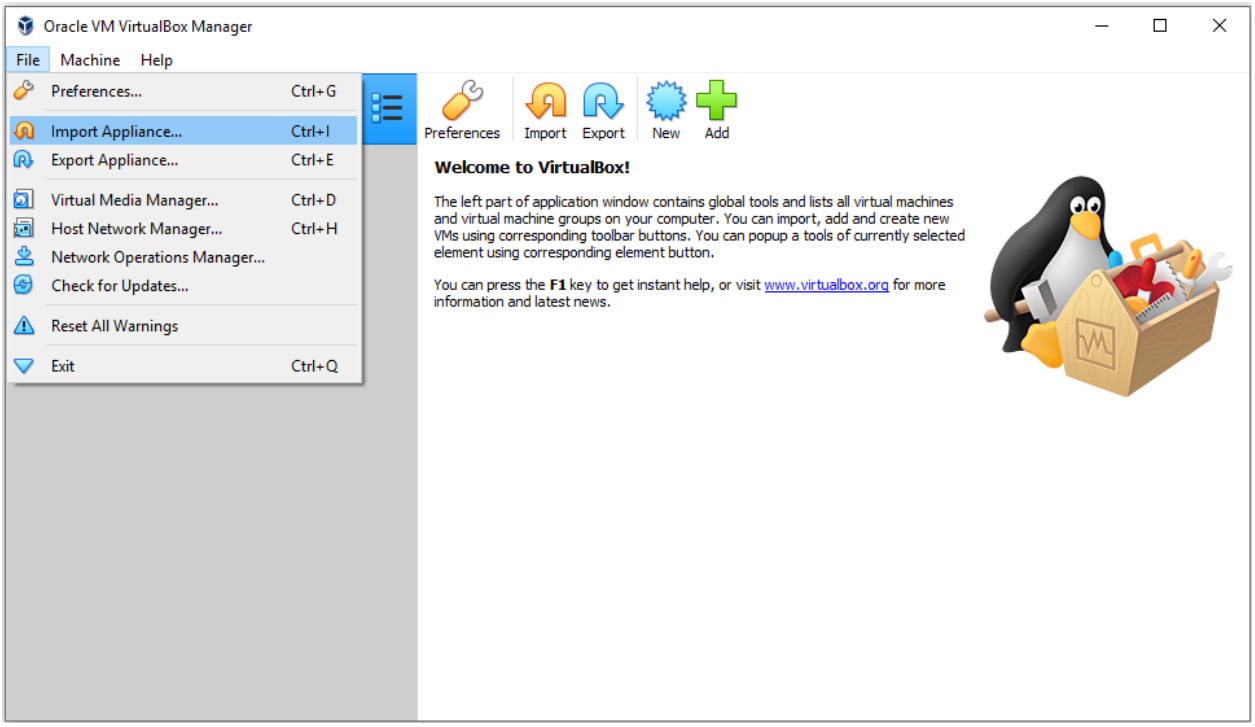


Der Upload und der Import der Allegro Virtual Edition beginnt. Bitte haben Sie etwas Geduld, bis dieser abgeschlossen ist.

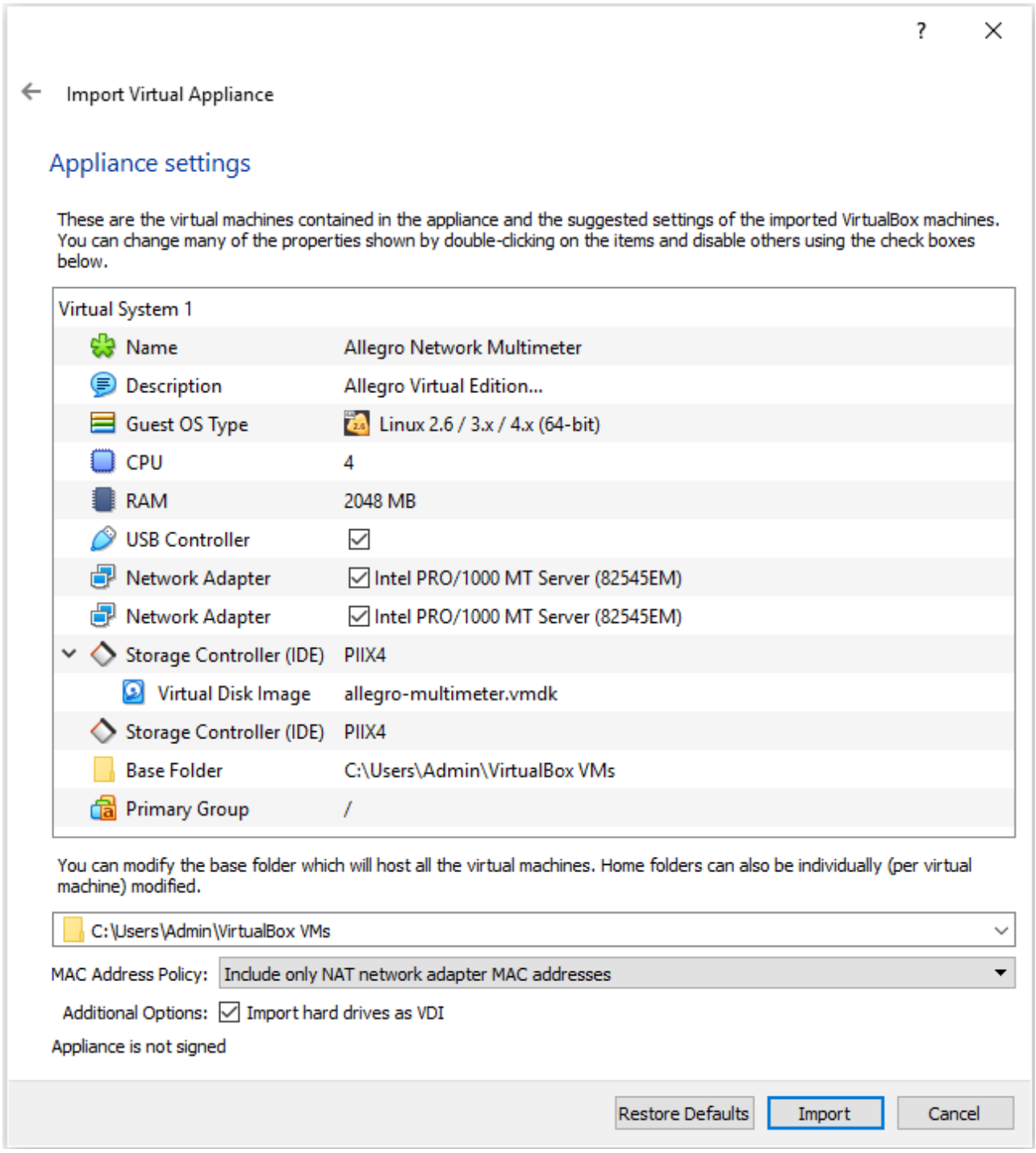


3.3 OVF-Bereitstellung für VirtualBox

Starten Sie die VirtualBox und wählen Sie aus dem Menü "File" → "Import Appliance " aus.

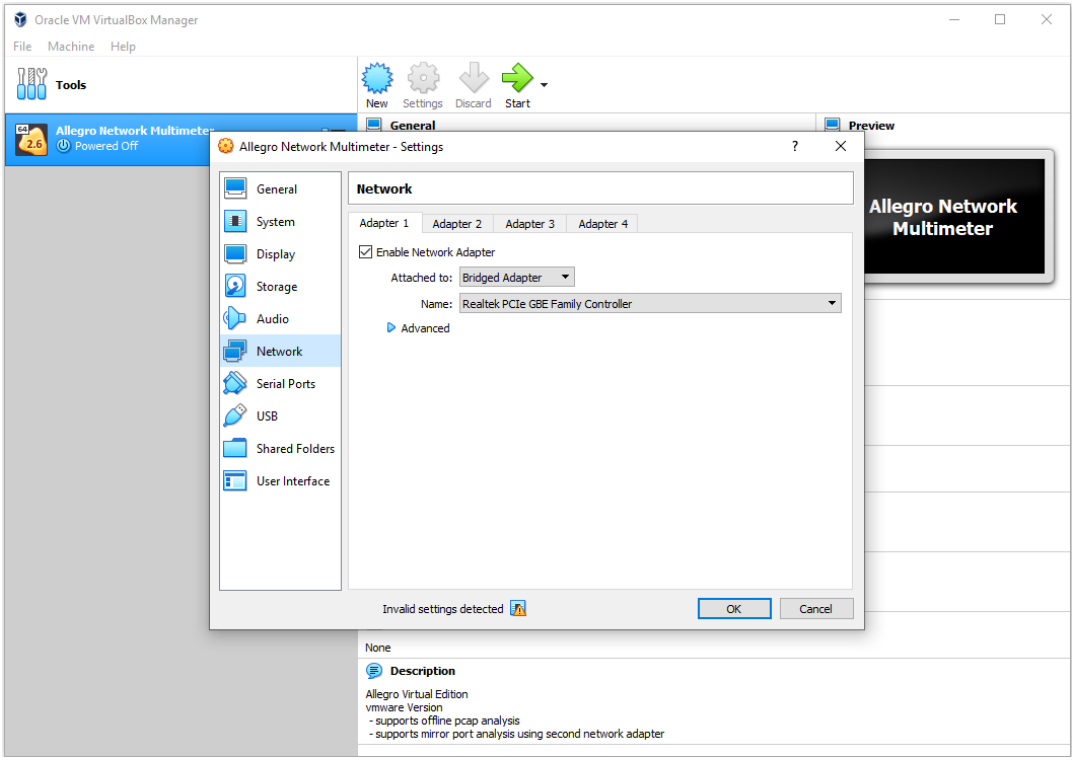


Klicken Sie in der nächsten Dialogbox auf die Verzeichnis-Schaltfläche, navigieren Sie zu dem extrahierten Zip-Archiv und wählen Sie "allegro-multimeter-virtualbox.ovf" aus. Klicken Sie dann auf "Next". Es wird ein Dialogfeld mit den Einstellungen der virtuellen Appliance geöffnet.



Überprüfen Sie als Nächstes den Speicherort der Dateien der Virtual Machine. Wenn Sie damit fertig sind, klicken Sie auf "Import".

Wählen Sie nun die neue virtuelle Maschine "Allegro Network Multimeter" aus. Klicken Sie auf "Settings" und wählen Sie "Network". Die Allegro Network Multimeter VirtualBox Einstellungen definieren standardmäßig zwei Netzwerkadapter. Einer davon wird als MGMT-Schnittstelle verwendet, der andere als Mess-Port. Stellen Sie sicher, dass für die Adapter 1 und 2 der richtige Name des Host-Netzwerkadapters ausgewählt wurde (z.B. für Windows: "Realtek PCIe GBE Family Controller").

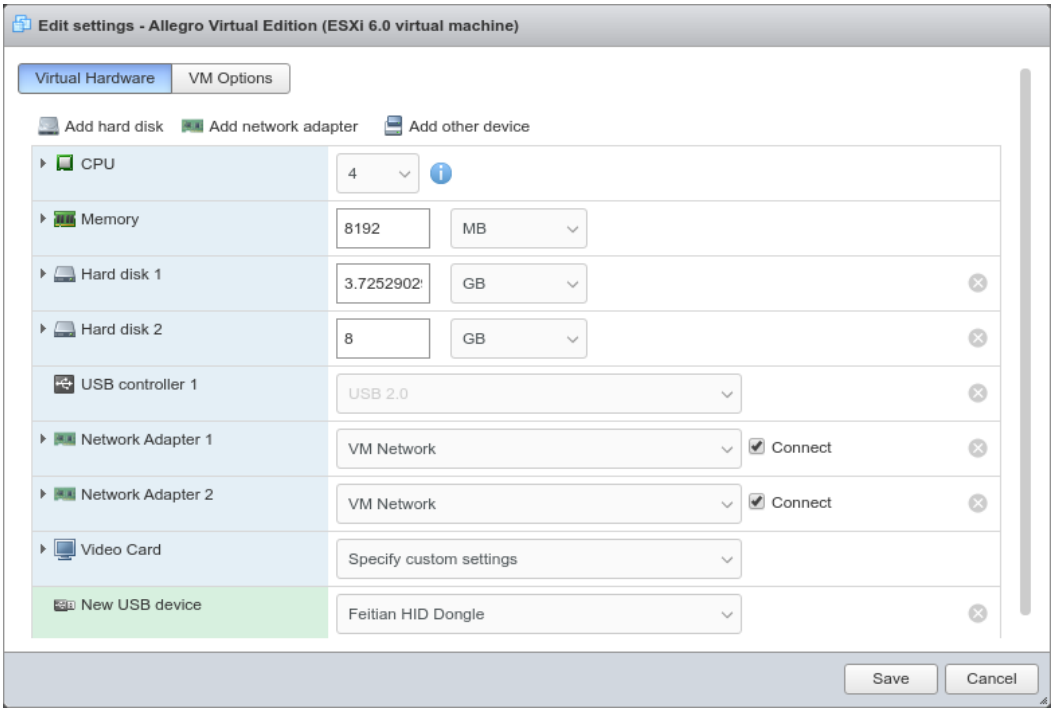


4. USB-Lizenz-Dongle installieren

Wenn die Allegro Virtual Edition mit einem USB-Lizenz-Dongle ausgeliefert wird, stecken Sie diesen in einen unbenutzten USB-Port des VM-Hosts. Der Dongle muss mit der Virtual Machine verbunden sein.

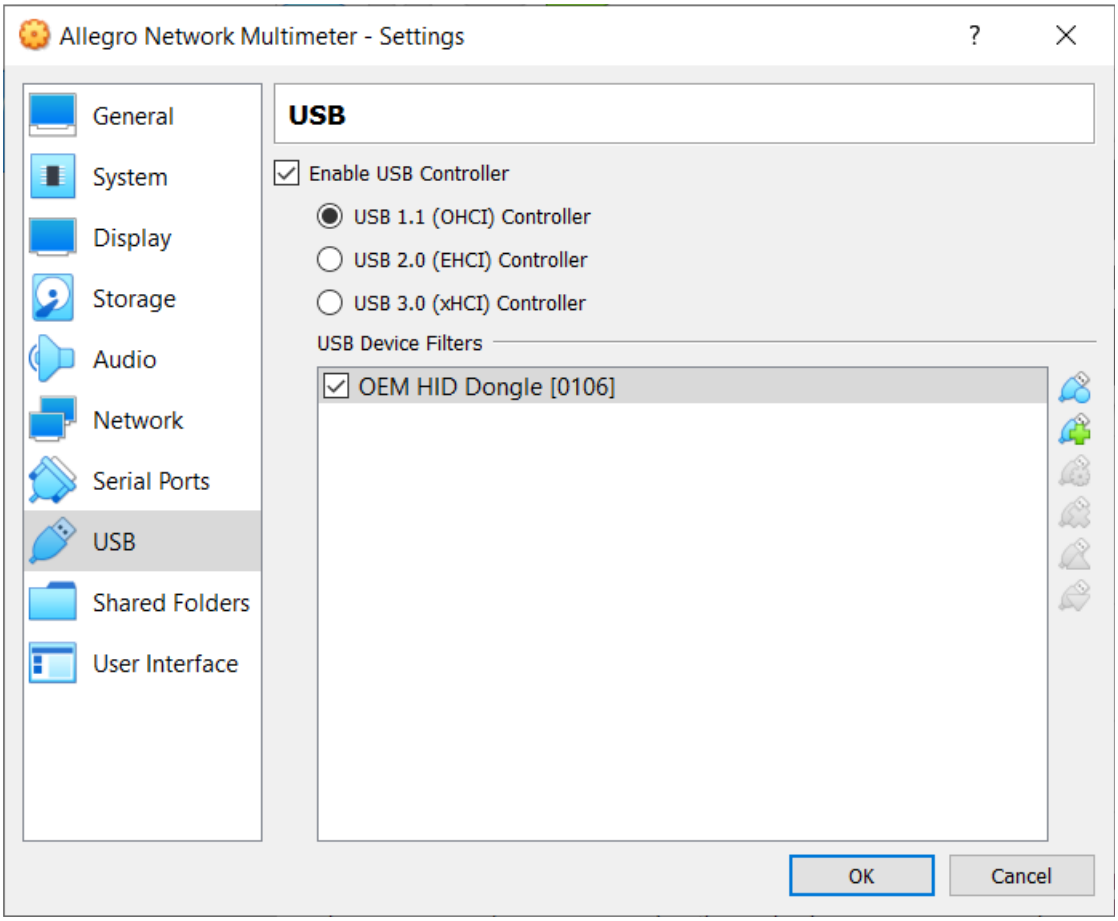
4.1 VMware ESXi

Drücken Sie im ausgeschalteten Zustand im VMware ESXi-Host auf "Edit" und klicken Sie auf "Add other device". Wählen Sie nun "USB device". In der Hardware-Liste erscheint unten ein neuer Eintrag. Wählen Sie hier "Feitian HID Dongle" oder Ähnliches aus.



4.2 VirtualBox

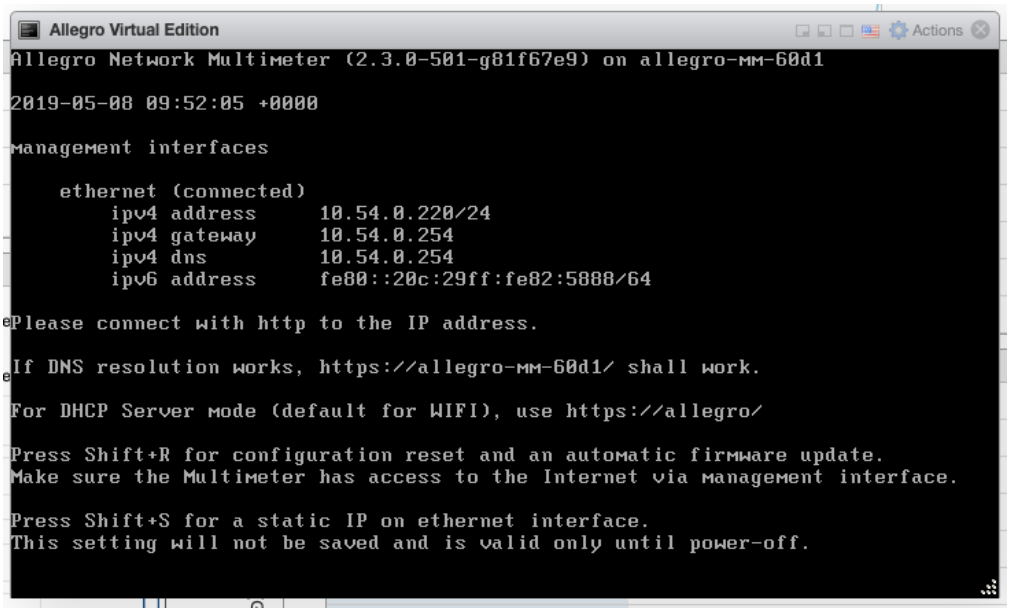
Klicken Sie im Einstellungsdialogfeld auf "USB" und verwenden Sie die zweite Schaltfläche auf der rechten Seite, um ein USB-Gerät hinzuzufügen. Wählen Sie "OEM HID Dongle" aus der Liste.



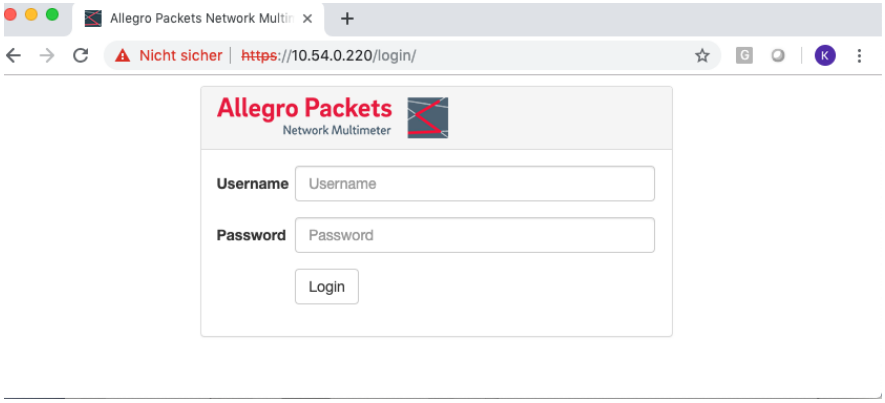
5. Die Virtual Machine anschalten

Schalten Sie die virtuelle Maschine ein, wenn der Import erfolgreich abgeschlossen ist. Die Allegro Virtual Edition startet, bereitet die Installation vor und startet einmal neu.

Die VM sucht eine IP-Adresse per DHCP am MGT-Port. Überprüfen Sie die Konsolenausgabe auf eine zugewiesene IP-Adresse.



Sie können sich nun mit der IP-Adresse Ihres Browsers verbinden, in unserem Fall: https://10.54.0.220/. Der Browser zeigt eine Zertifikatswarnung an. Akzeptieren Sie diese, um zum Anmeldebildschirm zu gelangen.



Verwenden Sie diese Anmeldedaten: Benutzer "admin" und Passwort "allegro".

6. Lizenz

Wenn die Allegro Virtual Edition mit einem USB-Lizenz-Dongle ausgeliefert und korrekt installiert wurde, sollte Ihr Allegro Network Multimeter einwandfrei funktionieren.

Die Seriennummer der Allegro Virtual Edition wäre z.B. "Dongle: 1234567890" und wird im Seriennummernfeld unter "Settings" → "License upload" angezeigt. Falls sie dort nicht angezeigt wird, obwohl der Dongle korrekt installiert wurde, kontaktieren Sie bitte den Support von Allegro Packets.

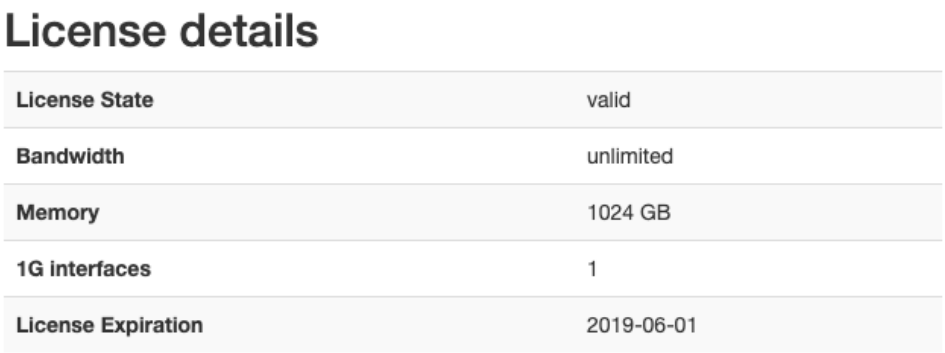
Wenn die Allegro Virtual Edition nicht mit einem USB-Lizenz-Dongle ausgeliefert wurde, befolgen Sie folgende Schritte. In der Web-Oberfläche wird eine Warnung angezeigt, dass die Allegro Virtual Edition noch nicht über eine Lizenz verfügt.

Navigieren Sie zu "Settings" → "License upload" und senden Sie die System-Seriennummer an

testlicense@allegro-packets.com.

Allegro Packets wird eine Testlizenz ausstellen, die mit dem "Upload new License"-Button installiert werden kann.

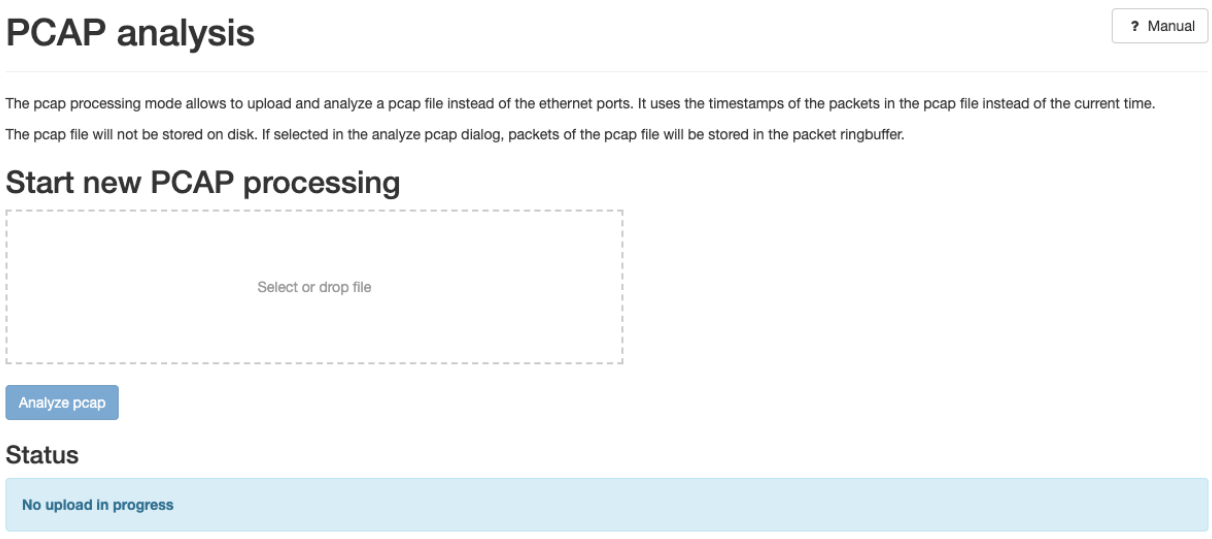
Sobald die Testlizenz angewendet wird, werden Ihnen die Lizenzdetails angezeigt:



Die VM ist jetzt bereit, Pcap-Dateien zu verarbeiten.

7. Pcap-Verarbeitung

Zur Verarbeitung von Pcap-Dateien navigieren Sie zu "Generic" → "Pcap analysis".



Ziehen Sie eine Pcap-Datei auf die Webseite und drücken Sie "Analyze pcap". Die Allegro VM wird dieses Pcap in Echtzeit verarbeiten, wenn dieses in die VM hochgeladen wird.

Sie können sofort nach der Einrichtung mit dem Hochladen der Pcap-Datei beginnen.

8. Speicher für den Paket-Ringpuffer einrichten

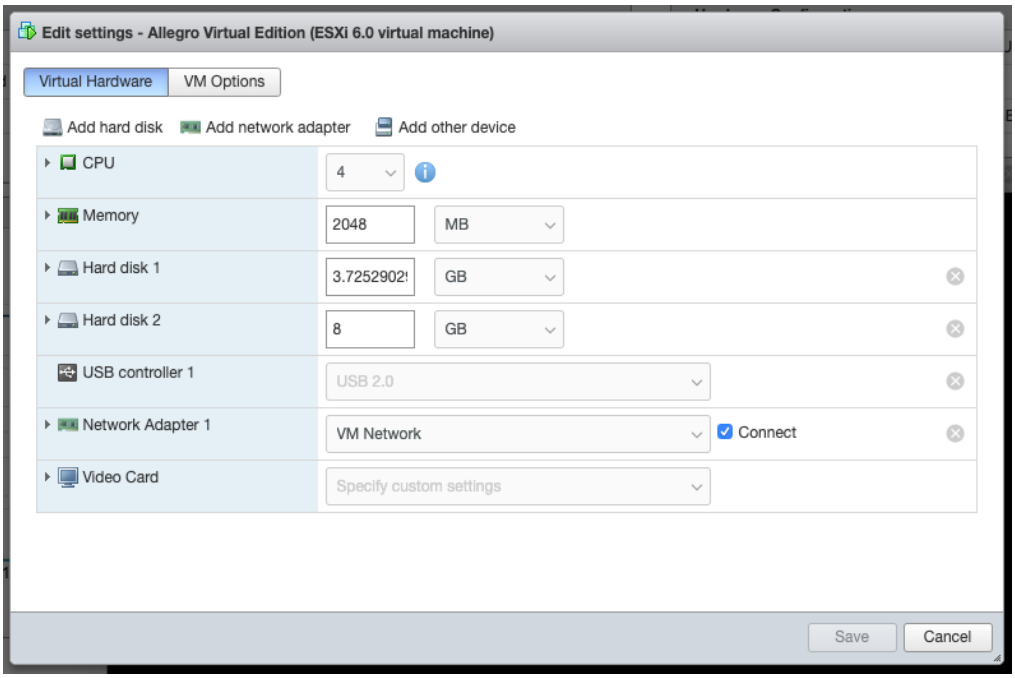
Standardmäßig erfasst die Allegro Virtual Edition die Pakete nicht im Ringpuffer und erlaubt keine Extraktion von Pcap-Dateien.

WARNUNG: Da der Ringpuffer bei der Aufzeichnung von Paketen auf die Festplatte hohe Plattenlasten verursachen kann, wird empfohlen, dedizierte Festplatten oder SSDs für den Ringpuffer zu verwenden, auch wenn dieser über USB3 angeschlossen ist. Wenn der Ringpuffer auf der gleichen Festplatte wie andere kritische Prozesse, wie z.B. einer Datenbank, verwendet wird, kann die Allegro Virtual Edition die Festplatten-Performance reduzieren.

Sie müssen das Allegro Network Multimeter ausschalten, um eine neue Festplatte anzuschließen.

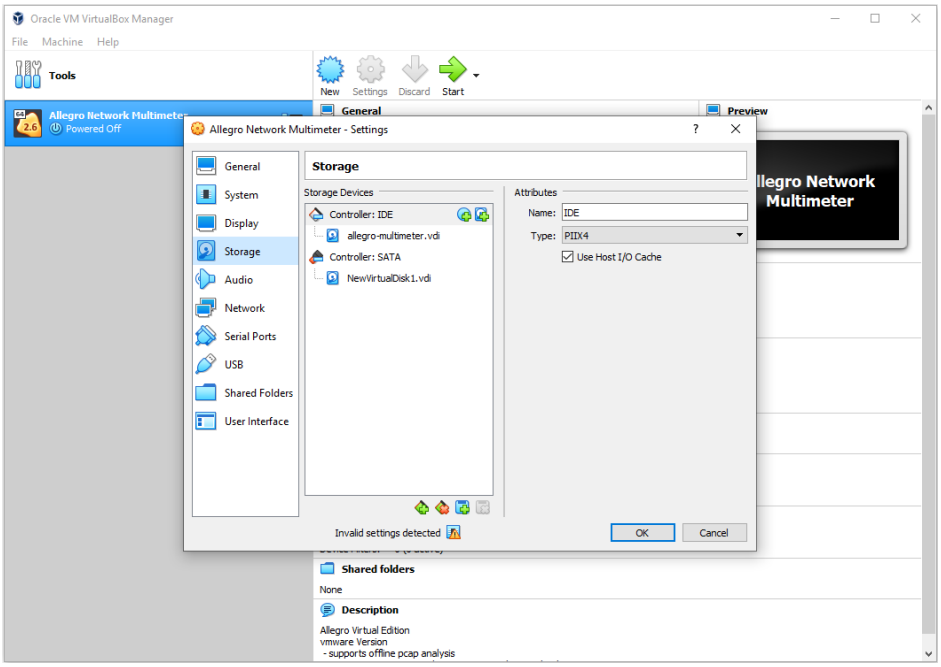
8.1 VMware ESXi

Drücken Sie im ausgeschalteten Zustand im VMware ESXi-Host auf "Edit" und fügen Sie eine neue Festplatte hinzu.



8.2 VirtualBox

Gehen Sie bitte auf die Seite "Storage". Fügen Sie einen virtuellen SATA-Controller und eine daran angeschlossene Festplatte hinzu. Wählen Sie entweder eine bereits vorhandene aus oder erstellen Sie eine neue Festplatte.



9. Weiterführende Konfiguration

9.1 Konfiguration der Verwaltungsschnittstelle

Sie können die Verwaltungsschnittstelle konfigurieren, indem Sie die Webschnittstelle unter "Settings" → "Management interfaces" aufrufen. Die verfügbaren Optionen sind im Online-Handbuch beschrieben, auf das Sie über die Webschnittstelle zugreifen können.

9.2 Zurücksetzen der Konfiguration und Firmware-Aktualisierung

Das Zurücksetzen der Konfiguration stellt die Konfiguration auf die Werkseinstellungen zurück.

- Webschnittstelle: Gehen Sie zum Menü "Settings" → "Administration" und klicken Sie auf "Reset system configuration". Alle Einstellungen einschließlich der Netzwerkkonfiguration werden auf die Werkseinstellungen zurückgesetzt.
- Boot-Menü: Folgen Sie den Anweisungen im Abschnitt 9.4 Werkseinstellungen.
- Konsole: Drücken Sie in der Konsolenausgabe der Allegro Virtual Edition "Shift+R". Nach erfolgreichem Reset und Update schaltet sich das Allegro Network Multimeter aus. Andernfalls bleibt es eingeschaltet. Kontrollieren Sie in diesem Fall die Konsolenausgabe auf Fehlermeldungen.

9.3 Benachrichtigung über Firmware-Update

Release-Information per E-Mail

Mit jedem Release erhalten Sie von Allegro Packets eine E-Mail mit Release Notes und einem Link zum Herunterladen des Updates. Wenn Sie in diese Mailing-Liste aufgenommen werden möchten, nutzen Sie bitte das Support-Formular unter allegro-packets.com/support und geben Sie Ihre Allegro Seriennummer ('Info' → 'System Info' → 'System ID') mit an.

Aktualisierung über die Allegro Network Multimeter Webschnittstelle

Starten Sie Ihr Allegro Network Multimeter und klicken Sie auf "Einstellungen" auf der linken Seite des Menüs und dann auf "Firmware Updates". Klicken Sie auf "Auf neue Firmware prüfen" und das Allegro Network Multimeter zeigt Ihnen an, ob eine neue Version zum Download zur Verfügung steht. Wenn ja, können Sie sich entscheiden, diese direkt auf das Gerät herunterzuladen.

Zusätzlich bietet diese Seite eine Übersicht über alle verfügbaren Versionen an. Um die neue Version zu starten, klicken Sie auf "Aktivieren".

9.4 Zurücksetzen auf Werkeinstellung

Der Factory Reset löscht die gesamte Systeminstallation und stellt die Firmware auf die Version zurück, die ursprünglich mit dem Allegro Network Multimeter ausgeliefert wurde.

- Schalten Sie die Allegro Virtual Edition ein.
- Nach der Initialisierung erscheint ein Boot-Menü. Wählen Sie "Factory reset" und drücken Sie Enter. Oder wählen Sie "Configuration reset", um die Konfigurationseinstellungen nur unter Beibehaltung der aktuellen Firmware-Installation zurückzusetzen.
- Die Allegro Virtual Edition startet, setzt alles auf die Werkseinstellungen zurück und startet erneut.
- Das Allegro Network Multimeter ist nun auf die Werkseinstellungen zurückgesetzt.

10. Bedienungsanleitung

Auf das Gerätehandbuch kann über die Webschnittstelle zugegriffen werden. Jeder Webabschnitt enthält eine Schaltfläche für den Zugriff auf die kontextspezifische Dokumentation. Das vollständige Handbuch kann durch Klicken auf den Link "Manual" im Menü geöffnet werden.

 © Rev 2020-08 All rights reserved