

Installation und Konfiguration von Secure Endpoint Virtual Private Cloud

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [VPC-Bereitstellung](#)
- [VM-Installation](#)
- [Erste Einrichtung der Admin-Schnittstelle](#)
- [Erstkonfiguration des vPC über die Web-GUI](#)
- [Konfiguration](#)
- [Services](#)
- [AirGap-Aktualisierungspaket](#)
- [Problem #1 - Erschöpfter Platz im Datenspeicher](#)
- [Problem #2 - Altes Update](#)
- [Grundlegende Fehlerbehebung](#)
- [Problem #1 - FQDN und DNS-Server](#)
- [Problem #2 - Problem mit Stammzertifizierungsstelle](#)

Einleitung

In diesem Dokument wird die erfolgreiche Bereitstellung von Virtual Private Cloud (VPC) auf Servern in der ESXi-Umgebung beschrieben und der Schwerpunkt darauf gelegt. Weitere Dokumente wie Schnellstartanleitung, Bereitstellungsstrategie, Berechtigungsleitfaden, Konsole und Administratoranleitung finden Sie auf dieser Website unter [Dokumentation](#)

Beitrag von Roman Valenta, Cisco TAC Engineers.

Voraussetzungen

Anforderungen:

VMware ESX 5 oder höher

- Cloud-Proxy-Modus (nur): 128 GB RAM, 8 CPU-Kerne (2 CPUs mit je 4 Kernen empfohlen), mindestens 1 TB freier Festplattenspeicher im VMware-Datenspeicher
- Laufwerkstyp: SSD für Luftspaltmodus erforderlich und für Proxy empfohlen
- RAID-Typ: Eine RAID-10-Gruppe (Stripespiegelung)
- Mindestgröße des VMware-Datenspeichers: 2 TB
- Minimaler zufälliger Datenspeicher-Lesevorgang für die RAID-10-Gruppe (4.000): 60.000 IOPS
- Minimale zufällige Schreibvorgänge für Datenspeicher für die RAID-10-Gruppe (4.000 U/min): 30.000 IO/s

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Grundkenntnisse im Umgang mit Zertifikaten.
- Grundkenntnisse der DNS-Einrichtung unter DNS-Server (Windows oder Linux)
- Installation einer OVA-Vorlage (Open Virtual Appliance) in VMWare ESXi

In dieser Übung verwendet:

VMware ESX 6.5

- Cloud-Proxy-Modus (nur): 48 GB RAM, 8 CPU-Kerne (2 CPUs mit je 4 Kernen empfohlen), mindestens 1 TB freier Festplattenspeicher im VMware-Datenspeicher
- Laufwerkstyp: SATA
- RAID-Typ: Ein RAID 1
- Mindestgröße des VMware-Datenspeichers: 1 TB
- MobaXterm 20.2 (Multi-Terminal Programm ähnlich PuTTY)
- Cygwin64 (Wird zum Herunterladen des AirGap-Updates verwendet)

Zusätzlich

- Zertifikat, das Sie entweder mit openssl oder XCA erstellen
- DNS-Server (Linux oder Windows) In meinem Labor habe ich Windows Server 2016 und CentOS-8 verwendet
- Windows VM für unseren Testendpunkt
- Lizenz

Wenn Ihr Speicher unter 48 GB RAM auf Version 3.2+ VPC unbrauchbar werden.

Hinweis: Die Private Cloud OVA erstellt die Festplattenpartitionen, sodass sie nicht in VMware.server angegeben werden müssen, der den Hostnamen der sauberen Schnittstelle auflöst. ⚠

Weitere Informationen zu den versionsspezifischen Hardwareanforderungen finden Sie im [Datenblatt](#) zur [VPC-Appliance](#).

Hinweis: Die Informationen in diesem Dokument stammen von den Geräten in einer bestimmten Laborumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen. ⚠

VPC-Bereitstellung

Wählen Sie die in der eDelivery- oder der Berechtigungs-E-Mail angegebene URL aus. Laden Sie die OVA-Datei herunter, und setzen Sie die Installation fort.

VM-Installation

Schritt 1:

Navigieren Sie zu **Datei > OVF-Vorlage bereitstellen**, um den Assistenten **OVF-Vorlage bereitstellen** zu öffnen, wie im Bild dargestellt.


- ✓ 1 Select creation type
- 2 Select OVF and VMDK files**
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

Virtual machine names can contain up to 80 characters and they must be unique within each

×  PrivateCloud-Latest.ova



Back

Next

- ✓ 1 Select creation type
- 2 Select OVF and VMDK files
- 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file**
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF or OVA file.



Back

Next

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- 4 License agreements
- 5 Deployment options
- 6 Additional settings
- 7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

The following datastores are accessible from the destination resource that you selected. Select the virtual machine configuration files and all of the virtual disks.

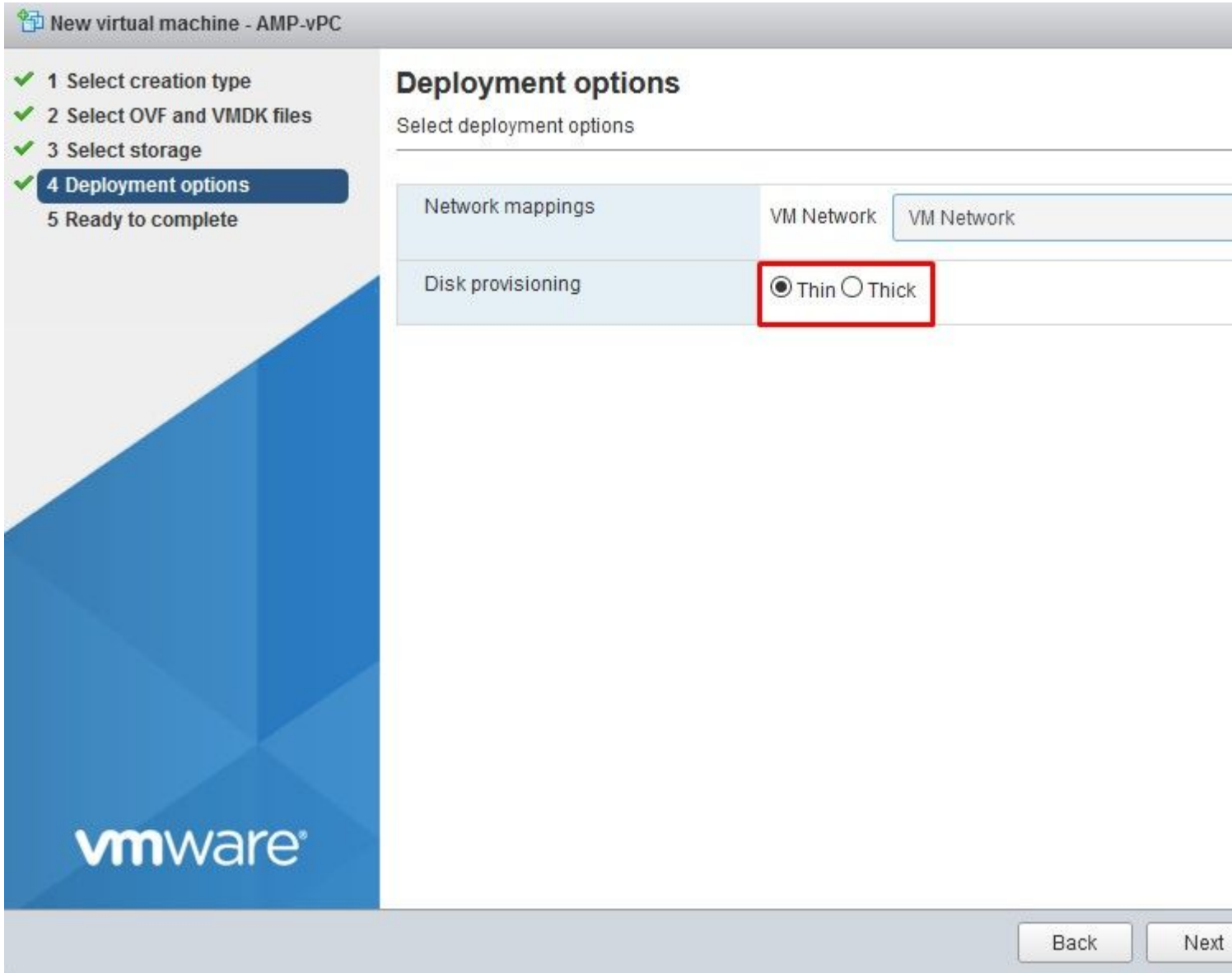
Name	Capacity	Free	Type	
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	S
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	S
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	S
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	S

vmware®

Back

Next

Hinweis: Thick Provisioning reserviert Speicherplatz, wenn ein Datenträger erstellt wird. Wenn Sie diese Option auswählen, kann sie die Leistung gegenüber **Thin Provisioned** verbessern. Dies ist jedoch nicht obligatorisch. Wählen Sie nun auf **Weiter**, wie im Bild gezeigt.



Phase 2:

Wählen Sie **Durchsuchen...** aus, um eine OVA-Datei auszuwählen, und wählen Sie dann **Weiter aus**. Sie sehen die voreingestellten OVA-Parameter auf der Seite **OVF Template Details (OVF-Vorlagendetails)**, wie in der Abbildung dargestellt. Wählen Sie auf **Next (Weiter)**.

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown



Do not refresh your browser while this VM is being deployed.

vmware®

Back

Next

Erste Einrichtung der Admin-Schnittstelle


New virtual machine - AMP-vPC

- ✓ 1 Select creation type
- ✓ 2 Select OVF and VMDK files
- ✓ 3 Select storage
- ✓ 4 Deployment options
- ✓ 5 Ready to complete

Ready to complete

Review your settings selection before finishing the wizard

Product	FireAMP PrivateCloud x86_64
VM Name	AMP-vPC
Disks	PrivateCloud_3.2.0_202010082118_v6.5_signed-disk1.vmdk,PrivateCloud_3.2.0_202010082118_v6-disk2.vmdk,PrivateCloud_3.2.0_202010082118_v6-disk3.vmdk,PrivateCloud_3.2.0_202010082118_v6
Datastore	vDisk-70_12
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

 Do not refresh your browser while this VM is being deployed.

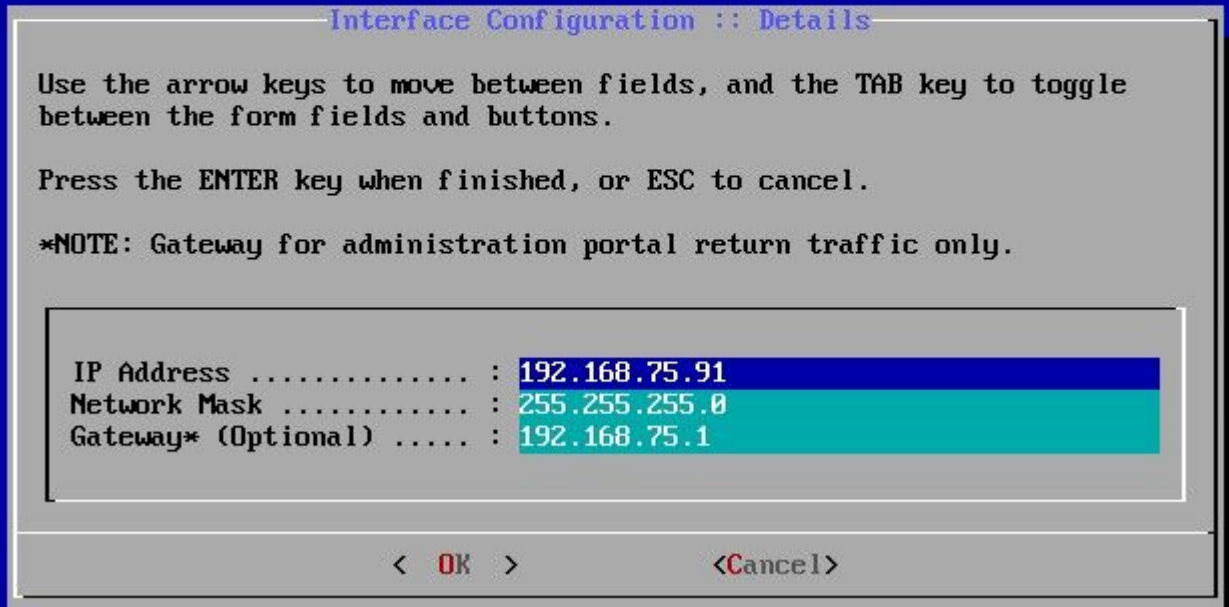
vmware

Back Next

Sobald das virtuelle System gestartet wurde, führen Sie die Erstkonfiguration über die VM-Konsole aus.

Schritt 1:

Sie können feststellen, dass die URL [UNCONFIGURED] anzeigt, wenn die Schnittstelle keine IP-Adresse vom DHCP-Server erhalten hat. Beachten Sie, dass diese Schnittstelle die **Management**-Schnittstelle ist. Dies ist nicht die **Produktions**-Schnittstelle.



Phase 2:

Sie können durch die Tasten **Tab**, **Enter** und **Arrow** navigieren.

Navigieren Sie zu **CONFIG_NETWORK**, und wählen Sie die **Eingabetaste** auf Ihrer Tastatur aus, um mit der Konfiguration der Management-IP-Adresse für die Secure Endpoint Private Cloud zu beginnen. Wenn Sie DHCP nicht verwenden möchten, wählen Sie **Nein** und **Enter** key.





Im erscheinenden Fenster wählen Sie **Ja** und wählen **Enter** key.



Wenn die IP bereits verwendet wird, werden Sie mit diesem Fehlerprotokoll behandelt. Einfach zurückgehen und etwas auswählen, das einzigartig ist und nicht verwendet wird.

Restarting eth0...

ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:14:00:00) already uses address 192.168.75.91.

ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:14:00:00) already uses address 192.168.75.91.

ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:14:00:00) already uses address 192.168.75.91.

=====
ERROR: The interface failed to reconfigure.
=====

Press ENTER key to continue...
-

AMP -- Private Cloud Advanced Malware Protection (ver. 3.2.0)

Interface Configuration :: Details

Use the arrow keys to move between fields, and the TAB key to toggle between the form fields and buttons.

Press the ENTER key when finished, or ESC to cancel.

*NOTE: Gateway for administration portal return traffic only.

IP Address	: 192.168.75.92
Network Mask	: 255.255.255.0
Gateway* (Optional)	: 192.168.75.1

< OK >

<Cancel>

Wenn alles gut geht, sehen Sie eine Ausgabe, die so aussieht

```

- execute semanage fcontext --add --type var_log_t "/data/log(/.*)?"
* execute[ConfigurePokedLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/poked(/.*)?"
* execute[ConfigureCloudLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/cloud/log(/.*)?"
* execute[ConfigureEventLogs] action run
- execute semanage fcontext --add --type var_log_t "/data/event_log_store(/.*)?"
* execute[RestoreSELinuxFileContextData] action run
- execute restorecon -R /data
Recipe: base::ssh
* template[etc/ssh/sshd_config] action create
- update content in file /etc/ssh/sshd_config from c85f41 to bad1ab
--- /etc/ssh/sshd_config      2021-04-09 13:25:01.969995024 +0000
+++ /etc/ssh/.chef-sshd_config20210410-8506-1ry0qx2 2021-04-10 06:13:11.8893895
@@ -18,7 +18,7 @@
 #AddressFamily any
 #ListenAddress 0.0.0.0
 #ListenAddress ::
-ListenAddress 192.168.75.208
+ListenAddress 192.168.75.92

# The default requires explicit activation of protocol 1
Protocol 2
- restore selinux security context
* template[etc/ssh/ssh_config] action create (up to date)
* service[ssh_server] action enable (up to date)
* service[ssh_server] action start (up to date)
Recipe: base::grub-conf
* cookbook_file[etc/default/grub] action create (up to date)
* execute[Update grub if new kernel installed] action run (skipped due to only_if)
* execute[Ensure grub menu displays Cisco not CentOS] action run (skipped due to)
Recipe: base::transparent-hugepages
* execute[disable transparent hugepage] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/enabled
* execute[disable transparent hugepage defrag] action run
- execute echo never > /sys/kernel/mm/transparent_hugepage/defrag
* execute[disable transparent hugepage for default kernel] action run

```

Restarting eth0...

Reconfiguring...

```

[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins configuration file to configure :disabled_plugins for ohai.
[2021-04-10T06:12:42+00:00] WARN: Ohai::Config[:disabled_plugins] is set. Ohai::Config[:disabled_plugins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins configuration file to configure :disabled_plugins for ohai.
Starting Chef Client, version 12.14.89

```

Schritt 3:

Warten Sie, bis der blaue Bildschirm mit Ihrer neuen STATIC IP erneut angezeigt wird. Bitte beachten Sie auch das **einmalige Passwort**. Machen Sie sich Notizen, und öffnen Sie unseren Browser.



Erstkonfiguration des vPC über die Web-GUI

Schritt 1:

Öffnen Sie einen Webbrowser, und navigieren Sie zur Management-IP-Adresse der Appliance. Sie können einen Zertifikatfehler erhalten, da die Secure Endpoint Private Cloud anfänglich ein eigenes HTTPS-Zertifikat generiert, wie im Bild gezeigt. Konfigurieren Sie den Browser so, dass er dem selbstsignierten HTTPS-Zertifikat von Secure Endpoint Private Cloud vertraut.

Geben Sie in Ihrem Browser die zuvor konfigurierte **STATIC IP (STATISCHE IP)** ein.

← → ↻ 🏠 <https://192.168.75.92> 🔒 🔍

⚙️ 📌 ⚙️ Most Visited 📄 Cisco 📄 Cisco WFH 📄 Isaac 📄 WHOIS 📄 Ting Speedtest - Spe... 📄 USD to CZK 📄 Internet Banka – MON... 📄 dCloud 📄 Google Translate 📄 News | Cisco dCloud 📄 E

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 192.168.75.92. If you visit this site, you may be asked to provide information that could be used to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support team. You can also notify the website's administrator about the problem.

[Learn more...](#)

[Go Back \(Recommended\)](#)

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 192.168.75.92 because its issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: `SEC_ERROR_UNKNOWN_ISSUER`

[View Certificate](#)

[Go Back \(Recommended\)](#) [Accept the Risk](#)

Phase 2:

Nach der Anmeldung müssen Sie das Kennwort zurücksetzen. Verwenden Sie das **ursprüngliche Kennwort** aus der Konsole im Feld **Altes Kennwort**. Verwenden Sie Ihr neues Kennwort im Feld **Neues Kennwort**. Geben Sie Ihr neues Kennwort erneut in das Feld **Neues Kennwort** ein. Wählen Sie auf **Kennwort ändern** aus.



Password Required

Authentication is required to administer your AMP for Endpoints Private Cloud device. The password can be found on the device console of your Private Cloud device.

Use one time password
PG&d'HbCgZ

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

[Password Recovery](#)

 Support

Schritt 3:

Nach der Anmeldung müssen Sie das Kennwort zurücksetzen. Verwenden Sie das **ursprüngliche Kennwort** aus der Konsole im Feld **Altes Kennwort**. Verwenden Sie Ihr neues Kennwort im Feld **Neues Kennwort**. Geben Sie Ihr neues Kennwort erneut in das Feld **Neues Kennwort** ein. Wählen Sie auf **Kennwort ändern** aus.



⚠ Password Expired



Change the password used to access the AMP for Endpoints Private Cloud Administration Portal. Note that this is also the root password for your device. ?

Warning

Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to enter complex passwords or passwords with non-keyboard characters into the device console.

🔒 [password field] ← Old one time password

Old one time password

🔒 [password field]

🔒 [password field]

Change Password

Schritt 4:

Scrollen Sie auf der nächsten Seite nach unten, um die Lizenzvereinbarung zu akzeptieren. **Ich habe gelesen und bin damit einverstanden.**

✓ I HAVE READ AND AGREE ✗ DECLINE

Schritt 5:

Nachdem Sie die Vereinbarung akzeptiert haben, wird der Installationsbildschirm angezeigt, wie im Bild gezeigt. Wenn Sie eine Wiederherstellung aus einer Sicherung durchführen möchten, können Sie dies hier tun. Dieses Handbuch enthält jedoch die Option **Saubere Installation**. Wählen Sie auf **Start** im Abschnitt **Installation reinigen** aus.

Installation Options

Only the License section can be altered after installation.

- > **Install or Restore**
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring, you will have the option to edit your configuration before restore proceeds.

Clean Installation

[Start >](#) ←

Restore

Local Remote

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

[+ Choose Restore File](#)

/data

[Start >](#)

Schritt 6:

Als Erstes benötigen Sie eine Lizenz, um auch nur einen Schritt vorwärts zu kommen. Sie erhalten beim Kauf des Produkts eine Lizenz und eine Passphrase. Wählen Sie on **+Upload License File (Lizenzdatei hochladen)**. Wählen Sie die Lizenzdatei aus, und geben Sie die Passphrase ein. Wählen Sie auf **Upload License**. Wenn der Upload nicht erfolgreich war, überprüfen Sie, ob die Passphrase richtig ist. Wenn der Upload erfolgreich war, wird ein Bildschirm mit gültigen Lizenzinformationen angezeigt. Wählen Sie auf **Weiter**. Wenn Sie Ihre Lizenz immer noch nicht installieren können, wenden Sie sich an den technischen Support von Cisco.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Installation Options

Only the License section can be altered after installation.

> Install or Restore



> License

License

Device ID

E6[REDACTED]V5

License

No license has been installed.

Install New License



license

+ Upload License



.....

Upload License

â€f



✔ License was successfully uploaded



Installation Options

Only the License section can be altered after installation.

- › Install or Restore ✓
- › License ✓
- › Welcome
- › Deployment Mode
- › AMP for Endpoints Console
- › Account
- › Hardware Requirements

Configuration

- › Network
- › Date and Time
- › Certificate Authorities
- › Upstream Proxy Server ✓
- › Email ✓
- › Notifications
- › Backup ✓
- › SSH ✓
- › Syslog ✓
- › Updates ✓

Services

- › Authentication
- › AMP for Endpoints Console
- › Disposition Server
- › Disposition Server

License

Device ID

E60[REDACTED]/5

License

Licensee	Roman Valenta rva[REDACTED].com
Business	Cisco - rvalenta 395a6444 [REDACTED] - 7a86fb49b7a5
Validity	2021-04-01 - 2025-12-31
Product SKU	FP-AMP-CLOUD=
Seats	50

Replace License

(cli

â€f

â€f

Schritt 7:

Sie erhalten die Willkommenseite, wie im Bild gezeigt. Auf dieser Seite werden die Informationen angezeigt, die Sie vor der Konfiguration der Private Cloud benötigen. Lesen Sie die Anforderungen aufmerksam durch. Wählen Sie auf **Weiter**, um die Konfiguration vor der Installation zu starten.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > **Welcome**
- > Deployment Mode
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

Start Installation

Welcome to Private Cloud

Before you begin

AMP for Endpoints Private Cloud needs certain network and infrastructure resources in place.



You will be asked to provide this information as you proceed through the installation. For more information and examples, please refer to the Private Cloud Deployment Strategy guide.



Two Static IP Addresses

One for administrative use, and the other for enterprise-facing services.



DNS Server

Provides hostname resolution to the Private Cloud device.



Hostnames and Trusted Certificates

One hostname and trusted certificate for each of the following services:

- Authentication.
- AMP for Endpoints Console.
- Disposition Server.
- Disposition Server - Extended Protocol.
- Disposition Update Service.
- Firepower Management Center Link.

Note: Hostnames can not be changed once the device has finished installation.



SMTP Server

Used for emails, alerts, and notifications.



NTP Server

Provides time synchronization across your Private Cloud device and endpoints.



External Internet connection (Proxy Mode only)

Proxy Mode devices perform anonymized disposition queries against the Cisco Cloud.

Konfiguration

Schritt 1:

Hinweis: Bitte beachten Sie, dass in den nächsten Folien einige exklusive Folien enthalten sind, die nur im AIR GAP-Modus vorkommen. Diese Folien können **NUR** als AIRGAP-Modus

eingeschlossen und gekennzeichnet werden.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes the Cisco logo, 'AMP for Endpoints', 'Private Cloud Administration Portal', and a 'Support' link. Below the navigation bar, there are tabs for 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support'. The main content area is titled 'Deployment Mode' and contains two options: 'Cloud Proxy' and 'Standalone'. The 'Cloud Proxy' button is highlighted with a red box. Below the buttons, there are two columns of bullet points describing the requirements and characteristics of each mode.

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > **Deployment Mode**
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs lookups against a local database.

Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

Standalone

- May require an Internet connection.
- Communication with AMP for Endpoints Connectors managed by this device is not needed.
- Disposition queries are handled by the local database on the device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately and applied automatically on this device.

¼ ¼ NUR LUFTSPALT ¼ ¼



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > **Deployment Mode** ✓
- > Standalone Operation
- AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Deployment Mode

Cloud proxy mode performs disposition lookups against Cisco Cloud disposition servers. Standalone mode disables upstream communication with Cisco Cloud disposition servers and performs disposition lookups against a local database.

 Cloud Proxy

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

 Standalone

- May require an Internet connection.
- Communication with AMP for Endpoints Connectors managed by this device.
- Disposition queries are handled locally on the Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded and applied automatically on this device.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation
- > AMP for Endpoints Console
- > Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Standalone Operation

Air Gap mode requires updates to be downloaded separately from this Private Cloud device, and an ISO file attached to the device.

Air Gap

- Does not require an Internet Connection
- Updates must be downloaded separately and applied to this Private Cloud device.

1/2 1/2 NUR 1/2 1/2

Phase 2:

Navigieren Sie zur Seite für das Konto der sicheren Endpunktkonsole. Ein administrativer Benutzer wird für die Konsole verwendet, um Richtlinien und Computergruppen zu erstellen und zusätzliche Benutzer hinzuzufügen. Geben Sie den Namen, die E-Mail-Adresse und das Kennwort für das Konsolenkonto ein. Wählen Sie auf **Weiter**.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints
- > Console Account
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

AMP for Endpoints Console Account

Configure the initial account for the AMP for Endpoints Console. The AMP for Endpoints Console is the main interface for your AMP for Endpoints Private Cloud.

Name	<input type="text" value="Roman"/>	<input type="text" value="Valenta"/>
Business Name	<input type="text" value="Cisco - rvalenta"/>	
Email Address	<input type="text" value="rval[REDACTED].com"/>	
	<input type="text" value="rval[REDACTED].com"/>	
Password	<input type="password" value="....."/>	
	<input type="password" value="....."/>	

â€f

Wenn Sie dieses Problem bei der Bereitstellung über die OVA-Datei beheben, haben Sie zwei Möglichkeiten: fahren Sie fort, und beheben Sie dieses Problem später, oder fahren Sie es herunter, um die bereitgestellte VM zu reparieren und entsprechend anzupassen. Nach dem Neustart fahren Sie dort fort, wo Sie gegangen sind.

Hinweis: Dies wurde in der OVA-Datei für Version 3.5.2 behoben, die mit 128 GB RAM und 8 CPU-Kernen richtig geladen wurde.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Hardware Requirements

⚠ Hardware Requirements Not Met

Your current configuration does not meet the hardware requirements.

It is recommended that you shutdown this device and adjust its hardware allocation to meet or exceed the minimum requirements. If you proceed, you may experience system instability.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	4	8
Memory	125 GB	128 GB

Shutdown

I understand

Hinweis: Verwenden Sie nur empfohlene Werte, es sei denn, dies dient Laborzwecken.

Edit settings - AMP-vPC (ESXi 5.0 virtual machine)

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8		
Memory	131072	MB	It will work with 48GB
Hard disk 1	376.52343	MB	
Hard disk 2	17.272949	GB	
Hard disk 3	1.7216082	TB	
Hard disk 4	4.765625	GB	
SCSI Controller 0	LSI Logic Parallel		
Network Adapter 1	VM Network		<input checked="" type="checkbox"/> Connect
Network Adapter 2	VM Network		<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1	Host device		<input type="checkbox"/> Connect
Video Card	Specify custom settings		

Nach dem Neustart fahren wir fort, wo wir links.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements

Configuration

- > Network
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Hardware Requirements

✓ **Hardware Requirements Met**

Your current configuration meets or exceeds the hardware requirements.

Hardware Configuration

	Installed	Minimum Required
CPU Cores	8	8
Memory	125 GB	128 GB

Stellen Sie sicher, dass Sie ETH1 auch mit STATIC IP konfigurieren.

Hinweis: Sie dürfen Ihr Gerät niemals für die Verwendung von DHCP konfigurieren, es sei denn, Sie haben MAC-Adressreservierungen für die Schnittstellen erstellt. Wenn sich die IP-Adressen Ihrer Schnittstellen ändern, kann dies zu ernsthaften Problemen mit den bereitgestellten sicheren Endgeräteanschlüssen führen. Wenn Sie Ihren DNS-Server nicht konfiguriert haben, können Sie das öffentliche DNS **temporär** verwenden, um die Installation abzuschließen.

Schritt 3:



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time
- > Certificate Authorities
- > Upstream Proxy Server ✓
- > Cisco Cloud
- > Email ✓
- > Notifications
- > Backup ✓
- > SSH
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Network Configuration

Clicking Next will apply your interface configuration before validating your settings. If you have DHCP, a release/renew will be performed to obtain the reserved DHCP lease.

Administration Portal

eth0 / 00:00:00

IP Assignment

Interface Configuration

eth1 / 00:00:00

IP Assignment 1

IP Assignment Static ←

IP Address

Check for IP Address conflict

Subnet Mask

Gateway

DNS

Primary DNS Server ← Use public DNS temporary.

Secondary DNS Server

Next (Applies to All)

Schritt 4:

Sie erhalten die Seite Datum und Uhrzeit. Geben Sie die Adressen eines oder mehrerer NTP-Server ein, die für die Datums- und Uhrzeitsynchronisierung verwendet werden sollen. Sie können interne oder externe NTP-Server verwenden und mehrere durch Kommas oder Leerzeichen getrennte Listen angeben. Synchronisieren Sie die Uhrzeit mit Ihrem Browser, oder führen Sie `amp-ctl ntpdate` von der Gerätekonsole aus, um eine sofortige Zeitsynchronisierung mit Ihren NTP-Servern zu erzwingen. Wählen Sie auf **Weiter**.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > **Date and Time** ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓

Date and Time

NTP Servers

<input checked="" type="radio"/>	192.168.75.254	← Optional	<input type="checkbox"/> Verify host
----------------------------------	----------------	------------	--------------------------------------

Current System Time

<input type="text"/>	2021	/	4	/	10	
<input type="text"/>	8	:	17	:	24	UTC
<input type="radio"/> Set by NTP						

¼ ¼ NUR LUFTSPALT ¼ ¼



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Prepare amp-sync ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Prepare amp-sync

You will need to load a snapshot of the Protect DB and retrieve the latest AMP updates from Cisco device has finished installing in air gap mode. Cisco provides a shell script called amp-sync that will download the updates and build an ISO file that you can then mount on your AMP device.

It is suggested that you begin the download process now since the initial update is very large.



1/2 1/2 NUR 1/2 1/2

Schritt 5:

Sie erhalten die Seite Zertifizierungsstellen, wie im Bild dargestellt. Wählen Sie auf **Zertifizierungsstelle hinzufügen aus**, um Ihr Stammzertifikat hinzuzufügen.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Certificate Authorities



No certificate authorities have been uploaded to this device.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓

Add Certificate Authority

● Certificate Root (PEM .crt) Disable Strict

- ✓ Certificate file has been uploaded.
- ✓ Certificate is in a readable format.
- ✓ Certificate start and end dates are valid.
- ✓ Certificate end date is later than 20 months from today.
- ✓ Certificate file only contains one certificate.
- ✓ Certificate does not use sha-1 signature algorithm.
- ✓ Certificate using RSA keys must use a key size of 2048 or more.

AMP-vPC-Root-CA.pem



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

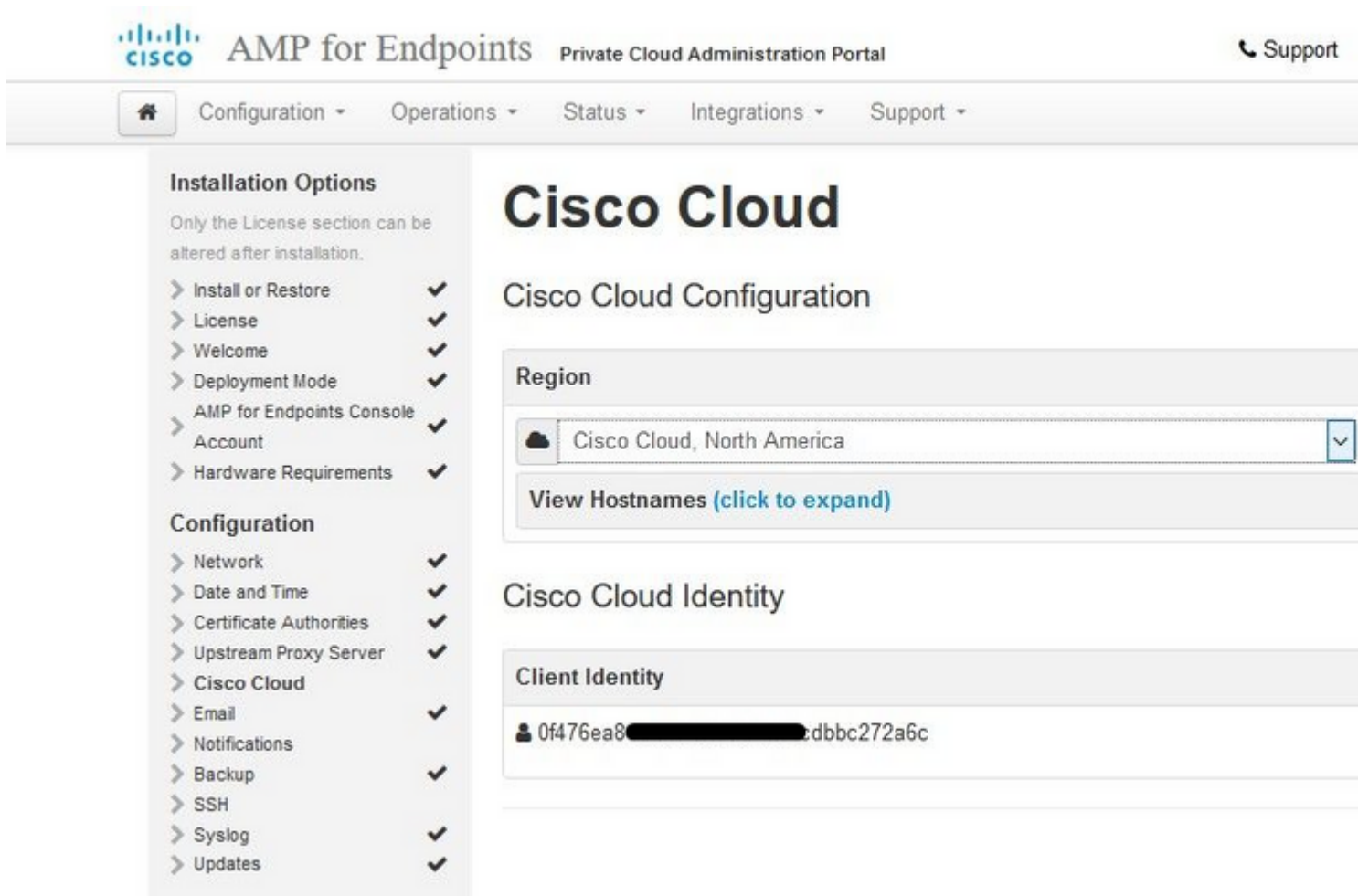
- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓

Certificate Authorities

Certificate			
Issuer	AMP-vPC		
Subject	AMP-vPC		
Validity	2021-04-09 16:28:00 UTC	-	2031-04-09 16:28:00 UTC

Schritt 6:

Der nächste Schritt ist die Konfiguration der Cisco Cloud-Seite, wie im Bild gezeigt. Wählen Sie die entsprechende Cisco Cloud-**Region** aus. Erweitern Sie **Ansicht Hostnamen**, wenn Sie Firewall-Ausnahmen für das Secure Endpoint Private Cloud-Gerät erstellen müssen, um mit der Cisco Cloud für Dateisuchen und Geräteaktualisierungen zu kommunizieren. Wählen Sie auf **Weiter**.



The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes the Cisco logo, the title "AMP for Endpoints Private Cloud Administration Portal", and a "Support" link. Below the navigation bar, there are tabs for "Configuration", "Operations", "Status", "Integrations", and "Support". The left sidebar contains a menu with "Installation Options" and "Configuration" sections. The main content area is titled "Cisco Cloud" and "Cisco Cloud Configuration". It features a "Region" dropdown menu set to "Cisco Cloud, North America" and a "View Hostnames (click to expand)" link. Below this is the "Cisco Cloud Identity" section, which includes a "Client Identity" field with the value "0f476ea8[REDACTED].dbbc272a6c".

â€f

Schritt 7:

Navigieren Sie zur Seite "Benachrichtigungen", wie im Bild dargestellt. Wählen Sie die Häufigkeit für kritische und regelmäßige Benachrichtigungen aus. Geben Sie die E-Mail-Adressen ein, die Warnmeldungen für das sichere Endgerät empfangen sollen. Sie können E-Mail-Aliase verwenden oder mehrere Adressen durch eine kommasetrennte Liste angeben. Sie können auch den Absendernamen und die E-Mail-Adresse angeben, die vom Gerät verwendet werden. Diese Benachrichtigungen unterscheiden sich von den Abonnements der Konsole für sichere Endgeräte. Sie können auch einen eindeutigen Gerätenamen angeben, wenn Sie über mehrere Secure Endpoint Private Cloud-Geräte verfügen. Wählen Sie auf **Weiter**.



- Installation Options**
Only the License section can be altered after installation.
 - Install or Restore ✓
 - License ✓
 - Welcome ✓
 - Deployment Mode ✓
 - AMP for Endpoints Console ✓
 - Account ✓
 - Hardware Requirements ✓
- Configuration**
 - Network ✓
 - Date and Time ✓
 - Certificate Authorities ✓
 - Upstream Proxy Server ✓
 - Cisco Cloud ✓
 - Email ✓
 - Notifications**
 - Backup ✓
 - SSH ✓
 - Syslog ✓
 - Updates ✓
- Services**
 - Authentication
 - AMP for Endpoints Console
 - Disposition Server
 - Disposition Server
 - Extended Protocol

Notifications

Notification Frequency		
Critical Notification Frequency	HELP	Every 5 Minutes
Notification Frequency	HELP	Every Week

Notification Addresses		
Notification Recipients	HELP	na[REDACTED]om
Notification Sender Address	HELP	donotreply@cisco.com
Notification Sender Name	HELP	AMP for Endpoints Device

Device Name		
Device Name	HELP	CyberNet vPC 2

â€f

Schritt 8:

Als Nächstes navigieren Sie zur Seite SSH-Schlüssel, wie im Bild dargestellt. Wählen Sie auf **SSH-Schlüssel hinzufügen**, um alle öffentlichen Schlüssel einzugeben, die Sie dem Gerät hinzufügen möchten. SSH-Schlüssel ermöglichen den Zugriff auf das Gerät über eine Remote-Shell mit Root-Berechtigungen. Nur vertrauenswürdigen Benutzern muss der Zugriff gewährt werden. Für Ihr Private Cloud-Gerät ist ein RSA-Schlüssel im OpenSSH-Format erforderlich. Weitere SSH-Schlüssel können Sie später über **Configuration > SSH** in Ihrem Administrationsportal hinzufügen. Wählen Sie auf **Weiter**.



Maintenance Mode

Sanity Check Failing

This page allows you to add and remove SSH keys on your Cisco AMP for Endpoints device. SSH keys allow administrators remote root authentication to the device. Only t should be granted access.

Add SSH Key

Windows PuTTY

2021-11-17 23:01:01 +0000
created 20 days ago

2021-11-17 23:01:01 +0000
20 days since last update

```
ecdsa-sha2-nistp256 AAAAE2V...oeCAvfEzyIea9PbgwnlB9DjTeJgFXt  
I4DKhrTNBv8/77T0d/Jagx7Przs=
```

â€f

Als Nächstes sehen Sie den Abschnitt "Services". Auf den nächsten Seiten müssen Sie Hostnamen zuweisen und die entsprechenden Zertifikat- und Schlüsselpaare für diese Gerätedienste hochladen. Auf den nächsten Folien sehen Sie die Konfiguration eines der 6 Zertifikate.

Services

Schritt 1:

Während des Konfigurationsprozesses können diese Fehler auftreten.

Der erste "Fehler", den Sie vielleicht bemerken, wird durch die 3 Pfeile hervorgehoben. Um dies zu umgehen, deaktivieren Sie einfach "**Strict TLS Check deaktivieren**"

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > **Authentication**
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local

Validate DNS Name

Authentication Certificate

Disable Strict TLS Check

Undo

Replace C...

● Certificate (PEM .crt)

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate contains a subject.
- Certificate contains a common name.
- Certificate contains a public key matching the uploaded key.
- Certificate matches hostname.
- Certificate is signed by a trusted root authority.
- Certificate issued after 07/01/2019 must have a validity period of 825 days or less.
- Certificate issued after 09/01/2020 must have a validity period of 398 days or less.
- Certificate does not use sha-1 signature algorithm.
- Certificate using RSA keys must use a key size of 2048 or more.
- Certificate must specify server certificate in Extended Key Usage extension.

🔍 Key (PEM .key)

- Key file has been uploaded.
- Key contains a supported key type.
- Key contains public key material.
- Key contains private key material.
- Key contains a public key matching uploaded certificate.

vPC2-Authenticator

+ Choose

vPC2-Authenticator

+ Choose Certificate

Ohne strenge TLS-Prüfung



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints Console ✓
- > Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > **Authentication** ✓
- > AMP for Endpoints Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

Validate DNS

Authentication Certificate

Disable Strict TLS Check Undo Refresh

Certificate (PEM .crt)		Key (PEM .key)	
<input checked="" type="checkbox"/>	Certificate file has been uploaded.	<input checked="" type="checkbox"/>	Key file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.	<input checked="" type="checkbox"/>	Key contains a supported key type.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.	<input checked="" type="checkbox"/>	Key contains public key.
<input checked="" type="checkbox"/>	Certificate contains a subject.	<input checked="" type="checkbox"/>	Key contains private key.
<input checked="" type="checkbox"/>	Certificate contains a common name.	<input checked="" type="checkbox"/>	Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/>	Certificate contains a public key matching the uploaded key.		
<input checked="" type="checkbox"/>	Certificate matches hostname.		
<input checked="" type="checkbox"/>	Certificate is signed by a trusted root authority.		

vPC2-Authenticatic +

vPC2-Authenticatic + Choose Certificate

Phase 2:

Der nächste Fehler, den Sie erhalten, ist, wenn Sie "DNS-Namen validieren" aktiviert lassen. Hier haben Sie zwei Möglichkeiten.

#1: Deaktivieren Sie das Kontrollkästchen DNS validieren.

#2: Kehren Sie zu Ihrem DNS-Server zurück, und konfigurieren Sie die übrigen Host-Einträge.

An error occurred while processing your request.

- Hostname does not resolve

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication
- > AMP for Endpoints
- > Console
- > Disposition Server
- > Disposition Server
- > Extended Protocol
- > Disposition Update
- > Service
- > Firepower Management Center

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local

Validate DNS Name

Authentication Certificate

Disable Strict TLS Check

Undo

Replace Cert

● Certificate (PEM .crt)	🔍 Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	



+ Choose Certificate



+ Choose Key

Wiederholen Sie diesen Vorgang jetzt noch fünf Mal für den Rest der Zertifikate.

Authentifizierung

- Der Authentifizierungsdienst kann in zukünftigen Versionen von Private Cloud zur Bearbeitung der

Benutzerauthentifizierung verwendet werden.

Konsole für sichere Endgeräte

- Konsole ist der DNS-Name, über den der Administrator des sicheren Endpunkts auf die Konsole des sicheren Endpunkts zugreifen kann, und Secure Endpoint Connectors neue Richtlinien und Aktualisierungen erhalten.

Dispositionsserver

- Disposition Server ist der DNS-Name, unter dem Secure Endpoint Connectors Cloud-Suchinformationen senden und abrufen.

Disposition Server - Extended Protocol

- Disposition Server - Extended Protocol ist der DNS-Name, über den neuere Secure Endpoint Connectors Cloud-Suchinformationen senden und abrufen.

Disposition aktualisierungsdienst

- Der Disposition Update Service wird verwendet, wenn Sie eine Cisco Threat Grid-Appliance mit Ihrem Private Cloud-Gerät verknüpfen. Die Threat Grid-Appliance sendet Dateien von der Konsole für sichere Endgeräte zur Analyse, und der Disposition Update Service wird von Threat Grid verwendet, um die Einstufung (*saubere oder schädliche*) von Dateien nach deren Analyse zu aktualisieren.

FirePOWER Management Center

- Mit dem FirePOWER Management Center Link können Sie ein Cisco FirePOWER Management Center (FMC)-Gerät mit Ihrem Private Cloud-Gerät verbinden. So können Sie Secure Endpoint-Daten in Ihrem FMC-Dashboard anzeigen. Weitere Informationen zur FMC-Integration mit Secure Endpoint finden Sie in Ihrer FMC-Dokumentation.

Achtung: Hostnamen können nicht geändert werden, nachdem das Gerät die Installation abgeschlossen hat.

Notieren Sie sich die erforderlichen Hostnamen. Sie müssen sechs eindeutige DNS A-Einträge für die Secure Endpoint Private Cloud erstellen. Jeder Datensatz verweist auf dieselbe IP-Adresse der Virtual Private Cloud-Konsolenschnittstelle (eth1) und muss sowohl von der Private Cloud als auch vom sicheren Endpunkt aufgelöst werden.

Schritt 3:

Auf der nächsten Seite herunterladen und dann überprüfen **Wiederherstellungsdatei**.

Sie erhalten die Wiederherstellungsseite, wie im Bild dargestellt. Vor Beginn der Installation müssen Sie eine Sicherungskopie Ihrer Konfiguration herunterladen und überprüfen. Die Wiederherstellungsdatei enthält alle Konfigurations- und Serverschlüssel. Wenn Sie eine Wiederherstellungsdatei verlieren, können Sie Ihre Konfiguration nicht wiederherstellen, und alle Secure Endpoint-Konnektoren müssen neu installiert werden. Ohne den ursprünglichen Schlüssel muss die gesamte Private Cloud-Infrastruktur mit neuen Schlüsseln neu konfiguriert werden. Die Wiederherstellungsdatei enthält alle Konfigurationen für das opadmin-Portal. Die Sicherungsdatei enthält den Inhalt der Wiederherstellungsdatei sowie alle Dashboard-Portaldaten wie Ereignisse, den Connector-Verlauf usw. Wenn Sie nur den opadmin ohne die Ereignisdaten und alle wiederherstellen möchten, können Sie die Wiederherstellungsdatei verwenden. Wenn Sie die Daten aus der Sicherungsdatei wiederherstellen, müssen die Daten des Opadmin- und Dashboard-Portals

wiederhergestellt werden.

Wählen Sie auf **Herunterladen**, um die Sicherung auf Ihrem lokalen Computer zu speichern. Wenn die Datei heruntergeladen wurde, wählen Sie **Choose File (Datei auswählen)** aus, um die Sicherungsdatei hochzuladen, und stellen Sie sicher, dass sie nicht beschädigt ist. Wählen Sie auf **Weiter**, um die Datei zu überprüfen und fortzufahren.

- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

- Services**
- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management ✓
- > Center ✓

1. Download Recovery File

Please keep a copy of this file in a safe place.

[Download](#)

2. Verify Recovery File

After downloading your backup, upload it to the system to verify that you have a matching copy.

[Browse...](#) pre-install-backup.bak

Recovery File Ready for Download
created less than a minute ago

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > AMP for Endpoints ✓
- > Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints ✓
- > Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

[▶ Start Installation](#)

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type**Cloud Proxy**

- Requires an Internet connection and communication with AMP for Endpoints Connectors managed device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

AMP for Endpoints Console Account

Name	Roman Valenta
Email Address	rva[REDACTED]@com
Business Name	Cisco - rvalenta

Recovery

Uploaded Recovery File Matches Current Settings

[▶ Start Installation](#)

â€f

i,¼ i,¼ NUR LUFTSPALT i,¼ i,¼



Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > Standalone Operation ✓
- > AMP for Endpoints Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Prepare amp-sync ✓
- > Email ✓
- > Notifications ✓
- > Backup ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > AMP for Endpoints Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

Review the following information and, once you are satisfied with your configuration settings, proceed with the installation. Note that the configuration shown below cannot be altered after installation.

Clean Installation

A clean installation will be performed.

Installation Type

Standalone Air Gap



- Does not require an Internet Connection
- Communication with AMP for Endpoints Connectors managed by this device are needed
- Disposition queries are handled by the Private Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates must be downloaded separately and applied to this Private Cloud device.

AMP for Endpoints Console Account

Name	Roman Valenta
Email Address	rvalenta@...m
Business Name	Cisco vamrodia PC v2

Recovery

Uploaded Recovery File Matches Current Settings

▶ Start Installation

â€f

â€f

ï½ï½ NUR ï½ï½

Sie sehen ähnliche Eingabe wie diese...

Vorsicht: Wenn Sie sich auf dieser Seite befinden, aktualisieren Sie diese nicht, da sie Probleme verursachen kann.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 10 minutes.

State	Started	Finished	Duration
▶ Running	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 14 seconds ago	⌛ Please wait...	⌛ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

le_chunk

```
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP::StreamHandler calling Chef::HTTP::Decompressor::NoopInflater#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_request
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::ValidateContentLength#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: HTTP server did not include a Content-Length header in response, cannot identify content length.
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::RemoteRequestID#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Authenticator#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::Decompressor#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::CookieManager#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONOutput#handle_stream_complete
[2021-04-10T17:36:20+00:00] DEBUG: Chef::HTTP calling Chef::HTTP::JSONInput#handle_stream_complete
[2021-04-10T17:36:20+00:00] INFO: Storing updated cookbooks/rabbitmq/recipes/default.rb in the cache.
[2021-04-10T17:36:20+00:00] DEBUG: Creating directory /var/run/cookbooks/rabbitmq/recipes
```

Download Output

Klicken Sie nach Abschluss der Installation auf die Schaltfläche zum Neustarten.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 5 minutes.

State	Started	Finished	Duration
✓ Successful	Sat Apr 10 2021 13:36:08 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 24 minutes, 14 seconds ago	Sat Apr 10 2021 13:57:05 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 3 minutes, 17 seconds ago	0 day, 0 hour, 3 minutes, 17 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-04-10T17:57:04+00:00] INFO: Running report handlers
[2021-04-10T17:57:04+00:00] INFO: Report handlers complete
[2021-04-10T17:57:04+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2021-04-10T17:57:04+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-04-10T17:57:04+00:00] DEBUG: Forked instance successfully reaped (pid: 2552)
[2021-04-10T17:57:04+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration against the AMP for Endpoints Disposition Server has previously succeeded.

=====
Installation has finished successfully! Please reboot!
=====
```

Download Output

¼¼¼ NUR LUFTSPALT ¼¼¼¼

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically un

State	Started	Finished	Duration
✓ Successful	Tue Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 21 minutes, 21 seconds ago	Tue Nov 02 2021 15:07:02 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 0 minute, 49 seconds ago	0 day, 0 h seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2021-11-02T19:07:01+00:00] INFO: Running report handlers
[2021-11-02T19:07:01+00:00] INFO: Report handlers complete
[2021-11-02T19:07:01+00:00] DEBUG: Server doesn't support resource history, skipping resource report
[2021-11-02T19:07:01+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2021-11-02T19:07:01+00:00] DEBUG: Forked instance successfully reaped (pid: 29292)
[2021-11-02T19:07:01+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.
=====
Chef run finished successfully
=====
Registration is not possible in air gap mode.
=====
Installation has finished successfully! Please reboot!
=====
```

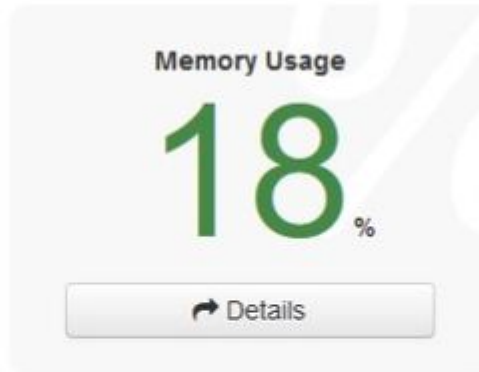
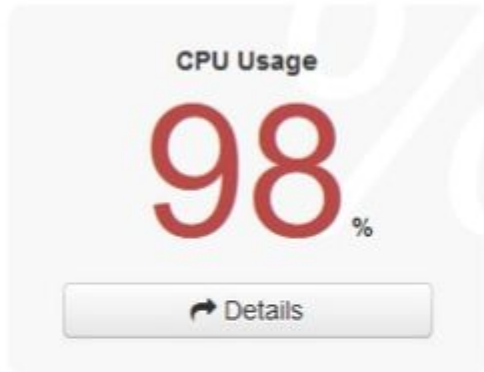
Download Output

½ ½ NUR ½ ½

Sobald die Appliance vollständig gestartet wurde, wird Ihnen das Dashboard angezeigt, wenn Sie sich das nächste Mal mit Ihrer Admin-Schnittstelle anmelden. Sie können feststellen, hohe CPU am Anfang, aber wenn Sie einige Minuten geben, wird es beruhigt.



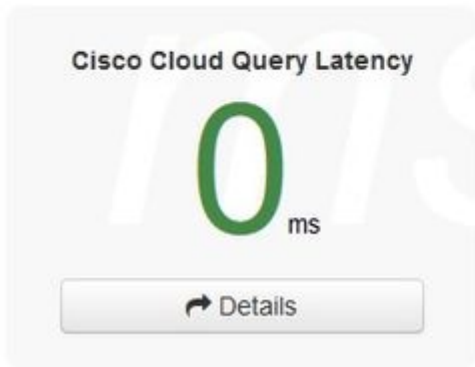
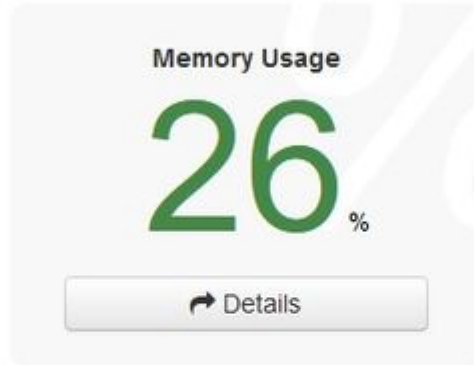
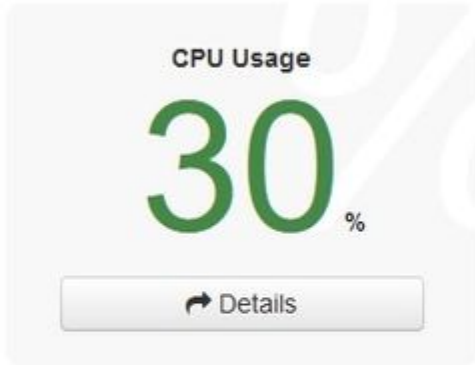
Key Metrics



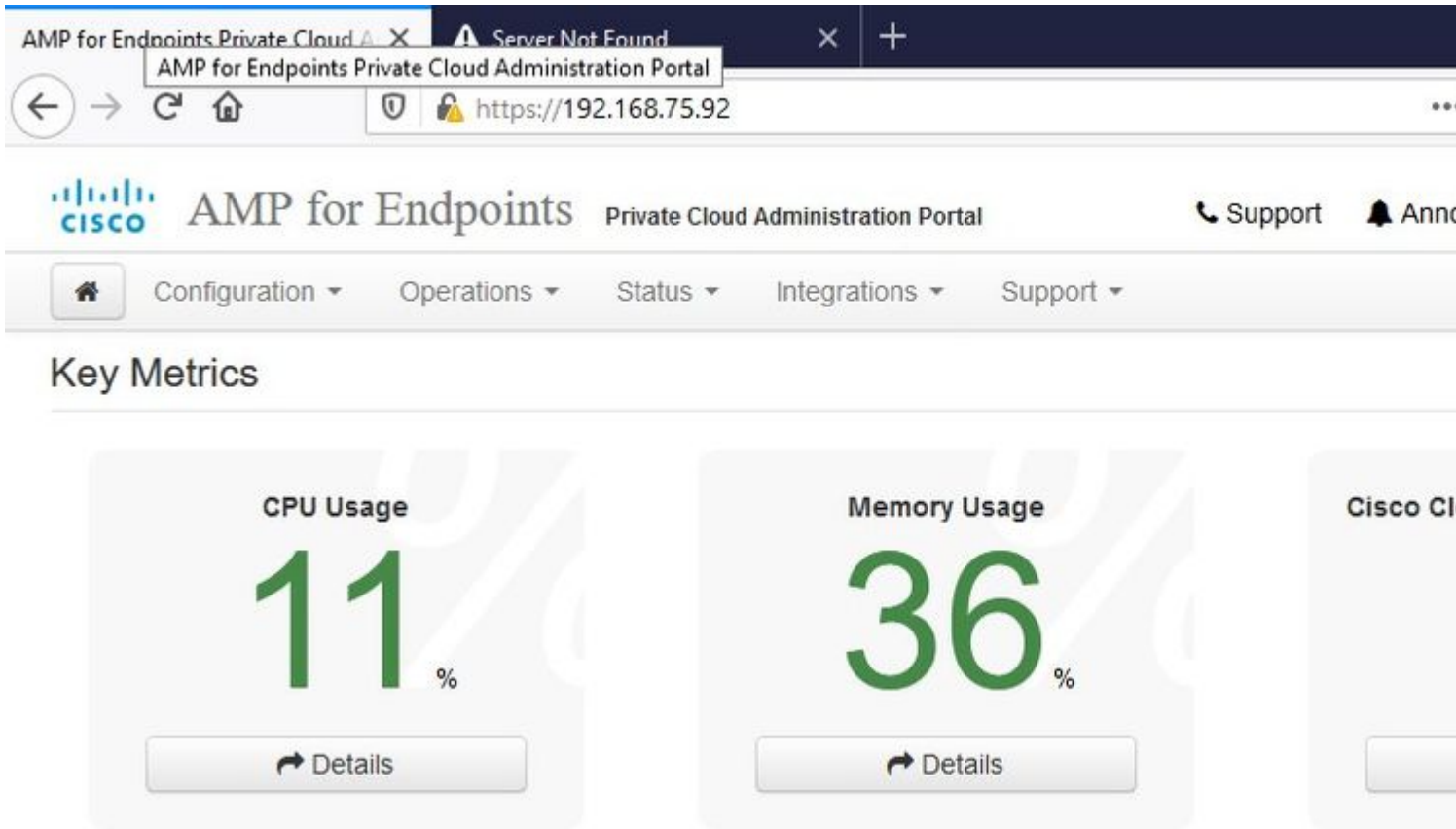
Nach wenigen Minuten...



Key Metrics



Navigieren Sie von hier zur Konsole für sichere Endgeräte. Klicke auf das kleine Symbol, das wie ein Feuer aussieht, in der rechten Ecke neben der Flagge.



¼¼ NUR LUFTSPALT ¼¼

Wie Sie sehen können, haben wir die Plausibilitätsprüfung aufgrund von **DB Protect Snapshot**, auch Client Definitions, DFC und Tetra nicht bestanden. Dies muss durch Offline-Update über eine heruntergeladene ISO-Datei erfolgen, die zuvor über **amp-sync** vorbereitet und auf die VM hochgeladen oder am NFS-Speicherort gespeichert wurde.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

❌ Sanity Check Failing

The device sanity check is failing; your device might not function properly until corrective measures are taken.

i Details

FAIL: A Protect DB snapshot has not been loaded. Devices configured in standalone mode should have a Protect DB snapshot loaded. Protect DB snapshots contain threat intelligence about known clean and known malicious files.

Key Metrics

CPU Usage

11%

↻ Details

Memory Usage

28%

↻ Details

Active Connections

0

↻ Details



✖ **Sanity Check Failing**

Updates keep your Private Cloud device up to date.

↻ Check Update ISO

✖ There is no ISO loaded. Load an ISO and try again.

Content

✖ **3.2.0_202010081917**

Client Definitions, DFC, Tetra Content Version

! **ABSENT**

Protect DB Version

! Import a Protect DB snapshot

Checked 1 minute ago; the update check failed.

Software

✖ **3.2.0_202010082118**

Private Cloud Software Version

Checked 1 minute ago; the update check failed.

AirGap-Aktualisierungspaket

Zum ersten Mal müssen wir diesen Befehl verwenden, um die Protect DB zu erhalten

```
./amp-sync all
```

Hinweis: Laden Sie alle Pakete über diesen Befehl herunter und überprüfen Sie, ob dies **mehr als 24 Stunden** dauern kann. Je nach Geschwindigkeit und Verbindungsqualität In meinem Fall mit 1Gig Glasfaser es noch fast 25hrs dauern zu vollenden. Teilweise liegt das auch daran, dass dieser Download direkt von AWS stammt und somit gedrosselt wird. Beachten Sie schließlich, dass dieser Download ziemlich groß ist. In meinem Fall war die heruntergeladene Datei **323GB**. ☹️

In diesem Beispiel haben wir **CygWin64** verwendet

1. Laden Sie die x64-Version von Cygwin herunter, und installieren Sie sie.
2. Führen Sie setup-x86_64.exe aus, und gehen Sie durch den Installationsvorgang. Wählen Sie alle Standardeinstellungen aus.
3. Wählen Sie einen Download-Spiegel.
4. Wählen Sie die zu installierenden Pakete:

Alle -> Net -> curl

Alle -> Utils -> genisoimage

Alle -> Utils -> xmlstarlet

* VPC 3.8.x oder höher - > xorriso

```

E
User@VMStation-1 ~
$ ./amp-sync all
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD
No MOTD for today, nothing to download. Continuing..
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7
No MOTD for today, nothing to download. Continuing..
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/MOTD-AmpSync-1.0.7-prod
No MOTD for today, nothing to download. Continuing..
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/repomd.xml
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 2991 100 2991 0 0 15991 0 --:--:-- --:--:-- --:--:-- 16167
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 11331 100 11331 0 0 98544 0 --:--:-- --:--:-- --:--:-- 97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bb
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 915k 100 915k 0 0 3324k 0 --:--:-- --:--:-- --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bb
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3d
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1094k 100 1094k 0 0 3302k 0 --:--:~ --:~:~ --:~:~ 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3d
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 135k 100 135k 0 0 747k 0 --:~:~ --:~:~ --:~:~ 756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 54480 100 54480 0 0 383k 0 --:~:~ --:~:~ --:~:~ 385k
```



```
99.91% done, estimate finish Thu Nov 4 08:39:50 2021
99.91% done, estimate finish Thu Nov 4 08:39:51 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:50 2021
99.92% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.93% done, estimate finish Thu Nov 4 08:39:51 2021
99.93% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.94% done, estimate finish Thu Nov 4 08:39:51 2021
99.94% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.95% done, estimate finish Thu Nov 4 08:39:51 2021
99.95% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:50 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.96% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.97% done, estimate finish Thu Nov 4 08:39:52 2021
99.97% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:51 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.98% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
99.99% done, estimate finish Thu Nov 4 08:39:52 2021
100.00% done, estimate finish Thu Nov 4 08:39:52 2021
Total translation table size: 0
Total rockridge attributes bytes: 345811
Total directory bytes: 512364
Path table size(bytes): 148
Max brk space used 2f0000
157803265 extents written (308209 MB)
Package successful: PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso
User@VMStation-1 ~
$
```



Hinweis: Im neuesten Update VPC 3.8.x mit CygWin64 als Haupt-Download-Tool können Sie dieses Problem unten beschrieben begegnen.

```
User@VMStation-1 ~
```

```
$ ./amp-sync all
```

```
=====
```

```
Prerequisite Program(s) Missing
```


```
=====
```

```
A prerequisite tool was not found in your PATH, or is not an appropriate version. You must have the following tools installed in order for the AMP for dpoints
```

```
Air-Gap Update Tool to function:
```

```
awk  
base64  
basename  
cat  
comm  
curl  
dirname  
mv
```

```
MISSING -> xorriso  
sha256 / sha256sum / shasum  
sort  
tr  
xmlstarlet
```



```
These tools should be available in both Windows Subsystem for Linux and most Unix-like operating systems.
```

â€f

[Versionshinweise](#) Seite #58. Wie Sie sehen können, ist "**xorriso**" jetzt erforderlich. Wir haben das ISO-Format in ISO 9660 geändert, und diese Abhängigkeit ist es, was das Bild in das richtige Format konvertiert, sodass die Aktualisierung abgeschlossen werden kann. Leider bieten CygWin64 xorriso in keinem ihrer eingebauten Repositorys an. Für diejenigen, die noch CygWin64 verwenden möchten, gibt es jedoch eine Möglichkeit, dieses Problem zu überwinden.

Installing dependencies

CentOS

To run amp-sync you will first have to install EPEL, xorriso, and xmlstarlet.

1. Enable the EPEL repo.
 - > `sudo yum install epel-release`
2. Install dependencies via yum.
 - > `sudo yum install xorriso`
 - > `sudo yum install xmlstarlet`

Ubuntu

To run amp-sync you will first have to install xorriso and xmlstarlet.

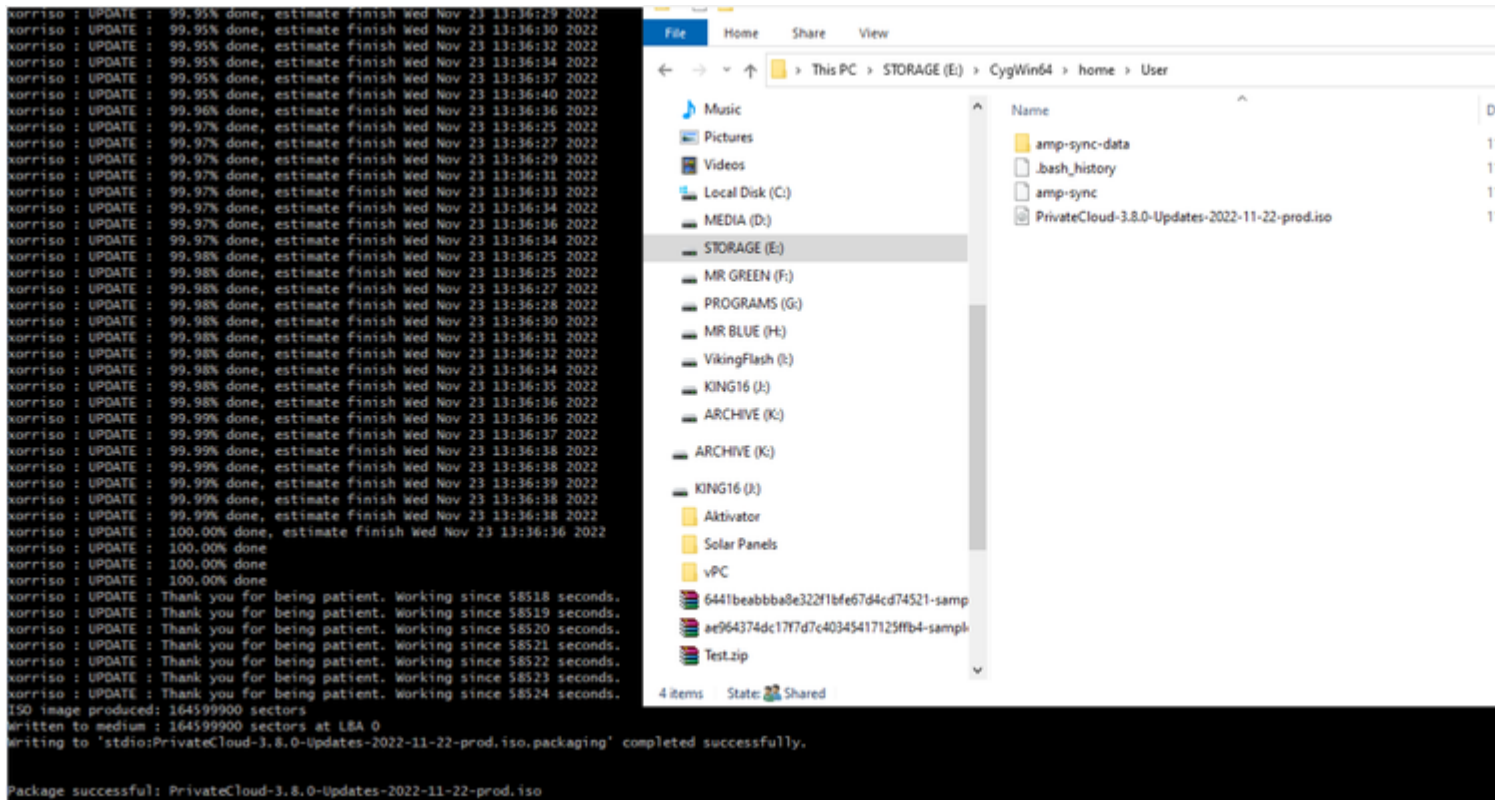
- Install dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

Windows

1. Set up Windows Subsystem for Linux (WSL) with the Ubuntu distribution. See the [Microsoft documentation](#) for details.
2. Expand the WSL virtual hard disk size to comply with minimum free disk space. See the [Microsoft documentation](#) for details.
3. Install xorriso and xmlstarlet dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

â€f

Um CygWin wieder verwenden zu können, müssen Sie xorriso manuell aus dem GitHub-Repository herunterladen. Öffnen Sie Ihren Browser und geben Sie <Latest xorriso.exe 1.5.2 pre-build for Windows> ein, um den ersten Link mit dem Namen <PeyTy/xorriso-exe-for-windows - GitHub> aufzurufen, zur GitHub-Seite zu navigieren und die <xorriso-exe-for-windows-master.zip>-Datei herunterzuladen. der ZIP-Datei, die Sie neben einigen anderen Dateien mit dem Namen <xorriso.exe> finden, kopieren und einfügen Sie diese Datei in den <CygWin64\bin> -Pfad der lokalen CygWin-Installation. Versuchen Sie erneut, den <amp-sync>-Befehl auszuführen. Sie sollten nicht mehr die Fehlermeldung und Download Start und Ende wie im Bild gezeigt.



Führen Sie die Sicherung der aktuellen (*in diesem Fall*) 3.2.0 VPC im Airgap-Modus durch.

Sie können diesen Befehl in der Befehlszeile verwenden.

```
rpm -qa | grep Pri
```

Sie können auch zu **Operationen > Backups** navigieren, wie im Bild dargestellt, und dort **eine Sicherung durchführen**.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

❌ **Sanity Check Failing**

Backups create a copy of your configuration and databases.

Manual Backup

[Perform Backup](#)

Last Backup Successful

Transferring Backups To External Storage Is Recommended

To facilitate disaster recovery, you are strongly encouraged to transfer backup archives to a secure external backup storage. Backup archives can be performed via download, sftp, or rsync.

[Backup Job Details](#)

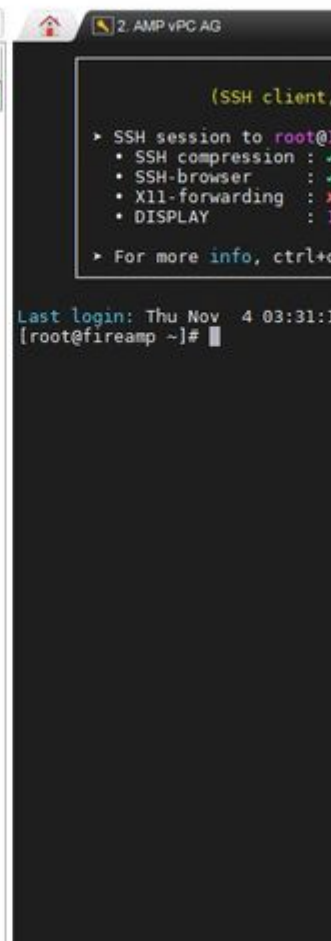
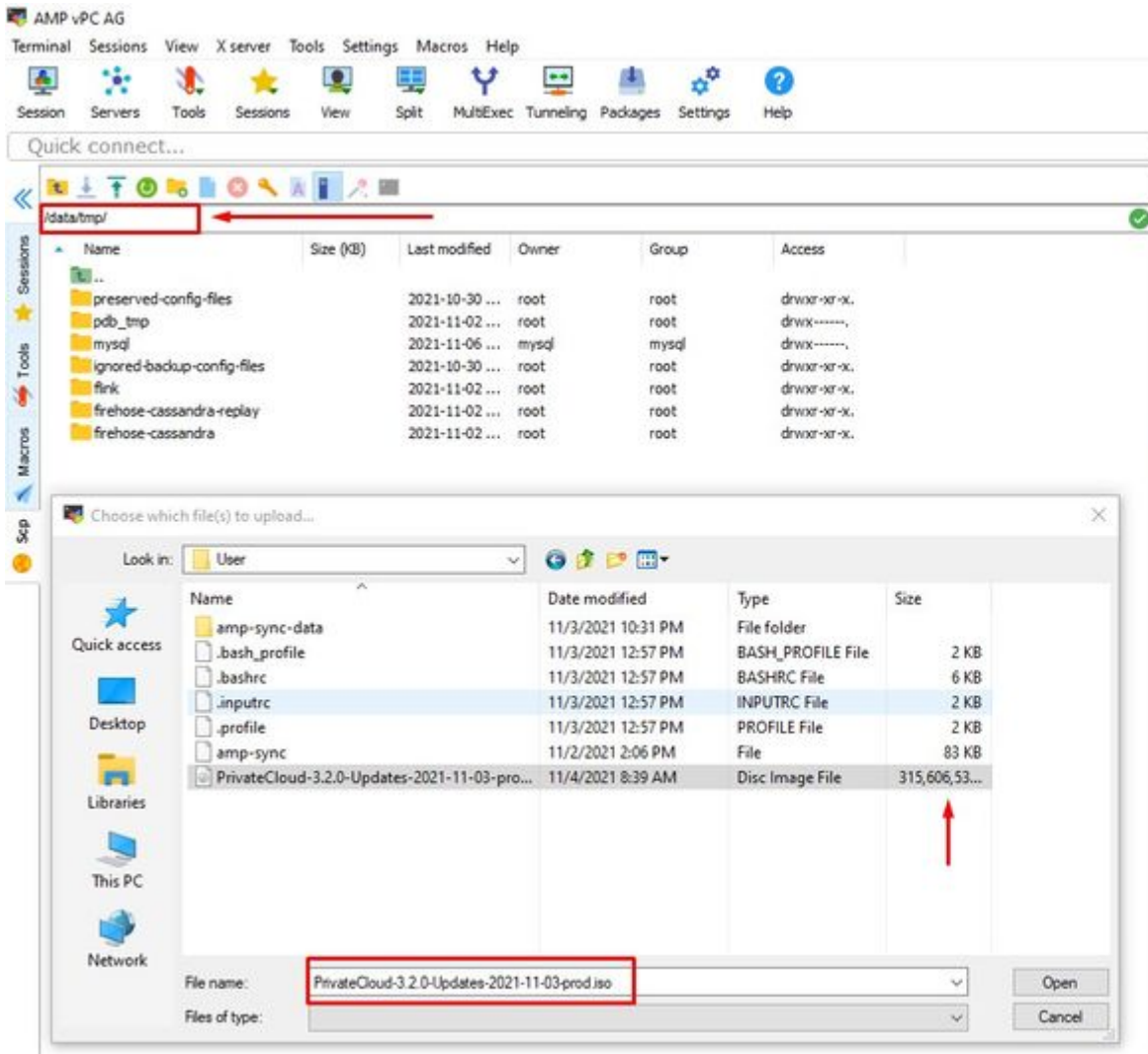
Previous Backups

The number of backups that will be stored on disk is: 1.

Name	📦 Size	📅 Timestamp
/data/backups/amp-backup-20211106-0000.18.bak	738 MB	2021-11-06 00:03:43 +0 about 17 hours ago

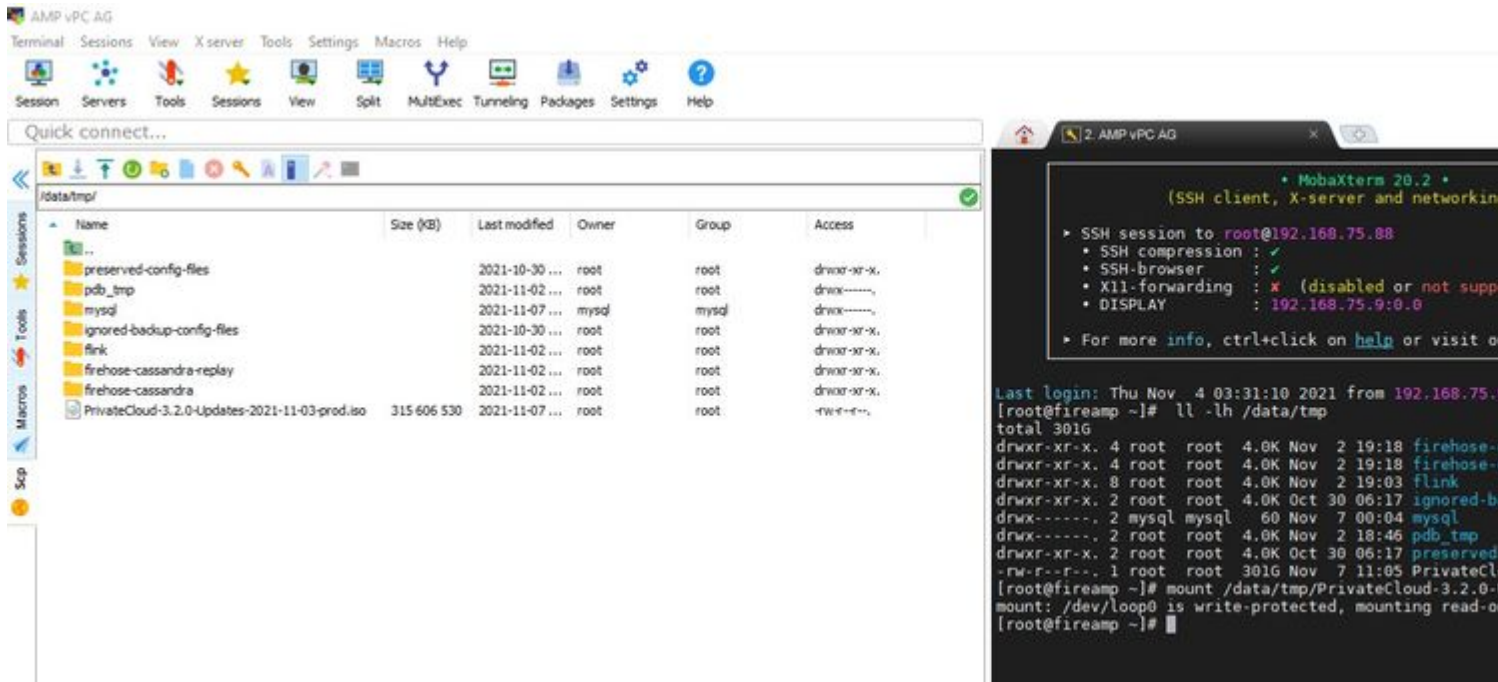
Übertragen Sie die neueste ISO, die mit amp-sync generiert wurde, auf die vPC. Dies kann je nach Ihrer Geschwindigkeit bis zu mehreren Stunden dauern. In diesem Fall übernahm der Transfer 16h

/data/tmp



Nachdem der Upload abgeschlossen ist, mounten Sie die ISO-

```
mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/
```

â€f

Navigieren Sie zur Benutzeroberfläche von opdamin, um die Aktualisierung durchzuführen. **Vorgänge > Gerät aktualisieren > Wählen Sie ISO-Aktualisierung überprüfen aus.**



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Check Update ISO

Checking ISO for updates...

Content

3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

ABSENT

Protect DB Version

Checked 9 minutes ago; the update check failed.

Software

3.2.0_202010082118

Private Cloud Software Version

A software update is available.

In diesem Beispiel gehe ich zuerst mit **Inhaltsaktualisierung** vor.



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update C
Import P

ABSENT
Protect DB Version

A content update is available.

ISO contains Protect DB snapshot version
Import a Protect DB snapshot to your st

Software

3.2.0_202010082118
Private Cloud Software Version

Update S

A software update is available.

Wählen Sie dann Protect DB importieren aus.

â€f



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Check Update ISO

Content

✓ 20211102210054
Client Definitions, DFC, Tetra Content Version

! ABSENT
Protect DB Version

Checked less than a minute ago; content is up to date.

Update

Import

! Import a Protect DB snapshot to your

Software

i 3.2.0_202010082118
Private Cloud Software Version

[A software update is available.](#)

Update

â€f

Wie Sie sehen können, ist dies ein weiterer sehr langwieriger Prozess, dessen Abschluss viel Zeit in Anspruch nehmen kann.

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

☰ State	📅 Started	📅 Finished	🕒 Duration
▶ Running	2021-11-07 18:48:44 +0000 less than a minute ago	🕒 Please wait...	🕒 Please wait...

☰ Output

```
Attempting to mount an ISO, if one is present.  
mount: special device /dev/cdrom does not exist  
Starting update.  
Stopping apply-cloud-deltas...  
Stopping authentication_web...  
Stopping authentication_worker...
```

📄 Download Output

â€f

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several h

☰ State	📅 Started	📅 Finished	🕒 Duration
▶ Running	2021-11-07 18:48:44 +0000 42 minutes ago	🕒 Please wait...	🕒 Please wait...

☰ Output

Extraction	14.9GB	at	6.5MB/s	eta:	9:29:00	6%	[==]
Extraction	14.9GB	at	6.6MB/s	eta:	9:28:21	6%	[==]
Extraction	14.9GB	at	6.6MB/s	eta:	9:28:27	6%	[==]
Extraction	14.9GB	at	6.5MB/s	eta:	9:28:40	6%	[==]
Extraction	14.9GB	at	6.5MB/s	eta:	9:28:46	6%	[==]
Extraction	14.9GB	at	6.5MB/s	eta:	9:28:58	6%	[==]
Extraction	14.9GB	at	6.5MB/s	eta:	9:29:12	6%	[==]
Extraction	14.9GB	at	6.5MB/s	eta:	9:29:26	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:28:56	6%	[==]
Extraction	15.0GB	at	6.6MB/s	eta:	9:28:20	6%	[==]
Extraction	15.0GB	at	6.6MB/s	eta:	9:28:28	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:28:44	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:28:51	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:28:48	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:28:56	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:29:10	6%	[==]
Extraction	15.0GB	at	6.5MB/s	eta:	9:29:23	6%	[==]

📄 Download Output

⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take several hours.

State	Started	Finished	Duration
▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌚ Please wait...	⌚ Please wait...

```
Output
Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

â€f

Problem #1 - Erschöpfter Platz im Datenspeicher

â€f

Hier können Sie auf zwei Probleme laufen. Da vPC vor 3.5.2 nicht in der Lage ist, externen NFS-Speicher zu mounten, müssen Sie die ISO-Aktualisierungsdatei in das Verzeichnis **/data/temp** hochladen. In meinem Fall, da mein Datenspeicher nur 1 TB betrug, rannte ich aus dem Raum und das virtuelle System stürzte ab. Mit anderen Worten, Sie benötigen mindestens 2 TB Speicherplatz in Ihrem Datenspeicher, um AirGap VPC erfolgreich bereitzustellen, das unter Version 3.5.2 liegt.

Dieses Bild unten stammt vom ESXi-Server. Es zeigt den Fehler, dass beim Booten des virtuellen Systems kein freier Speicherplatz mehr auf der Festplatte verfügbar ist. Ich war in der Lage, von diesem Fehler durch temporäre Umschaltung der 128 GB RAM auf 64 GB zu erholen. Dann konnte ich wieder hochfahren. Denken Sie auch daran, dass, wenn Sie diese VM als Thin Client bereitstellen, die Kehrseite der Thin Client-Bereitstellung ist, dass die Festplattengröße wachsen kann, aber nicht schrumpfen würde, selbst wenn Sie etwas Speicherplatz freigeben. Angenommen, Sie haben Ihre 300-GB-Datei in das Verzeichnis von vPC hochgeladen und dann gelöscht. Die Festplatte im ESXi weist immer noch 300 GB weniger Speicherplatz auf der Festplatte auf.

Event Details

Type: **error** User: **root** Time: **11/15/2021 12:24:43 PM** Target: [AMP-vPC AirGap](#)

Description: ⓘ

🔔 11/15/2021 12:24:43 PM, Error message on [AMP-vPC AirGap](#) on [UCS-2](#) in [ha-datacenter](#): Failed to power on VM.

Error Stack: [Hide](#)

- ↳ Failed to power on VM.
- ↳ Could not power on virtual machine: msg.vmk.status.VMK_NO_SPACE.
- ↳ Failed to extend the virtual machine swap file
- ↳ Current swap file size is 0 KB.
- ↳ Failed to extend swap file from 0 KB to 134217728 KB.
- ↳ File systemspecific implementation of LookupAndOpen[file] failed
- ↳ File systemspecific implementation of Lookup[file] failed

Related Events: [Show](#)

â€f

Problem #2 - Altes Update

Das ^{zweite} Problem ist, wenn Sie das Software-Update zuerst wie ich in meiner 2.^{ten} Testversion und von 3.2.0 Ich am Ende mit VPC auf 3.5.2 zu aktualisieren und aus diesem Grund musste ich eine brandneue ISO-Update-Datei herunterladen, da die 3.2.0 ungültig geworden, weil ich nicht mehr auf der ursprünglichen 3.2.0-Version war.



Configuration

Operations

Status

Integrations

Support

Maintenance Mode

The device is in maintenance mode.
External services are unavailable.

Sanity Check Failing

Disabling TLS

Updates keep your Private Cloud device up to date.

Check Update ISO

There is no ISO loaded. Load an ISO and try again.

Content

3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

ABSENT

Protect DB Version

Checked 24 minutes ago; the update check failed.

Import a Protect DB snapshot

The previous

Software

3.5.3_202111080345

Private Cloud Software Version

Checked 24 minutes ago; the update check failed.

Dies ist der Fehler, den Sie sehen, wenn Sie die ISO-Aktualisierungsdatei erneut mounten.

â€f



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

✖ Maintenance Mode

✖ Sanity Check Failing

i Disabling

Home / Operations - Update Device / Update Check Details

✖ The update check failed

Something went wrong while checking for updates.

☰ State	📅 Started	📅 Finished	🕒
✖ Failed	2021-11-16 16:29:23 +0000 less than a minute ago	2021-11-16 16:29:30 +0000 less than a minute ago	le

☰ Output

```
Attempting to mount an ISO, if one is present.
Starting update check.
http://127.0.0.1:8080/PrivateCloud/3.5.3/prod/repodata/repomd.xml: [Errno 14] HTTP Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below wiki article

https://wiki.centos.org/yum-errors

If above article doesn't help to resolve this issue please use https://bugs.centos.org/.

One of the configured repositories failed (FireAMP PrivateCloud Repository),
and yum doesn't have enough cached data to continue. At this point the only
safe thing yum can do is fail. There are a few ways to work "fix" this:

1. Contact the upstream for the repository and ask them to fix the problem
```

Download Output

â€f

Dieses Bild zeigt eine alternative Methode zum Mounten des Update-Images auf Ihrem VPC. In Version 3.5.x können Sie Remote-Speicherorte wie NFS-Speicher verwenden, um die Aktualisierungsdatei für Ihren VPC freizugeben.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

✖ Maintenance Mode

✖ Sanity Check Failing

ℹ Disabling T...

Mount an Update ISO

ISO Configuration

Mount Type

ISO ▾

ISO

NFS4

NFS3

Mount Status

No ISO mounted



❌ **Sanity Check Failing**

ℹ️ **Disabling TLS 1.0/1.1**

✅ **Config**

Mount an Update ISO

ISO Configuration	
Mount Type	NFS3 ▾
Remote Share	192.168.75.4:/AMPAG
Remote ISO File	PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso ←

✅ **Mount**

Mount Status

Mounted ISO
nfs 192.168.75.4:/AMPAG PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

Updates keep your Private Cloud device up to date.



 Check Update ISO

Content

 **3.5.2_202110122340**
Client Definitions, DFC, Tetra Content Version

 **ABSENT**
Protect DB Version

 [A content update is available.](#)

 ISO contains Protect DB snap
 Import a Protect DB snaps

Software

 **3.5.2_202110130433**
Private Cloud Software Version

 [A software update is available.](#)

â€f

Sanity Check Failing bezieht sich auf Protect DB, die derzeit nicht auf VPC verfügbar ist.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Check Update ISO

Content

3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

ABSENT

Protect DB Version

[A content update is available.](#)

ISO contains Protect DB s

Import a Protect DB sn

Software

3.5.2_202110130433

Private Cloud Software Version

[A software update is available.](#)

â€f


⚙️ Protect DB importing

The device is currently importing a Protect DB snapshot. This process can take

🗄️ State	🗄️ Started	🗄️ Finished
 ▶ Running	2021-11-19 17:04:05 +0000 about 20 hours ago	⌛ Please wait...

☰ Output

```
Extraction 233.2GB at 4.2MB/s eta: 0:00:02 99% [-----]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 99% [=====]
Extraction 233.2GB at 4.2MB/s eta: 0:00:00 100% [=====]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
Dropping samples table.
Dropping publishers table.
Dropping cas table.
Dropping certificates table.
Dropping cert_fingerprints table.
Recreating Protect DB tables from the schema in the snapshot.
Importing Protect DB data (this may take some time).
Importing detections table (this may take some time).
Importing binaries table (this may take some time).
```

 Download Output

â€f



✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

☰ State	📅 Started	📅 Finished
✔ Successful	2021-11-19 17:04:05 +0000 about 1 month ago	2021-12-21 01:08:11 +0000 less than a minute ago

☰ Output

```
Starting firehose_cassandra...
Starting firehose_cassandra_replay...
Starting firehose_publisher...
Starting firehose_publisher_replay...
Starting install-token-api...
Starting mgmt_unicorn...
Starting mongo_event_consumer...
Starting portal_unicorn...
Starting redis...
Starting retro-dipper...
Starting retrohose...
Starting retrohose-replay...
Starting tevent_listener...
Starting crond...
Starting flight...
Starting docker...
Sending notification (this may take some time).
```

[Download Output](#)

Nächstes Update automatisch starten



⚙ Importing Protect DB deltas.

Your Protect DB is being updated with threat intelligence that was queued during the last update. Each delta can take several hours to import, and system performance may be affected during this time.

You should run content updates at the end of the business day or week to ensure updates occur outside of peak use.

Queued Updates

20211116-2135

Queued Protect DB Update Version



2021

0.80%

Update Progress

â€f

Nach diesem sehr langwierigen Prozess des Imports von Protect DB Database können Sie Client Definition und Software verschieben und aktualisieren, was in etwa mehr als 3 Stunden in Anspruch nehmen kann.



✔ Content updated successfully

The device successfully performed a content update.

State	Started	Finished
✔ Successful	2021-12-21 03:10:11 +0000 28 minutes ago	2021-12-21 03:37:53 +0000 less than a minute ago

Output

```
Attempting to mount an ISO, if one is present.
PASS: The mount point / has sufficient space available: 23273033728 >= 1000000000
PASS: The mount point / has sufficient inodes available: 2018323 >= 100000
All checks succeeded!
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
Error: No matching Packages to list
Resolving Dependencies
--> Running transaction check
---> Package AMP-PrivateCloud-content.x86_64 0:3.5.2_202110122340-0 will be updated
---> Package AMP-PrivateCloud-content.x86_64 0:20211117234515-0 will be an update
---> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a64 will be updated
---> Package fireamp-amp-exprev-classifier.x86_64 0:3.4.0-0.1a76 will be an update
---> Package fireamp-apde-signatures.x86_64 0:935-1 will be updated
---> Package fireamp-apde-signatures.x86_64 0:1052-1 will be an update
---> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
---> Package fireamp-clamav-definitions.x86_64 0:1637186573-7 will be an update
---> Package fireamp-clamav-definitions.x86_64 0:1634076372-7 will be updated
```

Download Output

â€f

Und schließlich, bitte beachten Sie, dass dieser Prozess sehr lange dauern wird.

Für VPC-Appliance besuchen Sie diese TZ, die andere Methoden, wie HW-Appliance zu aktualisieren, Mounten ISO-Datei und Boot von USB enthalten.

<https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5>

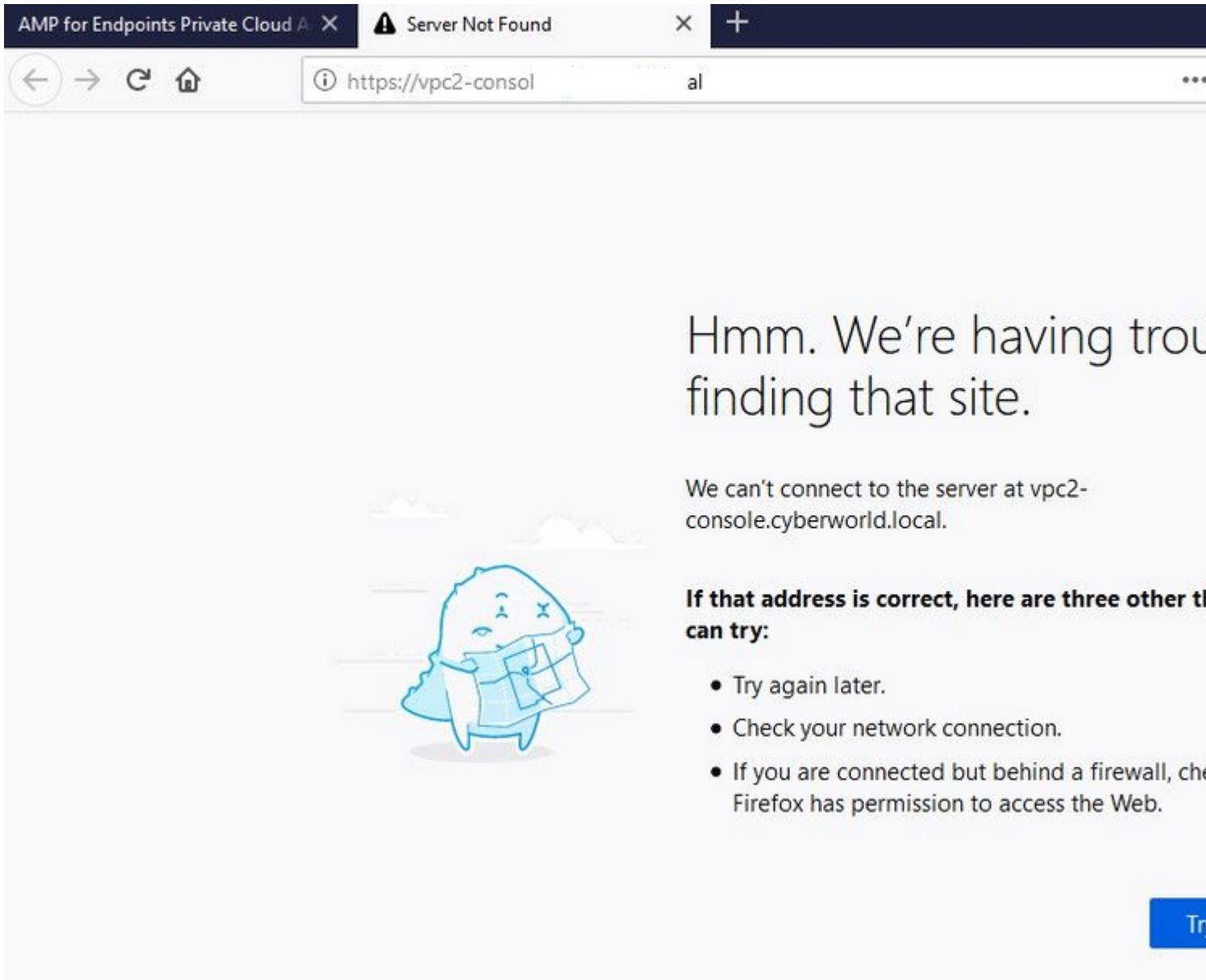
â€f

ï½ï½ NUR ï½ï½

Grundlegende Fehlerbehebung

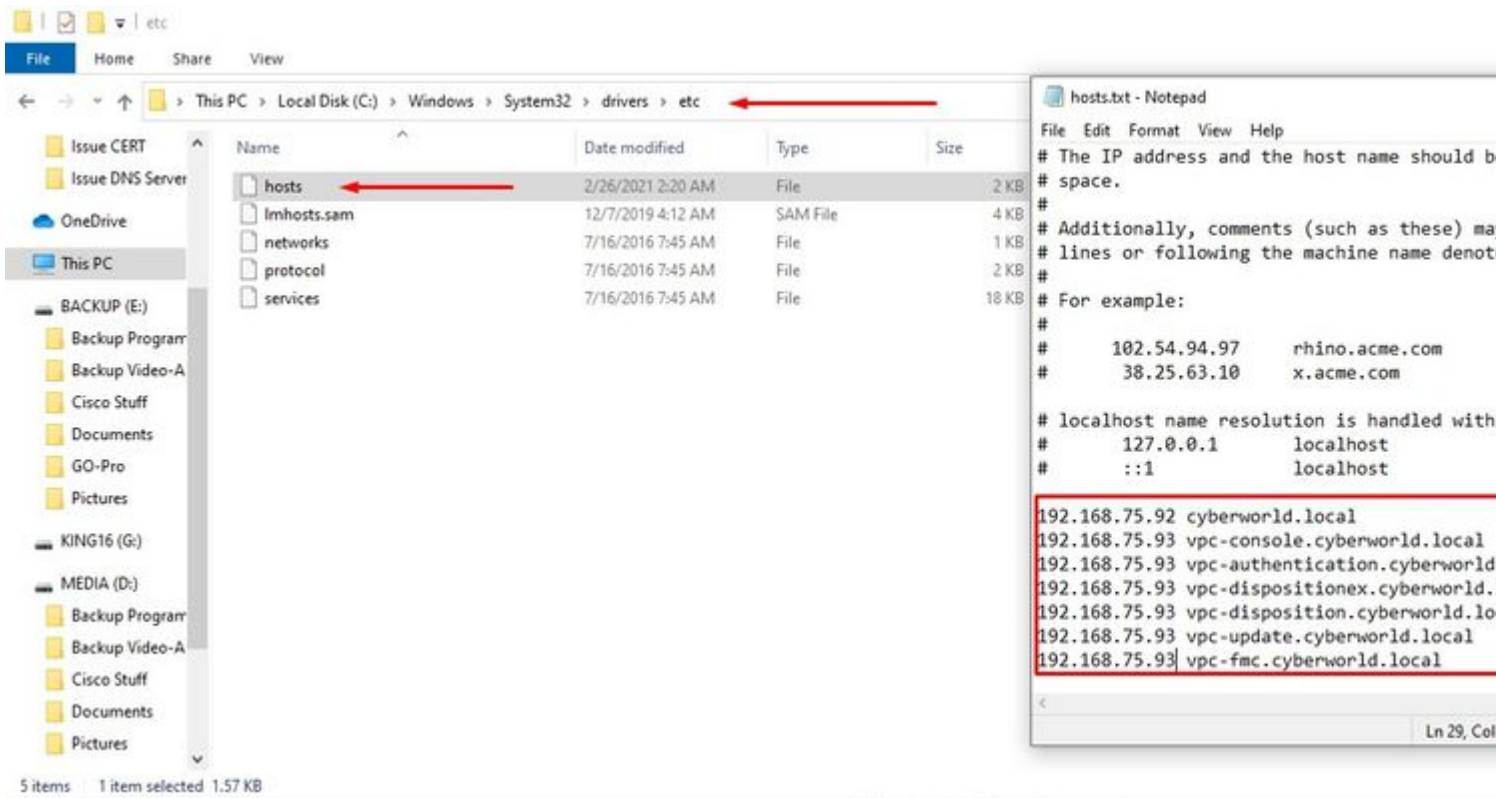
Problem #1 - FQDN und DNS-Server

Das erste Problem besteht darin, dass der DNS-Server nicht eingerichtet ist und nicht alle FQDN ordnungsgemäß aufgezeichnet und behoben wurden. Das Problem kann so aussehen, wenn Sie versuchen, über das "Feuer"-Symbol für Secure Endpoint zur Konsole für sichere Endgeräte zu navigieren. Wenn Sie nur die IP-Adresse verwenden, funktioniert es, aber Sie können den Connector nicht herunterladen. Wie Sie auf dem ^{dritten} Bild unten sehen können.

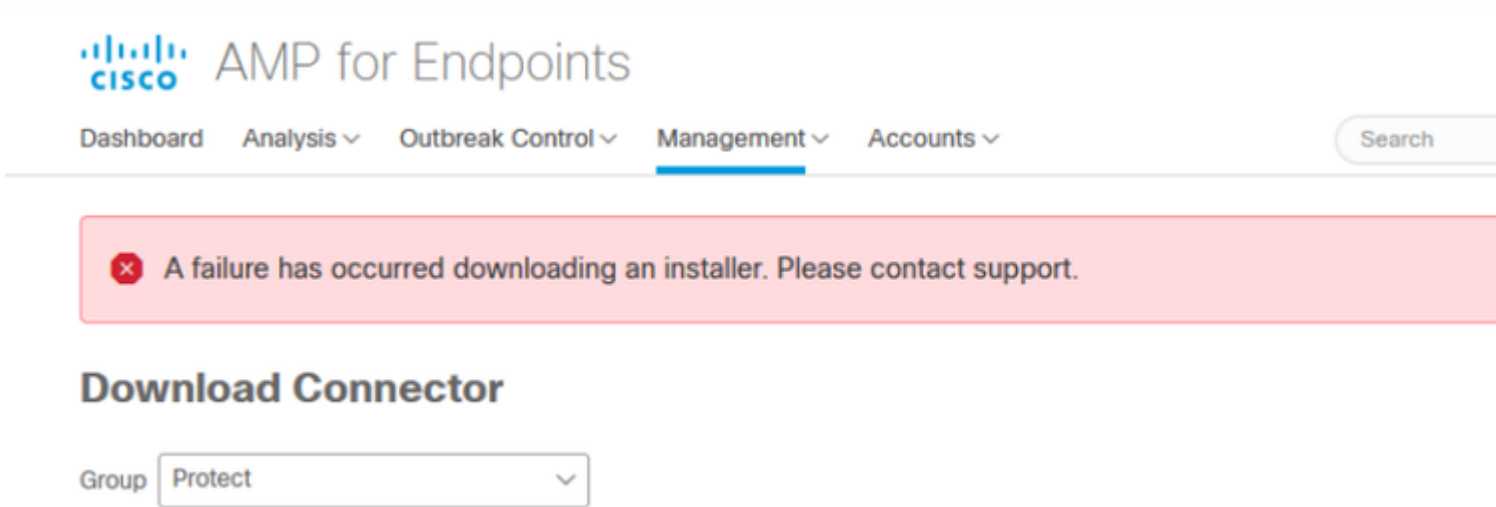


â€f

Wenn Sie die HOSTS-Datei auf Ihrem lokalen Computer wie im Bild gezeigt ändern, lösen Sie das Problem und Sie am Ende mit Fehlern.



Sie erhalten diese Fehlermeldung, wenn Sie versuchen, das Installationsprogramm für Secure Endpoint Connector herunterzuladen.



Nach einigen Fehlerbehebungen war die einzige richtige Lösung, den DNS-Server einzurichten.

```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0000)
=====
Server:          8.8.8.x
Address:         8.8.8.x#53

** server can't find vPC-Console.cyberworld.local: NXDOMAIN
```

Sobald Sie alle FQDNs in Ihrem DNS-Server aufzeichnen und den Eintrag in Virtual Private Cloud von Public DNS auf Ihren DNS-Server ändern, läuft alles wie es sollte.

The screenshot shows the AMP for Endpoints Private Cloud Administration Portal. The top navigation bar includes the Cisco logo, the title 'AMP for Endpoints Private Cloud Administration Portal', and links for 'Support' and 'An'. Below this is a secondary navigation bar with 'Configuration', 'Operations', 'Status', 'Integrations', and 'Support' menus. The 'Configuration' menu is expanded, showing options like 'Device Summary', 'Change Password', 'Cisco Cloud', 'Network' (highlighted with a red box), 'Date and Time', 'Certificate Authorities', 'Proxy', 'Notifications', 'License', 'Email', 'Backup', 'SSH', 'Syslog', 'Updates', and 'Services'. The background content shows network settings for an interface, including fields for 'IP Address' (192.168...), 'Subnet Mask' (255.255...), and 'Gateway' (192.168...).

Warning: Address and Hostname Changes

If you change the IP address of the interface you must also update the DNS records for each of your configured services to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS name.

[View the Configuration help page for a list of affected services.](#)

DNS

Primary DNS Server

192.168.75.4





Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

⚙️ Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

 **Reconfigure Now**

 Reconfiguration



✔️ **Configuration saved.**



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Home / Operations - Apply Configuration / Details

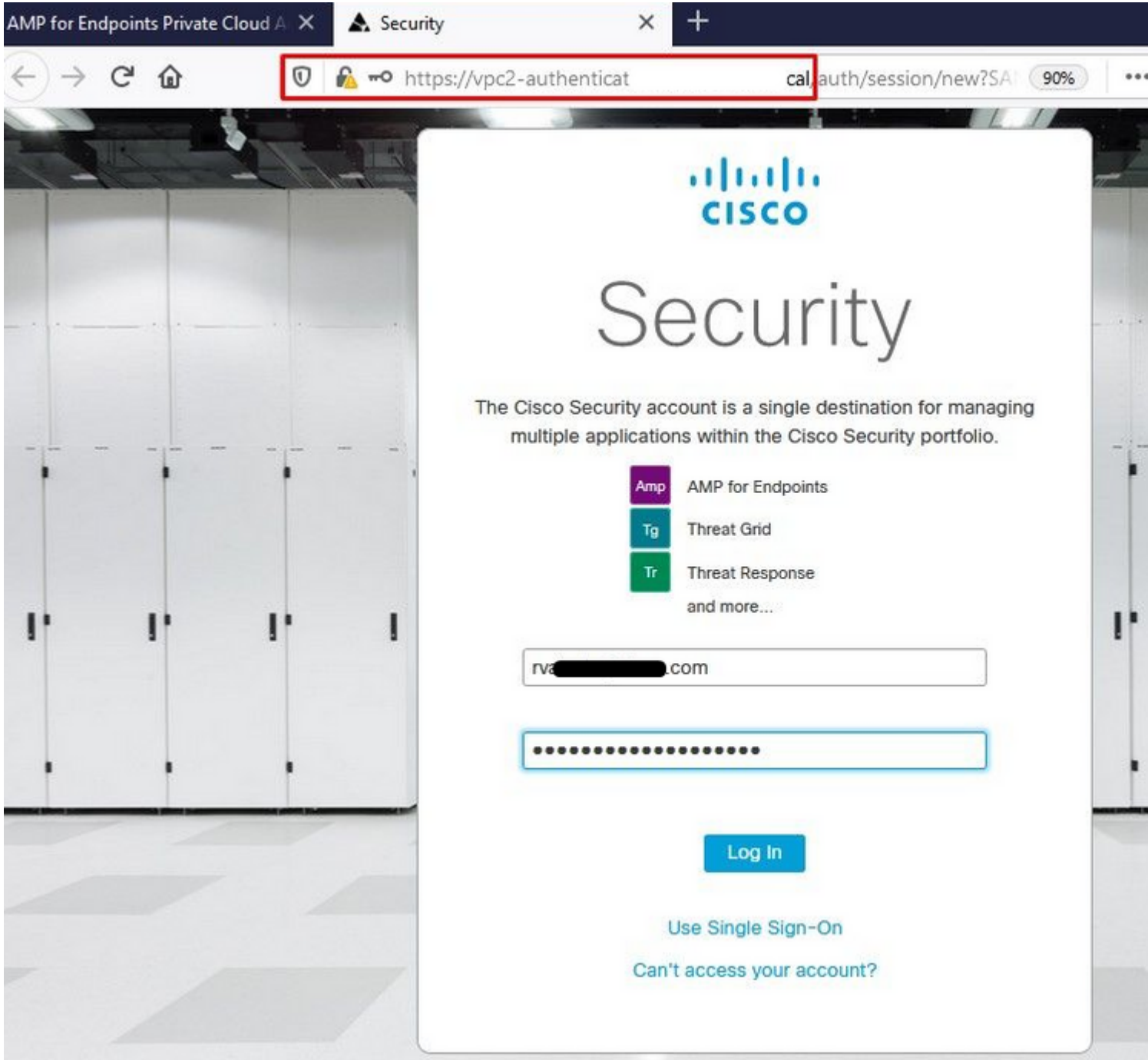
State	Started	Finished
Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...

Output

```
[2021-04-12T00:20:43+00:00] DEBUG: Found current_uid == nil, so we are creating a new file, updating o
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] owner changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_gid == nil, so we are creating a new file, updating g
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] group changed to 4015
[2021-04-12T00:20:43+00:00] DEBUG: Found current_mode == nil, so we are creating a new file, updating m
[2021-04-12T00:20:43+00:00] INFO: file[/tmp/cqlsh_check_superuser_password.cql] mode changed to 600
[2021-04-12T00:20:43+00:00] DEBUG: Restoring selinux security content with /sbin/restorecon -R "/tmp/c
rd.cql"
[2021-04-12T00:20:43+00:00] INFO: Processing execute[cqlsh_check_superuser_password] action run (/var/
viders/cqlsh.rb line 16)
[2021-04-12T00:20:43+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Ch
[2021-04-12T00:20:43+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_p
r::Execute
[2021-04-12T00:20:43+00:00] INFO: Retrying execution of execute[cqlsh_check_superuser_password], 19 at
[2021-04-12T00:20:45+00:00] DEBUG: Providers for generic execute resource enabled on node include: [Ch
[2021-04-12T00:20:45+00:00] DEBUG: Provider for action run on resource execute[cqlsh_check_superuser_p
r::Execute
```

Download Output

An dieser Stelle können Sie sich anmelden und den Connector herunterladen.



â€f

â€f

Sie erhalten den Assistenten für Richtlinien für sichere Endgeräte für Ihre Umgebung. Es führt Sie durch die Auswahl der Antiviren-Produkte, die Sie ggf. verwenden, sowie durch die Proxy-Server und die Richtlinien, die Sie bereitstellen möchten. Wählen Sie eine entsprechende Taste für die Einrichtung..., hängt vom Betriebssystem des Steckverbinders ab.

Die Seite "Vorhandene Sicherheitsprodukte" wird angezeigt, wie im Bild gezeigt. Wählen Sie die von Ihnen verwendeten Sicherheitsprodukte aus. Es werden automatisch anwendbare Ausschlüsse generiert, um Leistungsprobleme auf Ihren Endgeräten zu vermeiden. Wählen Sie auf **Weiter**.

AMP for Endpoints

Dashboard Analysis Outbreak Control Management Accounts Search

Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

Getting Started

- [View Online Help](#)
- [Download Cisco AMP for Endpoints User Guide](#)
- [Download Cisco AMP for Endpoints Deployment Strategy](#)

Deploy AMP for Endpoints Connectors

- [Set Up Windows Connector](#)
- [Set Up Mac Connector](#)
- [Set Up Linux Connector](#)

Demo Data

Demo Data allows you to see how Cisco AMP for Endpoints works by populating your Console with replayed data from actual malware infections. Enabling Demo Data will add computers and events to your Cisco AMP for Endpoints Console so you can see how the Dashboard, File Trajectory, Device Trajectory, Threat Root Cause, and Detections and Events displays behave when malware is detected. Demo Data can coexist with live data from your Cisco AMP for Endpoints deployment, however, because of the severity of some of the Demo Data

Demo Computers

WannaCry [Click here to view PDF](#)
The WannaCry attack involves a remote command and control (Server Message Block) service using the EternalBlue exploit to compromise, the attacker drops the WannaCry ransomware on the system identified by AMP for Endpoints using ransomware signatures later by AMP Cloud signatures.

SFEicar [Click here to view PDF](#)
Learn how Indications of Compromise can appear in your console and how to determine their effects.

ZAccess [Click here to view PDF](#)
Use Device Trajectory to watch a rootkit exploit a vulnerable computer, and use File Trajectory to discover files that were compromised.

ZBot [Click here to view PDF](#)
See how a vulnerable version of Internet Explorer can be exploited. Use Device Trajectory to learn what happened and how to stop the future execution of vulnerable processes.

CozyDuke [Click here to view PDF](#)
Trace a detection back to an abused DLL search path, identify the upstream CnC, and deploy an Endpoint Protection Agent.

â€f

Connector herunterladen.

Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

Audit Only
Used when you're still learning about the product and want to install it without any impact to your existing systems.

Policy Details

Files: Audited
Network: Blocked
Offline Engine: TETRA

Download

Protect
Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.

Policy Details

Files: Quarantined
Network: Blocked
Offline Engine: TETRA

Download

Triage
Used when you have a known or suspected infected machine.

Policy Details

Files: Quarantined
Network: Blocked
Offline Engine: TETRA

Download

Server
Used when you're installing a connector on standard Windows servers.

Requirements

Files: Audited
Network: Off
Offline Engine: TETRA

Download

installing a connector on Windows Domain Controllers.

Requirements

Files: Audited
Network: Off
Offline Engine: TETRA

Download

< Back

Step 4: Verify, Contain, and Protect

Opening amp_Protect.exe

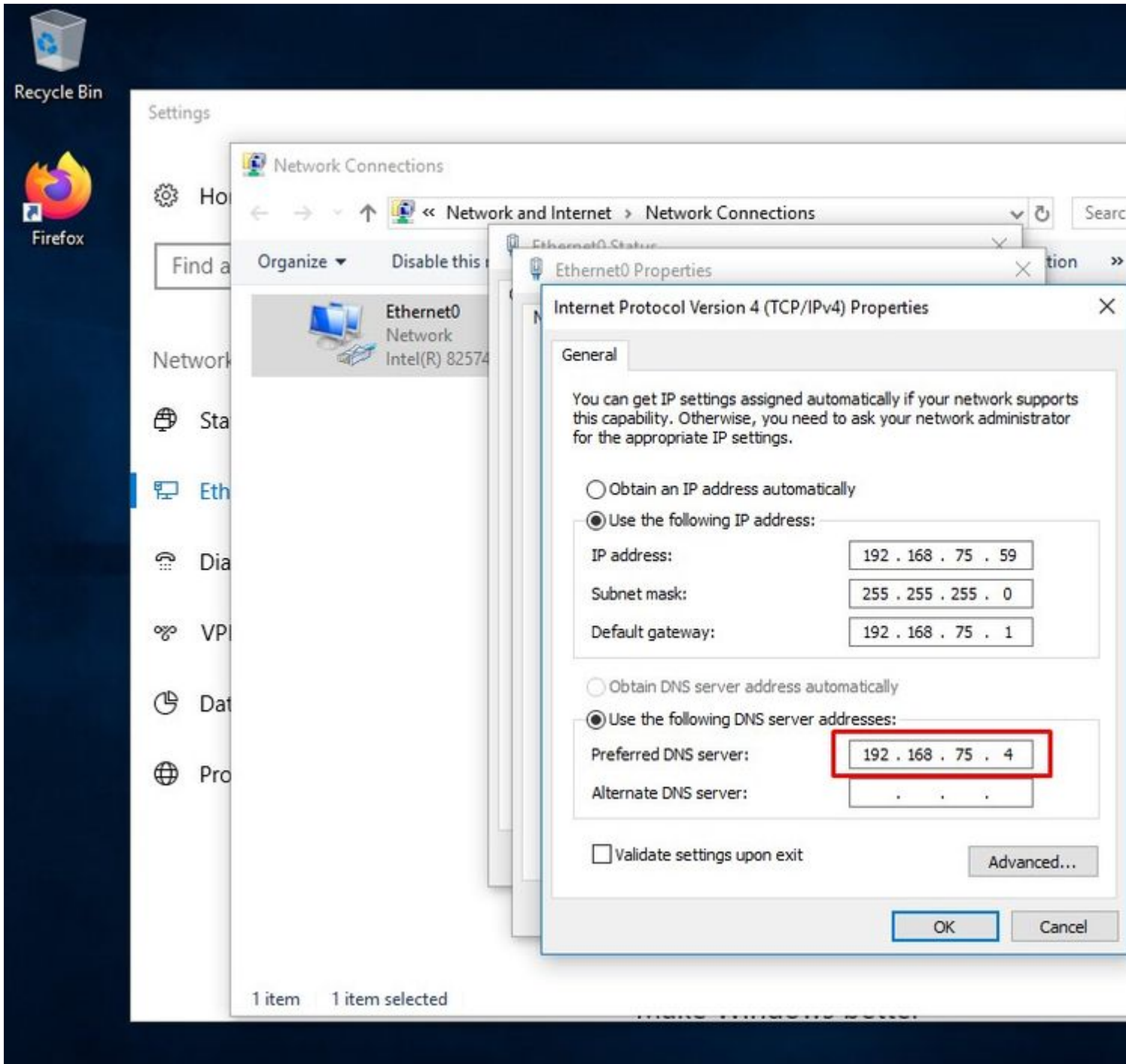
You have chosen to open:

amp_Protect.exe
which is: exe File
from: https://vpc-con...

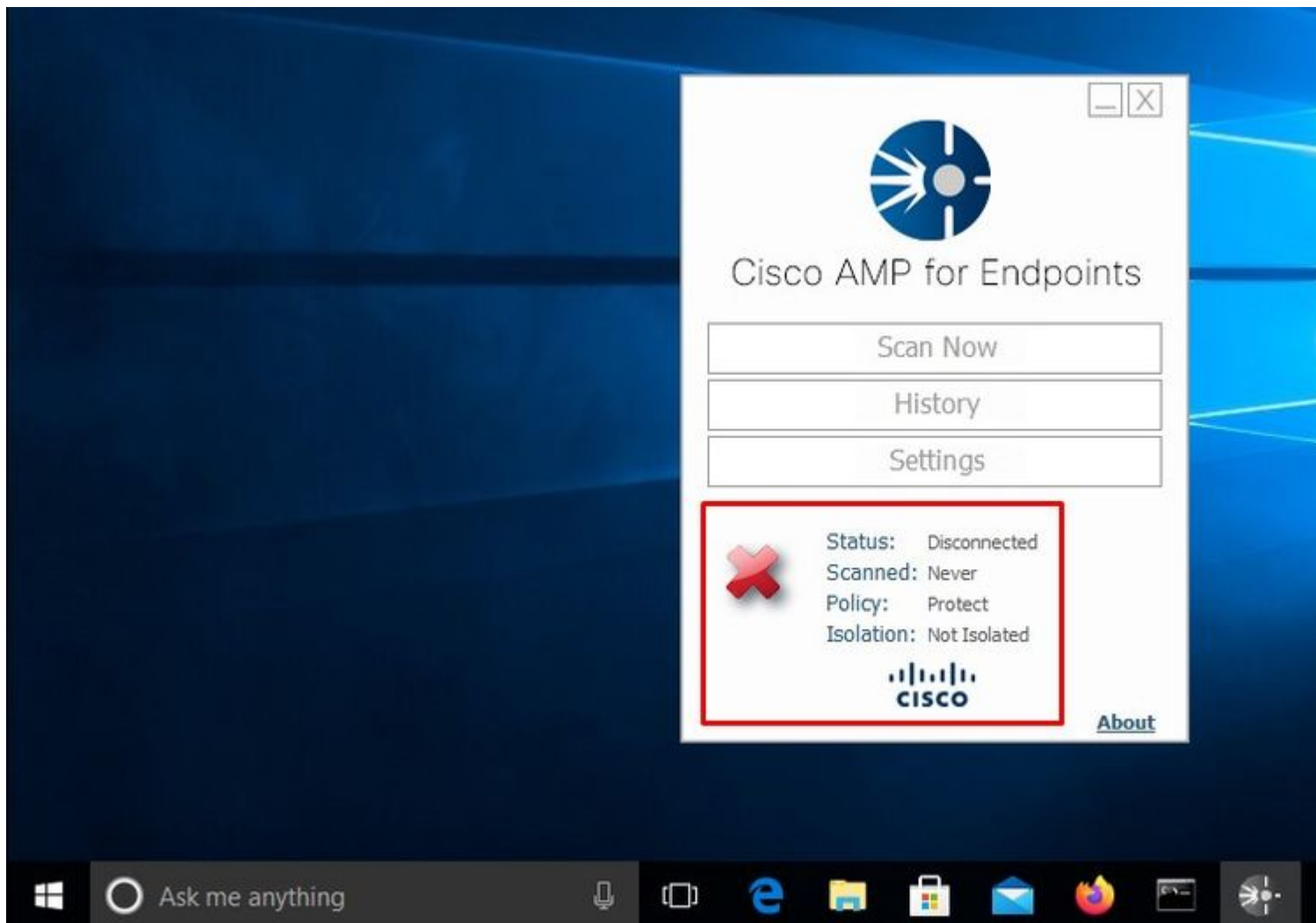
Would you like to save this f...

Problem #2 - Problem mit Stammzertifizierungsstelle

Das nächste Problem, mit dem Sie konfrontiert werden können, ist, dass nach der Ersteinstallation der Connector als nicht verbunden angezeigt werden kann, wenn Sie Ihre eigenen internen Zertifikate verwenden.



Nach der Installation des Connectors kann Secure Endpoint als "Disconnected" (Verbindung getrennt) angezeigt werden. Führen Sie das Diagnosepaket aus, und durchsuchen Sie die Protokolle. Sie können das Problem ermitteln.



Basierend auf dieser Ausgabe aus dem Diagnosepaket wird der Fehler der Stammzertifizierungsstelle angezeigt.


```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworld.com/
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificate
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

Nachdem Sie die Stammzertifizierungsstelle in den Speicher der vertrauenswürdigen Stammzertifizierungsstelle hochgeladen haben, starten Sie den Dienst für sichere Endgeräte neu. Alles beginnt wie erwartet zu funktionieren.



AMP-vPC-...







Cisco AMP for Endpoints

Scan Now

History

Settings

 Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated



[About](#)

Certificate

General Details Certifi



Certificate

**This CA Root certifi
install this certific
Authorities store.**

Issued to: All

Issued by: All

Valid from: 4/





Cisco AMP for Endpoints

Scan Now

History

Settings

 Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated

 [About](#)

← Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists from your disk to a certificate store.

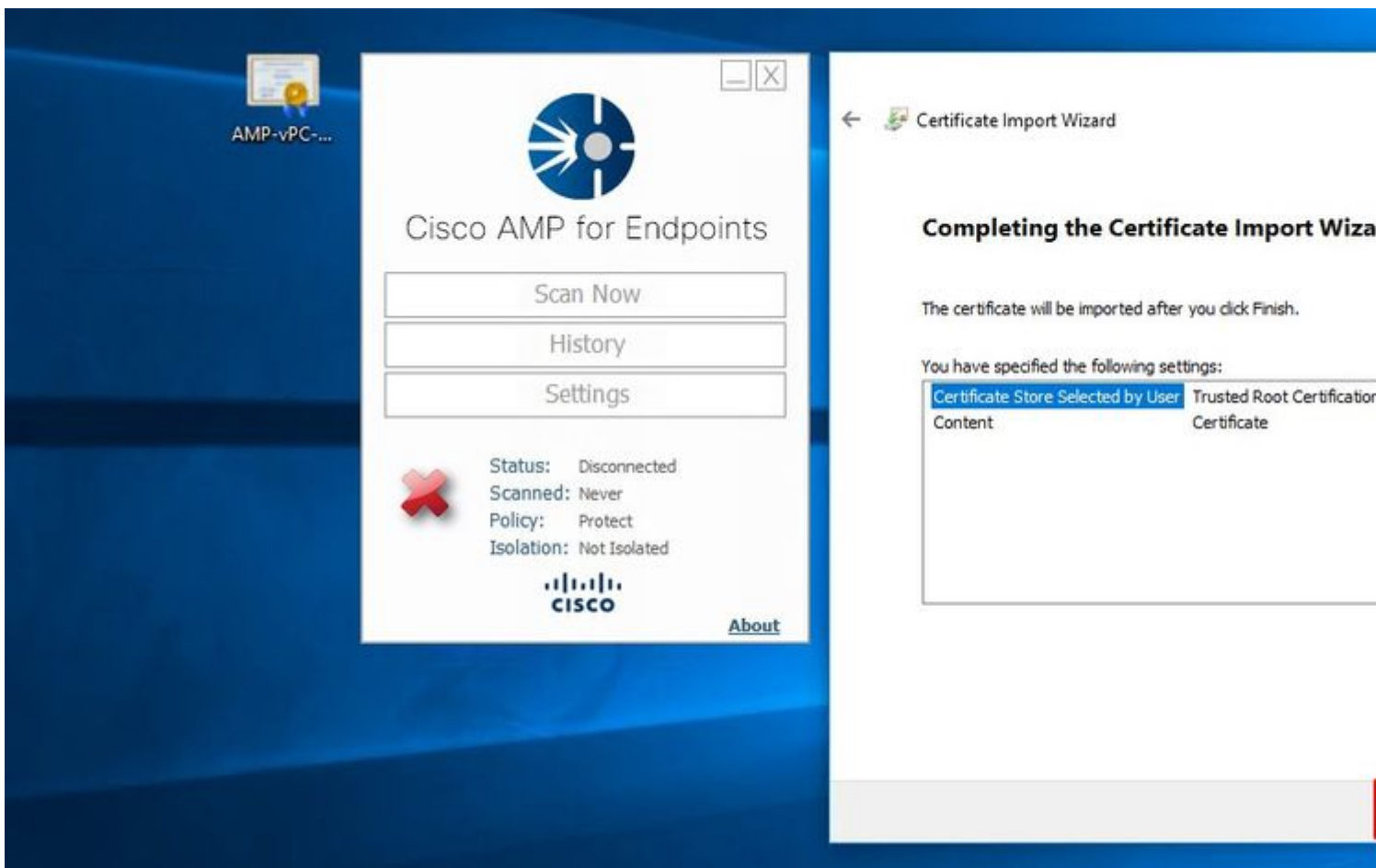
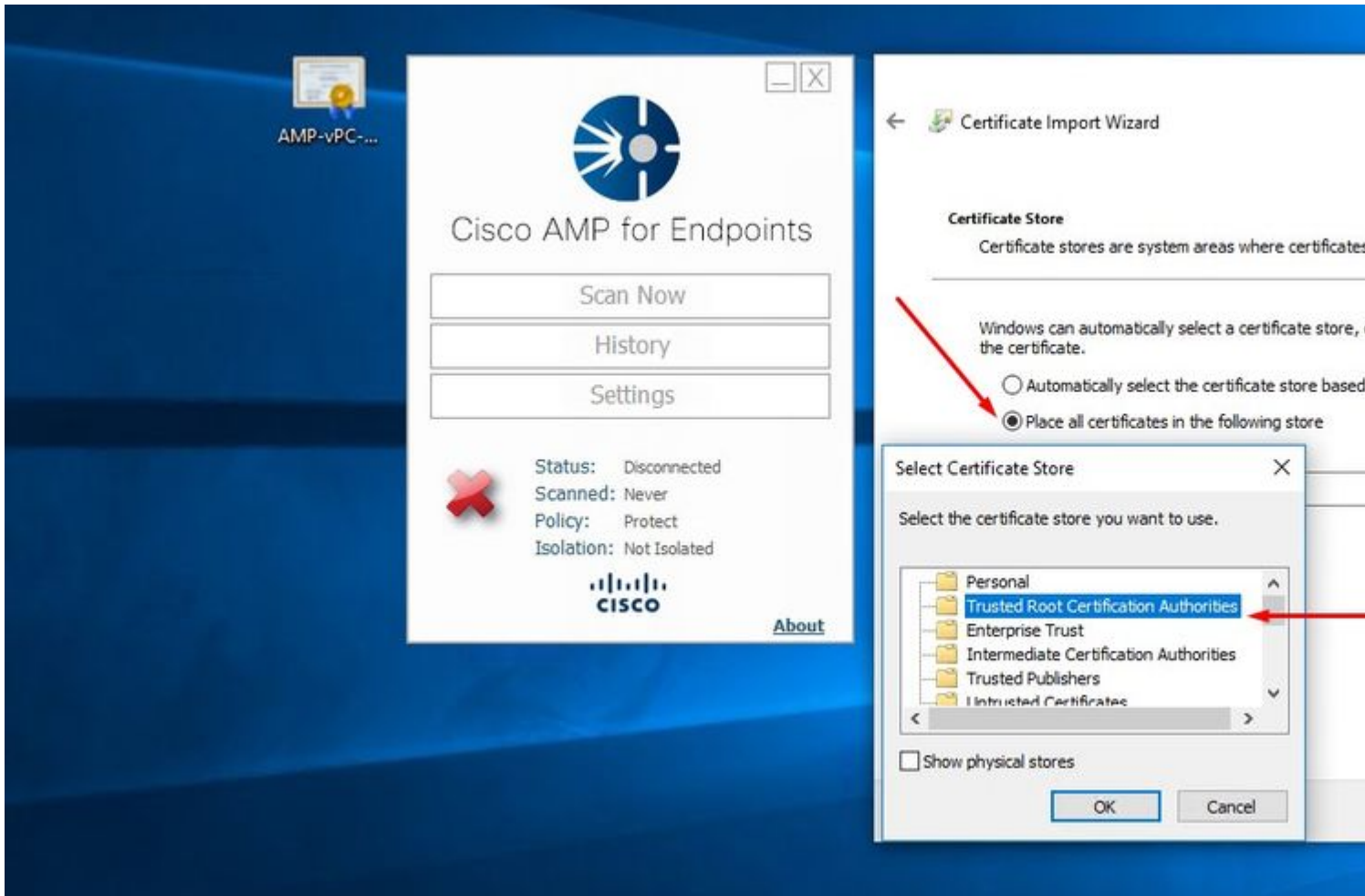
A certificate, which is issued by a certification authority and contains information used to protect data or to establish connections. A certificate store is the system area where certificates are stored.

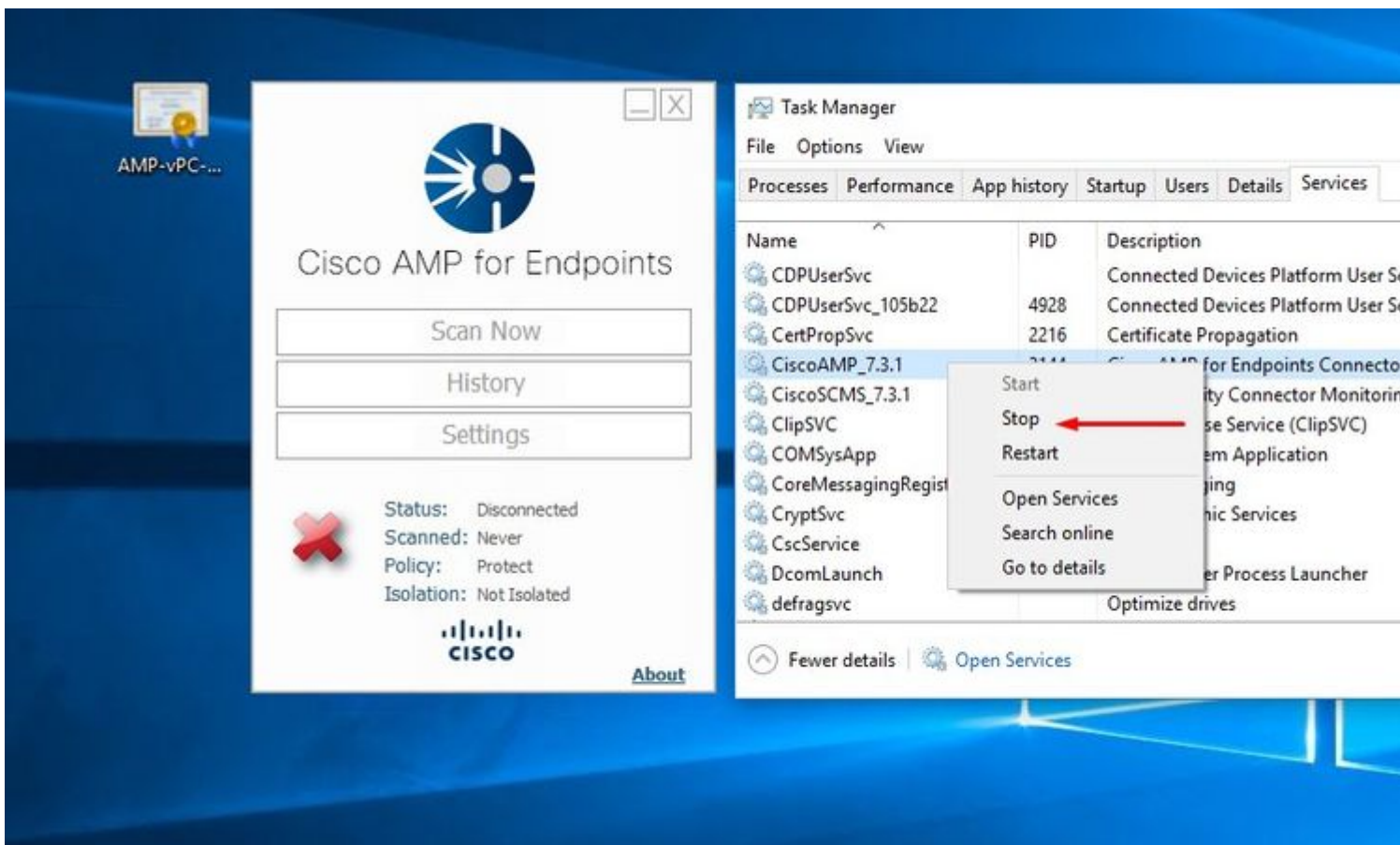
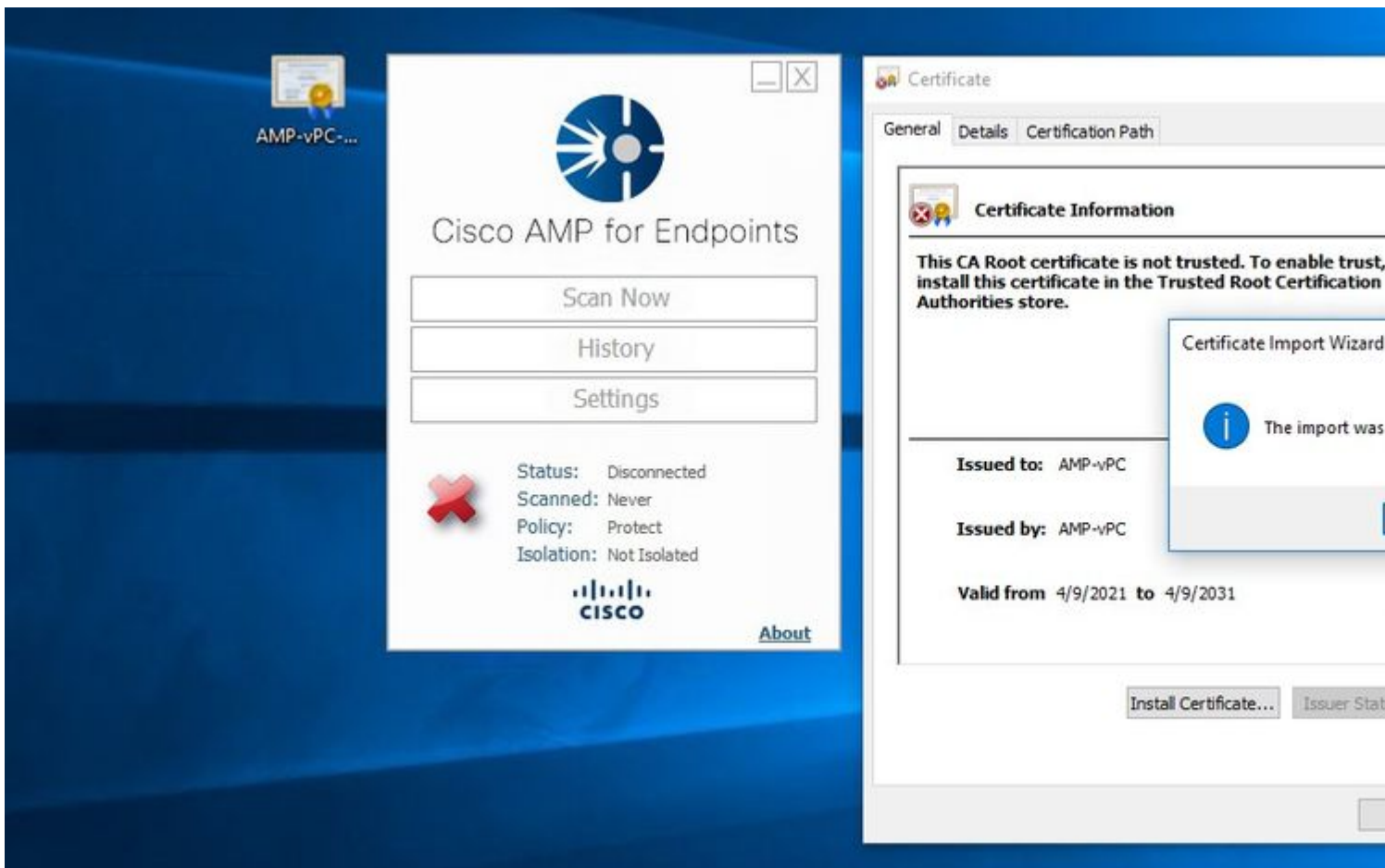
Store Location

Current User

Local Machine

To continue, click Next.





Sobald das Bounce des Secure Endpoint-Service-Connectors abgeschlossen ist, können Sie wie erwartet online gehen.






Cisco AMP for Endpoints

Scan Now

History

Settings



Status: Connected
Scanned: Never
Policy: Protect
Isolation: Not Isolated



CISCO

[About](#)

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	PID	Description
CDPUserSvc		Connected Devices Platform U
CDPUserSvc_105b22	4928	Connected Devices Platform U
CertPropSvc	2216	Certificate Propagation
CiscoAMP_7.3.1	1288	Cisco AMP for Endpoints Conn
CiscoSCMS_7.3.1	2844	Cisco Security Connector Mon
ClipSVC	5248	Client License Service (ClipSVC
COMSysApp		COM+ System Application
CoreMessagingRegistrar	2384	CoreMessaging
CryptSvc	2576	Cryptographic Services
CscService		Offline Files
DcomLaunch	880	DCOM Server Process Launche
defragsvc		Optimize drives

Fewer details | Open Services

AMP for Endpoints Private Cloud A X Dashboard X +

← → ↻ 🏠 <https://vpc2-console> dashboard 80%

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Dashboard

Dashboard **Inbox** Overview Events

[Refresh All](#) Auto-Refresh ▾ ⓘ [Reset](#) [New Filter](#) 30

0% compromised ⓘ

Compromises ⓘ Inbox

Top 0 / 1

Protect

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Quarantined Detections ⓘ Quarantine Events

Top 0 / 1

Protect

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Significant Compromise Artifacts ⓘ

No artifacts

Compromise Event Types ⓘ

No event types

â€f

Bösartige Aktivitäten getestet

Dashboard

Dashboard **Inbox** Overview Events

Refresh All Auto-Refresh ?

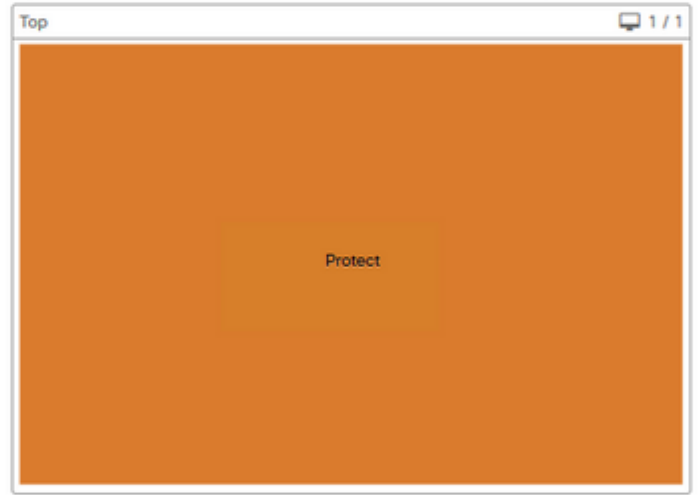
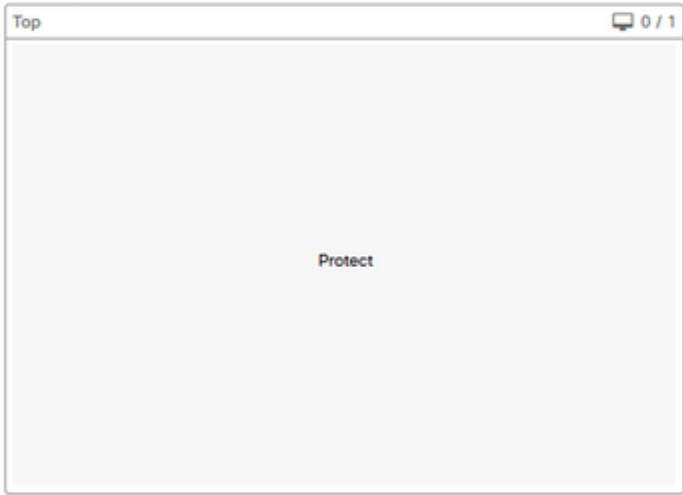
Reset New Filter

0% compromised ?

Inbox Status
0 Require Attention 0 In Progress 0 Resolved

Compromises ? [Inbox](#)

Quarantined Detections ? [Quarantine Events](#)



13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Significant Compromise Artifacts ?

Compromise Event Types ?

No artifacts

No event types

â€f

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.