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. â€Œ

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. â€Œ

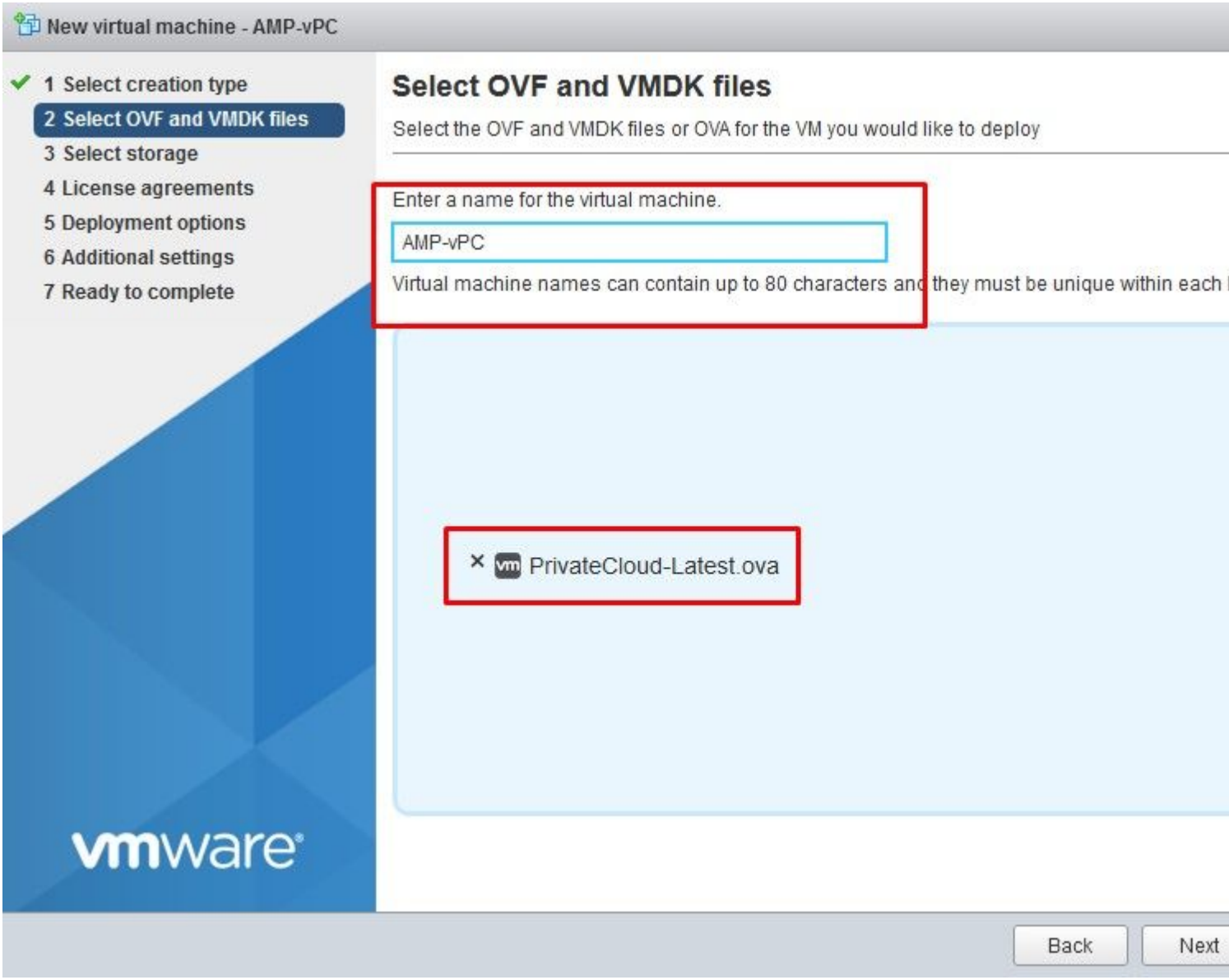
VPC-Bereitstellung

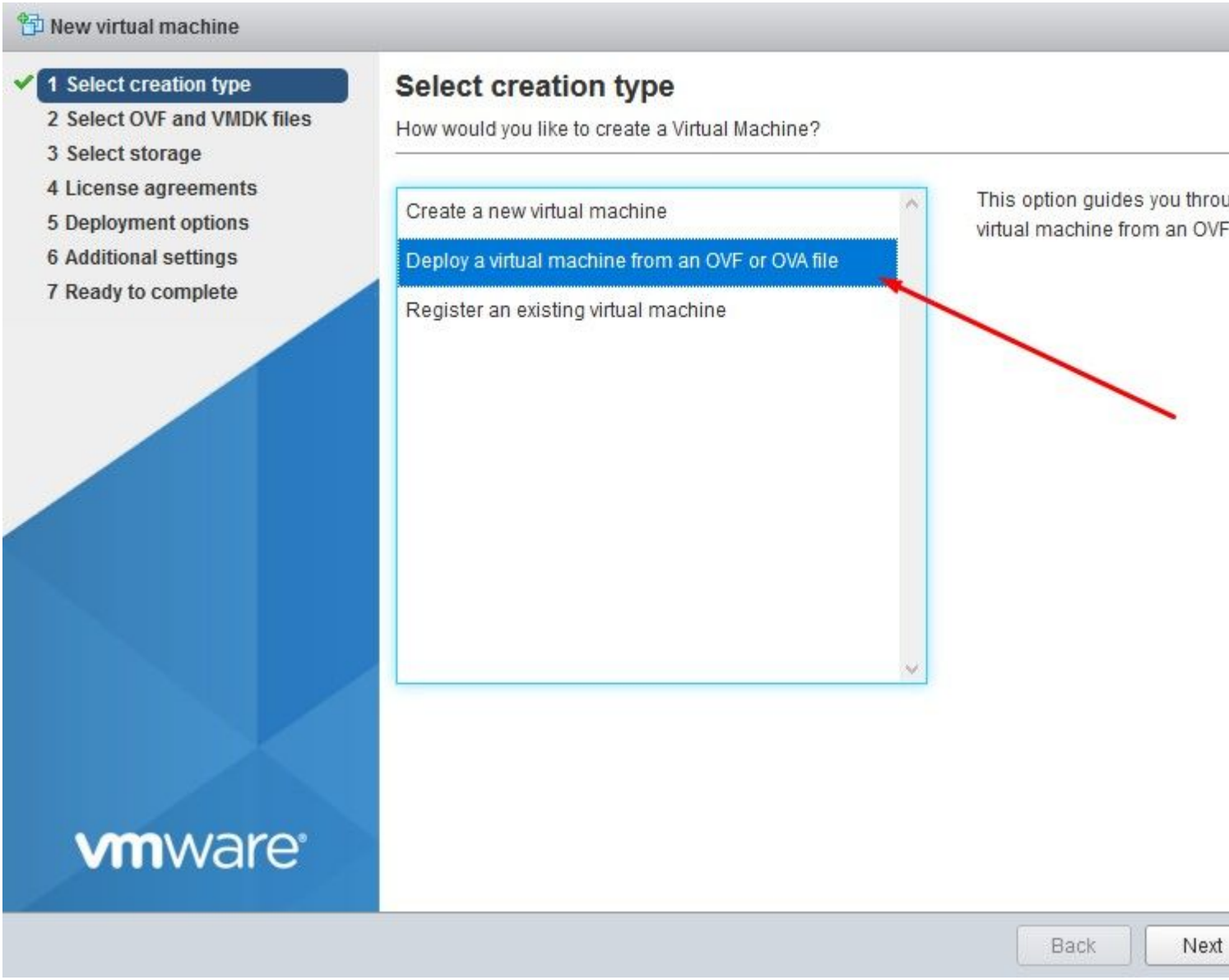
Wählen Sie die in der eDelivery- oder der Berechtigungs-E-Mail angegebene URL aus. Laden Sie die OVA-Datei herunter, und setzen Sie die Installation fort.

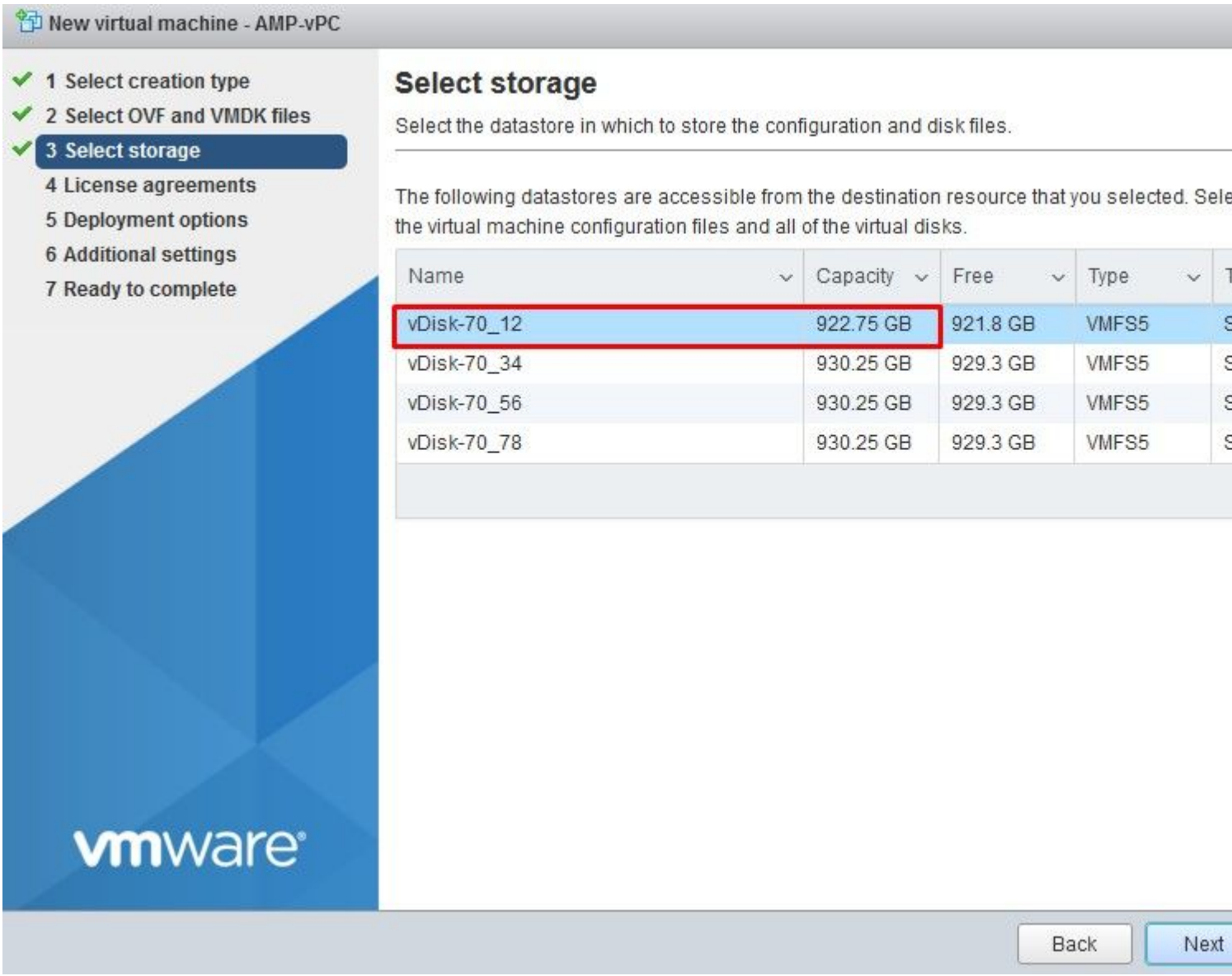
VM-Installation

Schritt 1:

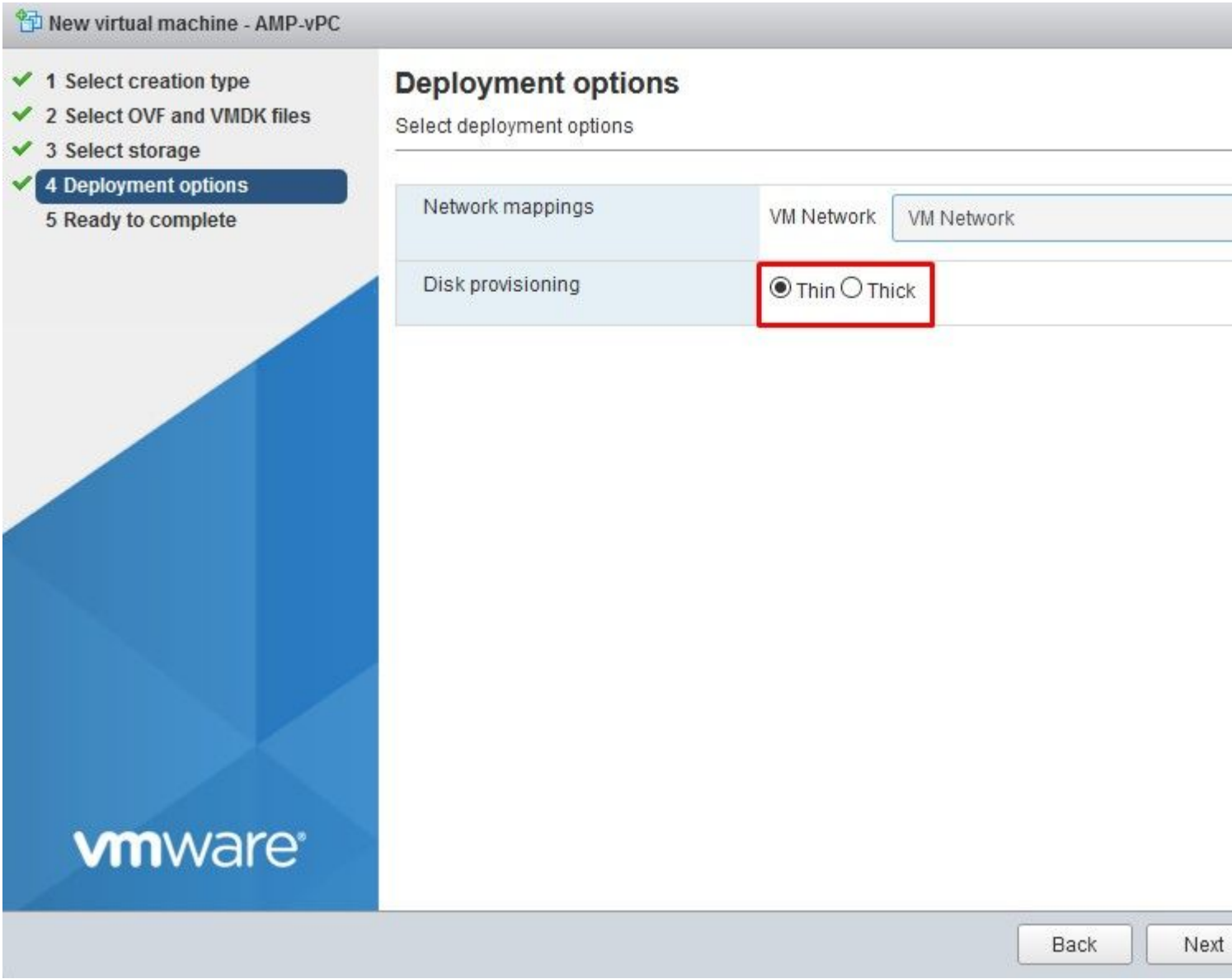
Navigieren Sie zu **Datei > OVF-Vorlage bereitstellen**, um den Assistenten **OVF-Vorlage bereitstellen** zu öffnen, wie im Bild dargestellt.


New virtual machine - AMP-vPC
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.
AMP-vPC
Virtual machine names can contain up to 80 characters and they must be unique within each
PrivateCloud-Latest.ova
vmware
Back
Next


New virtual machine
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 throu
virtual machine from an OVF
vmware
Back
Next

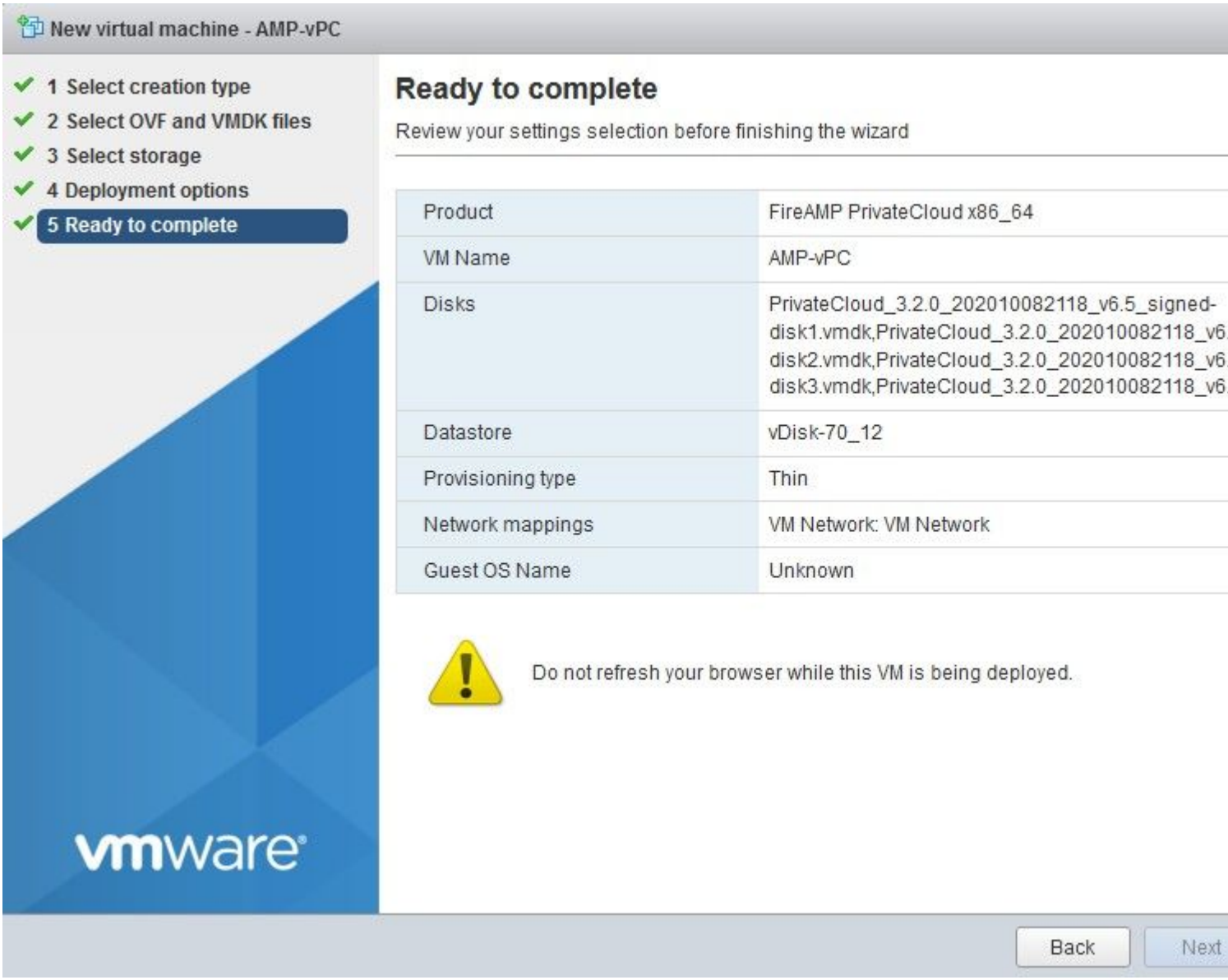


Hinweis: **Thick Provisioning** reserviert Speicherplatz, wenn ein Datenträger erstellt wird. Wenn Sie diese Option auswählen, kann sie die Leistung gegenüber **Thin Provisioned** verbessern. Dies ist jedoch nicht obligatorisch. Wählen Sie nun auf **Weiter**, wie im Bild gezeigt.

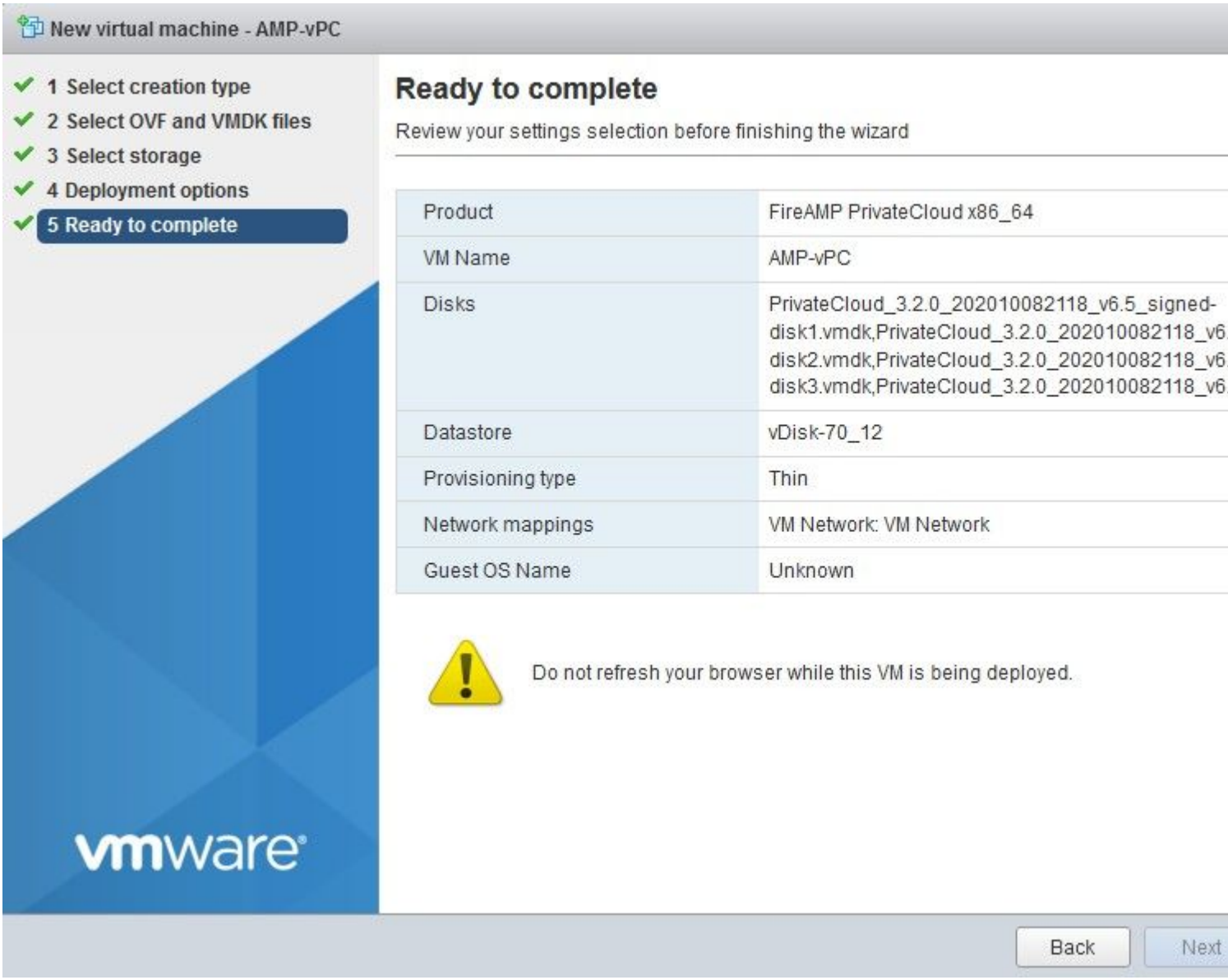


Phase 2:

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)**.



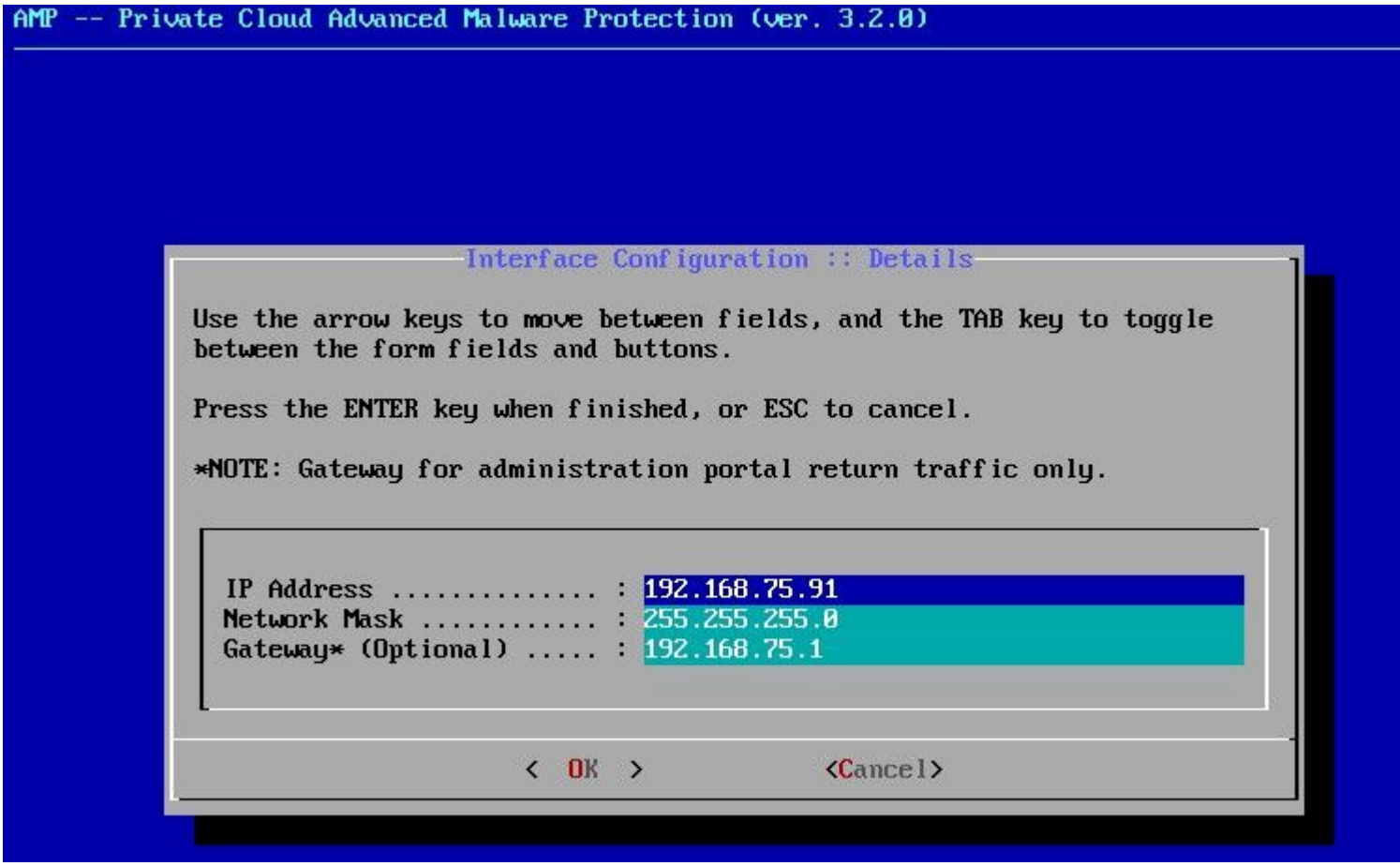
Erste Einrichtung der Admin-Schnittstelle



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

Schritt 1:

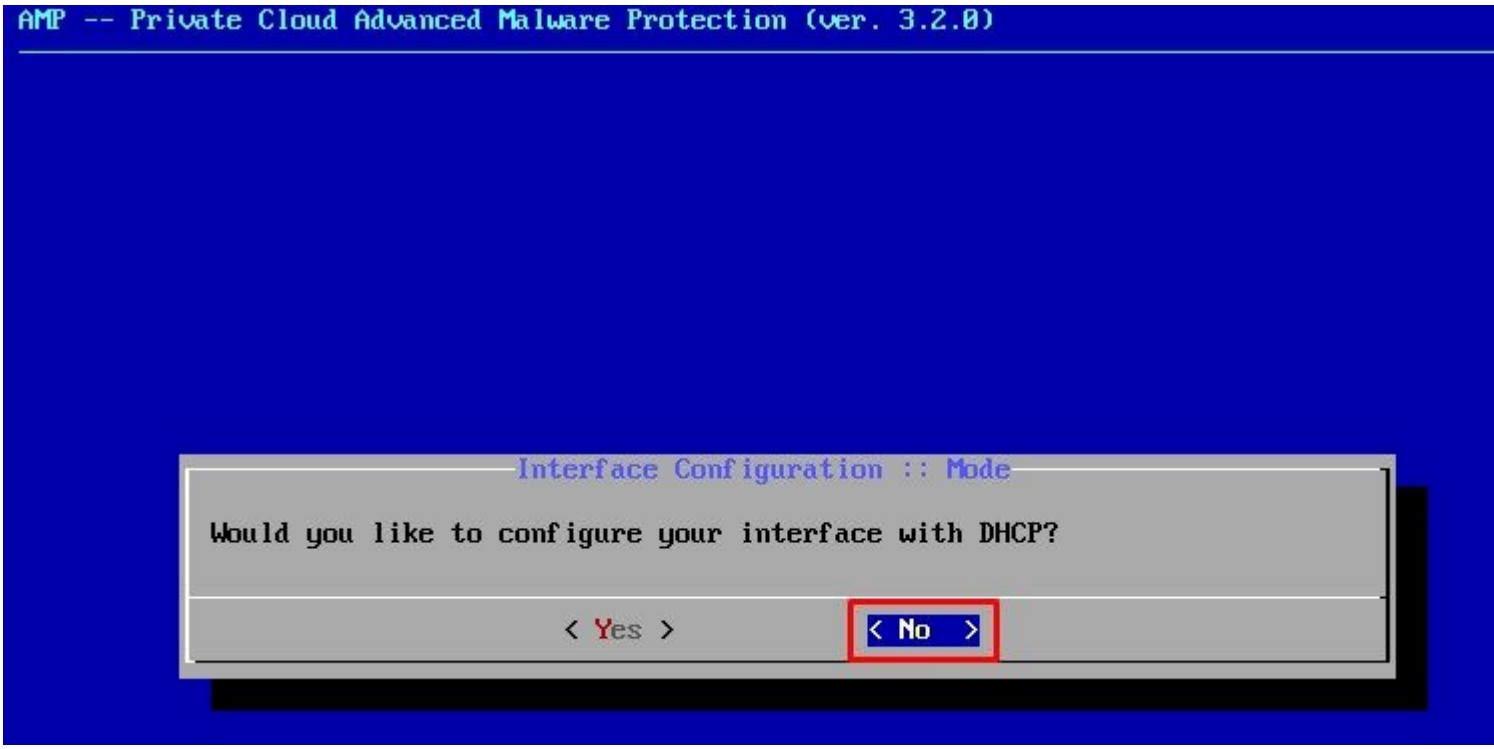
Sie können feststellen, dass die URL [**UNCONFIGURED]** anzeigt, wenn die Schnittstelle keine IP-Adresse vom DHCP-Server erhalten hat. Beachten Sie, dass diese Schnittstelle die **Management**-Schnittstelle ist. Dies ist nicht die **Produktions**-Schnittstelle.



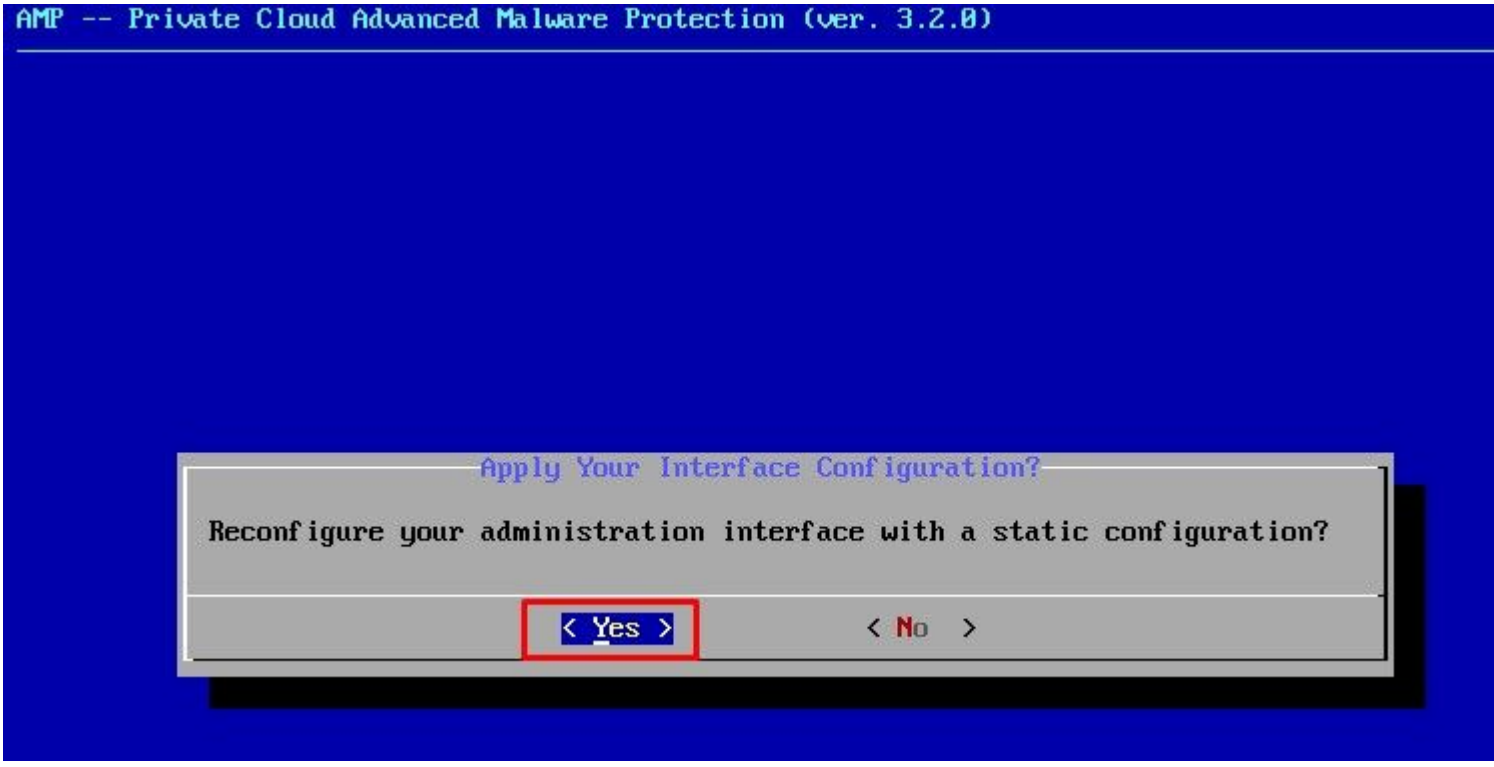
Phase 2:

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.

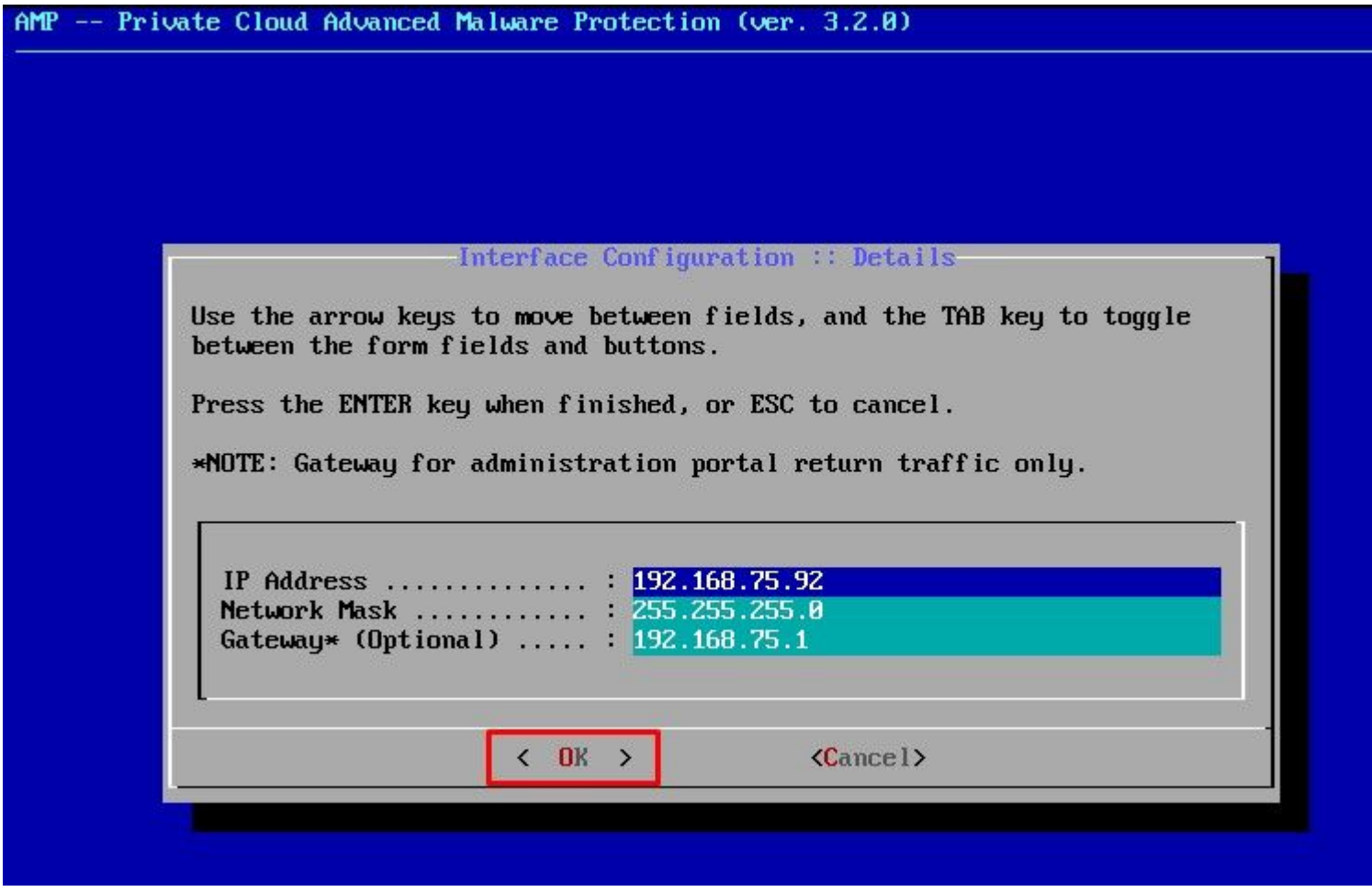


Im erscheinenden Fenster wählen Sie **Ja** und wählen **Enter** key.



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:
eady uses address 192.168.75.91.
ERROR      : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:
eady uses address 192.168.75.91.
ERROR      : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:
eady uses address 192.168.75.91.
================================================================================
ERROR: The interface failed to reconfigure.
================================================================================
Press ENTER key to continue...

_
```



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

Schritt 3:

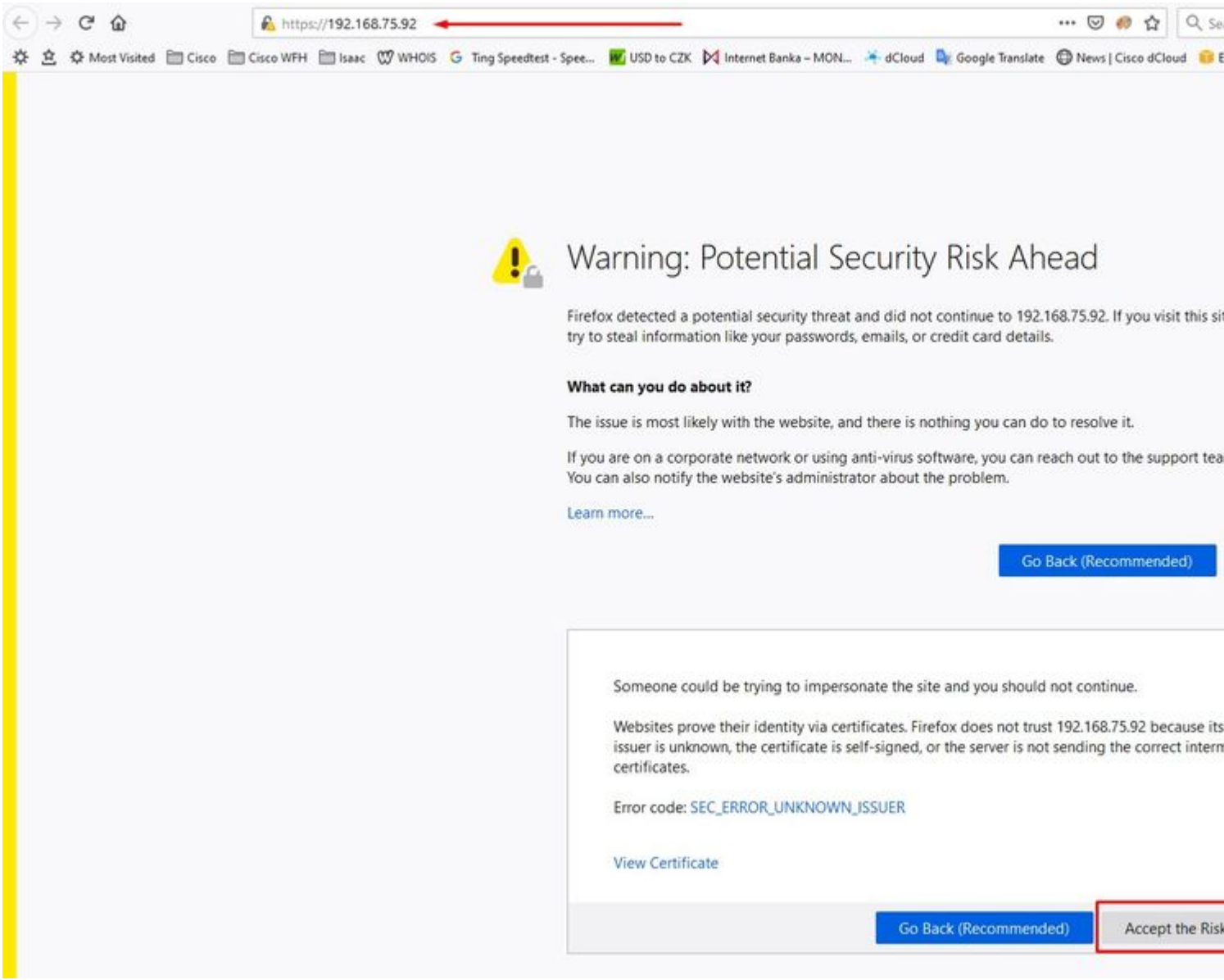
Warten Sie, bis der blaue Bildschirm mit Ihrer neuen STATIC IP erneut angezeigt wird. Bitte beachten Sie auch das **einmalige Passwort**. Machen Sie sich Notizen, und öffnen Sie unseren Browser.

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.

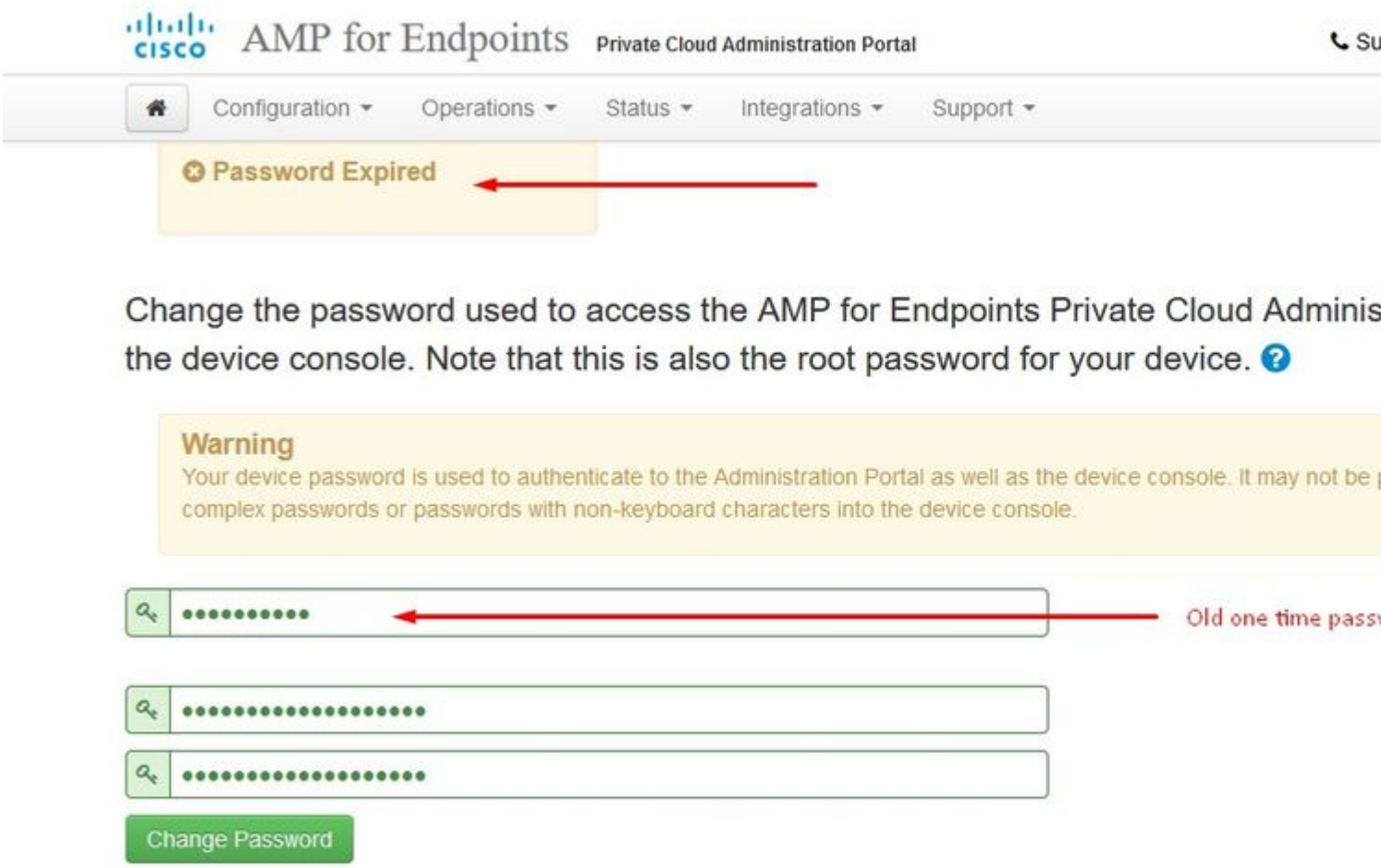


Phase 2:

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.

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.

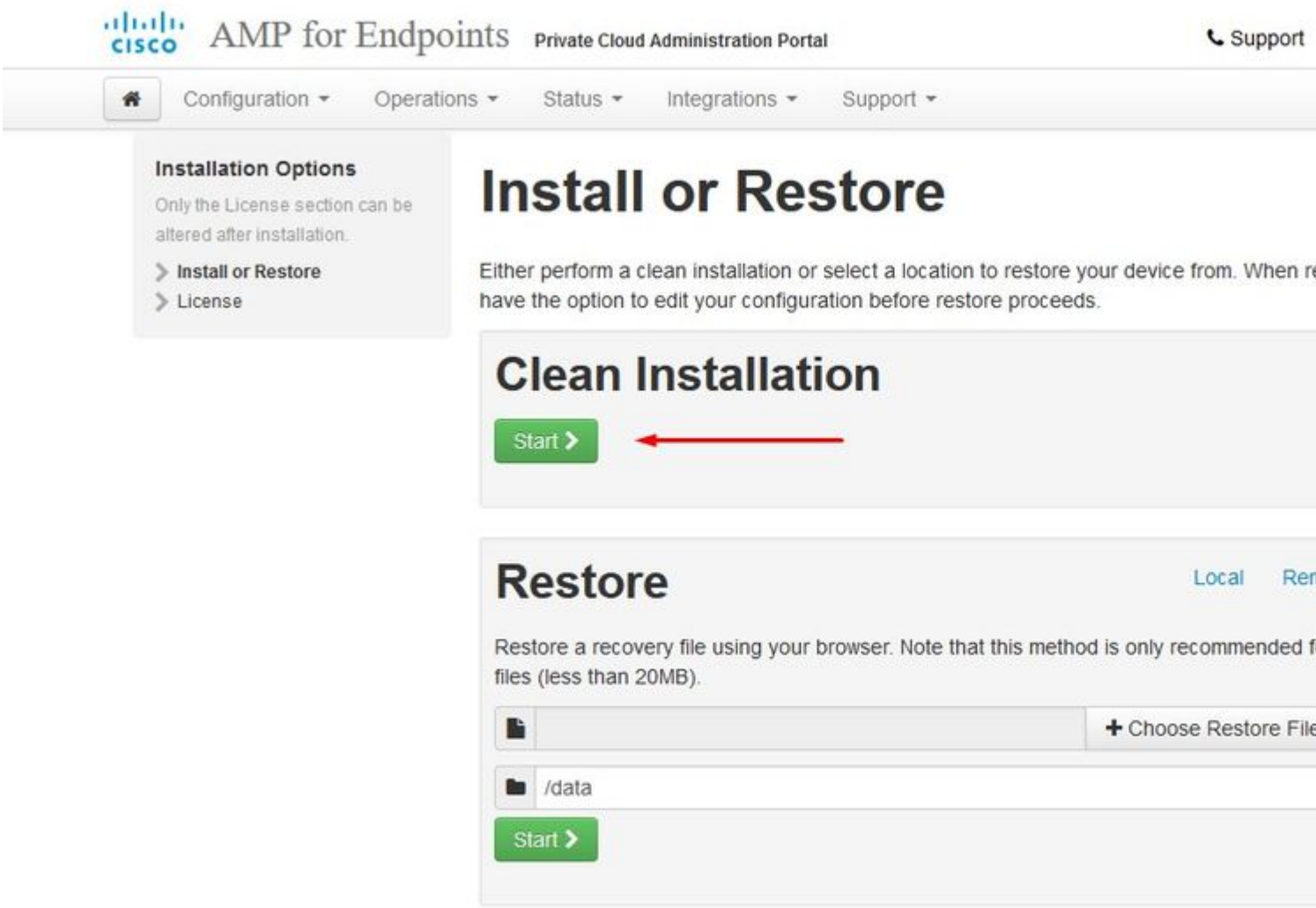


Schritt 4:

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

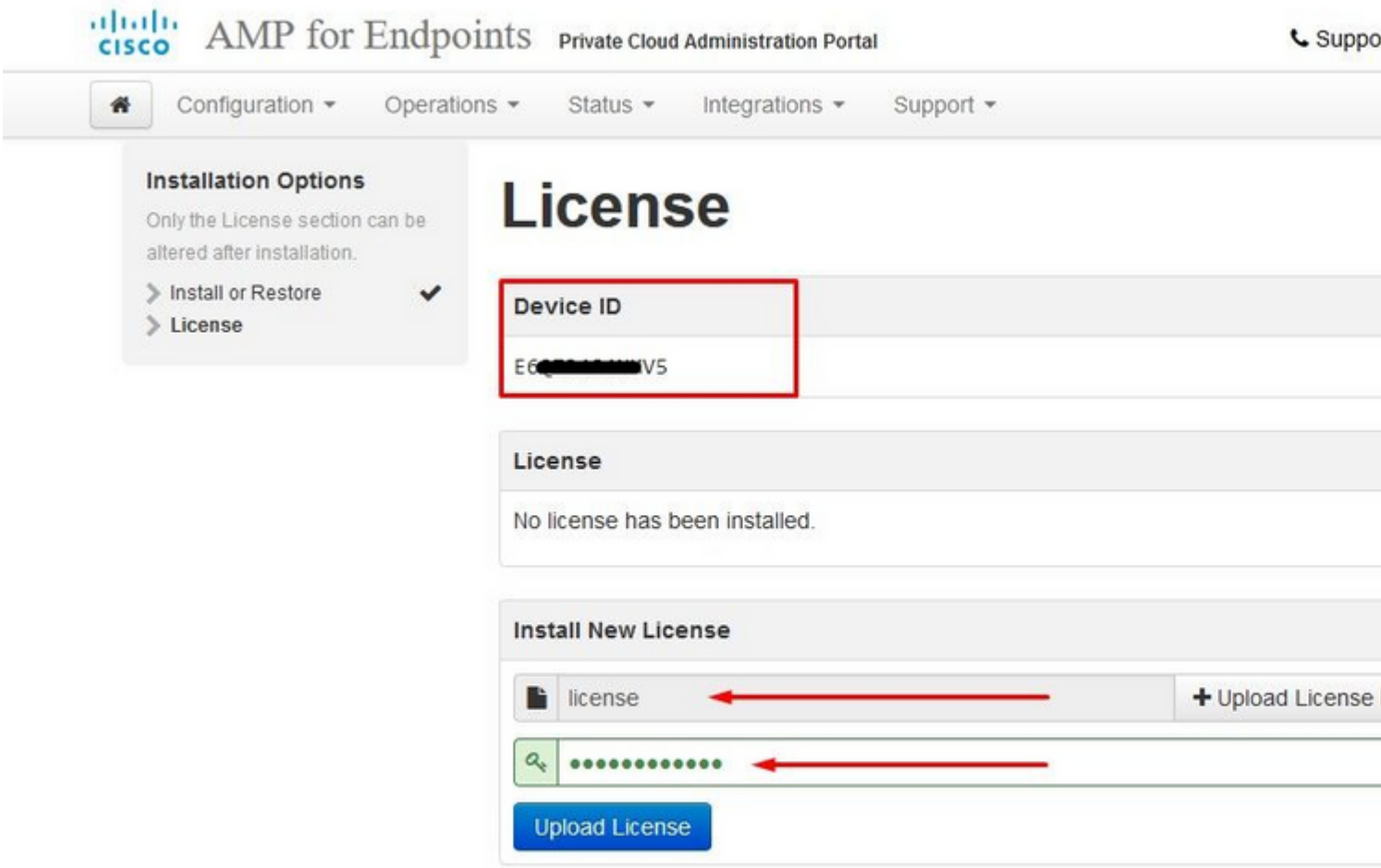
Schritt 5:

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.

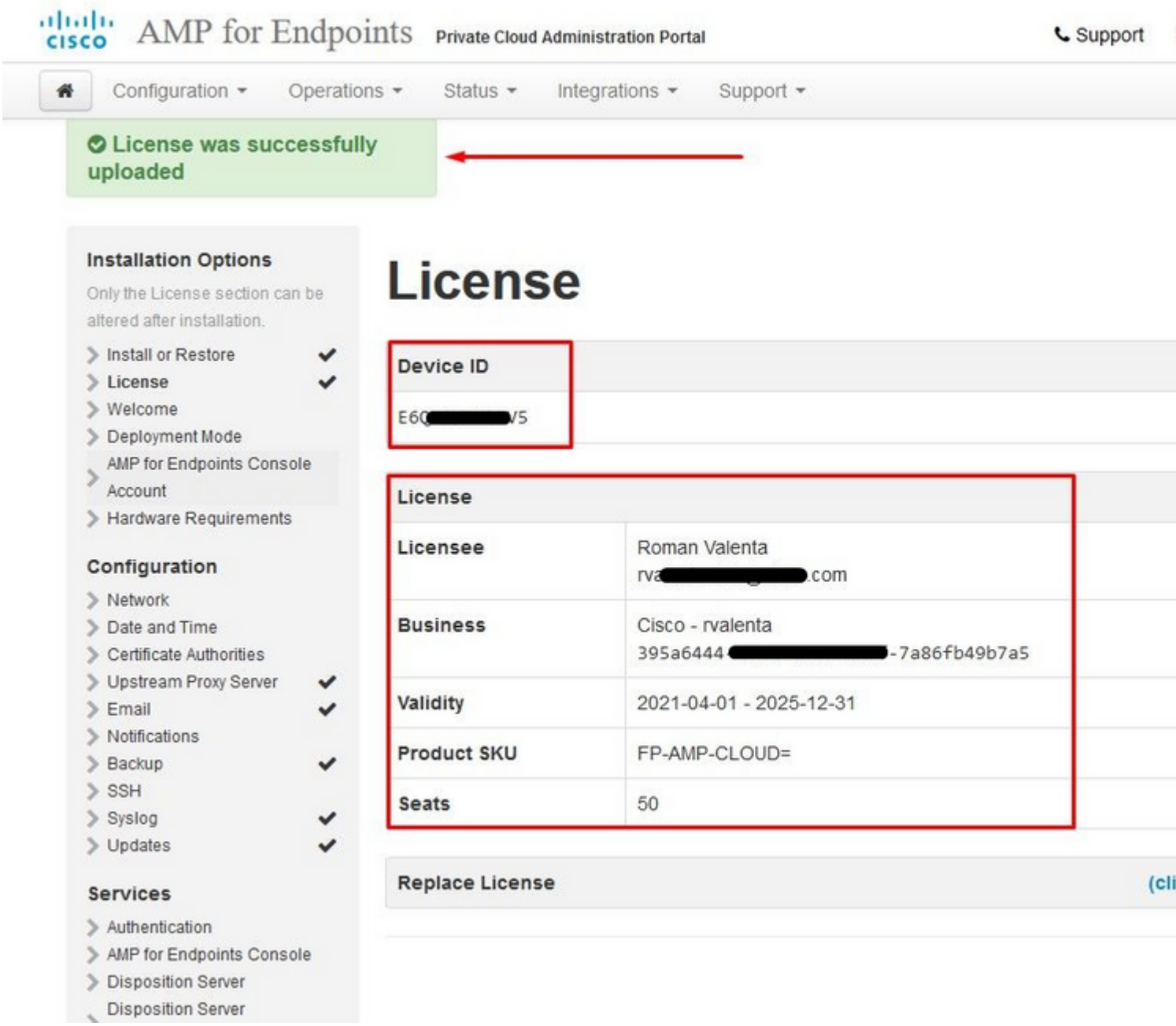


Schritt 6:

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.


AMP for Endpoints
Private Cloud Administration Portal
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€ƒ

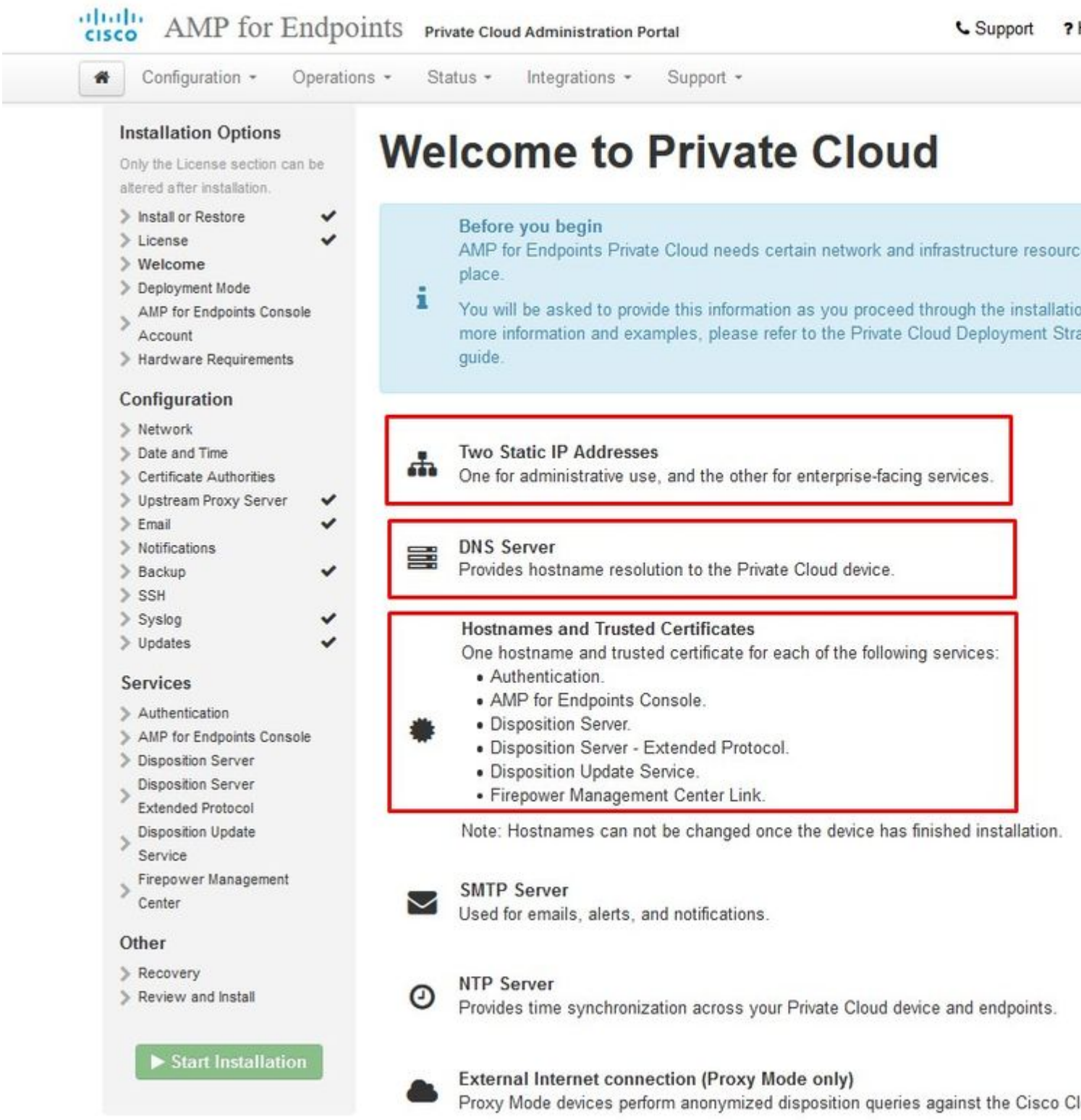


â€ƒ

â€ƒ

Schritt 7:

Sie erhalten die Willkommensseite, 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.



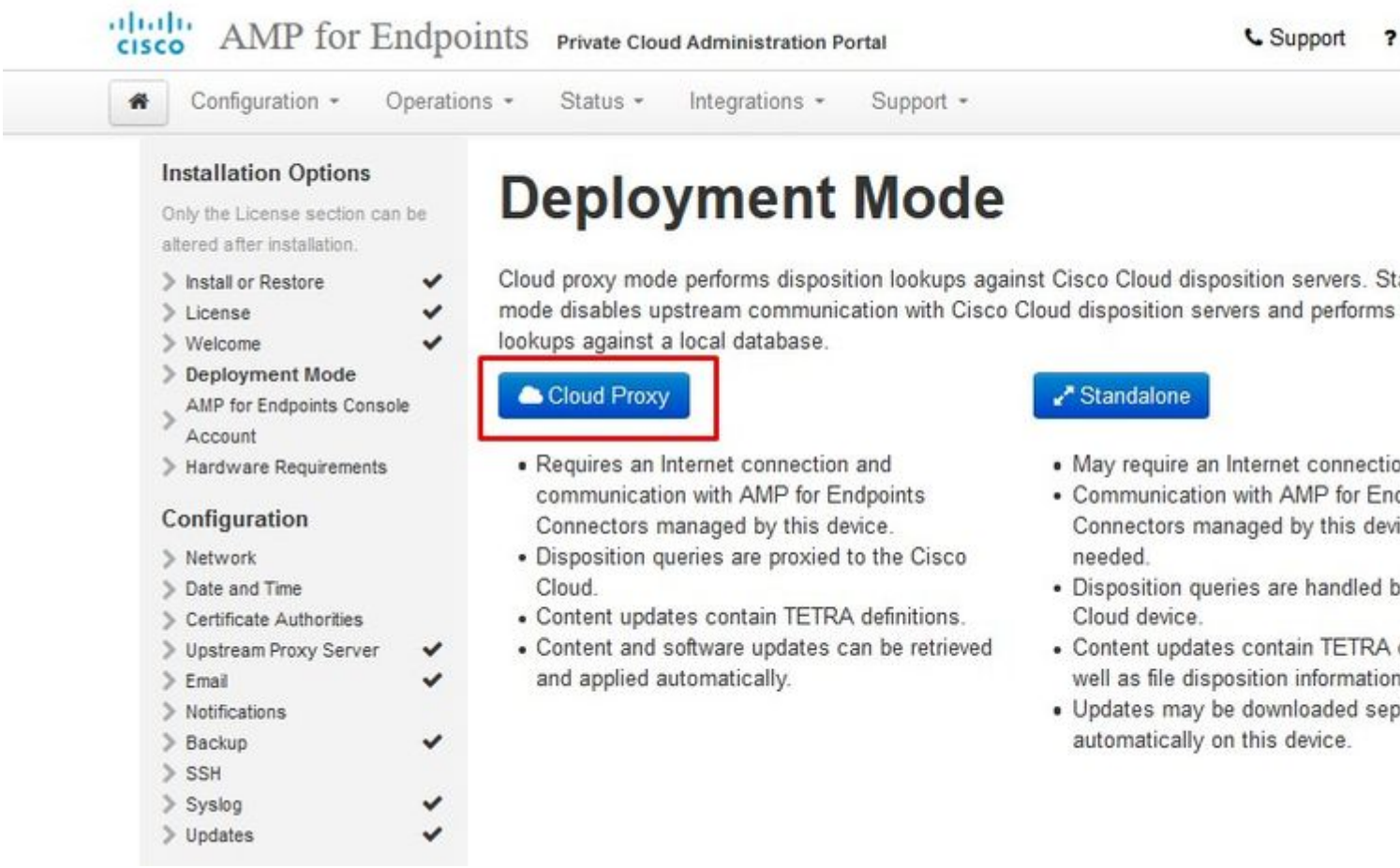
Konfiguration

Schritt 1:

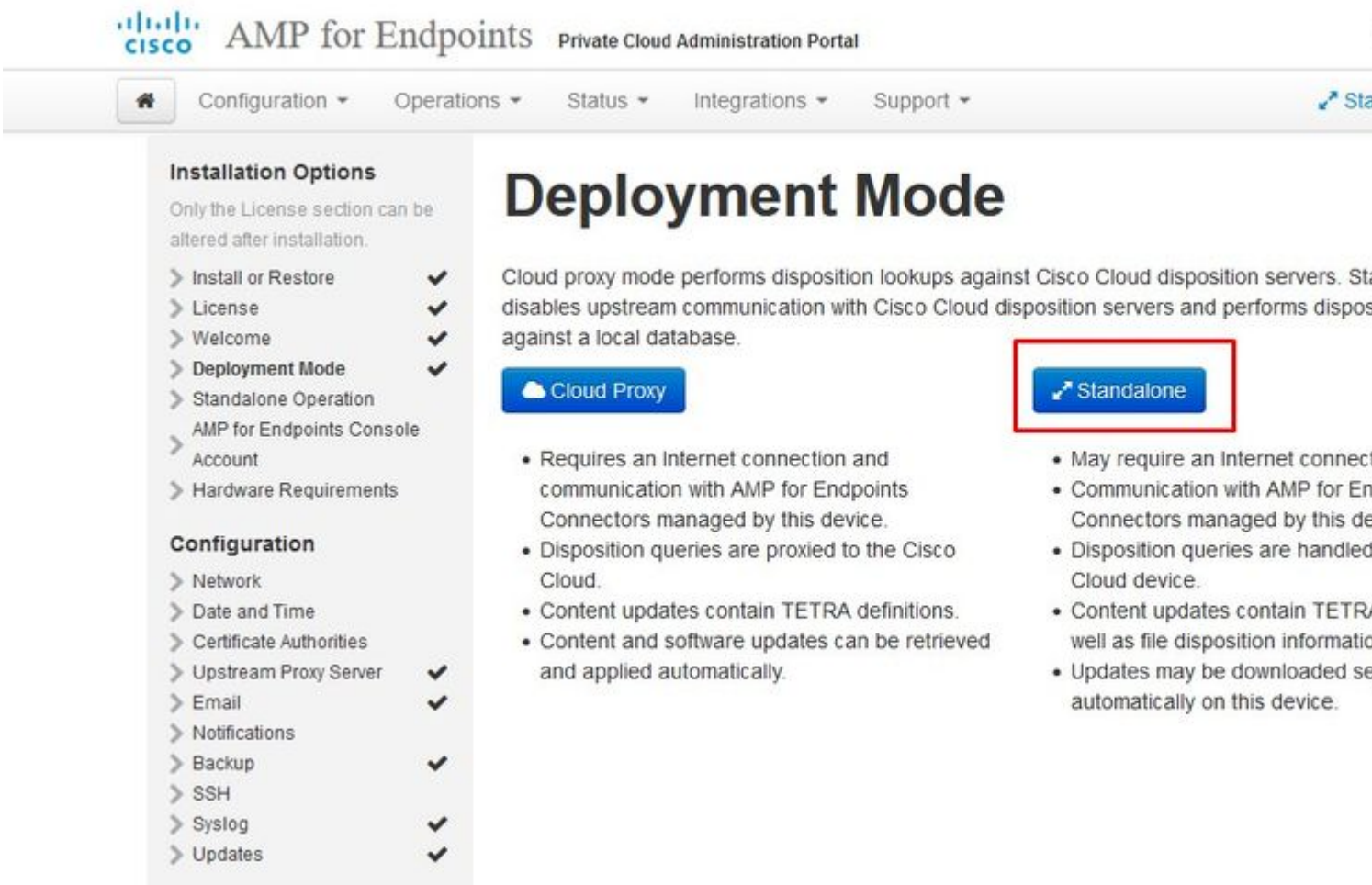
Hinweis: Bitte beachten Sie, dass in den nächsten Folien einige exklusive Folien enthalten sind, die nur im **AIR GAP**-Modus vorkommen. Diese Folien können **NUR** als **AIRGAP**-Modus

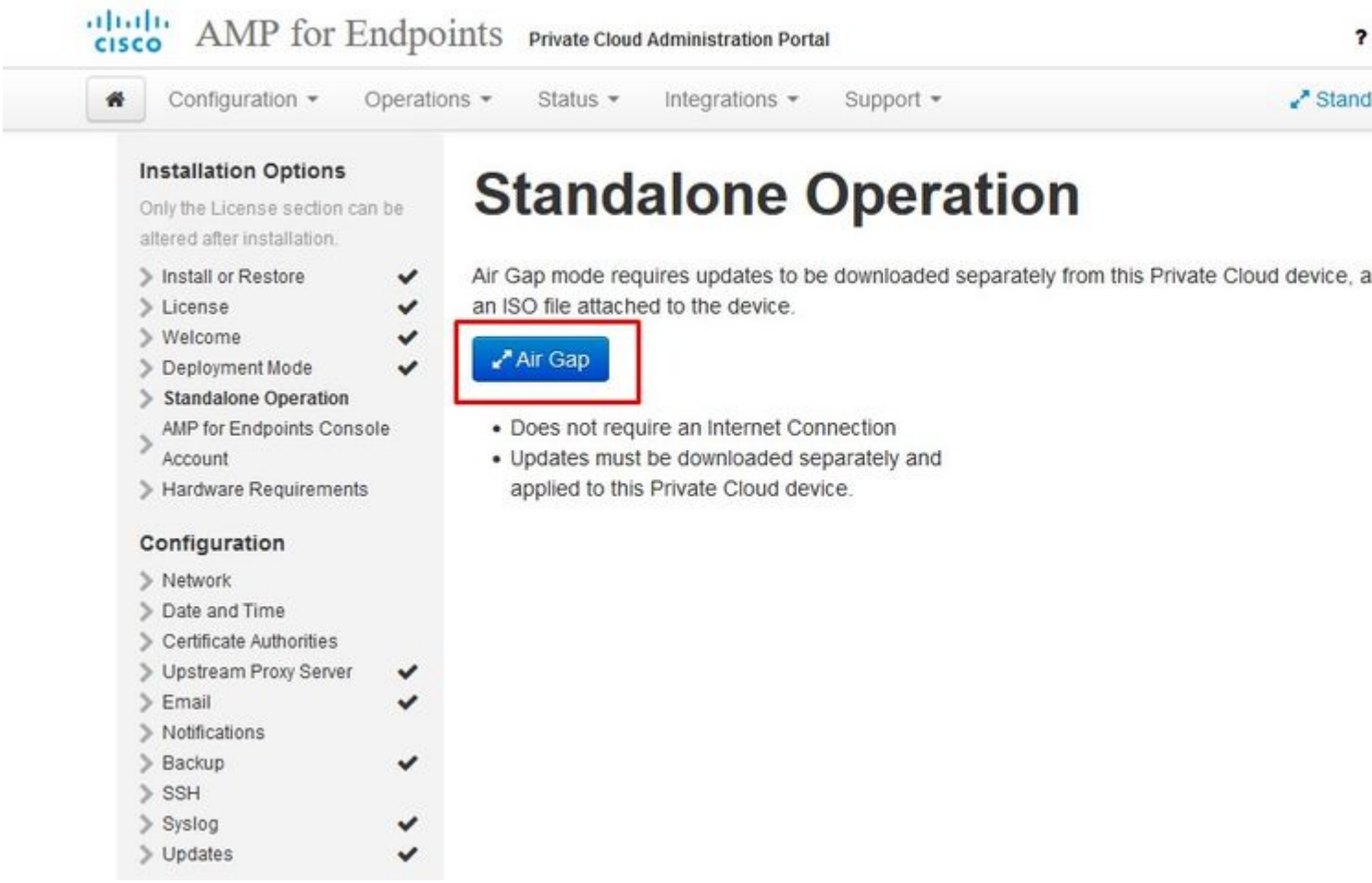
---

eingeschlossen und gekennzeichnet werden.



ï¿¾ ï¿¾ NUR LUFTSPALT ï¿¾ ï¿¾

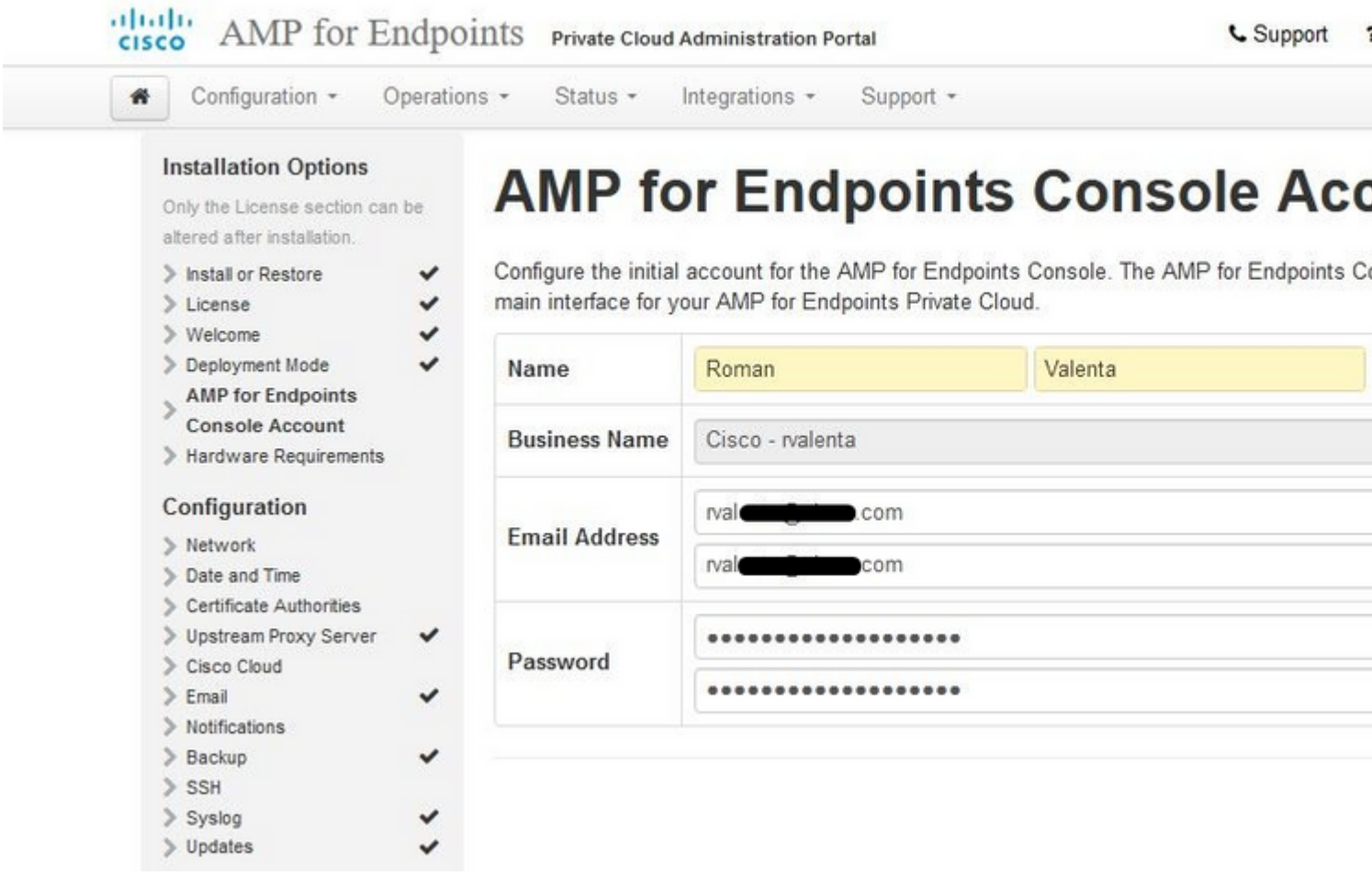

AMP for Endpoints
Private Cloud Administration Portal
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
Standalone Operation
AMP for Endpoints Console Account
Hardware 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. Sta
disables upstream communication with Cisco Cloud disposition servers and performs dispos
against a local database.
Cloud Proxy
Standalone
• 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.
• May require an Internet connect
• Communication with AMP for En Connectors managed by this de
• Disposition queries are handled Cloud device.
• Content updates contain TETRA well as file disposition informatio
• Updates may be downloaded se automatically on this device.



ï¸½ ï¸½ NUR ï¸½ ï¸½

Phase 2:

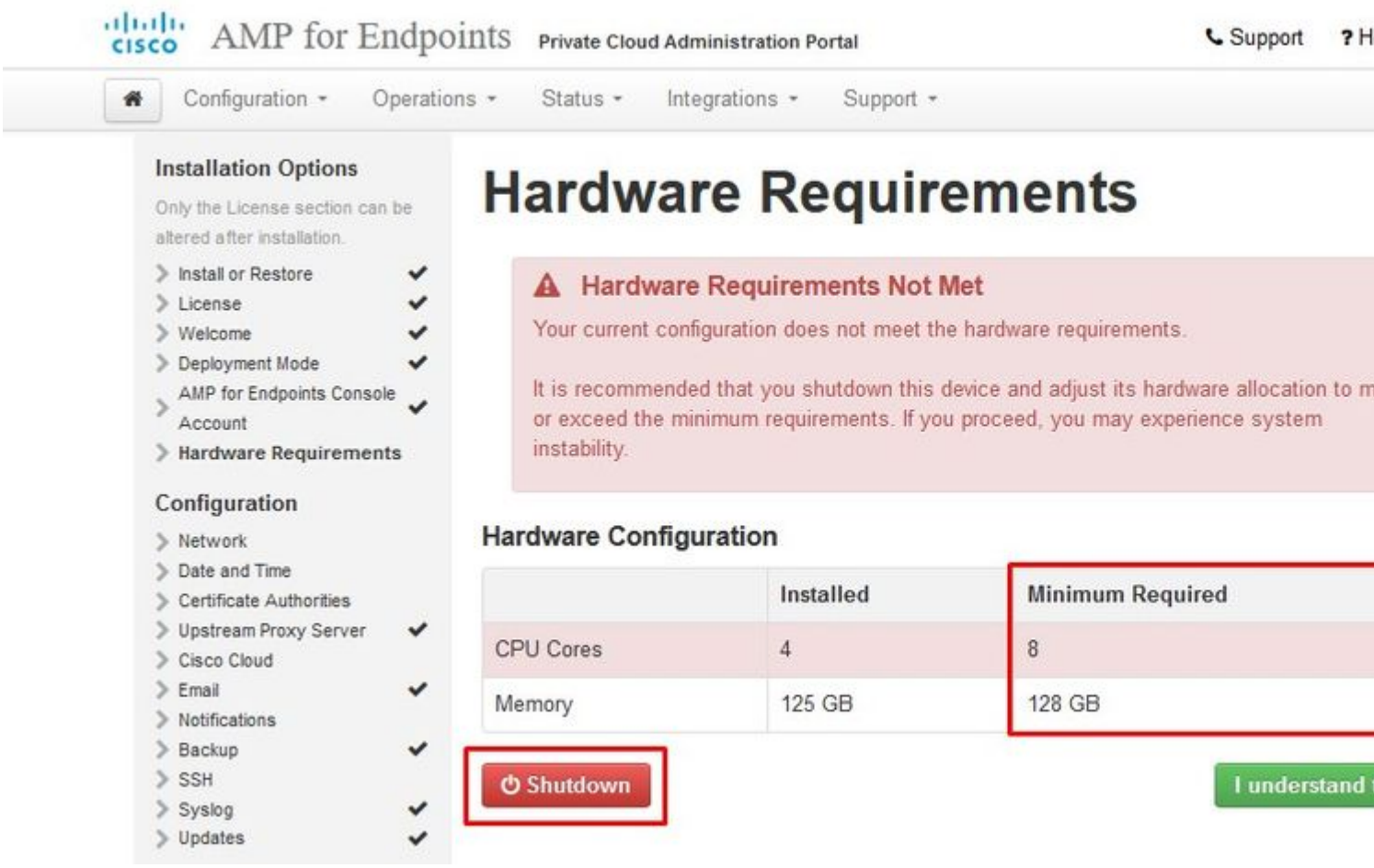
Navigieren Sie zur Seite für das Konto der sicheren Endpunktkonsole. Ein administrativer Benutzer wird für die Konsole verwendet, um Richtlinien und Computergruppen zu erstellen und zusätzliche Benutzer hinzuzufügen. Geben Sie den Namen, die E-Mail-Adresse und das Kennwort für das Konsolenkonto ein.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



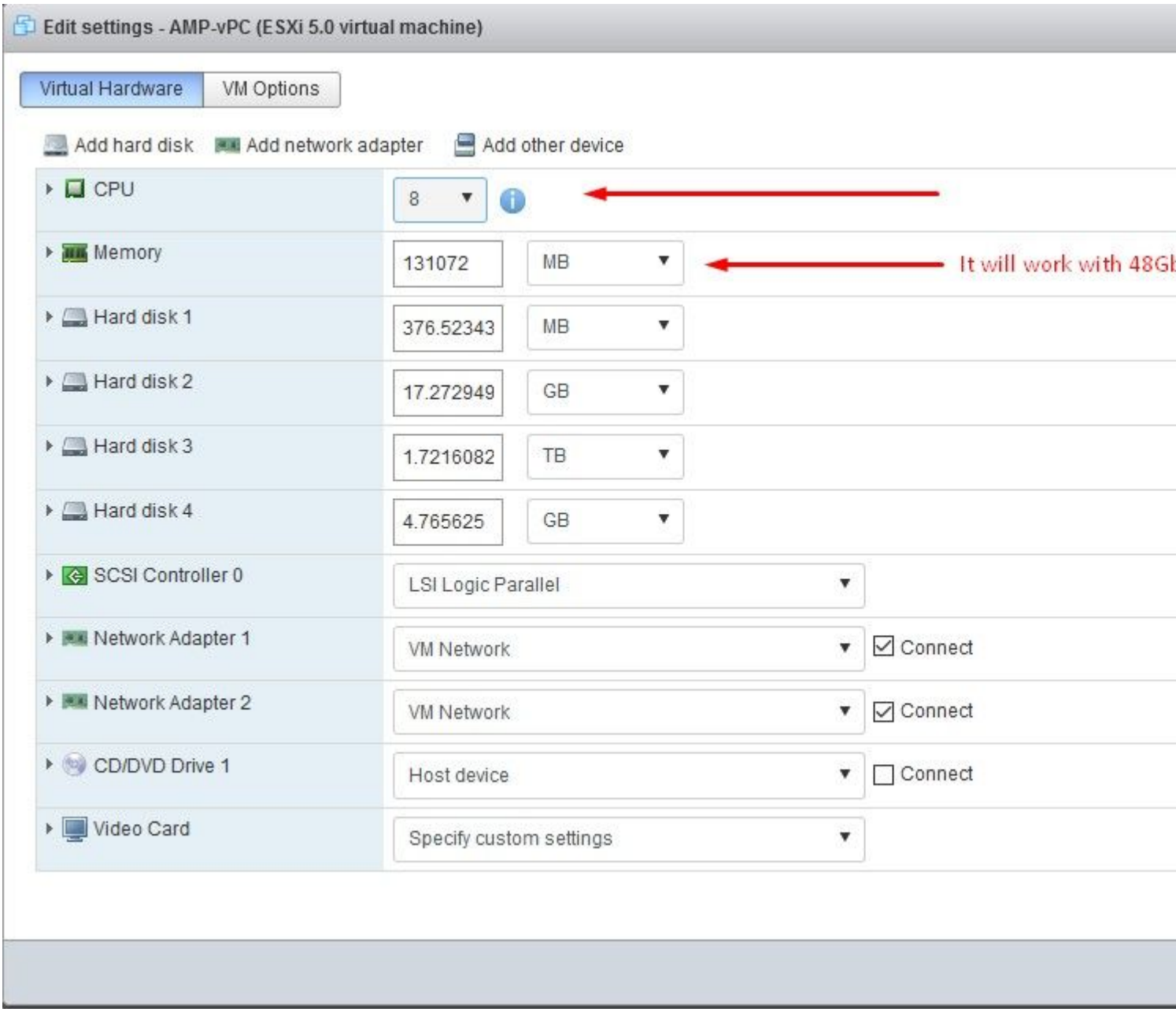
â€ƒ

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.

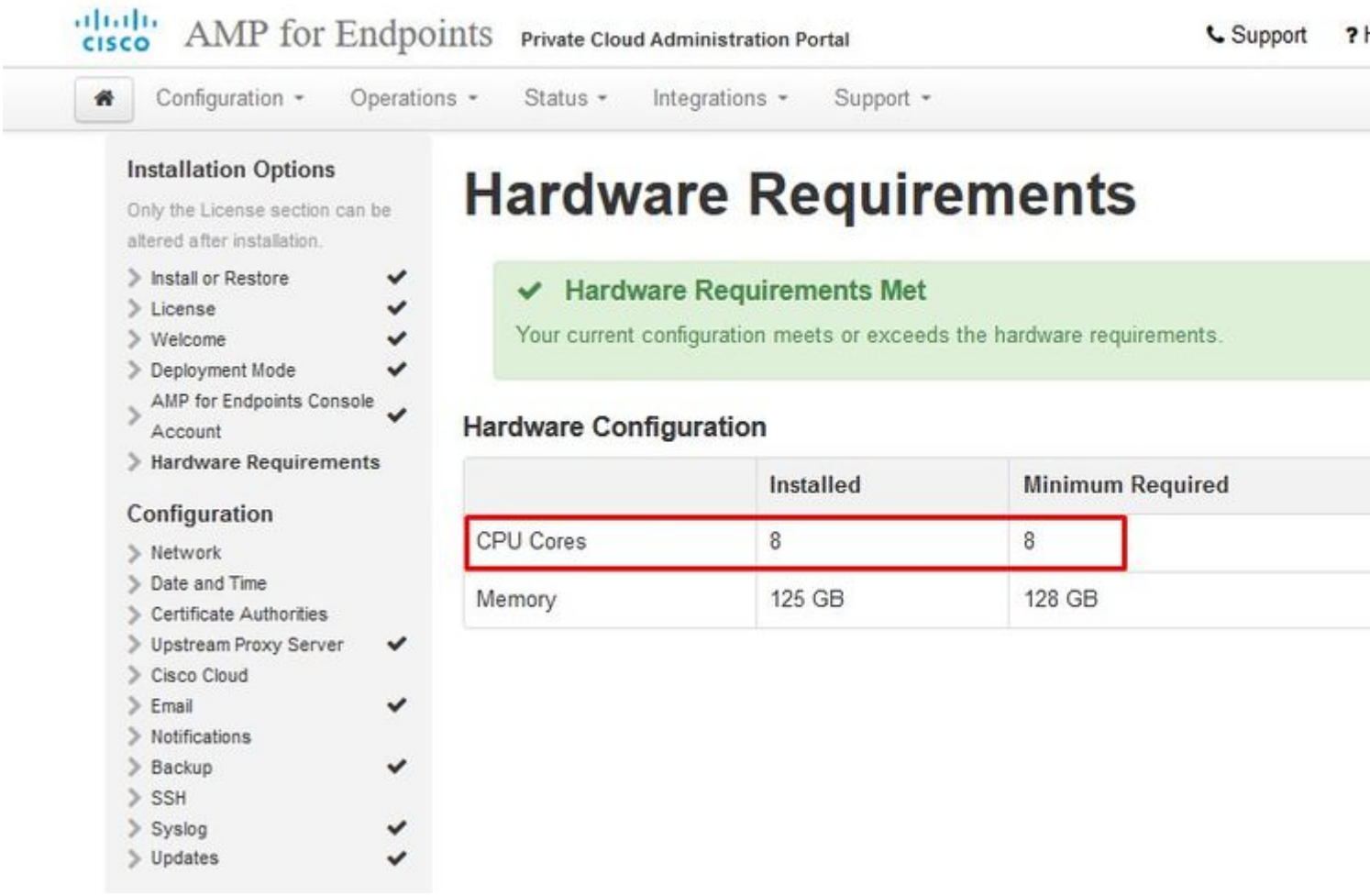
> **Hinweis**: Dies wurde in der OVA-Datei für Version 3.5.2 behoben, die mit 128 GB RAM und 8 CPU-Kernen richtig geladen wurde.



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



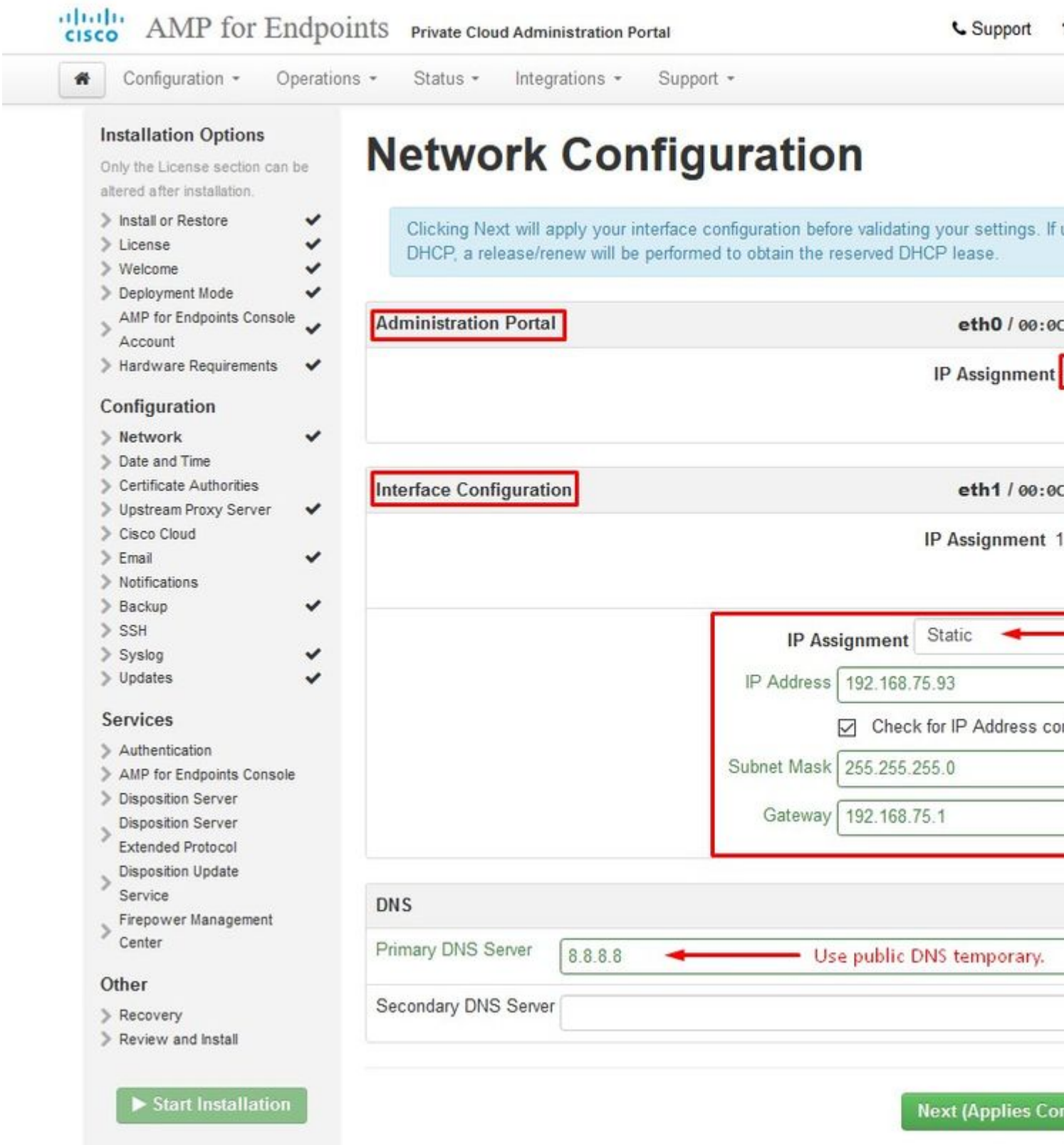
Nach dem Neustart fahren wir fort, wo wir links.



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

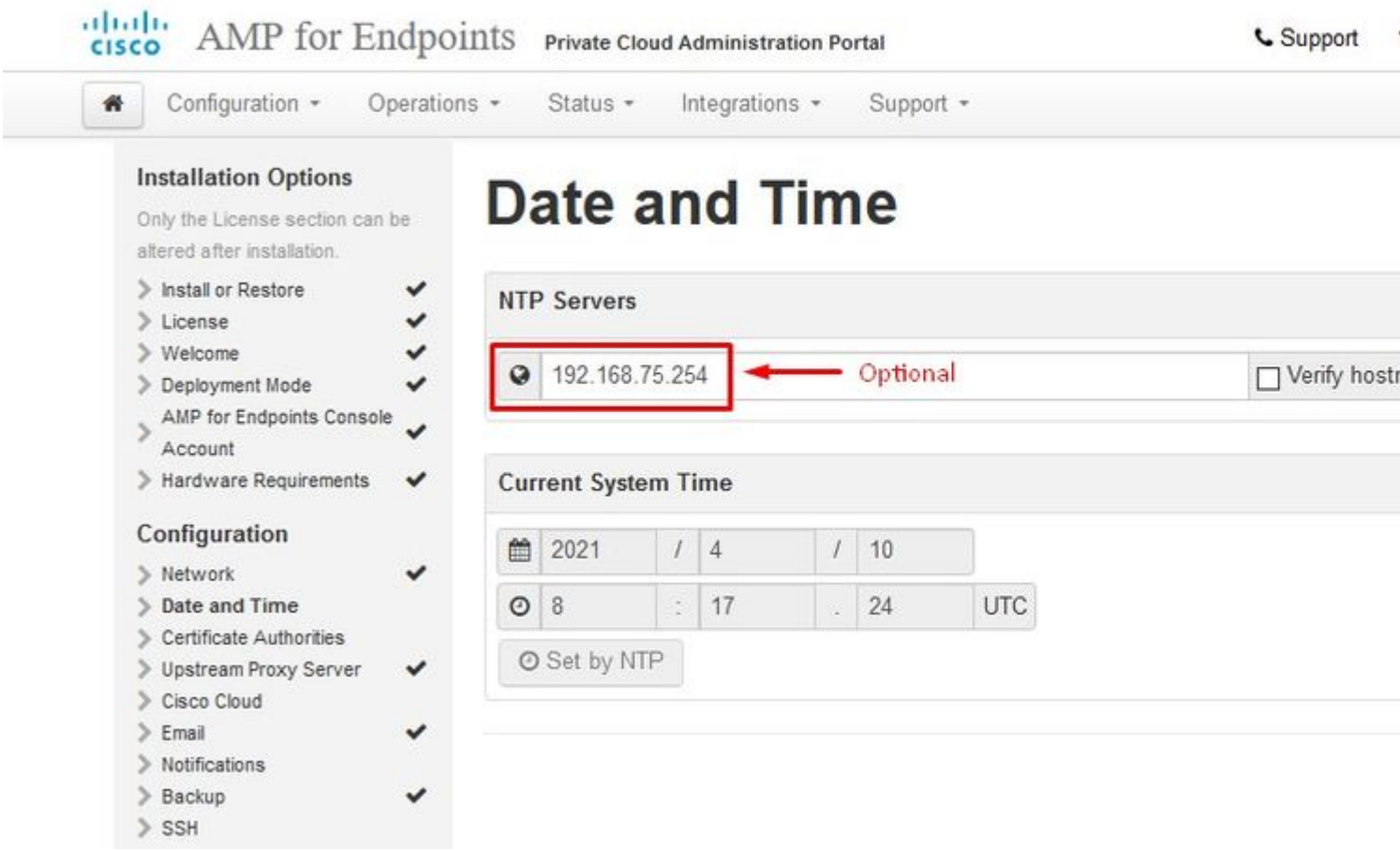
> **Hinweis**: Sie dürfen Ihr Gerät niemals für die Verwendung von DHCP konfigurieren, es sei denn, Sie haben MAC-Adressreservierungen für die Schnittstellen erstellt. Wenn sich die IP-Adressen Ihrer Schnittstellen ändern, kann dies zu ernsthaften Problemen mit den bereitgestellten sicheren Endgeräteanschlüssen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

Schritt 3:

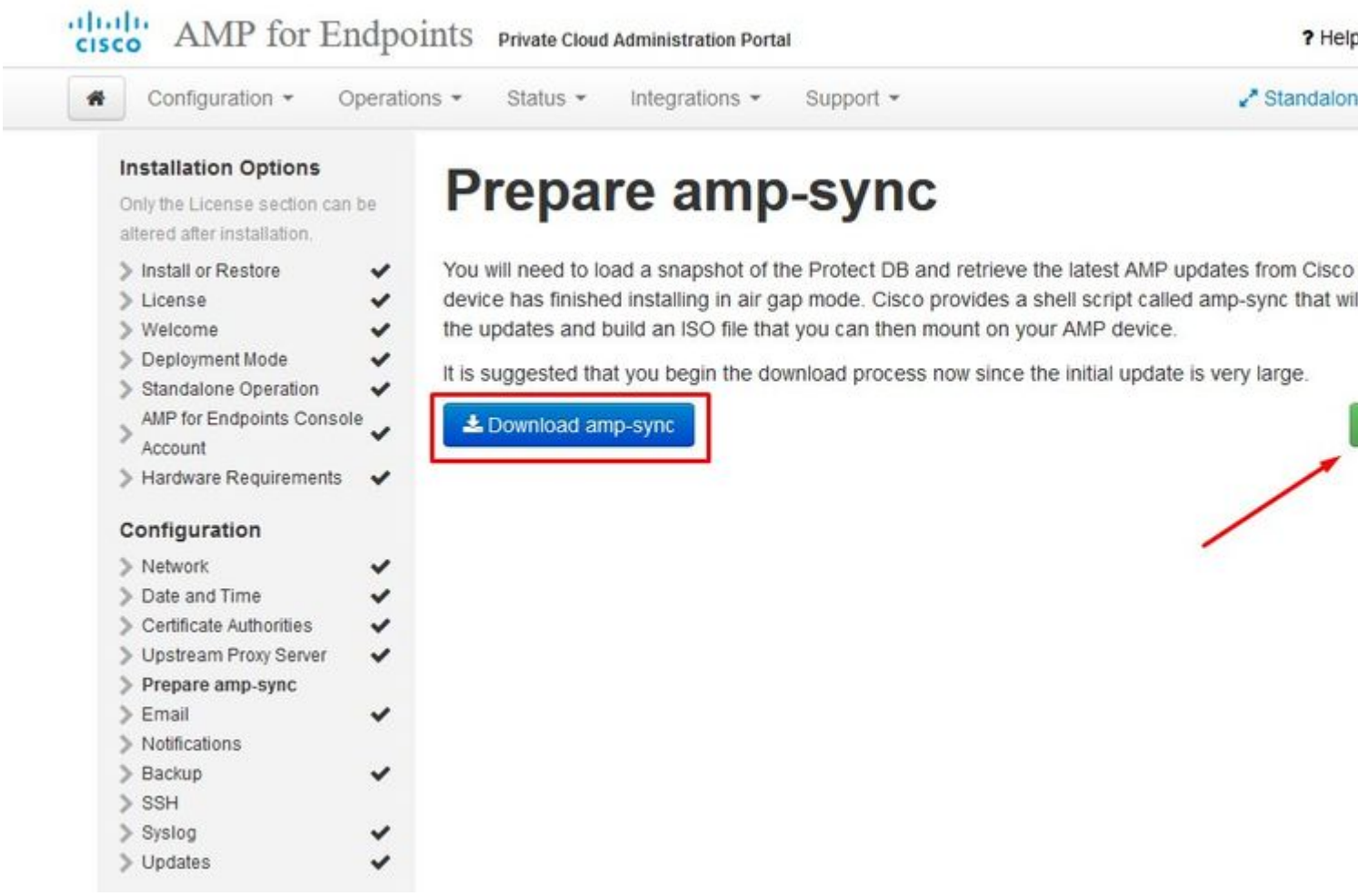


Schritt 4:

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.**



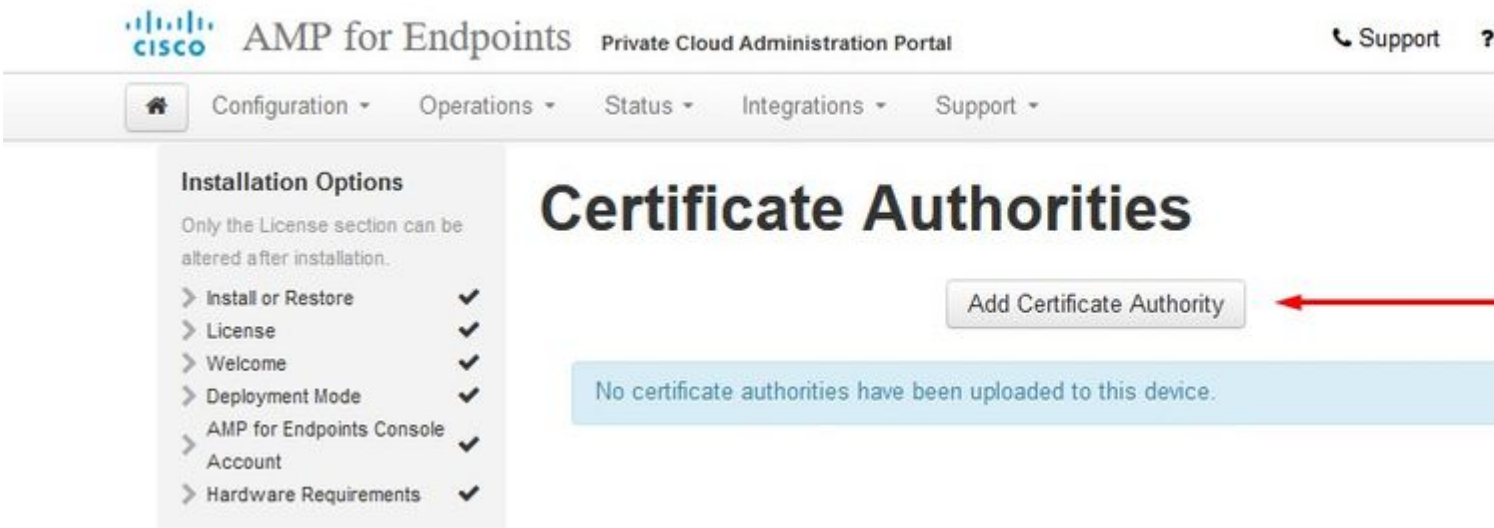
ï¸¾ ï¸¾ NUR LUFTSPALT ï¸¾ ï¸¾

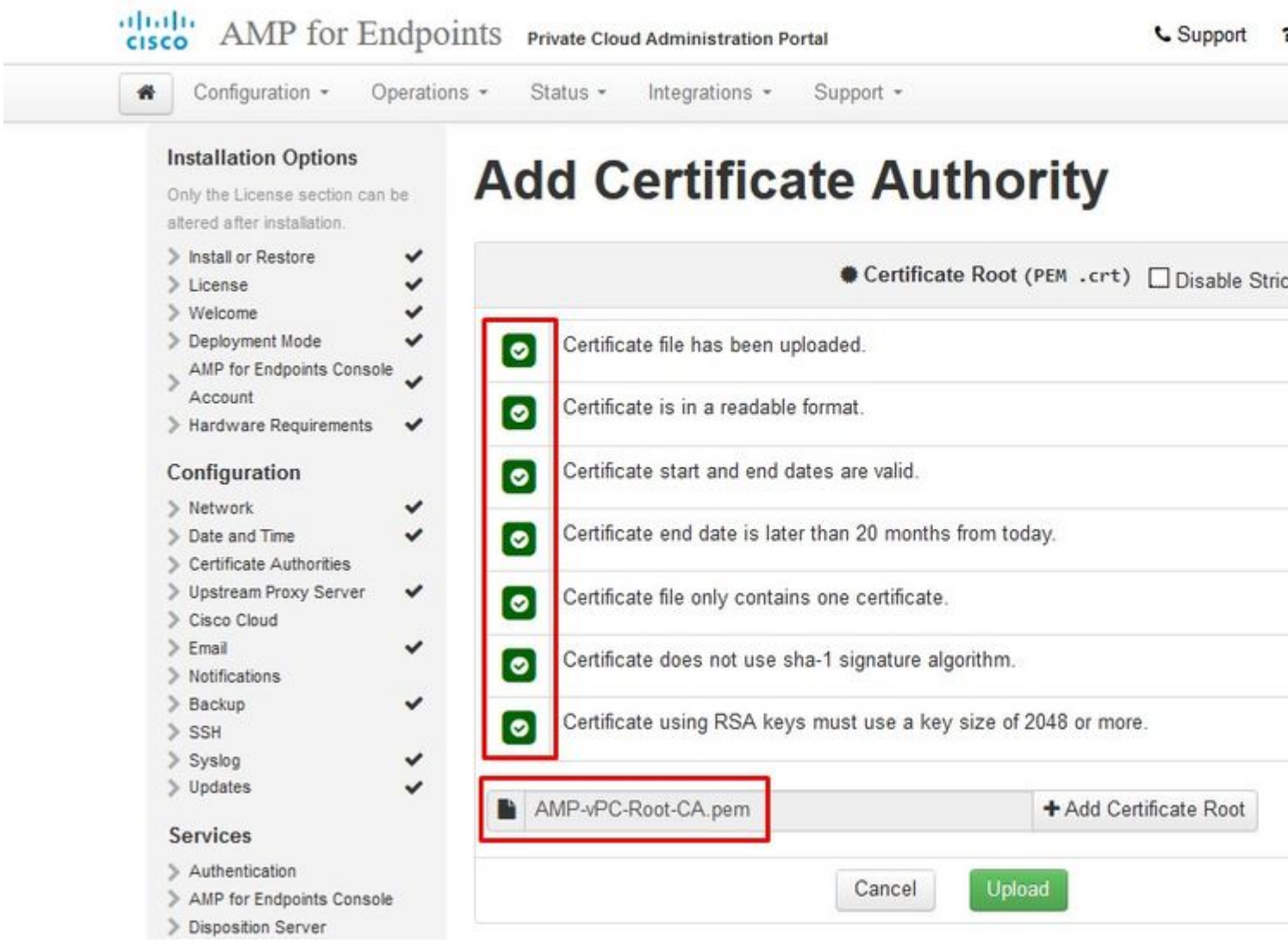


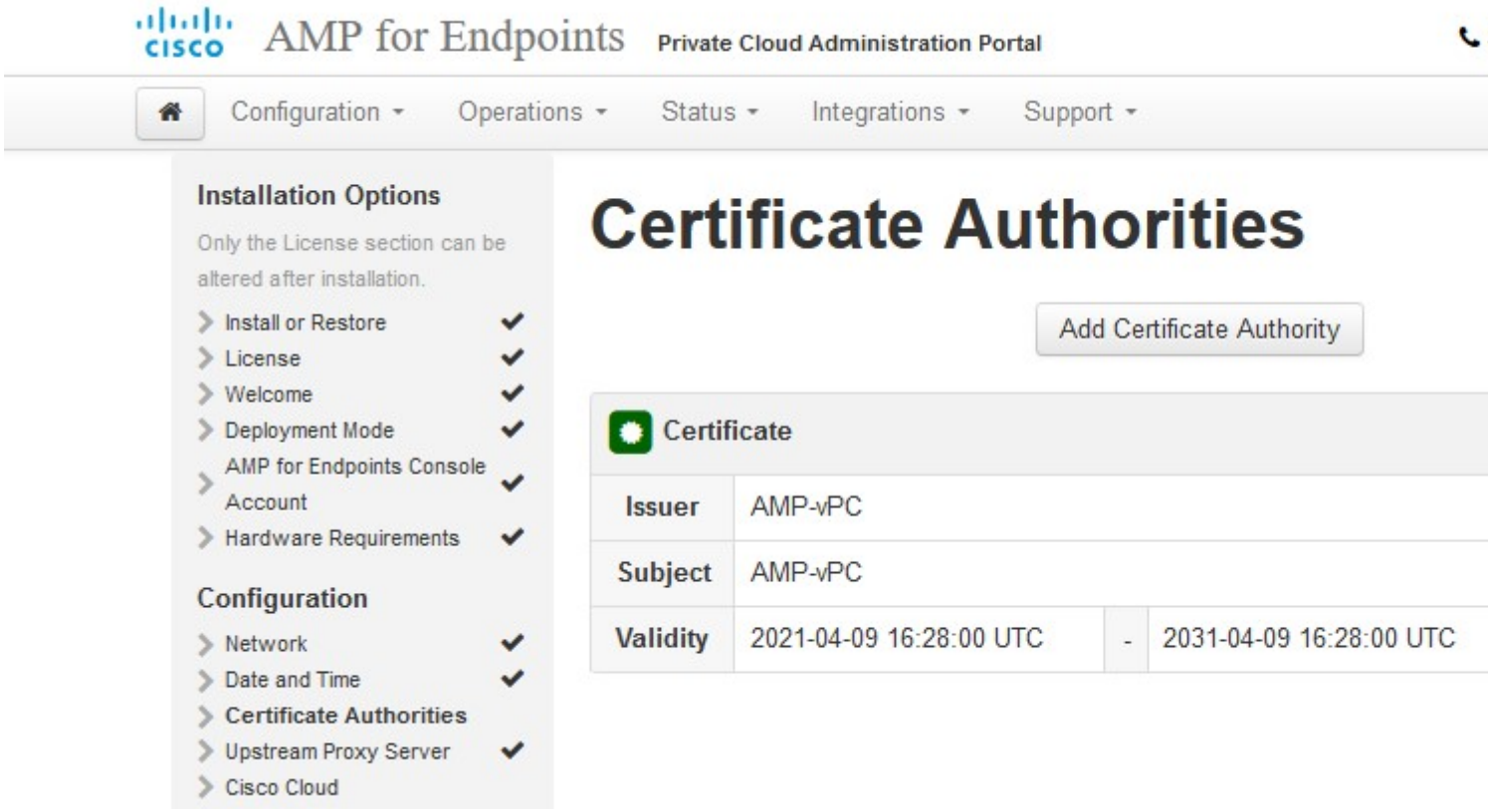
ï¸½ ï¸½ NUR ï¸½ ï¸½

Schritt 5:

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

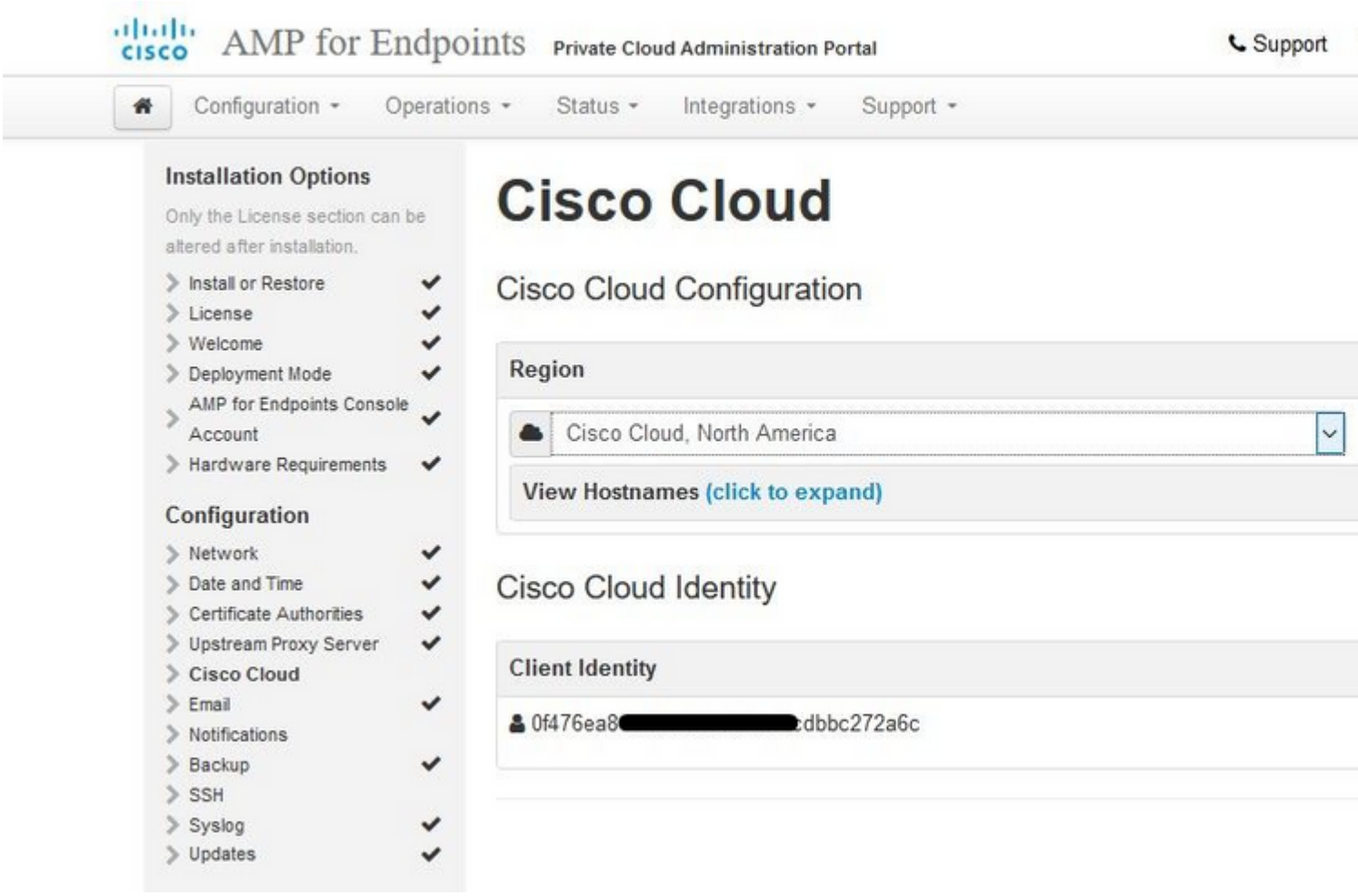



AMP for Endpoints
Private Cloud Administration Portal
Support
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware Requirements
Configuration
Network
Date and Time
Certificate Authorities
Upstream Proxy Server
Cisco Cloud
Email
Notifications
Backup
SSH
Syslog
Updates
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
Add Certificate Root
Cancel
Upload


AMP for Endpoints
Private Cloud Administration Portal
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
Certificate Authorities
Add Certificate Authority
Certificate
Issuer
AMP-vPC
Subject
AMP-vPC
Validity
2021-04-09 16:28:00 UTC
-
2031-04-09 16:28:00 UTC

Schritt 6:

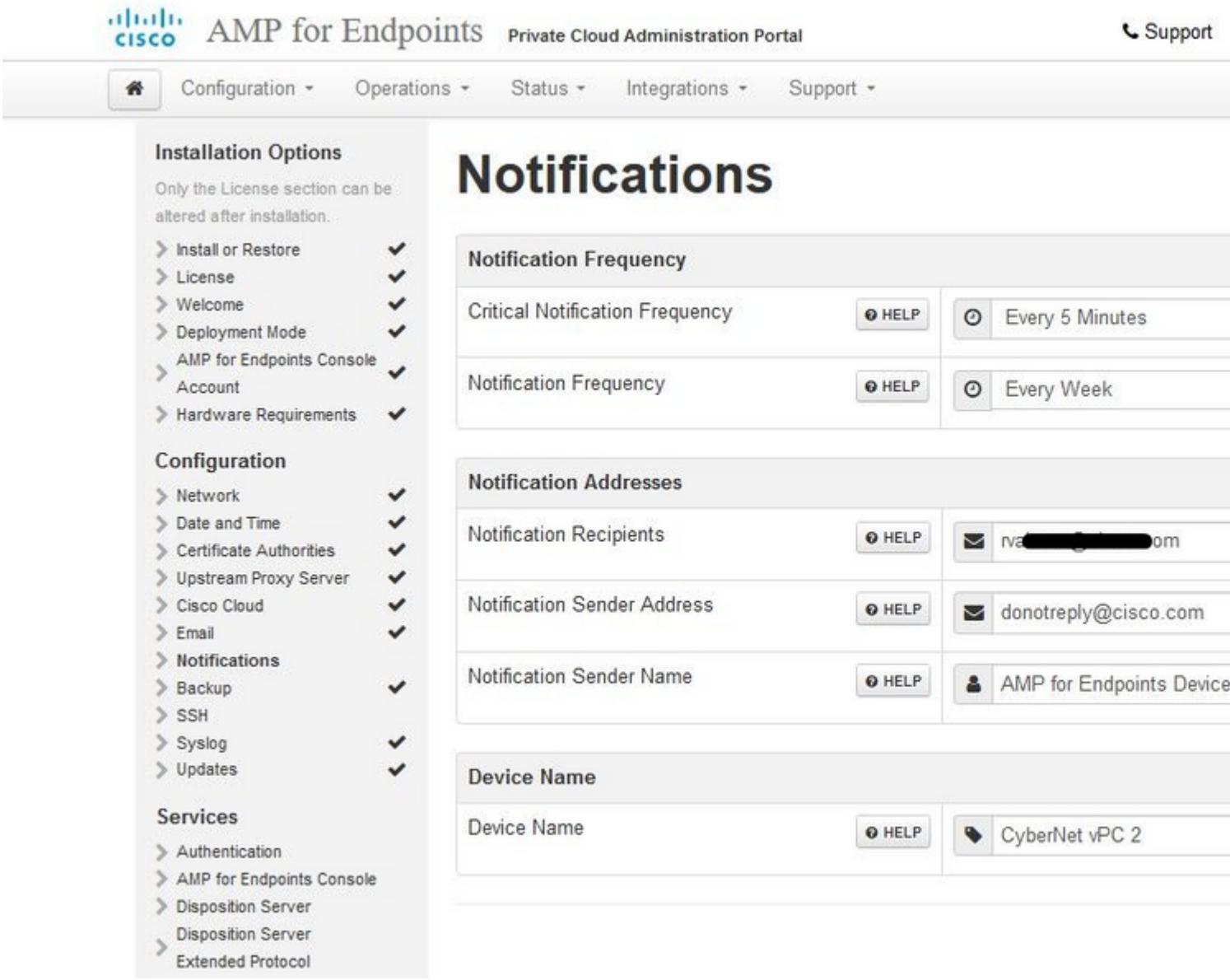
Der nächste Schritt ist die Konfiguration der Cisco Cloud-Seite, wie im Bild gezeigt. Wählen Sie die entsprechende Cisco Cloud-**Region aus**. Erweitern Sie **Ansicht Hostnamen,** wenn Sie Firewall-Ausnahmen für das Secure Endpoint Private Cloud-Gerät erstellen müssen, um mit der Cisco Cloud für Dateisuchen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



â€ƒ

Schritt 7:

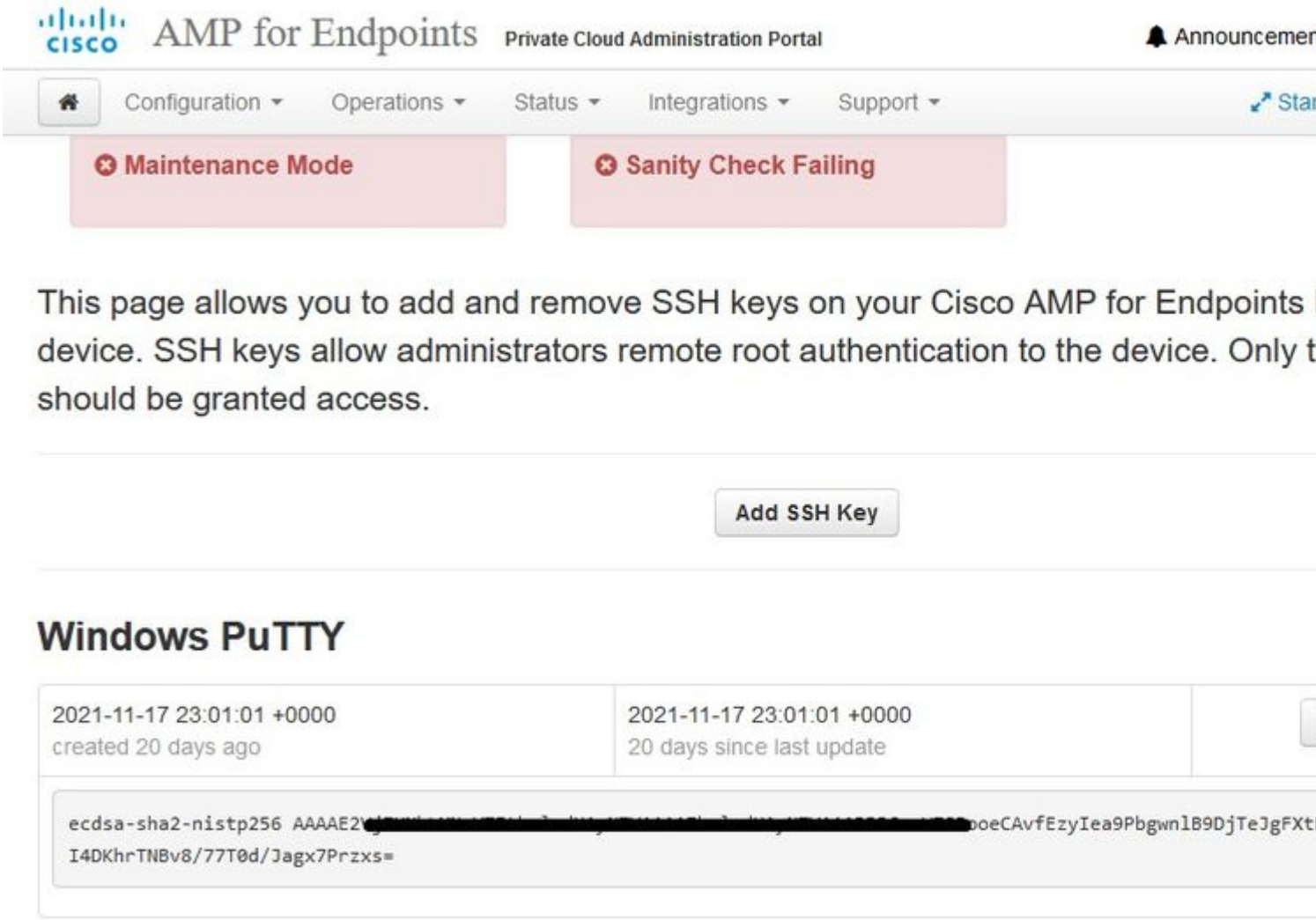
Navigieren Sie zur Seite "Benachrichtigungen", wie im Bild dargestellt. Wählen Sie die Häufigkeit für kritische und regelmäßige Benachrichtigungen aus. Geben Sie die E-Mail-Adressen ein, die Warnmeldungen für das sichere Endgerät empfangen sollen. Sie können E-Mail-Aliase verwenden oder mehrere Adressen durch eine kommagetrennte 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.**



â€ƒ

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**.



â€ƒ

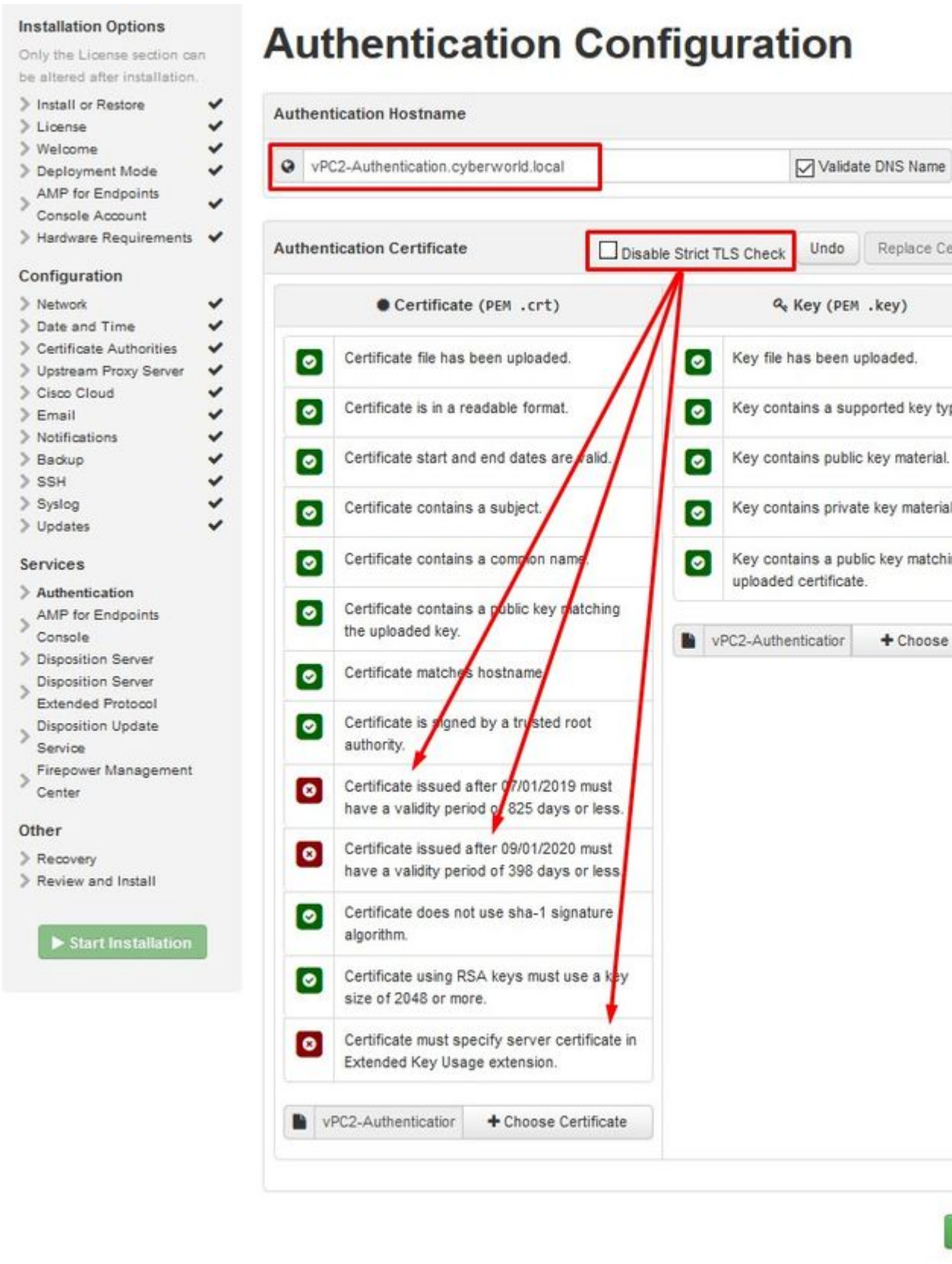
Als Nächstes sehen Sie den Abschnitt "Services". Auf den nächsten Seiten müssen Sie Hostnamen zuweisen und die entsprechenden Zertifikat- und Schlüsselpaare für diese Gerätedienste hochladen. Auf den nächsten Folien sehen Sie die Konfiguration eines der 6 Zertifikate.

Services

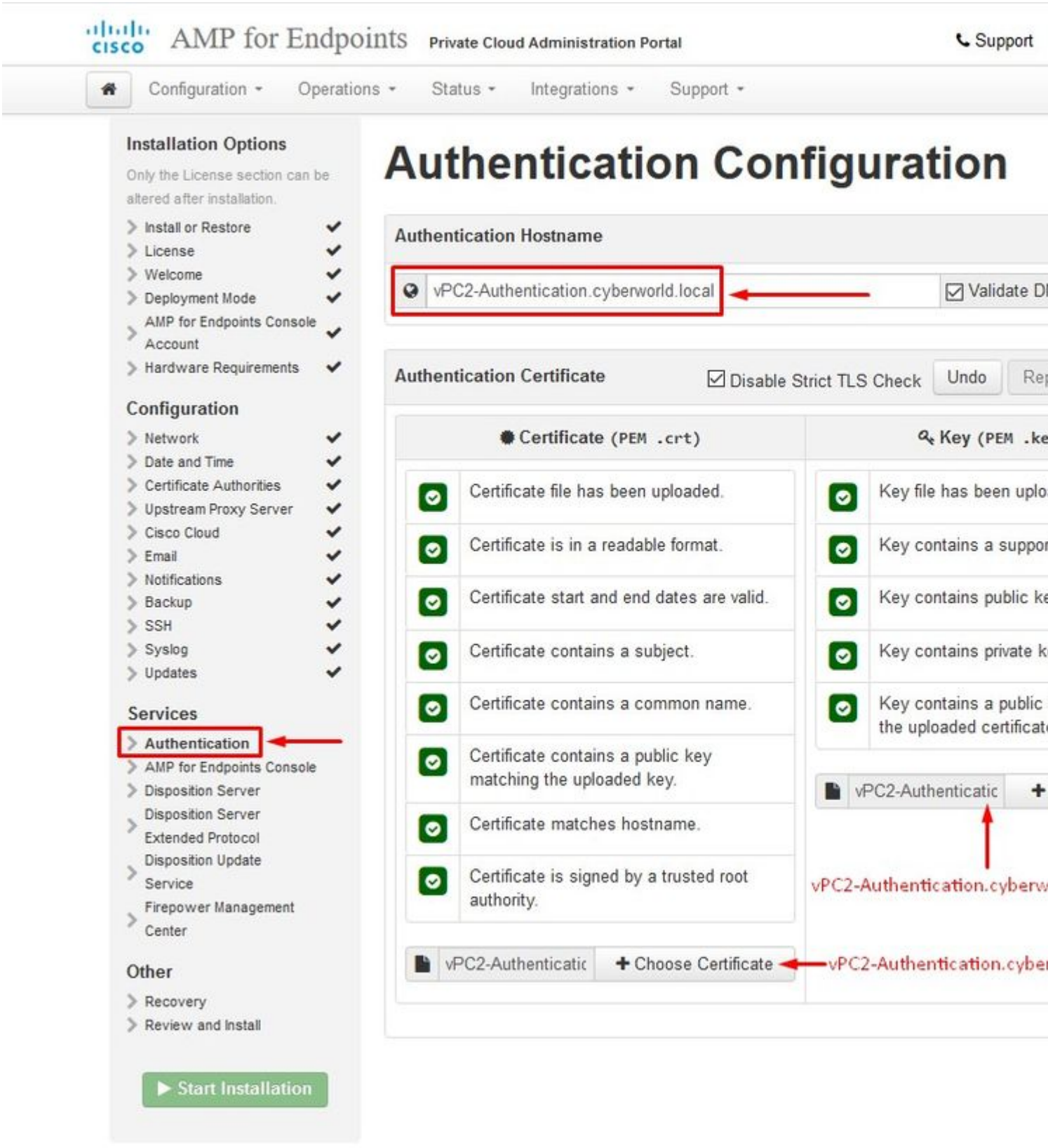
Schritt 1:

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**"



Ohne strenge TLS-Prüfung

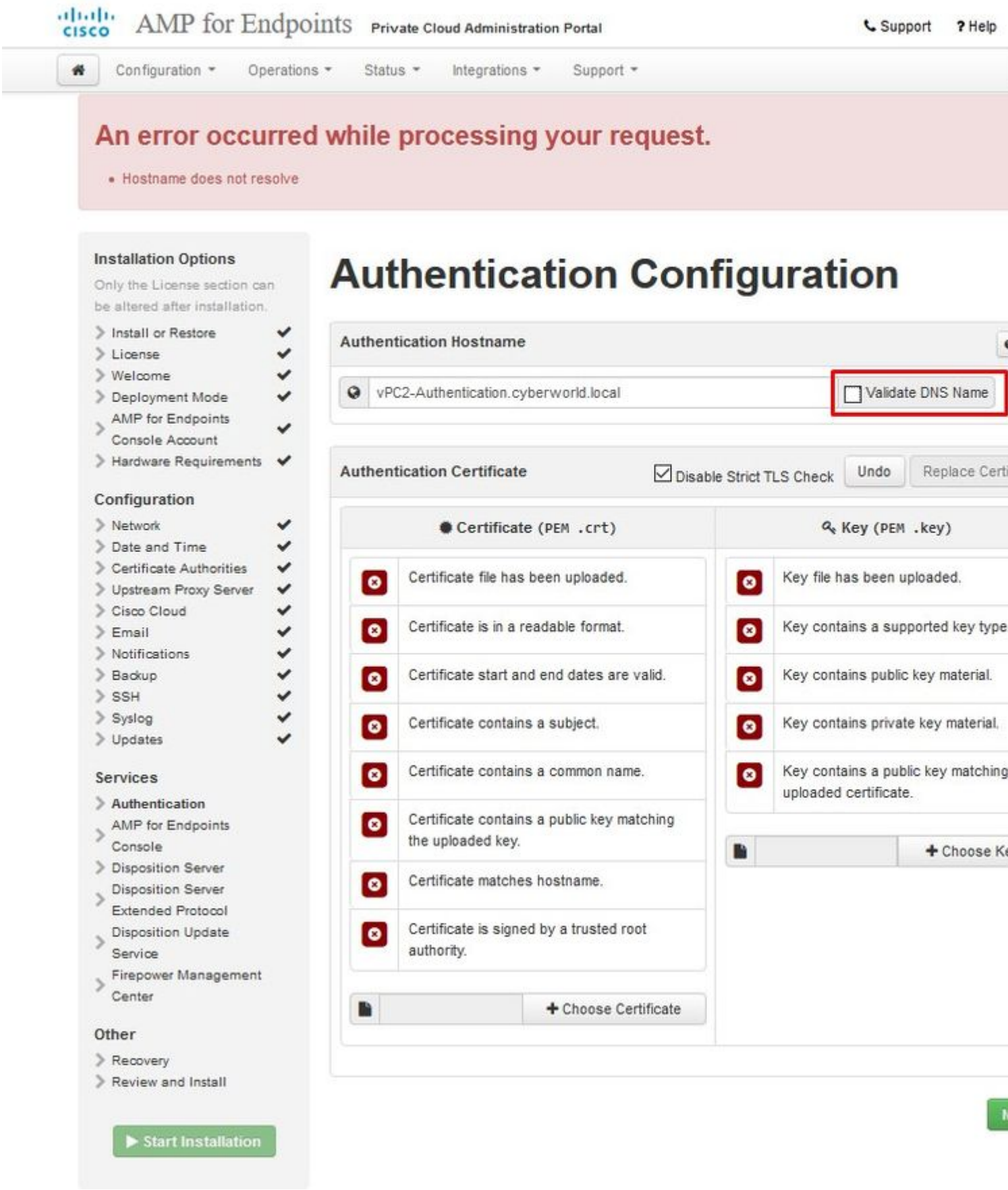


Phase 2:

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.



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.

Dispositionsaktualisierungsdienst

- 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.

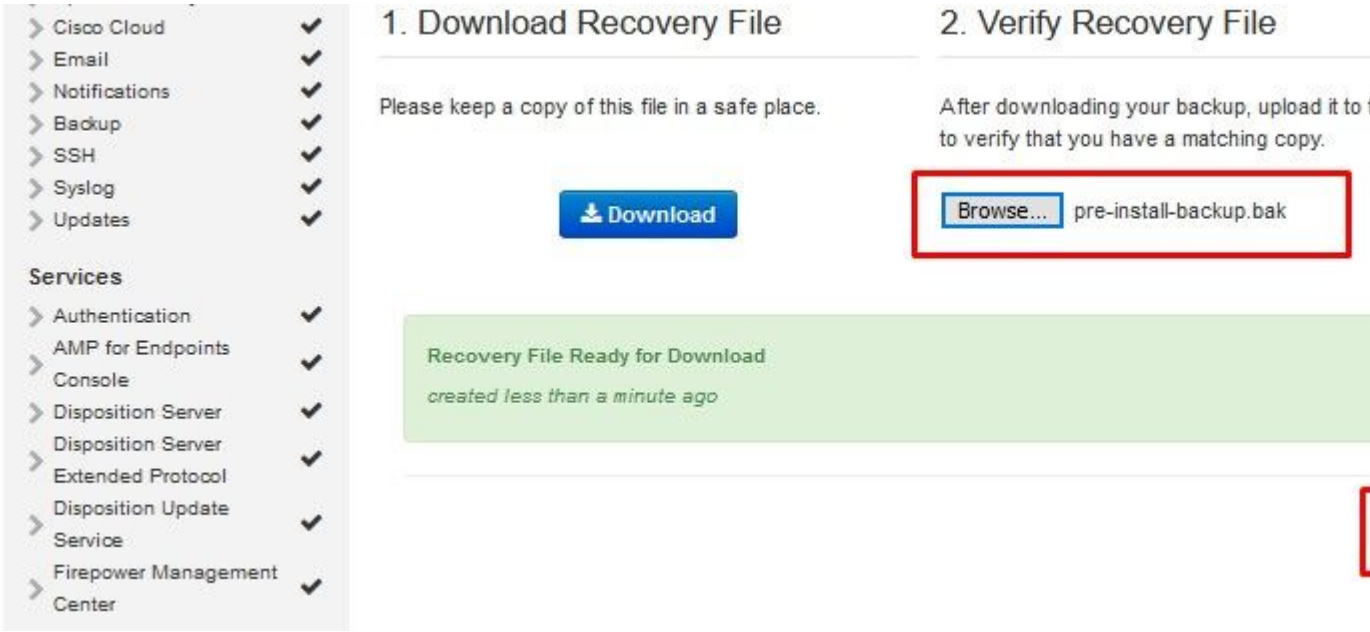
Schritt 3:

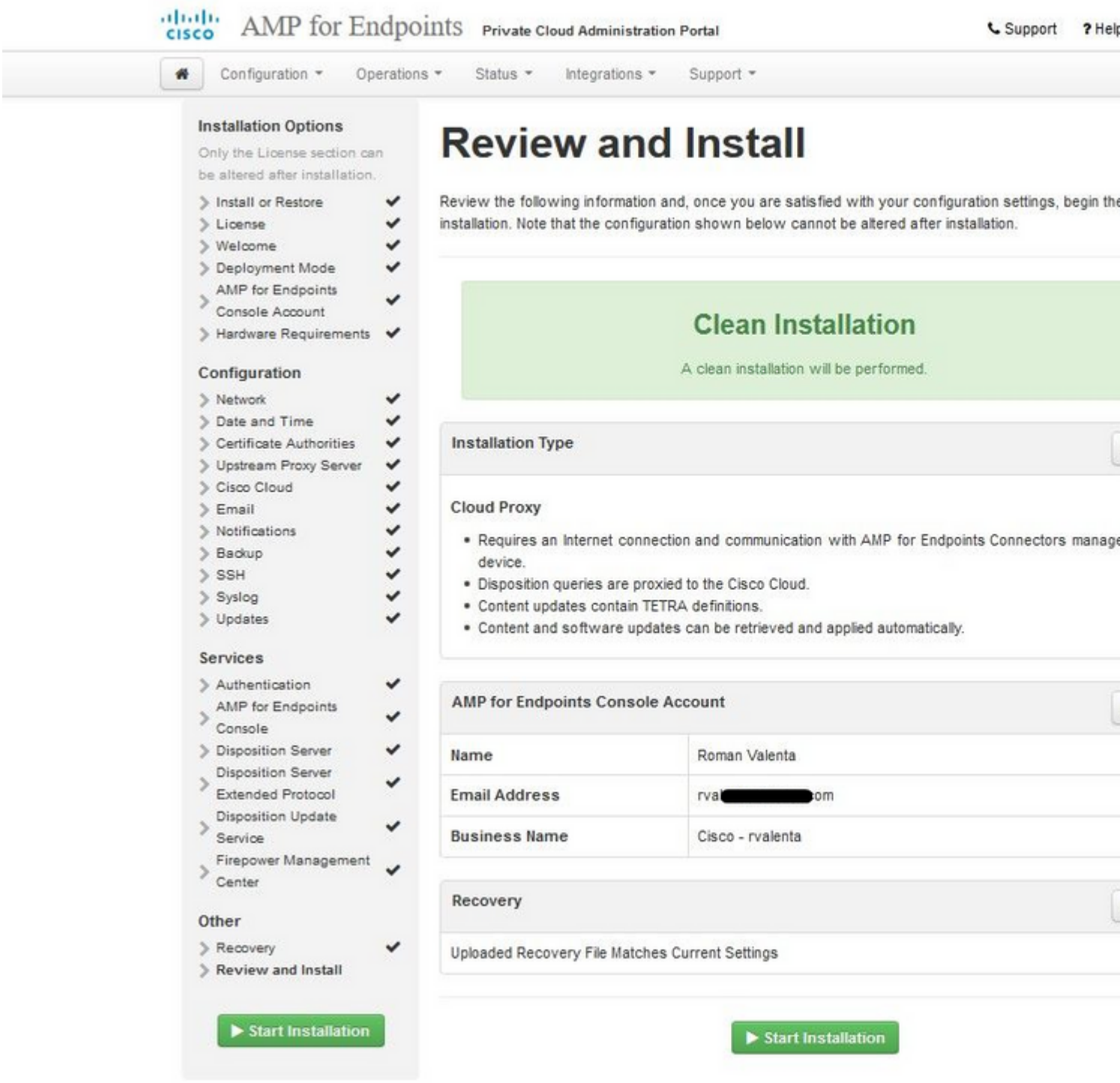
Auf der nächsten Seite herunterladen und dann überprüfen **Wiederherstellungsdatei**.

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.

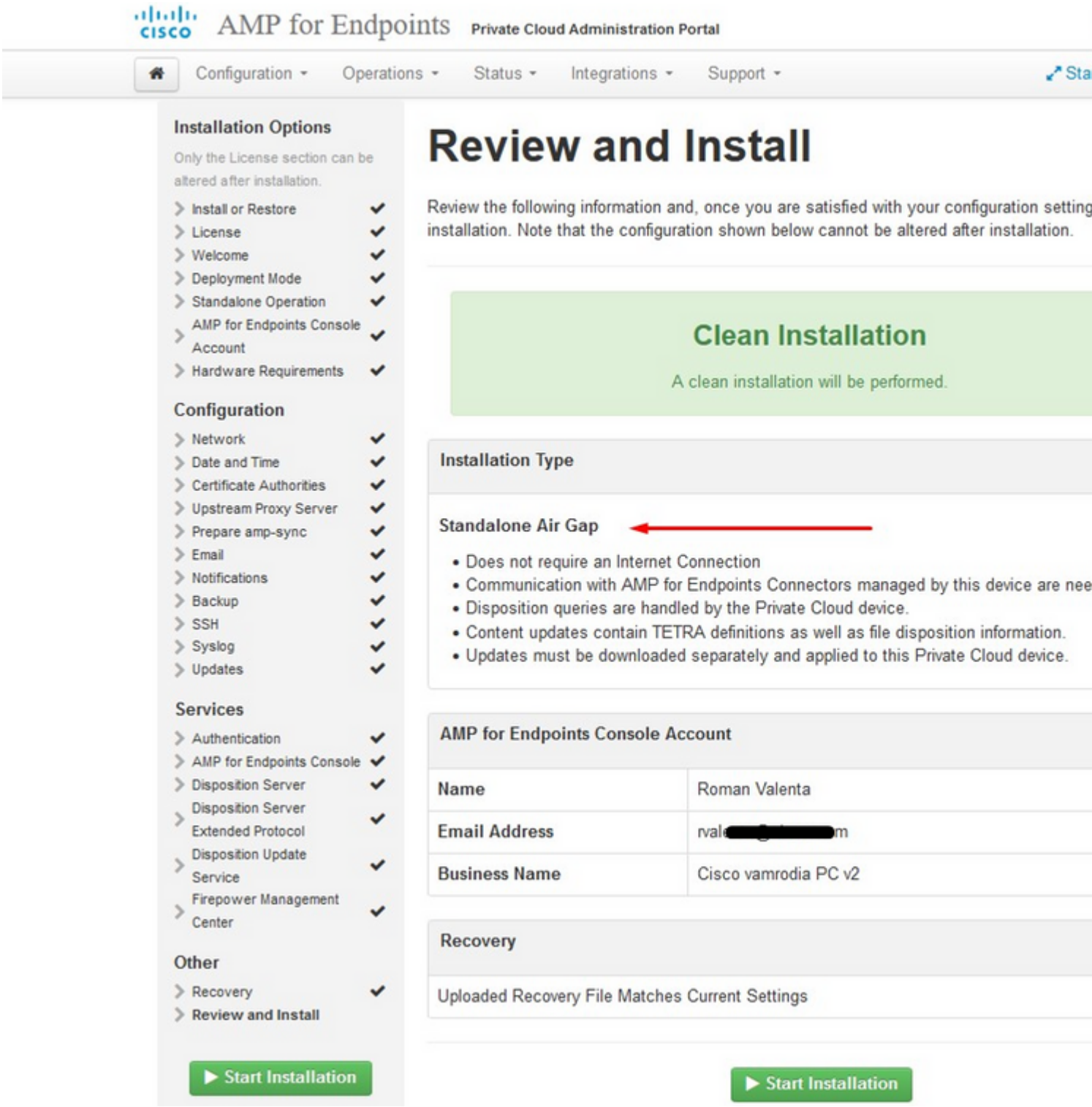
Wählen Sie auf **Herunterladen**, um die Sicherung auf Ihrem lokalen Computer zu speichern. Wenn die Datei heruntergeladen wurde, wählen Sie **Choose File (Datei auswählen**) aus, um die Sicherungsdatei hochzuladen, und stellen Sie sicher, dass sie nicht beschädigt ist. Wählen Sie auf **Weiter**, um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





â€f

ï¸¾ ï¸¾ NUR LUFTSPALT ï¸¾ ï¸¾



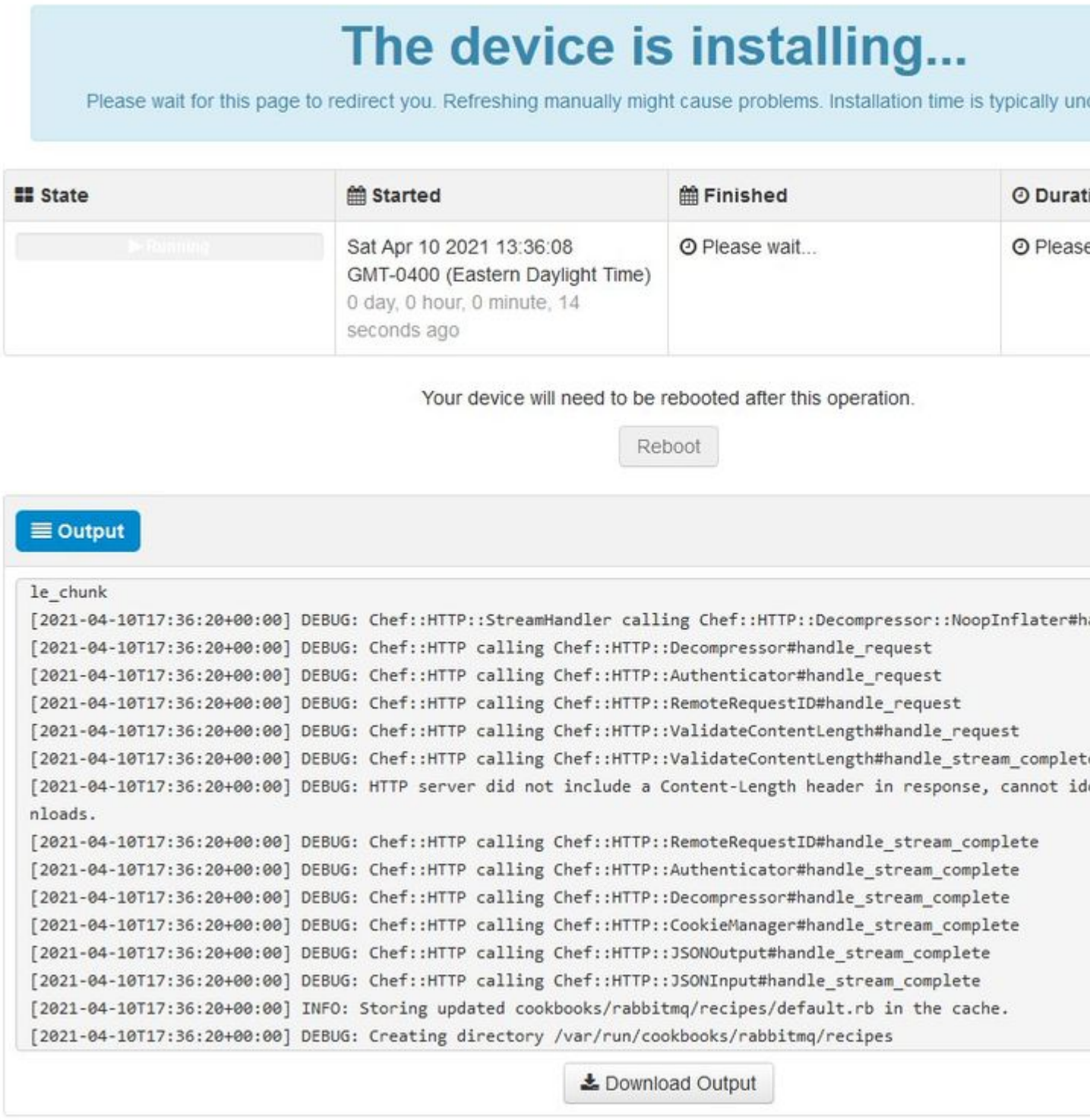
â€ƒ

â€ƒ

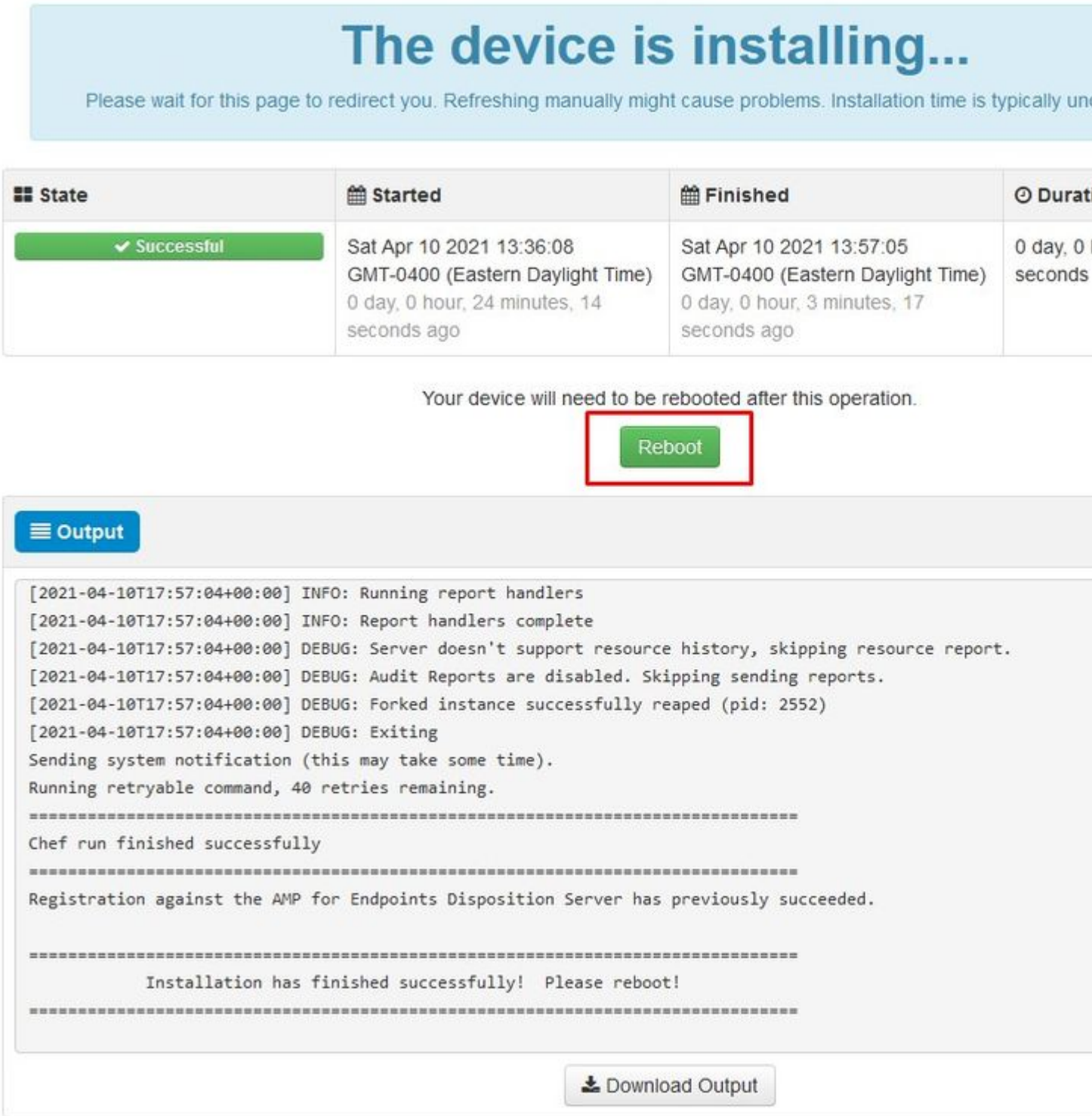
ï¸½ ï¸½ NUR ï¸½ ï¸½

Sie sehen ähnliche Eingabe wie diese...

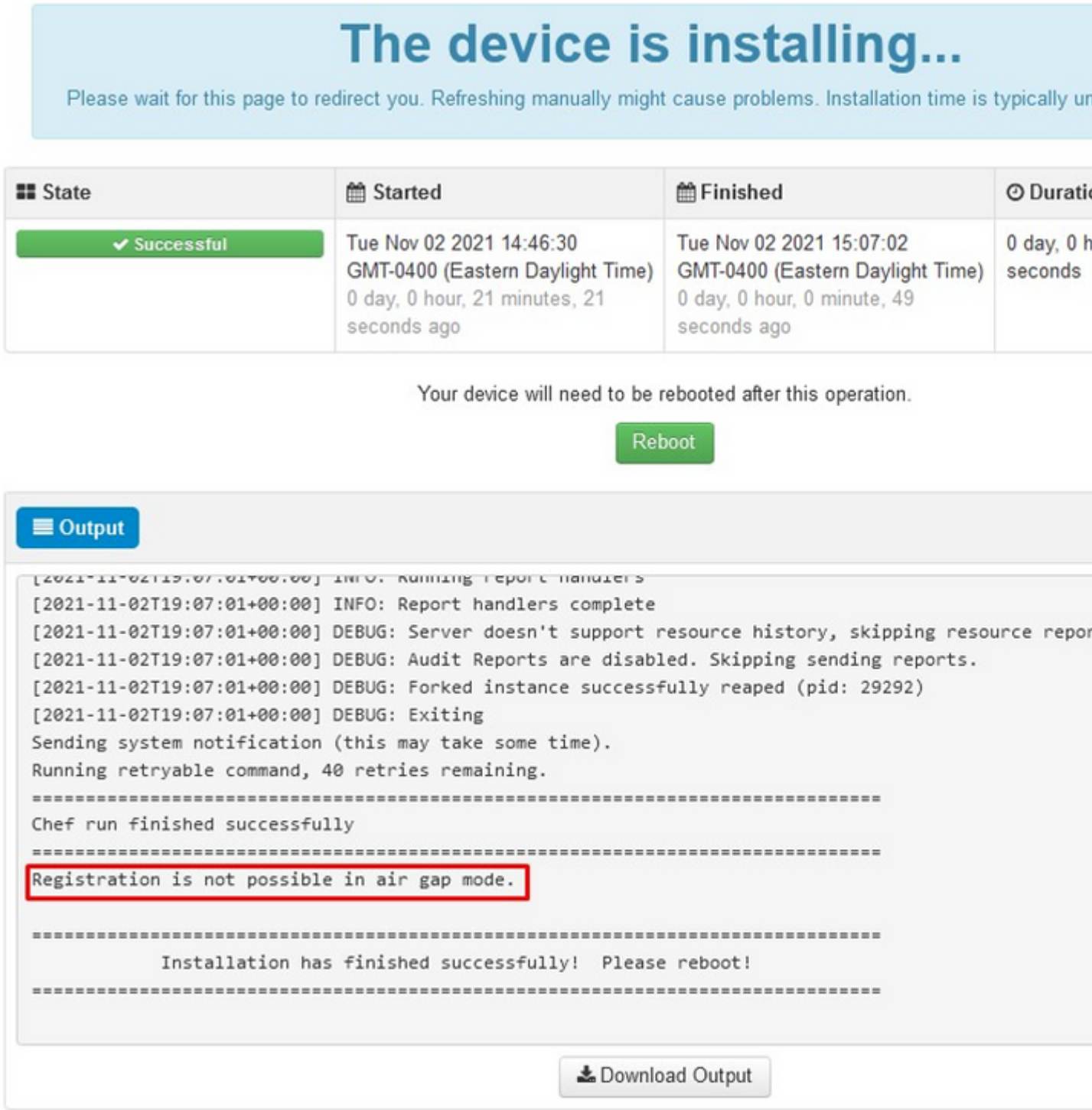
> **Vorsicht**: Wenn Sie sich auf dieser Seite befinden, aktualisieren Sie diese nicht, da sie Probleme verursachen kann.



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

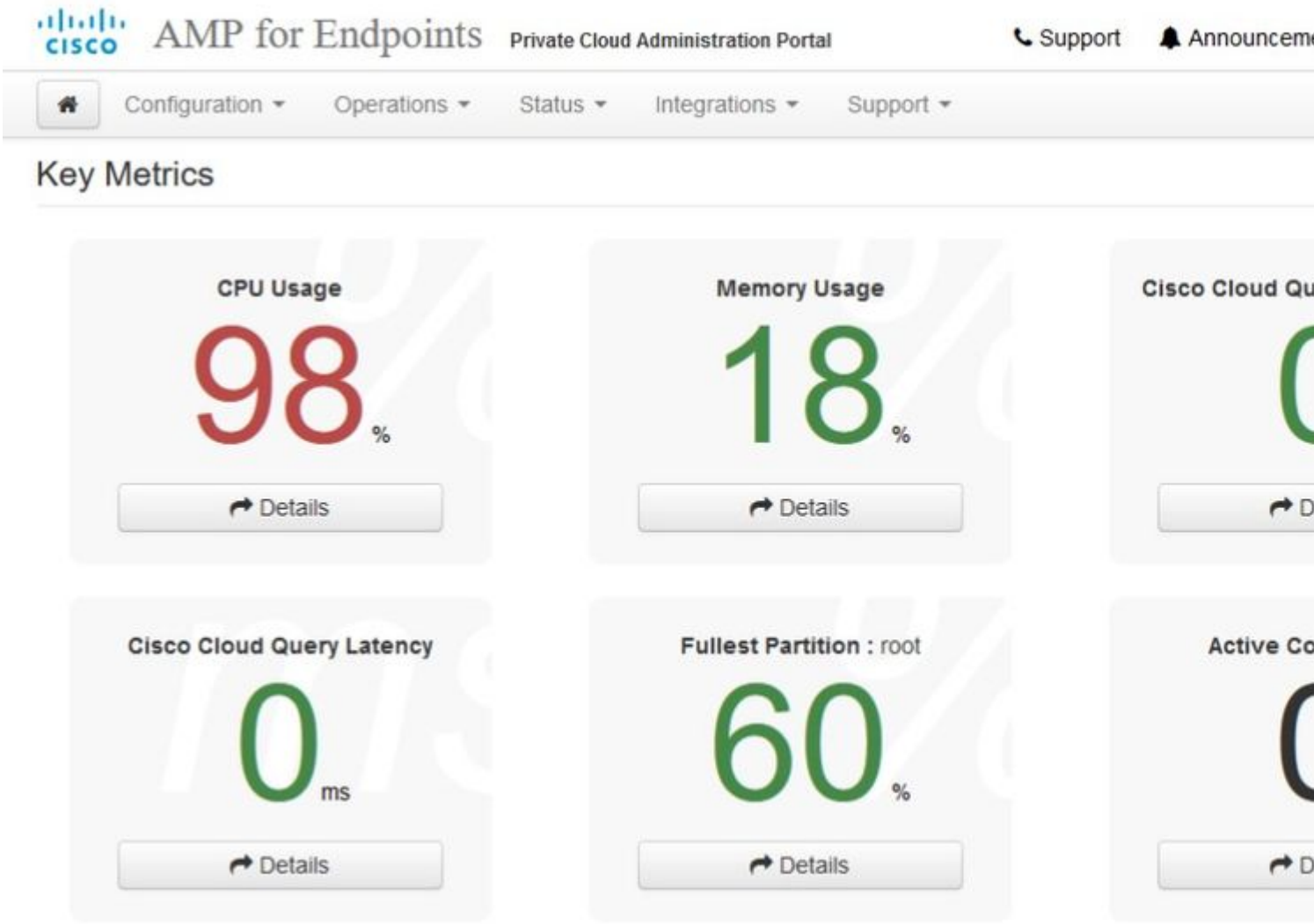


ï¸¾ ï¸¾ NUR LUFTSPALT ï¸¾ ï¸¾

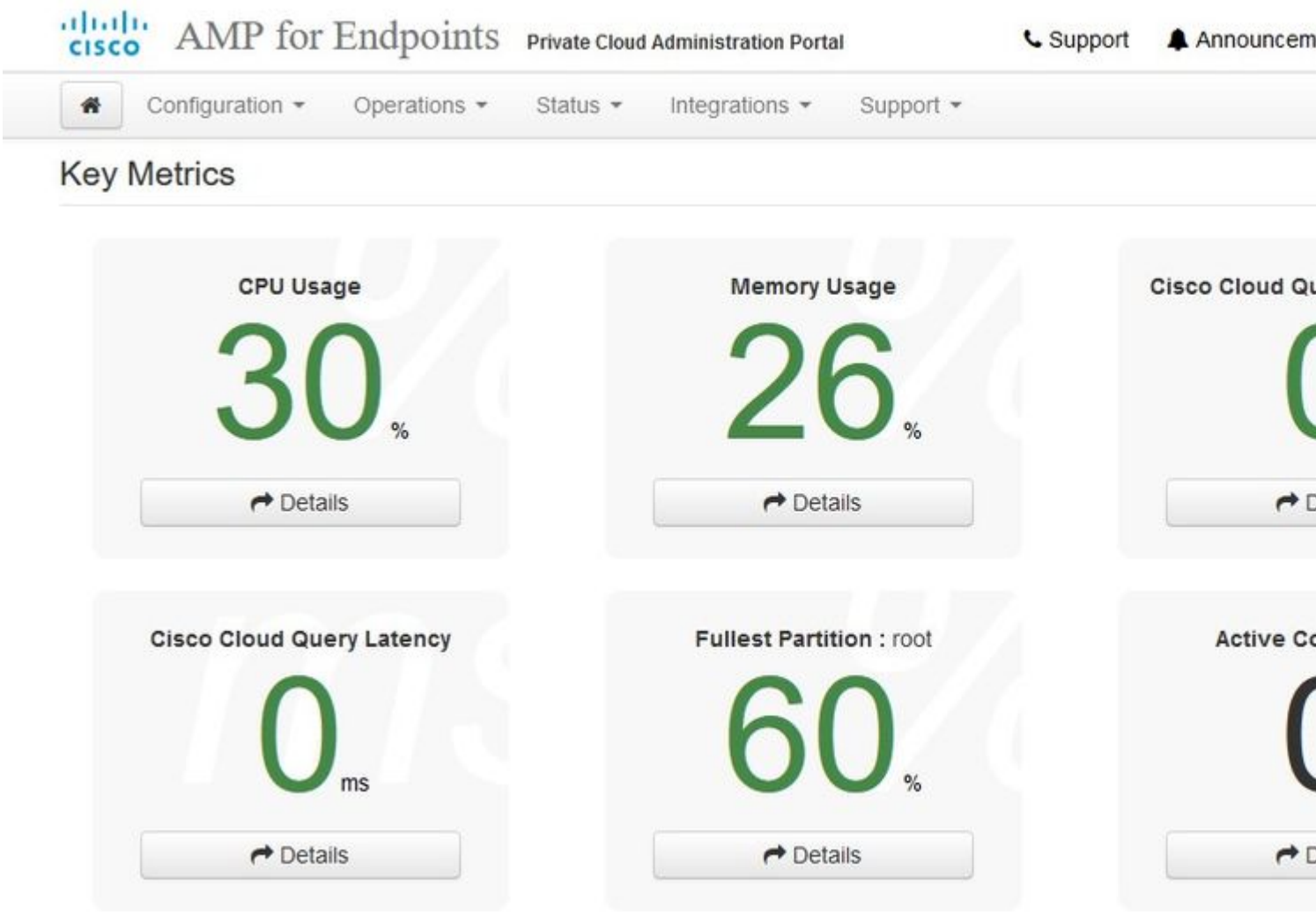


ï¸½ ï¸½ NUR ï¸½ ï¸½

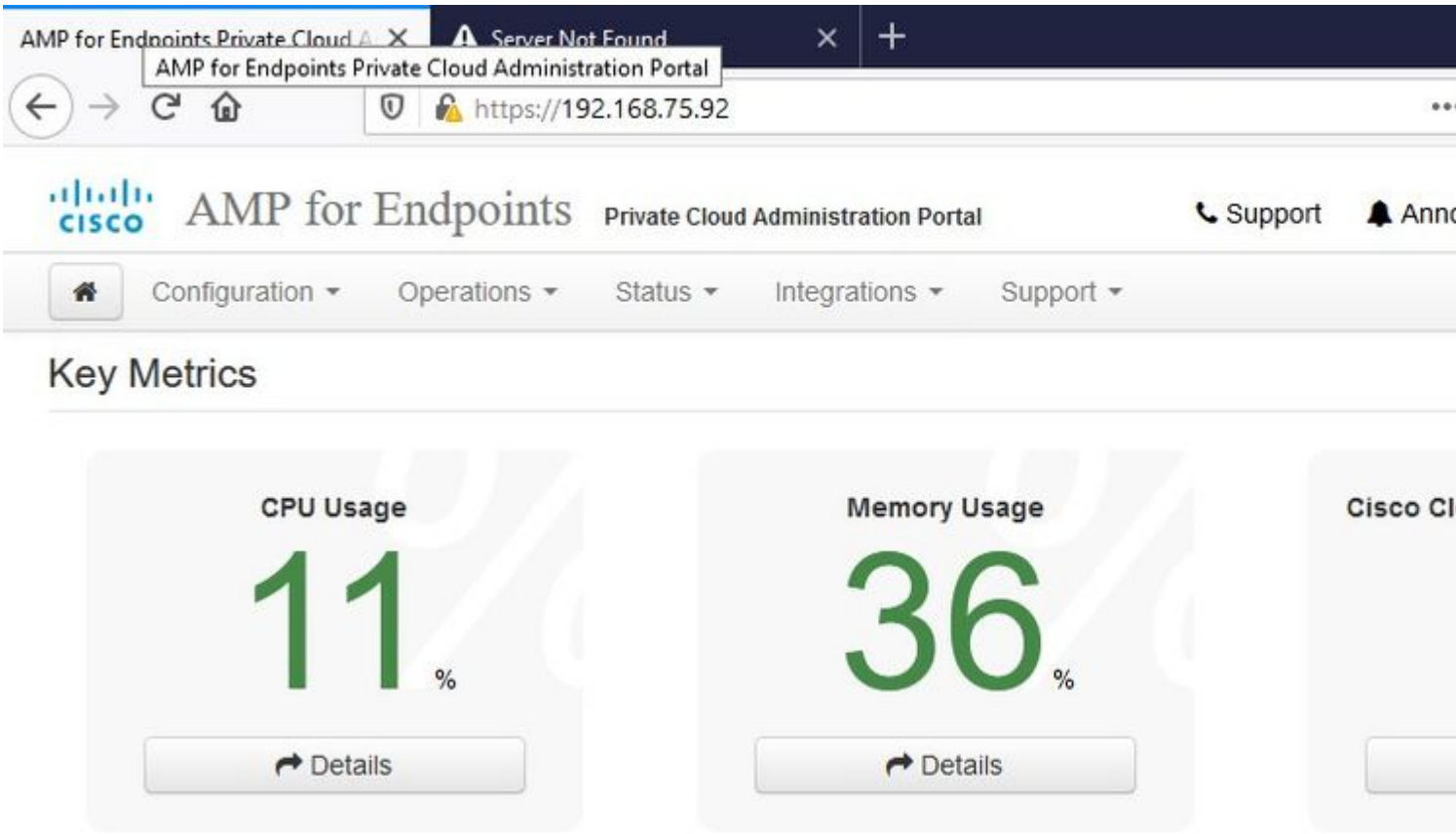
Sobald die Appliance vollständig gestartet wurde, wird Ihnen das Dashboard angezeigt, wenn Sie sich das nächste Mal mit Ihrer Admin-Schnittstelle anmelden. Sie können feststellen, hohe CPU am Anfang, aber wenn Sie einige Minuten geben, wird es beruhigt.



Nach wenigen Minuten...

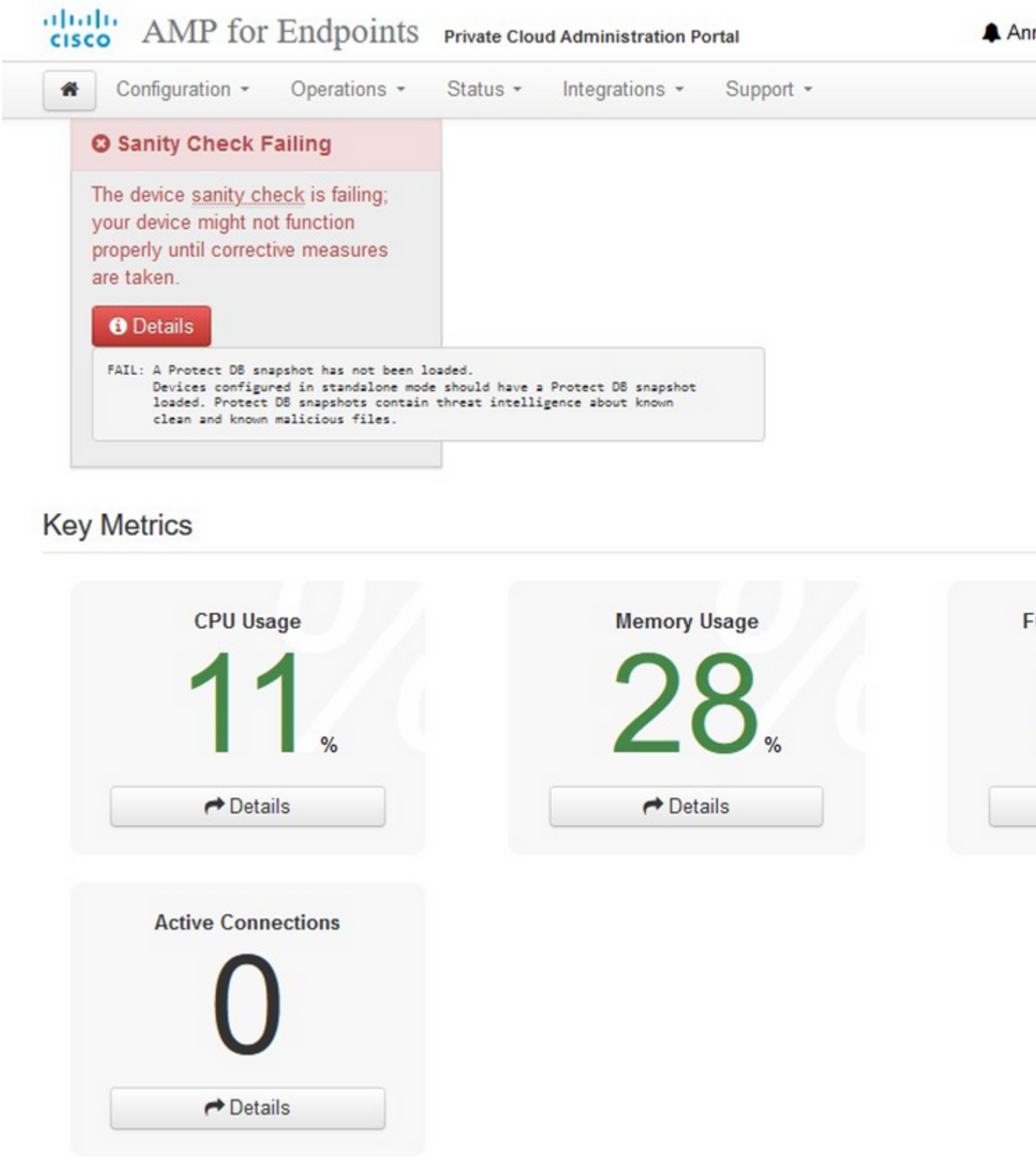


Navigieren Sie von hier zur Konsole für sichere Endgeräte. Klicke auf das kleine Symbol, das wie ein Feuer aussieht, in der rechten Ecke neben der Flagge.

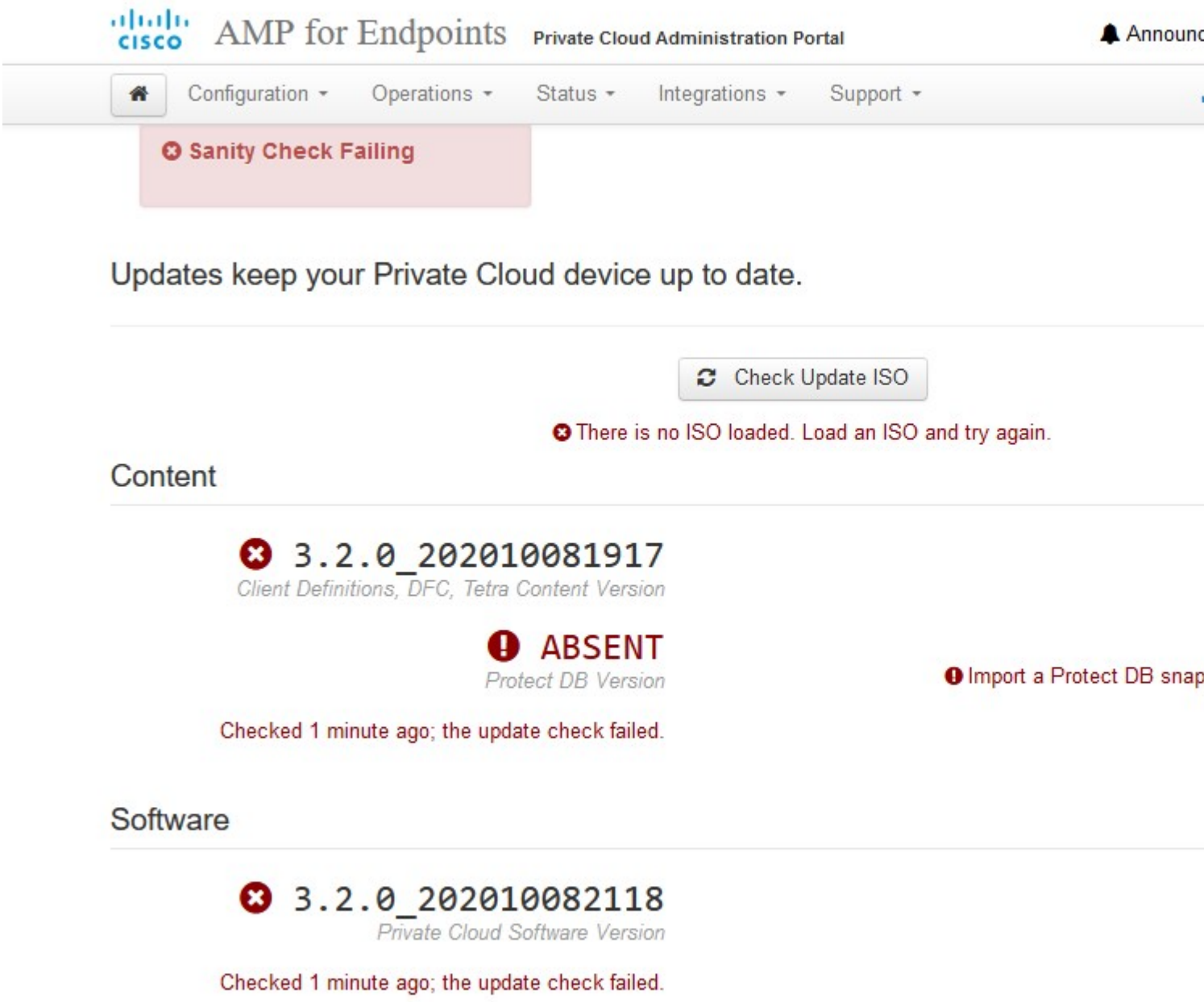


ï¸¾ ï¸¾ NUR LUFTSPALT ï¸¾ ï¸¾

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.


AMP for Endpoints
Private Cloud Administration Portal
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.
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

â€ƒ



AirGap-Aktualisierungspaket

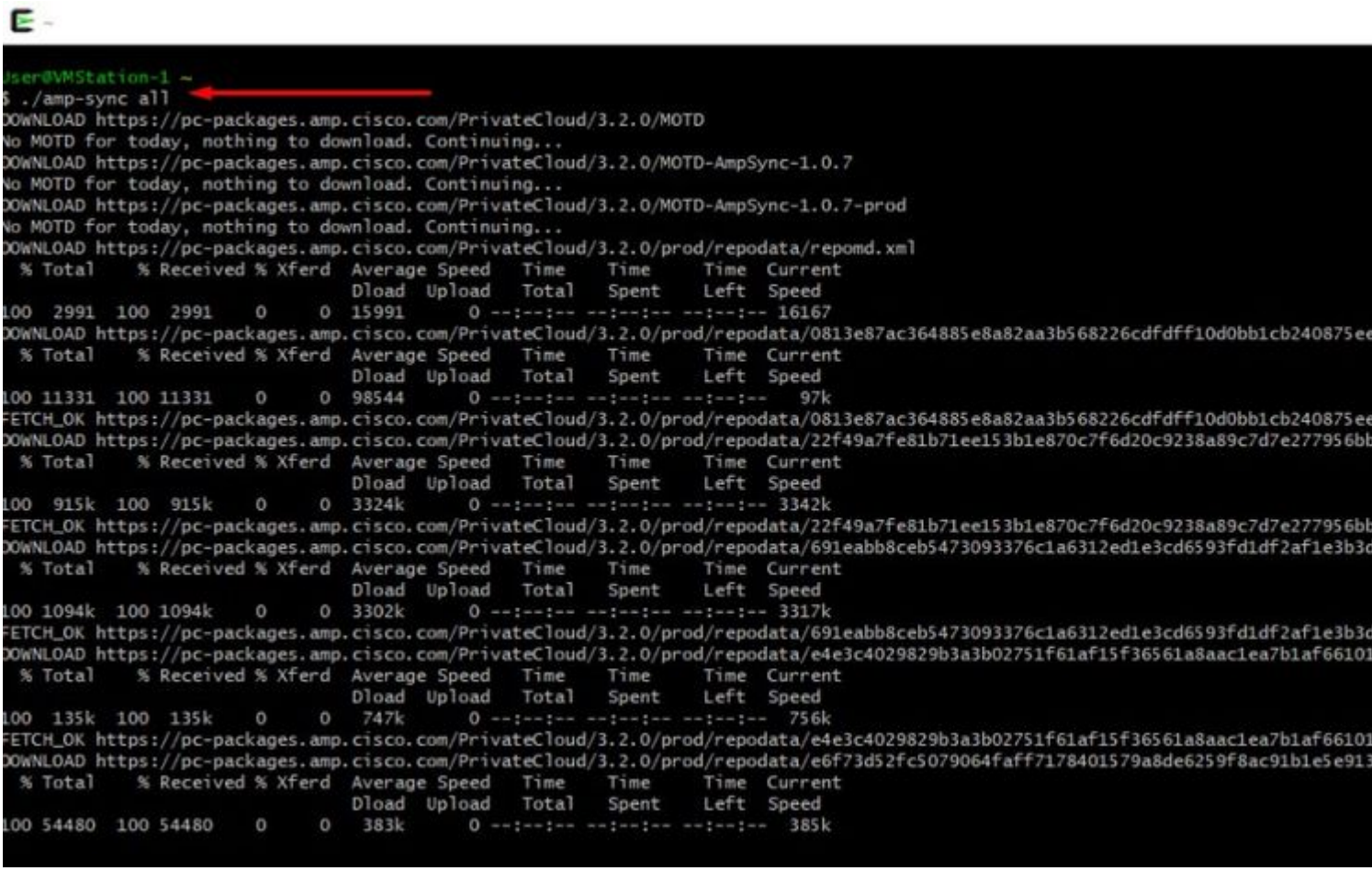
Zum ersten Mal müssen wir diesen Befehl verwenden, um die Protect DB zu erhalten

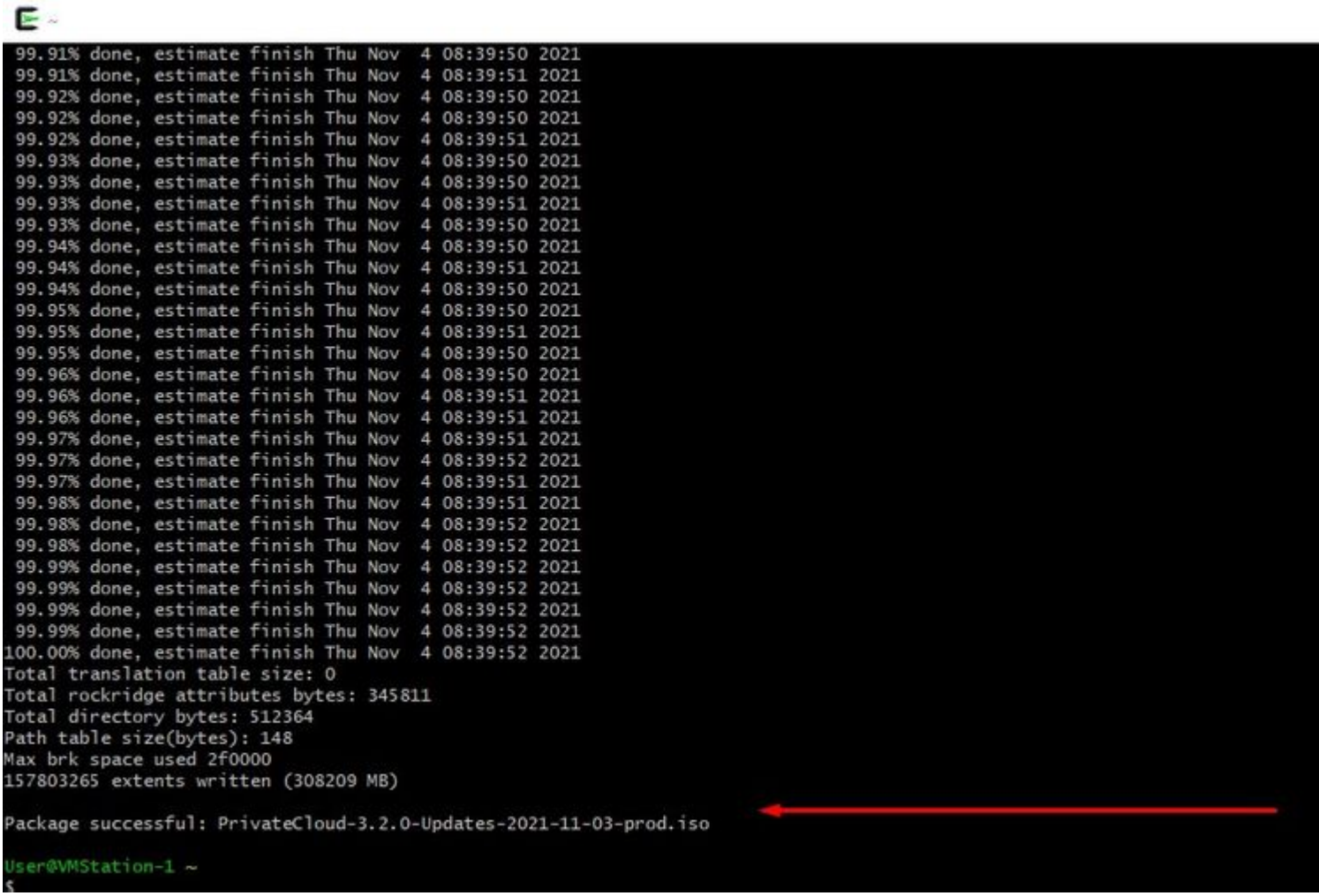
```
./amp-sync all
```

> **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.** â€Œ

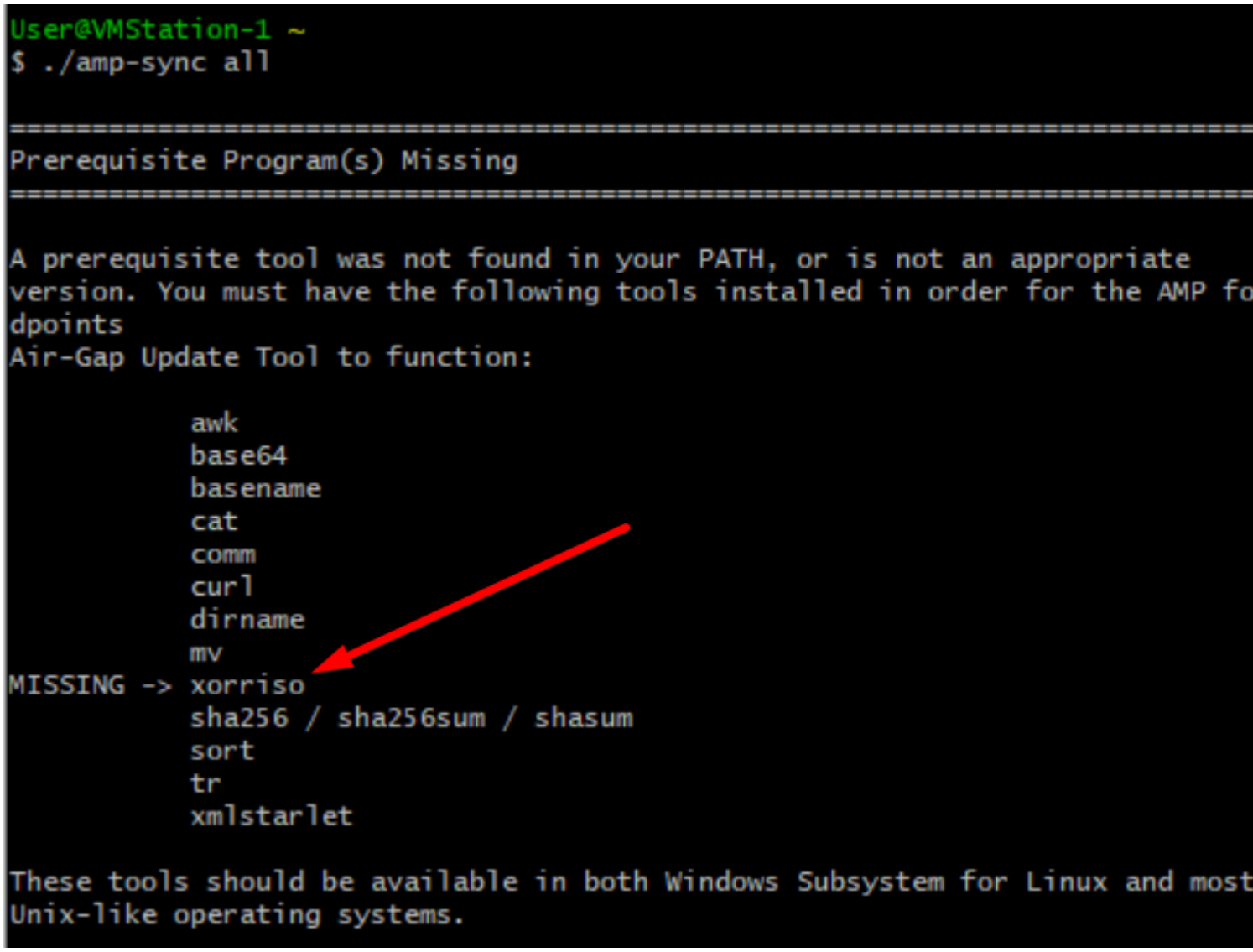
In diesem Beispiel haben wir **CygWin64** verwendet

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**





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



â€ƒ

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
```

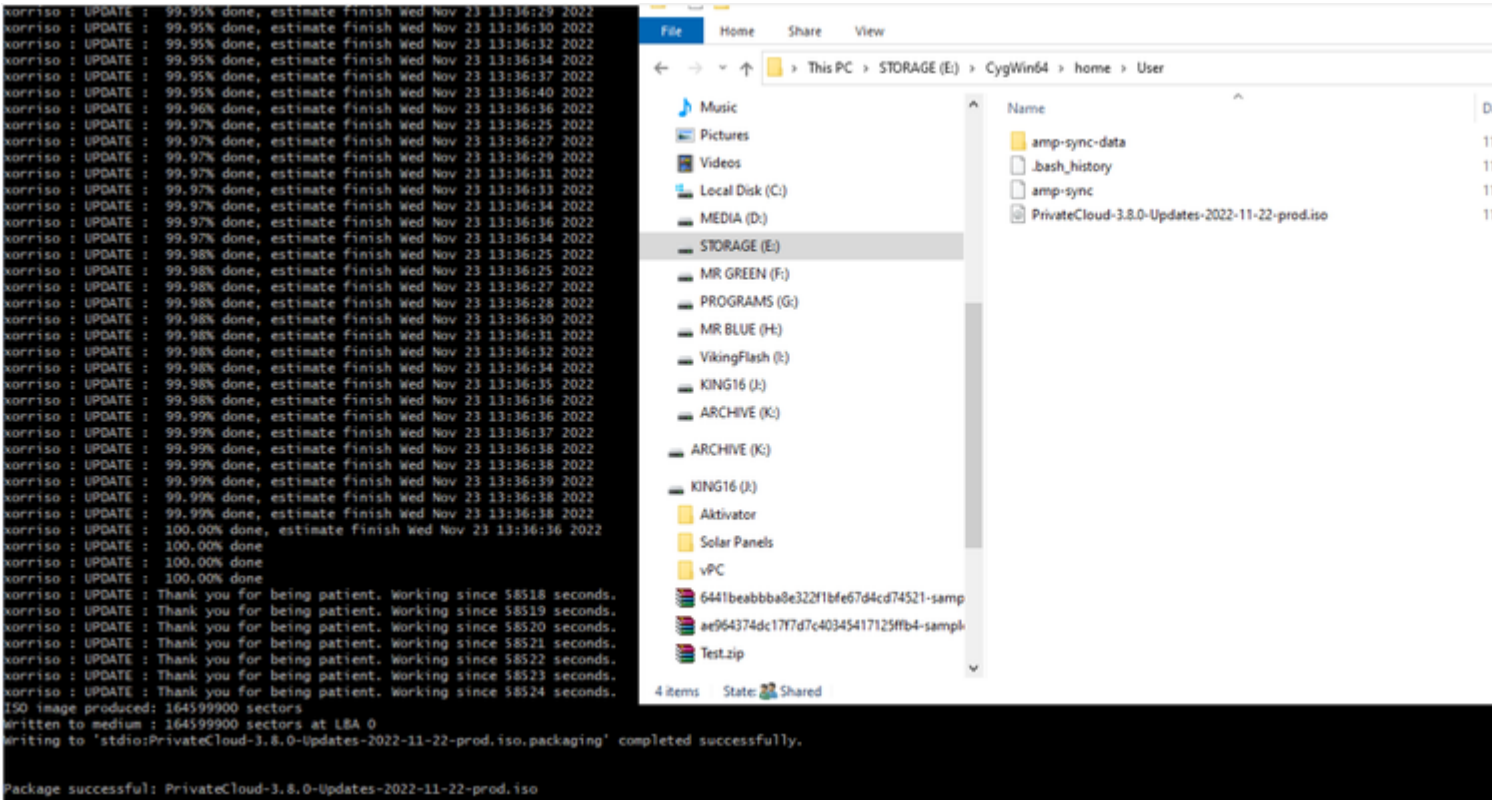
Windows

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€ƒ

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.

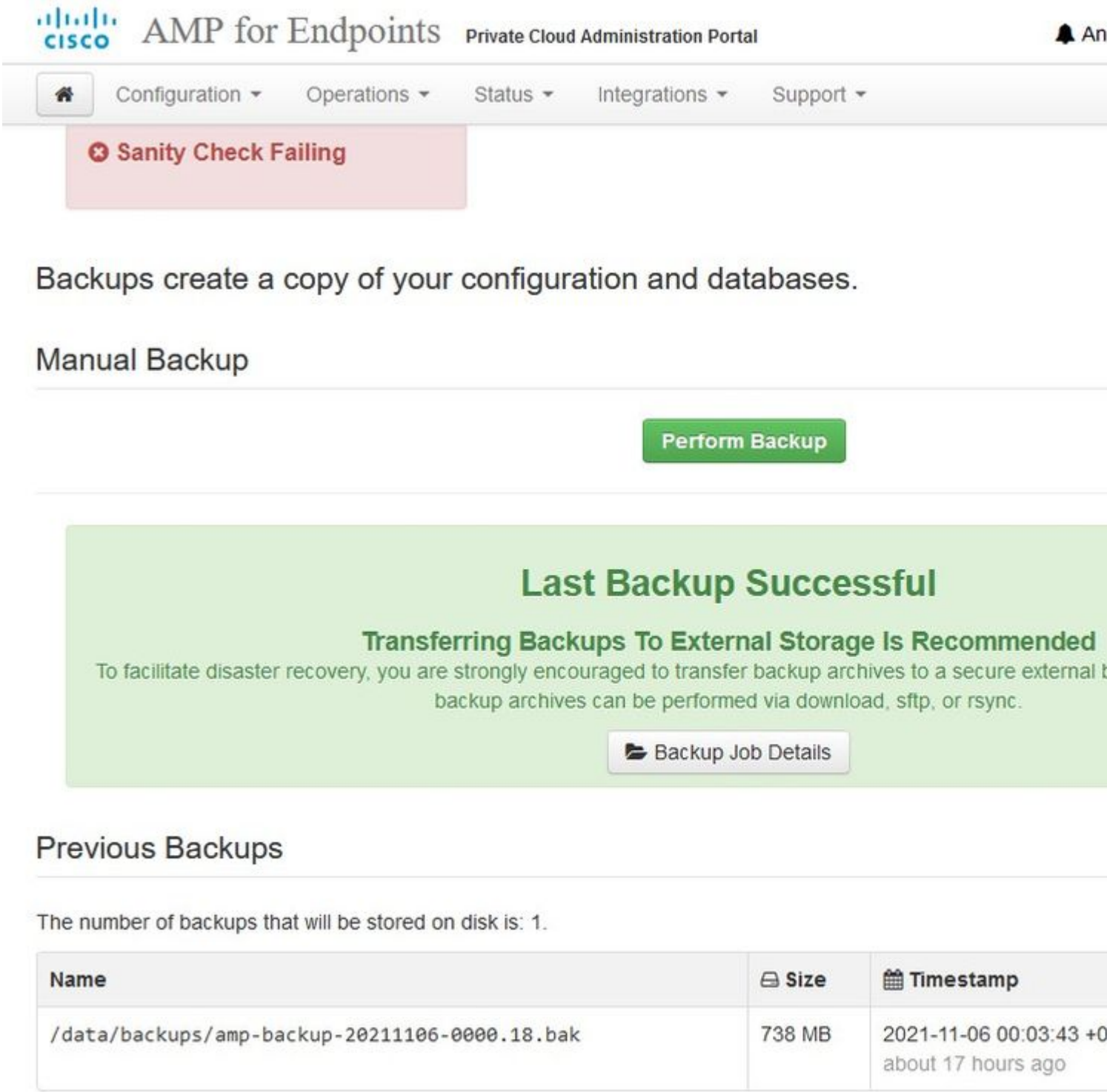


Führen Sie die Sicherung der aktuellen (*in diesem Fall)* 3.2.0 VPC im Airgap-Modus durch.

Sie können diesen Befehl in der Befehlszeile verwenden.

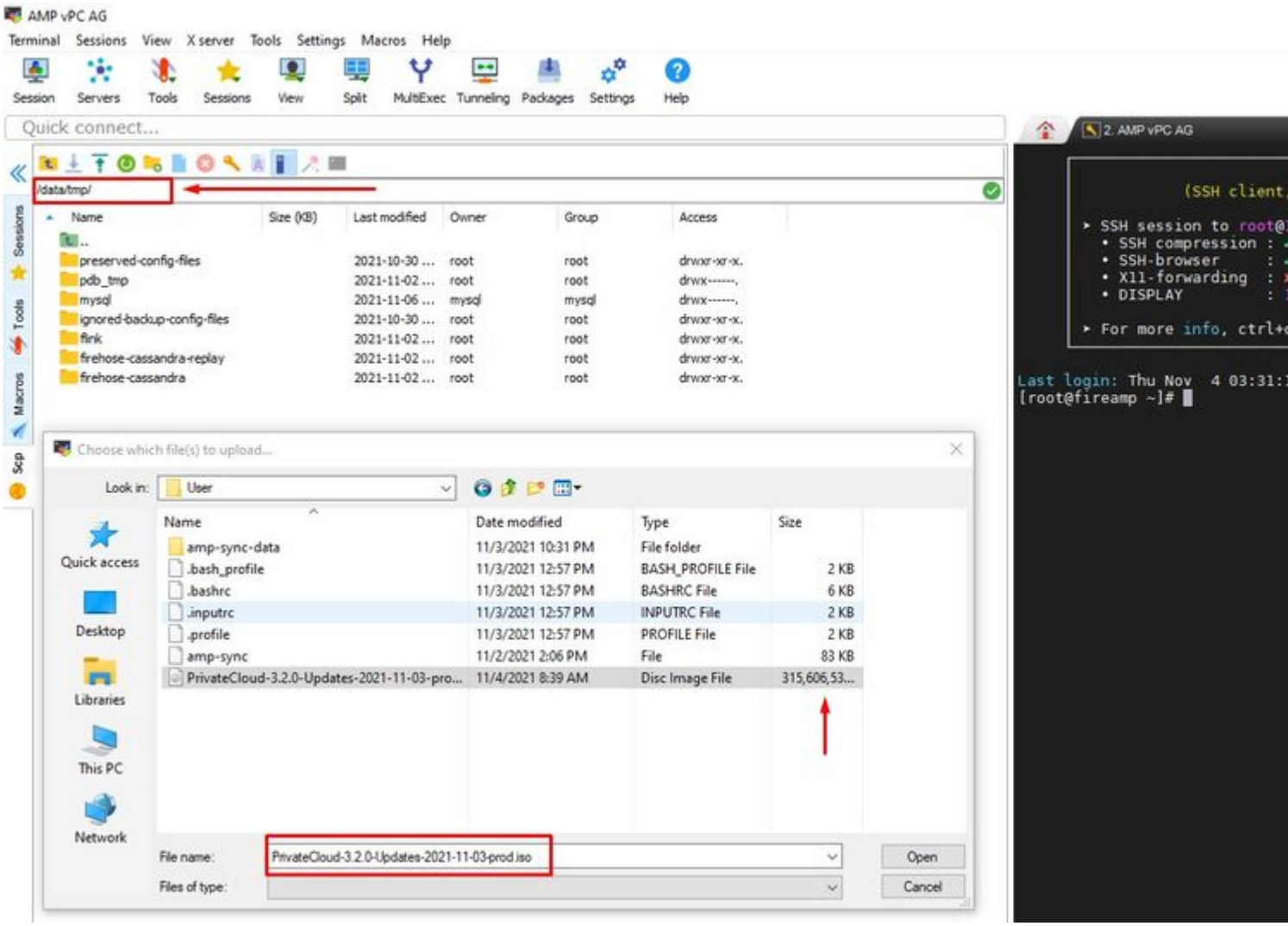
```
rpm -qa | grep Pri
```

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



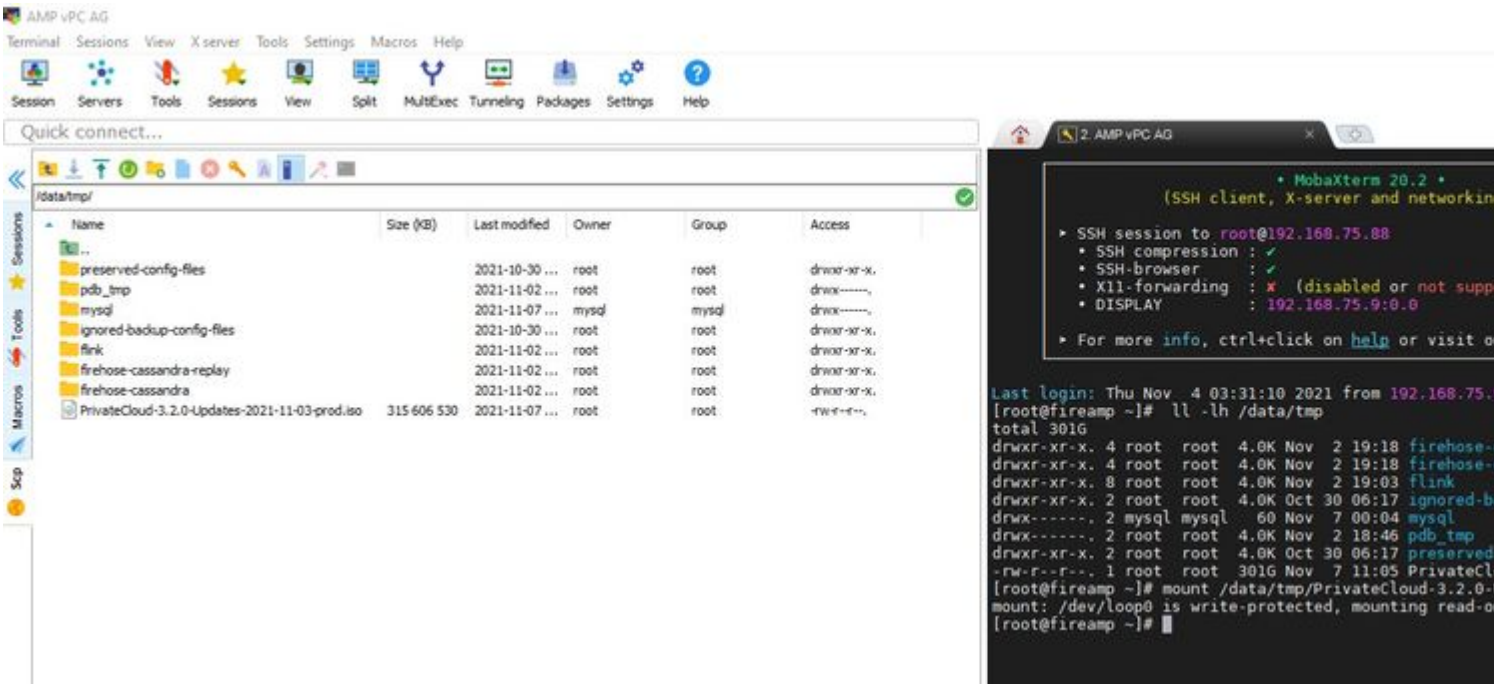
Übertragen Sie die neueste ISO, die mit amp-sync generiert wurde, auf die vPC. Dies kann je nach Ihrer Geschwindigkeit bis zu mehreren Stunden dauern. In diesem Fall übernahm der Transfer 16h

```
/data/tmp
```



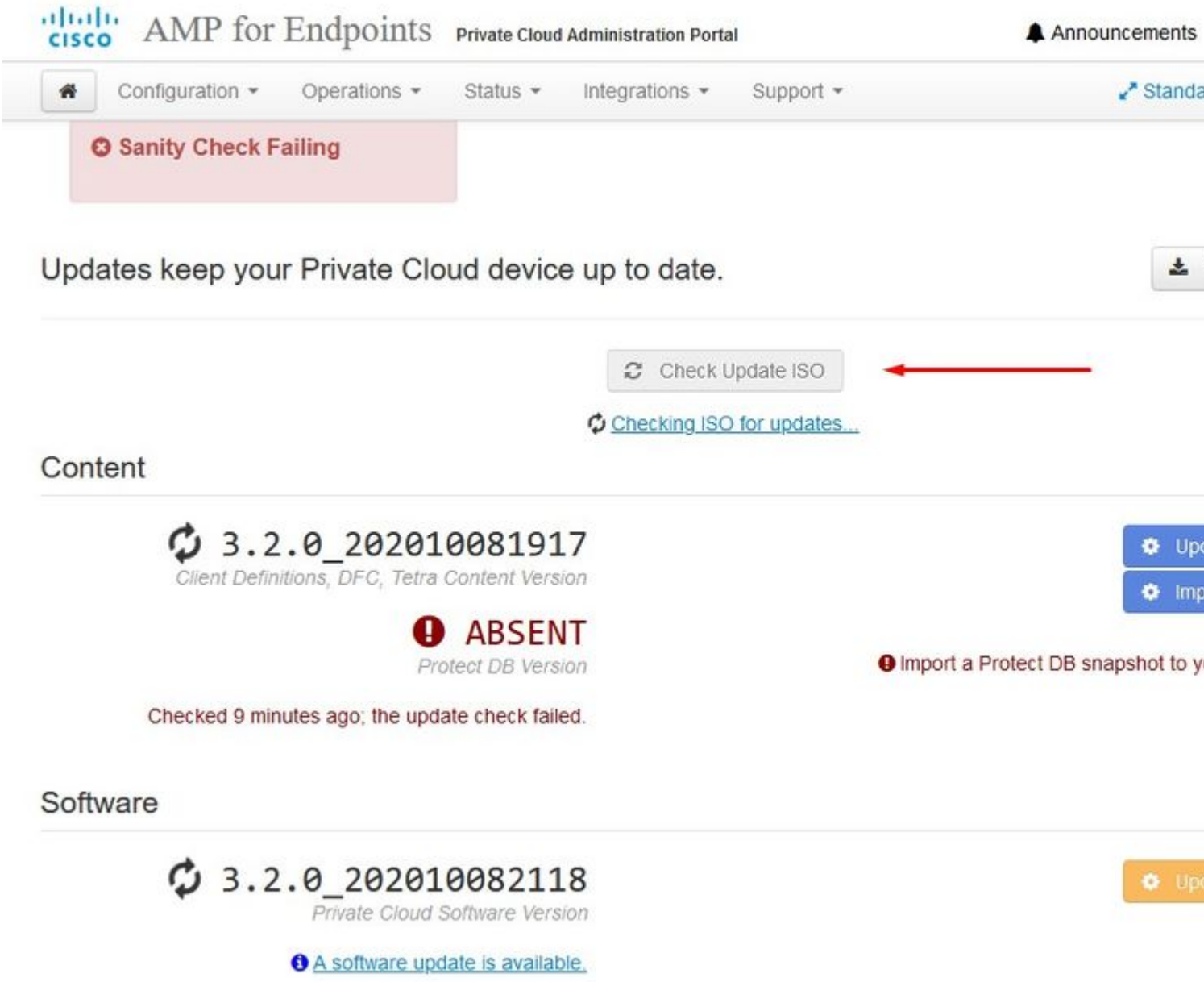
Nachdem der Upload abgeschlossen ist, mounten Sie die ISO-

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

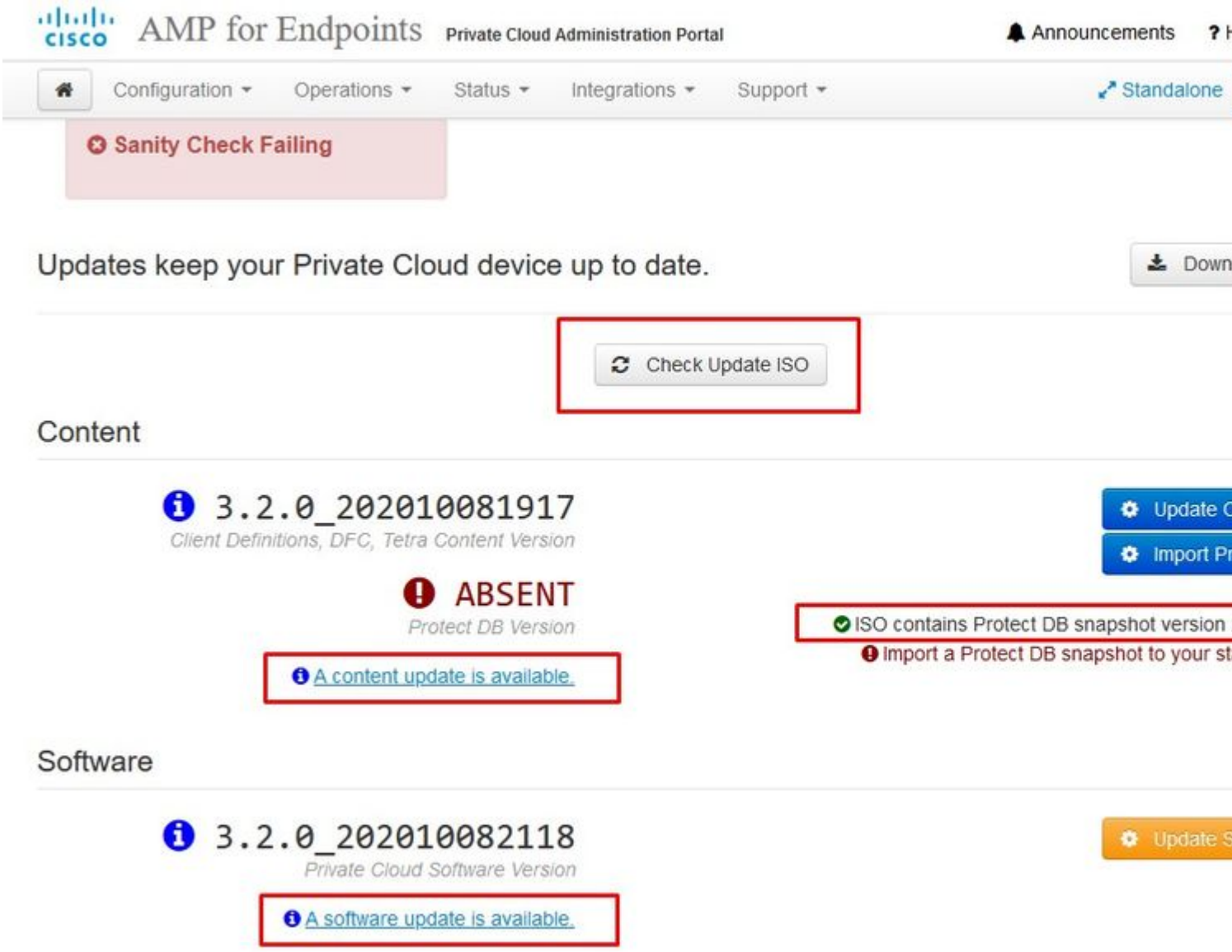


â€ƒ

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

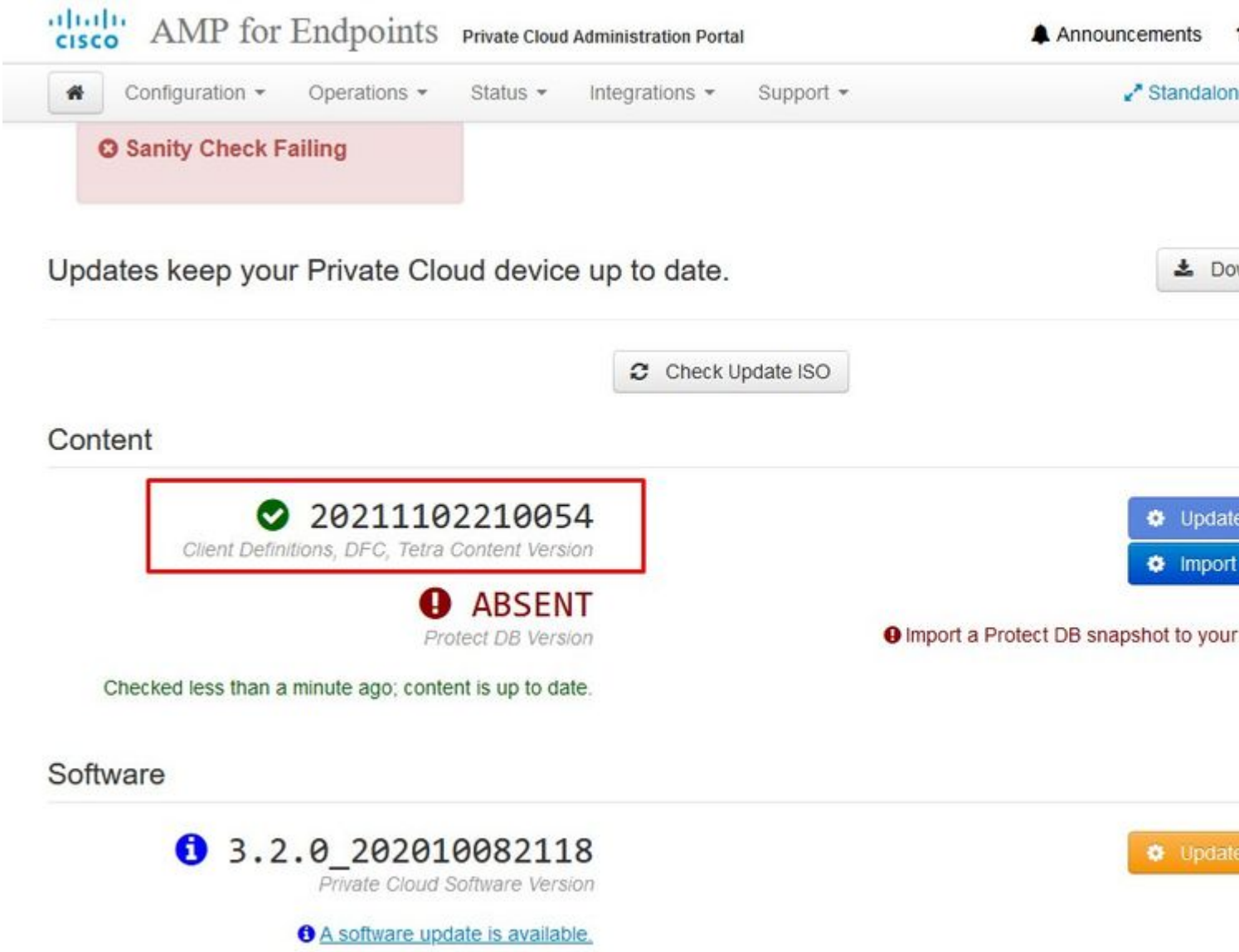


In diesem Beispiel gehe ich zuerst mit **Inhaltsaktualisierung** vor.

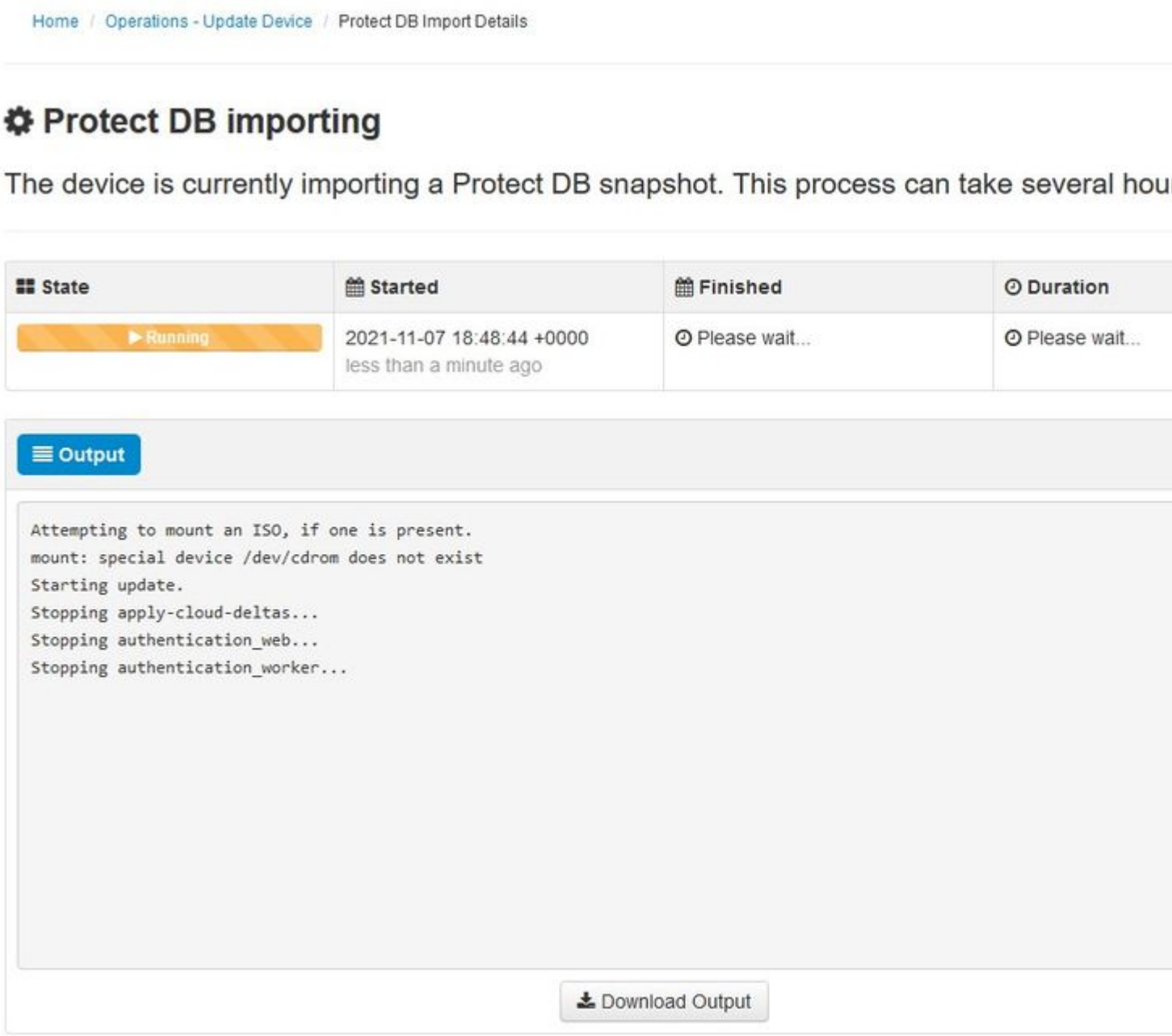


Wählen Sie dann Protect DB importieren aus.

â€ƒ



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


Home / Operations - Update Device / Protect DB Import Details
Protect DB importing
The device is currently importing a Protect DB snapshot. This process can take several hou
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€ƒ

Home / Operations - Update Device / Protect DB Import Details

Protect DB importing

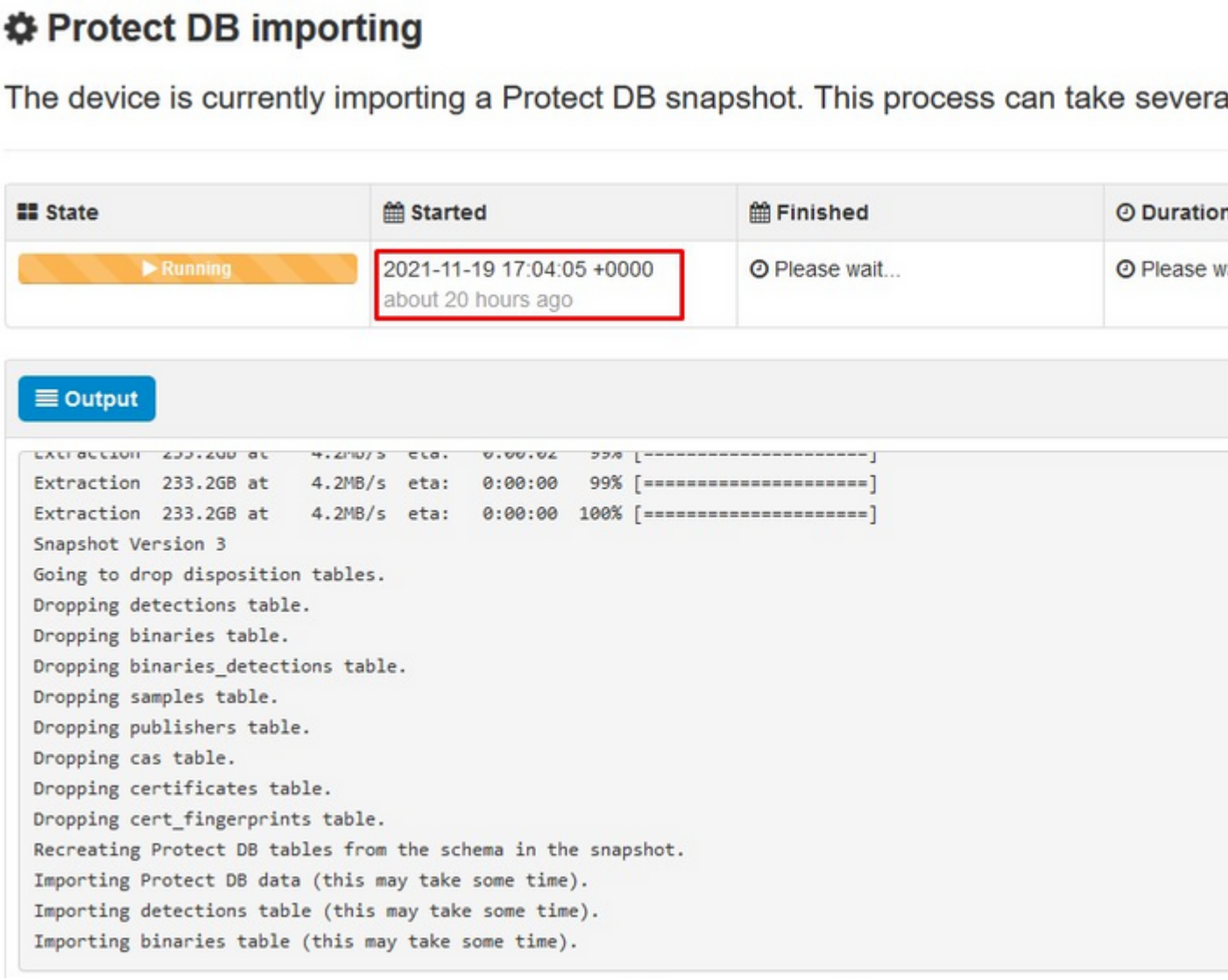
The device is currently importing a Protect DB snapshot. This process can take several h

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

Output

```
Extraction   14.9GB at   6.6MB/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



â€ƒ

Problem #1 - Erschöpfter Platz im Datenspeicher

â€ƒ

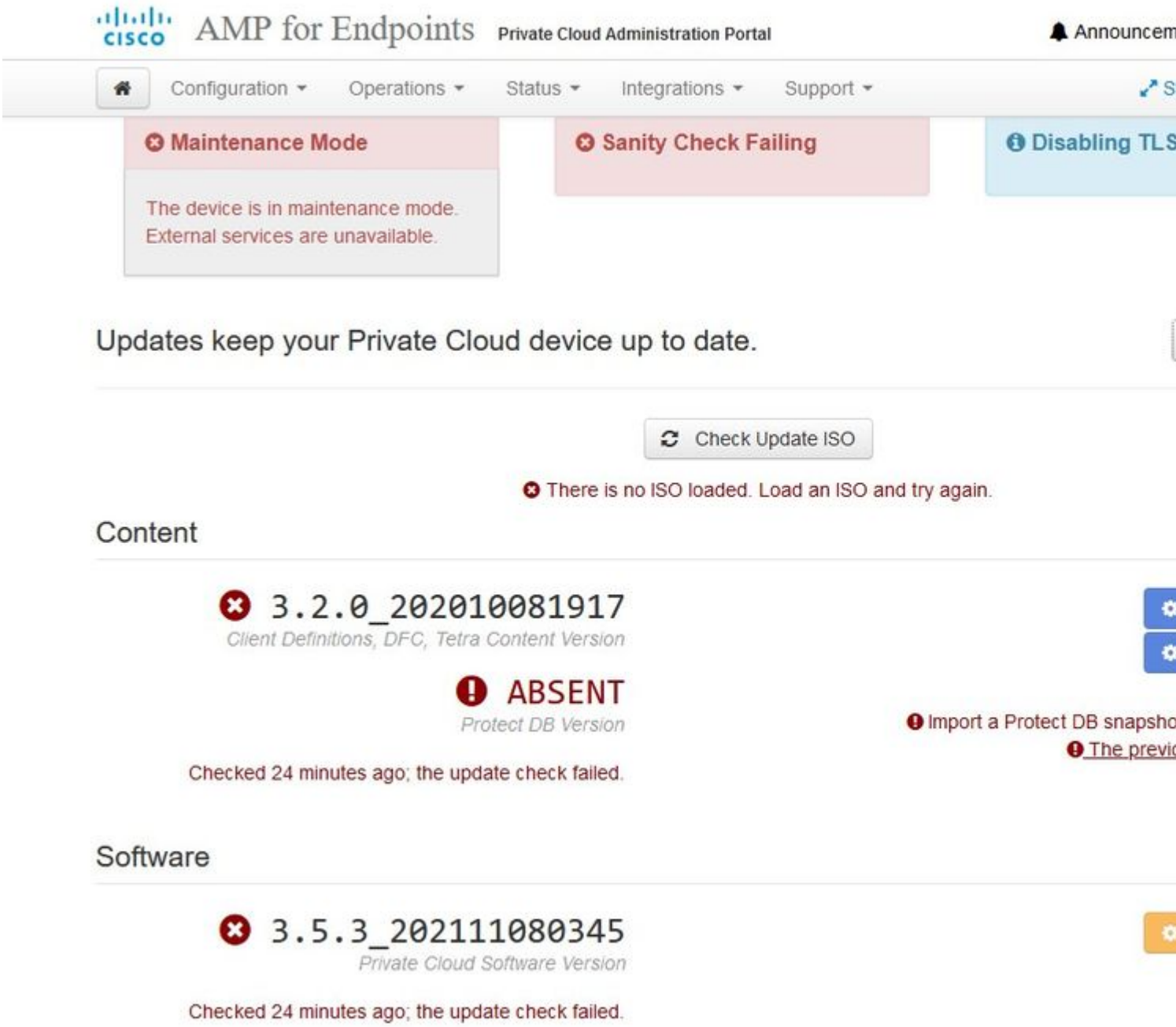
Hier können Sie auf zwei Probleme laufen. Da vPC vor 3.5.2 nicht in der Lage ist, externen NFS-Speicher zu mounten, müssen Sie die ISO-Aktualisierungsdatei in das Verzeichnis **/data/temp** hochladen. In meinem Fall, da mein Datenspeicher nur 1 TB betrug, rannte ich aus dem Raum und das virtuelle System 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.

â€ƒ

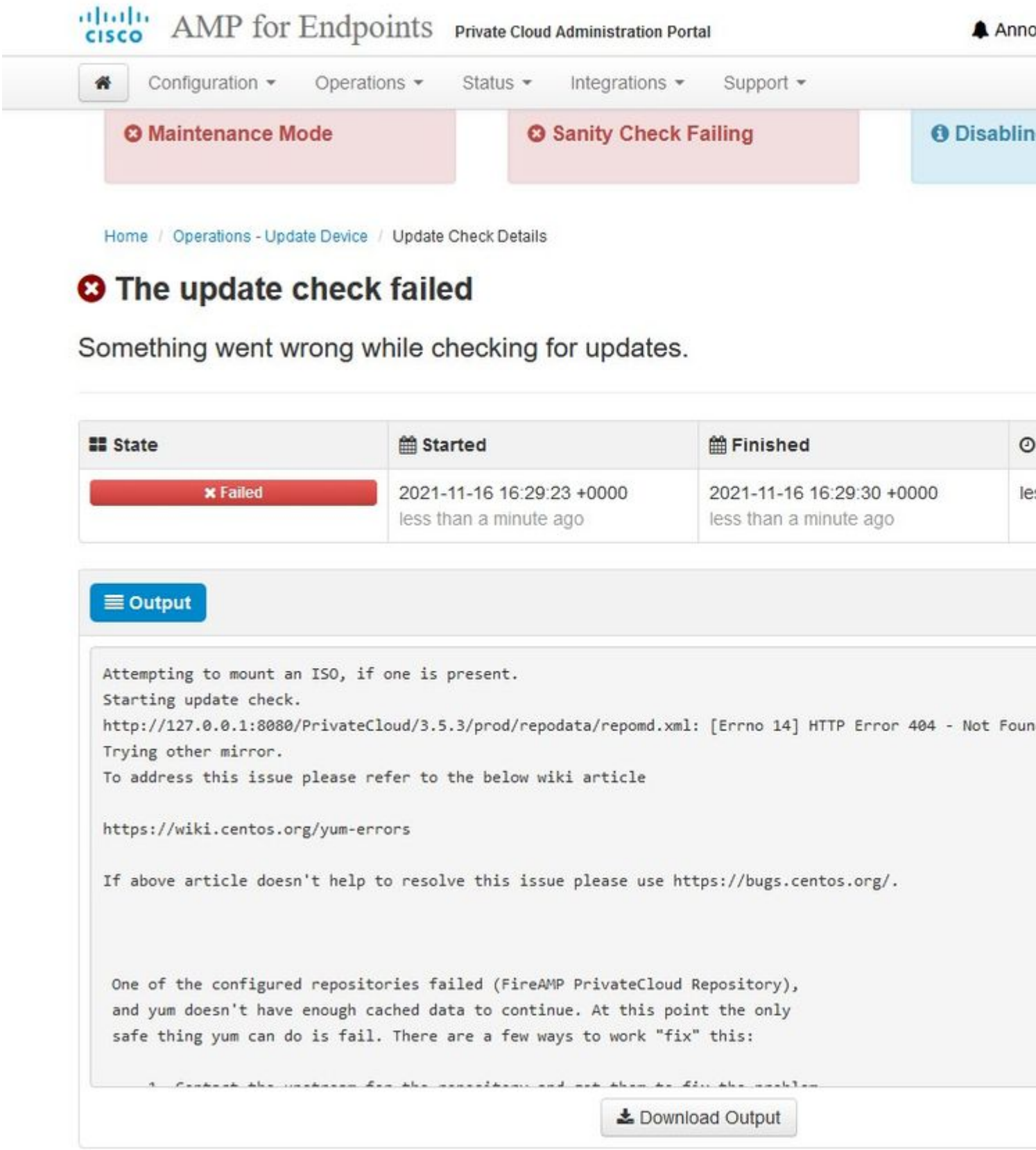
Problem #2 - Altes Update

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.



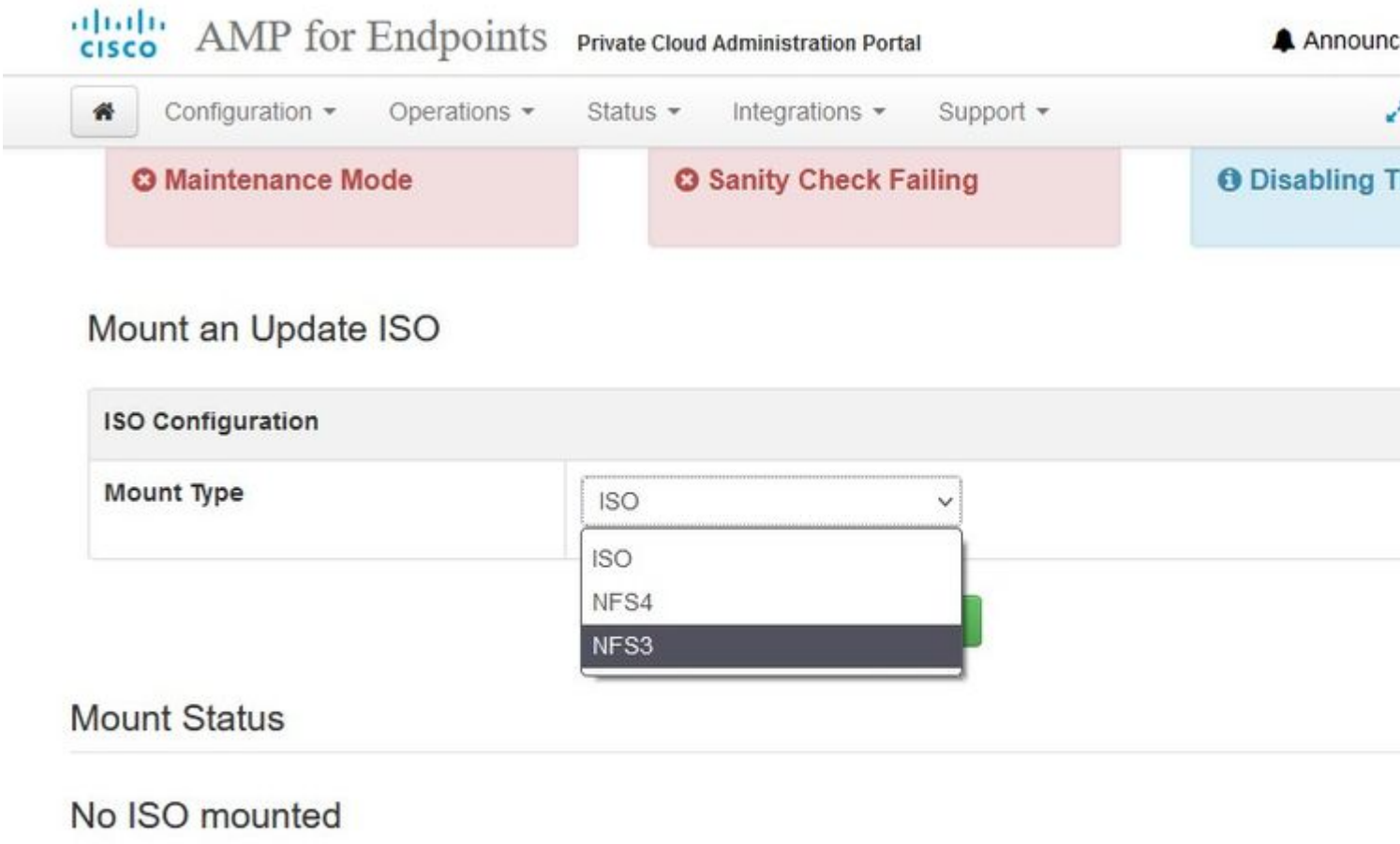
Dies ist der Fehler, den Sie sehen, wenn Sie die ISO-Aktualisierungsdatei erneut mounten.

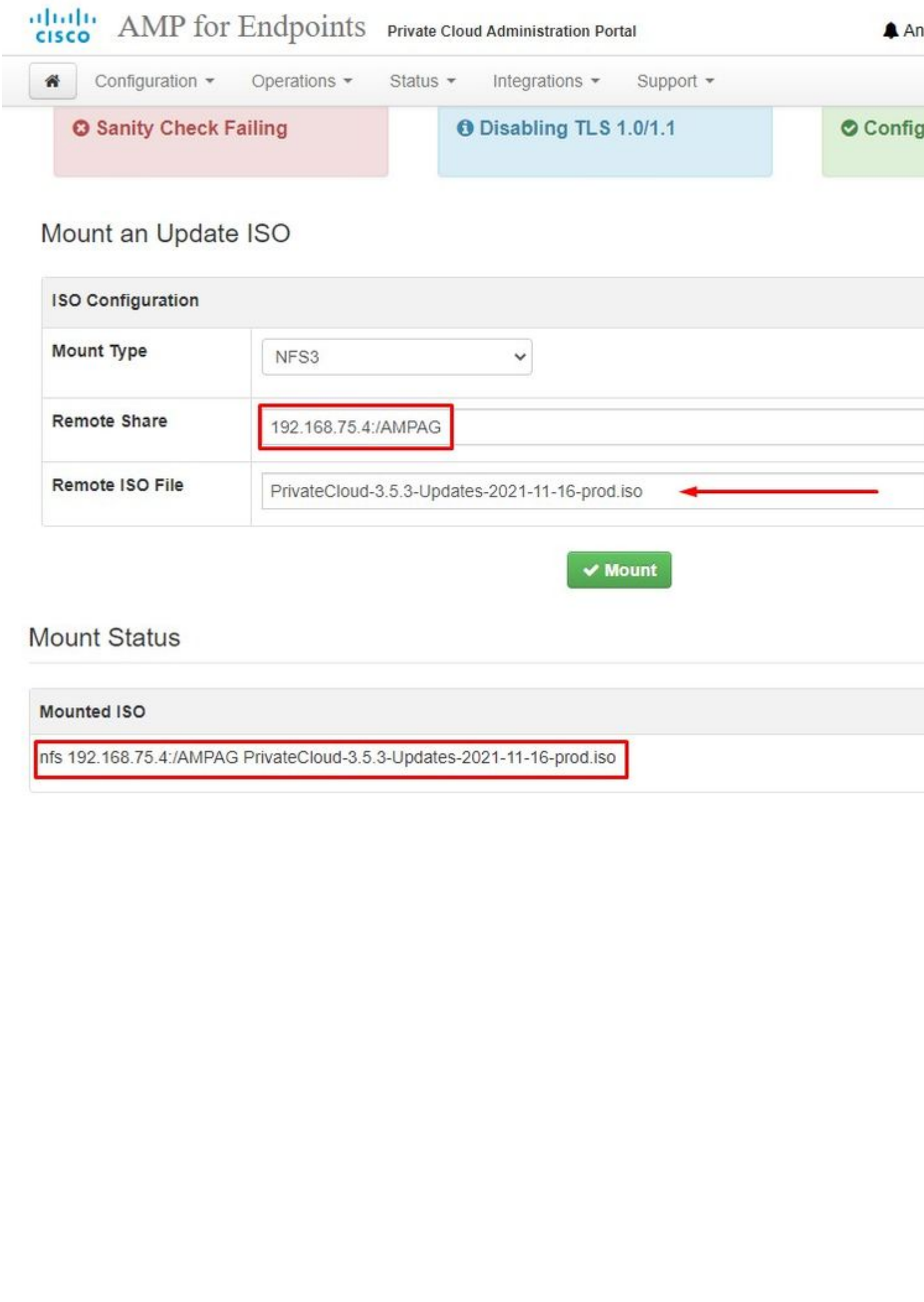
â€ƒ

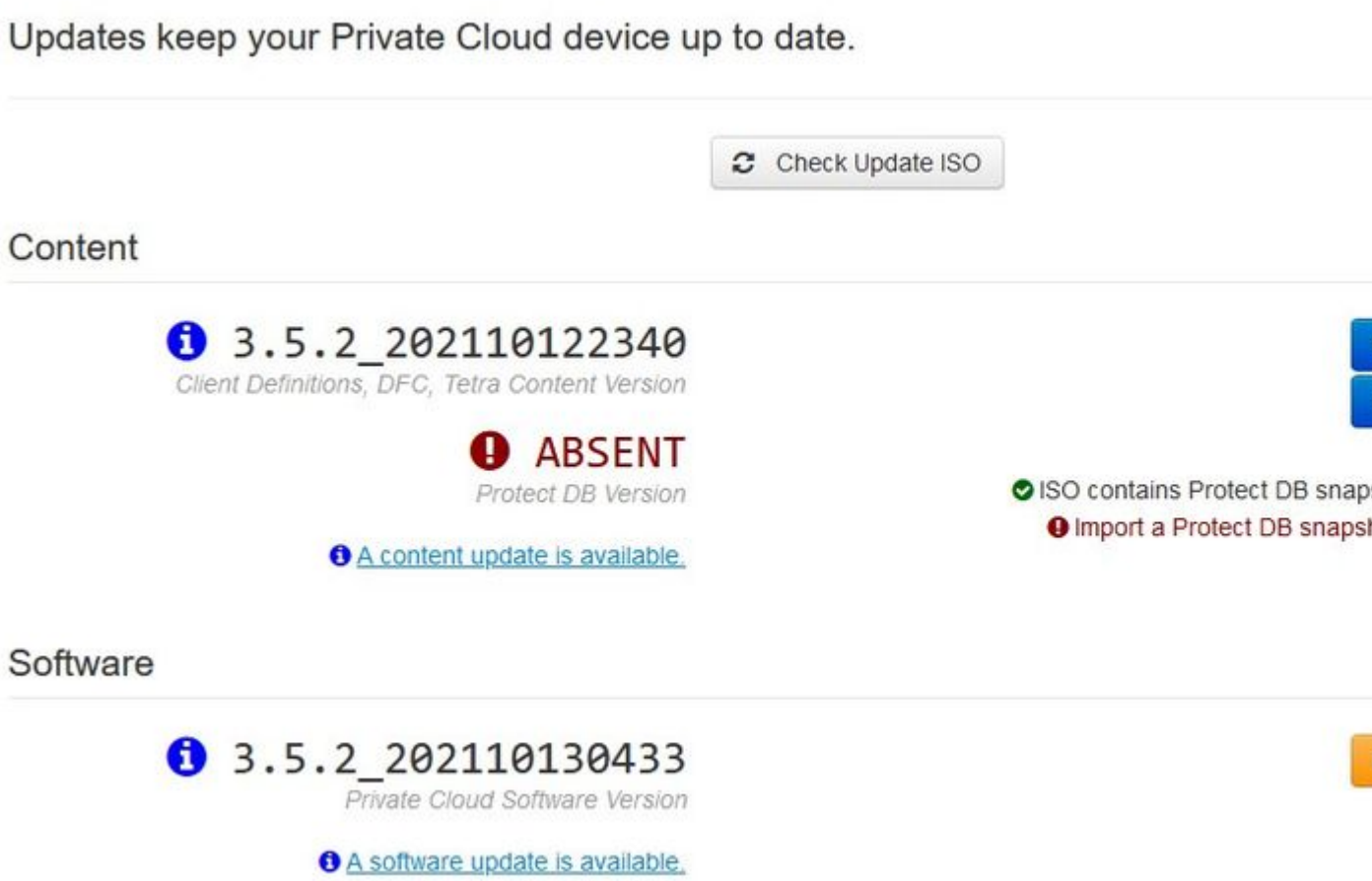


â€ƒ

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.

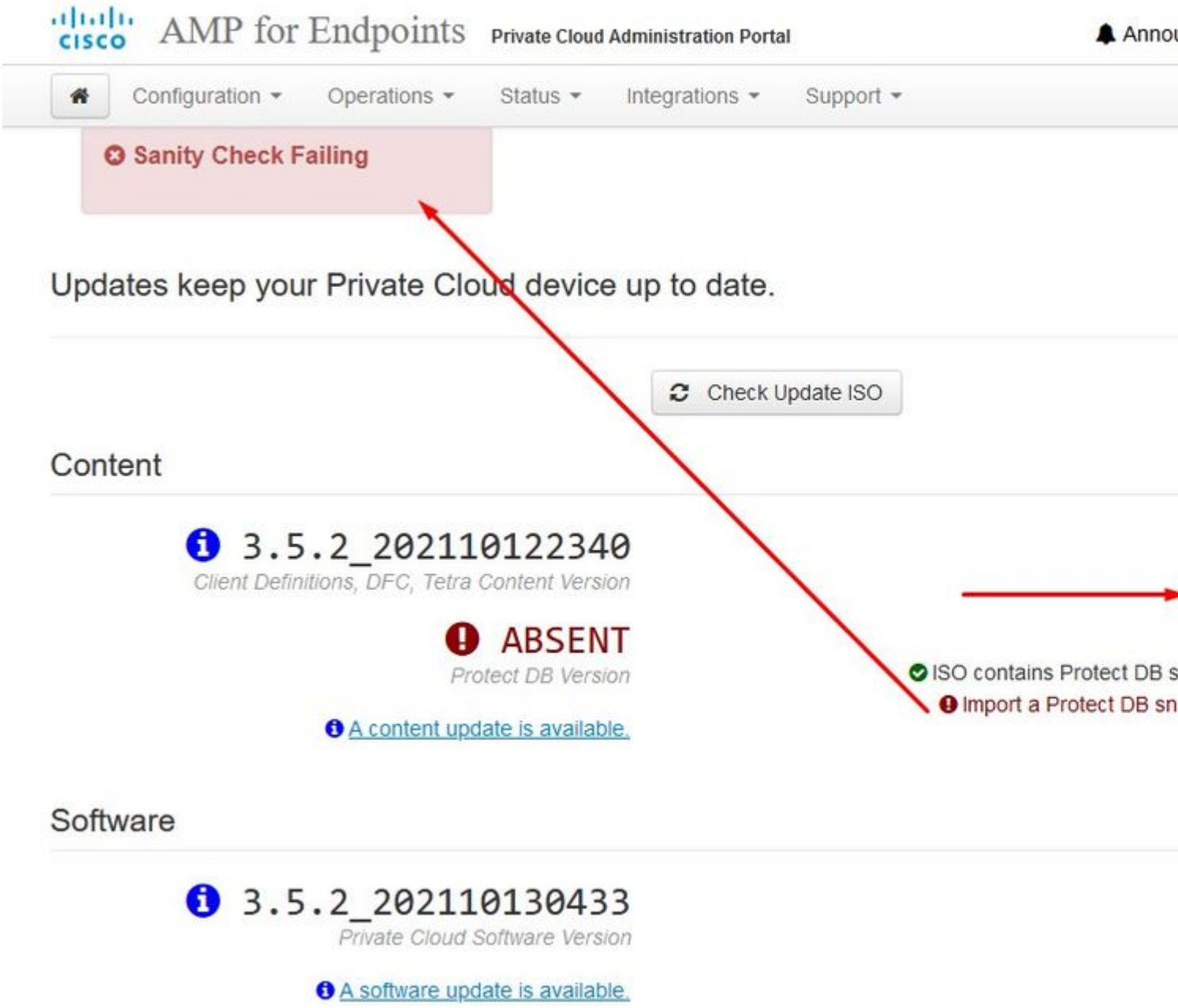

AMP for Endpoints
Private Cloud Administration Portal
Announc
Configuration
Operations
Status
Integrations
Support
Maintenance Mode
Sanity Check Failing
Disabling T
Mount an Update ISO
ISO Configuration
Mount Type
ISO
ISO
NFS4
NFS3
Mount Status
No ISO mounted


AMP for Endpoints
Private Cloud Administration Portal
Configuration
Operations
Status
Integrations
Support
Sanity Check Failing
Disabling TLS 1.0/1.1
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



â€ƒ

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


AMP for Endpoints
Private Cloud Administration Portal
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€ƒ

Protect DB importing

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

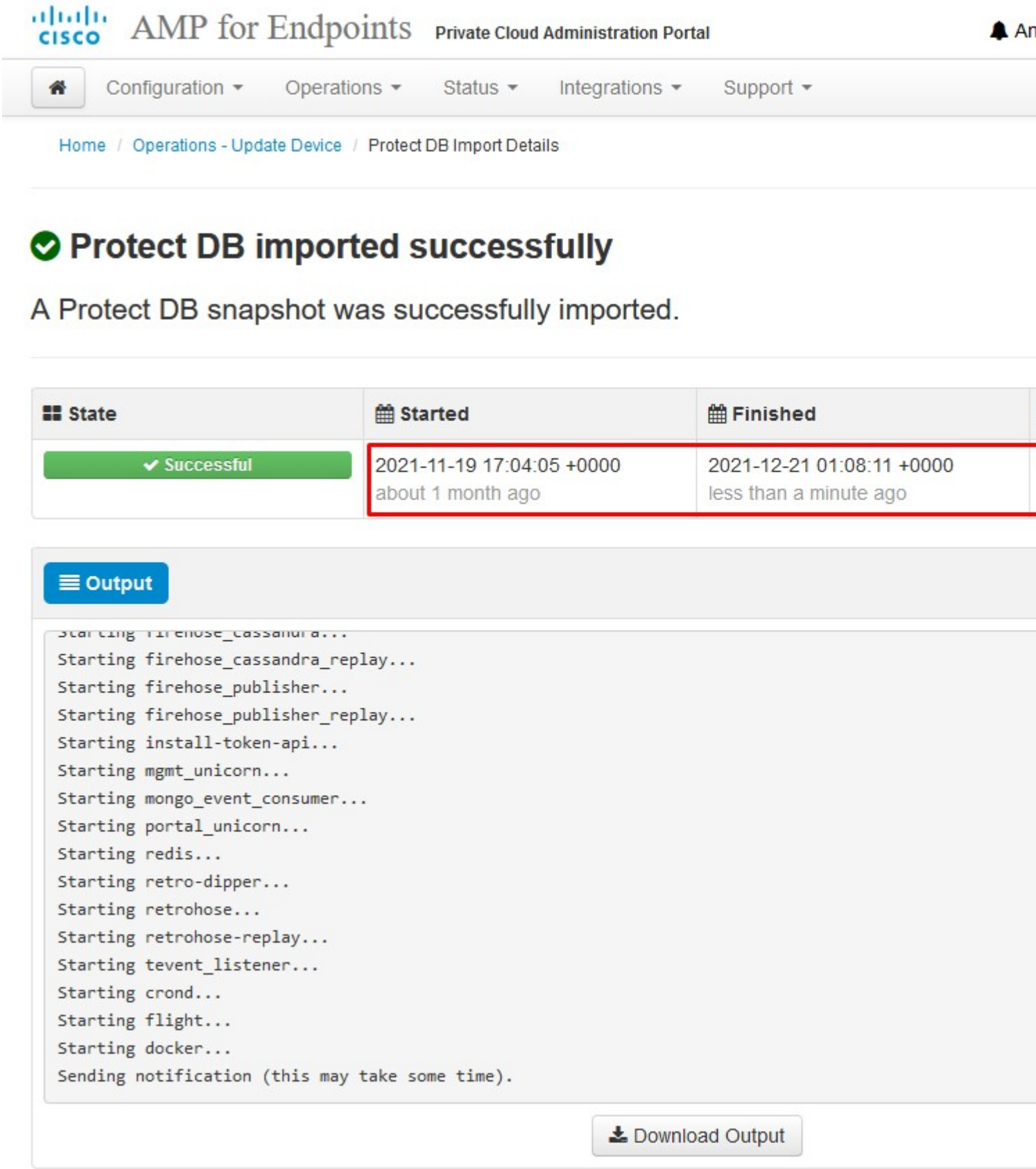
State	Started	Finished
Running	2021-11-19 17:04:05 +0000 about 20 hours ago	Please wait...

Output

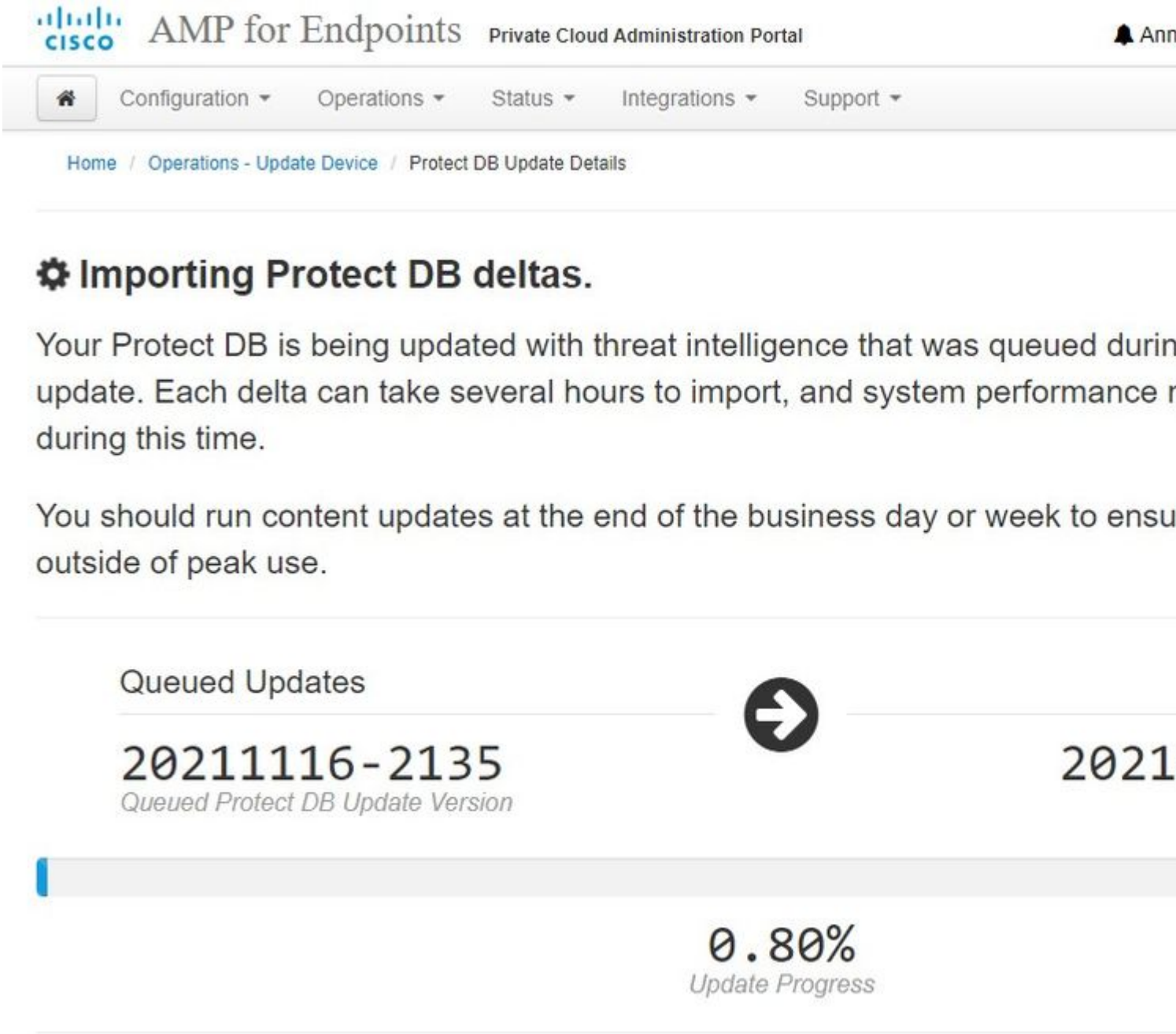
```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   99% [====================]
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00  100% [====================]
Snapshot Version 3
Going to drop disposition tables.
Dropping detections table.
Dropping binaries table.
Dropping binaries_detections table.
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€ƒ

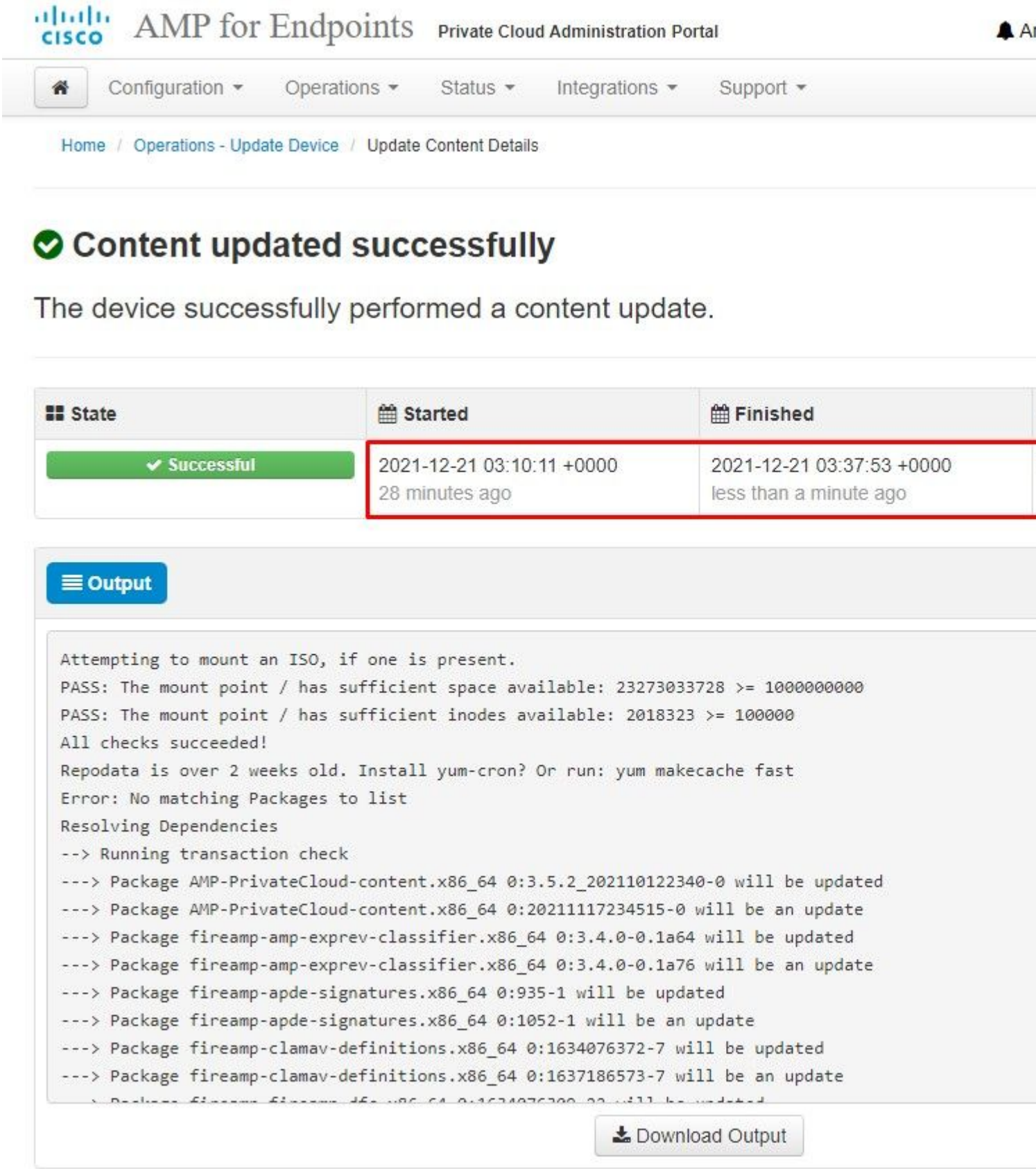


Nächstes Update automatisch starten



â€ƒ

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.



â€ƒ
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

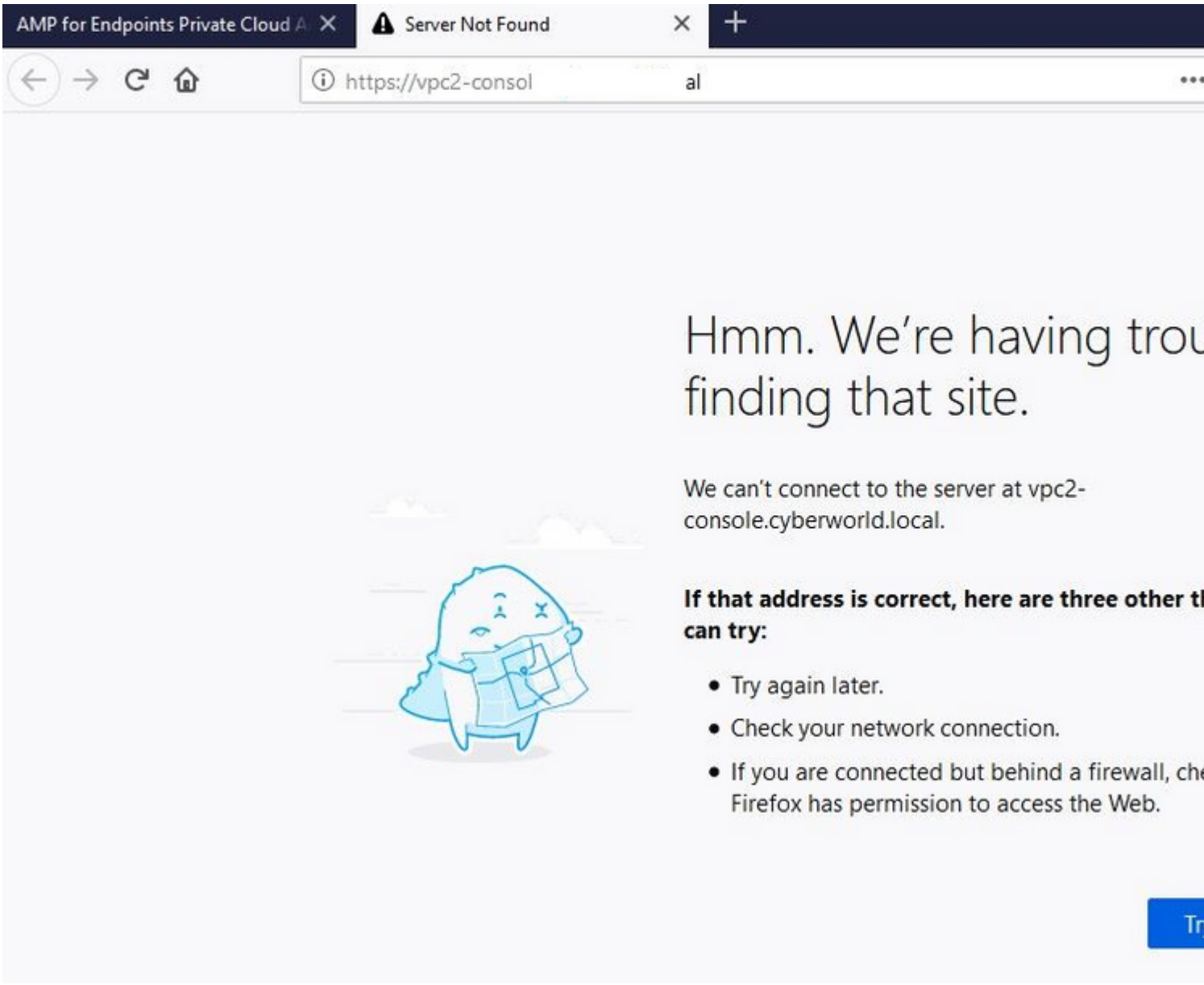
â€ƒ

ï¸½ ï¸½ NUR ï¸½ ï¸½

Grundlegende Fehlerbehebung

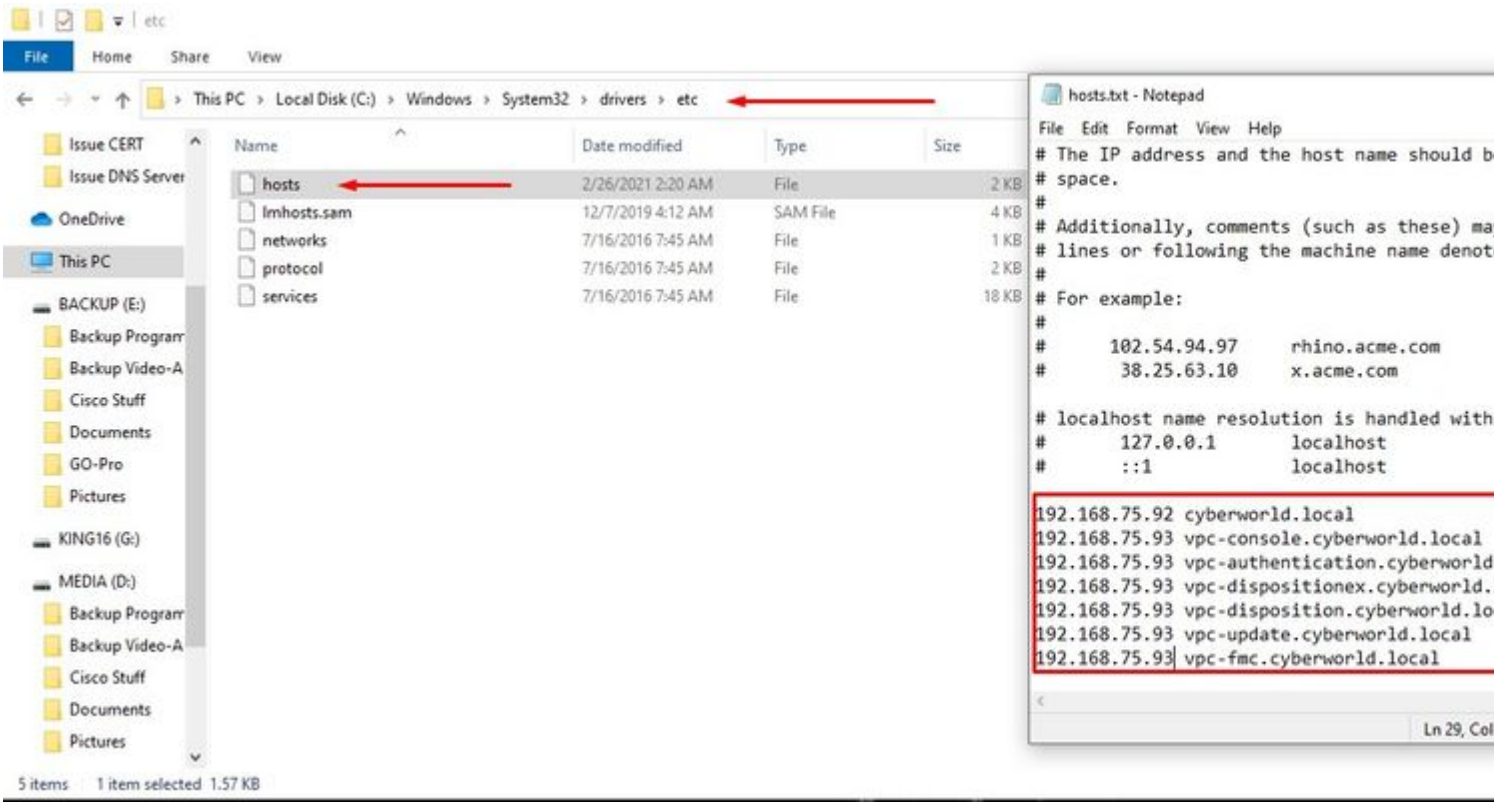
Problem #1 - FQDN und DNS-Server

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.

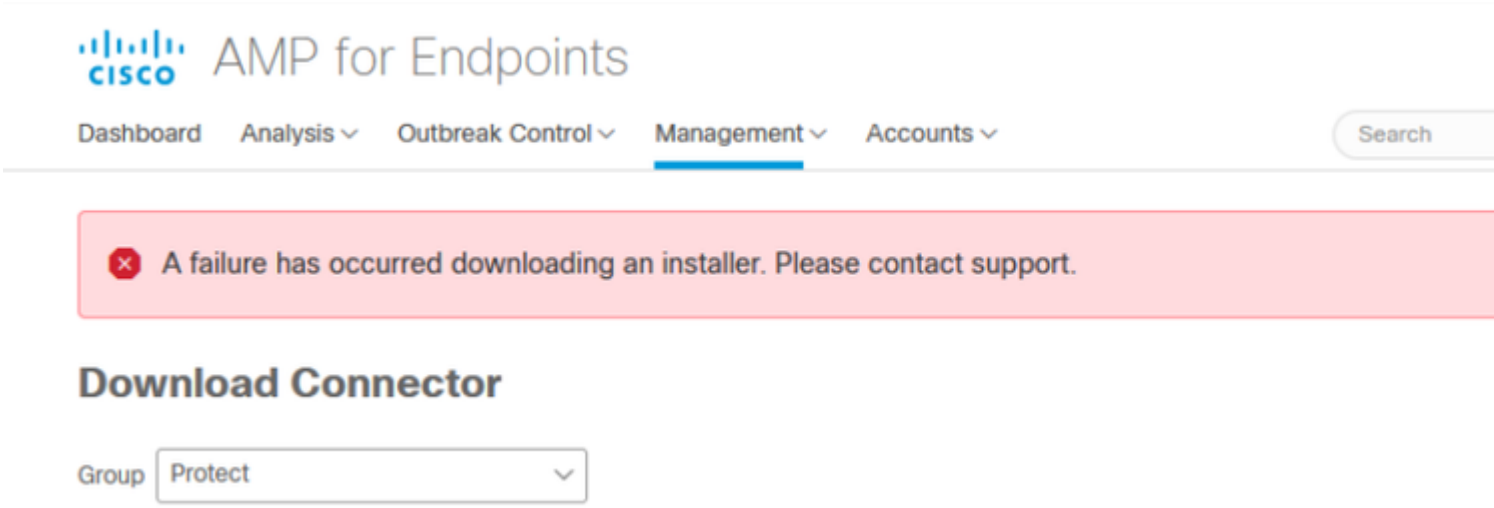


â€ƒ

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



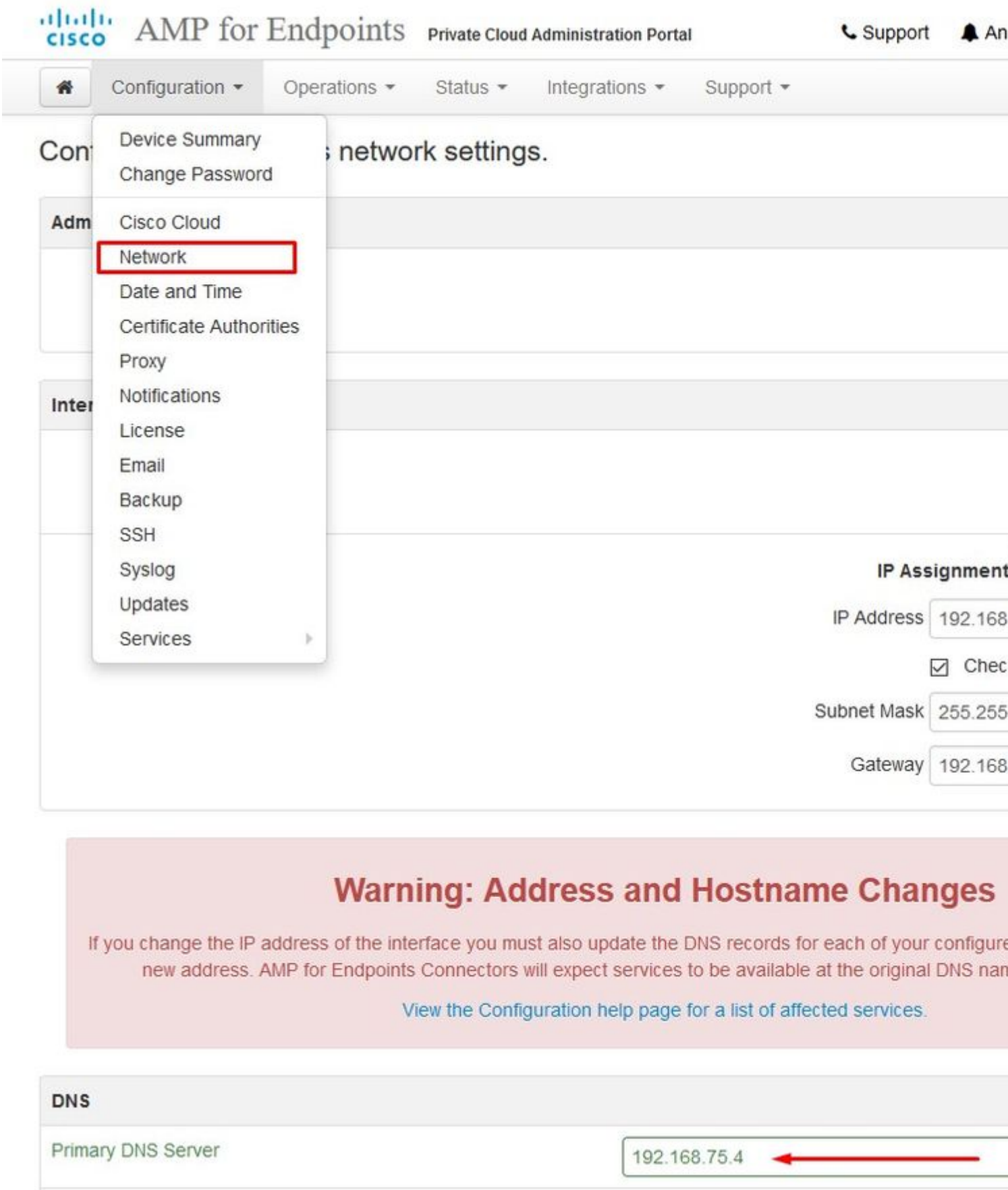
Sie erhalten diese Fehlermeldung, wenn Sie versuchen, das Installationsprogramm für Secure Endpoint Connector herunterzuladen.

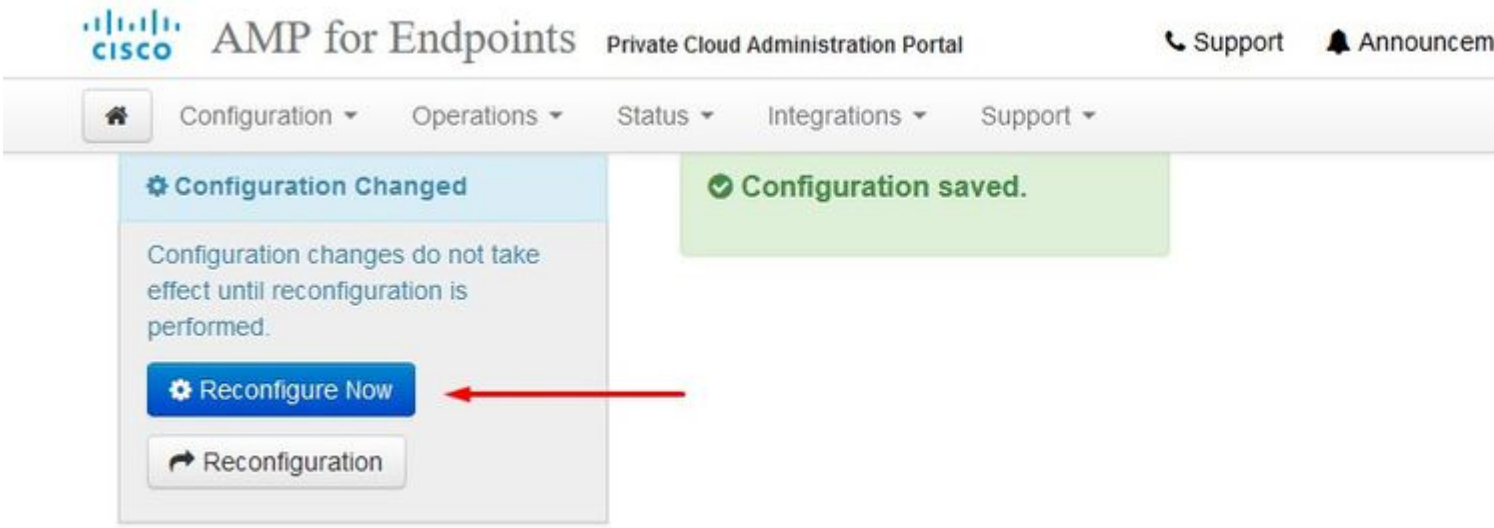


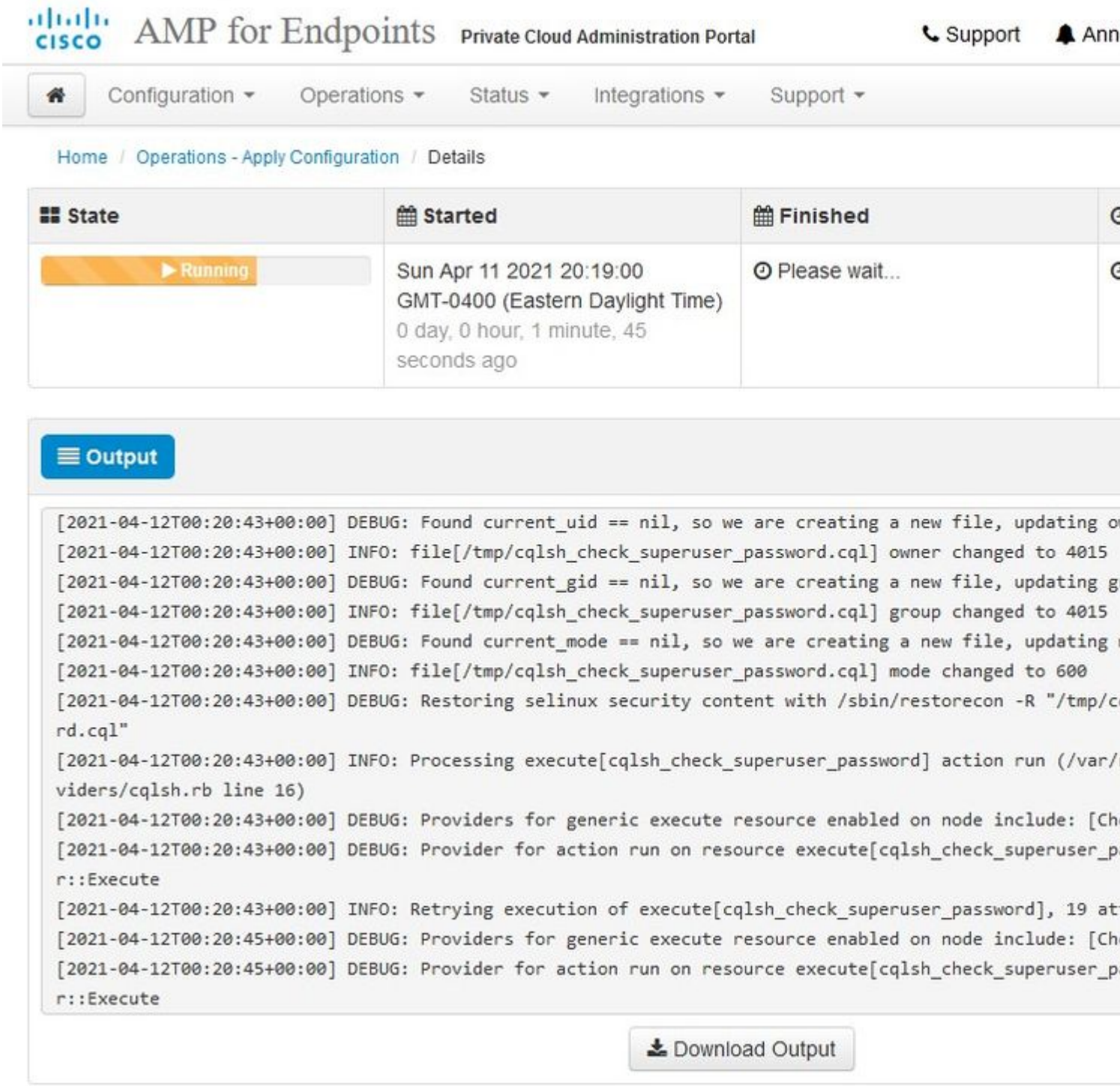
Nach einigen Fehlerbehebungen war die einzige richtige Lösung, den DNS-Server einzurichten.

```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +00

================================================================================

Server:         8.8.8.x
Address:        8.8.8.x#53

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

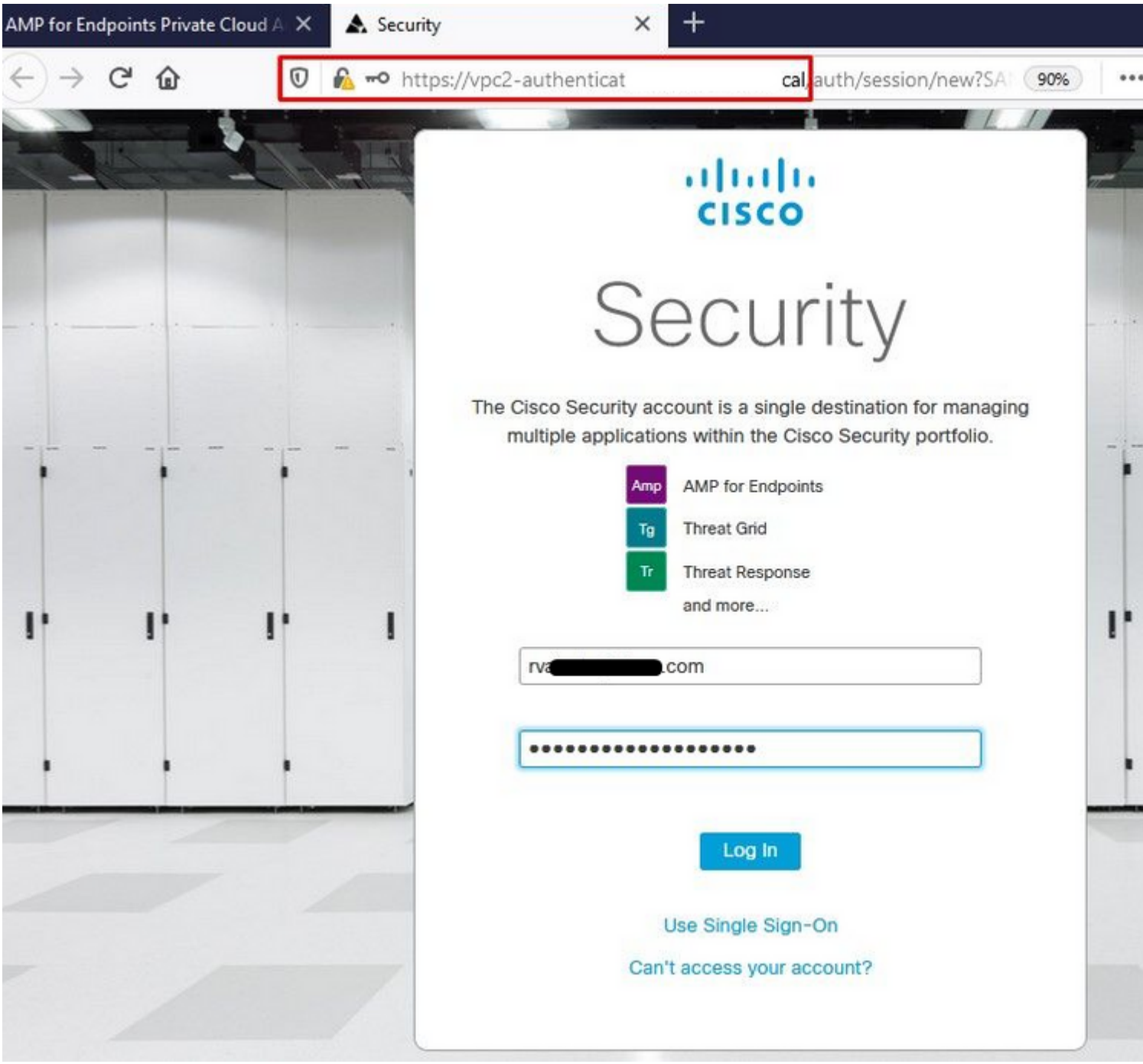
Sobald Sie alle FQDNs in Ihrem DNS-Server aufzeichnen und den Eintrag in Virtual Private Cloud von Public DNS auf Ihren DNS-Server ändern, läuft alles wie es sollte.




AMP for Endpoints
Private Cloud Administration Portal
Support
Announcem
Configuration
Operations
Status
Integrations
Support
Configuration Changed
Configuration changes do not take effect until reconfiguration is performed.
Reconfigure Now
Reconfiguration
Configuration saved.



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

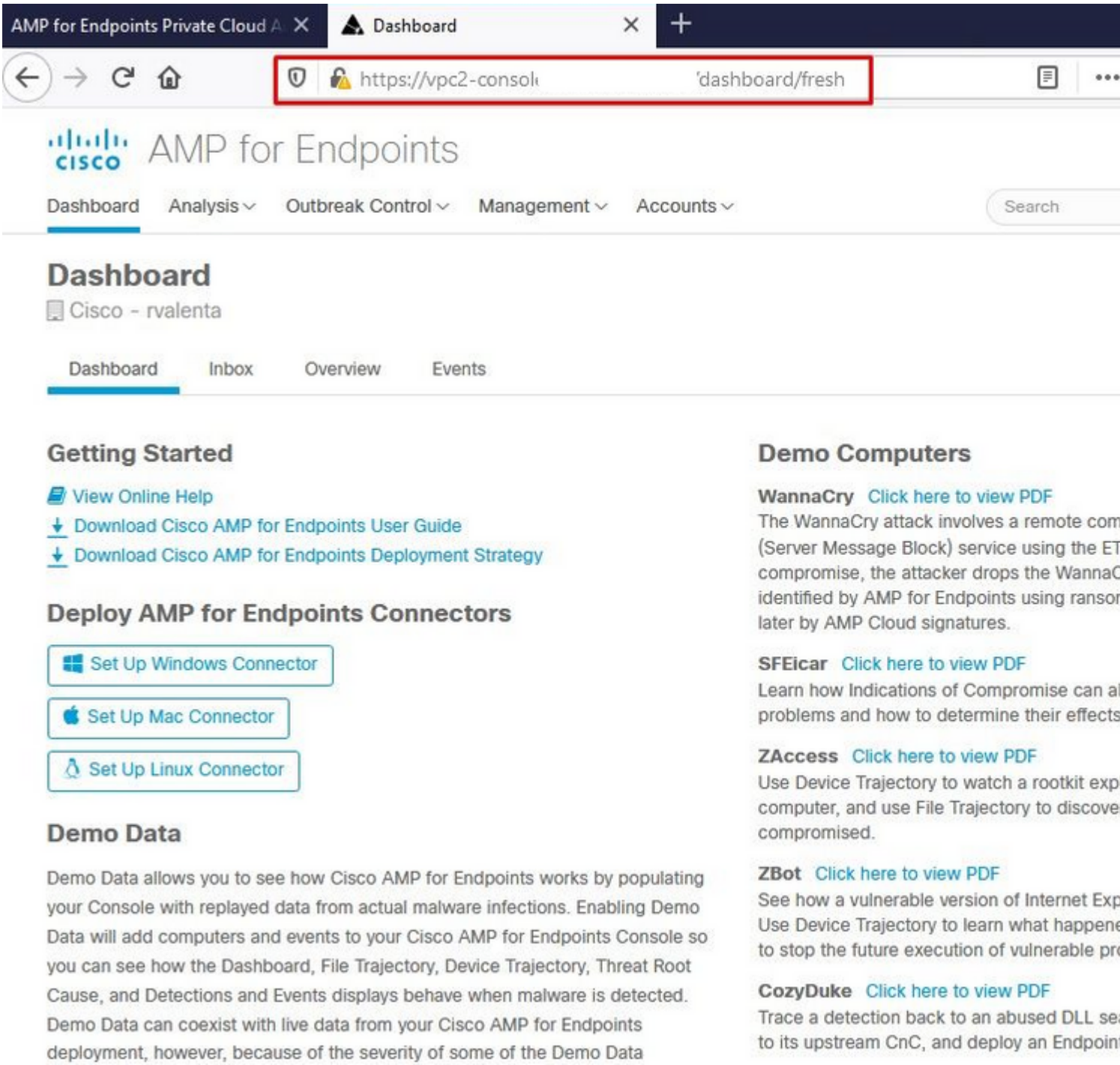


â€ƒ

â€ƒ

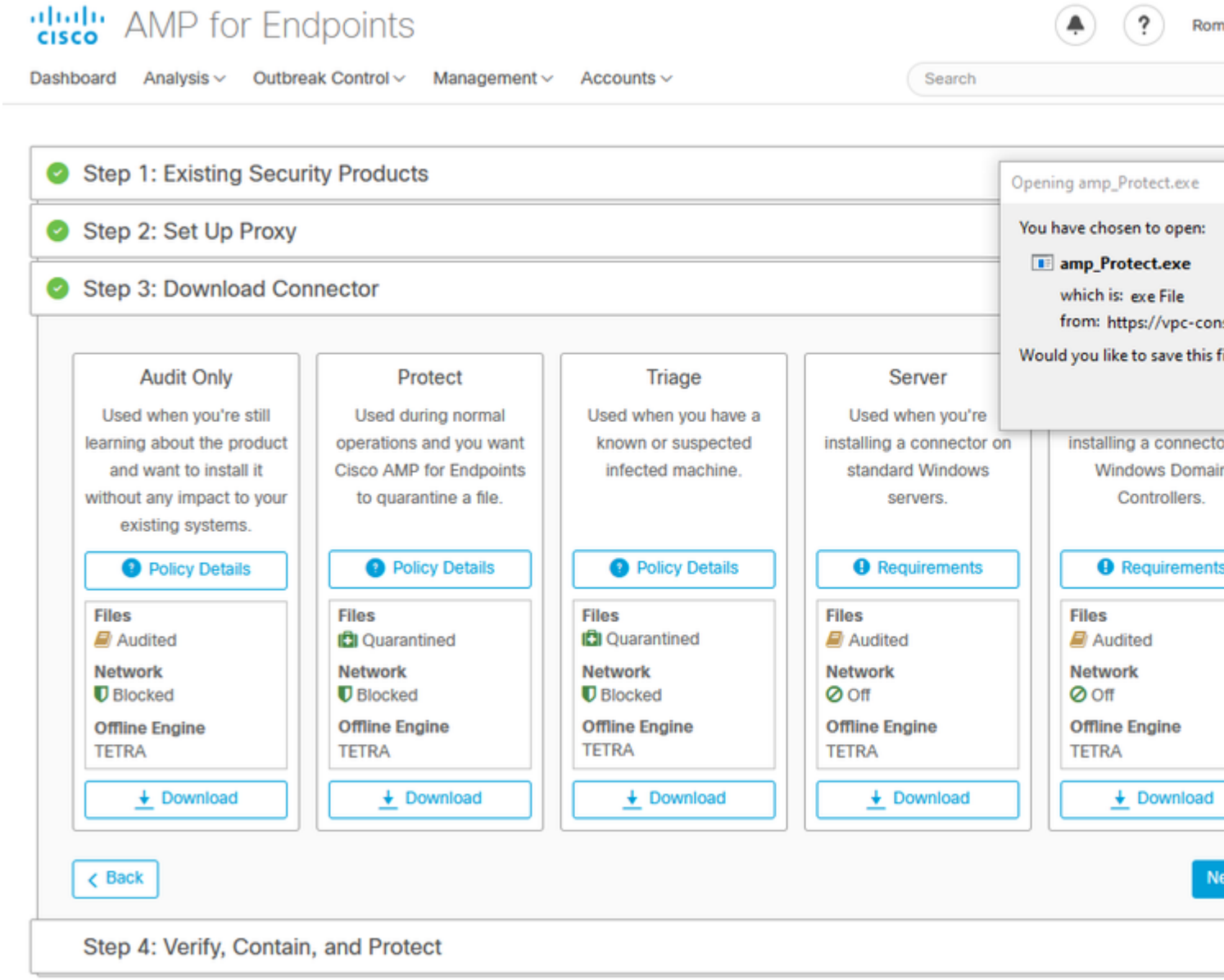
Sie erhalten den Assistenten für Richtlinien für sichere Endgeräte für Ihre Umgebung. Es führt Sie durch die Auswahl der Antiviren-Produkte, die Sie ggf. verwenden, sowie durch die Proxy-Server und die Richtlinien, die Sie bereitstellen möchten. Wählen Sie eine entsprechende Taste für die Einrichtung...,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



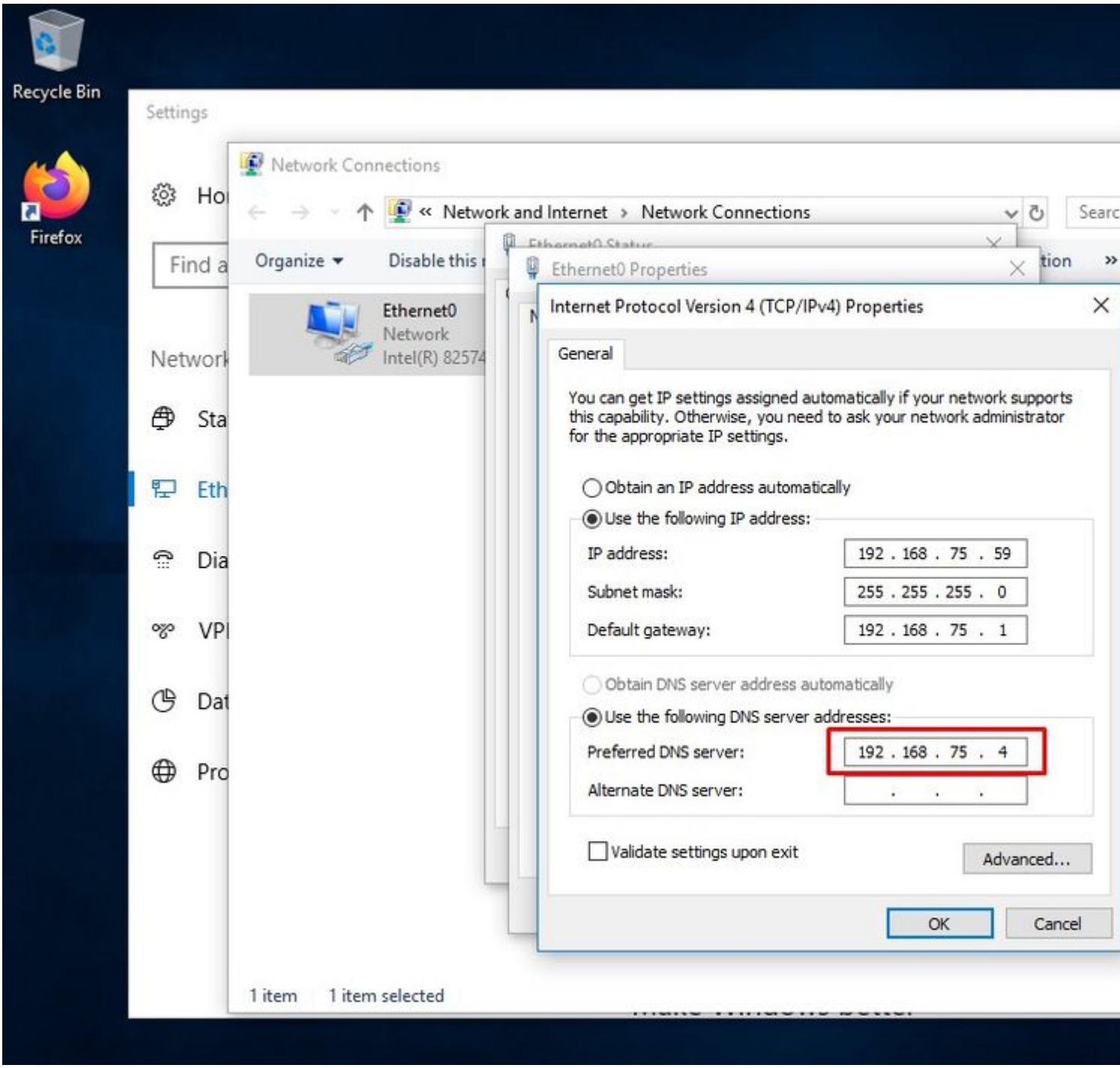
â€ƒ

Connector herunterladen.

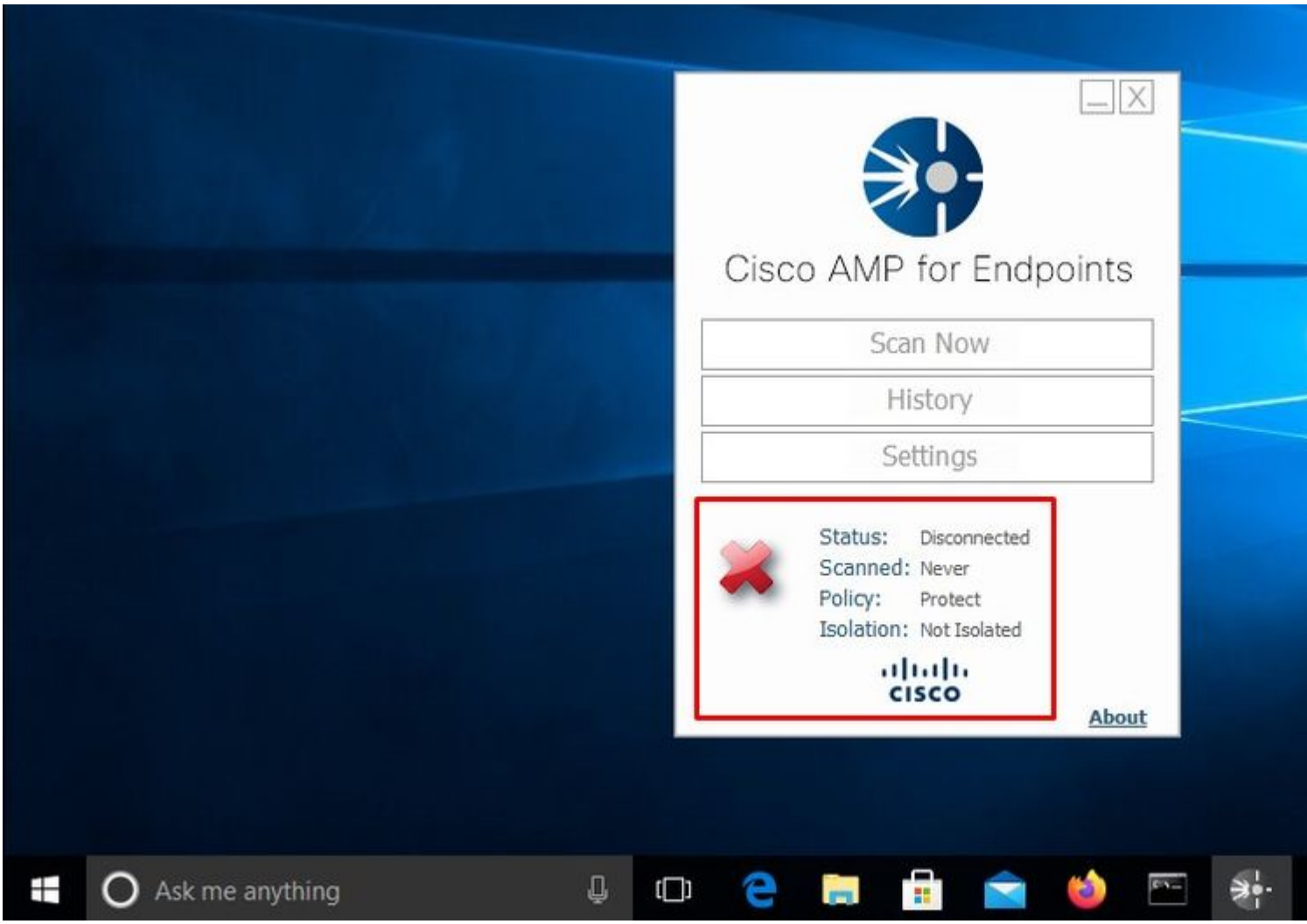


Problem #2 - Problem mit Stammzertifizierungsstelle

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



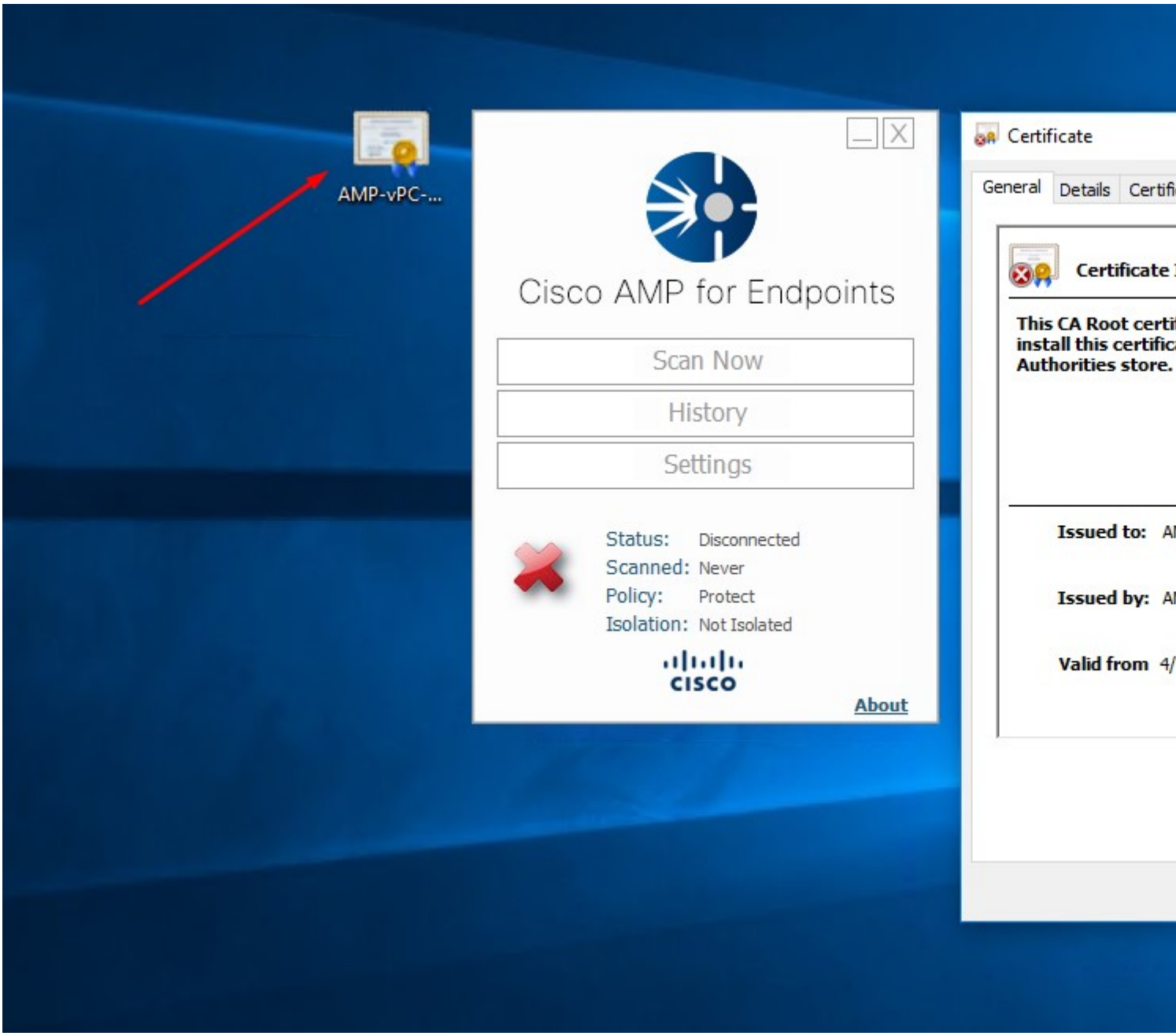
Nach der Installation des Connectors kann Secure Endpoint als "Disconnected" (Verbindung getrennt) angezeigt werden. Führen Sie das Diagnosepaket aus, und durchsuchen Sie die Protokolle. Sie können das Problem ermitteln.

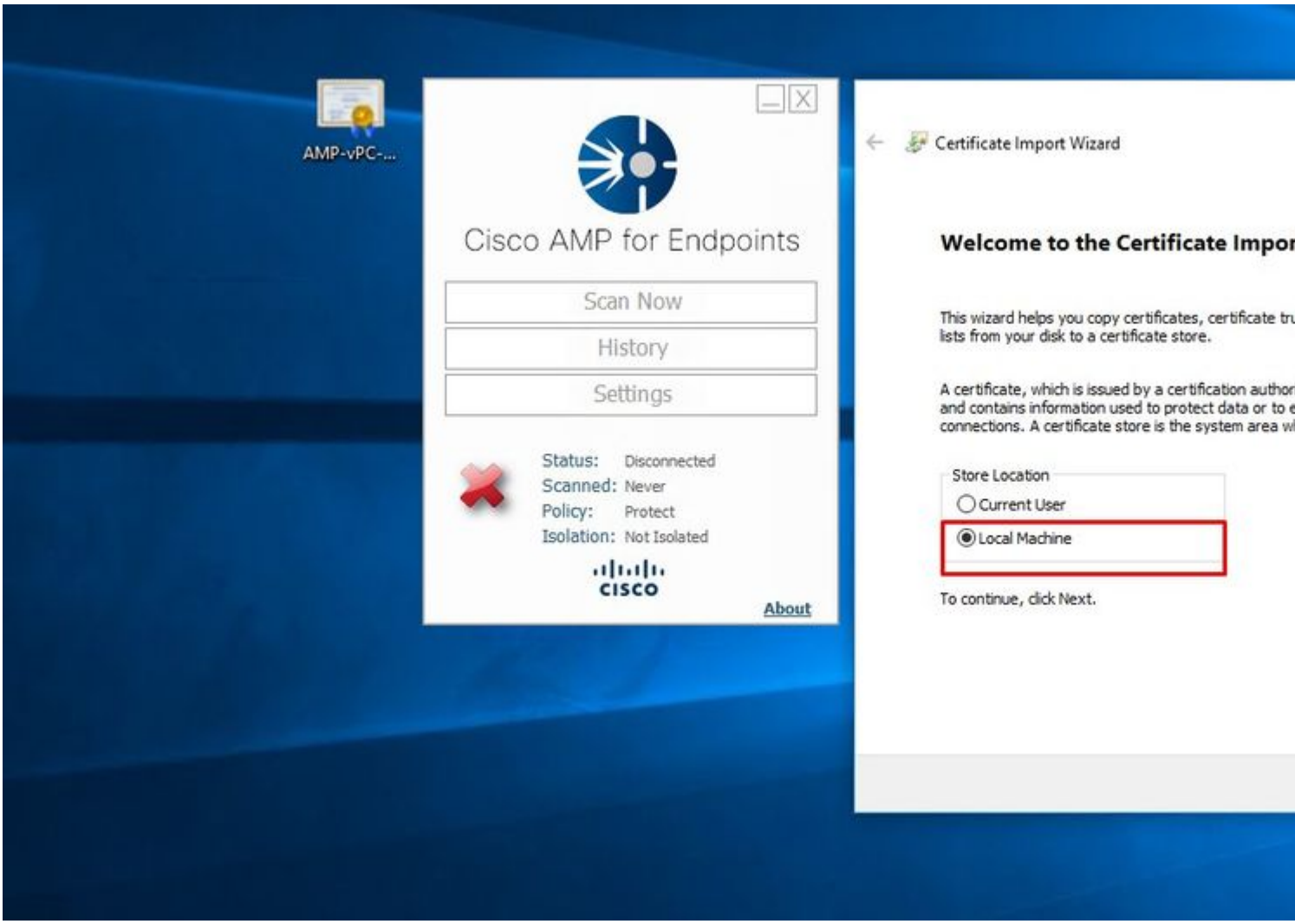


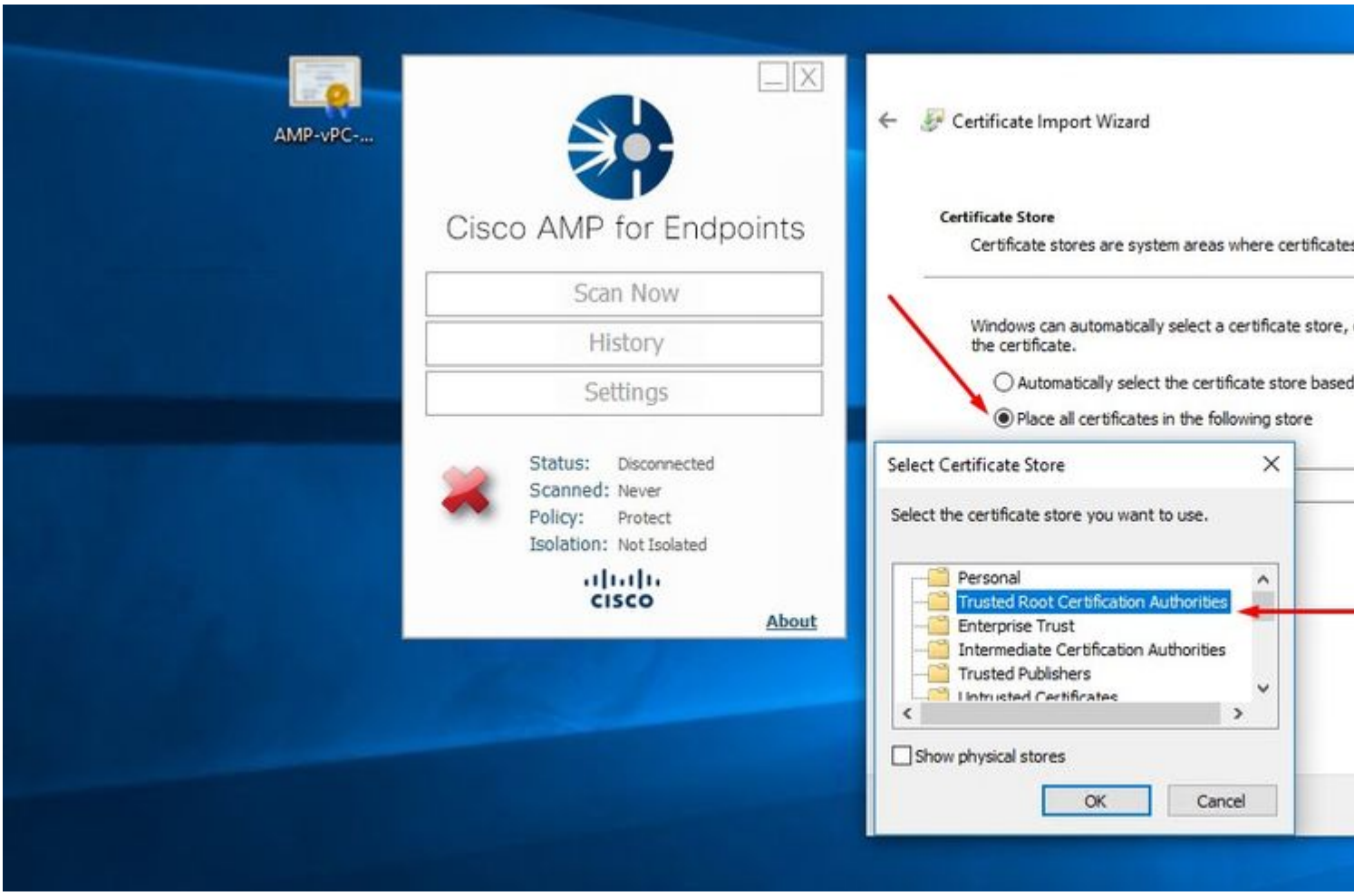
Basierend auf dieser Ausgabe aus dem Diagnosepaket wird der Fehler der Stammzertifizierungsstelle angezeigt.

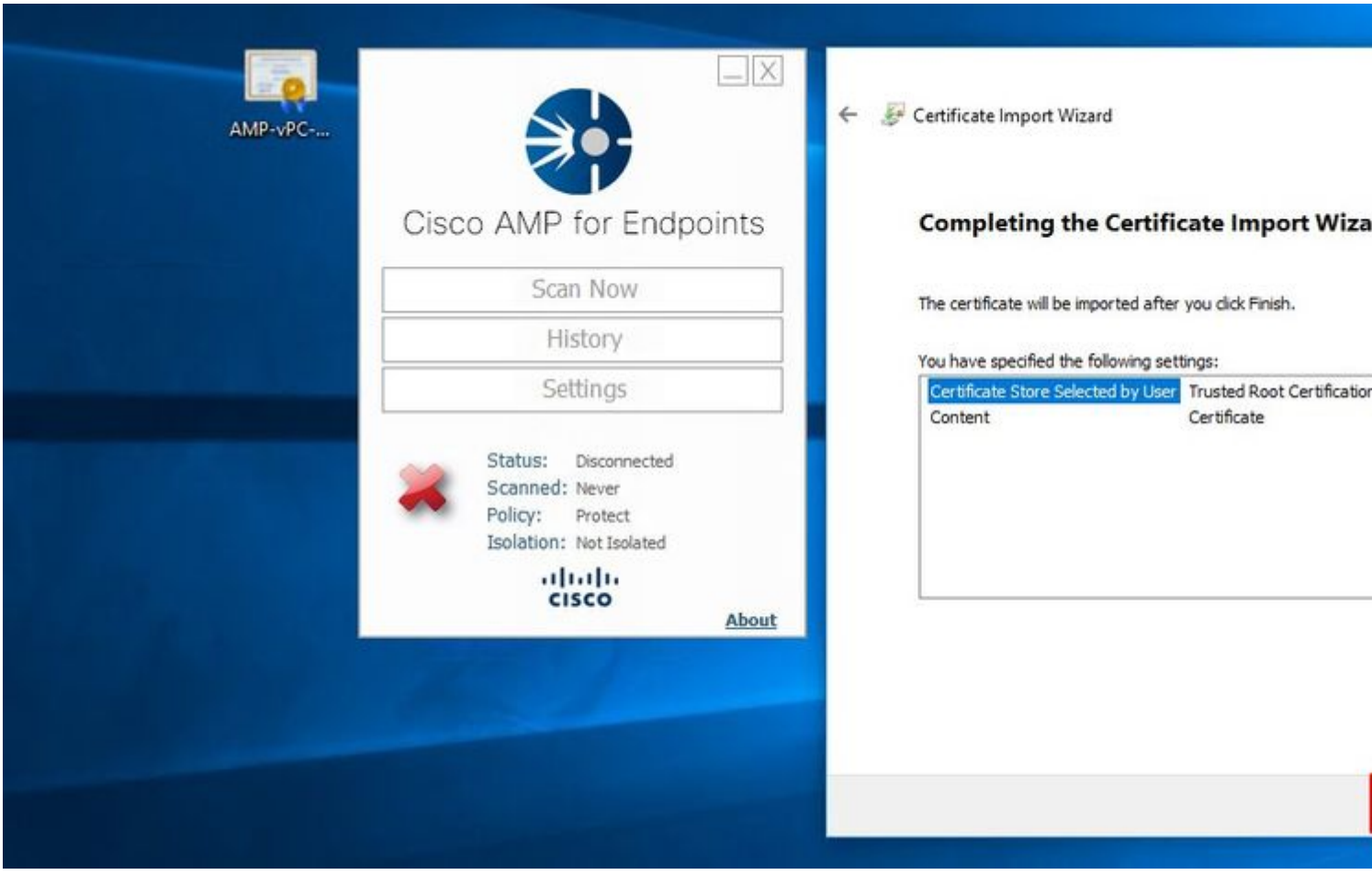
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworld

(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
```

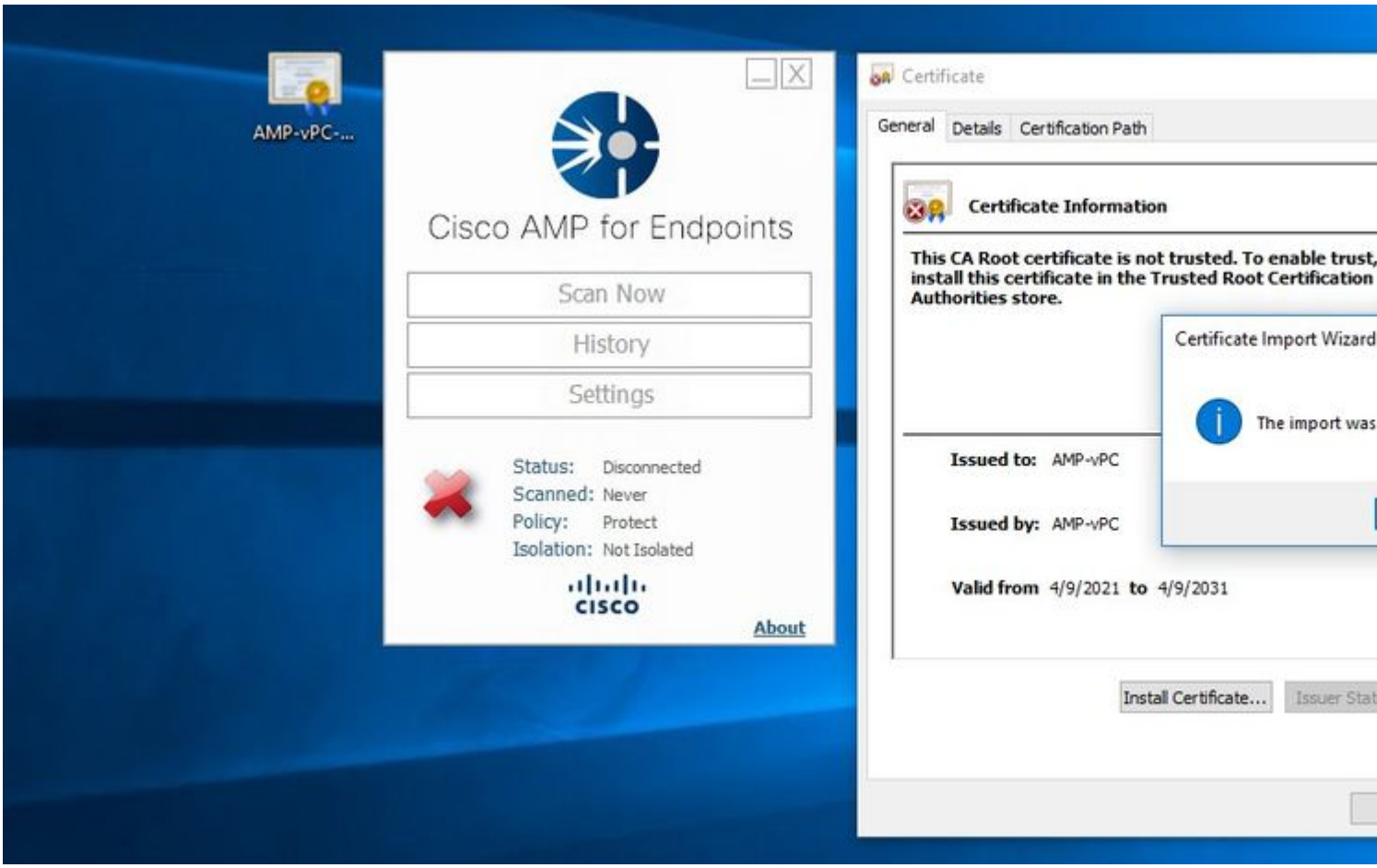
Nachdem Sie die Stammzertifizierungsstelle in den Speicher der vertrauenswürdigen Stammzertifizierungsstelle hochgeladen haben, starten Sie den Dienst für sichere Endgeräte neu. Alles beginnt wie erwartet zu funktionieren.

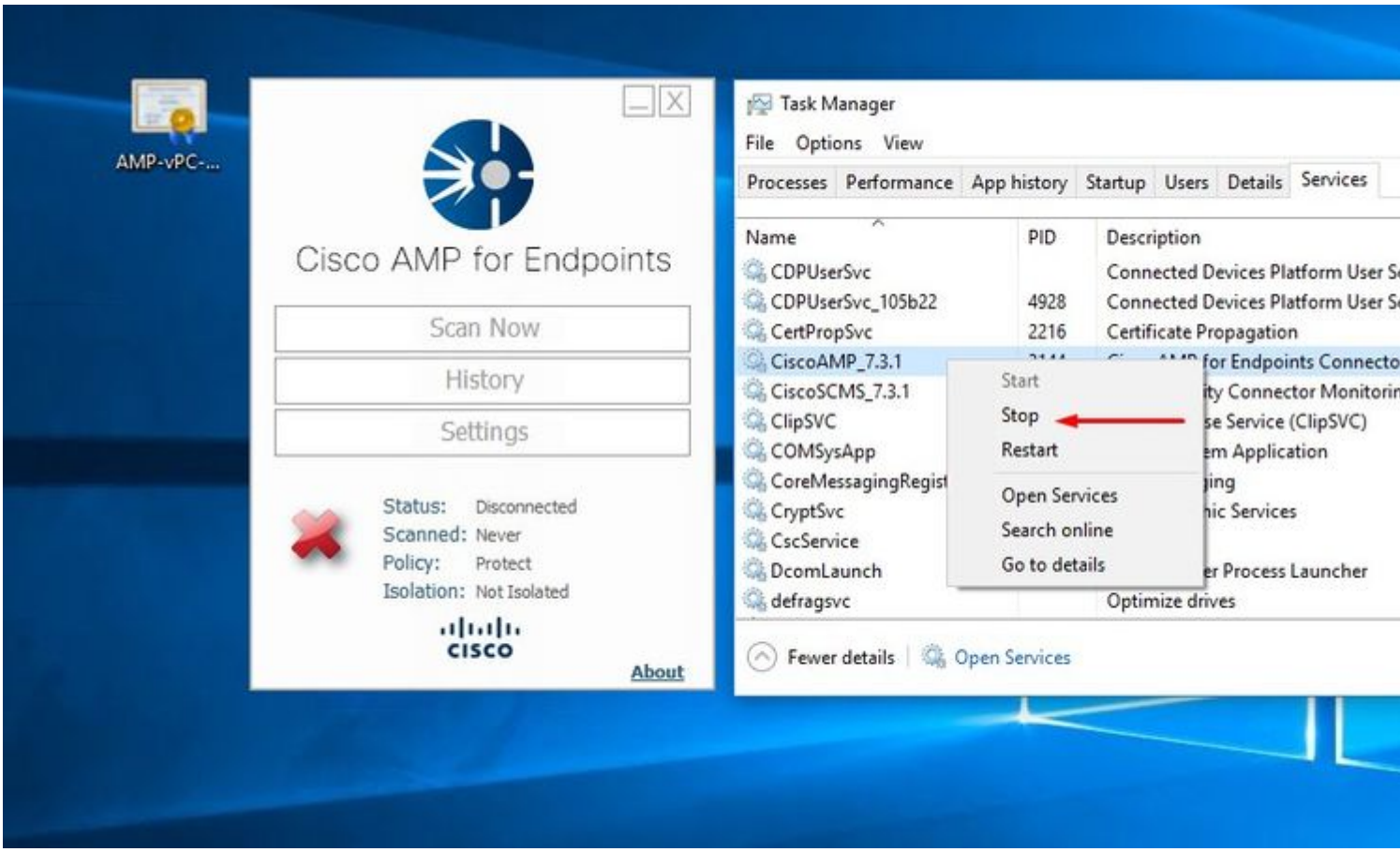

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate
General
Details
Certifi
Certificate
This CA Root certi
install this certific
Authorities store.
Issued to: A
Issued by: A
Valid from 4/


AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Welcome to the Certificate Impor
This wizard helps you copy certificates, certificate tru
lists from your disk to a certificate store.
A certificate, which is issued by a certification author
and contains information used to protect data or to e
connections. A certificate store is the system area wh
Store Location
Current User
Local Machine
To continue, click Next.

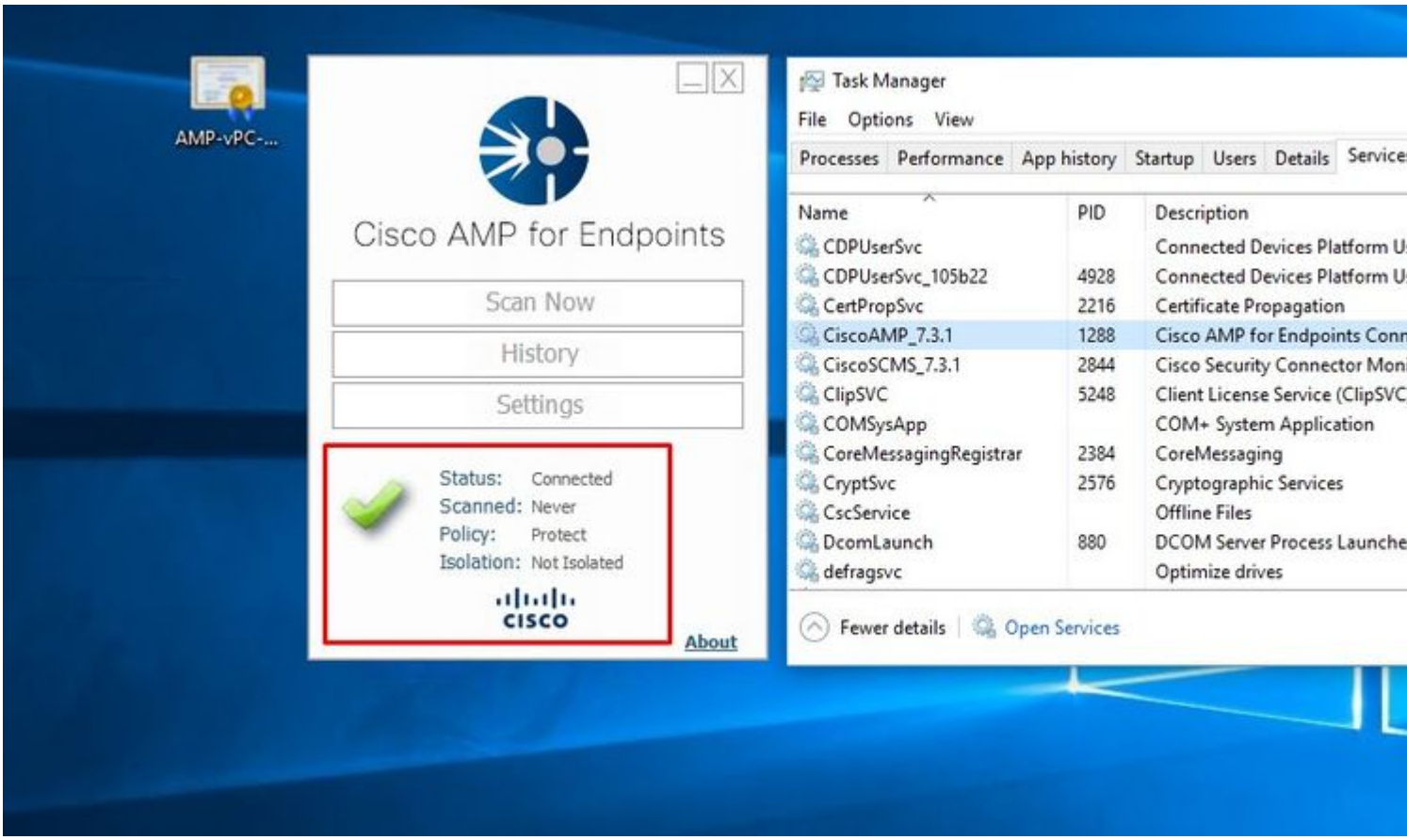

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates
Windows can automatically select a certificate store,
the certificate.
Automatically select the certificate store based
Place all certificates in the following store
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Show physical stores
OK
Cancel

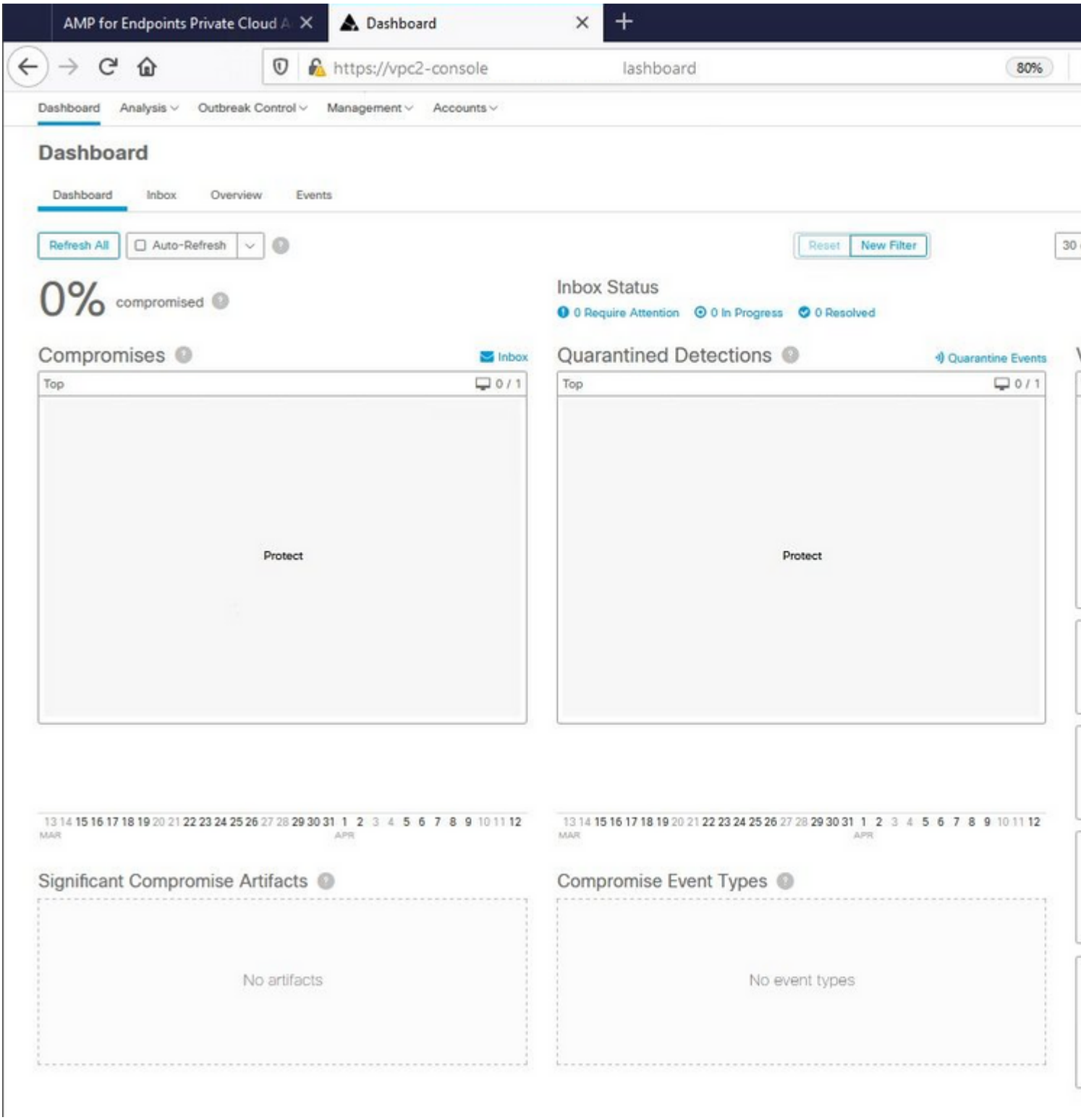

AMP-vPC-...
Cisco AMP for Endpoints
Scan Now
History
Settings
Status: Disconnected
Scanned: Never
Policy: Protect
Isolation: Not Isolated
cisco
About
Certificate Import Wizard
Completing the Certificate Import Wiza
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certificatio
Content
Certificate





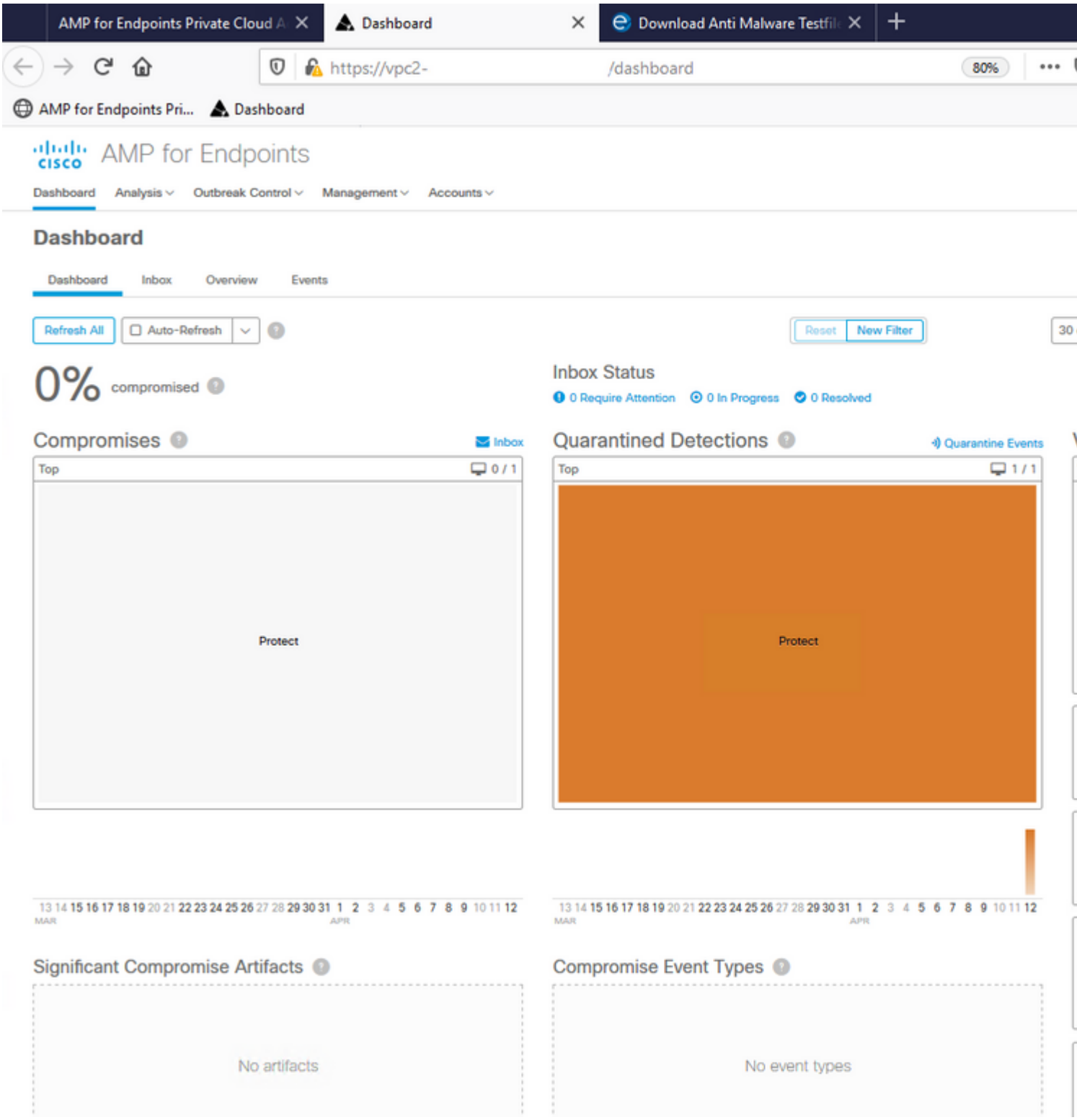
Sobald das Bounce des Secure Endpoint-Service-Connectors abgeschlossen ist, können Sie wie erwartet online gehen.


AMP-vPC-...
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 Service
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



â€ƒ

Bösartige Aktivitäten getestet


AMP for Endpoints Private Cloud A
Dashboard
Download Anti Malware Testfil
https://vpc2-
/dashboard
80%
AMP for Endpoints Pri...
Dashboard
AMP for Endpoints
Dashboard
Analysis
Outbreak Control
Management
Accounts
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
Top
0 / 1
Protect
Quarantined Detections
Quarantine Events
Top
1 / 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€ƒ

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.