Install and Configure of Secure Endpoint Virtual Private Cloud

Contents

Introduction

Prerequisites

VPC Deployment

- VM Installation
- Initial Admin Interface Setup
- Initial Configuration of the vPC via web GUI
- Configuration
- Services
- AirGap Update Package
  - Problem #1 - Exhausted room in Data Store
  - Problem #2 - Old Update

Basic Troubleshooting

- Problem #1 - FQDN and DNS Server
- Problem #2 - Issue with Root CA

Introduction

This document describes and focus on how to successfully deploy Virtual Private Cloud (VPC) on servers in ESXi environment. For other documents such as Quick Start Guide, Deployment Strategy, Entitlement Guide, Console and Administrator User Guide please visit this site Documentation

Contributed by Roman Valenta, Cisco TAC Engineers.

Prerequisites

Requirements:

VMware ESXi 5 or later

- Cloud-proxy mode (only): 128 GB RAM, 8 CPU cores (2 CPUs with 4 cores each recommended), 1 TB minimum free disk space on VMware datastore
- Type of drives: SSD required for air gap mode and recommended for proxy
- RAID Type: One RAID 10 group (striped mirror)
- Minimum VMware datastore size: 2 TB
- Minimum datastore random reads for the RAID 10 group (4K): 60K IOPS
- Minimum datastore random writes for the RAID 10 group (4K): 30K IOPS

Cisco recommends that you have knowledge of this topic:

- Basic knowledge how to work with certificates.
- Basic knowledge on how to setup DNS under DNS server (Windows or Linux)
- Installation an Open Virtual Appliance (OVA) Template in the VMWare ESXi

Used in this LAB:

VMware ESX 6.5

- Cloud-proxy mode (only): 48 GB RAM, 8 CPU cores (2 CPUs with 4 cores each recommended), 1 TB minimum free disk space on VMware datastore
- Type of drives: SATA
- RAID Type: One RAID 1
- Minimum VMware datastore size: 1 TB
- MobaXterm 20.2 (Multi-Terminal Program similar to PuTTY)
- Cygwin64 (Used to download AirGap Update)

Additionally

- Certificate that you create either with openSSL or any other supported methods.
- DNS Server (Linux or Windows) In my lab I used Windows Server 2016 and CentOS-8
- Windows VM for our test endpoint
- License

If your memory is bellow 48GB RAM on version 3.2+ VPC become unusable.

Note: The Private Cloud OVA creates the drive partitions so there is no need to specify them in VMWare. server which resolves the clean interface hostname.

Refer to the VPC Appliance Data Sheet for more information about version-specific hardware requirements.

Note:The information in this document was created from the devices in a **specific lab environment a**nd its only intend to give you a guidance through the deployment which might vary depending on the version that is being deployed**.** All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

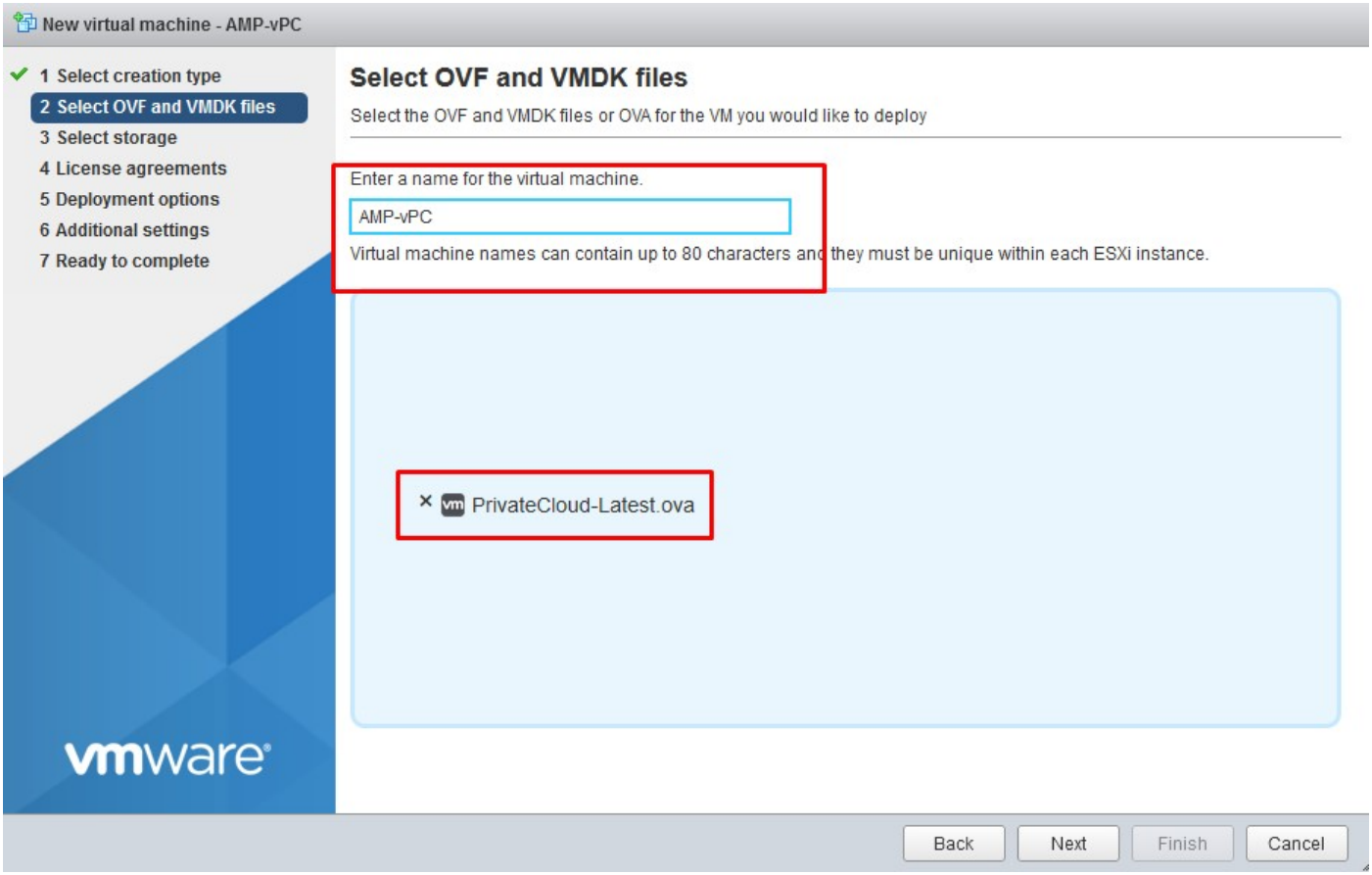
VPC Deployment

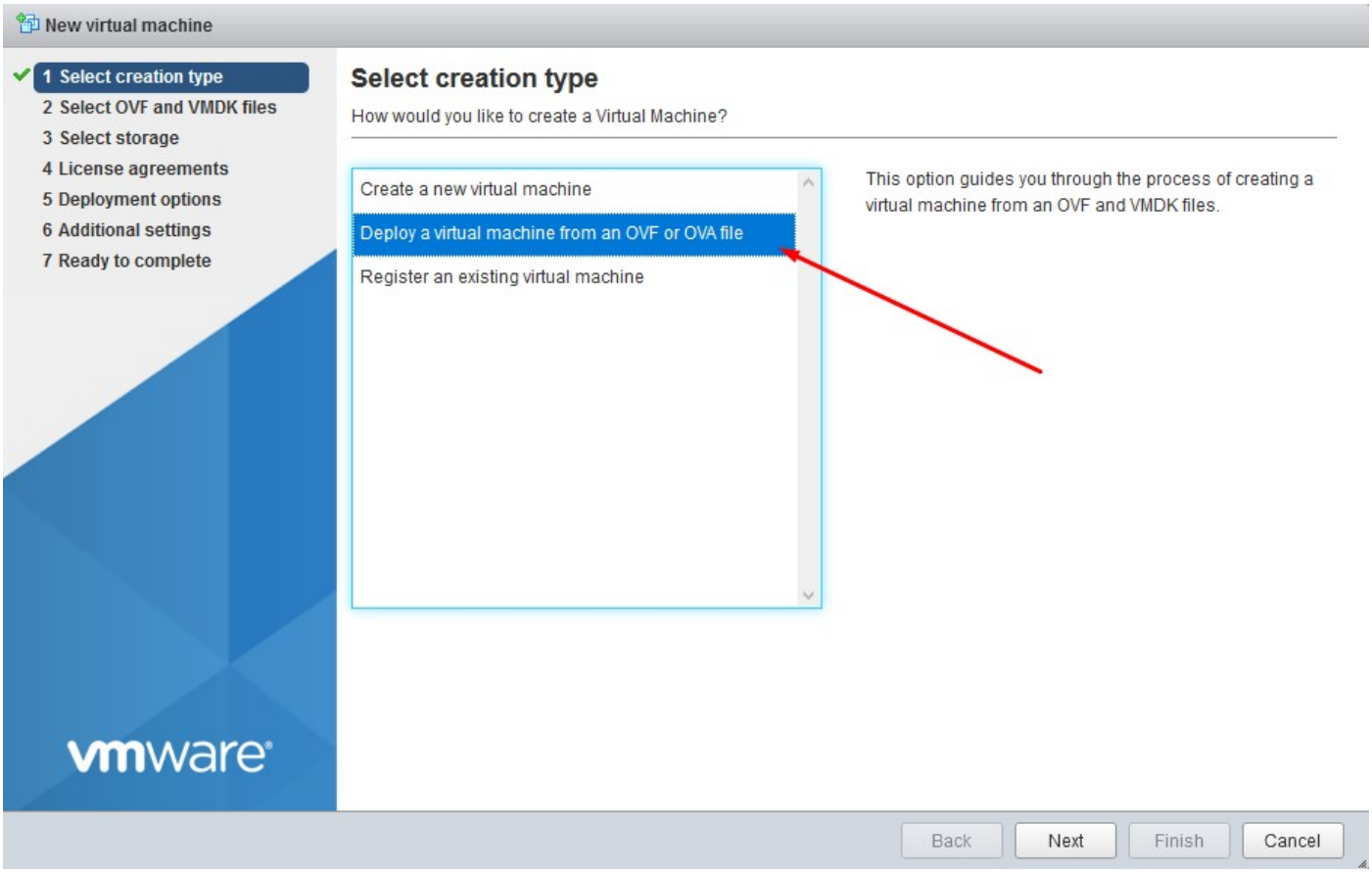
Select the URL provided in the eDelivery or entitlement email. Download the OVA file and proceed with install

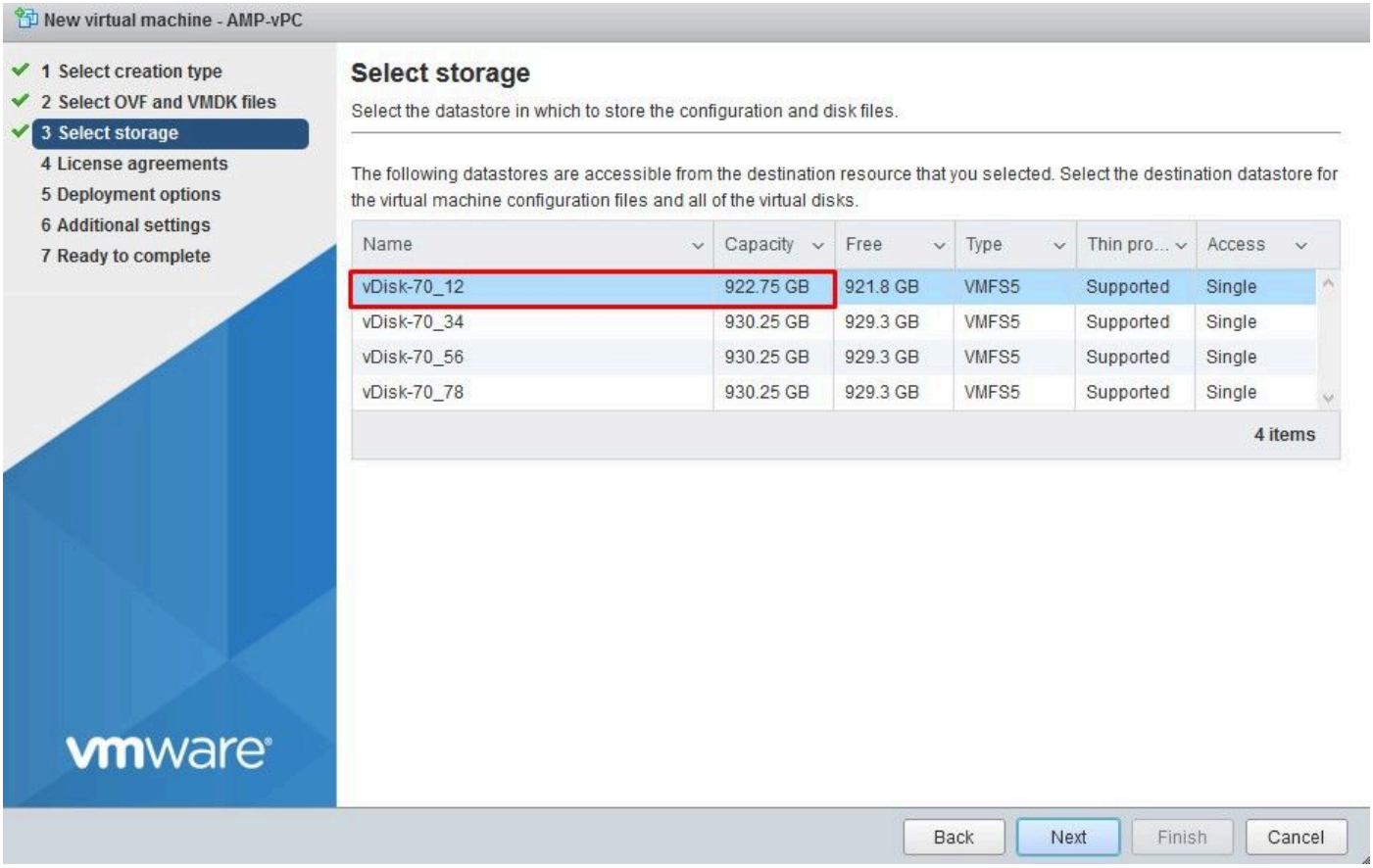
VM Installation

Step1:

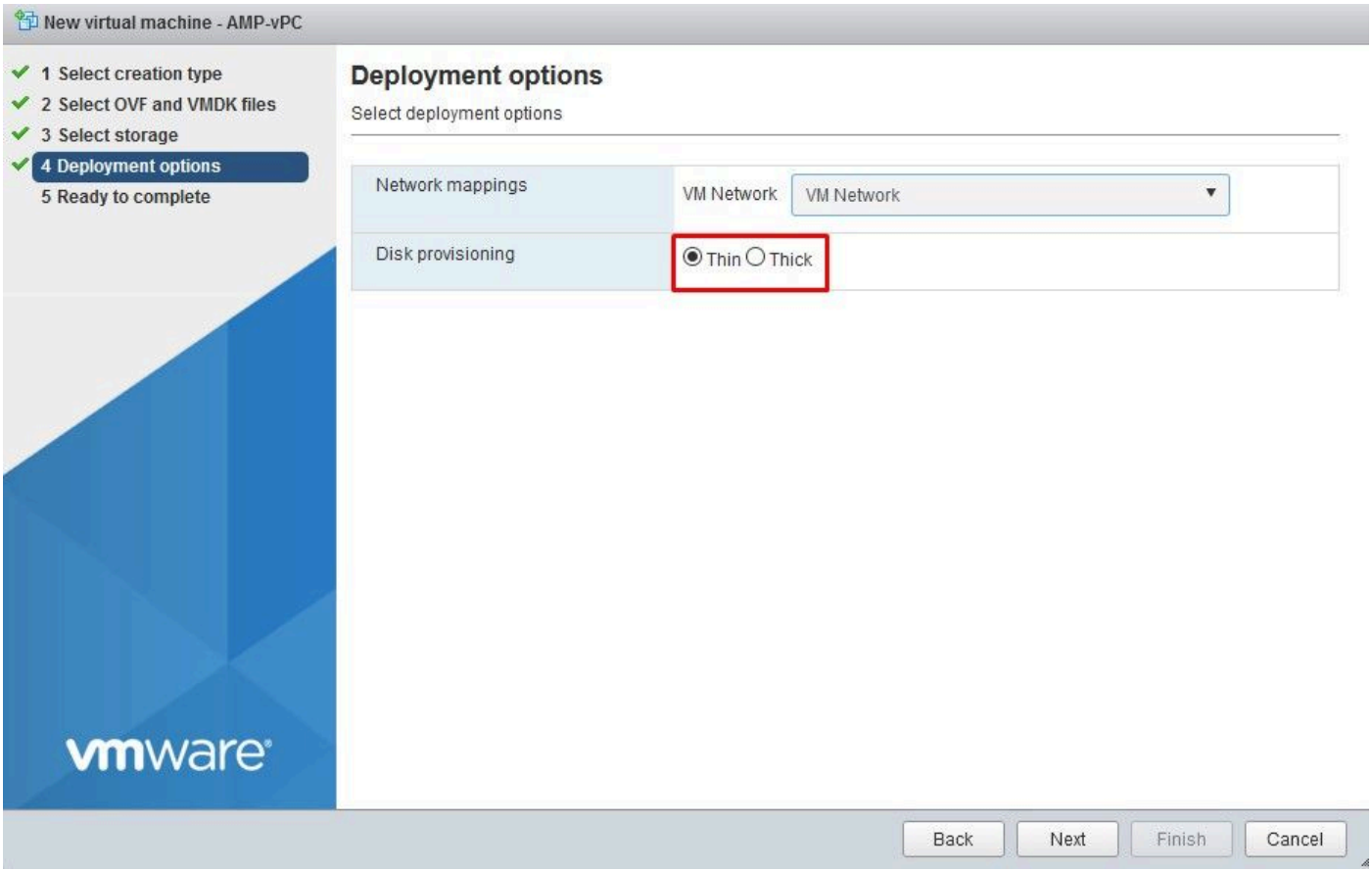
Navigate to **File > Deploy OVF Template** to open the **Deploy OVF Template** wizard, as shown in the image.


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 ESXi instance.
PrivateCloud-Latest.ova
vmware
Back
Next
Finish
Cancel


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 through the process of creating a virtual machine from an OVF and VMDK files.
vmware
Back
Next
Finish
Cancel

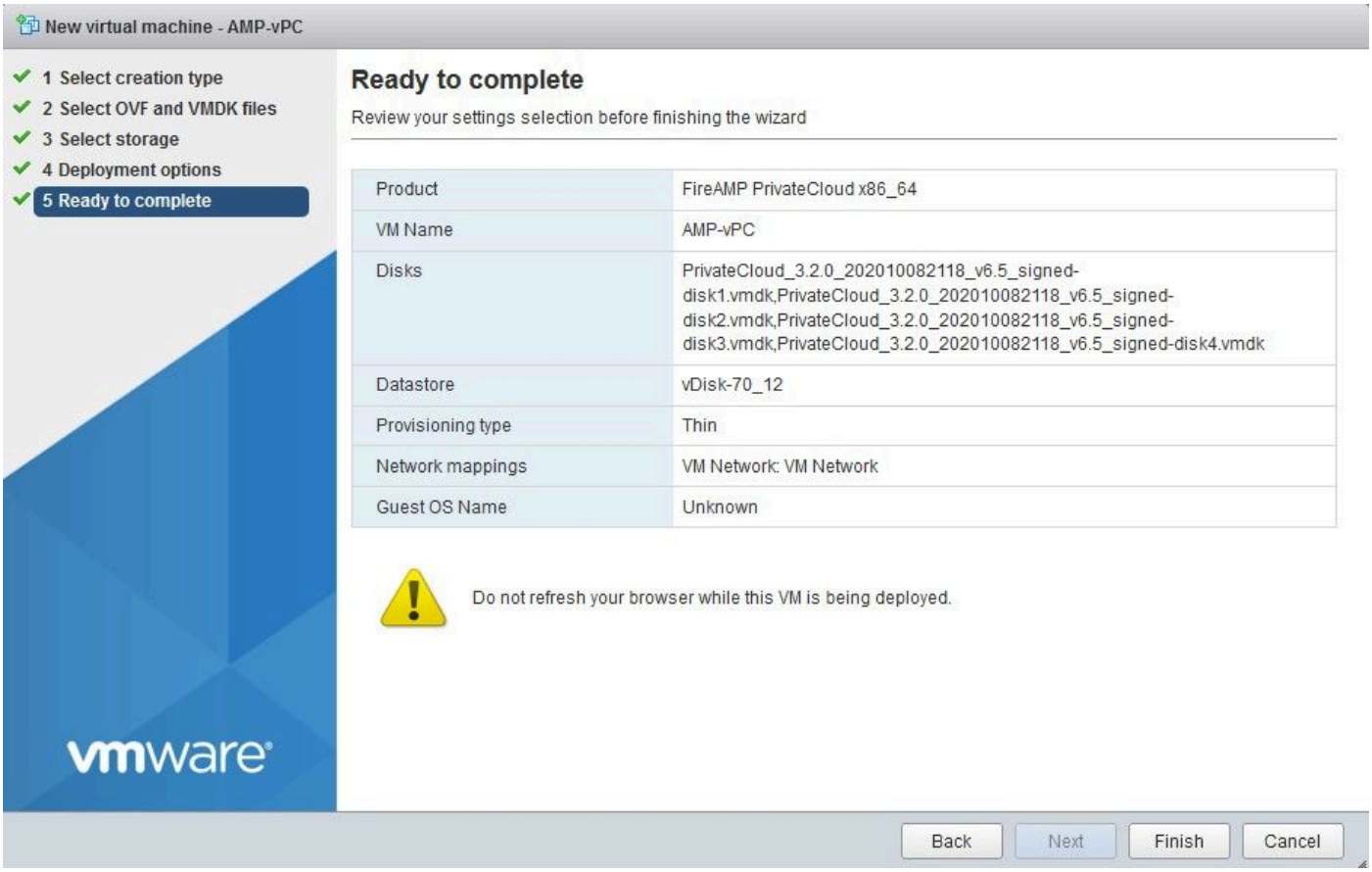


Note: **Thick Provisioning** reserves space when a disk is created. If you select this option, it can improve the performance over **Thin Provisioned**. However, this is not mandatory. Now select on **Next**, as shown in the image.

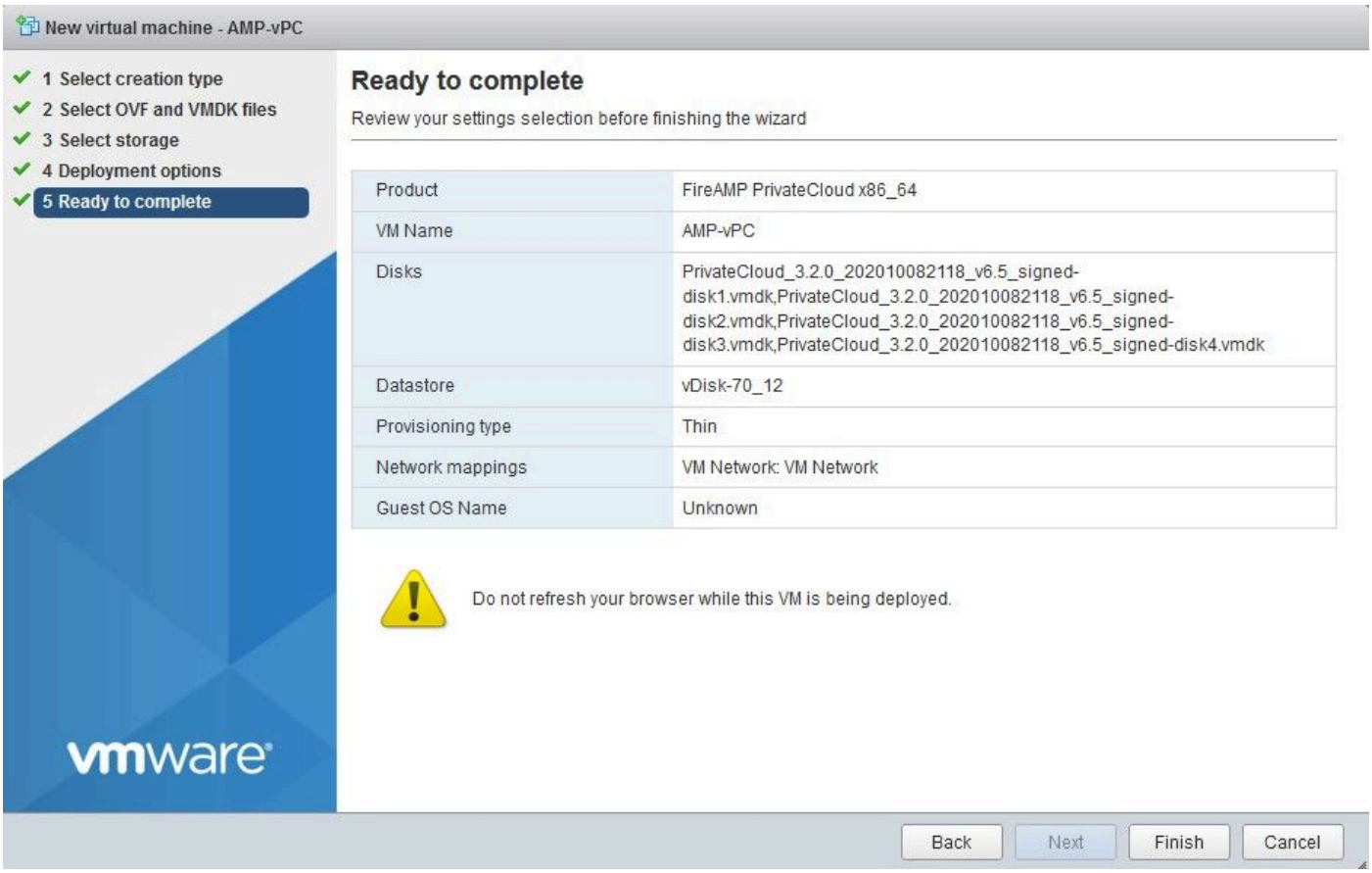


Step 2:

Select **Browse…** to select an OVA file, and then select on **Next**. You notice the default OVA parameters on the **OVF Template Details** page, as shown in the image. select on **Next**.



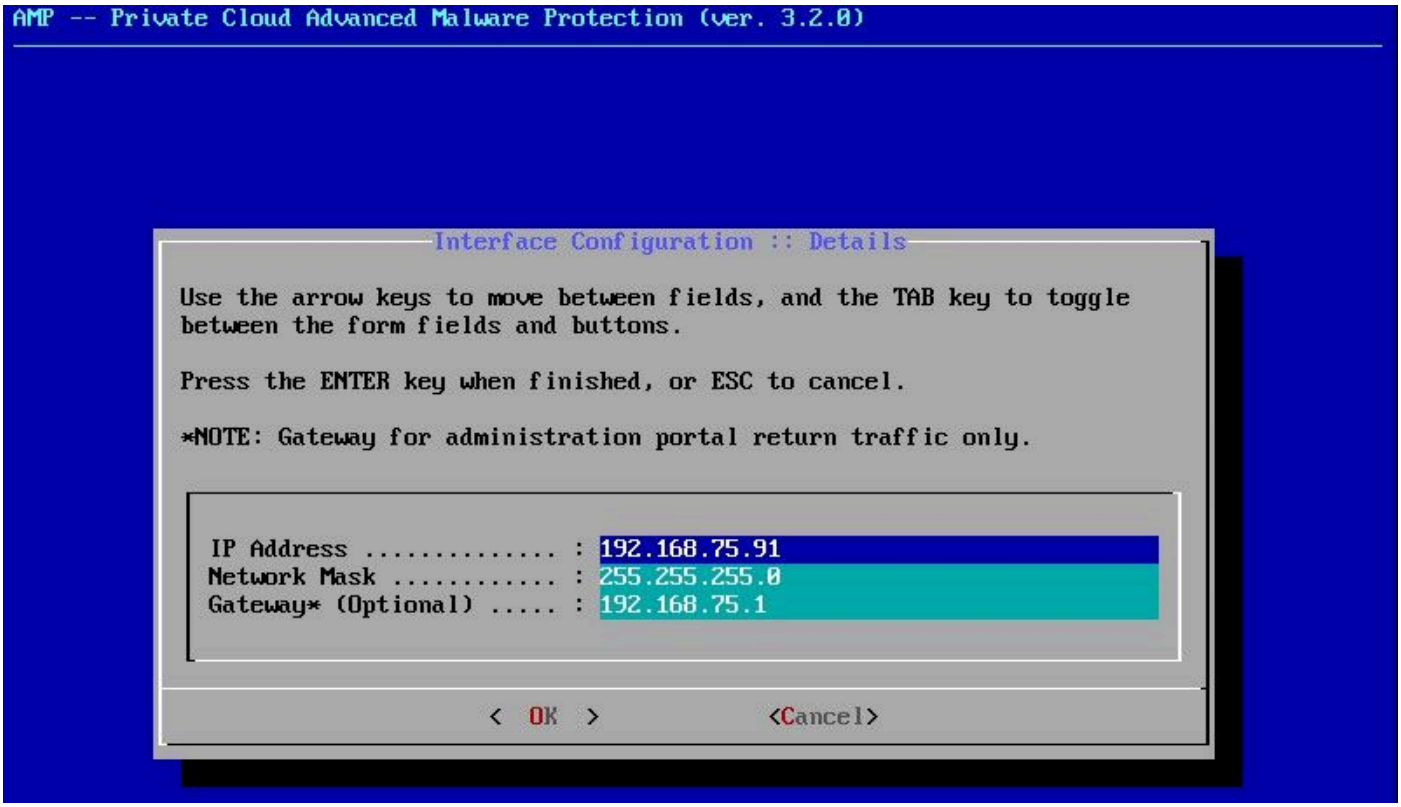
Initial Admin Interface Setup



Once the VM boots up you do the initial configuration through VM Console.

Step 1:

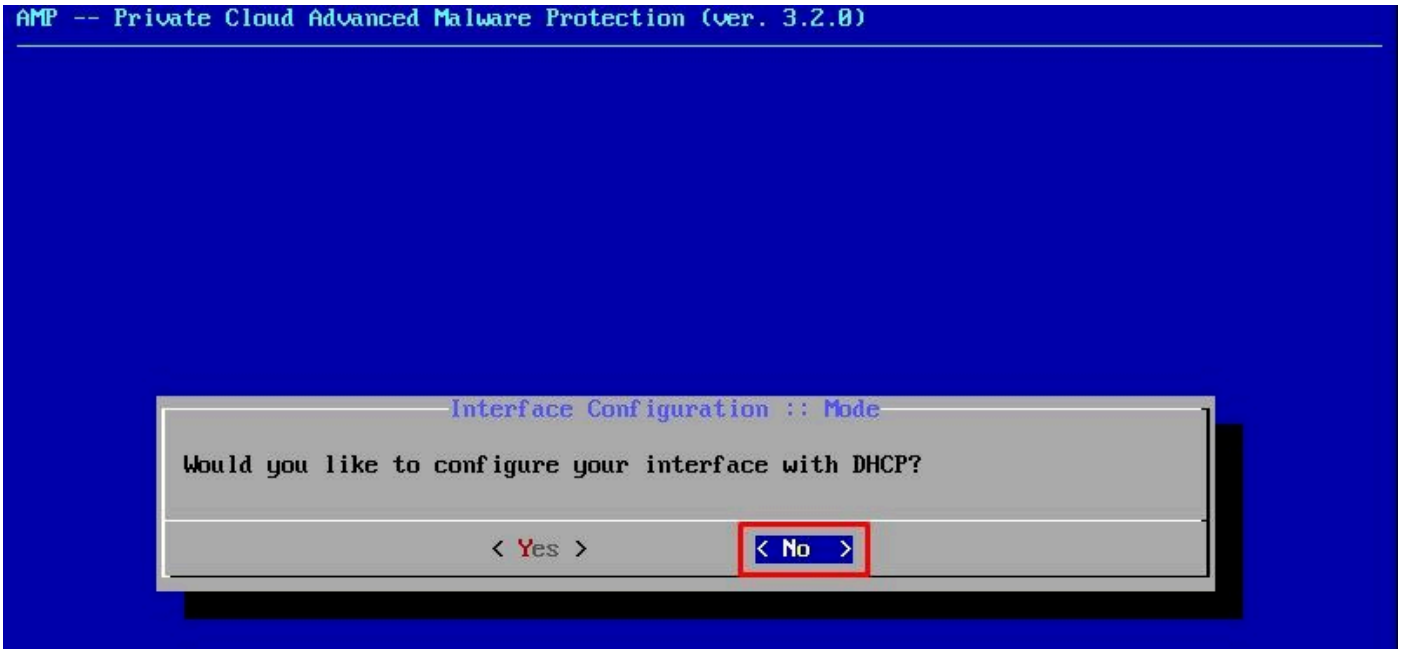
You might notice that the URL shows **[UNCONFIGURED]** if the interface did not receive an IP address from the DHCP server. Please note that this interface is the **Management** interface. This is not the **Production** interface.

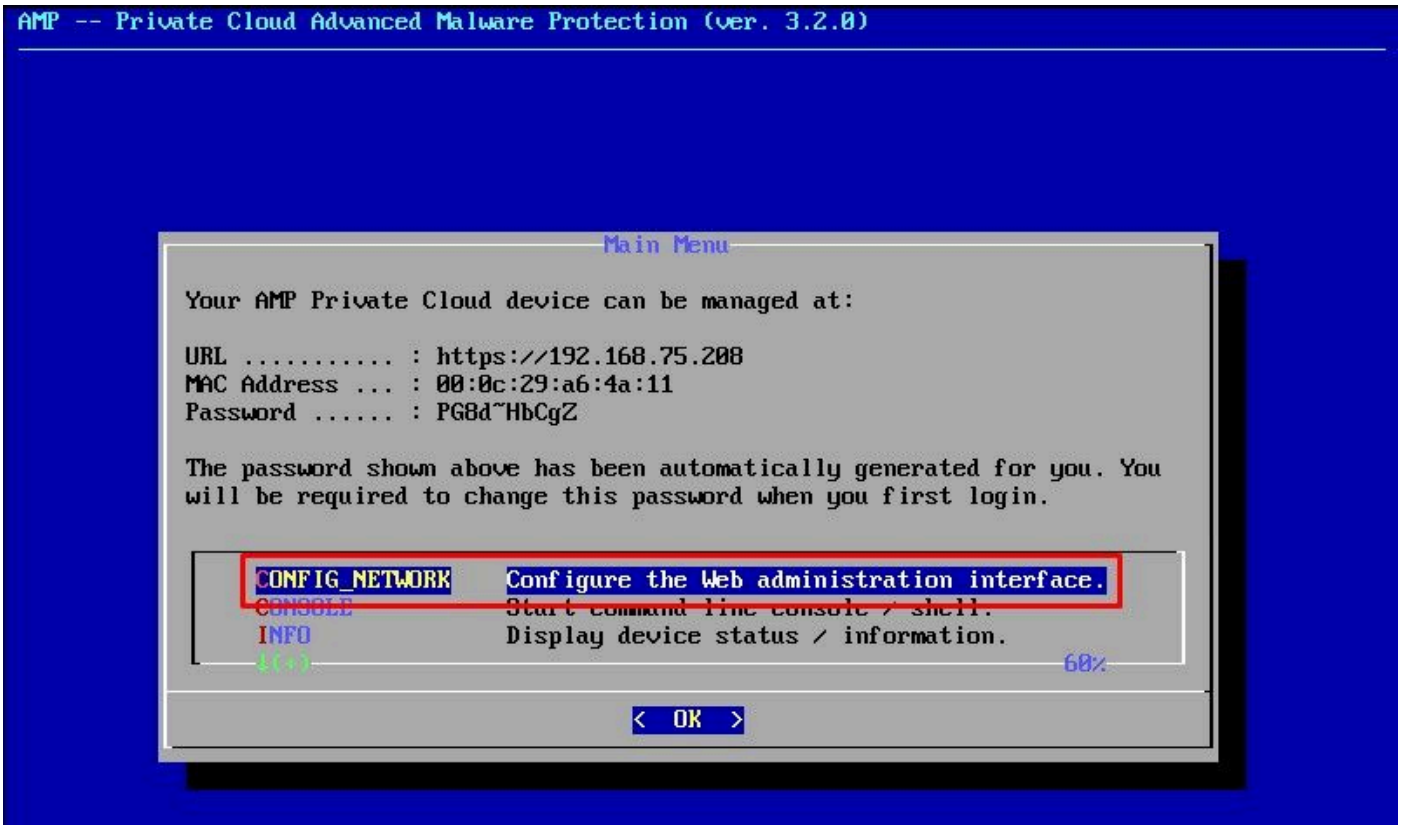


Step 2:

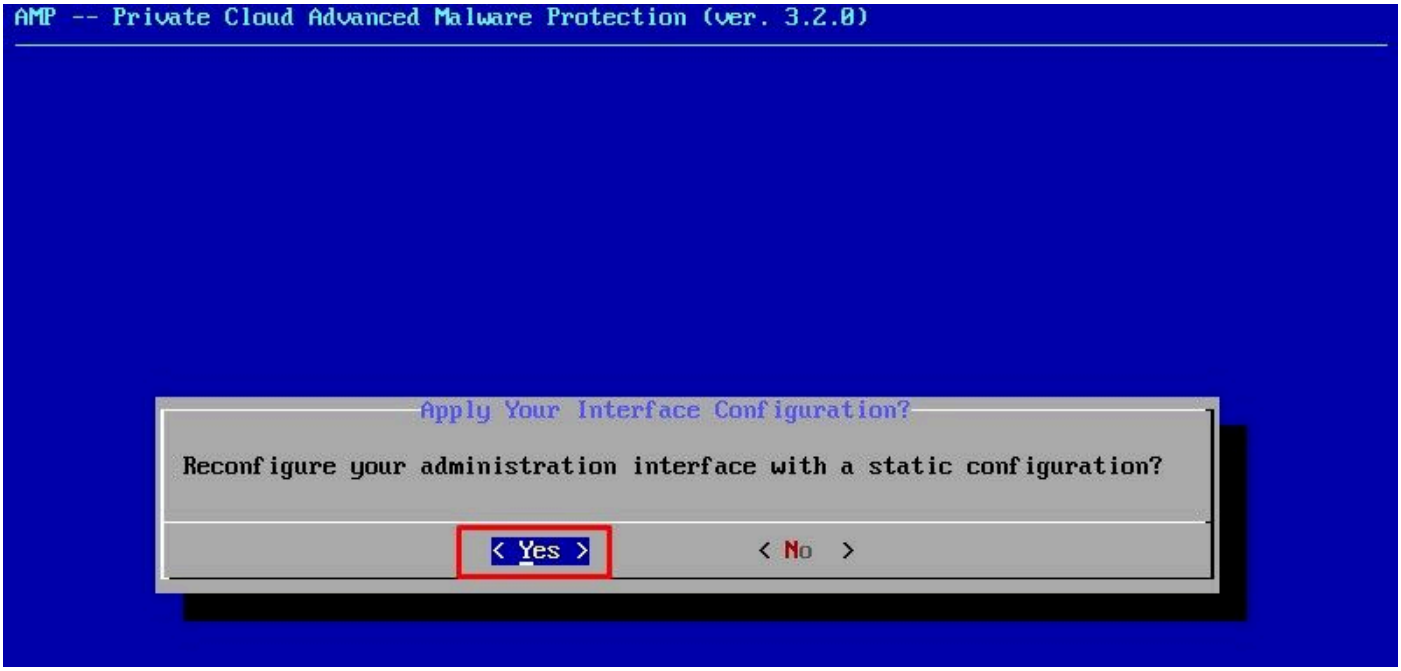
You can navigate through **Tab**, **Enter**, and **Arrow** keys.

Navigate to **CONFIG_NETWORK** and select the **Enter** key on your keyboard to begin the configuration of the management IP address for the Secure Endpoint Private Cloud. If you do not want to use DHCP, select **No** and select **Enter** key.





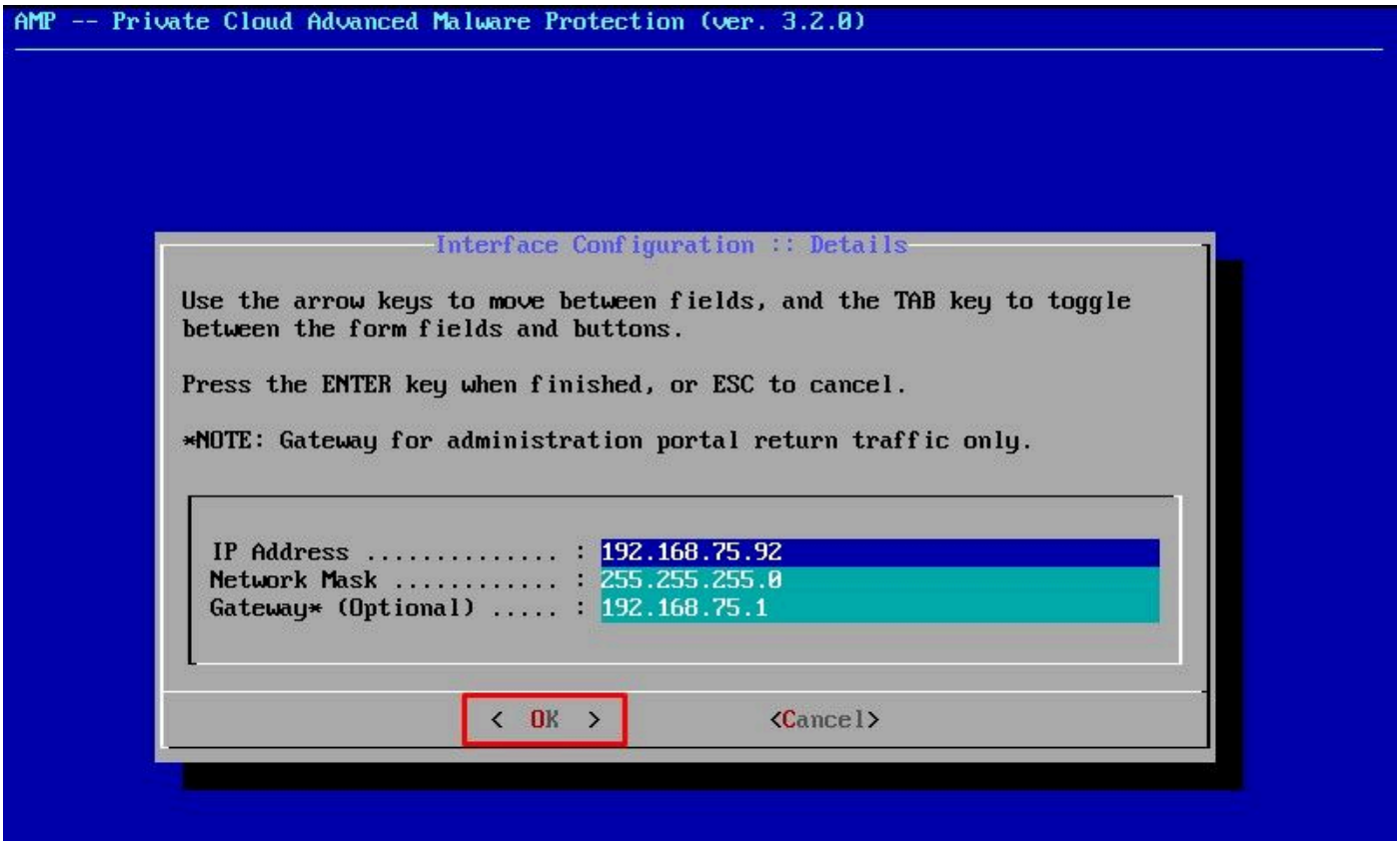
In the appeared window choose **Yes** and select **Enter** key.



If the IP is already in use you be treated with this error log. Just simply go back and pick something that is unique and not in use.

```
Restarting eth0...

ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
ERROR     : [/etc/sysconfig/network-scripts/ifup-eth] Error, some other host (00:0C:29:41:74:E3) alr
eady uses address 192.168.75.91.
================================================================================
ERROR: The interface failed to reconfigure.
================================================================================
Press ENTER key to continue...
_
```



If all goes well, you see output that looks like this

```
    - 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 06:13:11.889389544 +0000
    @@ -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 only_if)
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_plu
gins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in you
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[:disabled_plu
gins] is deprecated and will be removed in future releases of ohai. Use ohai.disabled_plugins in you
r configuration file to configure :disabled_plugins for ohai.
Starting Chef Client, version 12.14.89
```

Step 3:

Wait until the blue screen pops again with your new STATIC IP. Also, please note the **One Time Password**. Take a note and let's open our browser.

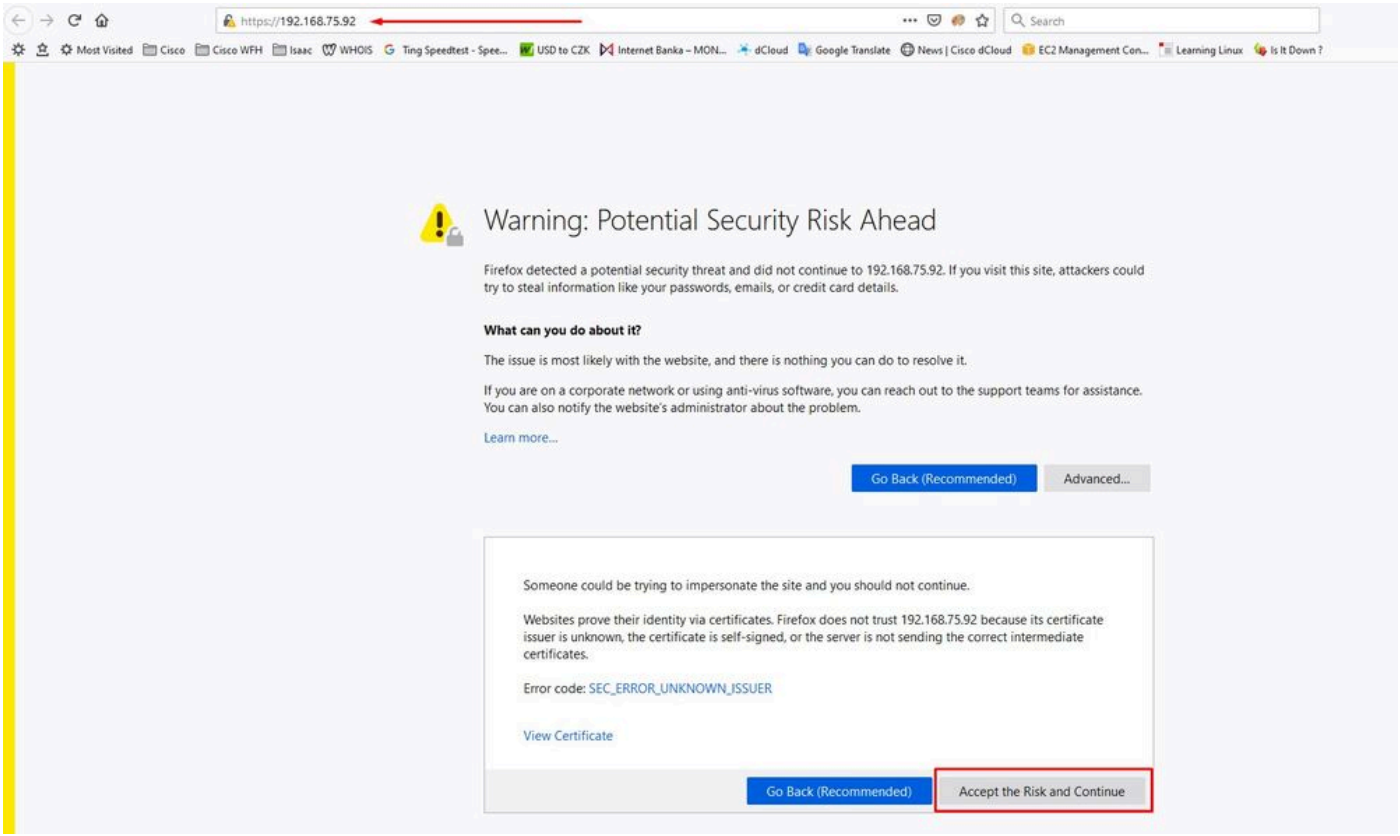


Initial Configuration of the vPC via web GUI

Step 1:

Open a web browser and navigate to the management IP address of the appliance. You can receive a certificate error as the Secure Endpoint Private Cloud initially generates its own HTTPS certificate, as shown in the image. Configure your browser to trust the self-signed HTTPS certificate of Secure Endpoint Private Cloud.

In your browser type the **STATIC IP** that you configured previously.



Step 2:

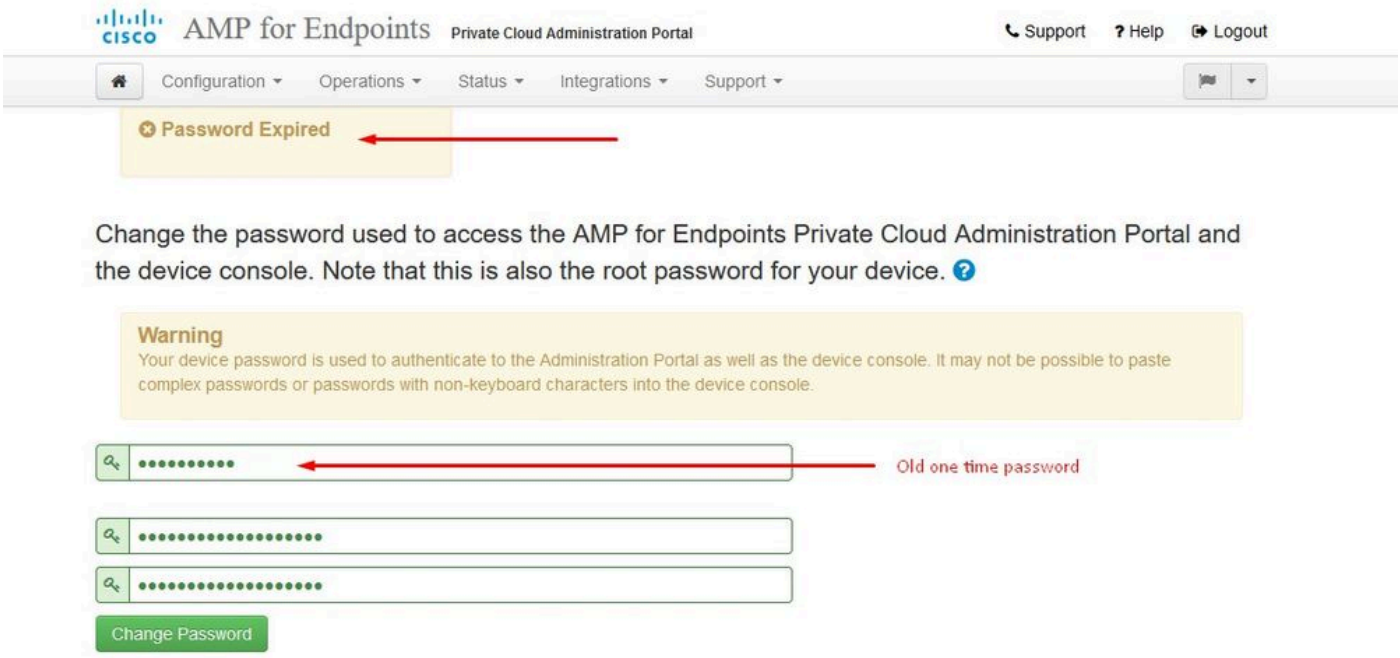
After you log in, you are required to reset the password. Use the **initial password** from the console in the **Old Password** field. Use your new password in the **New Password** field. Re-enter your new password in the **New Password** field. select on **Change Password**.



Step 3:

After you log in, you are required to reset the password. Use the **initial password** from the console in the **Old Password** field. Use your new password in the **New Password** field. Re-enter your new password in

the **New Password** field. select on **Change Password**.



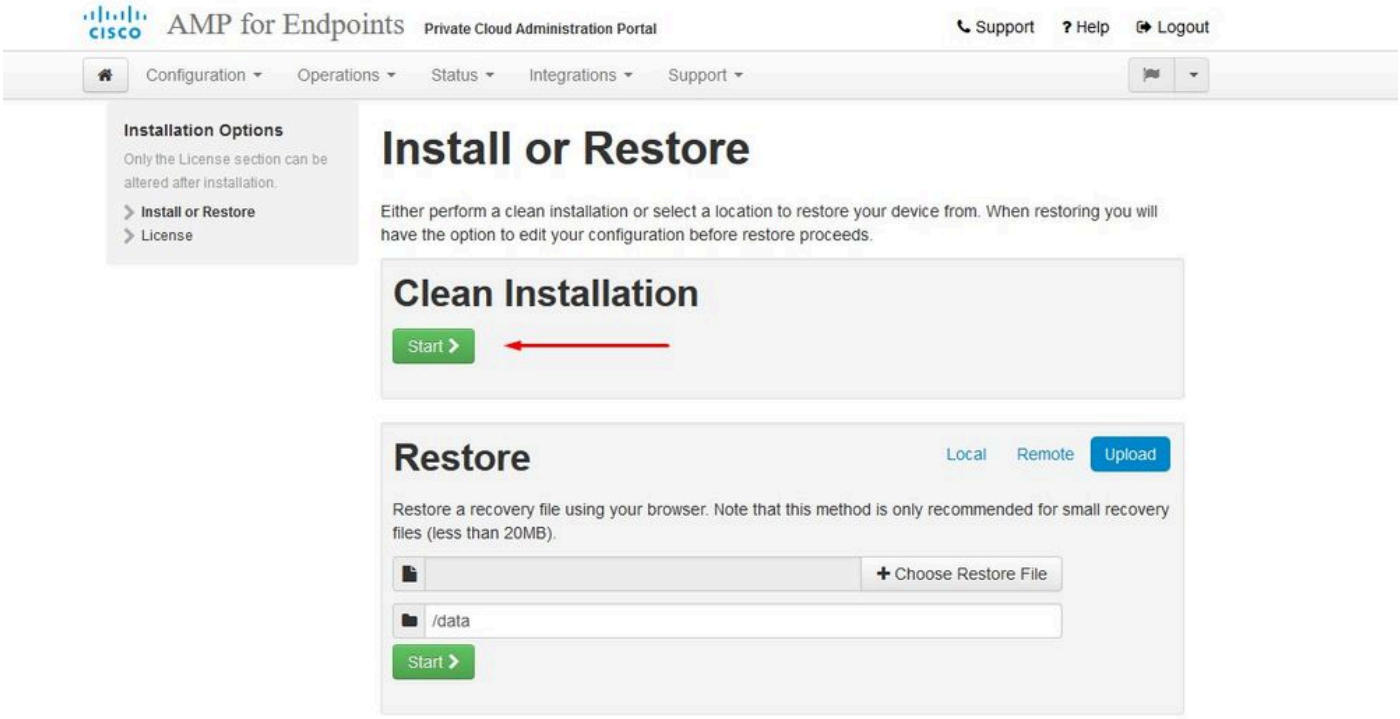
Step 4:

On the next page scroll down to the bottom to accept the license agreement. select on **I have read and agree**.



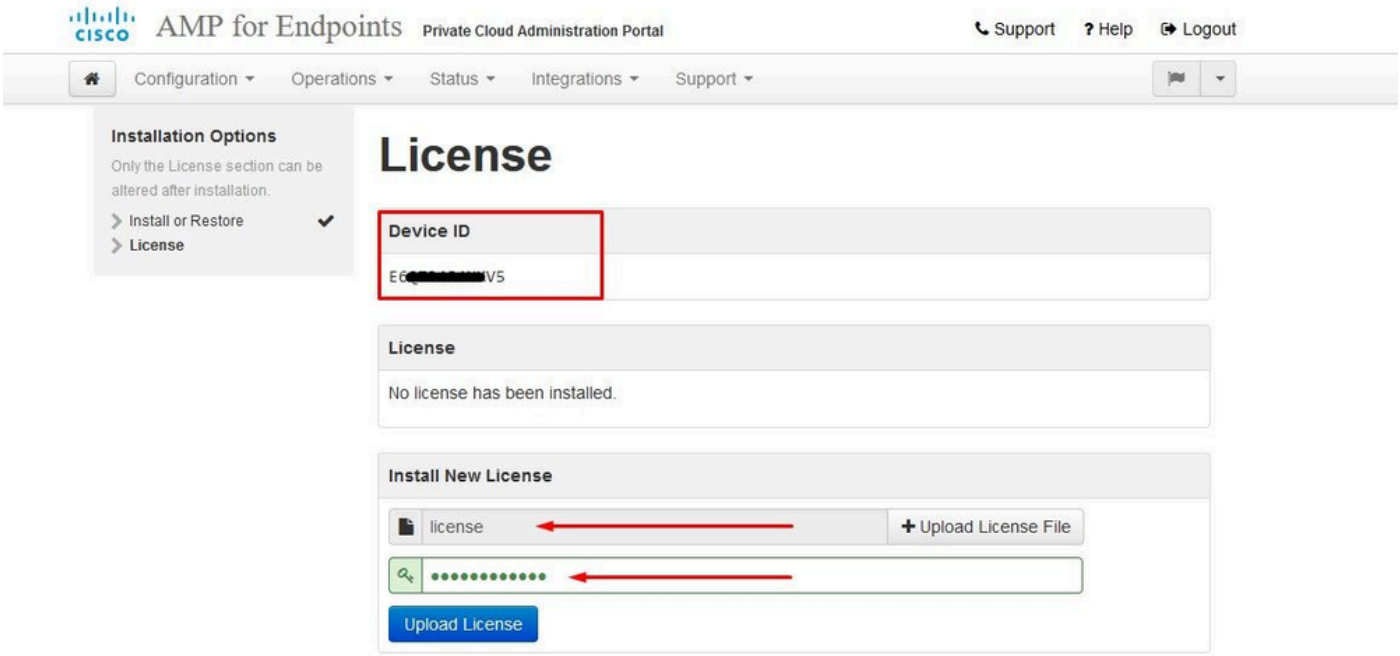
Step 5:

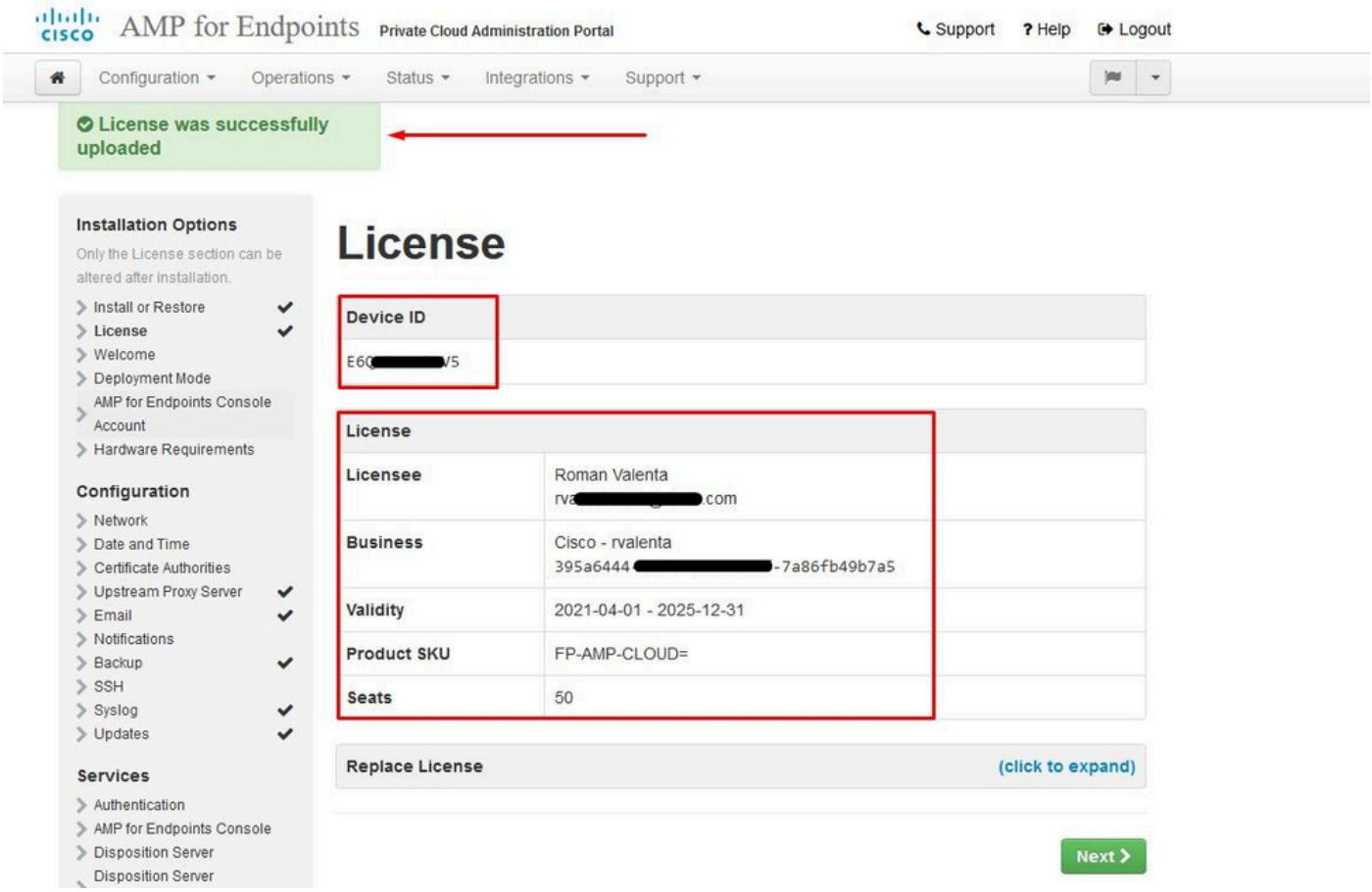
After you accept the agreement, you get the installation screen, as shown in the image. If you want to restore from a backup, you can do that here, however, this guide proceeds with the **Clean Installation** option. Select on **Start** in the **Clean Installation** section.



Step 6:

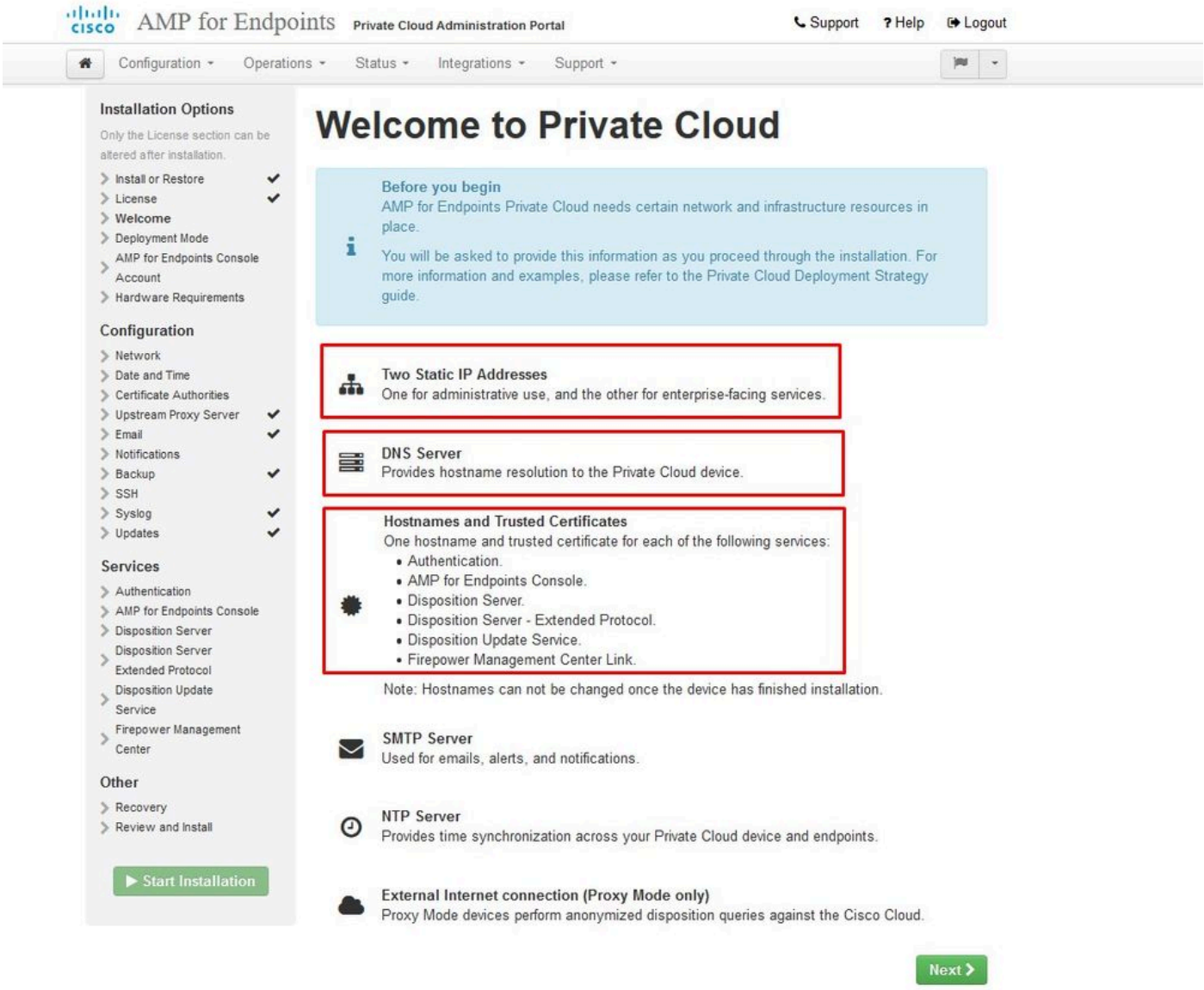
The very first thing you need is license to even move forward. You receive a license and passphrase when you purchase the product. Select on **+Upload License File.** Choose the license file and enter the passphrase. Select on **Upload License**. If the upload is unsuccessful, please check if the passphrase is correct. If the upload is successful, a screen with valid license information is displayed. Select on **Next.** If you still cannot install your license, contact Cisco Technical Support.





Step 7:

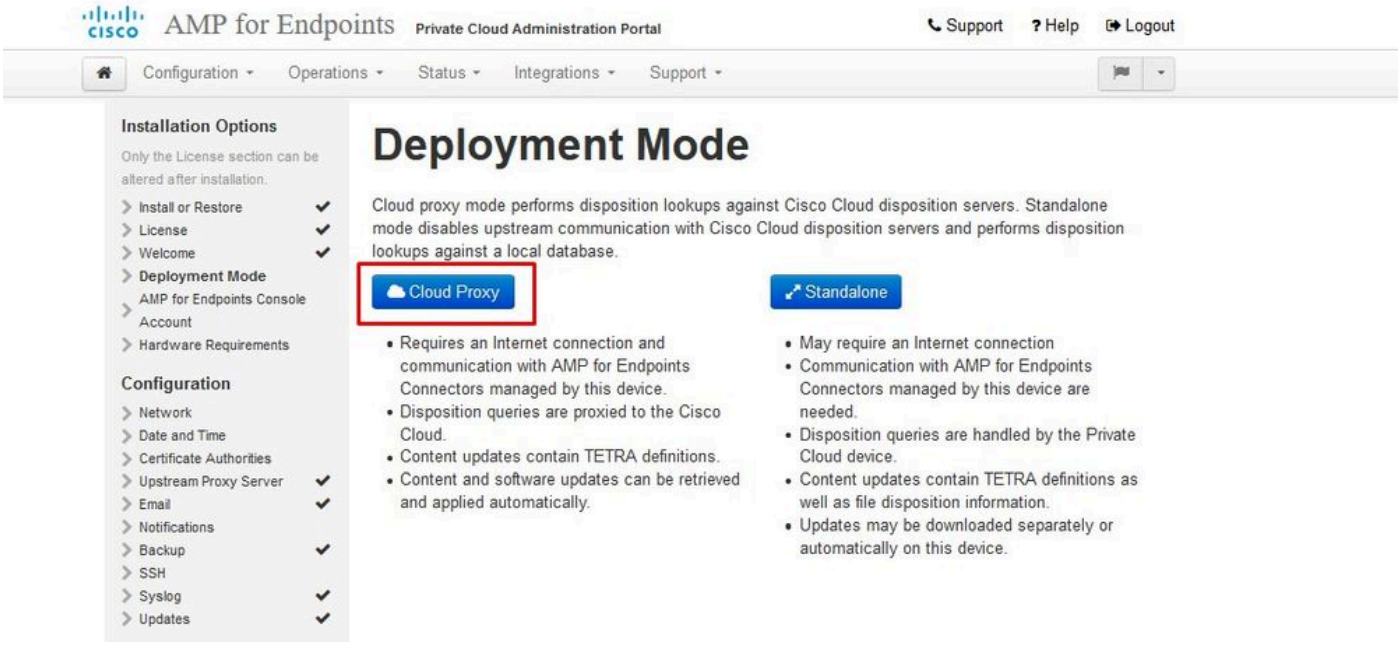
You receive the Welcome Page, as shown in the image. This page shows you the information you must have before the configuration of the Private Cloud. Read the requirements attentively. Select on **Next** to start the pre-installation configuration.



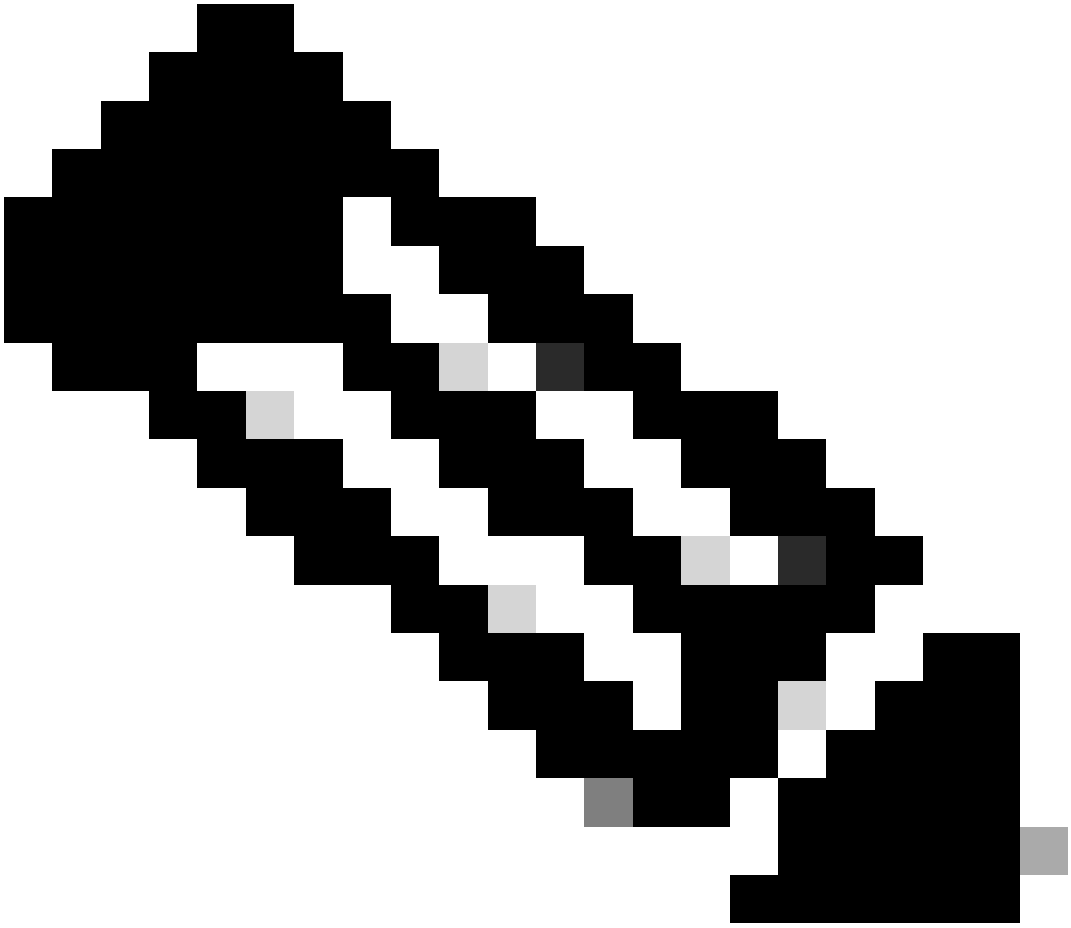
Configuration

Step 1:

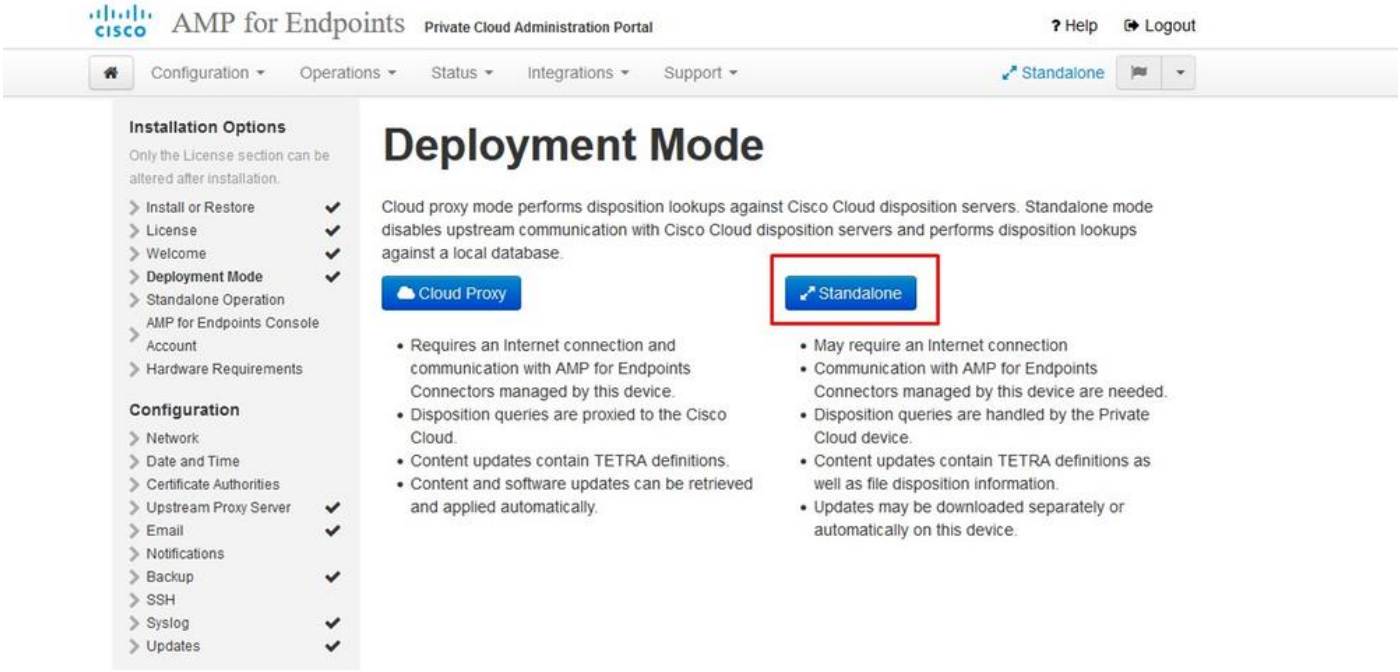
Note: Please note that in next sets of slide we include some exclusive as shown in the image that are unique only to **AIR GAP** mode , those be enclosed and marked as **AIRGAP ONLY**

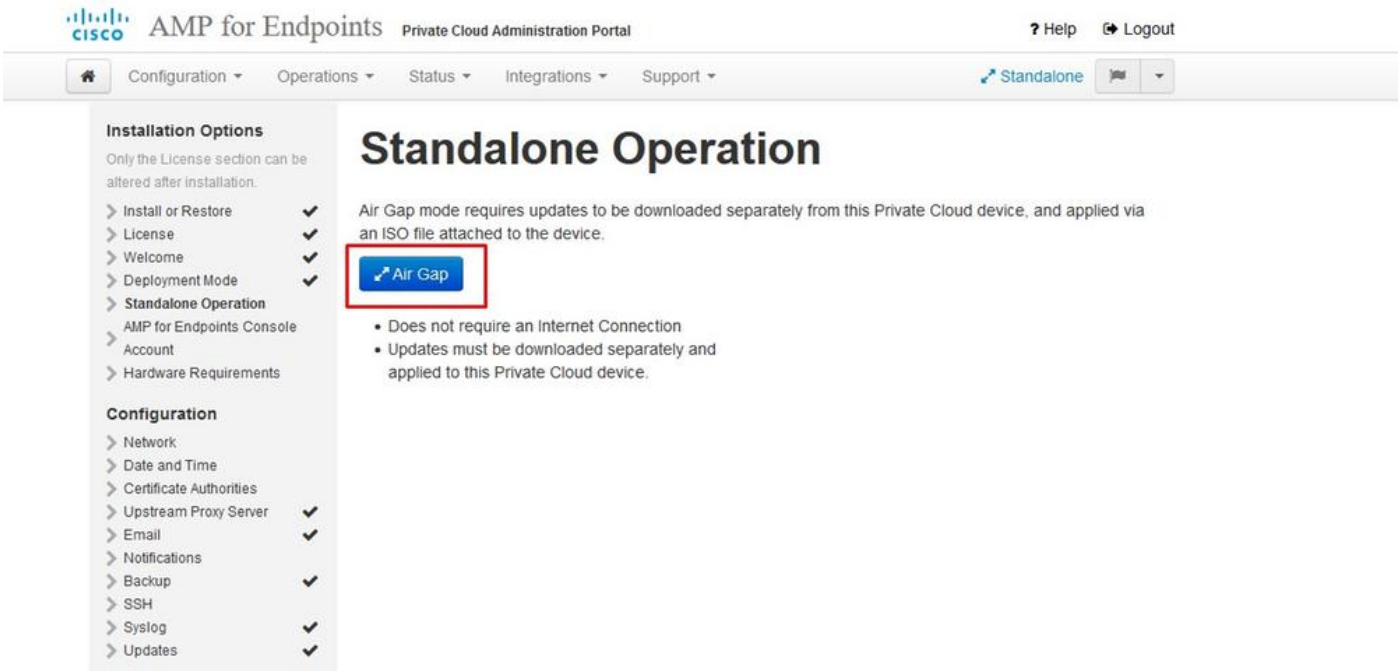

AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware Requirements
Configuration
Network
Date and Time
Certificate Authorities
Upstream Proxy Server
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
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 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 may be downloaded separately or automatically on this device.

⌄⌄ **AIRGAP ONLY** ⌄⌄



Note: These steps are applicable only for physical appliance.

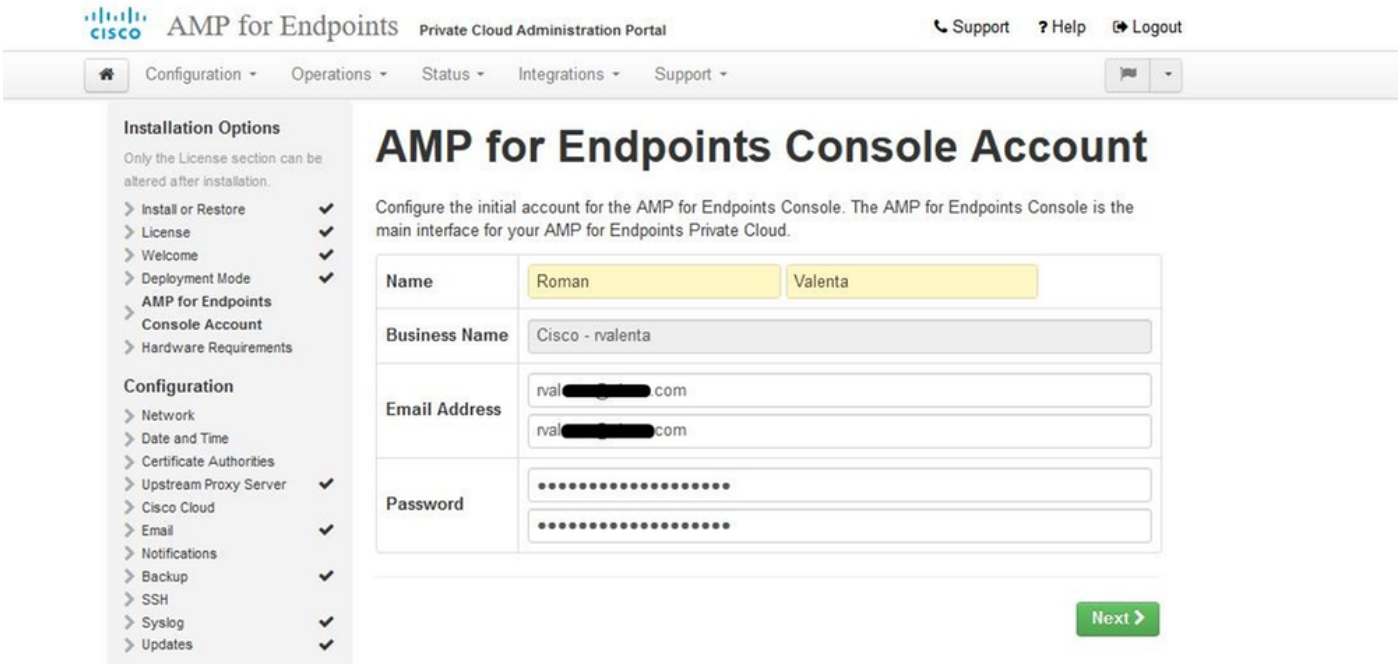




⩓ ⩓ AIRGAP ONLY ⩓ ⩓

Step 2:

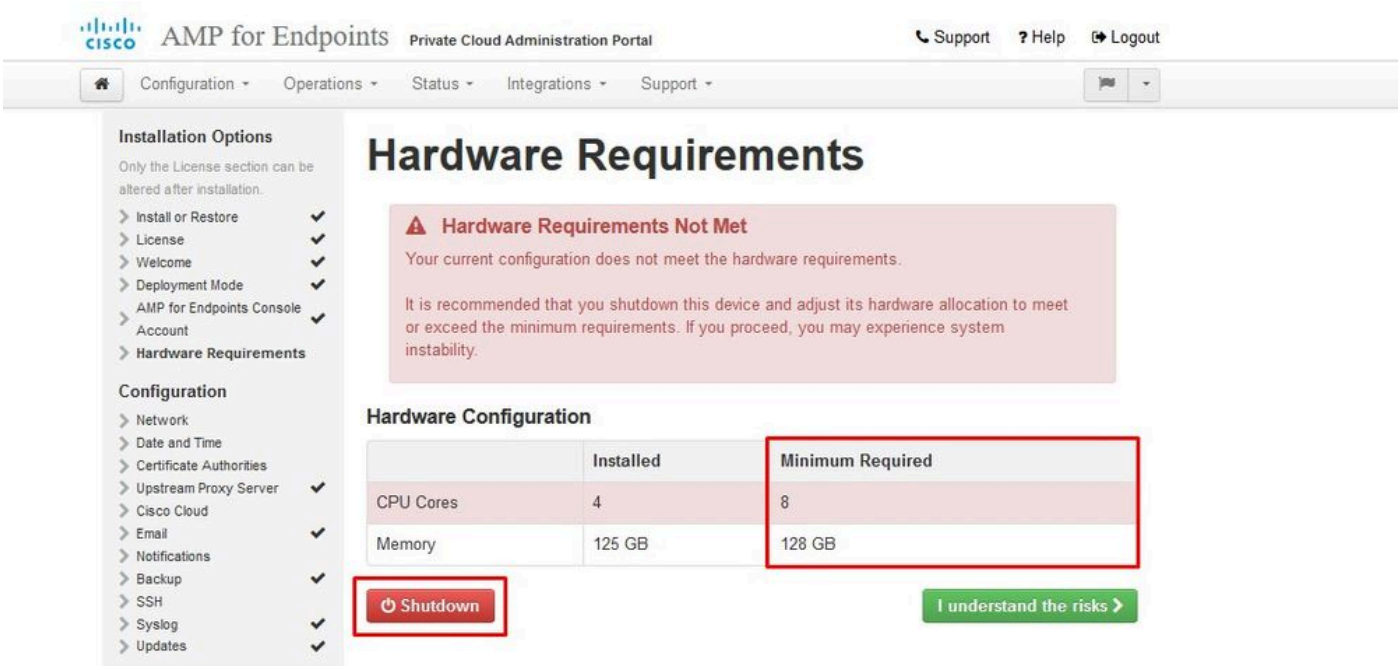
Navigate to the Secure Endpoint Console Account page. An administrative user is used for the console to create policies, computer groups, and add additional users. Enter Name, Email Address and Password for the Console Account. Select on **Next**.



If you run in to this issue when you deploy from the OVA file then you have two choices either, continue and fix this issue later or shutdown then in order to your deployed VM and adjust accordingly. After restart you continue where you left.

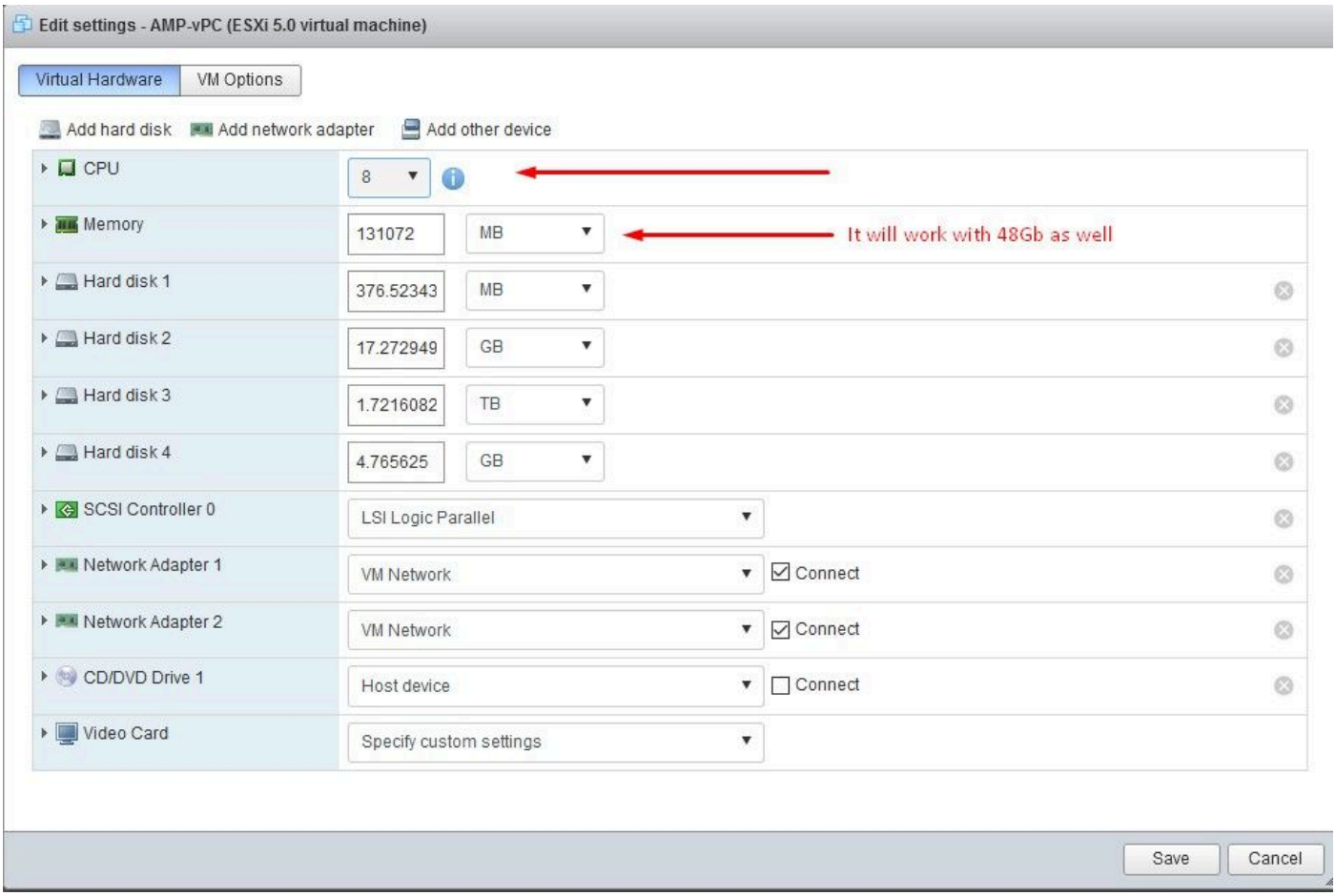
Note: This was fixed in OVA file for version 3.5.2 which loads correctly with 128GB RAM and 8CPU Cores

---

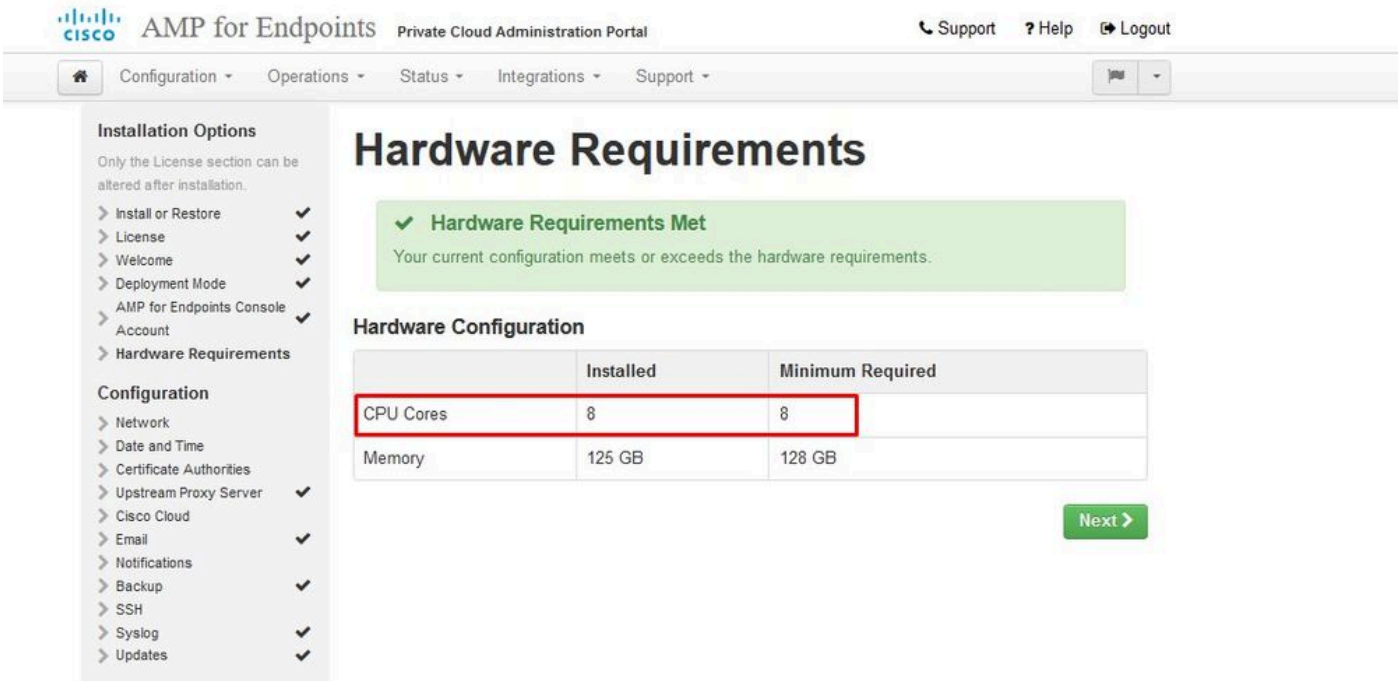


Note: Use only recommended values unless this is for lab purposes

---



Once rebooted we continue where we left.



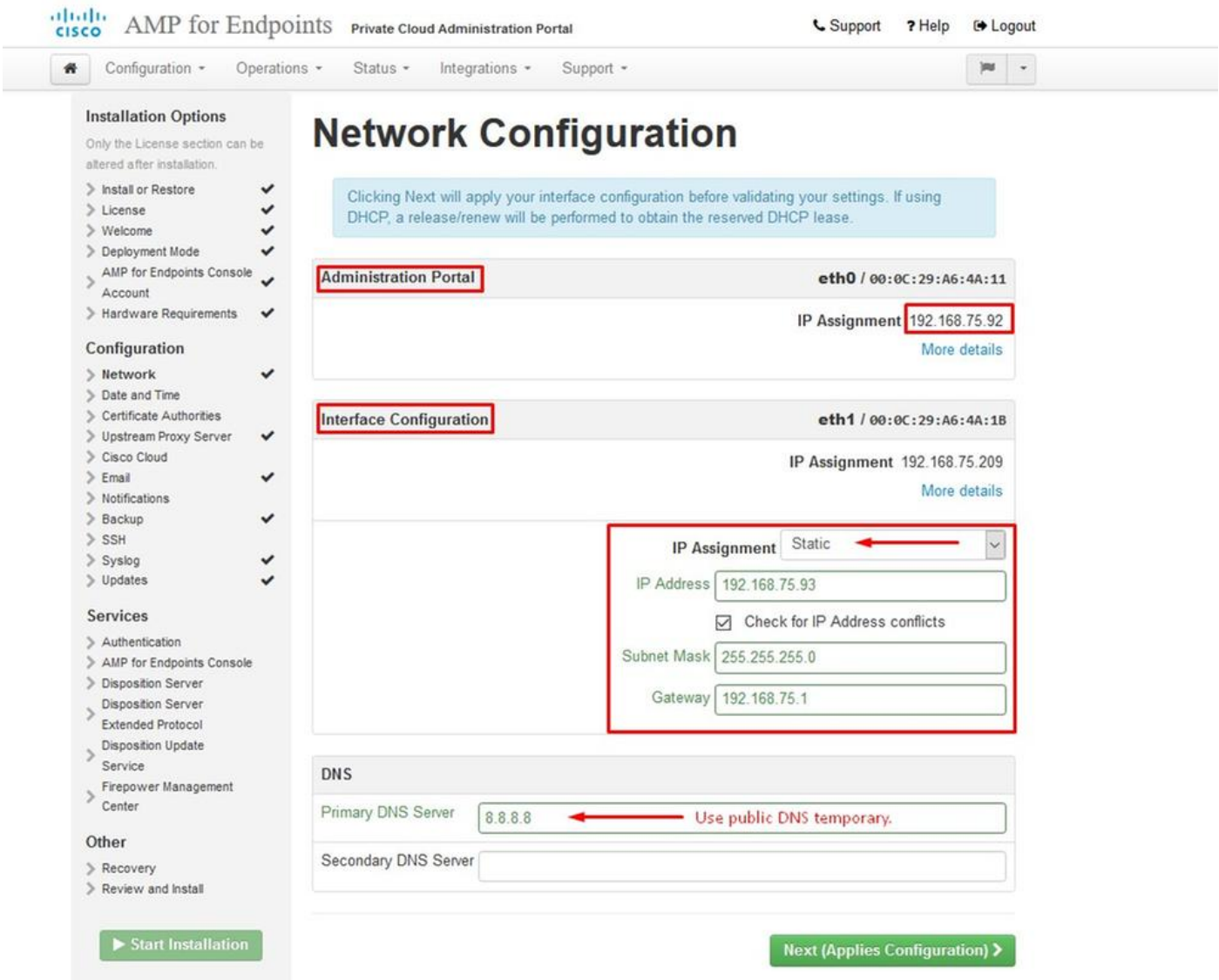
Ensure you configure ETH1 with STATIC IP as well.

Note: You must never configure your device to use DHCP unless you have created MAC address reservations for the interfaces. If the IP addresses of your interfaces change this can cause serious problems with your deployed Secure Endpoint Connectors. If you don't have your DNS server

---

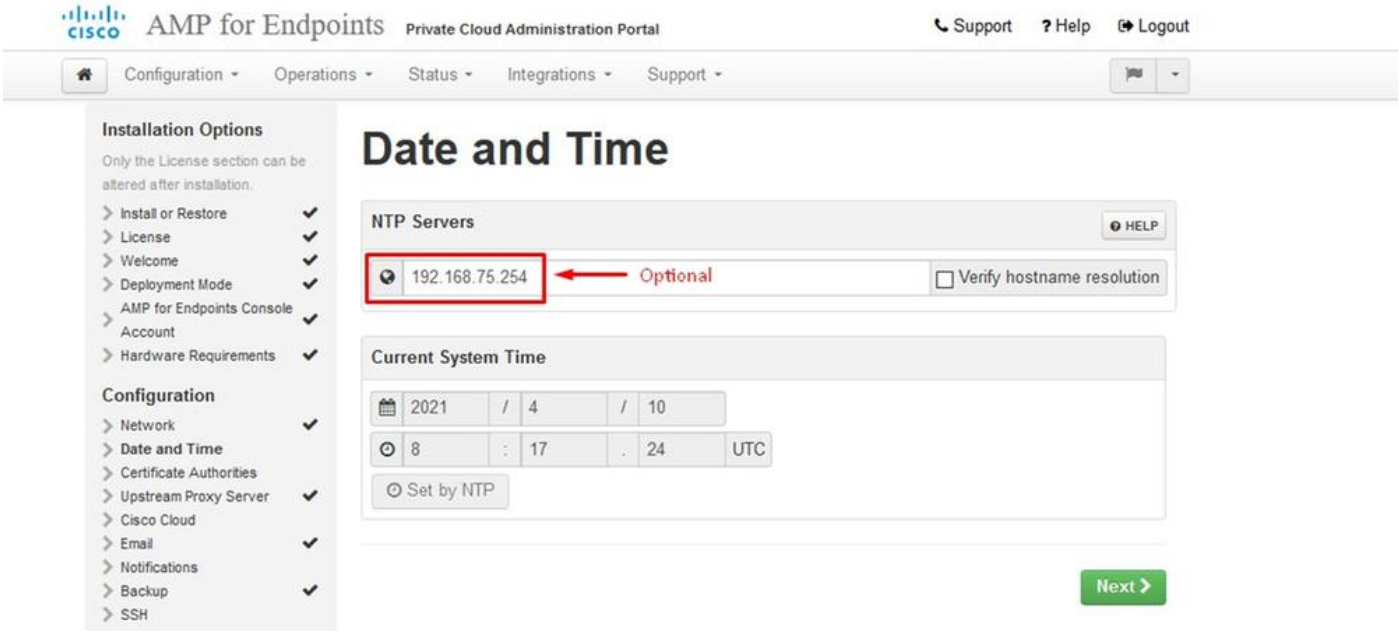
configured you can use public DNS **temporary** to finish your installation.

Step 3:

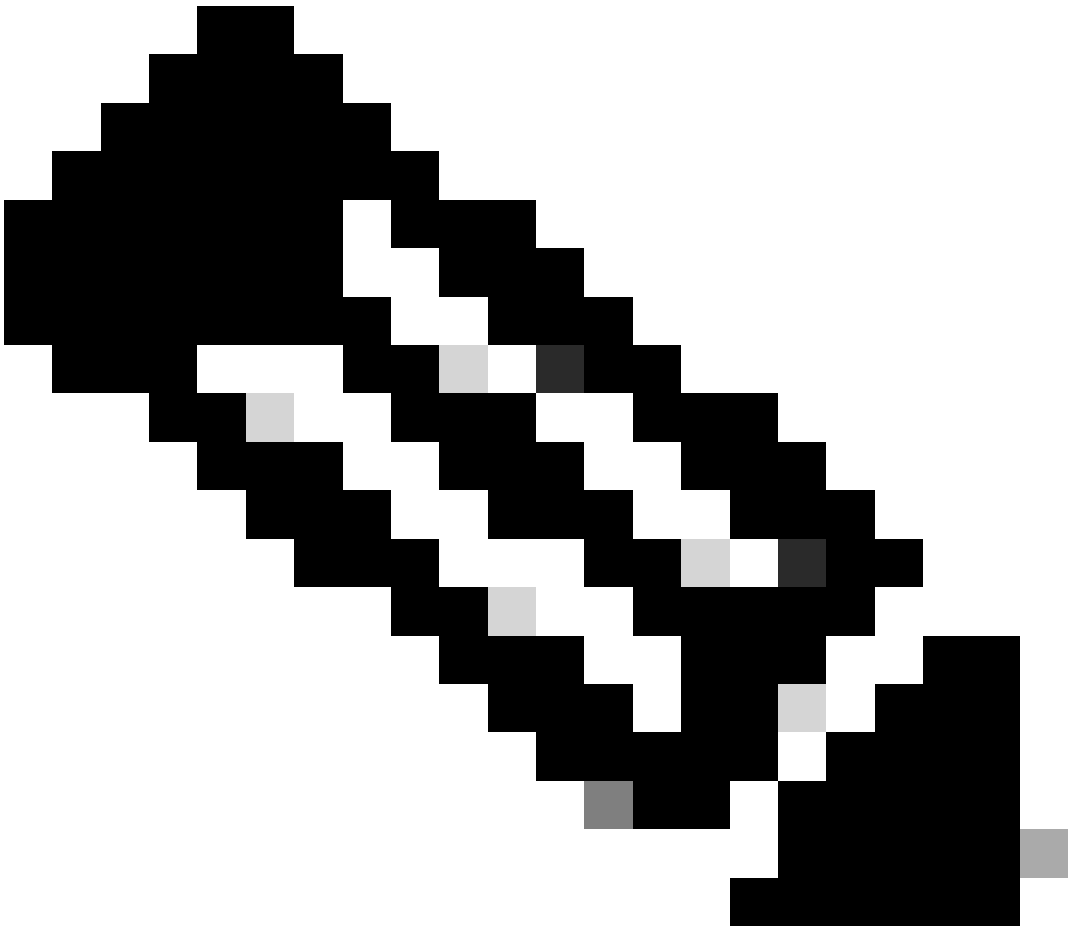


Step 4:

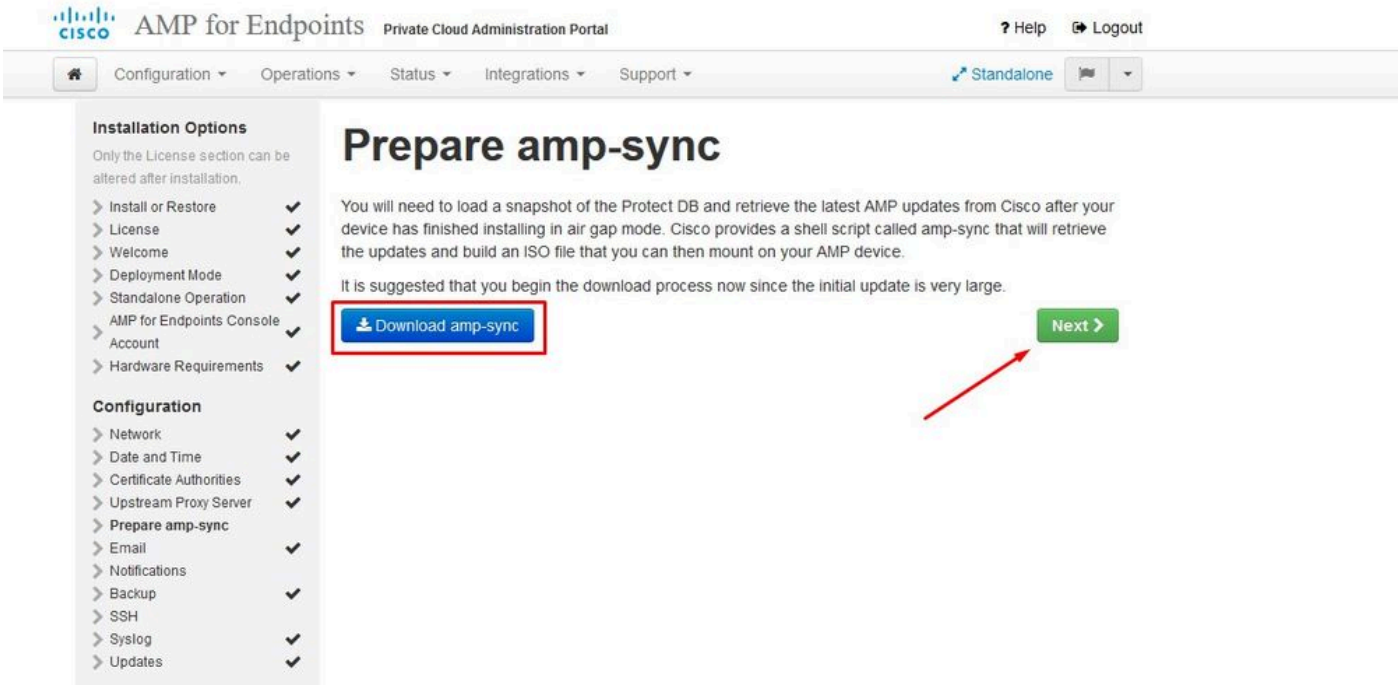
You get the Date and Time page. Enter the addresses of one or more NTP servers you want to use for Date and Time synchronization. You can use internal or external NTP servers and specify more than one through a comma or space delimited list. Synchronize the time with your browser or run amp-ctl ntpdate from the device console to force an immediate time synchronization with your NTP servers. Select on **Next.**


AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
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
Date and Time
NTP Servers
HELP
192.168.75.254
Optional
Verify hostname resolution
Current System Time
2021 / 4 / 10
8 : 17 . 24 UTC
Set by NTP
Next

AIRGAP ONLY



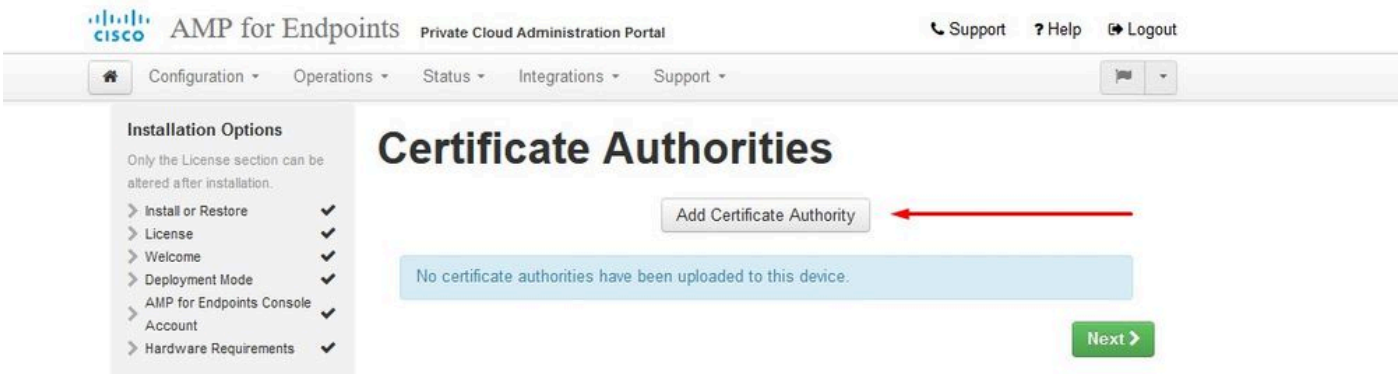
Note: These steps are applicable only for physical appliance.

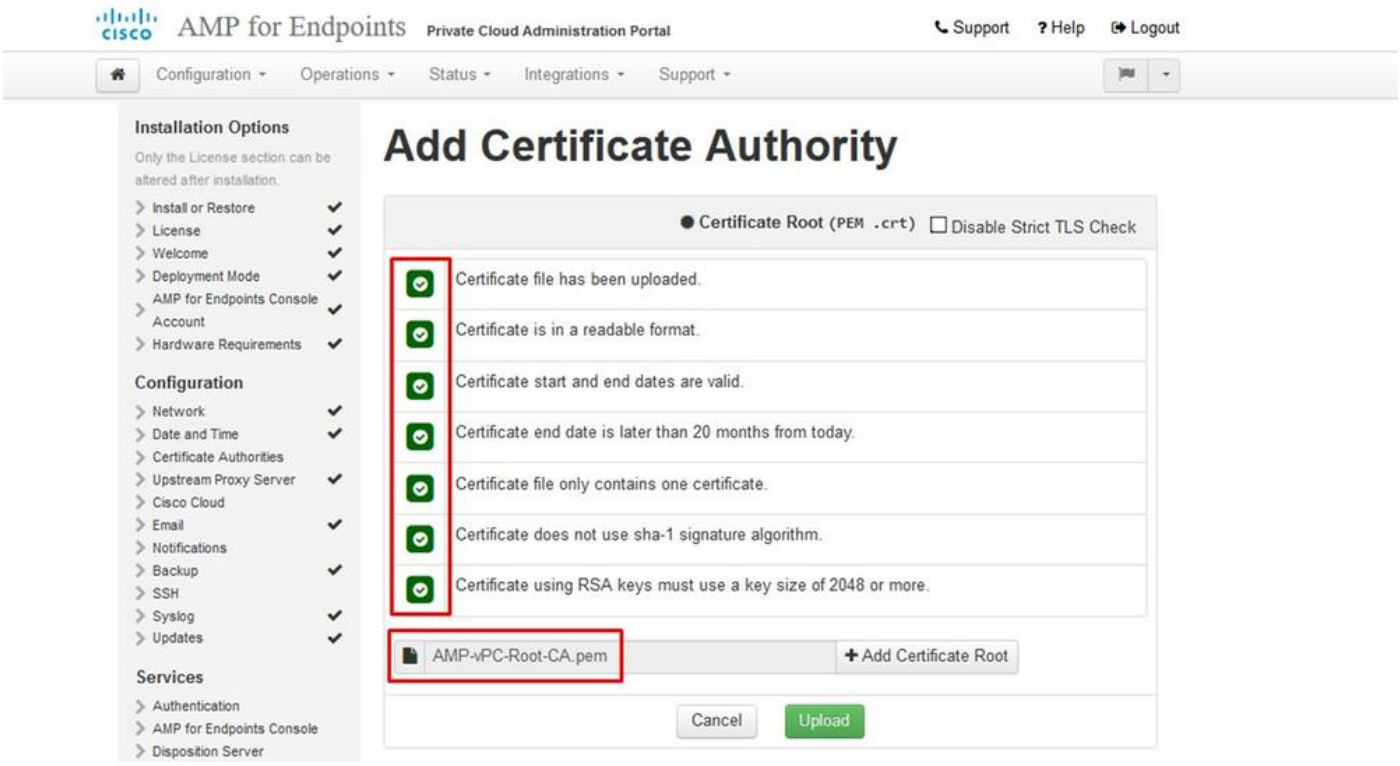


⩓ ⩓ AIRGAP ONLY ⩓ ⩓

Step 5:

You get the Certificate Authorities page, as shown in the image. Select on **Add Certificate Authority** to add your root certificate.

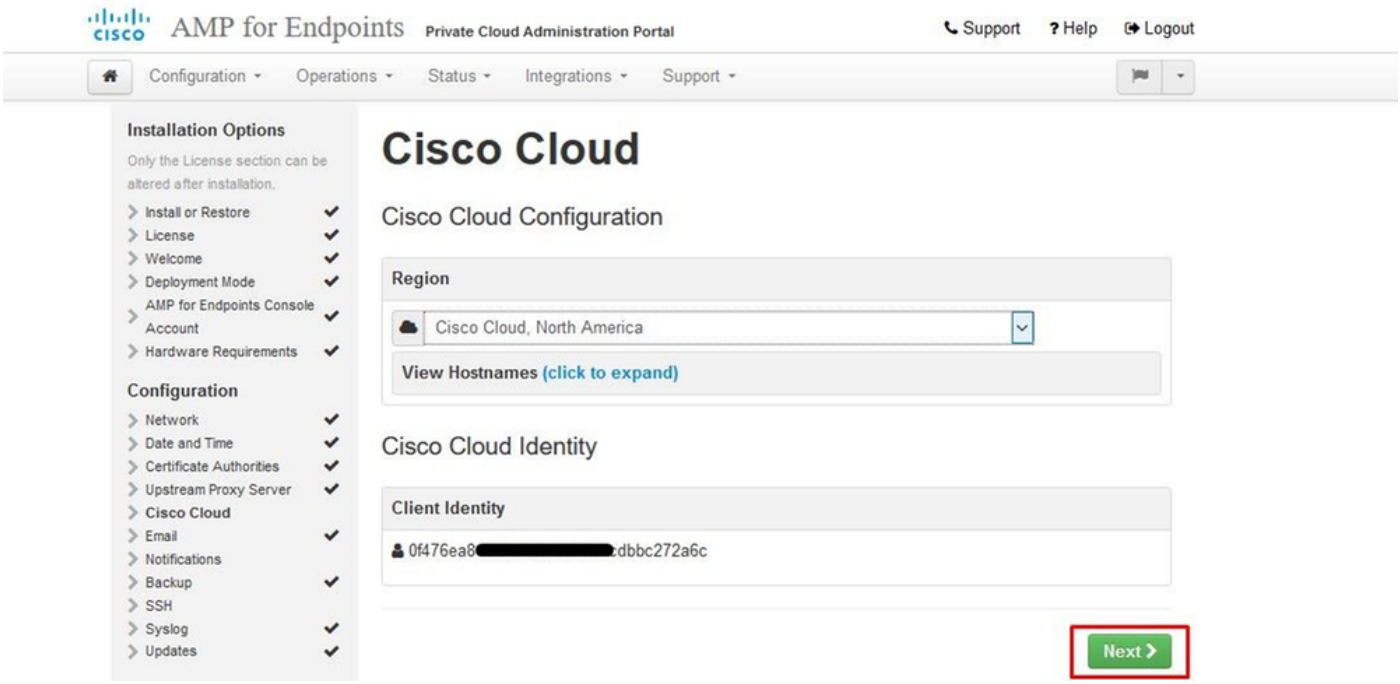






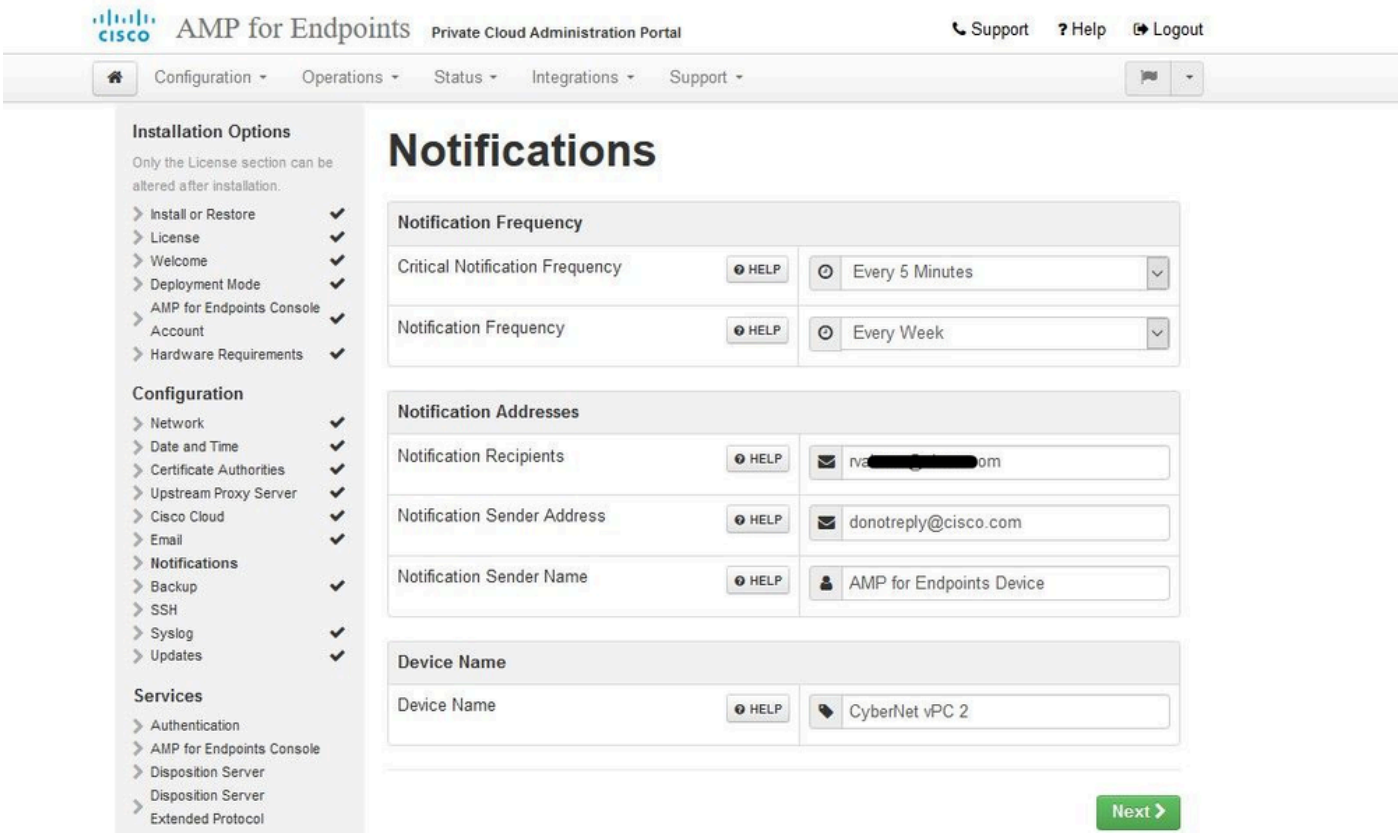
Step 6:

The next step is configure Cisco Cloud page, as shown in the image. Select the appropriate Cisco Cloud **Region**. Expand **View Hostnames** if you need to create firewall exceptions for your Secure Endpoint Private Cloud device to communicate with the Cisco Cloud for file lookups and device updates. Select on **Next**.



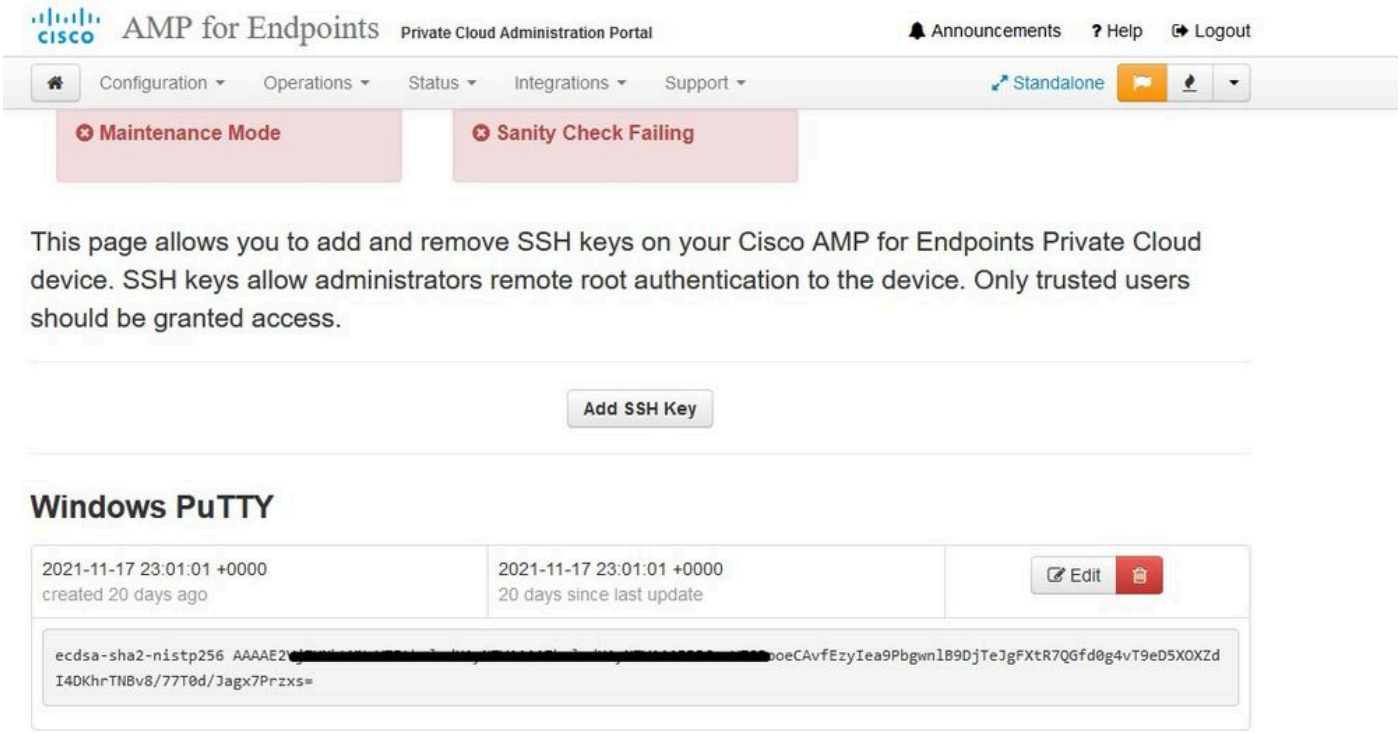
Step 7:

Navigate to notifications page, as shown in the image. Select the frequency for critical and regular Notifications. Enter the email addresses you want to receive alert notifications for the Secure Endpoint device. You can use email aliases or specify multiple addresses through a comma-separated list. You can also specify the sender name and email address used by the device. These notifications are not the same as Secure Endpoint Console subscriptions. You can also specify a unique Device Name if you have multiple Secure Endpoint Private Cloud devices. Select on **Next.**



Step 8:

Next you navigate to SSH Keys page, as shown in the image. Select on **Add SSH Key** to enter any public keys you want to add to the device. SSH keys allow you to access the device via a remote shell with root privileges. Only trusted users must be granted access. Your Private Cloud device requires an OpenSSH formatted RSA key. You can add more SSH keys later through **Configuration > SSH** in your Administration Portal. Select on **Next**.



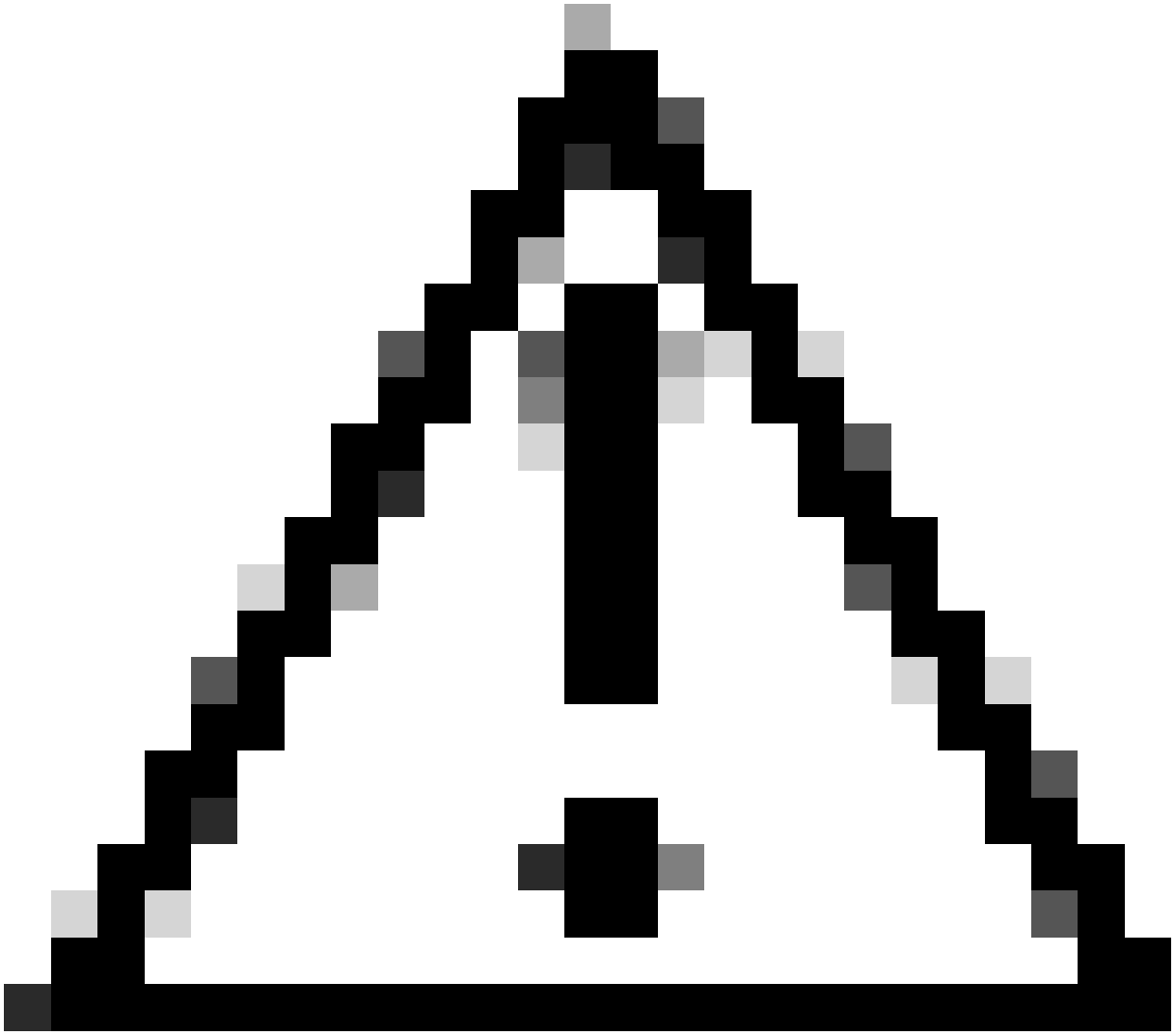
Next you get the Services section. On the next pages you need to assign hostnames and upload the appropriate certificate and key pairs for these device services. In next few slides we can see configuration of one of the 6 certificates.

Services

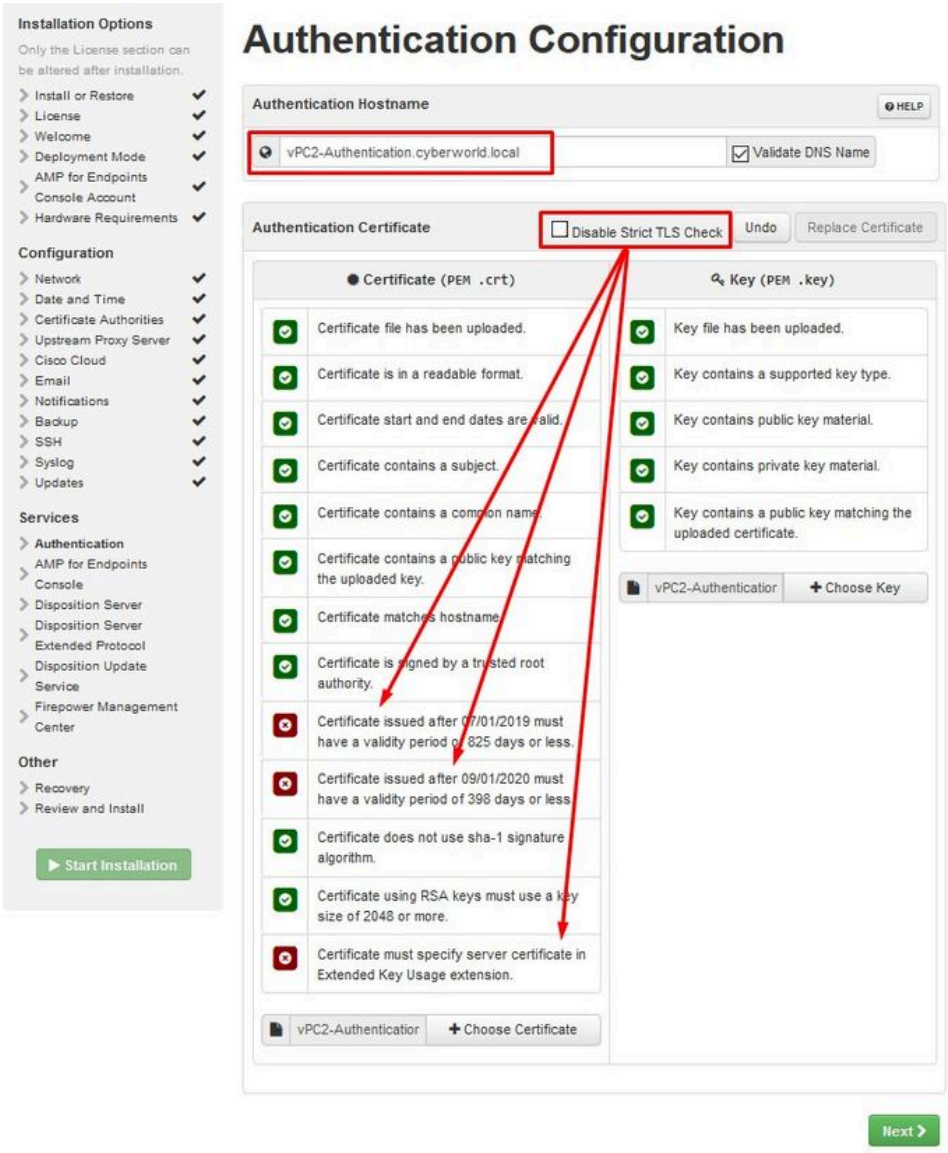
Step 1:

During configuration process you might run in to these errors.

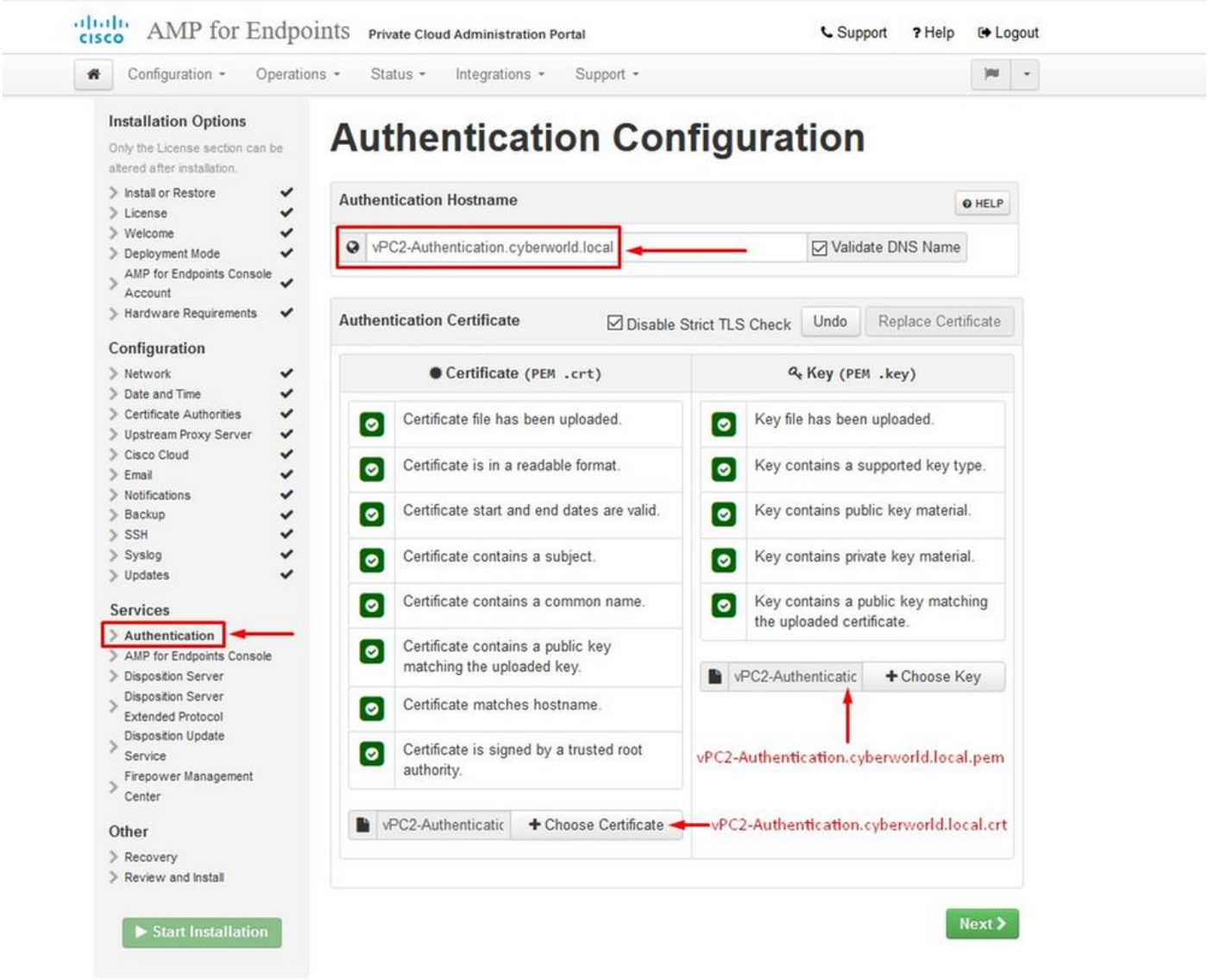
First “error” that you might notice is highlighted with the 3 arrows. To bypass this just simply un-check “**Disable Strict TLS Check**”



Caution: On VPC 3.8.2 and up **TLS Web Server Authentication is now required** for the certificate to be accepted, Service Certificate cannot exceed validity of **398 Days**.



Without Strict TLS Check

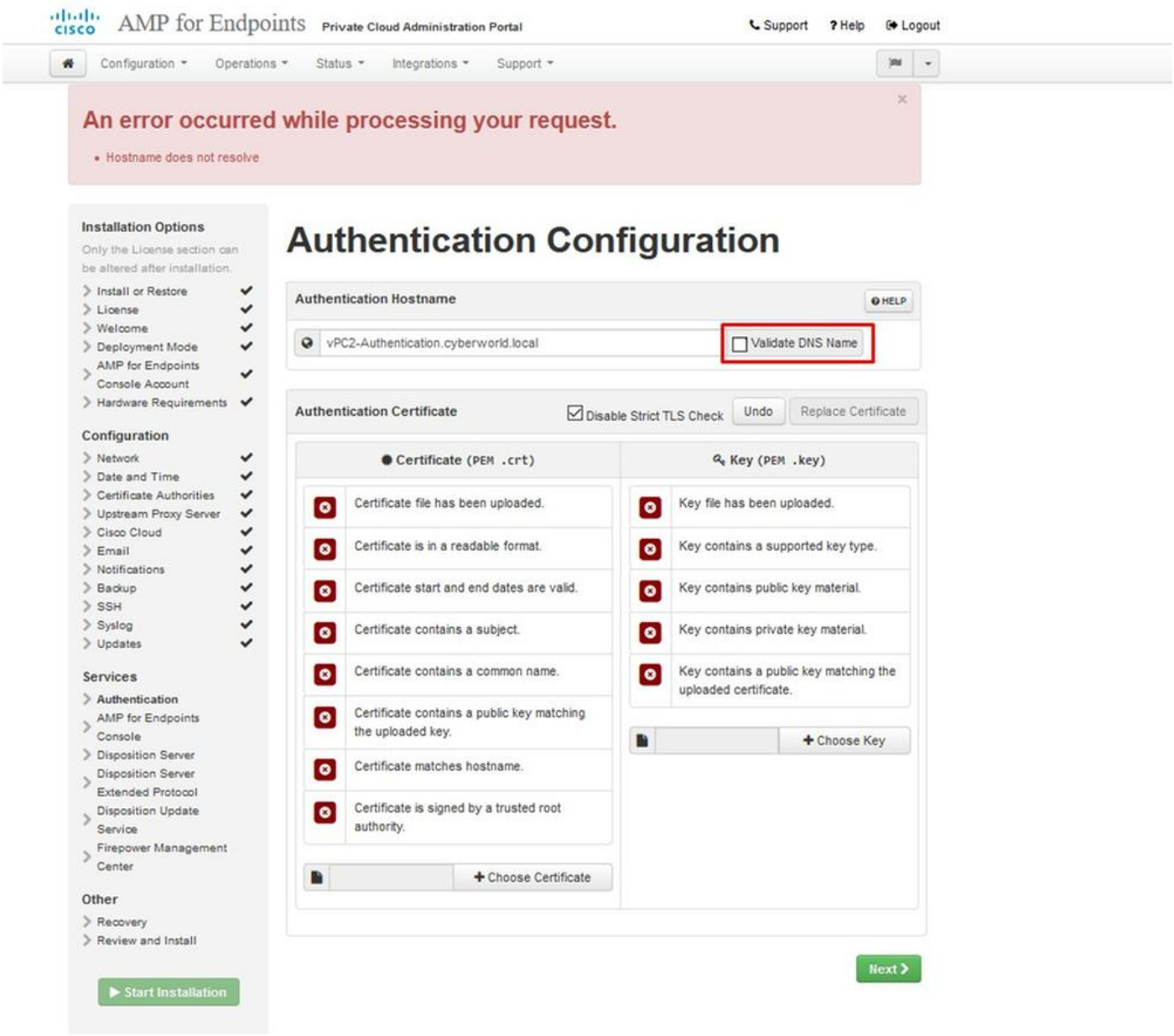


Step 2:

The next error you get is if you leave "**Validate DNS Name**" checked. Here you have two choices.

#1: Either un-check the Validate DNS check mark

#2: Return to your DNS Server and configure rest of your host records.



Now repeat the same process five more times for the rest of the certificates.

Authentication

- The Authentication service be used in future versions of Private Cloud to handle user authentication.

Secure Endpoint Console

- Console is the DNS name where the Secure Endpoint administrator can access the Secure Endpoint Console and Secure Endpoint Connectors receive new policies and updates.

Disposition Server

- Disposition Server is the DNS name where the Secure Endpoint Connectors send and retrieve cloud lookup information.

Disposition Server - Extended Protocol

- Disposition Server - Extended Protocol is the DNS name where newer Secure Endpoint Connectors send and retrieve cloud lookup information.

Disposition Update Service

- Disposition Update Service is used when you link a Cisco Threat Grid appliance to your Private Cloud device. The Threat Grid appliance is used to send files for analysis from the Secure Endpoint Console and the Disposition Update Service is used by Threat Grid to update the disposition *(clean or malicious)* of files after they have been analyzed.

Firepower Management Center

-Firepower Management Center Link lets you link a Cisco Firepower Management Center (FMC) device to your Private Cloud device. This allows you to display Secure Endpoint data in your FMC dashboard. For more information on FMC integration with Secure Endpoint see your FMC documentation.

⚠ Caution: hostnames cannot be changed once the device has finished the installation.

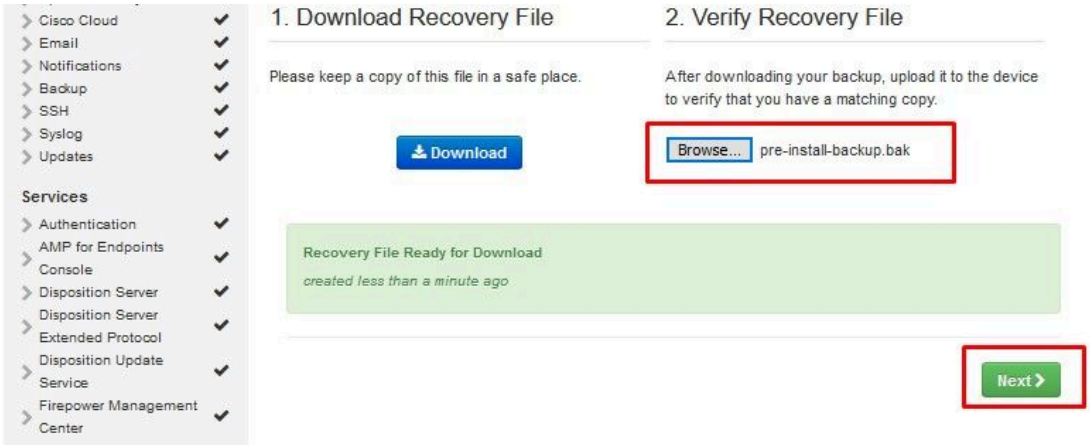
Make a note of the required hostnames. You need to create six unique DNS A records for the Secure Endpoint Private Cloud. Each record points to the same IP Address of the Virtual Private Cloud Console interface (eth1) and must be resolved by both the Private Cloud and the Secure Endpoint.

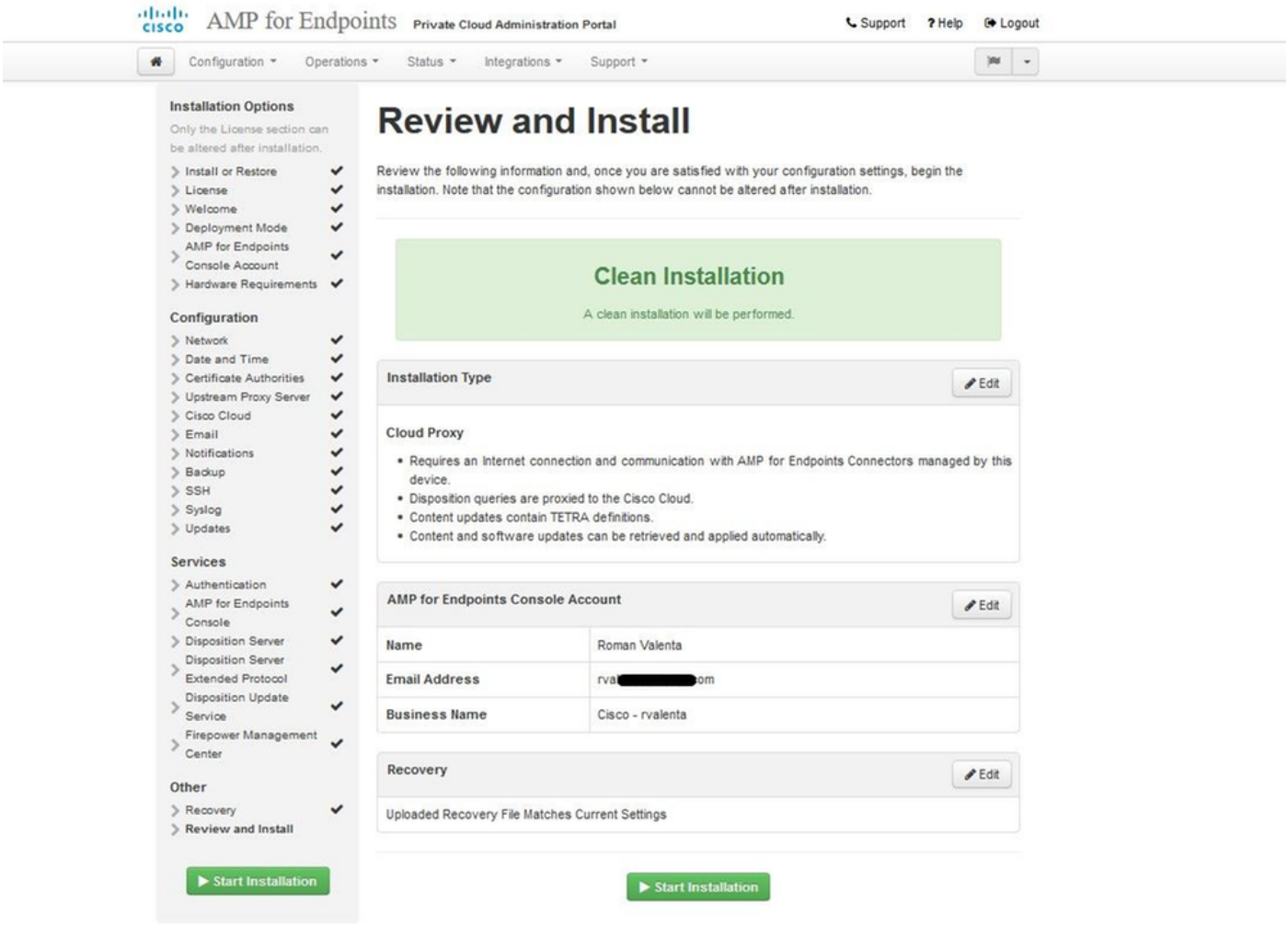
Step 3:

On next page download and then verify **Recovery File**.

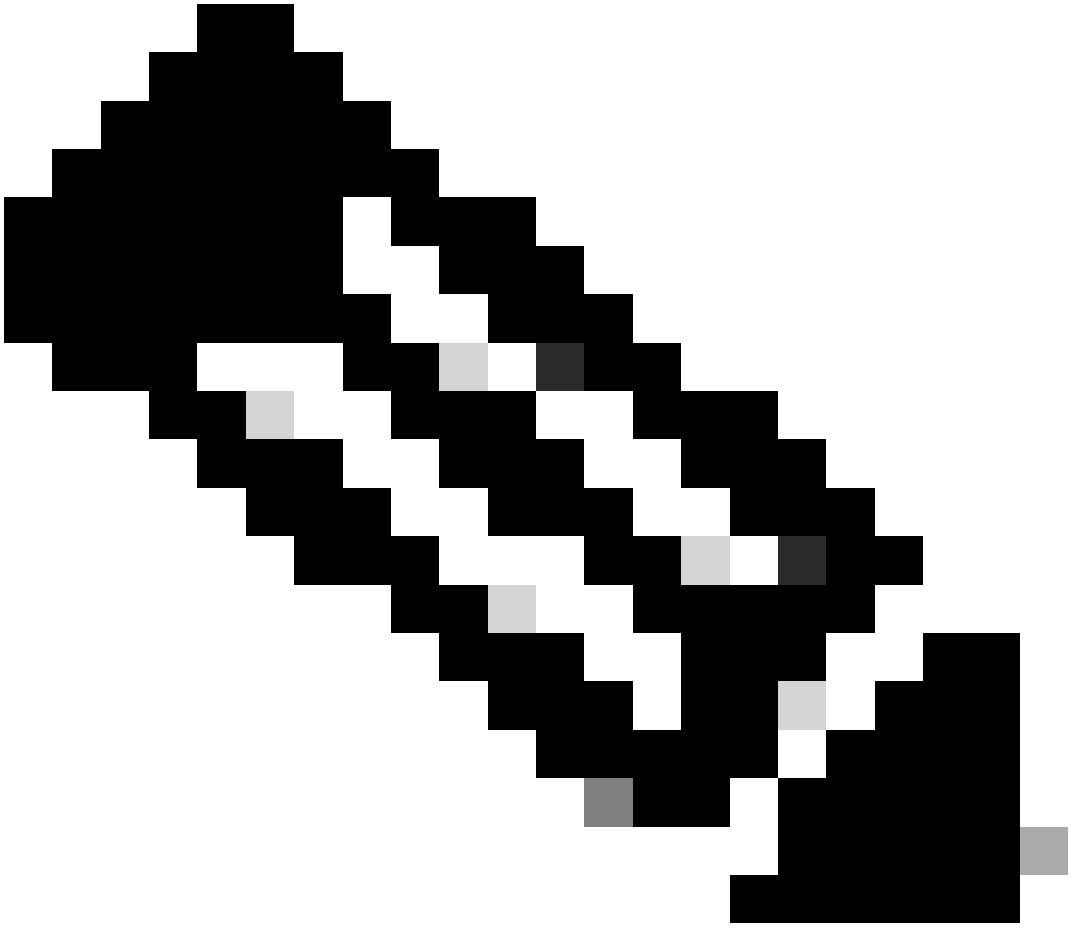
You get the Recovery page, as shown in the image. You must download and verify a backup of your configuration before the start of the installation. The recovery file contains all of the configuration as well as the server keys. If you lose a recovery file, you are unable to restore your configuration and all Secure Endpoint connectors have to be reinstalled. Without an original key, you have to reconfigure the entire private cloud infrastructure with new keys. The recovery file contains all the configurations related to the opadmin portal. The backup file contains the contents of recovery file as well as any dashboard portal data like events, connector history and so on. If you would like to restore just the opadmin without the event data and all, you can use the recovery file. If you restore from the backup file, then the opadmin and dashboard portal data be restored.

Select on **Download** to save the backup to your local computer. Once the file has been downloaded, select on **Choose File** to upload the backup file and verify that it is not corrupt. Select on **Next** to verify the file and proceed.

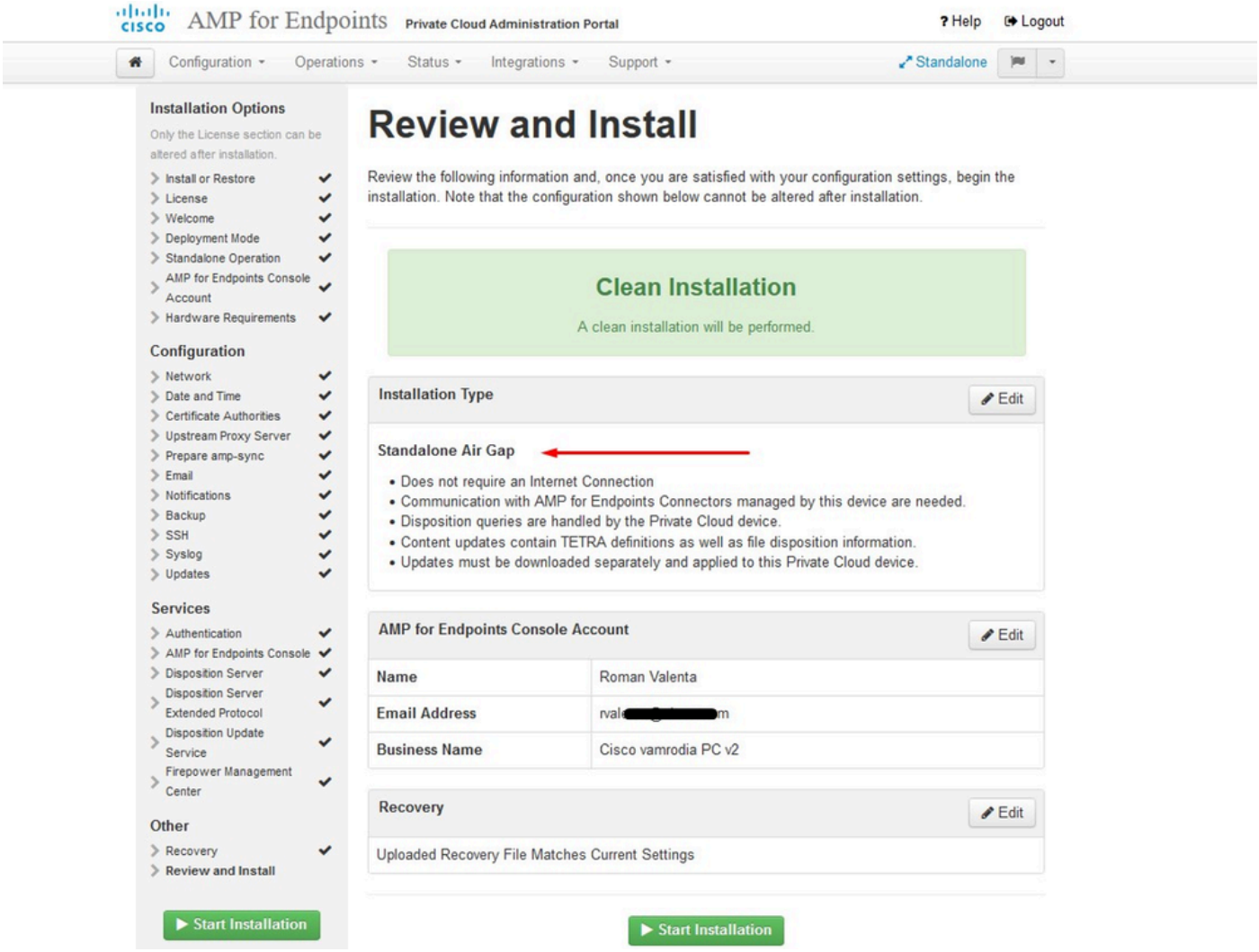



AMP for Endpoints
Private Cloud Administration Portal
Support
Help
Logout
Configuration
Operations
Status
Integrations
Support
Installation Options
Only the License section can be altered after installation.
Install or Restore
License
Welcome
Deployment Mode
AMP for Endpoints Console Account
Hardware 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
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
Edit
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.
AMP for Endpoints Console Account
Edit
Name
Roman Valenta
Email Address
Business Name
Cisco - rvalenta
Recovery
Edit
Uploaded Recovery File Matches Current Settings
Start Installation

⌄⌄ AIRGAP ONLY ⌄⌄



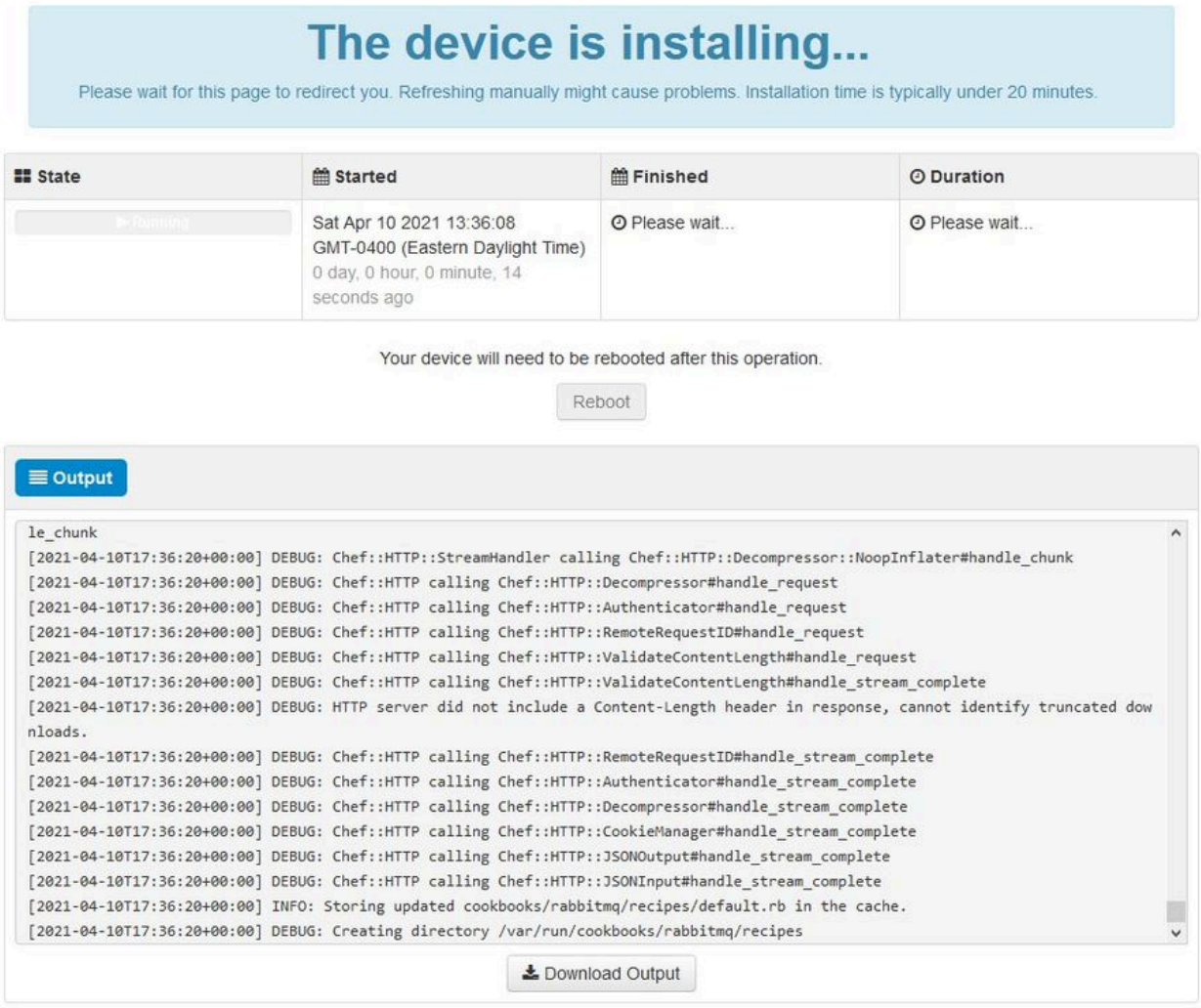
Note: These steps are applicable only for physical appliance.



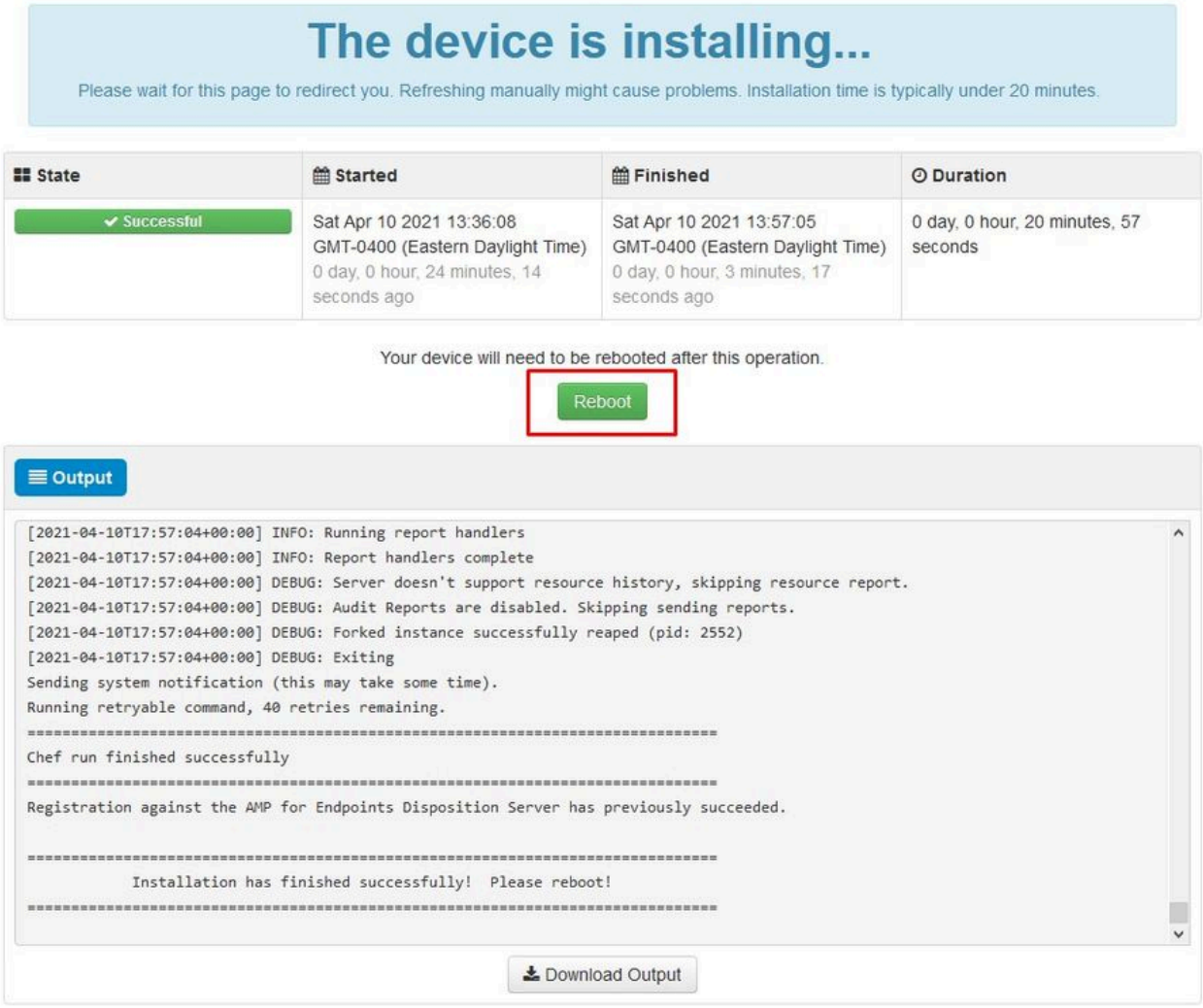
⩓ ⩓ AIRGAP ONLY ⩓ ⩓

You see similar input like this…

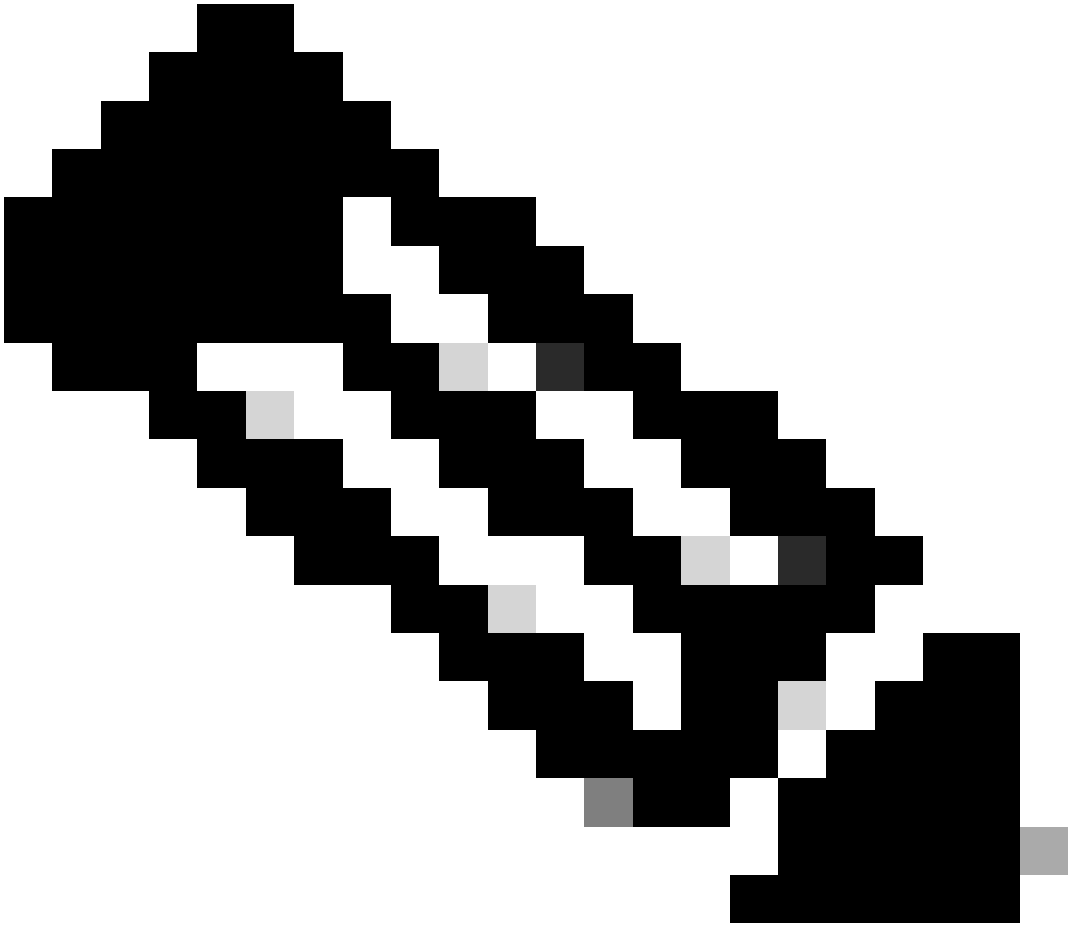
⚠ **Caution**: When you are on this page do not refresh as it can cause issues.



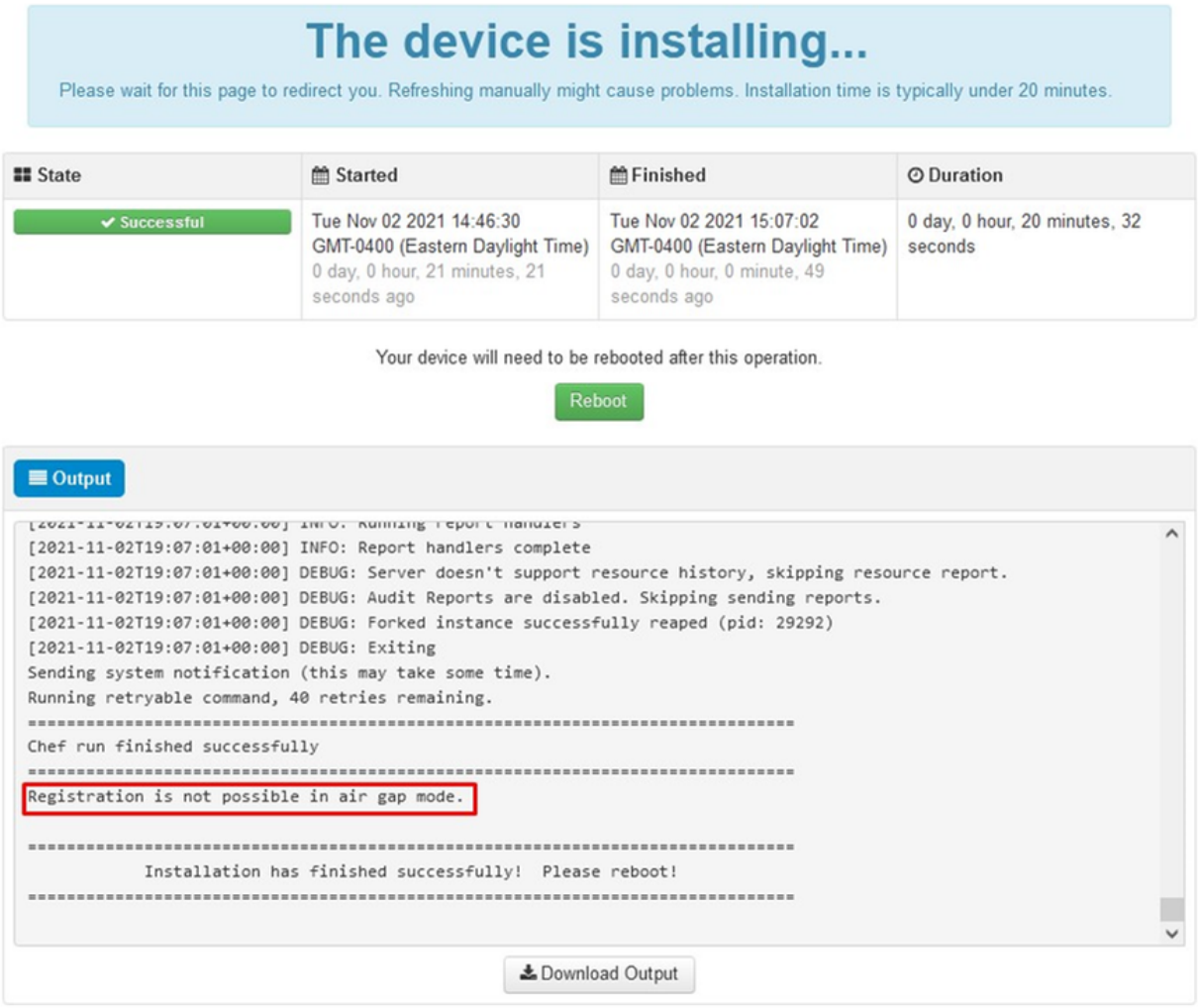
Once the installation is done hit the reboot button


The device is installing...
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 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, 20 minutes, 57 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

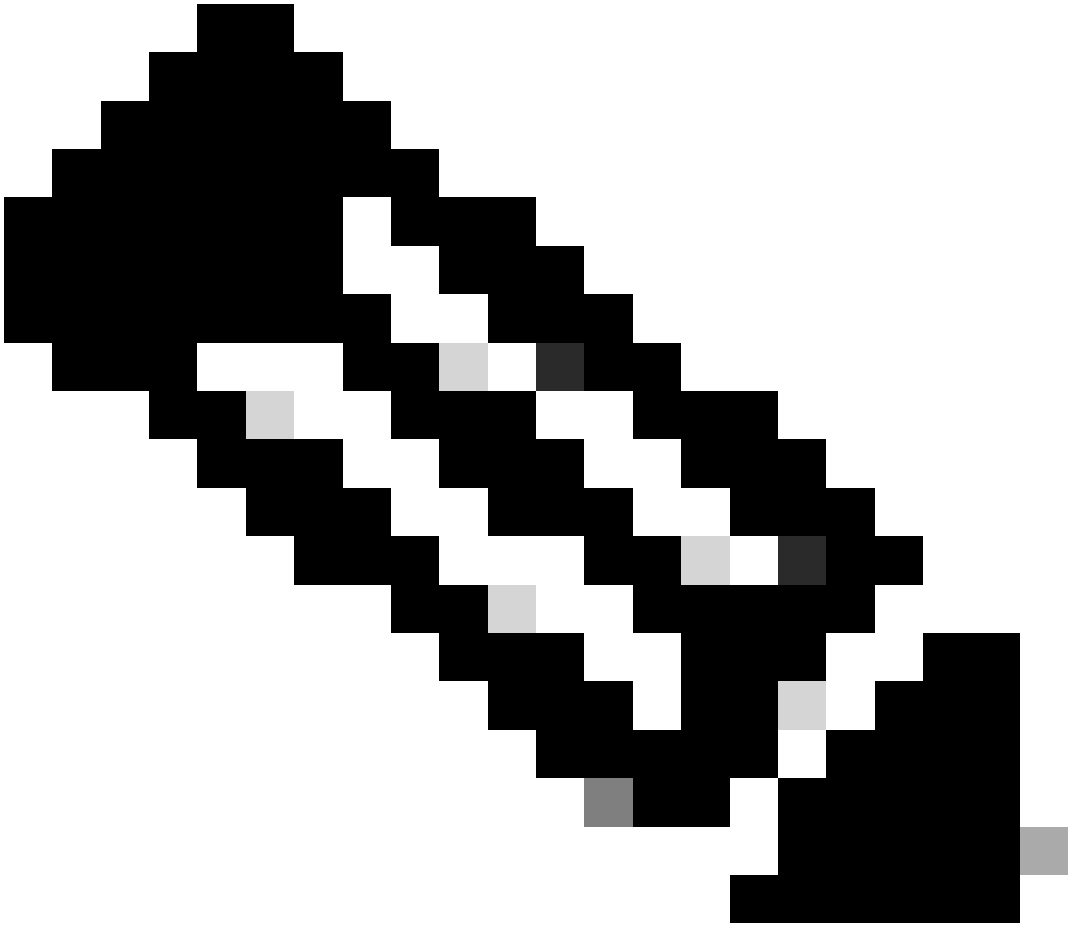
AIRGAP ONLY



Note: These steps are applicable only for physical appliance.

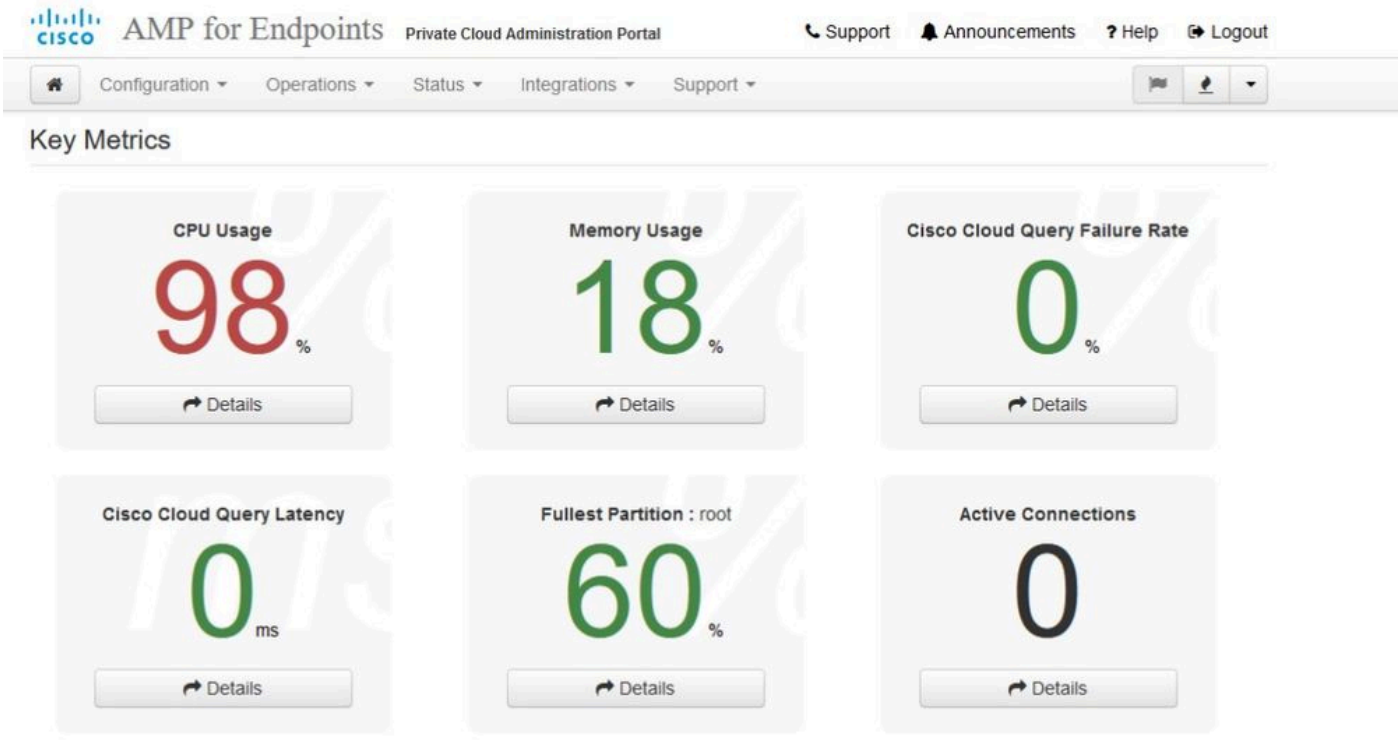

The device is installing...
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.
State
Started
Finished
Duration
Successful
Tue Nov 02 2021 14:46:30 GMT-0400 (Eastern Daylight Time)
0 day, 0 hour, 21 minutes, 21 seconds 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 hour, 20 minutes, 32 seconds
Your device will need to be rebooted after this operation.
Reboot
Output
[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

⩓ ⩓ AIRGAP ONLY ⩓ ⩓

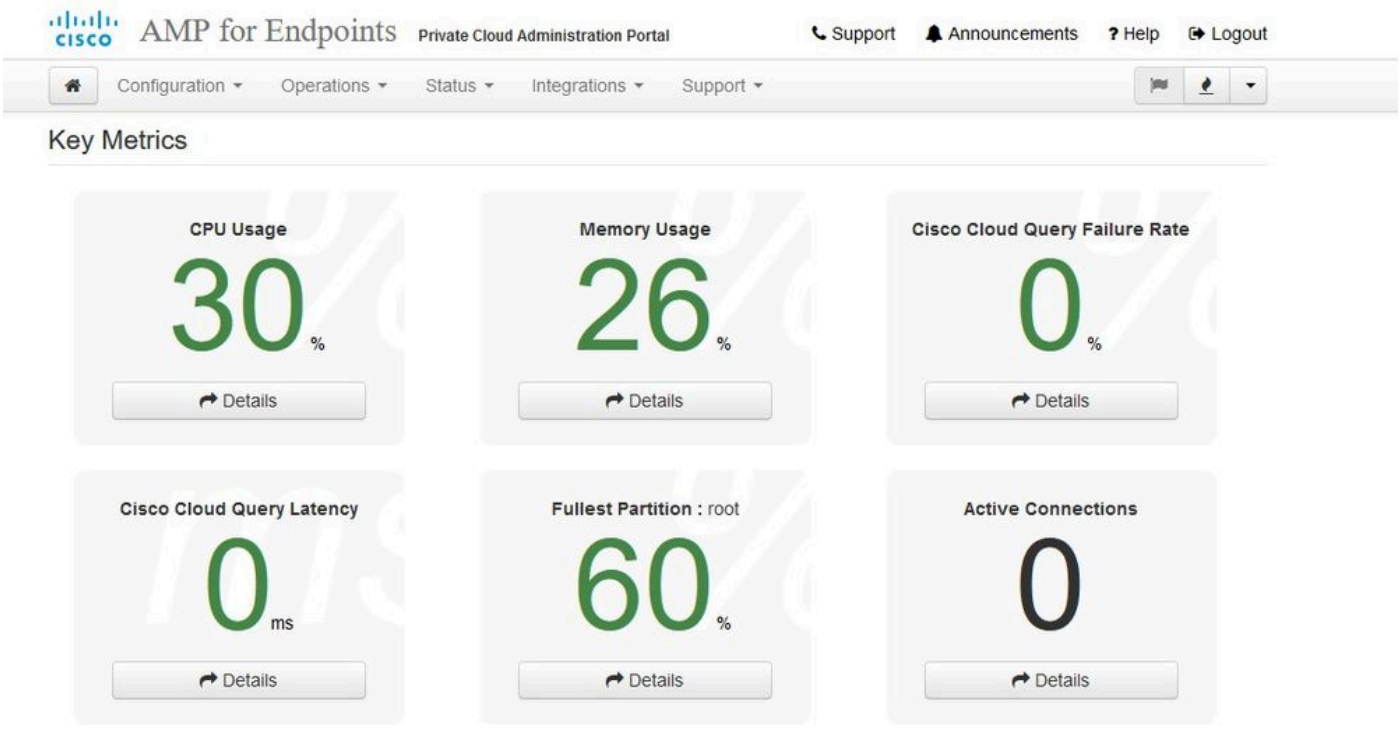


Note: These steps are applicable only for physical appliance.

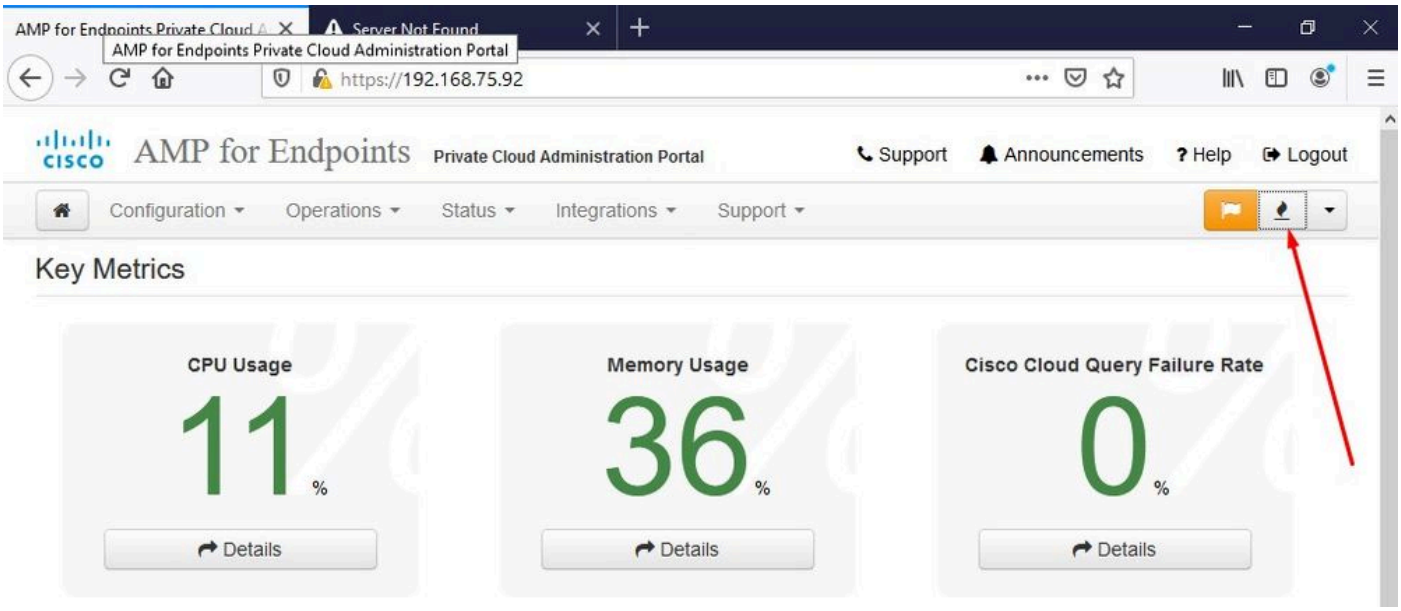
Once the appliance is fully booted, next time you log in with your admin interface you get presented with this dashboard. You might notice high CPU at the beginning but if you give few minutes it gets settle down.



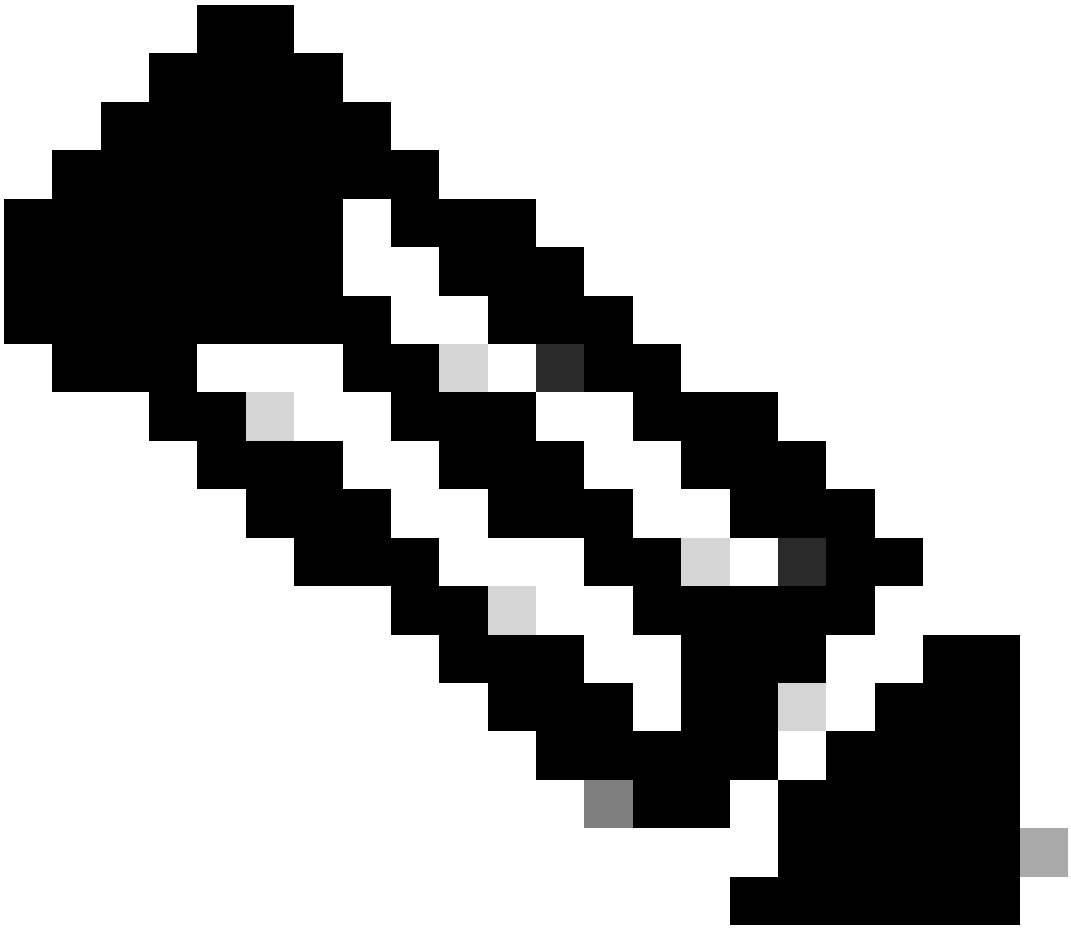
After few minutes...



From here you navigate to Secure Endpoint console. Click on the little icon that looks like fire in right corner next to the flag.

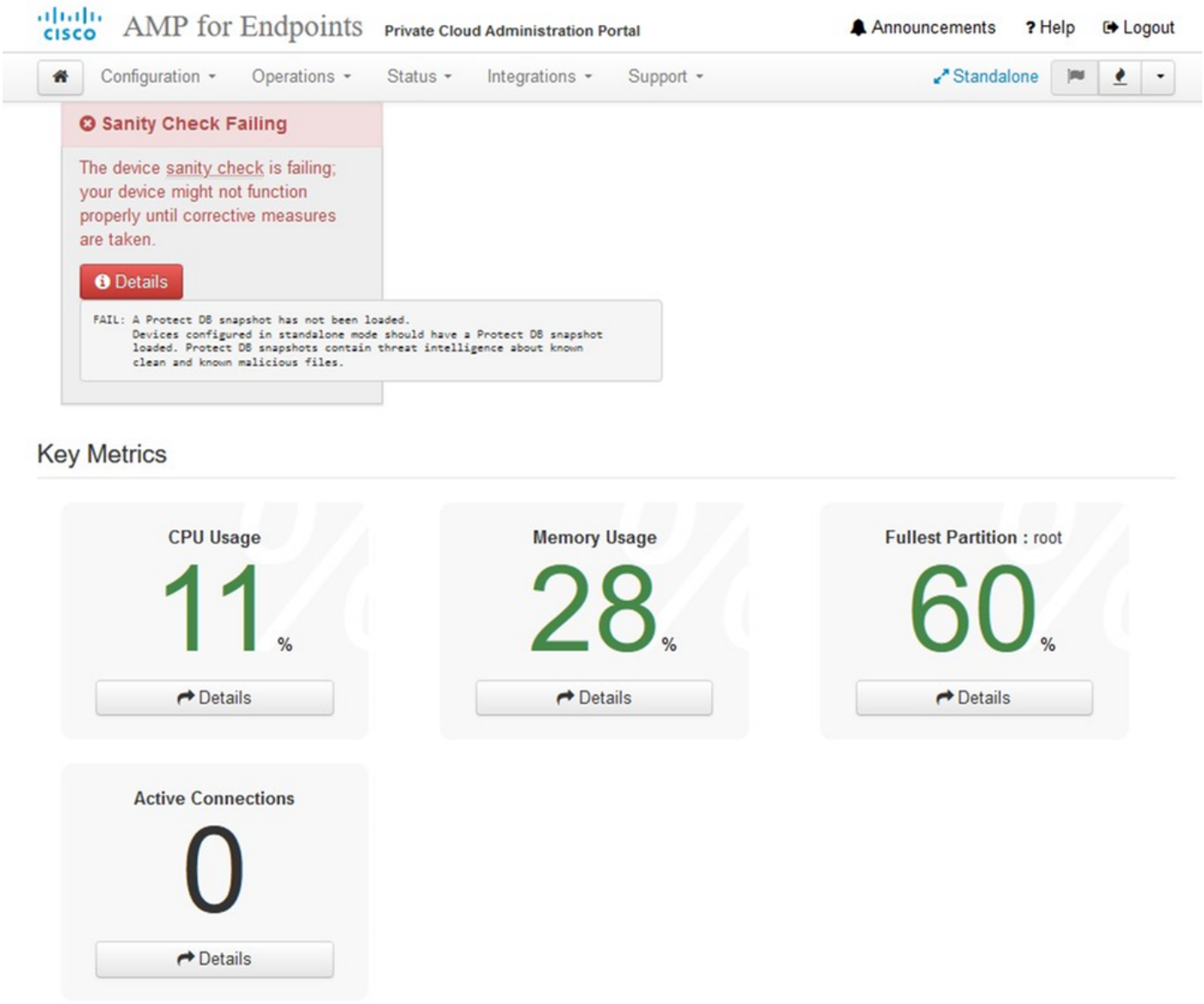

AMP for Endpoints Private Cloud
Server Not Found
AMP for Endpoints Private Cloud Administration Portal
https://192.168.75.92
AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Key Metrics
CPU Usage
11 %
Details
Memory Usage
36 %
Details
Cisco Cloud Query Failure Rate
0 %
Details

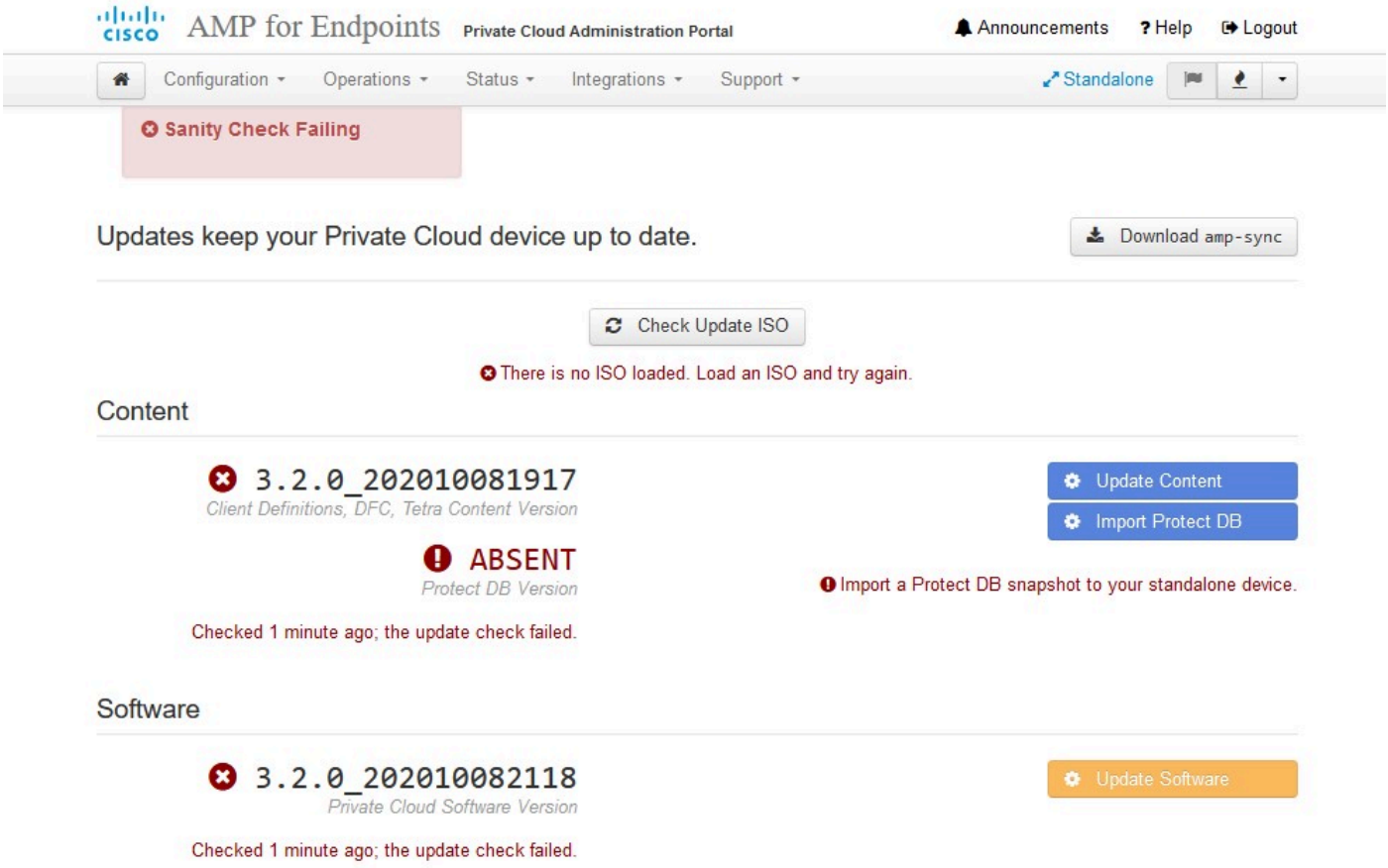
AIRGAP ONLY



Note: These steps are applicable only for physical appliance.

As you can see, we failed sanity check due to **DB Protect Snapshot** , also Client Definitions, DFC and Tetra. This must be done by offline update via downloaded ISO file previously prepared through **amp-sync** and uploaded to NFS location.





AirGap Update Package

For the first time we have to use this command in order to receive the Protect DB

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

Note: Download all the packages via this command and then verify could take **long time**. Depend on the speed and link quality. In my case with 1Gig fiber it still end up take almost 25hrs to complete. Partially this is also due to fact that this download is directly from AWS and hence is throttled. Lastly note that this download is rather big. In my case the downloaded file was **323GB.**

In this example we used **CygWin64**

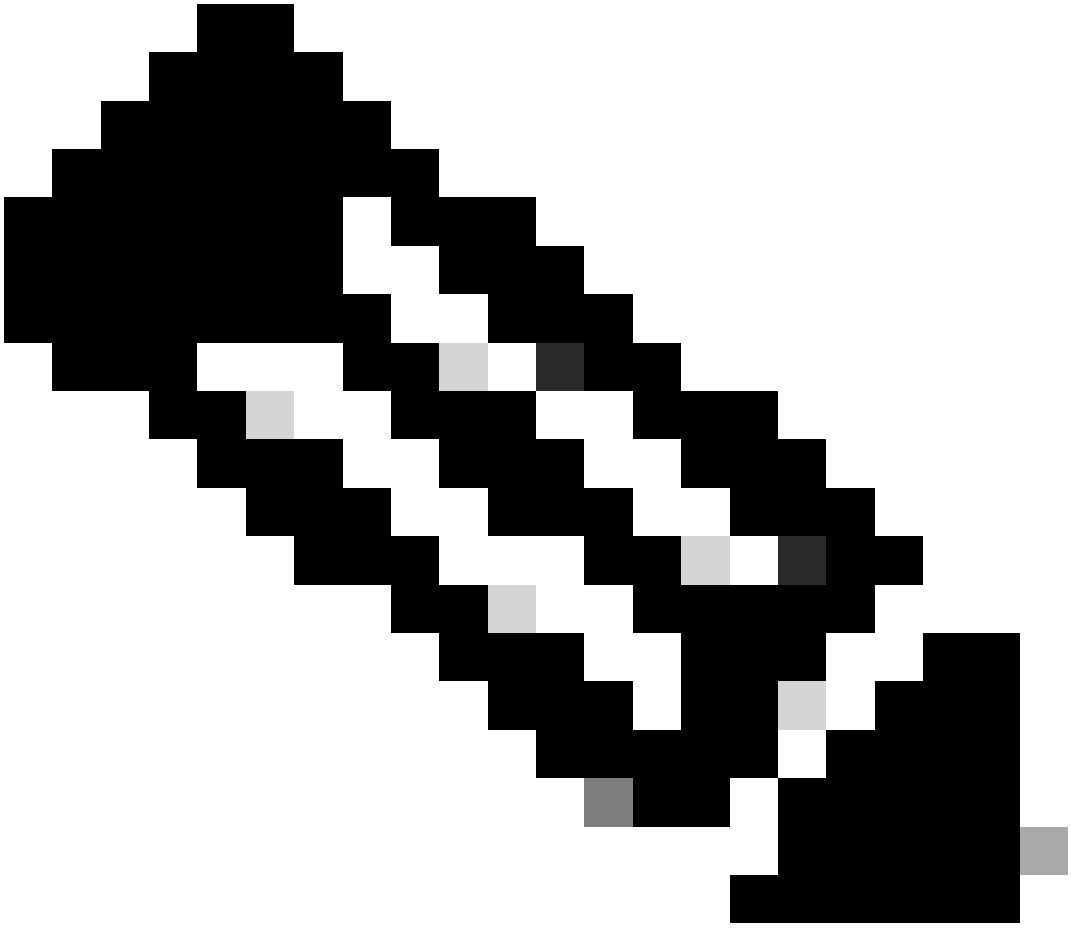
1. Download and install the x64 version of Cygwin.
2. Run setup-x86_64.exe and go through the installation process choose all the defaults.
3. Choose a download mirror.
4. Select packages to install:
All -> Net -> curl
All -> Utils -> genisoimage
All -> Utils -> xmlstarlet
*** VPC 3.8.x up - > xorriso**

```
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/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
  % 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/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee43a89240ea0-other.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
  % 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/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bbccb2c2f41d8-filelists.xml.gz
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
  % 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/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3dbe472d84ff9-filelists.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
  % 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/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101d0eab569014-primary.sqlite.bz2
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913cdb4a7ff069-primary.xml.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 54480  100 54480    0     0   383k      0 --:--:-- --:--:-- --:--:--  385k
```

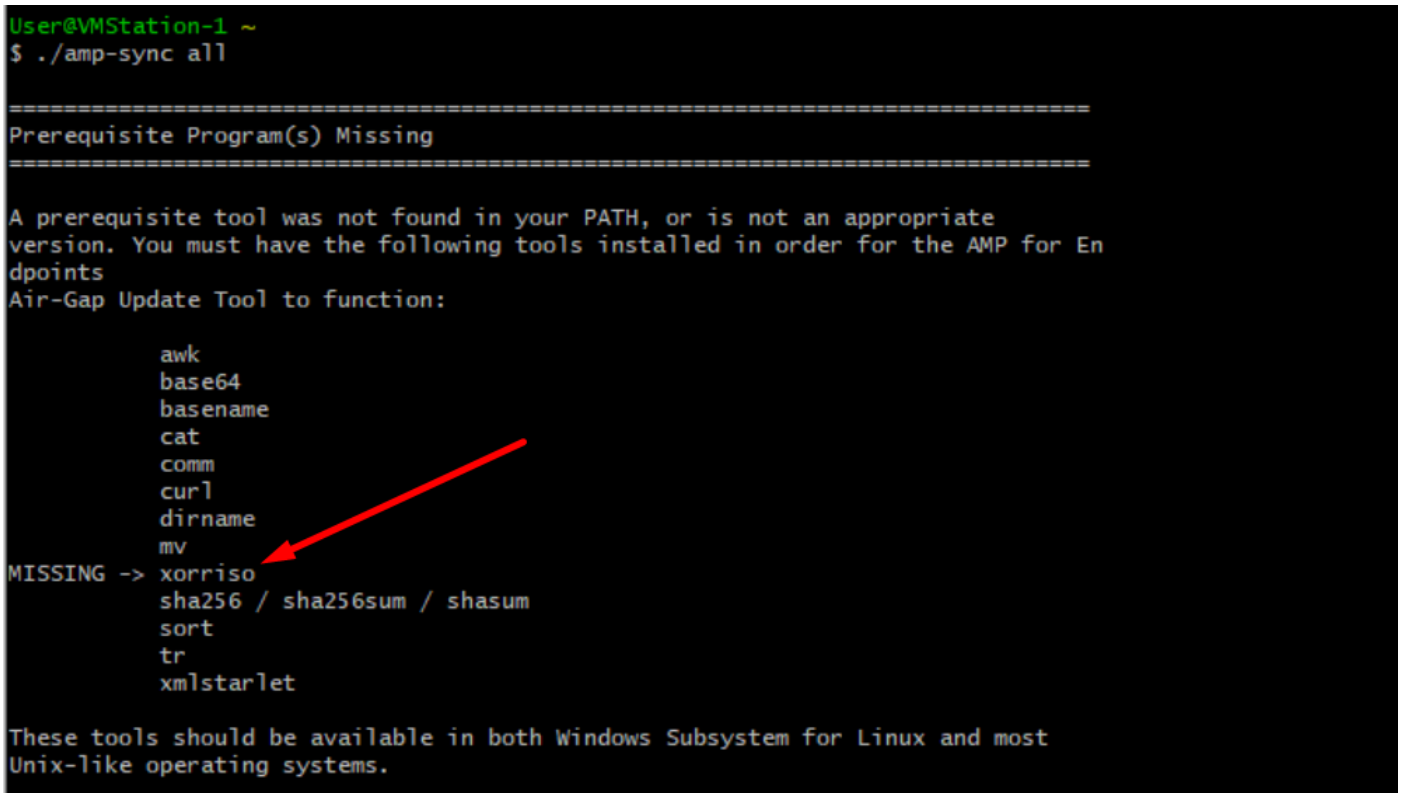
```
 99.91% done, estimate finish Thu Nov  4 08:39:50 2021
 99.91% done, estimate finish Thu Nov  4 08:39:51 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:50 2021
 99.92% done, estimate finish Thu Nov  4 08:39:51 2021
 99.93% done, estimate 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 ~
$
```



Note: In the newest update VPC 3.8.x with CygWin64 as your main downloading tool you can encounter this issue described below.



Release notes Page #58. As you can see "**xorriso**" is now required. We changed the format of the ISO to the ISO 9660 and that dependency is what converts the image to proper format so the update can complete. Unfortunately, CygWin64 do not offer xorriso in any of their built-in repositories. However, for those that would still like to use CygWin64 there is a way to overcome this issue.

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.

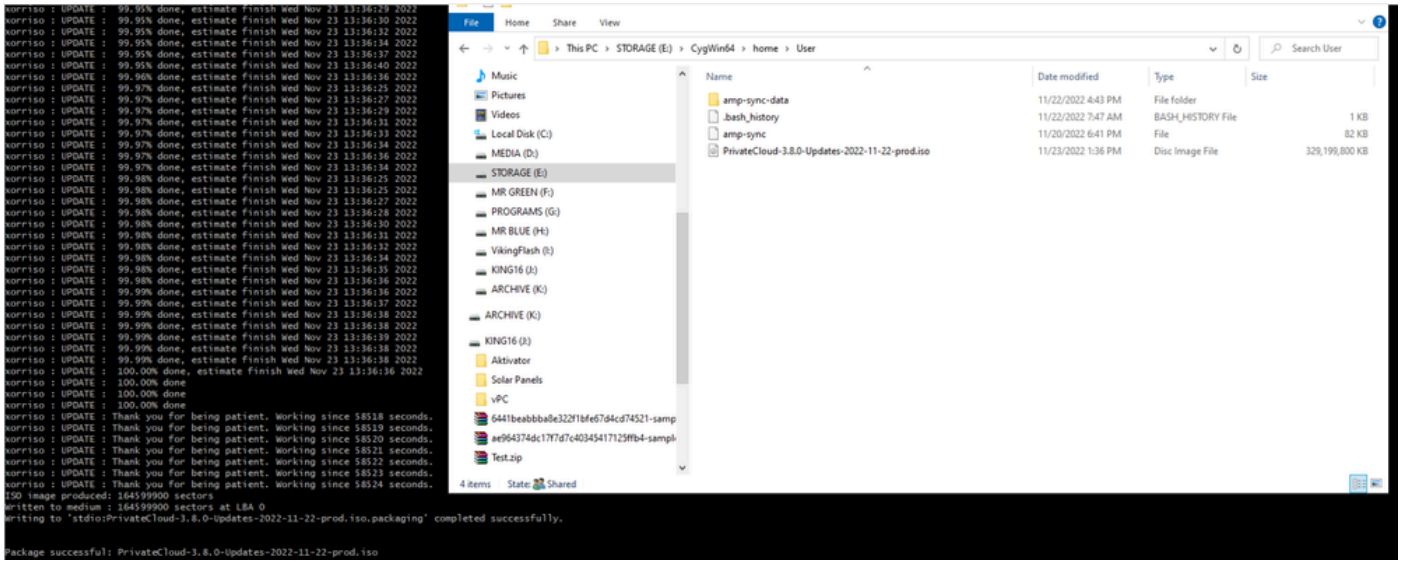
```
> sudo apt install xorriso
> sudo apt install xmlstarlet
```

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
```

To be able use CygWin once again you must to manually download xorriso from GitHub repository. Open your browser and type <**Latest xorriso.exe 1.5.2 pre-build for Windows**> it should come up as first link named as <**PeyTy/xorriso-exe-for-windows – GitHub**> navigate to that GitHub page and download <**xorriso-exe-for-windows-master.zip**> file inside of the zip file you find among few other file named <**xorriso.exe**> copy and paste this file in to <**CygWin64\bin**> path of your local CygWin installation. Try again run <**amp-sync**> command. You should no longer see the error message and download start and finish as shown in the picture.

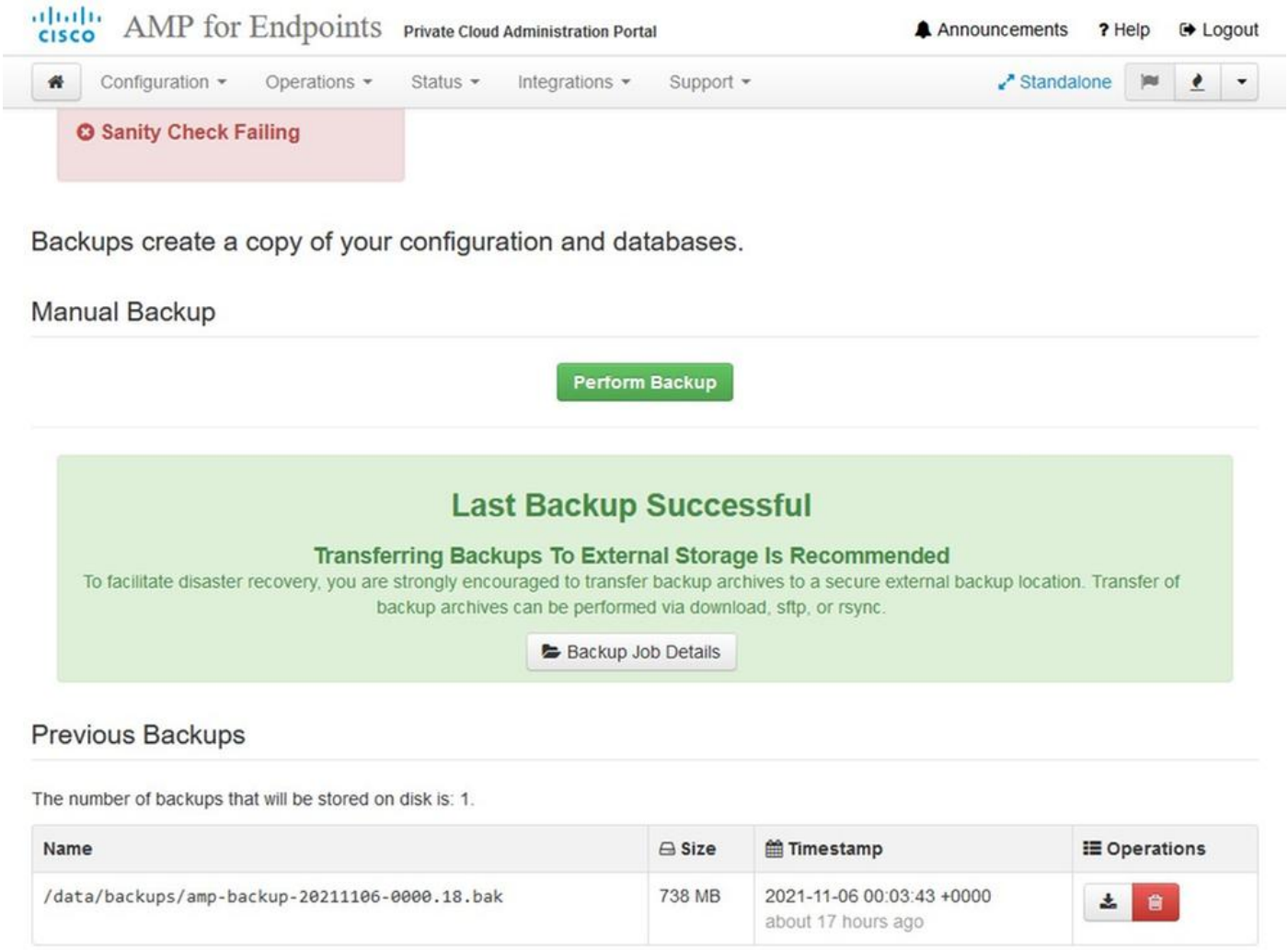


Perform the backup of the current *(in this case)* 3.2.0 VPC in Airgap Mode.

You can use this command form CLI

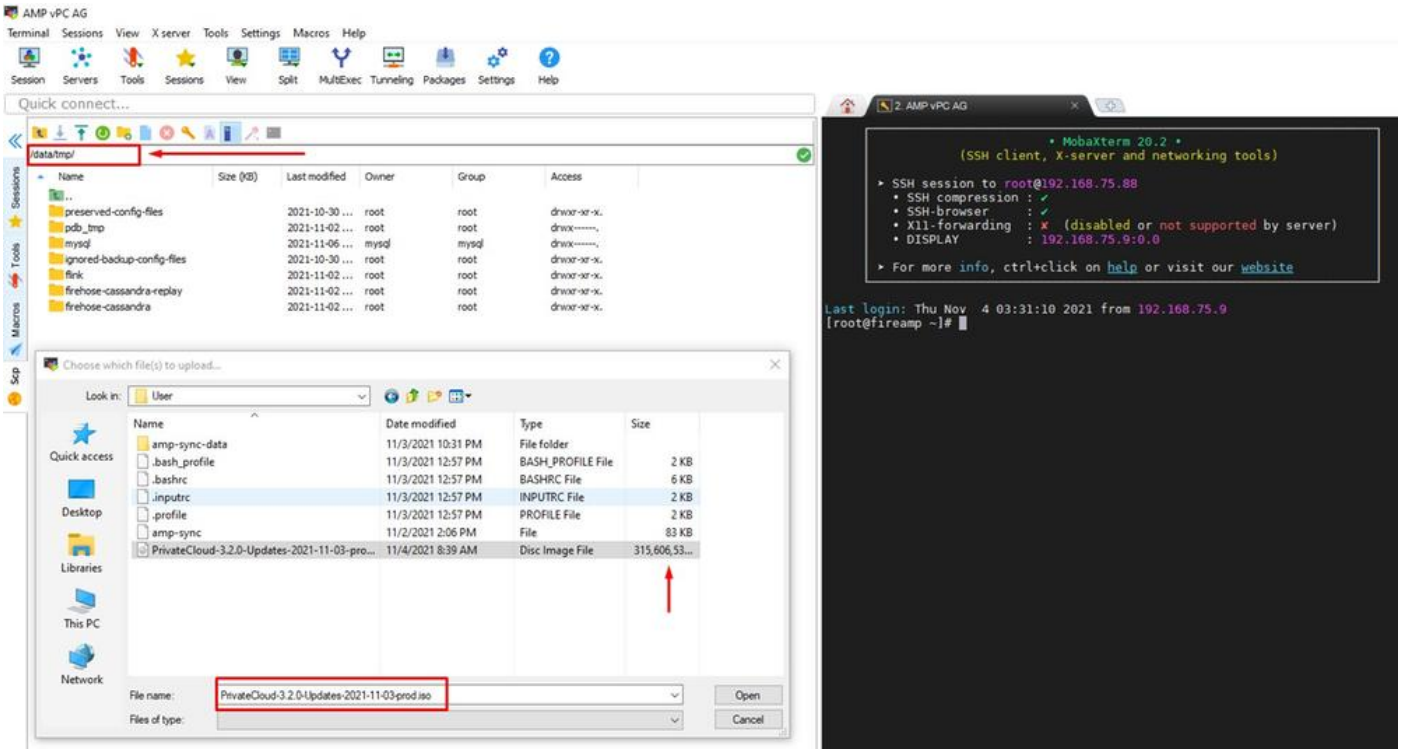
```
rpm -qa | grep Pri
```

Or you can also Navigate to **Operations > Backups**, as shown in the image and **Perform Backup** there.



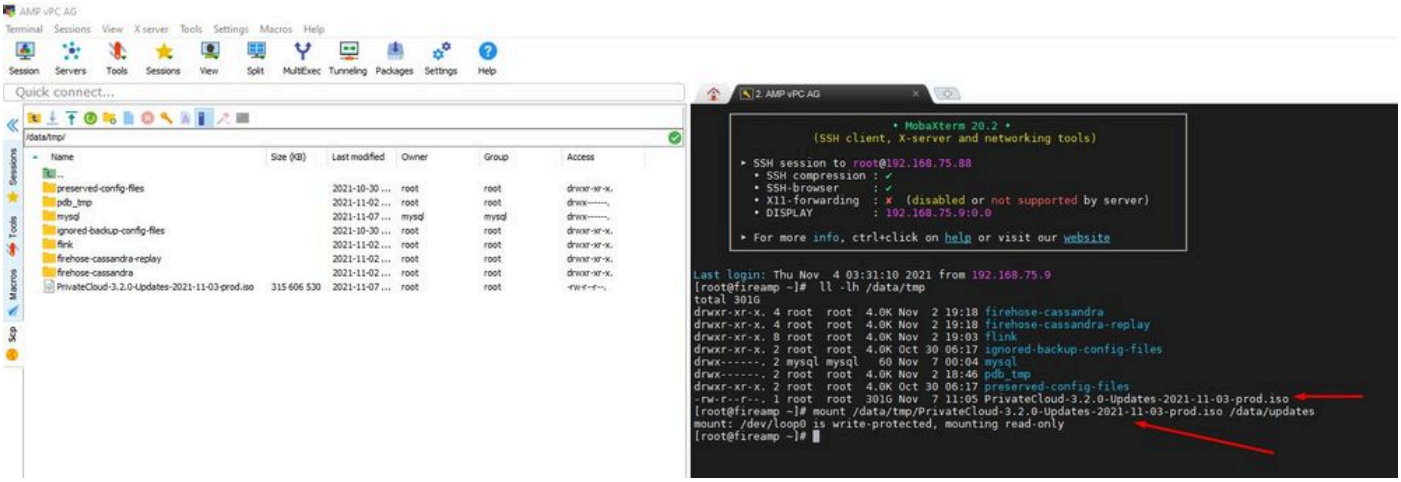
Transfer the latest ISO generated with amp-sync to the VPC. This can take up to several hours as well based on your speed. In this case the transfer took over 16Hrs

`/data/tmp`

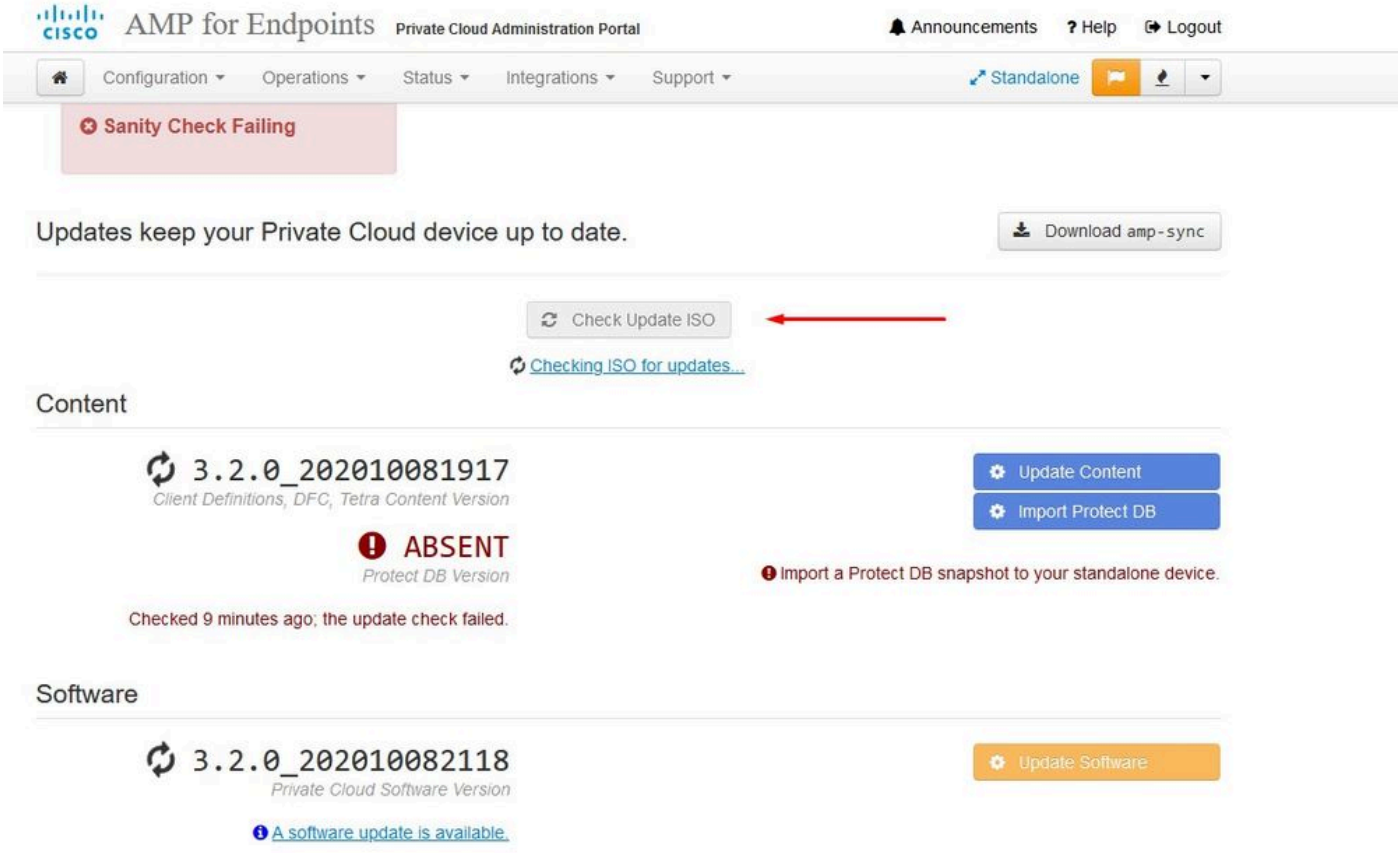


After the upload is done mount the ISO

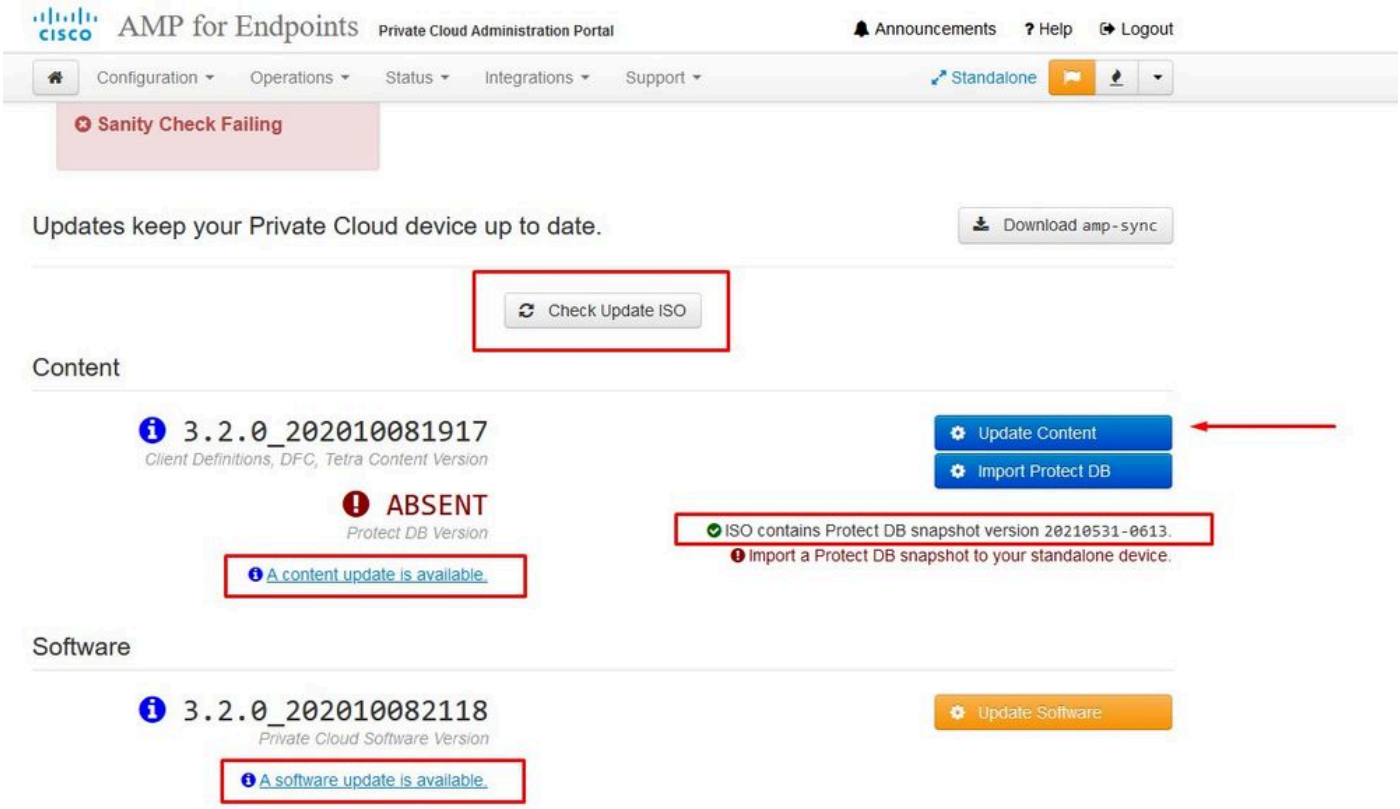
```
mount /data/tmp/PrivateCloud-3.2.0-Updates-2021-11-03-prod.iso /data/updates/
```



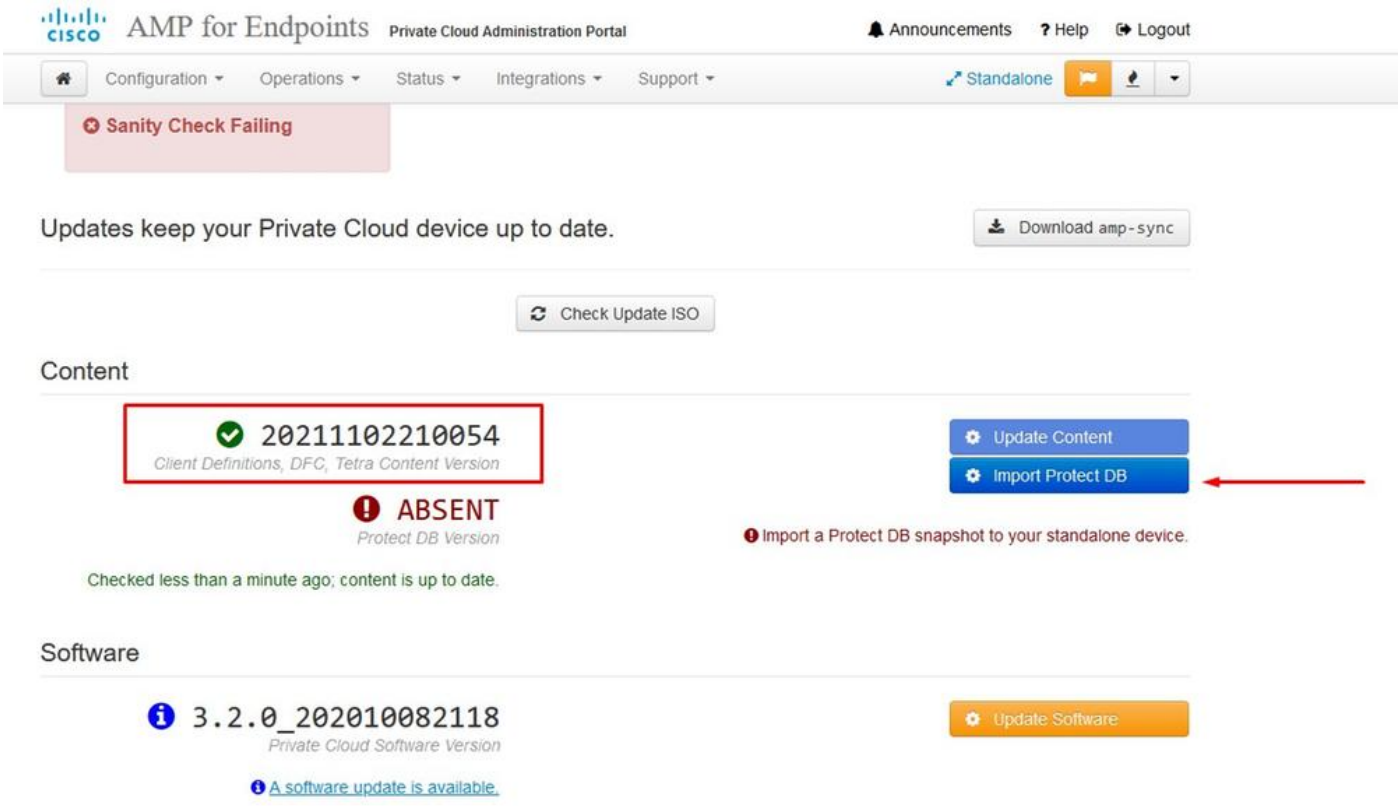
Navigate to opdamin UI to perform the update **Operations > Update Device > Select Check update ISO.**



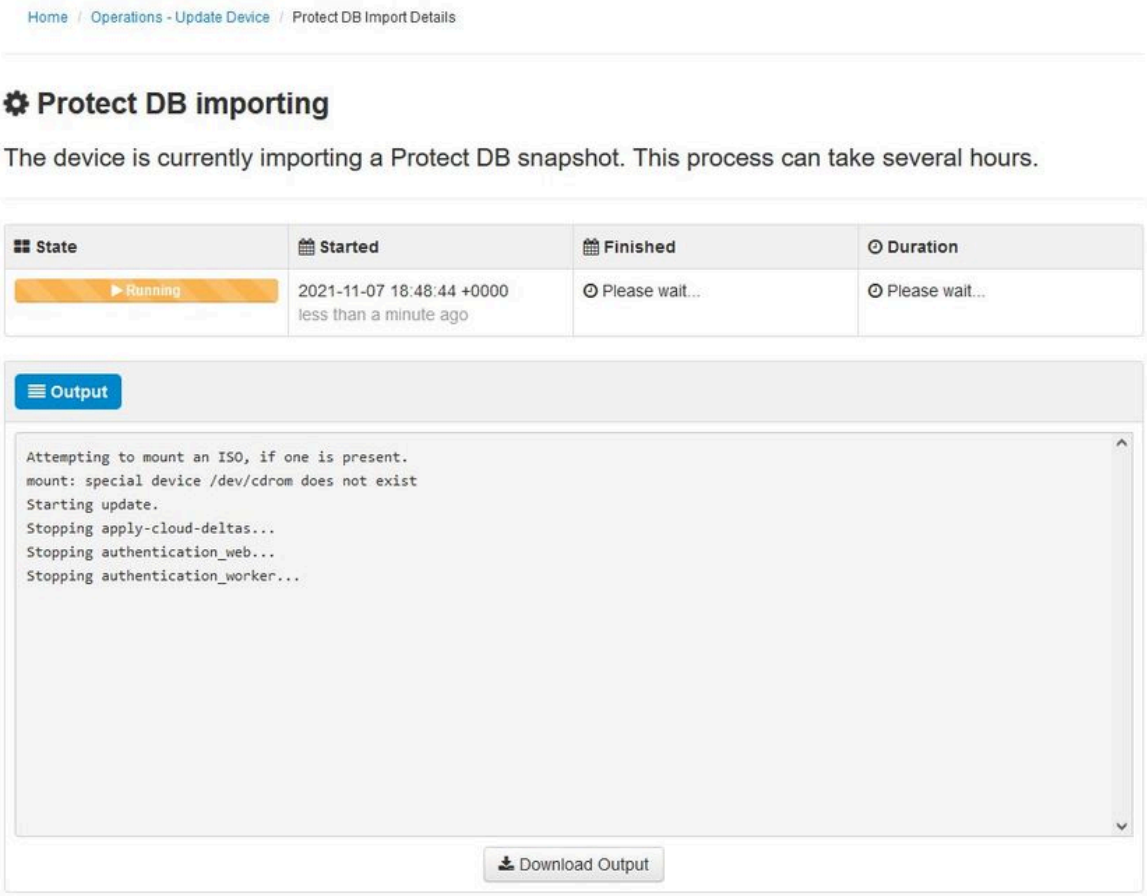
In this example I proceed with **Update Content** first



Then select Import Protect DB.



As you can see this is another very lengthy process that can take long time to complete.



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 hours.

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

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:   0:00:00   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).
```

Problem #1 - Exhausted room in Data Store

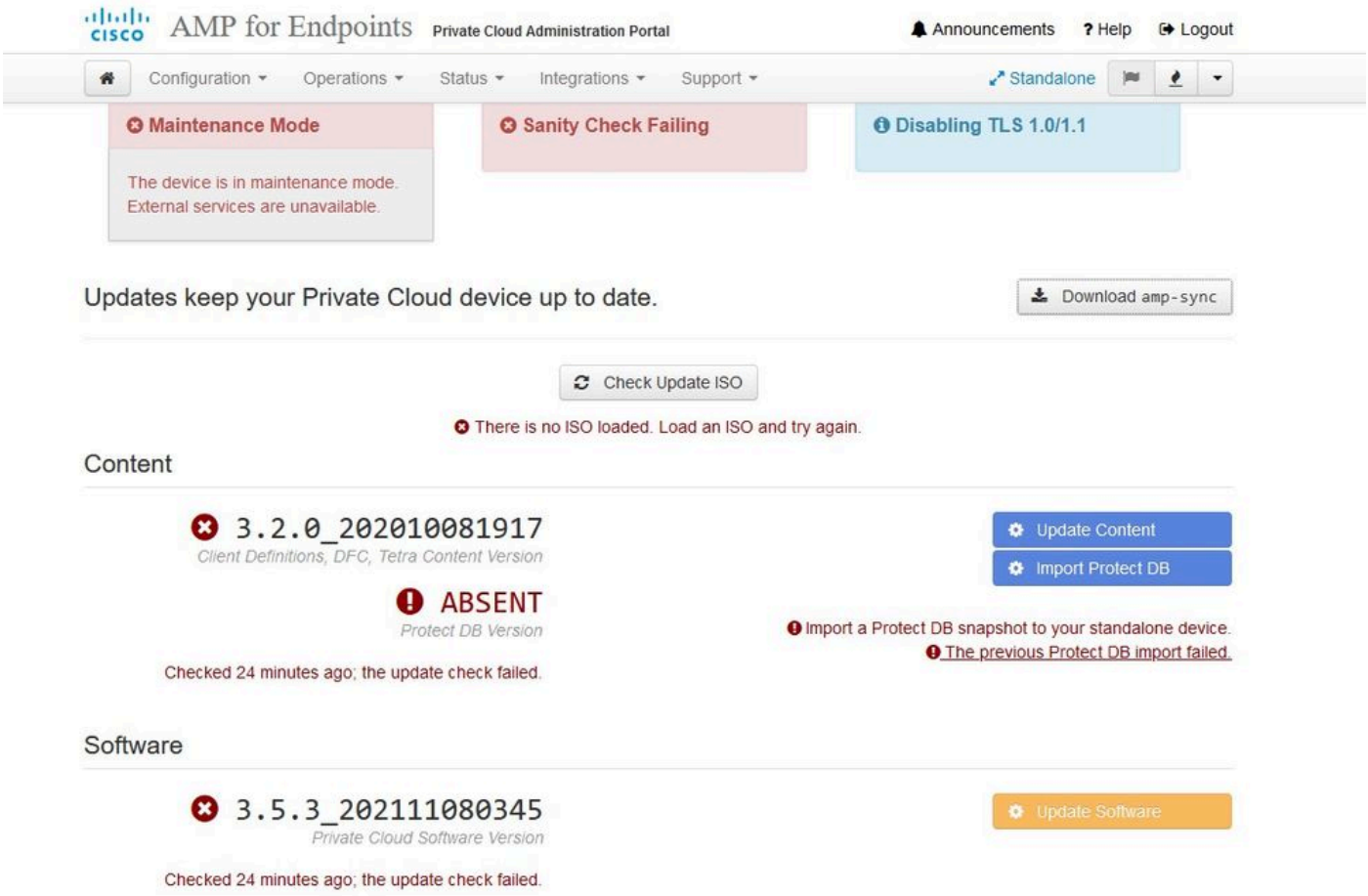
Here you can ran in to two issues. Since vPC prior to 3.5.2 don't have the ability to mount external NFS storage you have to upload the update ISO file to the **/data/temp** directory. In my case since my datastore was only 1TB I ran out of the room and the VM crashed. In other words you need at least 2TB of space on your Data Store to successfully deploy AirGap VPC that is bellow version 3.5.2

This image bellow is from the ESXi server which shows the error that there is no more available space on the HDD when you try to boot the VM. I was able to recover from this error by temporary switch the 128 GB RAM to 64GB. Then I was able to boot up again. Also remember that if you provision this VM as Thin Client the downside of the Thin Client deployment is that disk size can grow, but it wouldn't shrink even if you free up some space. In other word let’s say you uploaded your 300GB file to the directory of the vPC and then deleted. The disk in ESXi still show 300GB less space on your HDD

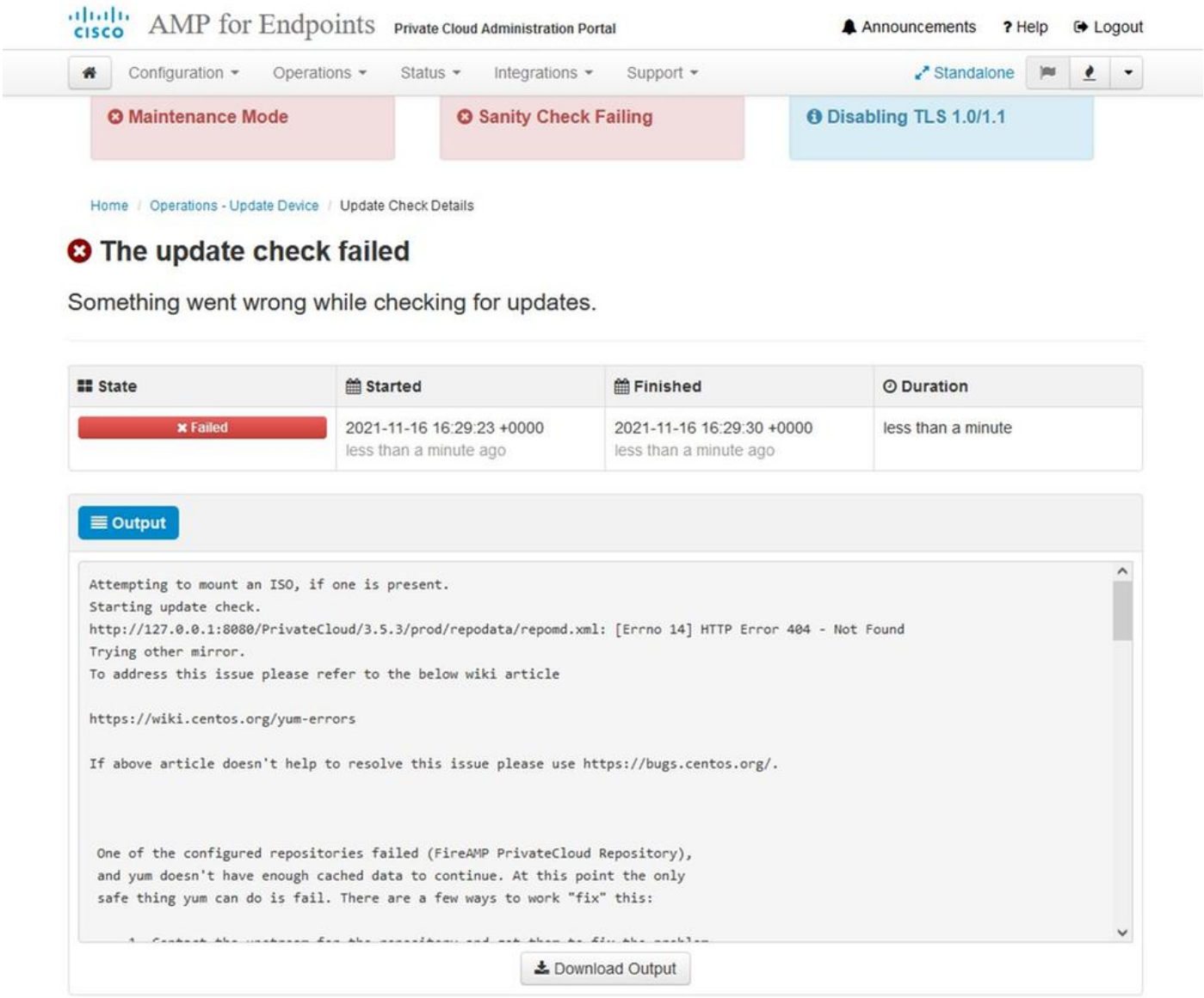


Problem #2 - Old Update

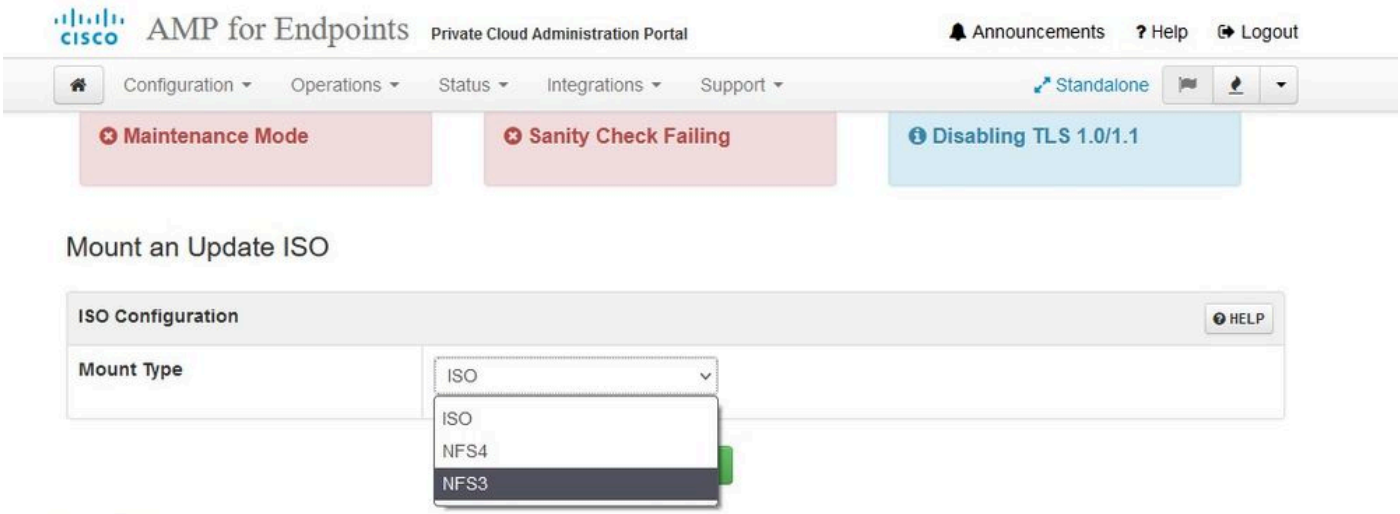
The 2nd problem is if you run the software update first like I did in my 2nd trial and from 3.2.0 I end up with VPC to upgrade to 3.5.2 and because of that I had to download brand new ISO update file since the 3.2.0 become invalid due to a fact that I was no longer on the original 3.2.0 version.

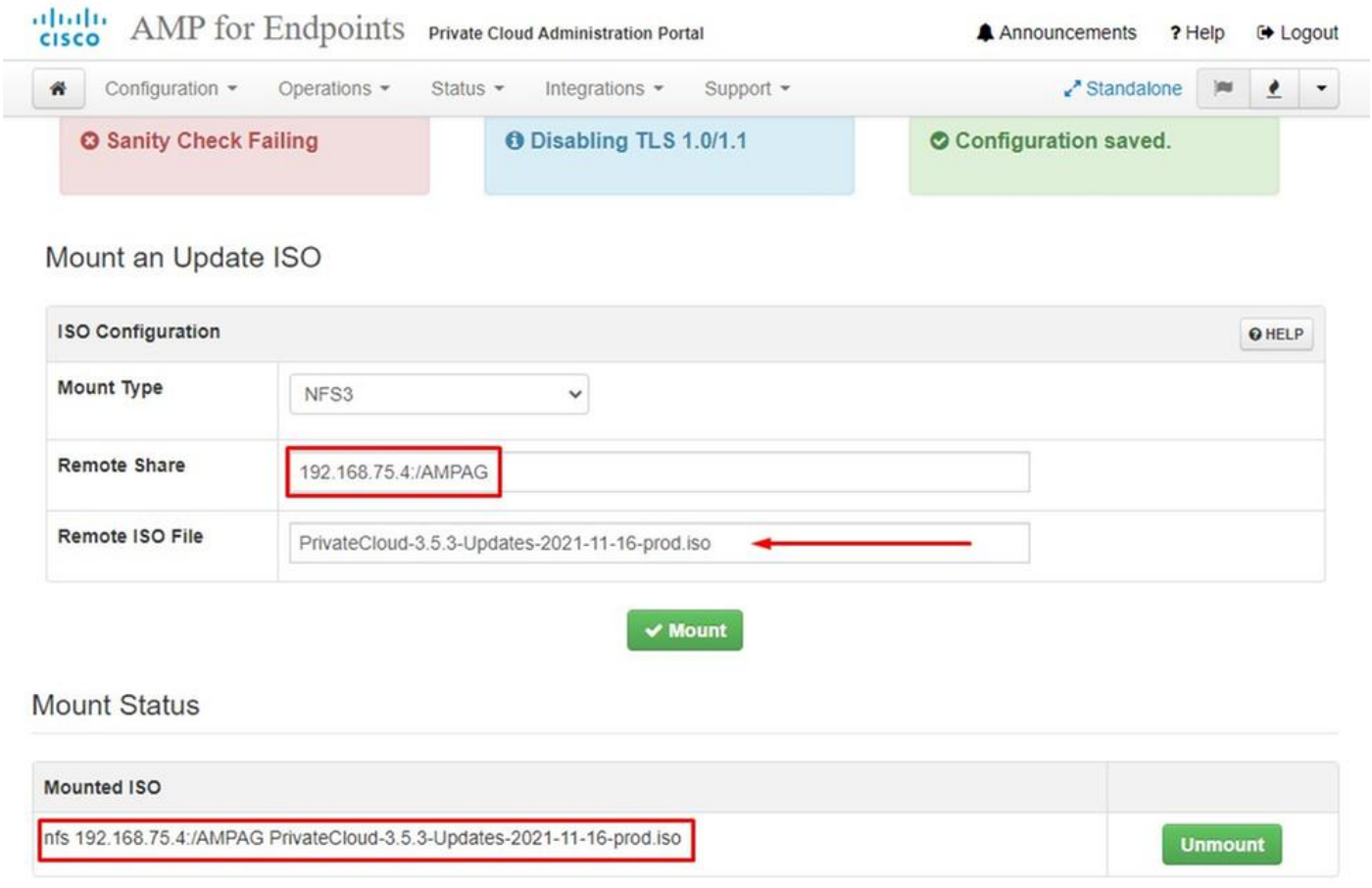


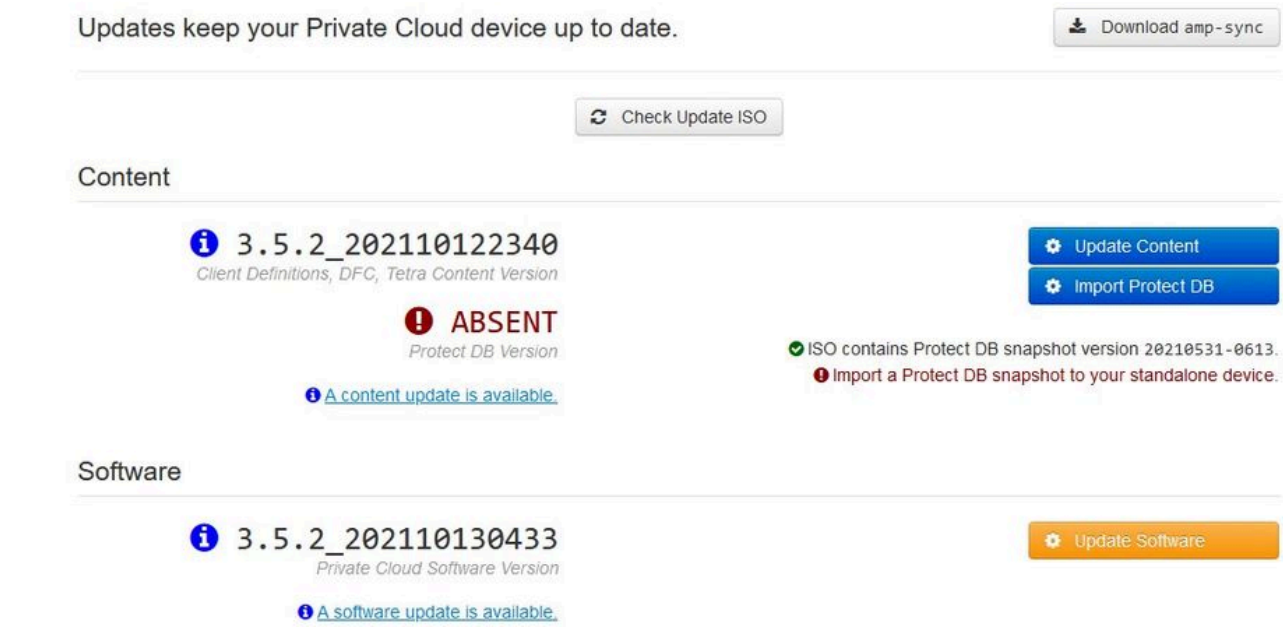
This is the error you see if you try mount the ISO update file again.



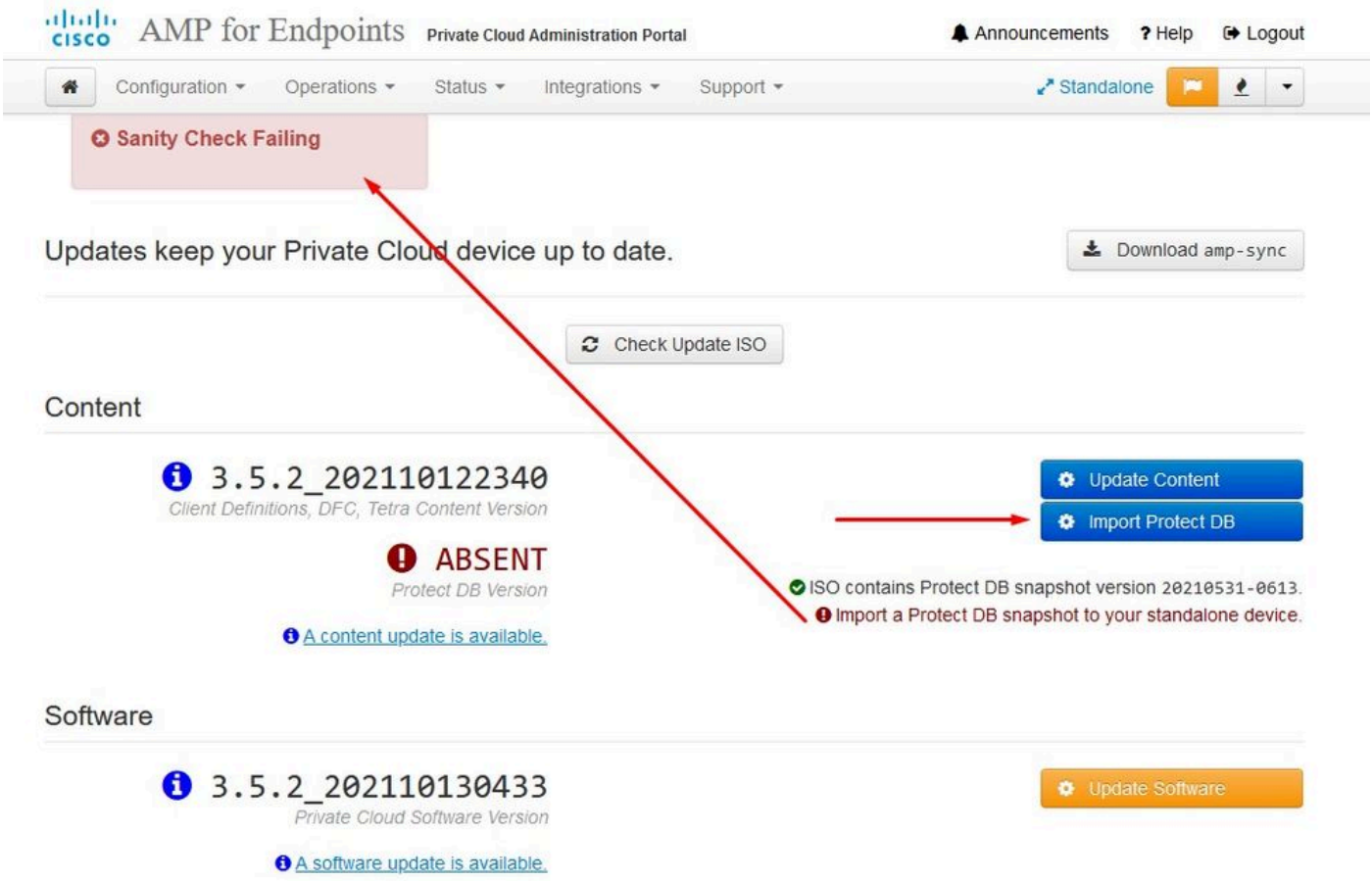
This picture shows alternative way how to mount update image to your VPC. In version 3.5.x you can use remote location such as NFS storage to share the update file with your VPC.


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Maintenance Mode
Sanity Check Failing
Disabling TLS 1.0/1.1
Mount an Update ISO
ISO Configuration
HELP
Mount Type
ISO
ISO
NFS4
NFS3
Mount Status
No ISO mounted


AMP for Endpoints
Private Cloud Administration Portal
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
Sanity Check Failing
Disabling TLS 1.0/1.1
Configuration saved.
Mount an Update ISO
ISO Configuration
HELP
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
Unmount



Sanity Check Failing is related to Protect DB not currently available on the VPC



Protect DB importing

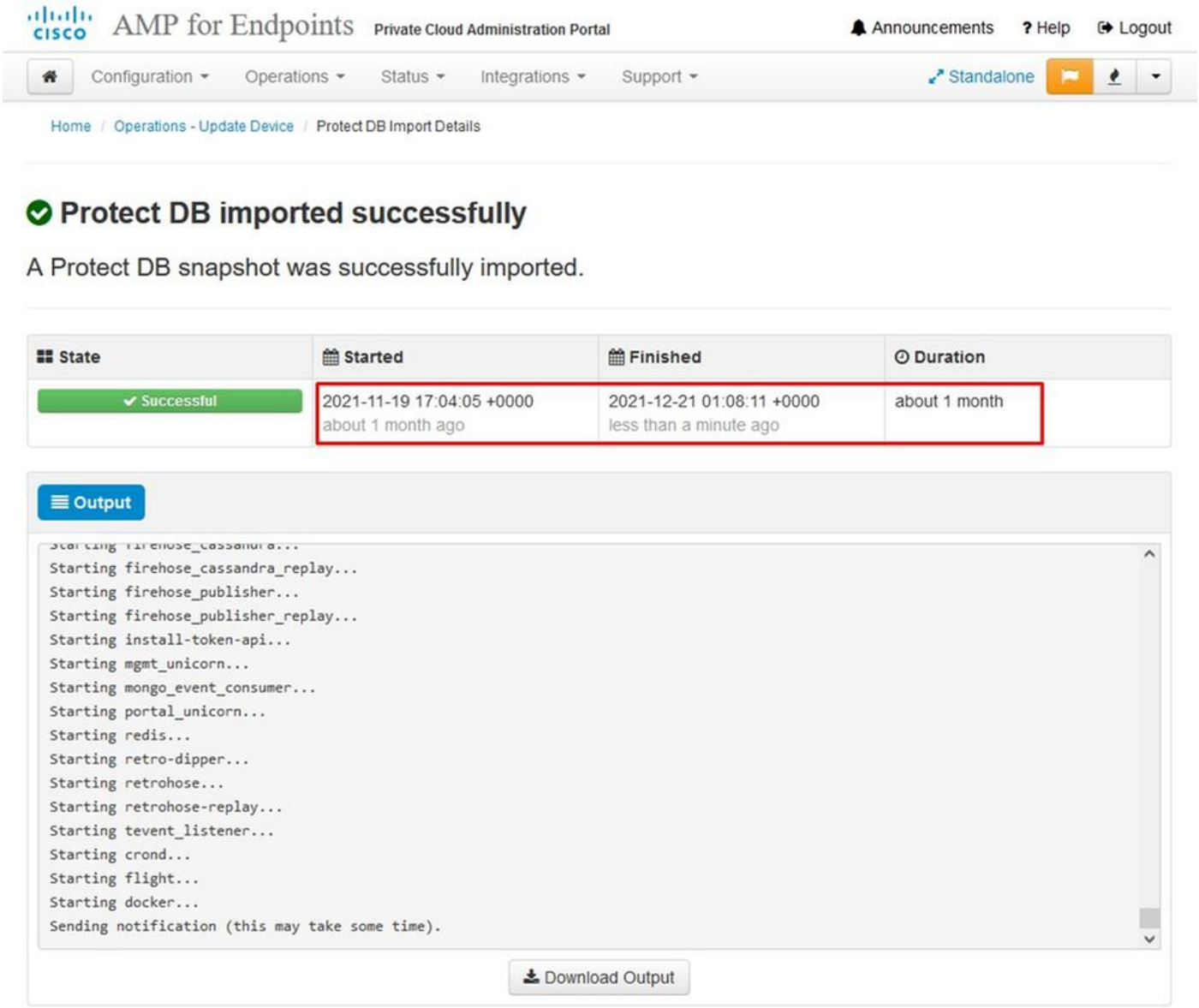
The device is currently importing a Protect DB snapshot. This process can take several hours.

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

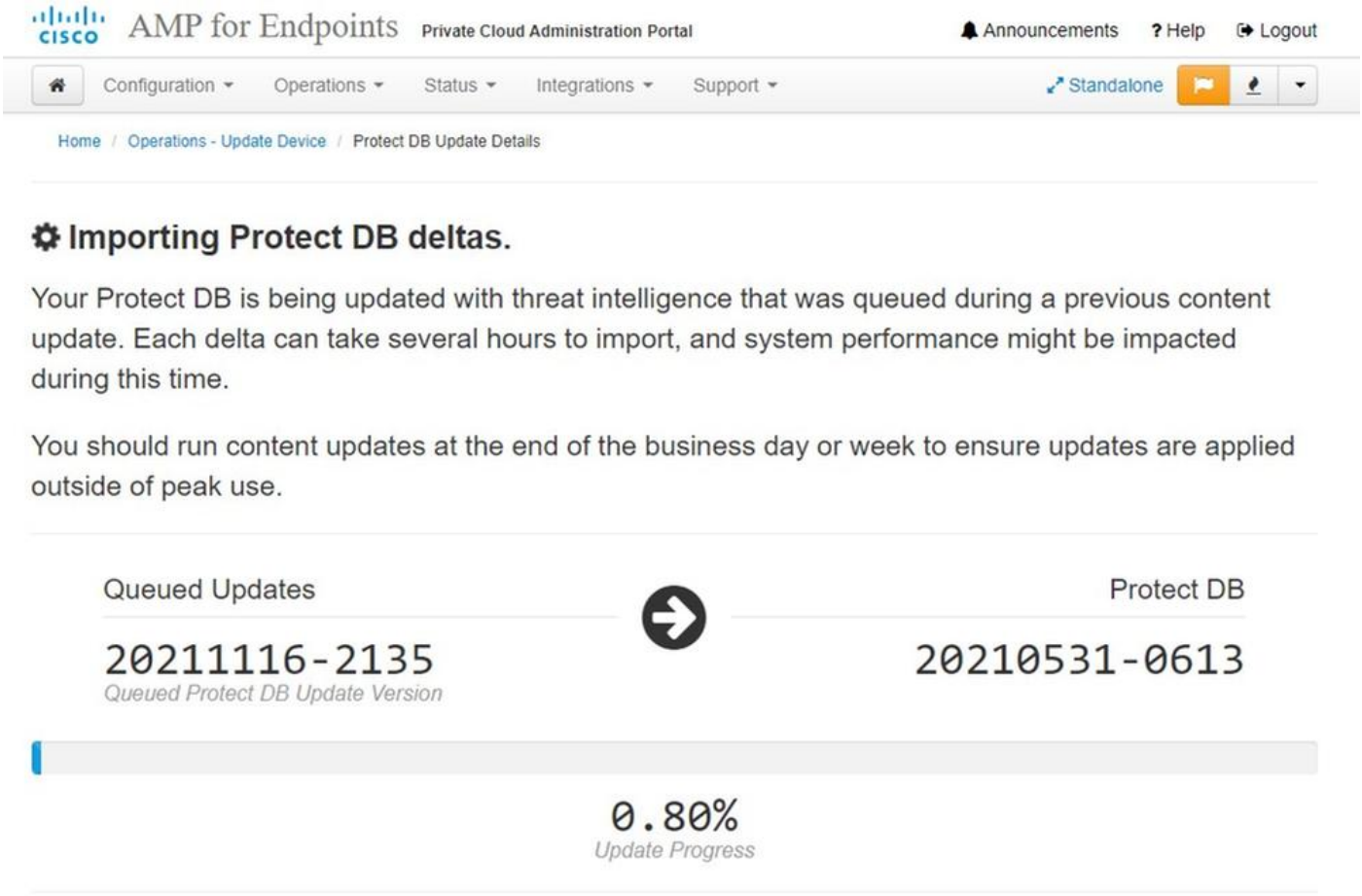
Output

```
Extraction  233.2GB at    4.2MB/s  eta:   0:00:00   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).
```

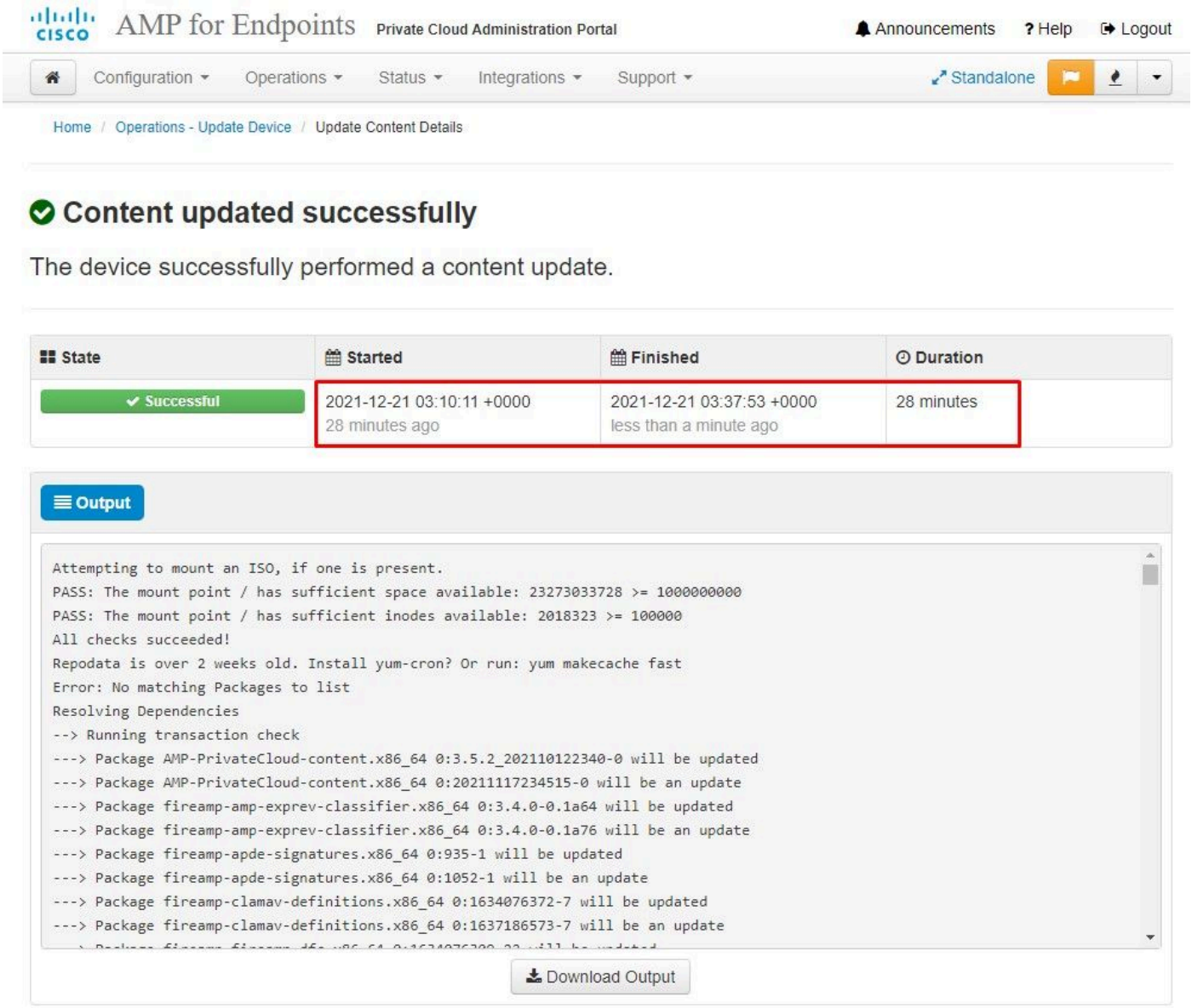
Download Output



Next update start automatically



After this very lengthy process of the import Protect DB Database you can move and update Client Definition and Software which roughly can take additional 3+ Hrs.



And finally done, please note that this process will take very long time.

For VPC appliance visit this TZ which contain other methods how to update HW Appliance, mount ISO file and boot from USB.

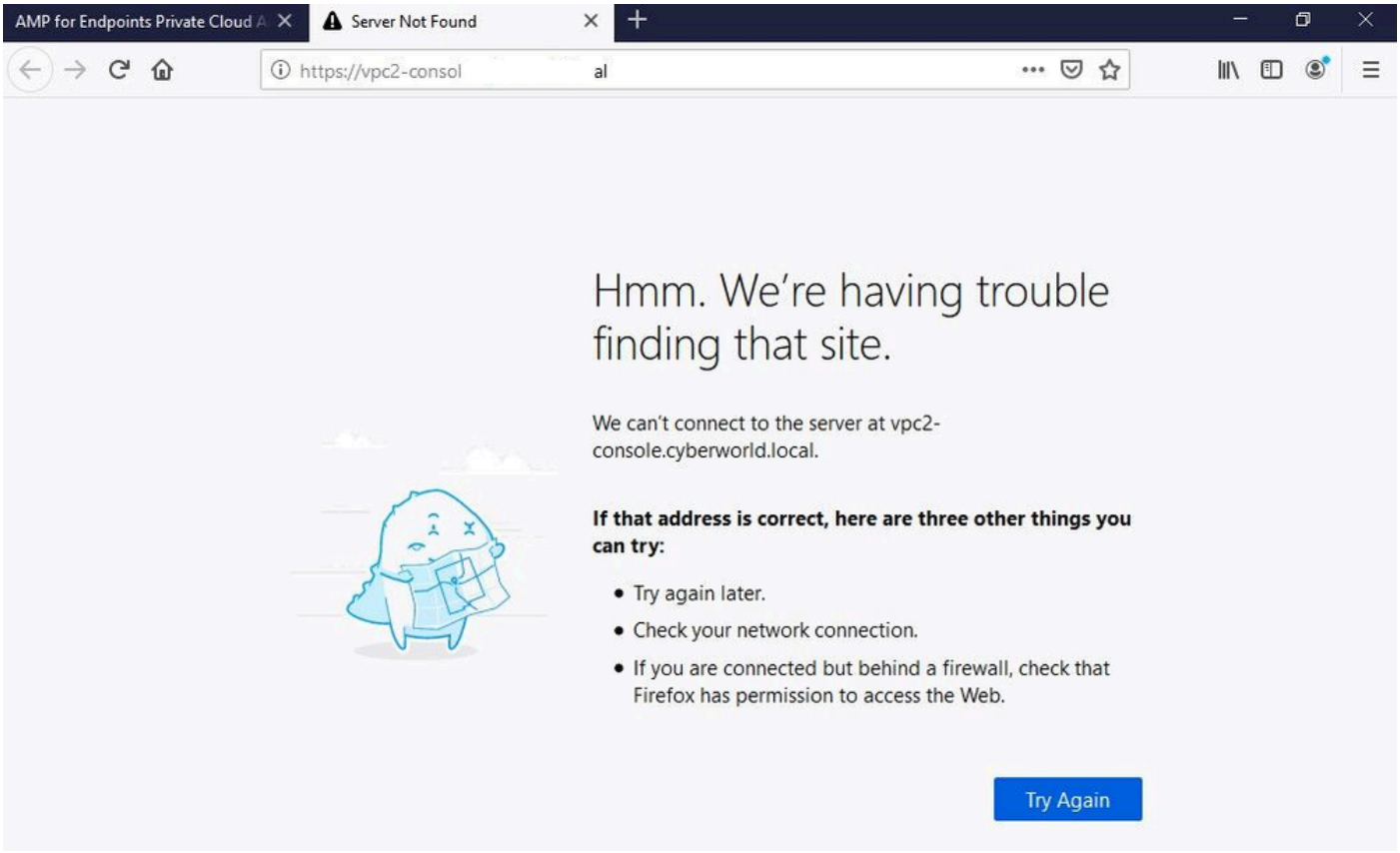
https://www.cisco.com/c/en/us/support/docs/security/amp-virtual-private-cloud-appliance/217134-upgrade-procedure-for-airgapped-amp-priv.html#anc5

⩓ ⩓ AIRGAP ONLY ⩓ ⩓

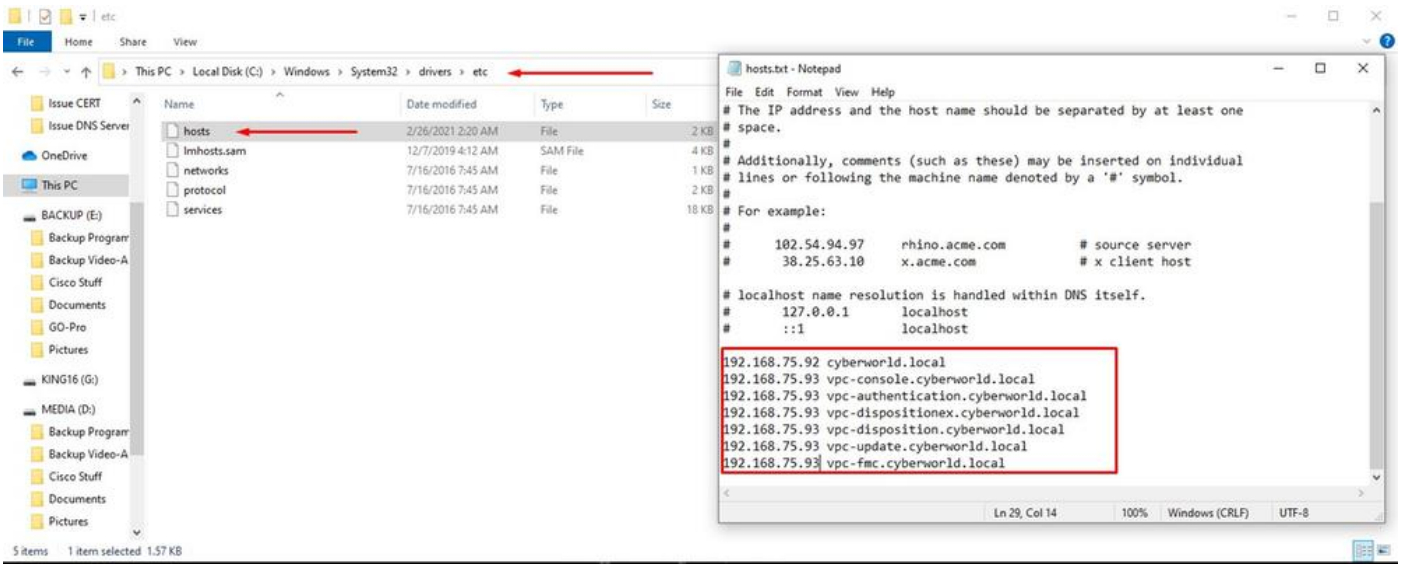
Basic Troubleshooting

Problem #1 - FQDN and DNS Server

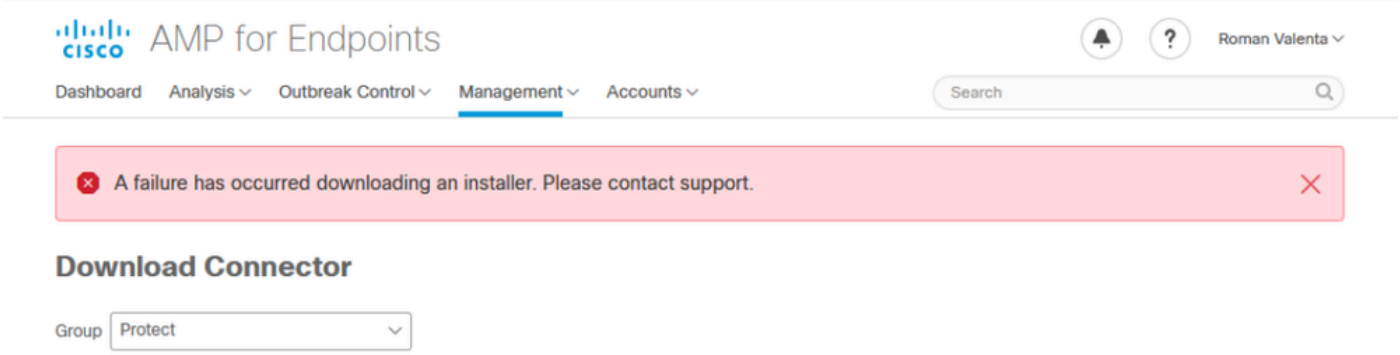
The first issue you can encounter is if your DNS server is not established and all FQDN are not properly recorded and resolved. The issue might look like this when you try navigate to Secure Endpoint console through Secure Endpoint "fire" icon. If you use just IP address it work, but you be not able to download the connector. As you can see in 3rd picture bellow.



If you modify HOSTS file on your local machine like as shown in the image solve the issue and you end up with errors.



You receive this error while you try to download the Secure Endpoint connector installer.



After some troubleshooting, the only correct solution was to setup DNS server.

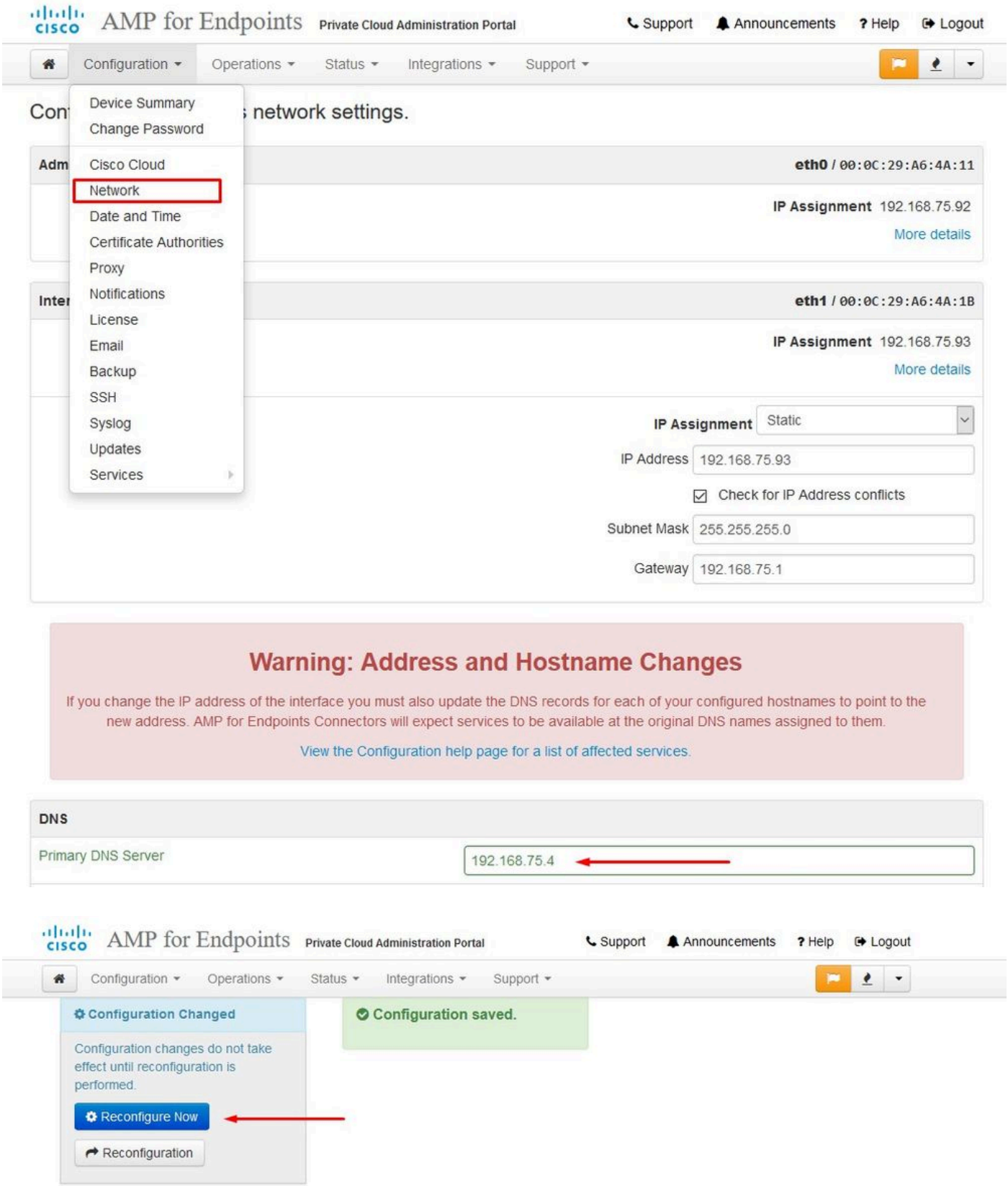
```
DNS Resolution Console: nslookup vPC-Console.cyberworld.local (Returned 1, start 2021-03-02 15:43:00 +0

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

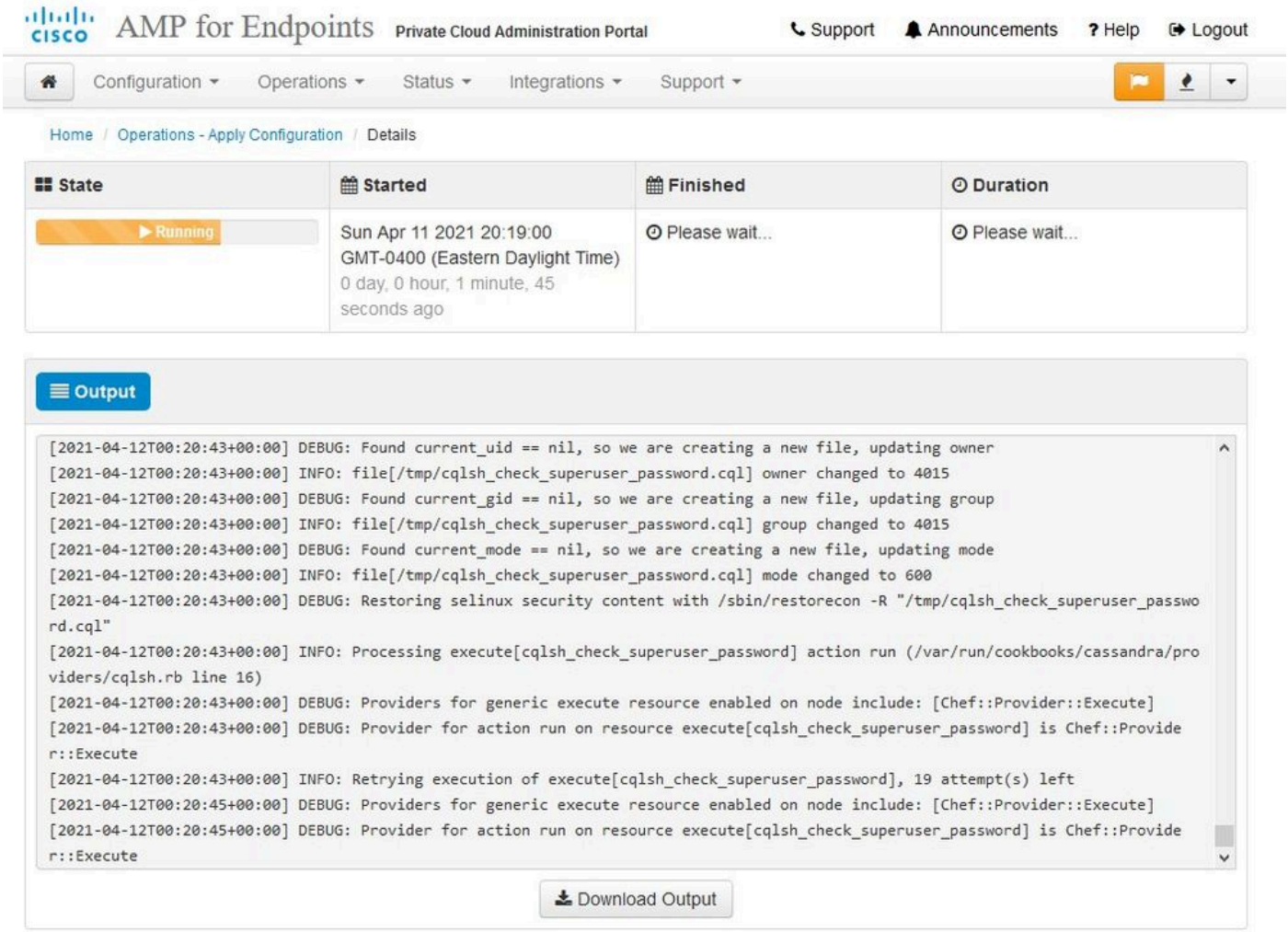
Server:         8.8.8.x
Address:        8.8.8.x#53

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

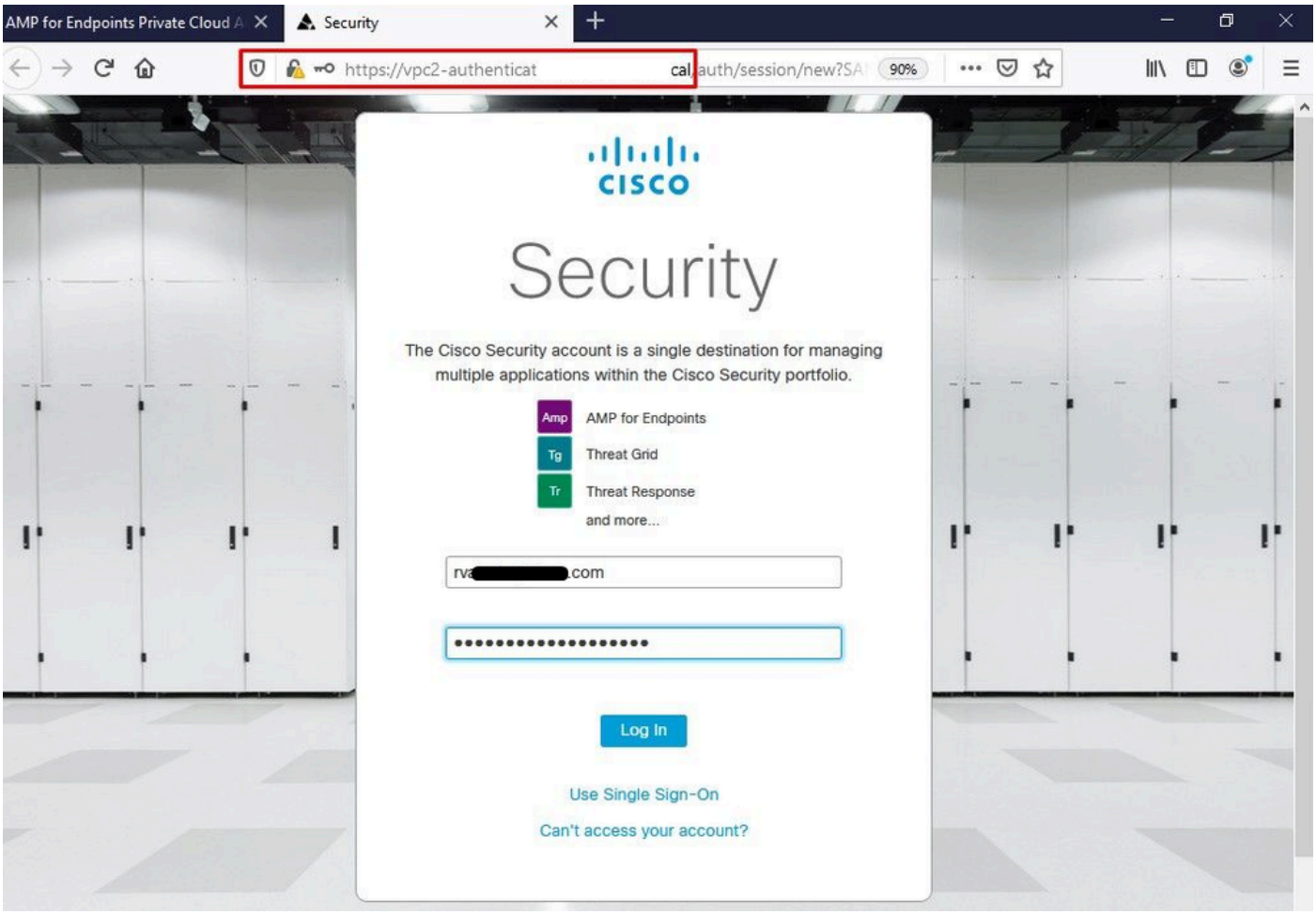
Once you record all FQDN's in your DNS server and change the record in Virtual Private Cloud from public DNS to your DNS Server everything start work as it supposed to.


AMP for Endpoints
Private Cloud Administration Portal
Support
Announcements
Help
Logout
Configuration
Operations
Status
Integrations
Support
Device Summary
Change Password
Cisco Cloud
Network
Date and Time
Certificate Authorities
Proxy
Notifications
License
Email
Backup
SSH
Syslog
Updates
Services
network settings.
eth0 / 00:0C:29:A6:4A:11
IP Assignment 192.168.75.92
More details
eth1 / 00:0C:29:A6:4A:1B
IP Assignment 192.168.75.93
More details
IP Assignment Static
IP Address 192.168.75.93
Check for IP Address conflicts
Subnet Mask 255.255.255.0
Gateway 192.168.75.1
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 hostnames to point to the new address. AMP for Endpoints Connectors will expect services to be available at the original DNS names assigned to them.
View the Configuration help page for a list of affected services.
DNS
Primary DNS Server
192.168.75.4

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

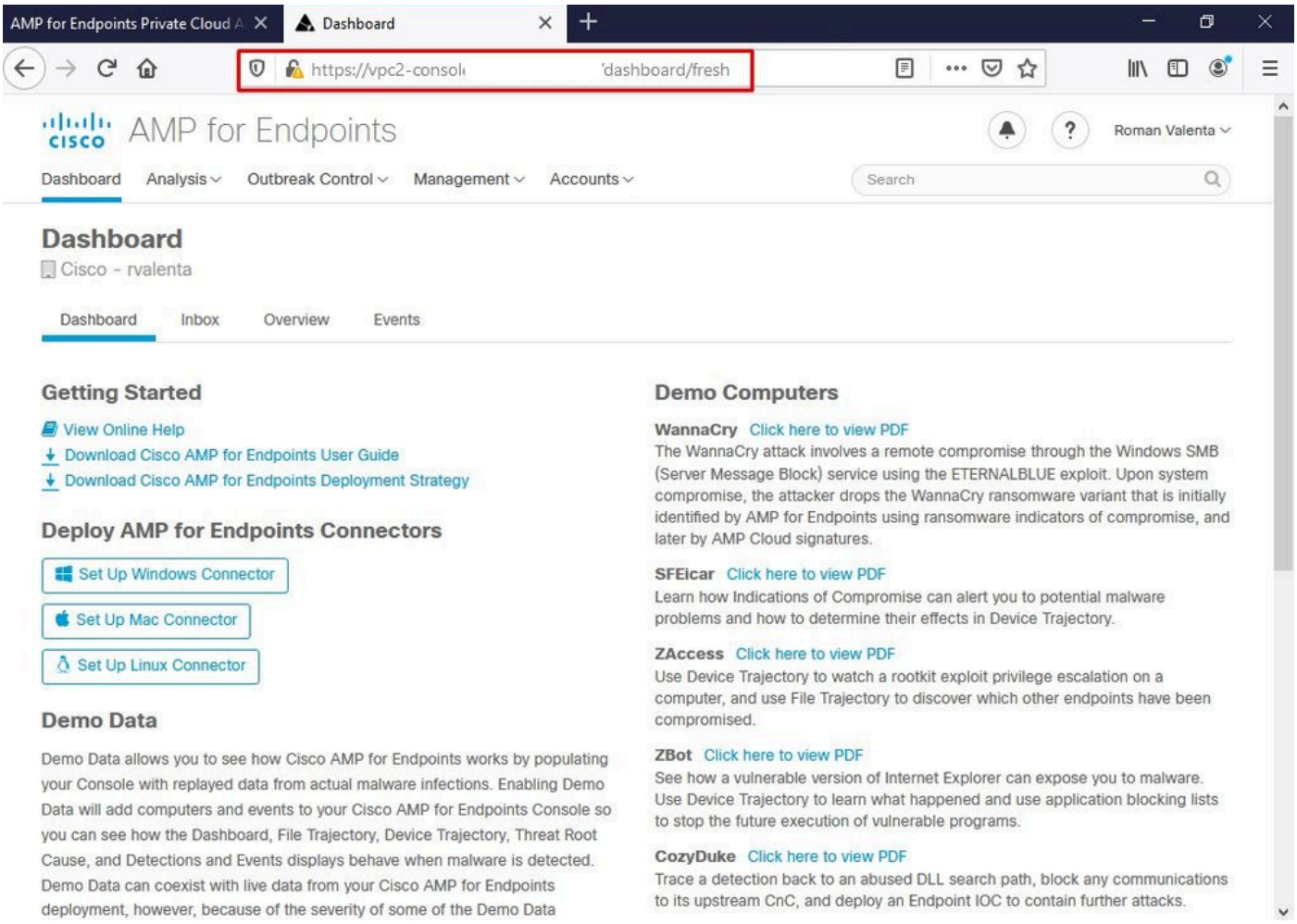


At this point you be able to log in and download the connector

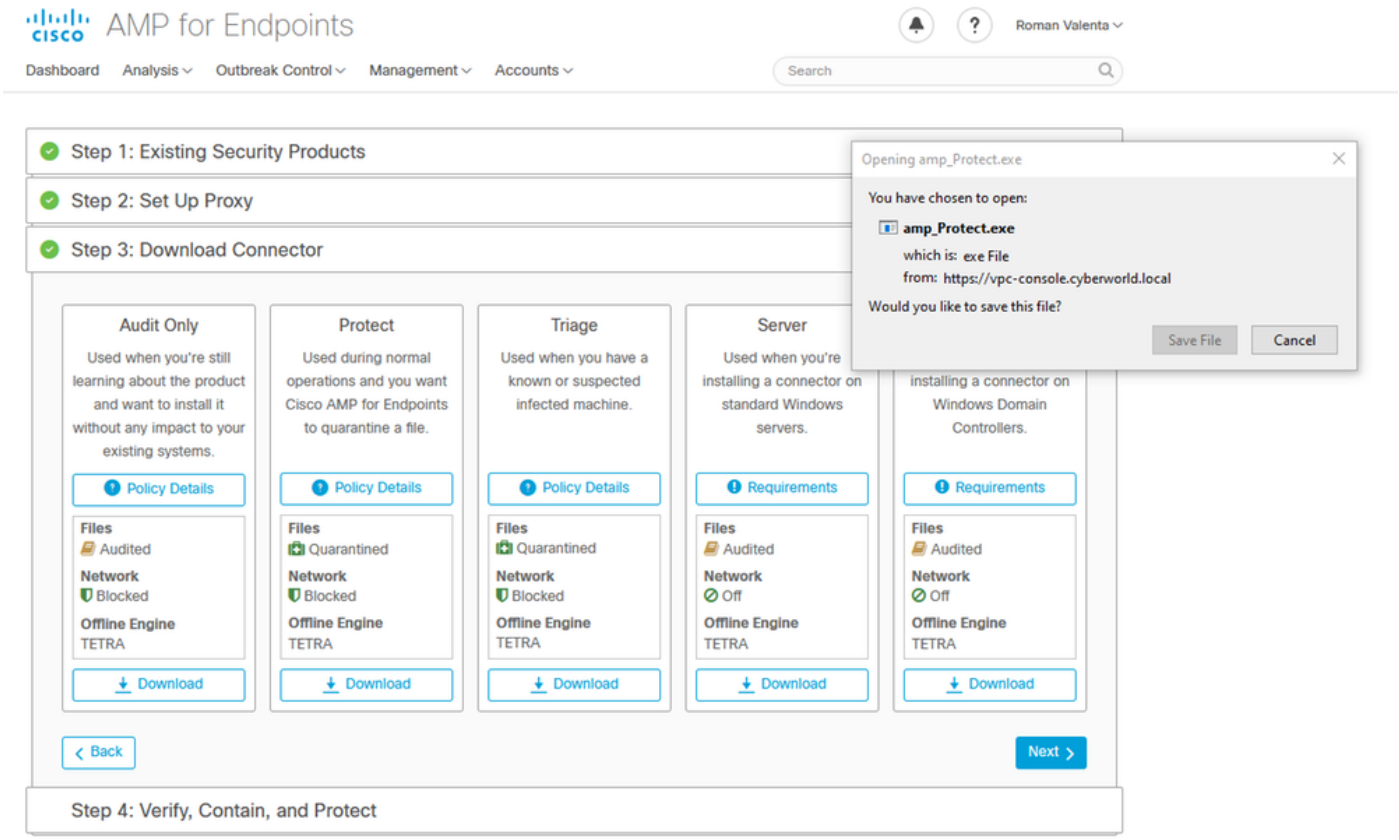


You get the initial Secure Endpoint policy wizard for your environment. It walks you through the selection of anti-virus product you use, if any, as well as proxy , and the types of policies you wish to deploy. Select on appropriate Set Up... button depends on the operating system of the connector.

You get the Existing Security Products page, as shown in the image. Choose the security products you use. It automatically generates applicable exclusions to prevent performance issues on your endpoints. Select on **Next.**

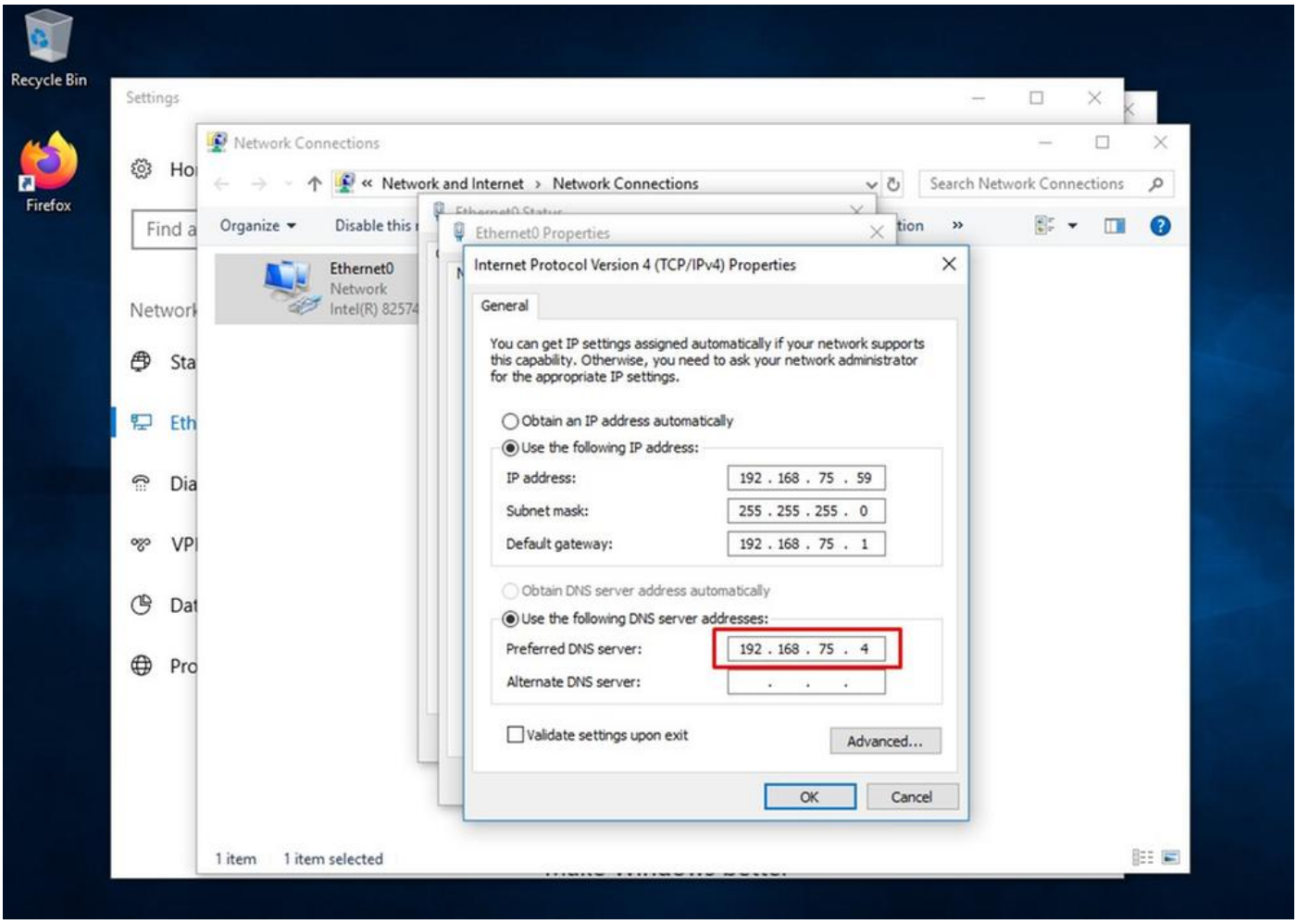


Download connector.

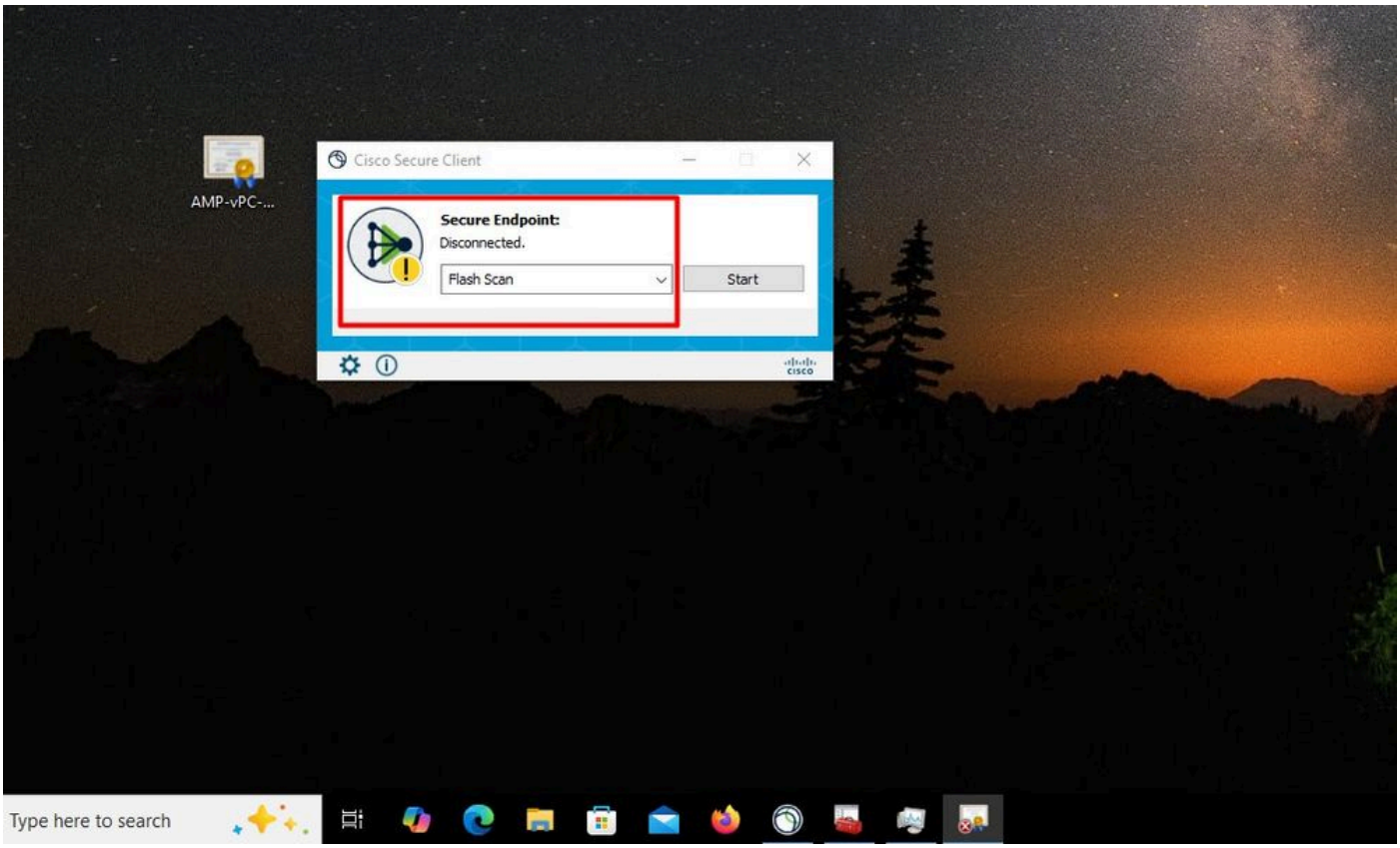


Problem #2 - Issue with Root CA

The next issue you can face is if you use your own in-house certificates is that after the initial install, connector can show as disconnected.



Once you install the connector Secure Endpoint can be seen as Disconnected. Run diagnostic bundle and look through the logs, you be able to determine the issue.



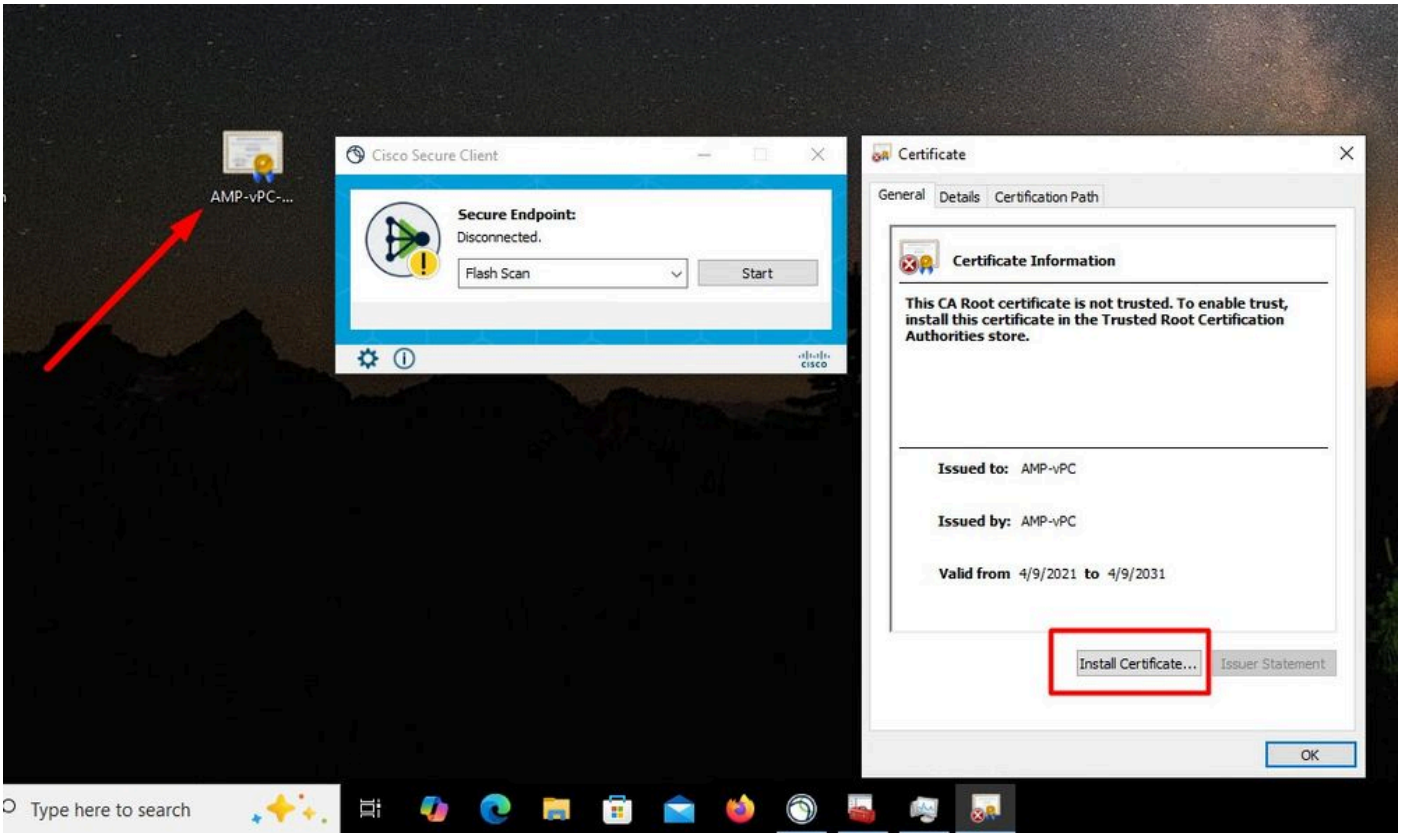
Based on this output collected from diagnostic bundle you can see the Root CA error

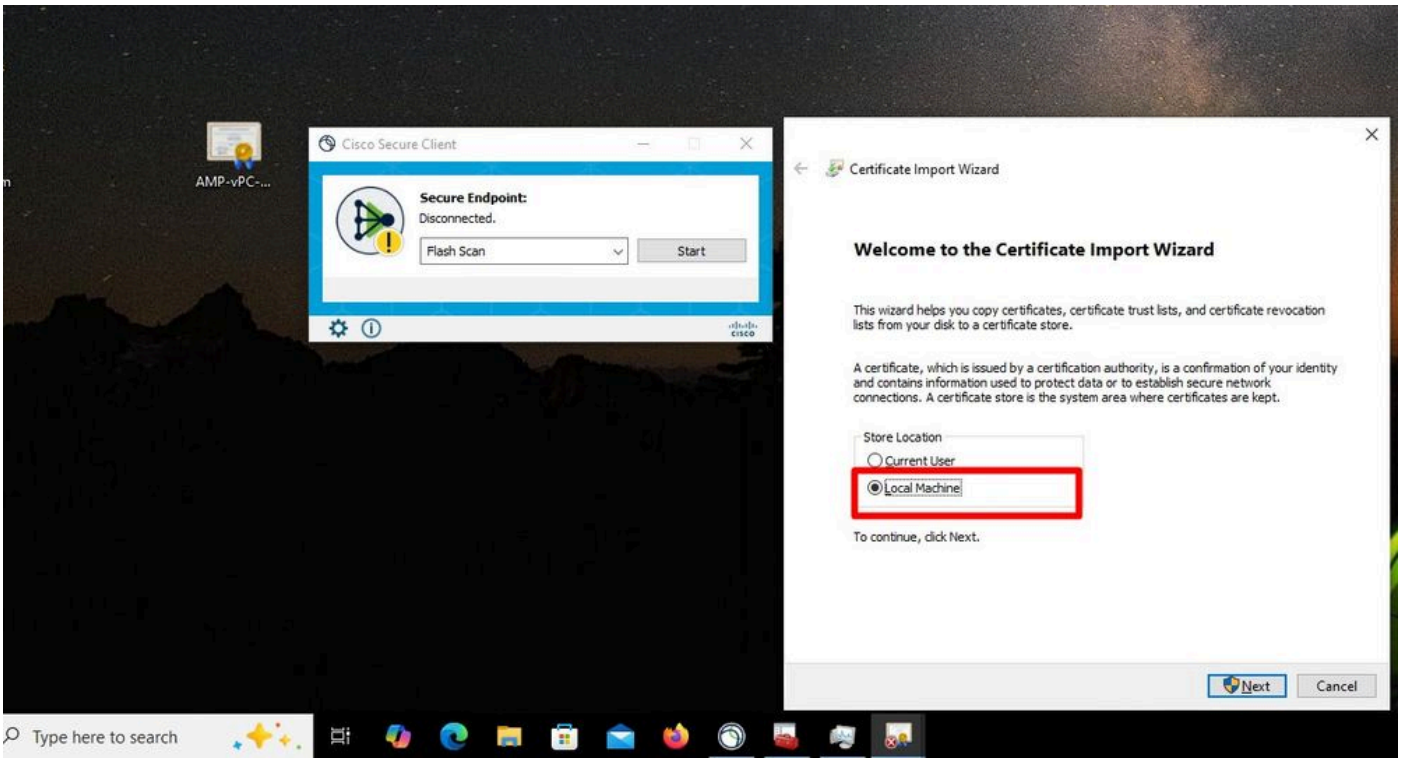
```
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1011]: GET request https://vPC-Console.cyberworl

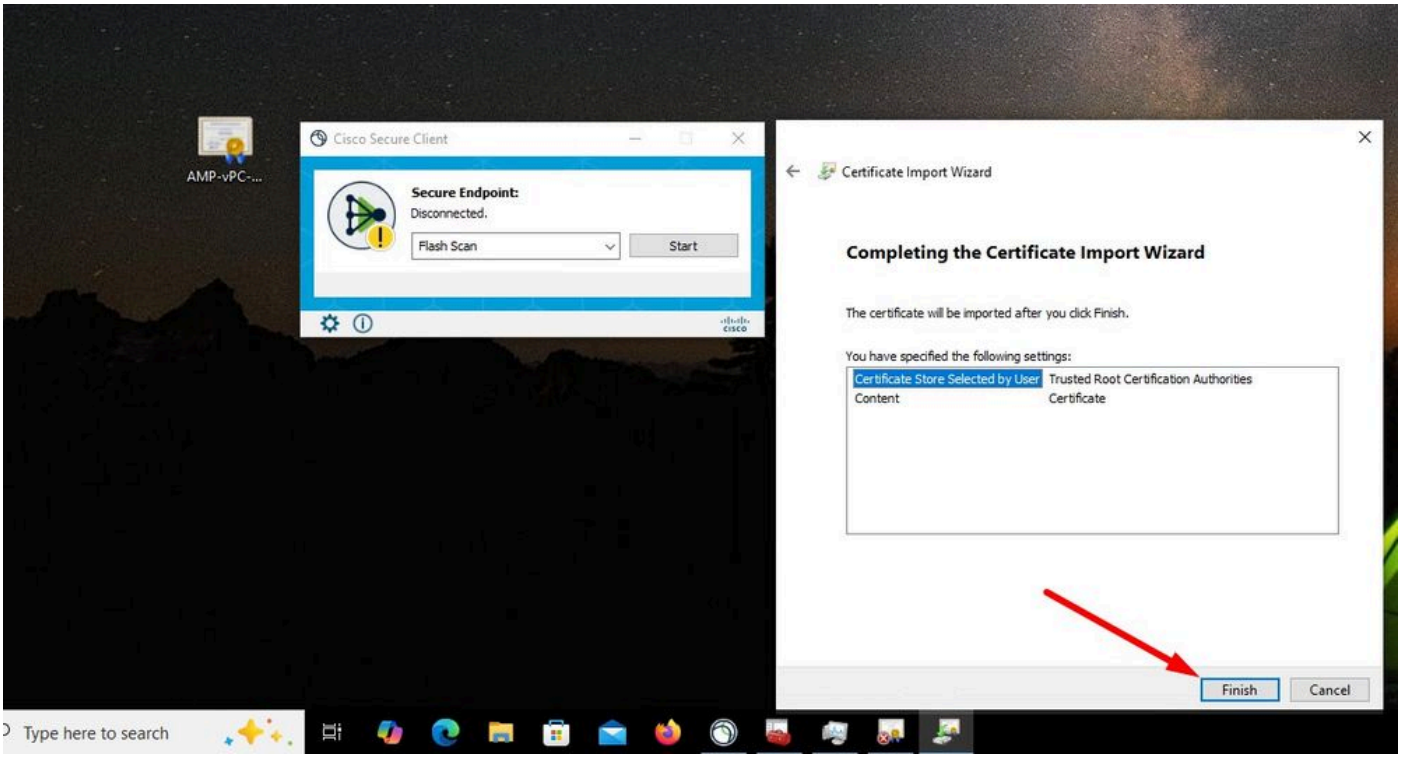
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1051]: async request failed (SSL peer certificat

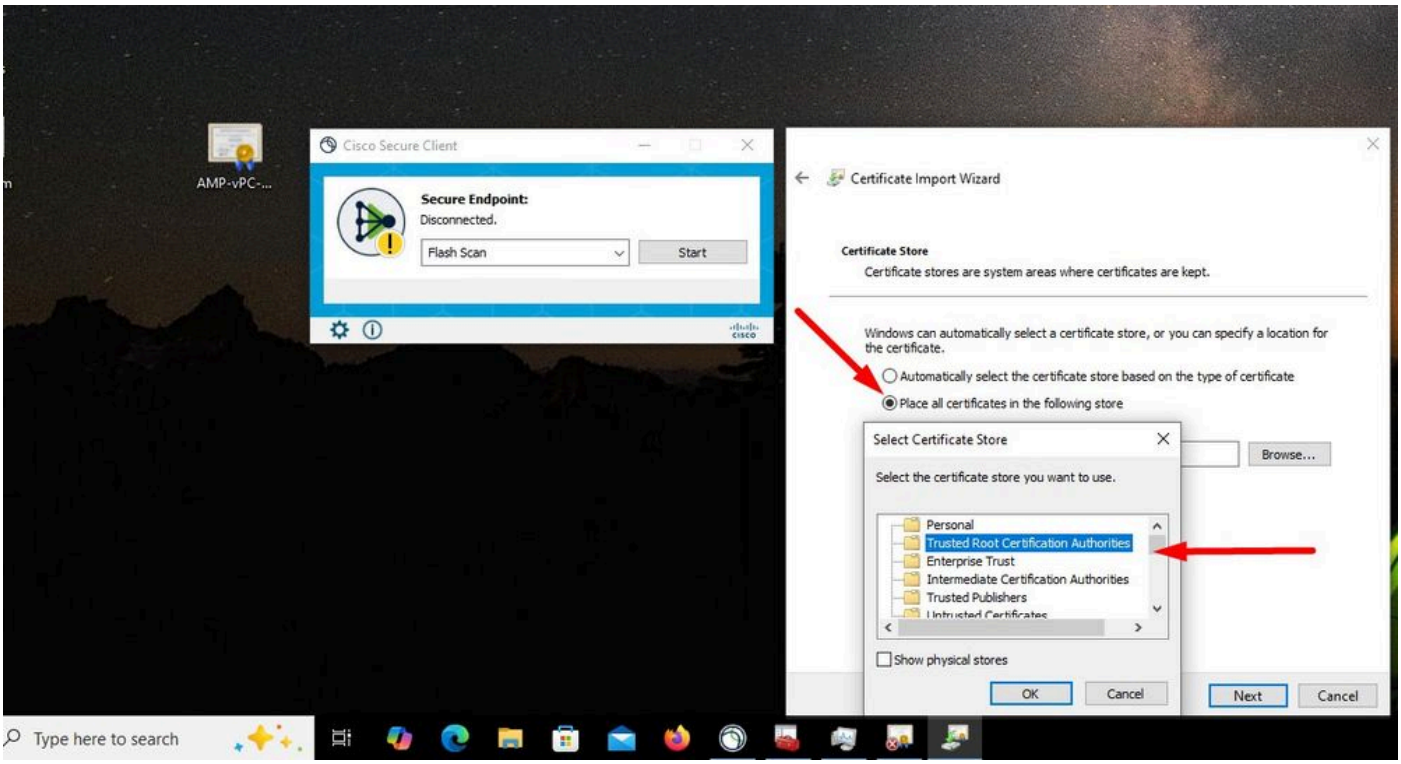
(804765, +0 ms) Mar 06 00:47:07 [8876]: [http_client.c@1074]: response failed with code 60
```

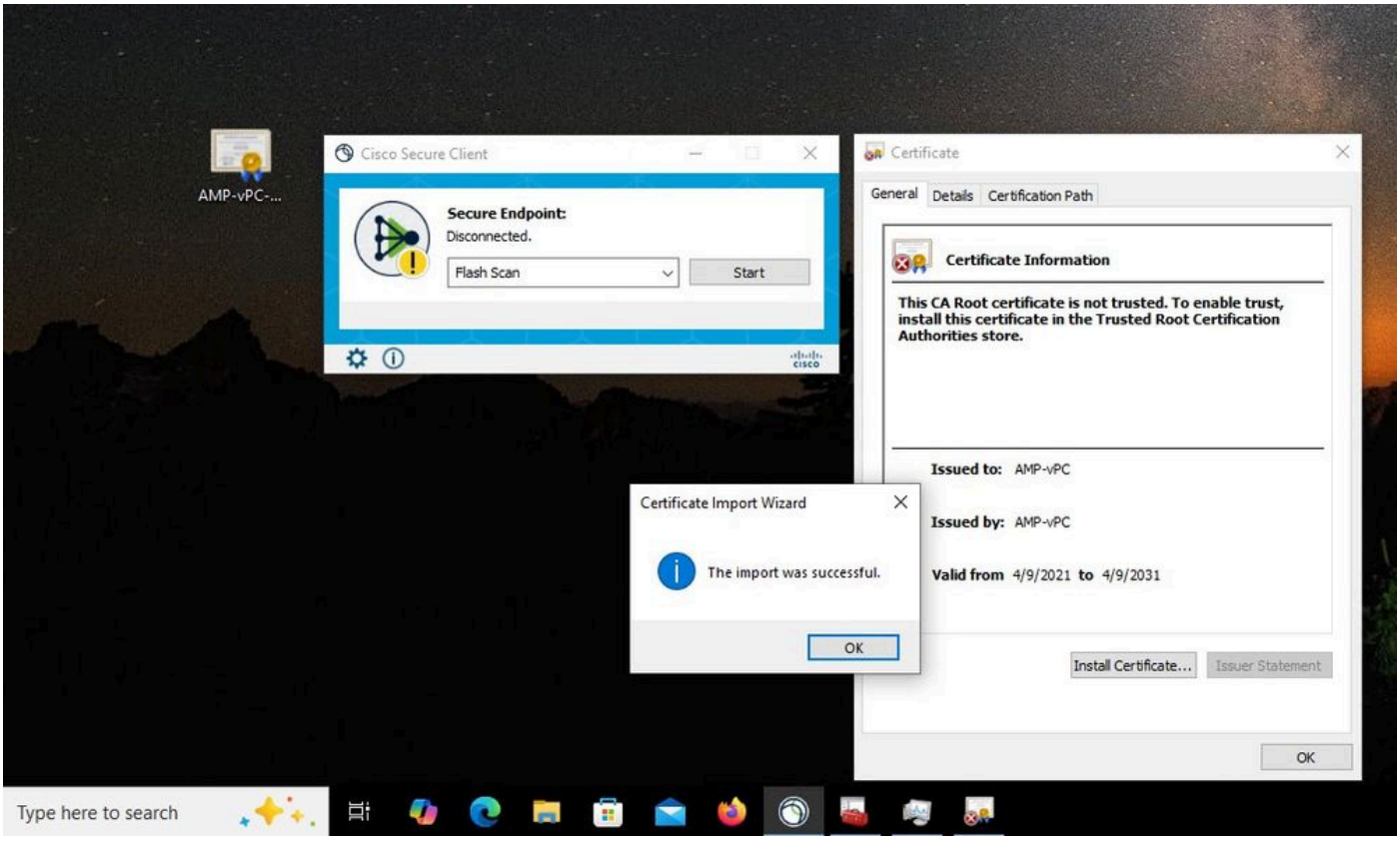
Once you upload the Root CA into trusted Root CA store and restart the Secure Endpoint service. Everything start work as expected.

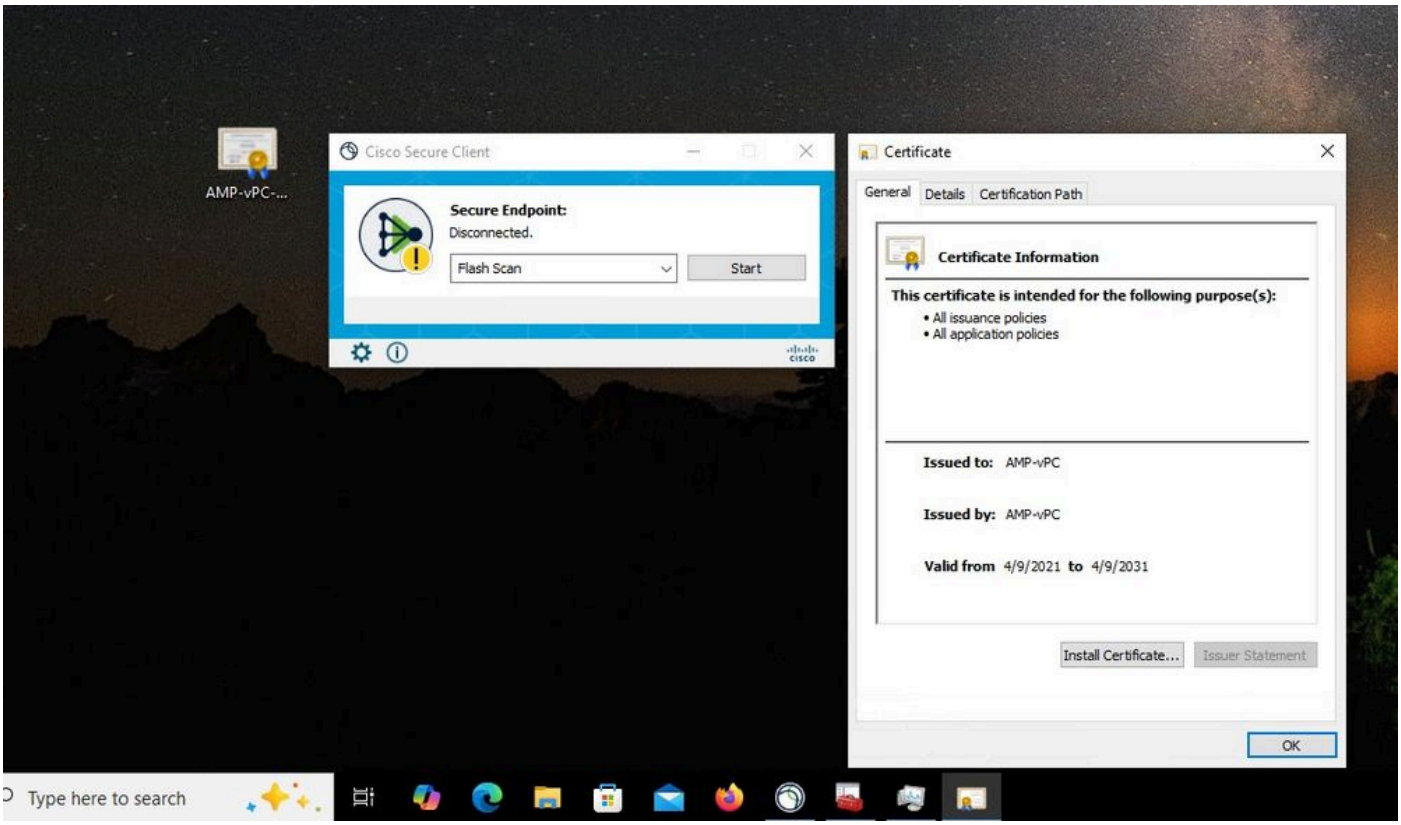


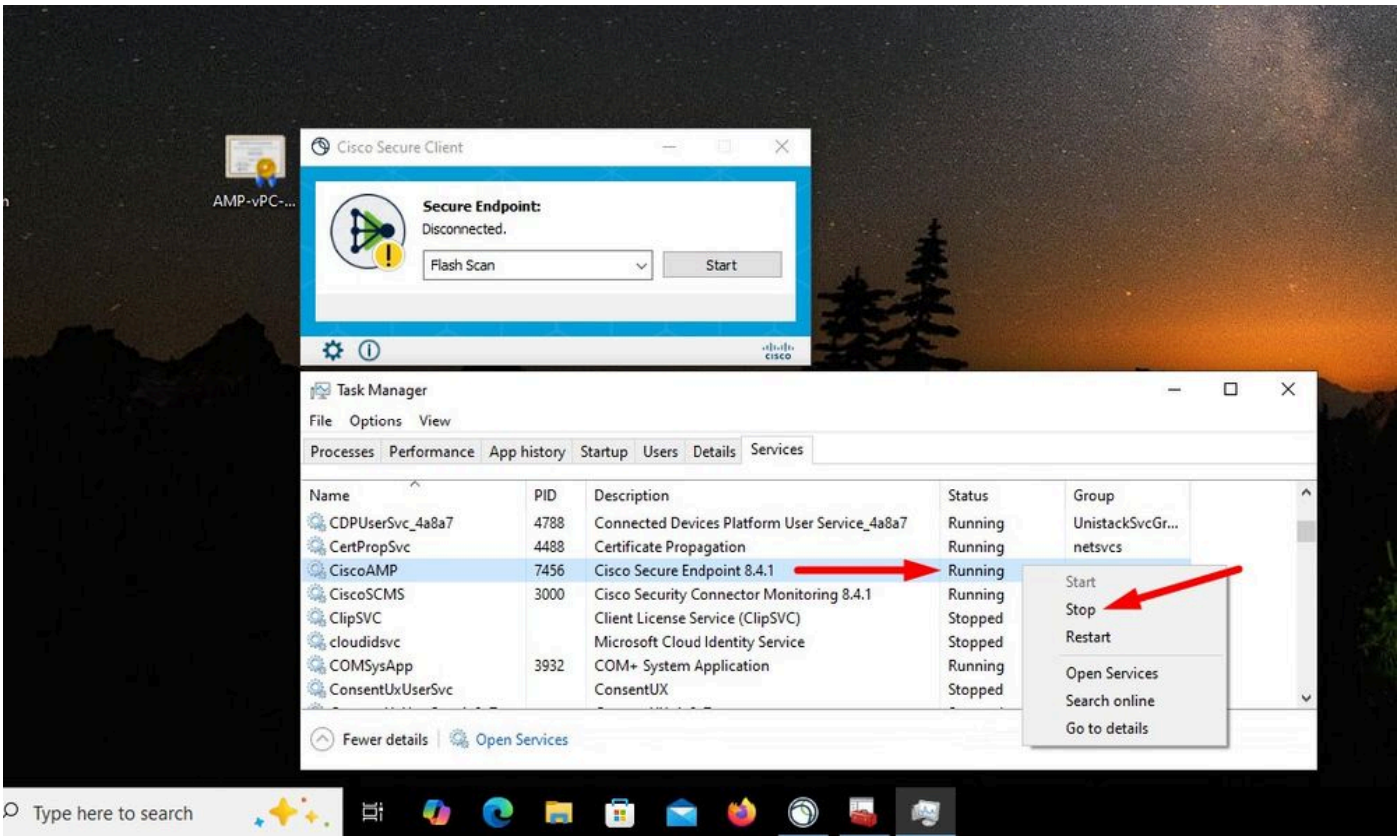

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel
Type here to search

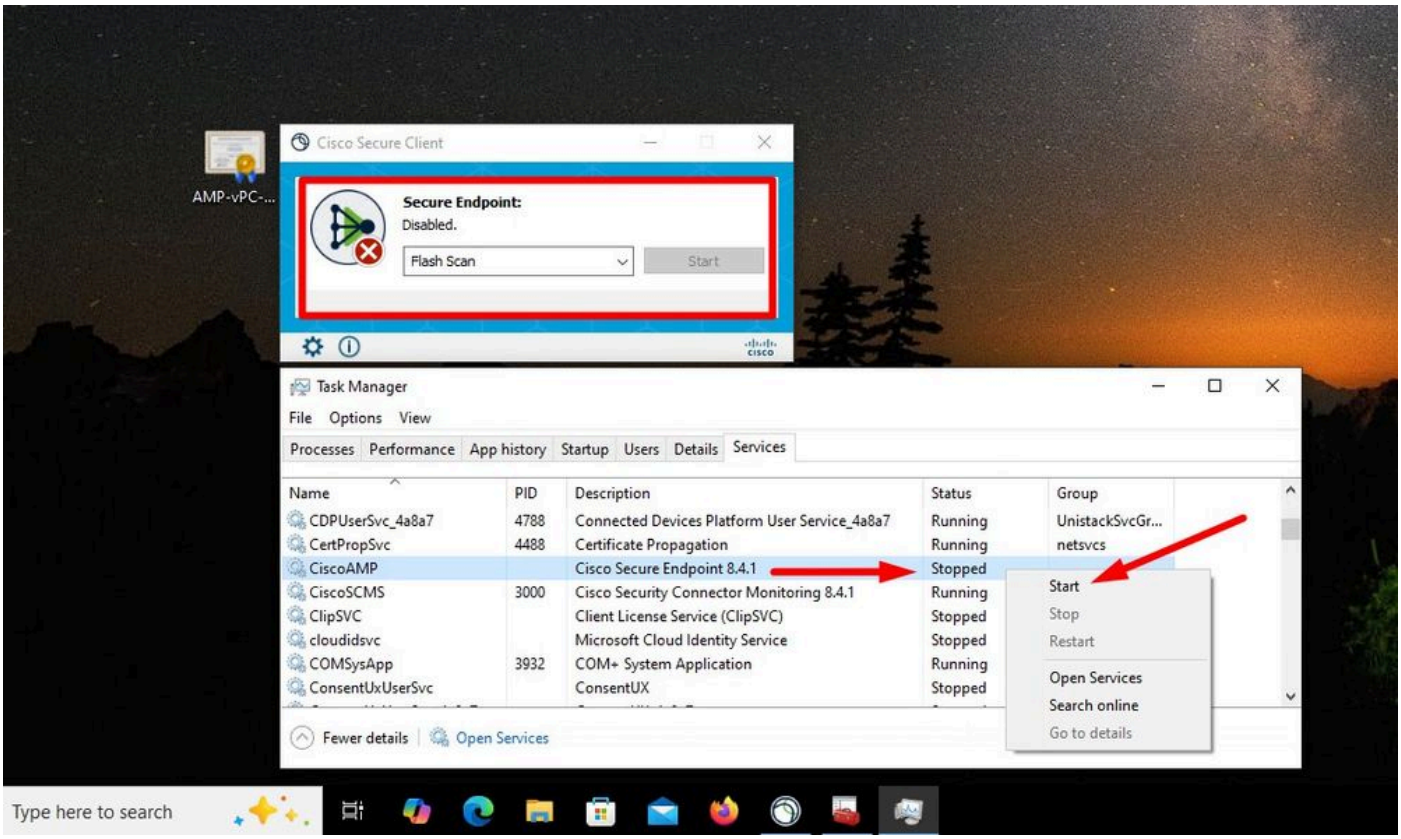

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
Finish
Cancel
Type here to search


AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
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
Browse...
Next
Cancel
Type here to search

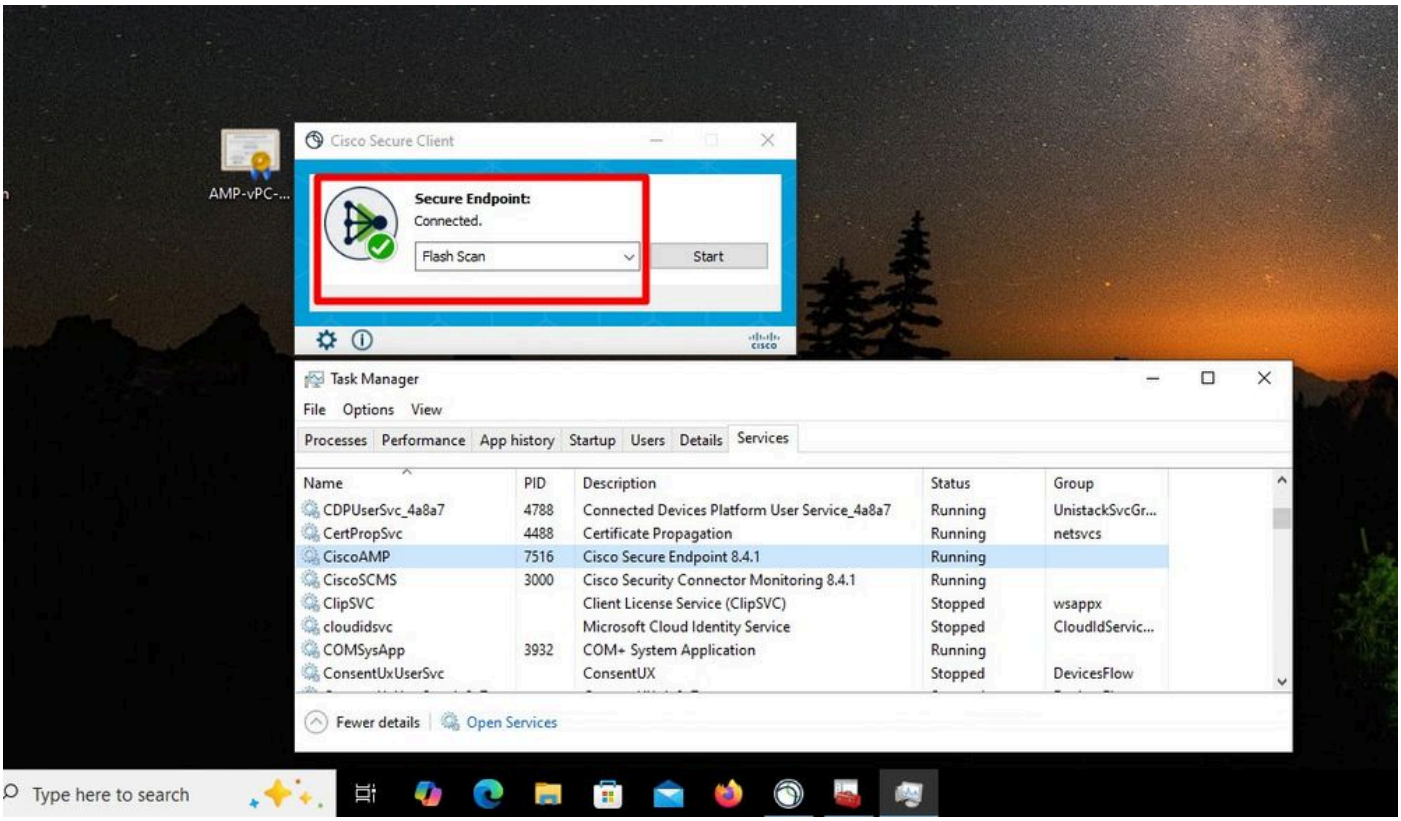

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Certificate Import Wizard
The import was successful.
OK
Type here to search

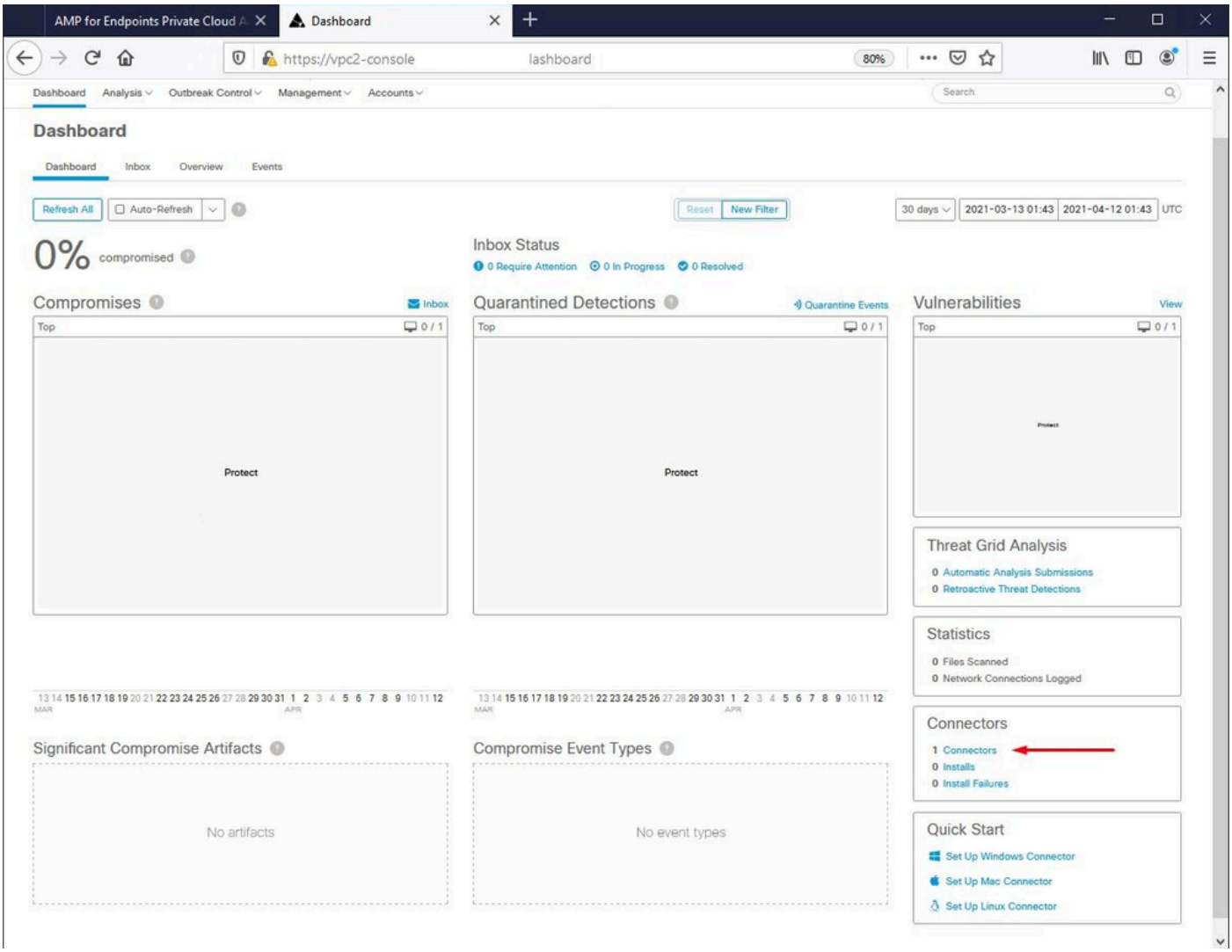

AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: AMP-vPC
Issued by: AMP-vPC
Valid from 4/9/2021 to 4/9/2031
Install Certificate...
Issuer Statement
OK
Type here to search


AMP-vPC-...
Cisco Secure Client
Secure Endpoint:
Disconnected.
Flash Scan
Start
Task Manager
File
Options
View
Processes
Performance
App history
Startup
Users
Details
Services
Name
PID
Description
Status
Group
CDPUserSvc_4a8a7
4788
Connected Devices Platform User Service_4a8a7
Running
UnistackSvcGr...
CertPropSvc
4488
Certificate Propagation
Running
netsvcs
CiscoAMP
7456
Cisco Secure Endpoint 8.4.1
Running
CiscoSCMS
3000
Cisco Security Connector Monitoring 8.4.1
Running
ClipSVC
Client License Service (ClipSVC)
Stopped
cloudidsvc
Microsoft Cloud Identity Service
Stopped
COMSysApp
3932
COM+ System Application
Running
ConsentUxUserSvc
ConsentUX
Stopped
Start
Stop
Restart
Open Services
Search online
Go to details
Fewer details
Open Services
Type here to search

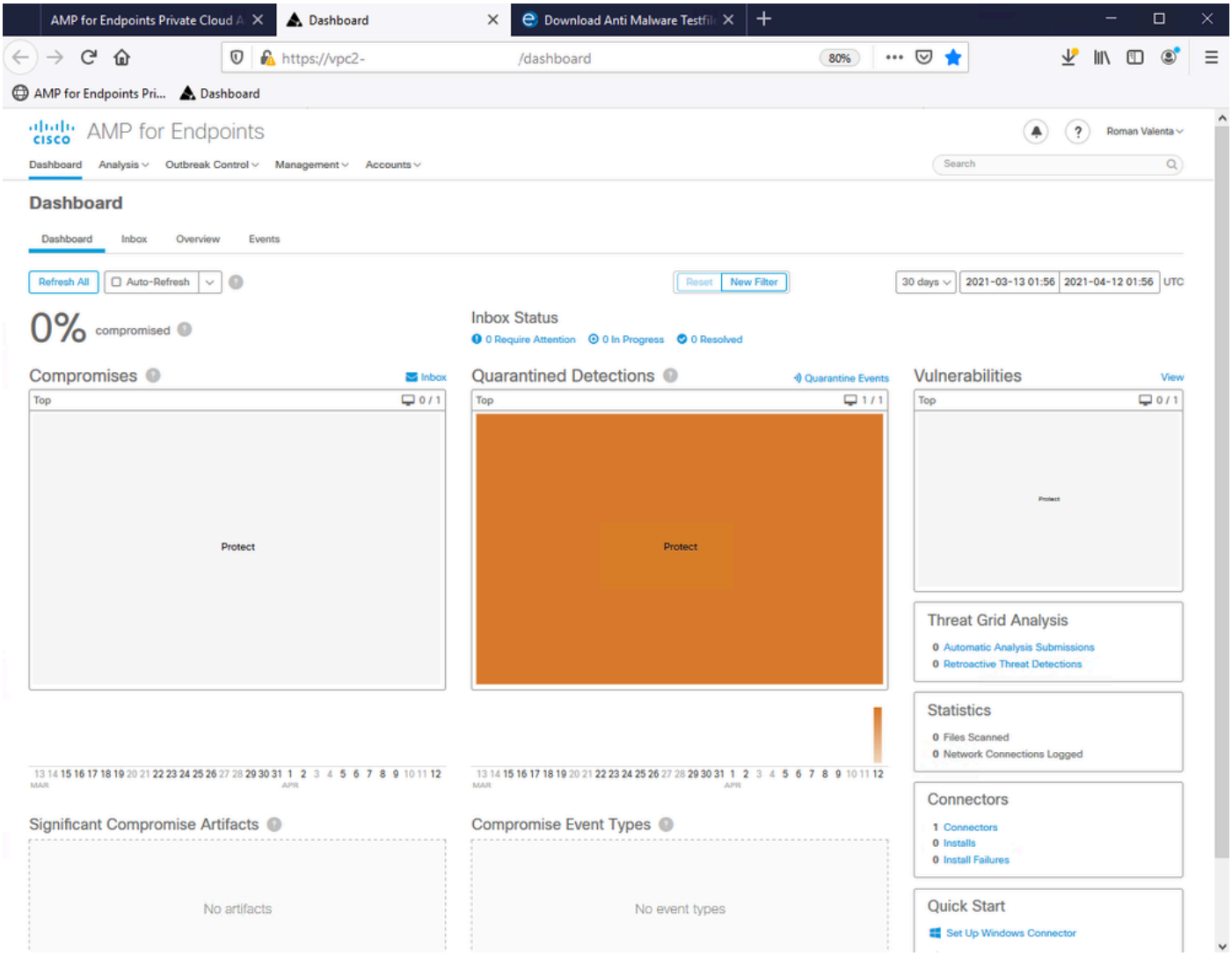


Once we bounce the Secure Endpoint service connector become online as expected.





Tested malicious activity


AMP for Endpoints Private Cloud A
Dashboard
Download Anti Malware Testfil
https://vpc2-
/dashboard
80%
AMP for Endpoints Pri...
Dashboard
AMP for Endpoints
Roman Valenta
Dashboard
Analysis
Outbreak Control
Management
Accounts
Search
Dashboard
Dashboard
Inbox
Overview
Events
Refresh All
Auto-Refresh
Reset
New Filter
30 days
2021-03-13 01:56
2021-04-12 01:56
UTC
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
Vulnerabilities
View
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
Threat Grid Analysis
0 Automatic Analysis Submissions
0 Retroactive Threat Detections
Statistics
0 Files Scanned
0 Network Connections Logged
Connectors
1 Connectors
0 Installs
0 Install Failures
Quick Start
Set Up Windows Connector
Significant Compromise Artifacts
No artifacts
Compromise Event Types
No event types