

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 ESX 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 XCA
- 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 below 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. 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.

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

Select OVF and VMDK files

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

Enter a name for the virtual machine.

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

×  PrivateCloud-Latest.ova



Back

Next

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

Select creation type

How would you like to create a Virtual Machine?

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

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



Back

Next

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

Select storage

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

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

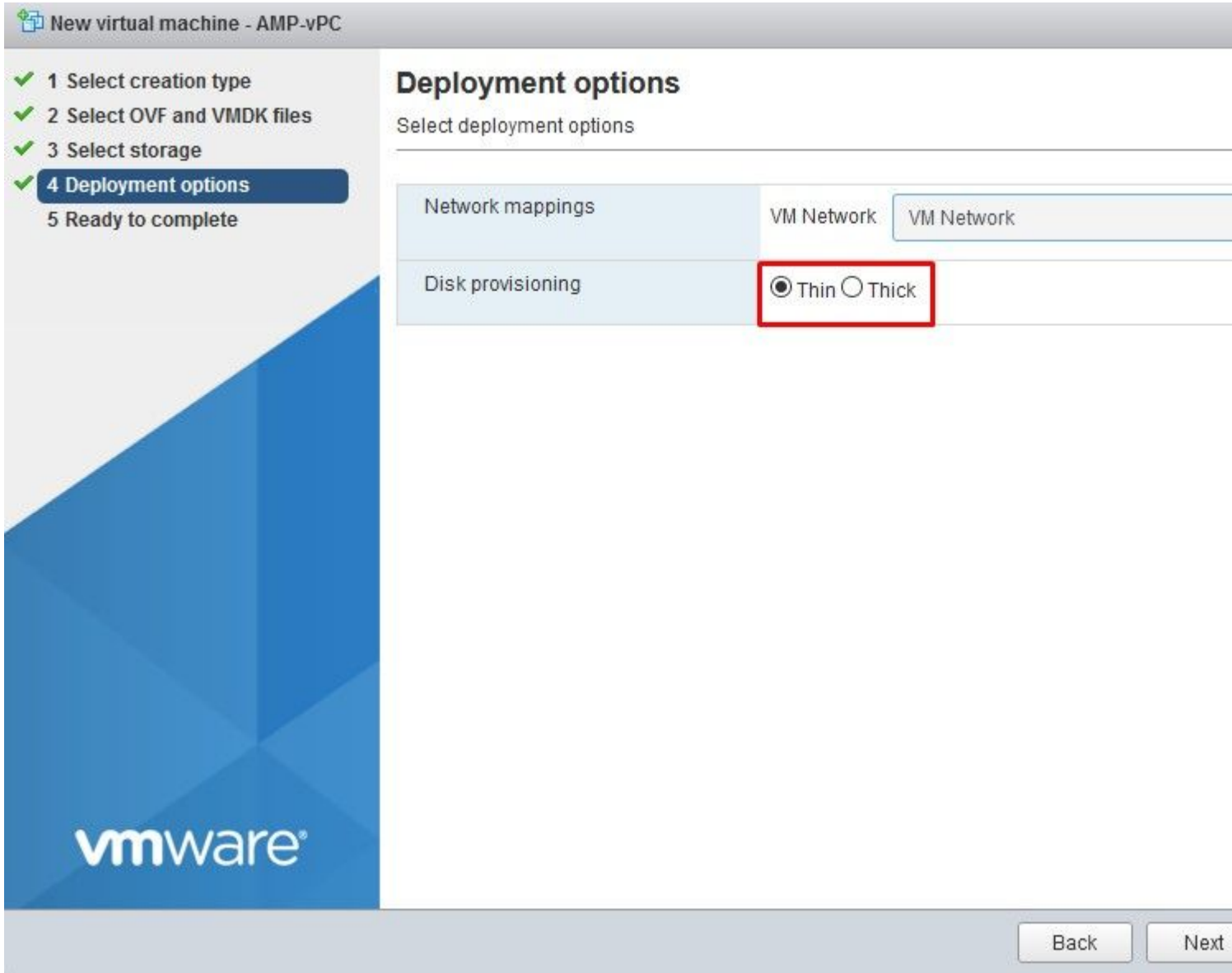
Name	Capacity	Free	Type	
vDisk-70_12	922.75 GB	921.8 GB	VMFS5	S
vDisk-70_34	930.25 GB	929.3 GB	VMFS5	S
vDisk-70_56	930.25 GB	929.3 GB	VMFS5	S
vDisk-70_78	930.25 GB	929.3 GB	VMFS5	S



Back

Next

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**.

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

Ready to complete

Review your settings selection before finishing the wizard

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



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

vmware®

Back

Next

Initial Admin Interface Setup


New virtual machine - AMP-vPC

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

Ready to complete

Review your settings selection before finishing the wizard

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

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

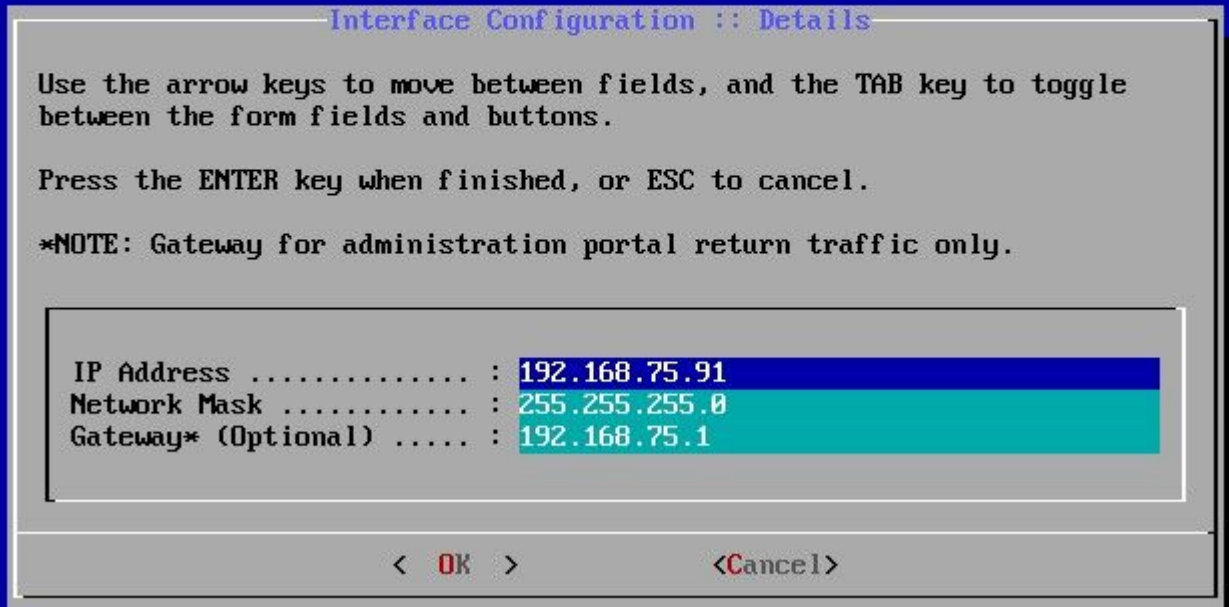
vmware

Back Next

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:29:14:00:00) already uses address 192.168.75.91.

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

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

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

Press ENTER key to continue...
-

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

Interface Configuration :: Details

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

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

*NOTE: Gateway for administration portal return traffic only.

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

< OK >

<Cancel>

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 06:13:11.8893895
@@ -18,7 +18,7 @@
 #AddressFamily any
 #ListenAddress 0.0.0.0
 #ListenAddress ::
-ListenAddress 192.168.75.208
+ListenAddress 192.168.75.92

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

```

Restarting eth0...

Reconfiguring...

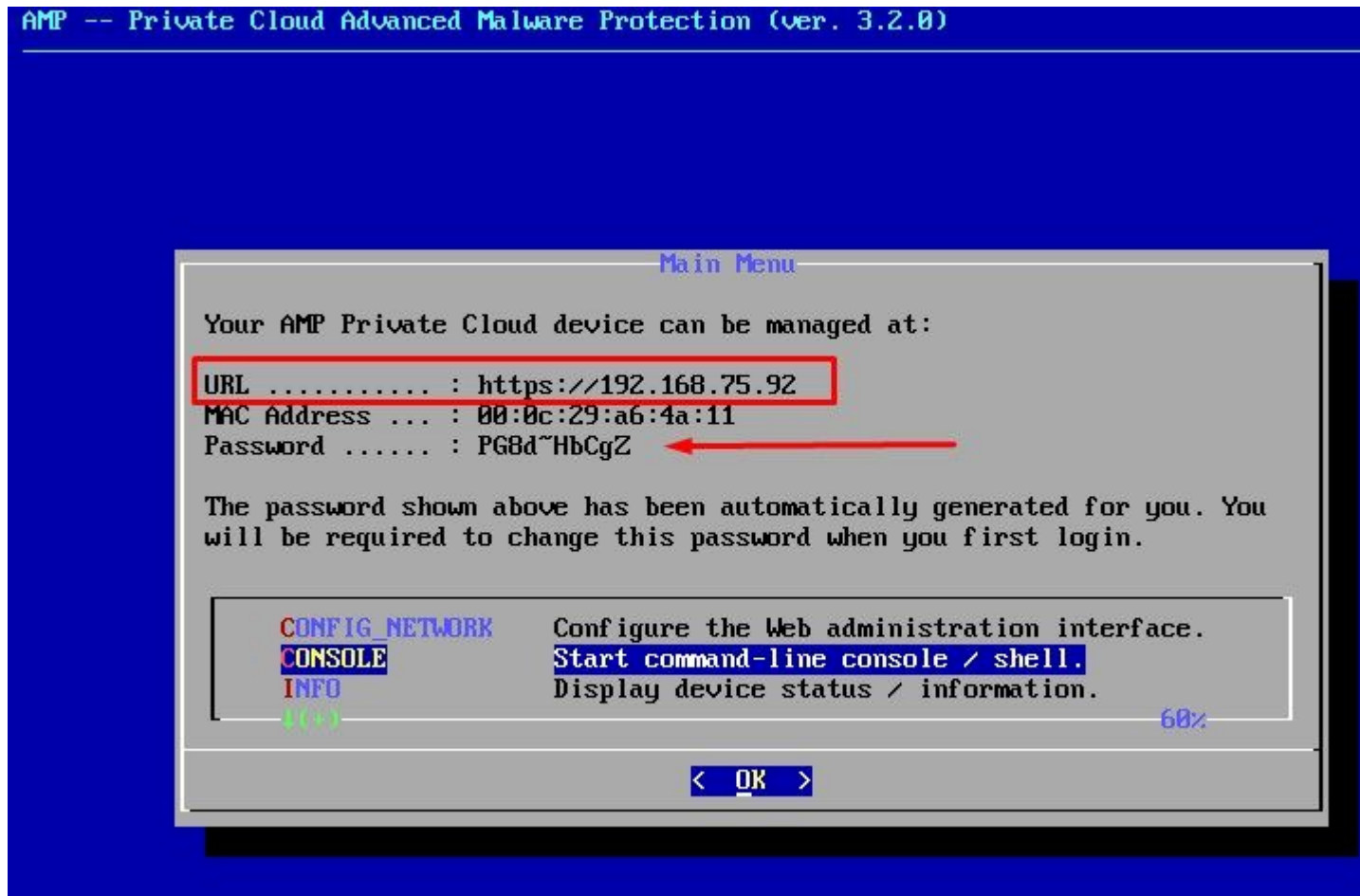
```

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

```

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.

← → ↻ 🏠 <https://192.168.75.92> 🔒 🔍

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

Warning: Potential Security Risk Ahead

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

What can you do about it?

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

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

[Learn more...](#)

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

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

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

Error code: `SEC_ERROR_UNKNOWN_ISSUER`

[View Certificate](#)

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

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**.



Password Required

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

Use one time password
PG&d'HbCgZ

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

[Password Recovery](#)



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**.



⚠ Password Expired

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

Warning

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

Old one time password

New password

Confirm new password

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**.

✓ I HAVE READ AND AGREE

✗ DECLINE

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.



Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

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

Clean Installation

Start > ←

Restore

Local Remote

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

+ Choose Restore File

/data

Start >

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.



- Home
- Configuration
- Operations
- Status
- Integrations
- Support

Installation Options

Only the License section can be altered after installation.

- Install or Restore
- License ✓

License

Device ID

E6[REDACTED]V5

License

No license has been installed.

Install New License

license + Upload License

Upload License

â€f



License was successfully uploaded



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

License

Device ID
E60[redacted]/5

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

Replace License [\(cli\)](#)

â€f

â€f

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.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

[▶ Start Installation](#)

Welcome to Private Cloud

Before you begin

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



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



Two Static IP Addresses

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



DNS Server

Provides hostname resolution to the Private Cloud device.



Hostnames and Trusted Certificates

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

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

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



SMTP Server

Used for emails, alerts, and notifications.



NTP Server

Provides time synchronization across your Private Cloud device and endpoints.



External Internet connection (Proxy Mode only)

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

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**



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Deployment Mode

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



- 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 is not needed.
- Disposition queries are handled by the local database on the Cloud device.
- Content updates contain TETRA definitions as well as file disposition information.
- Updates may be downloaded separately and applied automatically on this device.

¼¼ AIRGAP ONLY ¼¼



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Deployment Mode

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

 Cloud Proxy

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

 Standalone

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



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

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

Configuration

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

Standalone Operation

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



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

⌘ 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**.



- Configuration ▾
- Operations ▾
- Status ▾
- Integrations ▾
- Support ▾

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

AMP for Endpoints Console Account

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

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

â€f

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



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Hardware Requirements

⚠ Hardware Requirements Not Met

Your current configuration does not meet the hardware requirements.

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

Hardware Configuration

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

Shutdown

I understand

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

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

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

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

Once rebooted we continue where we left.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Hardware Requirements

✓ Hardware Requirements Met

Your current configuration meets or exceeds the hardware requirements.

Hardware Configuration

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

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:



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Network Configuration

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

Administration Portal

eth0 / 00:00:00

IP Assignment

Interface Configuration

eth1 / 00:00:00

IP Assignment 1

IP Assignment Static ←

IP Address

Check for IP Address conflict

Subnet Mask

Gateway

DNS

Primary DNS Server ← Use public DNS temporary.

Secondary DNS Server

Next (Applies to All)

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**.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Date and Time

NTP Servers

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

Current System Time

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

¼¼ AIRGAP ONLY ¼¼



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Prepare amp-sync

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

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



½ AIRGAP ONLY ½

Step 5:

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



Installation Options

Only the License section can be altered after installation.

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

Certificate Authorities

Add Certificate Authority



No certificate authorities have been uploaded to this device.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Add Certificate Authority

● Certificate Root (PEM .crt) Disable Strict

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

AMP-vPC-Root-CA.pem



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Certificate Authorities

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

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**.

The screenshot shows the Cisco AMP for Endpoints Private Cloud Administration Portal. The main heading is "Cisco Cloud". Below it, the "Cisco Cloud Configuration" section is visible, with a "Region" dropdown menu set to "Cisco Cloud, North America". A link "View Hostnames (click to expand)" is present. The "Cisco Cloud Identity" section shows "Client Identity" with a partially redacted ID: "0f476ea8[REDACTED]dbbc272a6c". On the left, a navigation menu lists "Installation Options" and "Configuration" sections, with "Cisco Cloud" highlighted under Configuration.

â€f

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**.



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

- Authentication
- AMP for Endpoints Console
- Disposition Server
- Disposition Server
- Extended Protocol

Notifications

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

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

Device Name		
Device Name	HELP	CyberNet vPC 2

â€f

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**.



Maintenance Mode

Sanity Check Failing

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

Add SSH Key

Windows PuTTY

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

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

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

â€f

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 â€œerrorâ€ that you might notice is highlighted with the 3 arrows. To bypass this just simply un-check â€œDisable Strict TLS Checkâ€

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local

Validate DNS Name

Authentication Certificate

Disable Strict TLS Check

Undo

Replace C...

● Certificate (PEM .crt)

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

🔍 Key (PEM .key)

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

vPC2-Authenticator

+ Choose

vPC2-Authenticator

+ Choose Certificate

Without Strict TLS Check



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

Validate DNS Name

Authentication Certificate

Disable Strict TLS Check Undo Refresh

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

vPC2-Authenticatic + Choose Certificate

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.

An error occurred while processing your request.

- Hostname does not resolve

Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery
- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

vPC2-Authentication.cyberworld.local

Validate DNS Name

Authentication Certificate

Disable Strict TLS Check

Undo

Replace Cert

● Certificate (PEM .crt)

- ✗ Certificate file has been uploaded.
- ✗ Certificate is in a readable format.
- ✗ Certificate start and end dates are valid.
- ✗ Certificate contains a subject.
- ✗ Certificate contains a common name.
- ✗ Certificate contains a public key matching the uploaded key.
- ✗ Certificate matches hostname.
- ✗ Certificate is signed by a trusted root authority.

+ Choose Certificate

🔍 Key (PEM .key)

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

+ Choose Key

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.

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

Services

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

1. Download Recovery File

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

[Download](#)

Recovery File Ready for Download

created less than a minute ago

2. Verify Recovery File

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

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



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

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

Clean Installation

A clean installation will be performed.

Installation Type

Cloud Proxy

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

AMP for Endpoints Console Account

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

Recovery

Uploaded Recovery File Matches Current Settings

▶ Start Installation

â€f

ï¼¼ï¼¼ AIRGAP ONLY ï¼¼ï¼¼



Installation Options

Only the License section can be altered after installation.

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

Configuration

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

Services

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

Other

- > Recovery ✓
- > Review and Install ✓

▶ Start Installation

Review and Install

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

Clean Installation

A clean installation will be performed.

Installation Type

Standalone Air Gap



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

AMP for Endpoints Console Account

Name	Roman Valenta
Email Address	rval[REDACTED]@m
Business Name	Cisco vamrodia PC v2

Recovery

Uploaded Recovery File Matches Current Settings

▶ Start Installation

â€f

â€f

ï½ï½ AIRGAP ONLY ï½ï½

You see similar input like thisâ€!

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

The device is installing...

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

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

Your device will need to be rebooted after this operation.

Reboot

Output

le_chunk

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

Download Output

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 5 minutes.

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

Your device will need to be rebooted after this operation.

Reboot

Output

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

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

Download Output

⌘ AIRGAP ONLY ⌘

The device is installing...

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

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

Your device will need to be rebooted after this operation.

Reboot

Output

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

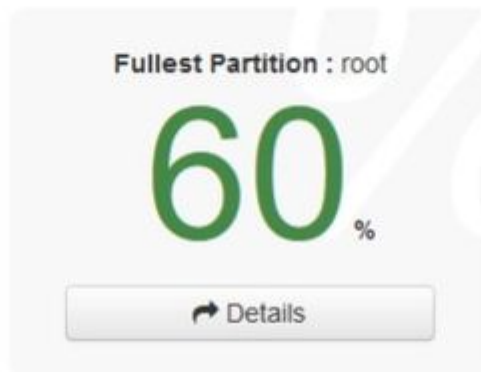
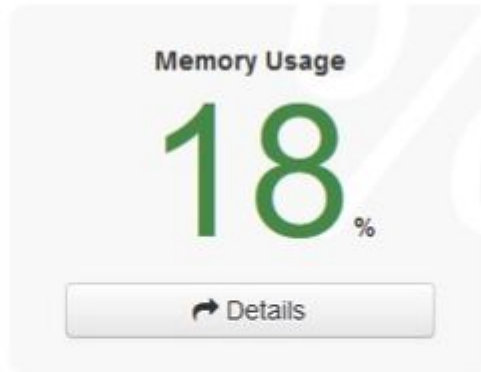
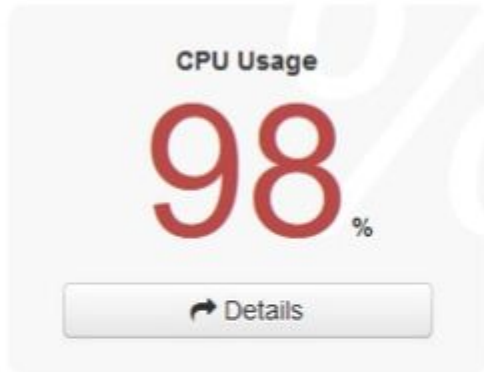
Download Output

½½ AIRGAP ONLY ½½

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.



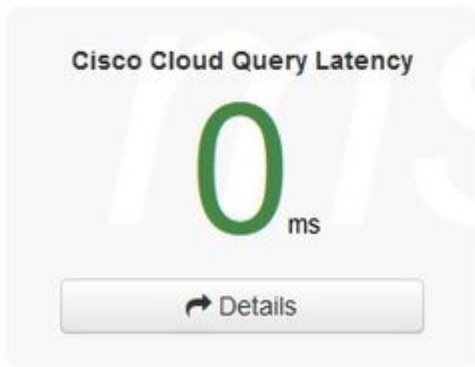
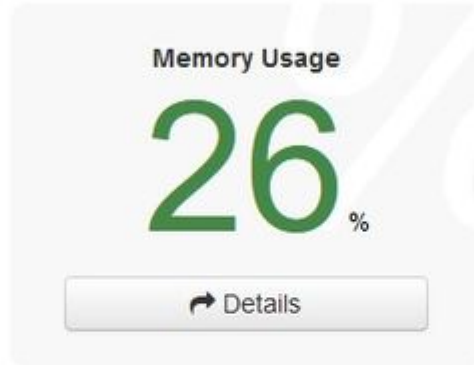
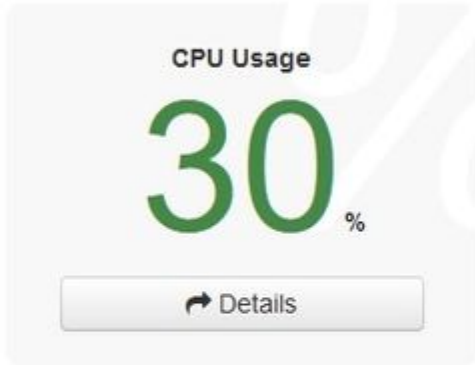
Key Metrics



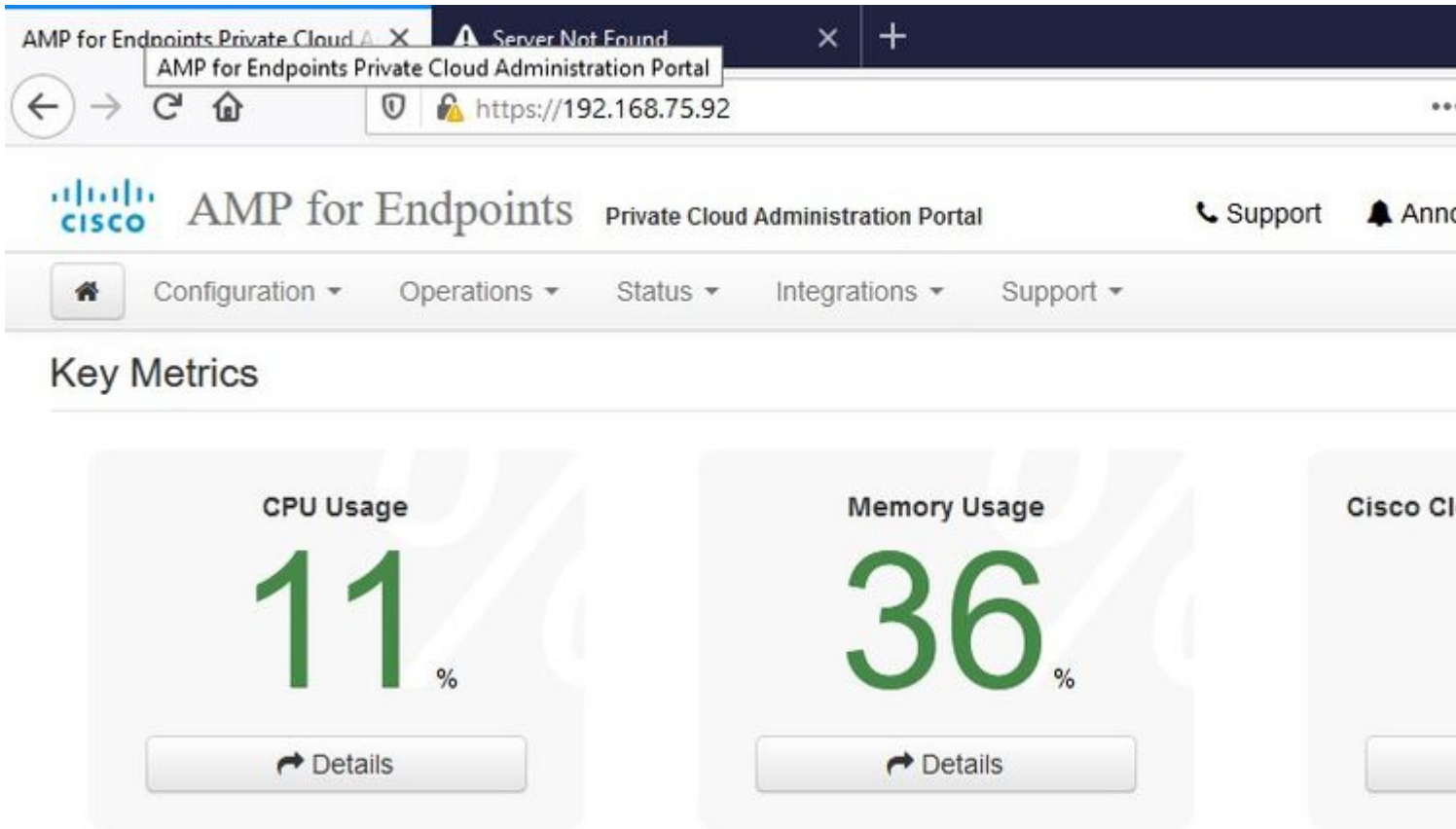
After few minutes...



Key Metrics



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



⚠️ AIRGAP ONLY ⚠️

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 the VM or stored in NFS location.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

❌ Sanity Check Failing

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

i Details

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

Key Metrics

CPU Usage

11%

↶ Details

Memory Usage

28%

↶ Details

Active Connections

0

↶ Details



✖ **Sanity Check Failing**

Updates keep your Private Cloud device up to date.

↻ Check Update ISO

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

Content

✖ **3.2.0_202010081917**

Client Definitions, DFC, Tetra Content Version

! **ABSENT**

Protect DB Version

! Import a Protect DB snapshot

Checked 1 minute ago; the update check failed.

Software

✖ **3.2.0_202010082118**

Private Cloud Software Version

Checked 1 minute ago; the update check failed.

AirGap Update Package

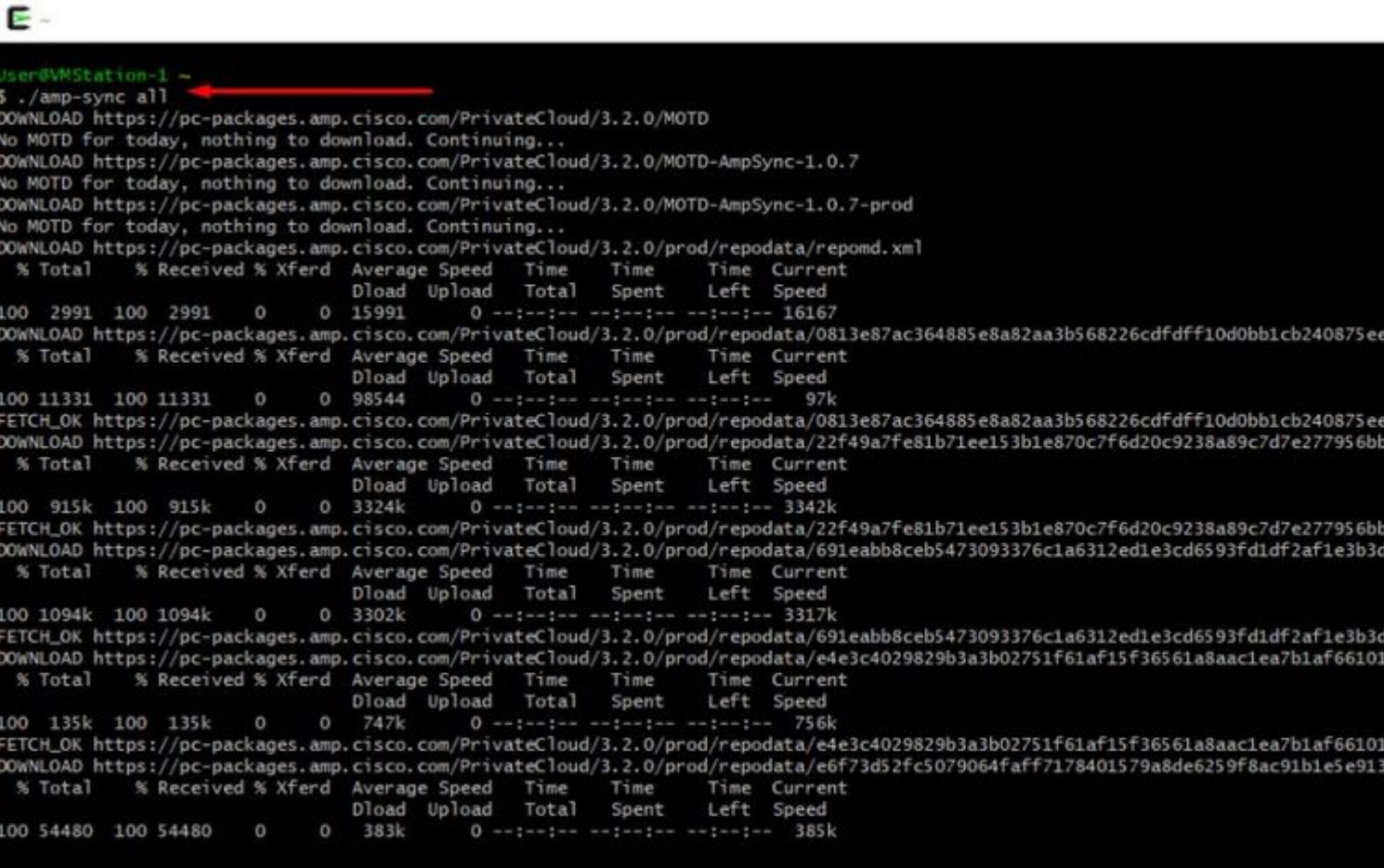
For the first time we have to use this command in order to receive the Protect DB

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

Note: Download all the packages via this command and then verify could take **more than 24Hrs.** 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/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100 11331    100 11331    0    0 98544      0  --:--:--  --:--:--  --:--:--  97k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/0813e87ac364885e8a82aa3b568226cdfdff10d0bb1cb240875ee
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100 915k    100 915k    0    0 3324k      0  --:--:--  --:--:--  --:--:-- 3342k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/22f49a7fe81b71ee153b1e870c7f6d20c9238a89c7d7e277956bb
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3d
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100 1094k    100 1094k    0    0 3302k      0  --:--:--  --:--:--  --:--:-- 3317k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/691eabb8ceb5473093376c1a6312ed1e3cd6593fd1df2af1e3b3d
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100 135k    100 135k    0    0 747k      0  --:--:--  --:--:--  --:--:--  756k
FETCH_OK https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e4e3c4029829b3a3b02751f61af15f36561a8aac1ea7b1af66101
DOWNLOAD https://pc-packages.amp.cisco.com/PrivateCloud/3.2.0/prod/repodata/e6f73d52fc5079064faff7178401579a8de6259f8ac91b1e5e913
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100 54480    100 54480    0    0 383k      0  --:--:--  --:--:--  --:--:-- 385k
```



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



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


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

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

```
=====
```

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

```
=====
```

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

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

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

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

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

â€f

[Release notes](#) Page #58. As you can see â€xorrisoâ€ 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.

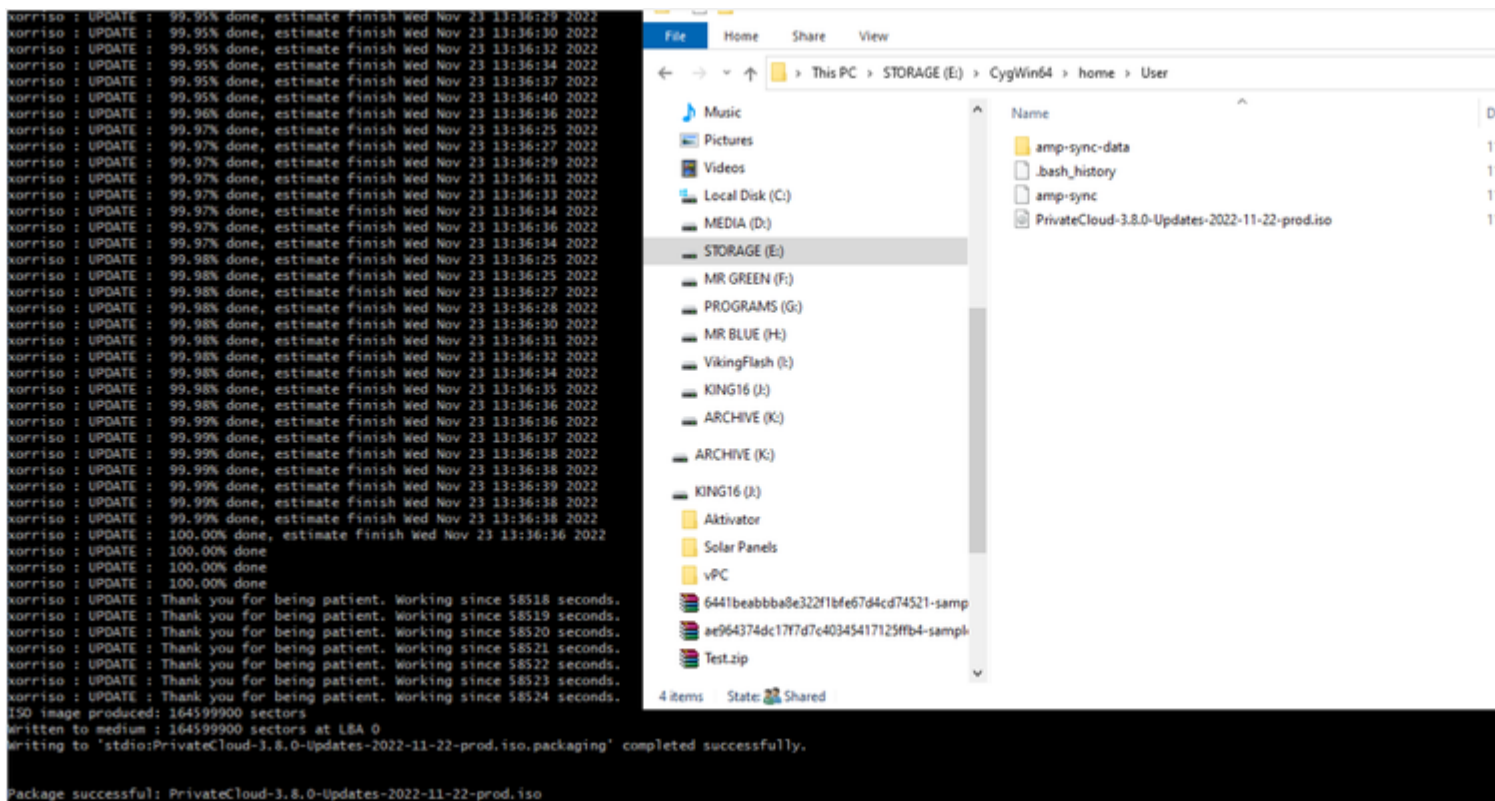
- Install dependencies via apt.
 - > `sudo apt install xorriso`
 - > `sudo apt install xmlstarlet`

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`

â€f

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 â€“ 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.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

❌ **Sanity Check Failing**

Backups create a copy of your configuration and databases.

Manual Backup

[Perform Backup](#)

Last Backup Successful

Transferring Backups To External Storage Is Recommended

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

[Backup Job Details](#)

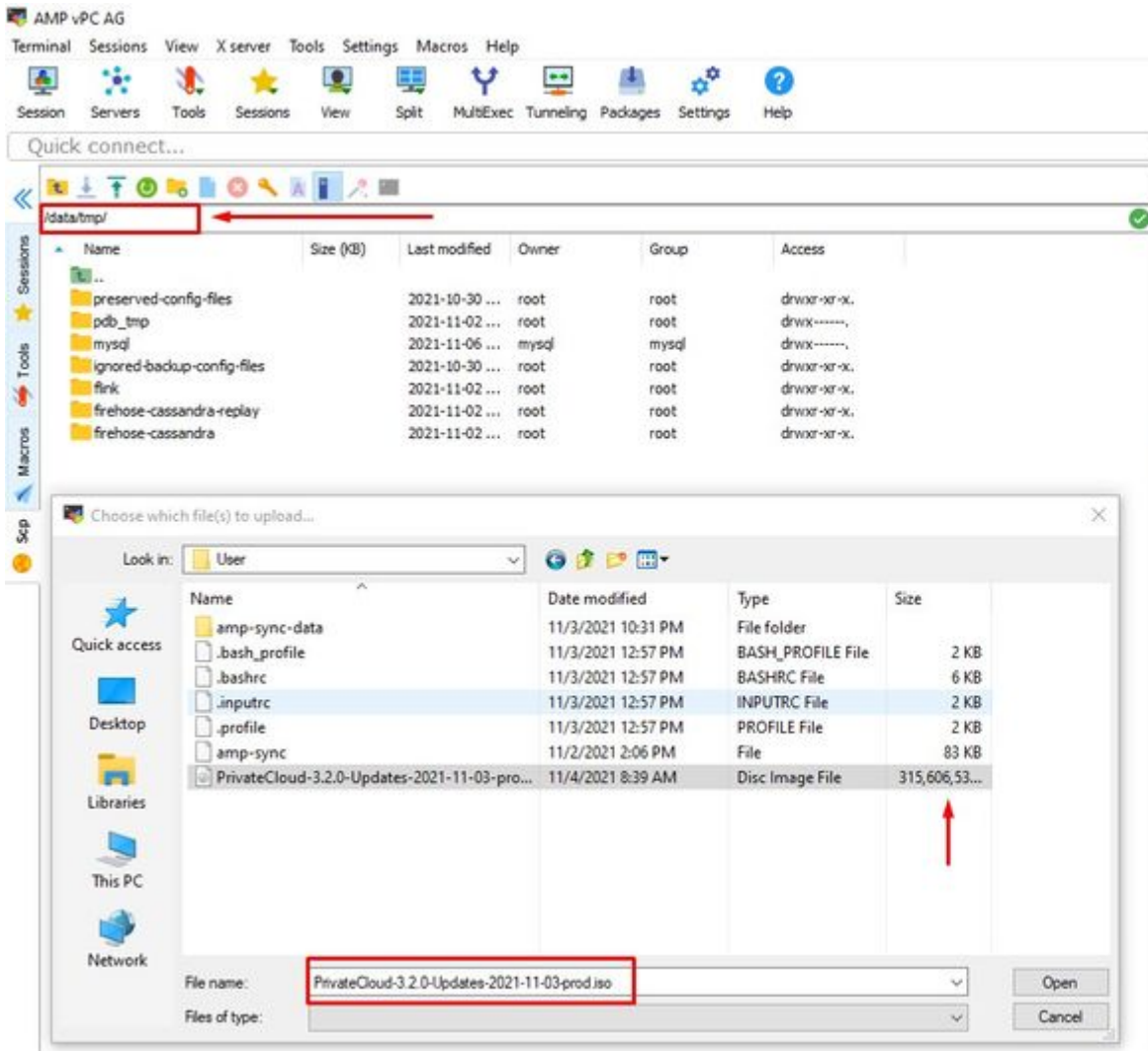
Previous Backups

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

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

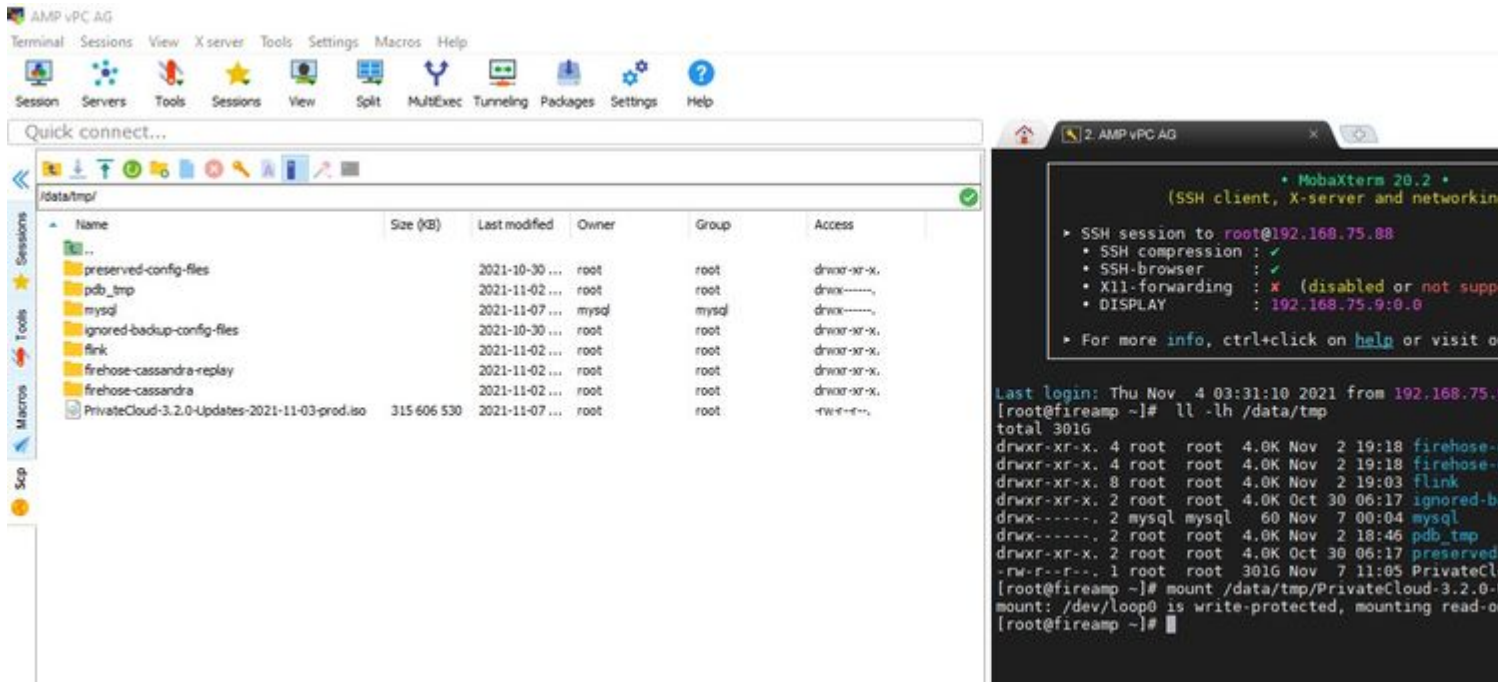
Transfer the latest ISO generated with amp-sync to the VPC. This can take up to several hours as well based on your speed. In this case the transfer took over 16Hrs

/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/
```

â€f

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



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Check Update ISO

Checking ISO for updates...

Content

3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

ABSENT

Protect DB Version

Checked 9 minutes ago; the update check failed.

Software

3.2.0_202010082118

Private Cloud Software Version

A software update is available.

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



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download

Check Update ISO

Content

3.2.0_202010081917
Client Definitions, DFC, Tetra Content Version

Update C
Import P

ABSENT
Protect DB Version

A content update is available.

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

Software

3.2.0_202010082118
Private Cloud Software Version

Update S

A software update is available.

Then select Import Protect DB.

â€f



Sanity Check Failing

Updates keep your Private Cloud device up to date.

Download

Check Update ISO

Content

 **20211102210054**
Client Definitions, DFC, Tetra Content Version

Update

Import

 **ABSENT**
Protect DB Version

Import a Protect DB snapshot to your

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

Software

 **3.2.0_202010082118**
Private Cloud Software Version

Update

 [A software update is available.](#)

â€f

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

⚙️ Protect DB importing

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

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

☰ Output

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

📄 Download Output

â€f

⚙️ Protect DB importing

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

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

☰ Output

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

📄 Download Output

⚙️ Protect DB importing

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

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

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

â€f

Problem #1 - Exhausted room in Data Store


â€f


Here you can run 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 below version 3.5.2

This image below 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 temporarily 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 words 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

Event Details

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

Description: 

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

Error Stack: [Hide](#)

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

Related Events: [Show](#)

â€f

Problem #2 - 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.



Configuration

Operations

Status

Integrations

Support

Maintenance Mode

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

Sanity Check Failing

Disabling TLS

Updates keep your Private Cloud device up to date.

Check Update ISO

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

Content

3.2.0_202010081917

Client Definitions, DFC, Tetra Content Version

ABSENT

Protect DB Version

Checked 24 minutes ago; the update check failed.

Import a Protect DB snapshot

The previous

Software

3.5.3_202111080345

Private Cloud Software Version

Checked 24 minutes ago; the update check failed.

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

â€f



Maintenance Mode

Sanity Check Failing

Disabling

Home / Operations - Update Device / Update Check Details

✖ The update check failed

Something went wrong while checking for updates.

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

Output

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

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

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

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

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

Download Output

â€f

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.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

✖ Maintenance Mode

✖ Sanity Check Failing

ℹ Disabling T...

Mount an Update ISO

ISO Configuration

Mount Type

ISO ▾

ISO

NFS4

NFS3

Mount Status

No ISO mounted



❌ **Sanity Check Failing**

ℹ️ **Disabling TLS 1.0/1.1**

✅ **Config**

Mount an Update ISO

ISO Configuration

Mount Type

NFS3

Remote Share

192.168.75.4:/AMPAG

Remote ISO File

PrivateCloud-3.5.3-Updates-2021-11-16-prod.iso

✔ Mount

Mount Status

Mounted ISO

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

Updates keep your Private Cloud device up to date.



 Check Update ISO

Content

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

 **ABSENT**
Protect DB Version

 [A content update is available.](#)

 ISO contains Protect DB snap
 Import a Protect DB snaps

Software

 **3.5.2_202110130433**
Private Cloud Software Version

 [A software update is available.](#)

â€f

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



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Sanity Check Failing

Updates keep your Private Cloud device up to date.

Check Update ISO

Content

i 3.5.2_202110122340

Client Definitions, DFC, Tetra Content Version

! **ABSENT**

Protect DB Version

i [A content update is available.](#)

✓ ISO contains Protect DB s

! Import a Protect DB sn

Software

i 3.5.2_202110130433

Private Cloud Software Version


i [A software update is available.](#)

â€f


⚙️ Protect DB importing

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

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

 **Output**

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

 Download Output

â€f



✔ Protect DB imported successfully

A Protect DB snapshot was successfully imported.

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

☰ Output

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

📄 Download Output

Next update start automatically



⚙ Importing Protect DB deltas.

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

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

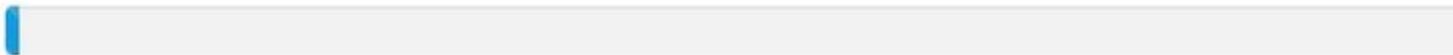
Queued Updates

20211116-2135

Queued Protect DB Update Version



2021



0.80%

Update Progress

â€f

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.



✔ Content updated successfully

The device successfully performed a content update.

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

Output

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

Download Output

â€f

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>

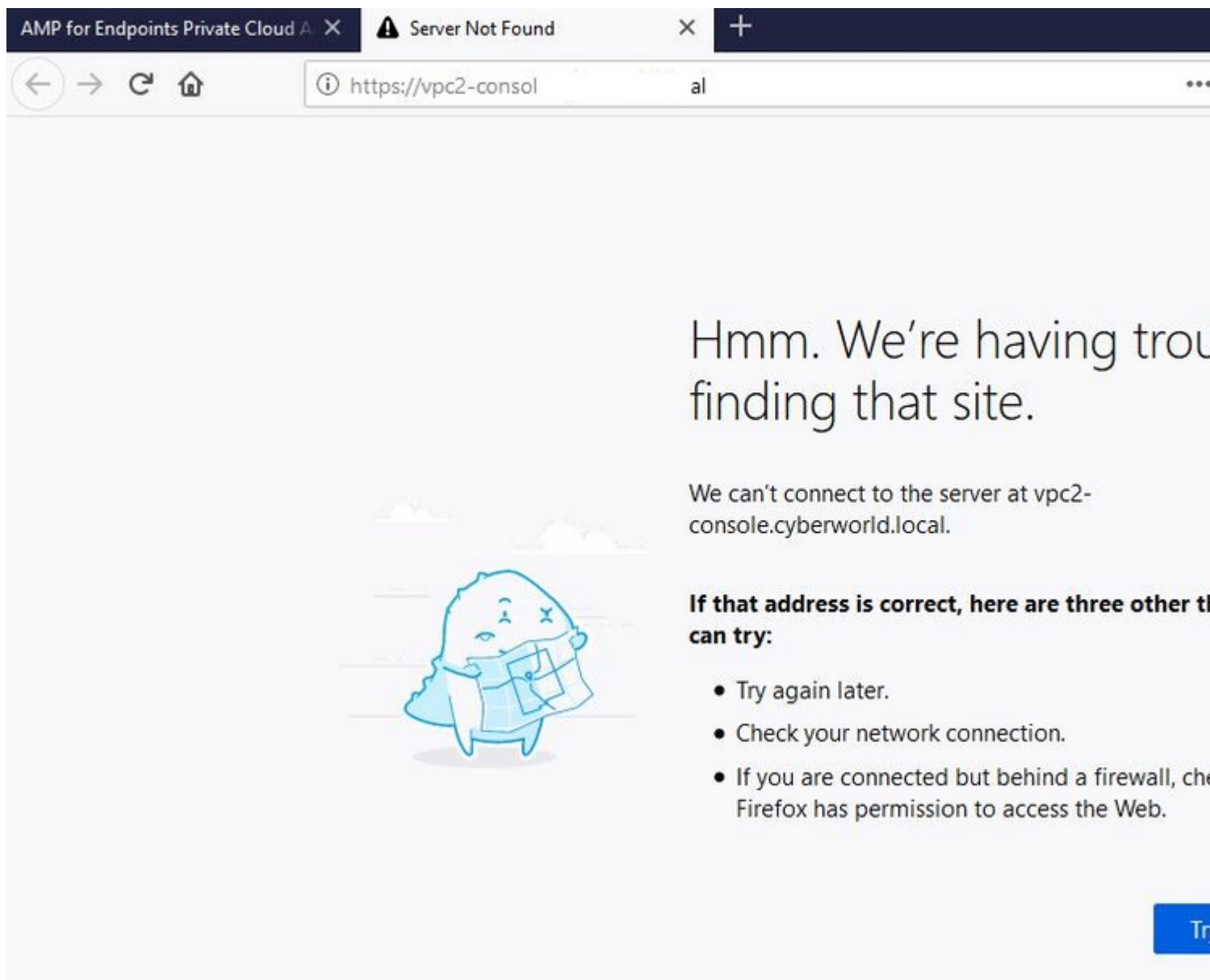
â€f

ï½ï½ AIRGAP ONLY ï½ï½

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.



AMP for Endpoints Private Cloud A X Server Not Found X +

https://vpc2-consol al

Hmm. We're having trouble finding that site.

We can't connect to the server at vpc2-console.cyberworld.local.

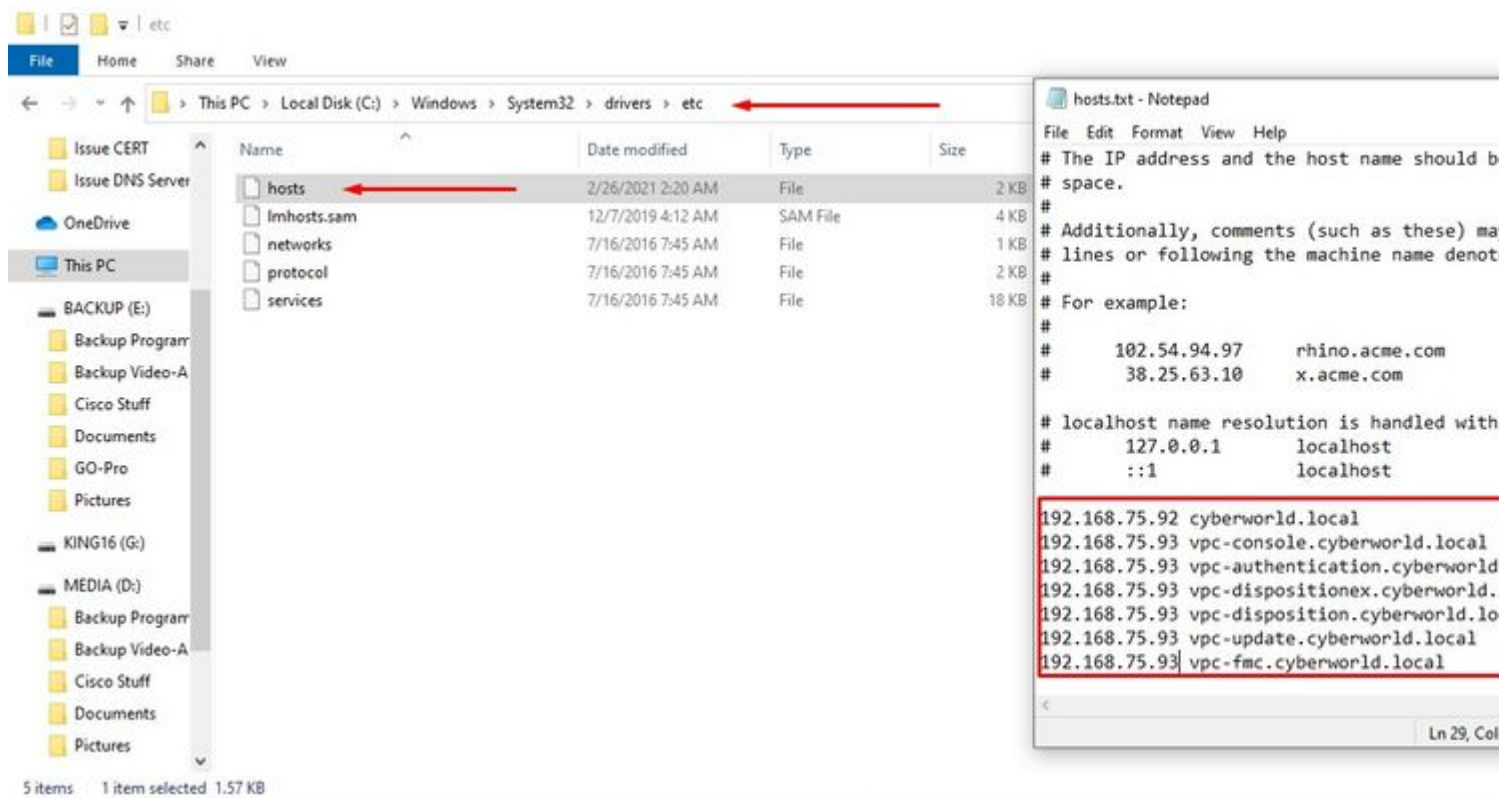
If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

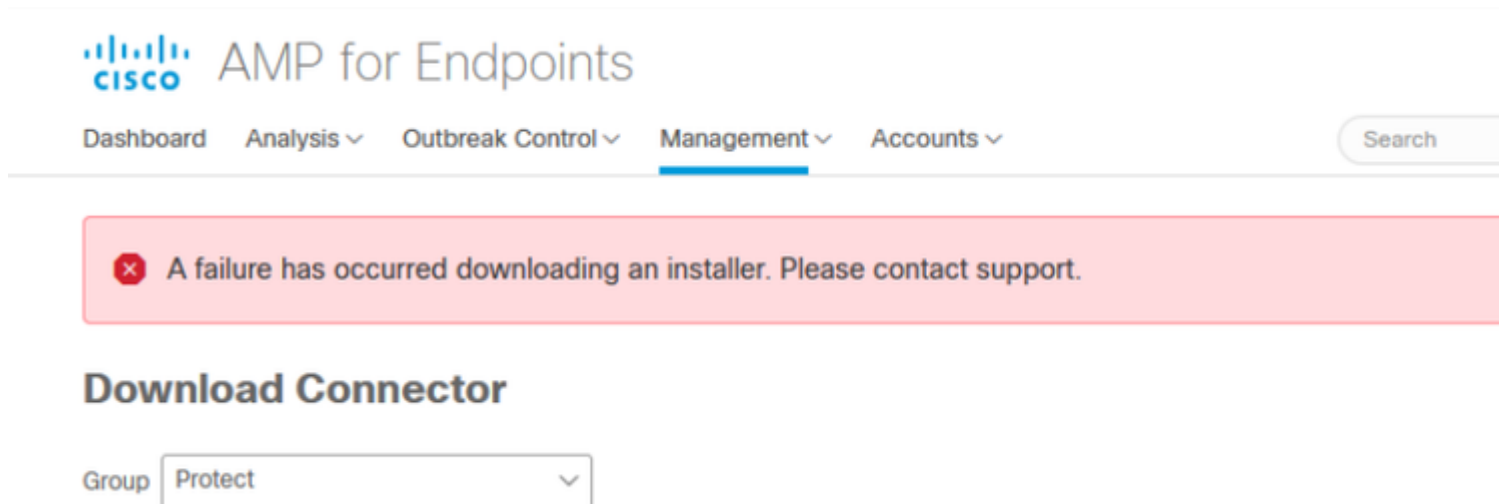
Tr

â€f

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 +0000)

=====

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.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Con

- Device Summary
- Change Password

network settings.

Adm

Cisco Cloud

Network

Date and Time

Certificate Authorities

Proxy

Inter

Notifications

License

Email

Backup

SSH

Syslog

Updates

Services ▶

IP Assignment

IP Address 192.168

Check

Subnet Mask 255.255

Gateway 192.168

Warning: Address and Hostname Changes

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

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

DNS

Primary DNS Server

192.168.75.4





Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

⚙ Configuration Changed

Configuration changes do not take effect until reconfiguration is performed.

 [Reconfigure Now](#)

 [Reconfiguration](#)



✔ Configuration saved.



Configuration ▾

Operations ▾

Status ▾

Integrations ▾

Support ▾

Home / Operations - Apply Configuration / Details

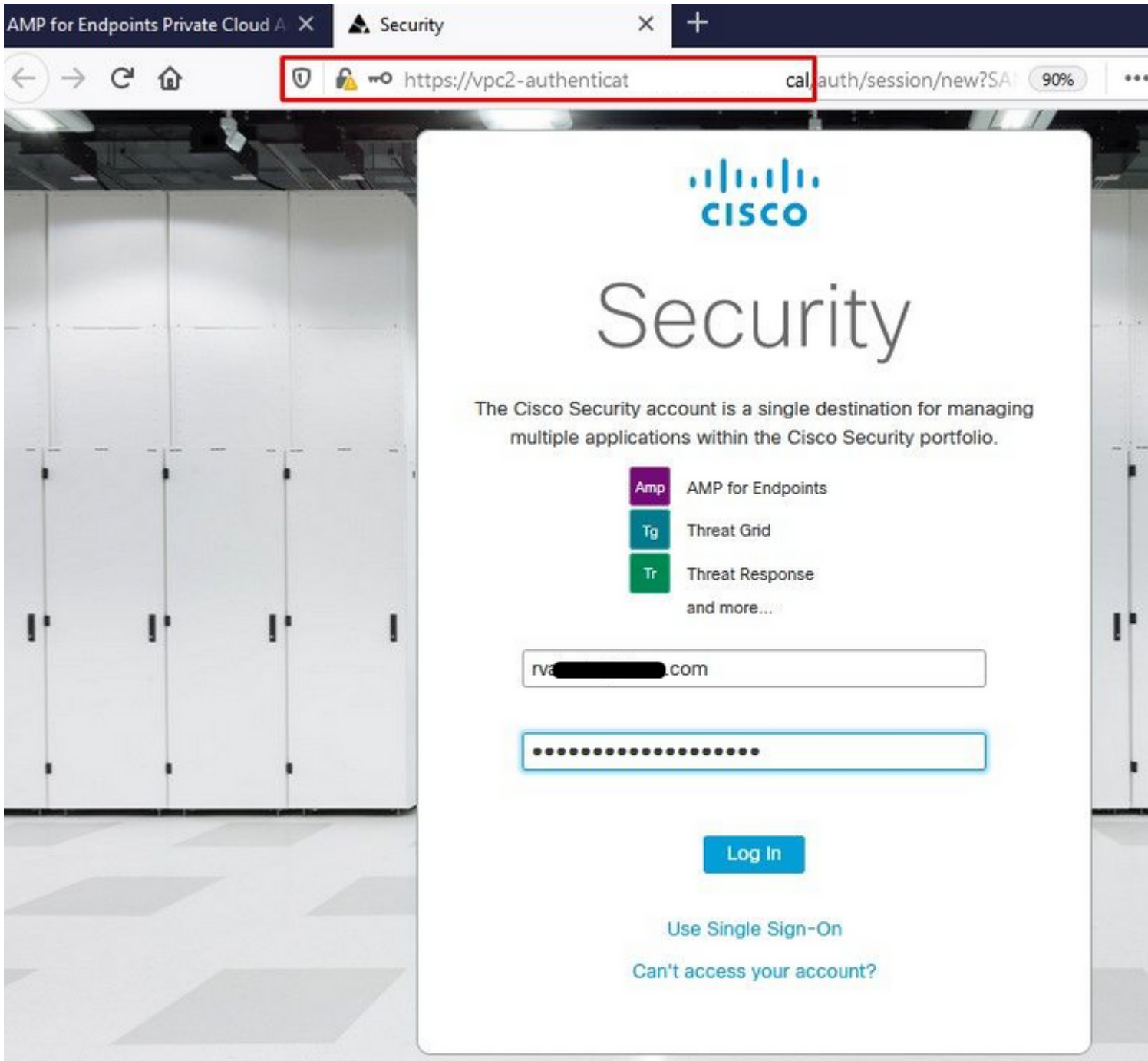
State	Started	Finished
Running	Sun Apr 11 2021 20:19:00 GMT-0400 (Eastern Daylight Time) 0 day, 0 hour, 1 minute, 45 seconds ago	Please wait...

Output

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

Download Output

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



â€f

â€f

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**.

AMP for Endpoints

Dashboard Analysis Outbreak Control Management Accounts Search

Dashboard

Cisco - rvalenta

Dashboard Inbox Overview Events

Getting Started

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

Deploy AMP for Endpoints Connectors

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

Demo Data

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

Demo Computers

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

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

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

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

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

â€f

Download connector.

Opening amp_Protect.exe

You have chosen to open:

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

Would you like to save this f

Step 1: Existing Security Products

Step 2: Set Up Proxy

Step 3: Download Connector

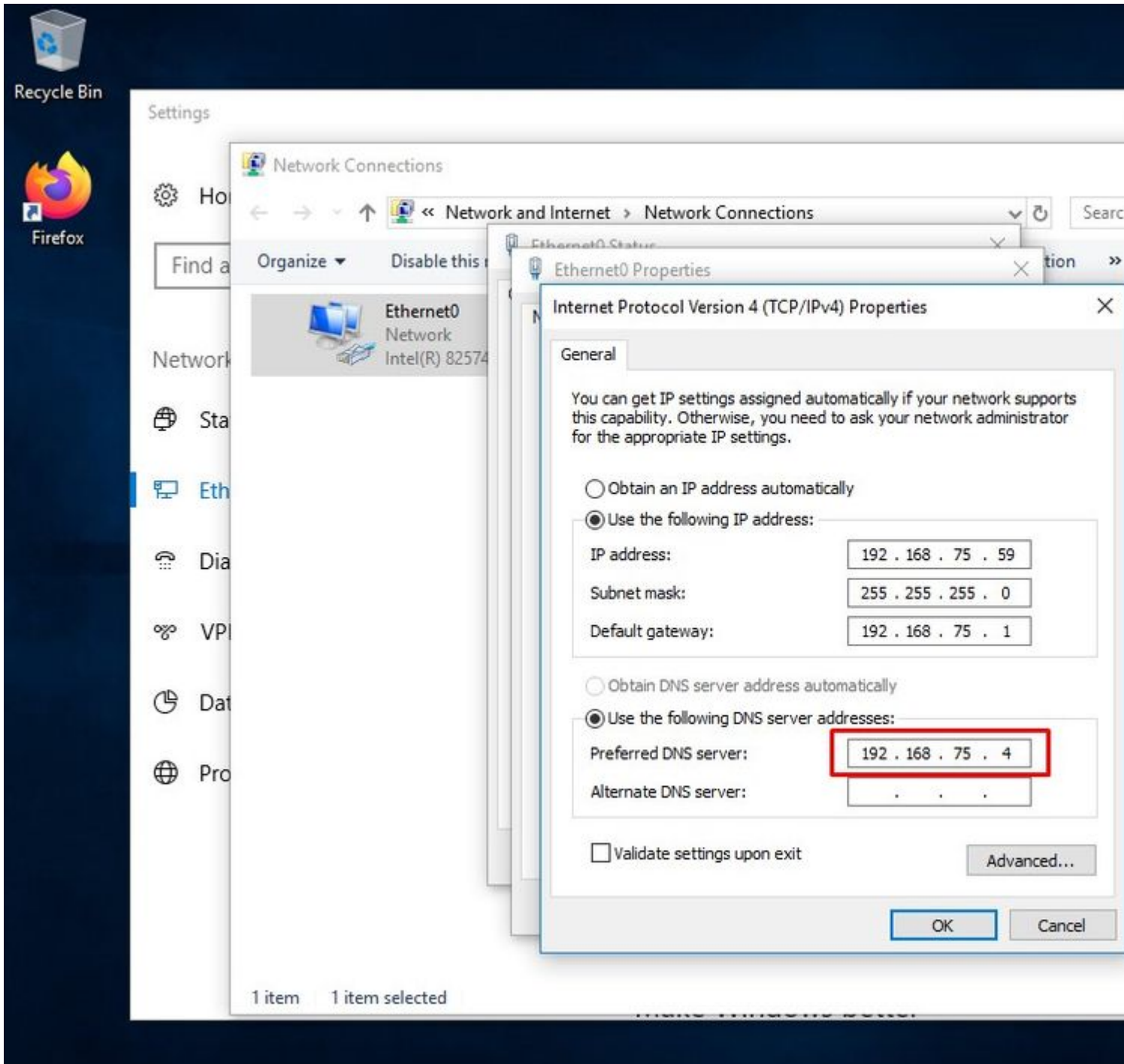
Audit Only	Protect	Triage	Server	Windows Domain Controllers
Used when you're still learning about the product and want to install it without any impact to your existing systems.	Used during normal operations and you want Cisco AMP for Endpoints to quarantine a file.	Used when you have a known or suspected infected machine.	Used when you're installing a connector on standard Windows servers.	Used when you're installing a connector on Windows Domain Controllers.
Policy Details	Policy Details	Policy Details	Requirements	Requirements
Files Audited	Files Quarantined	Files Quarantined	Files Audited	Files Audited
Network Blocked	Network Blocked	Network Blocked	Network Off	Network Off
Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA	Offline Engine TETRA
Download	Download	Download	Download	Download

[Back](#) [Next](#)

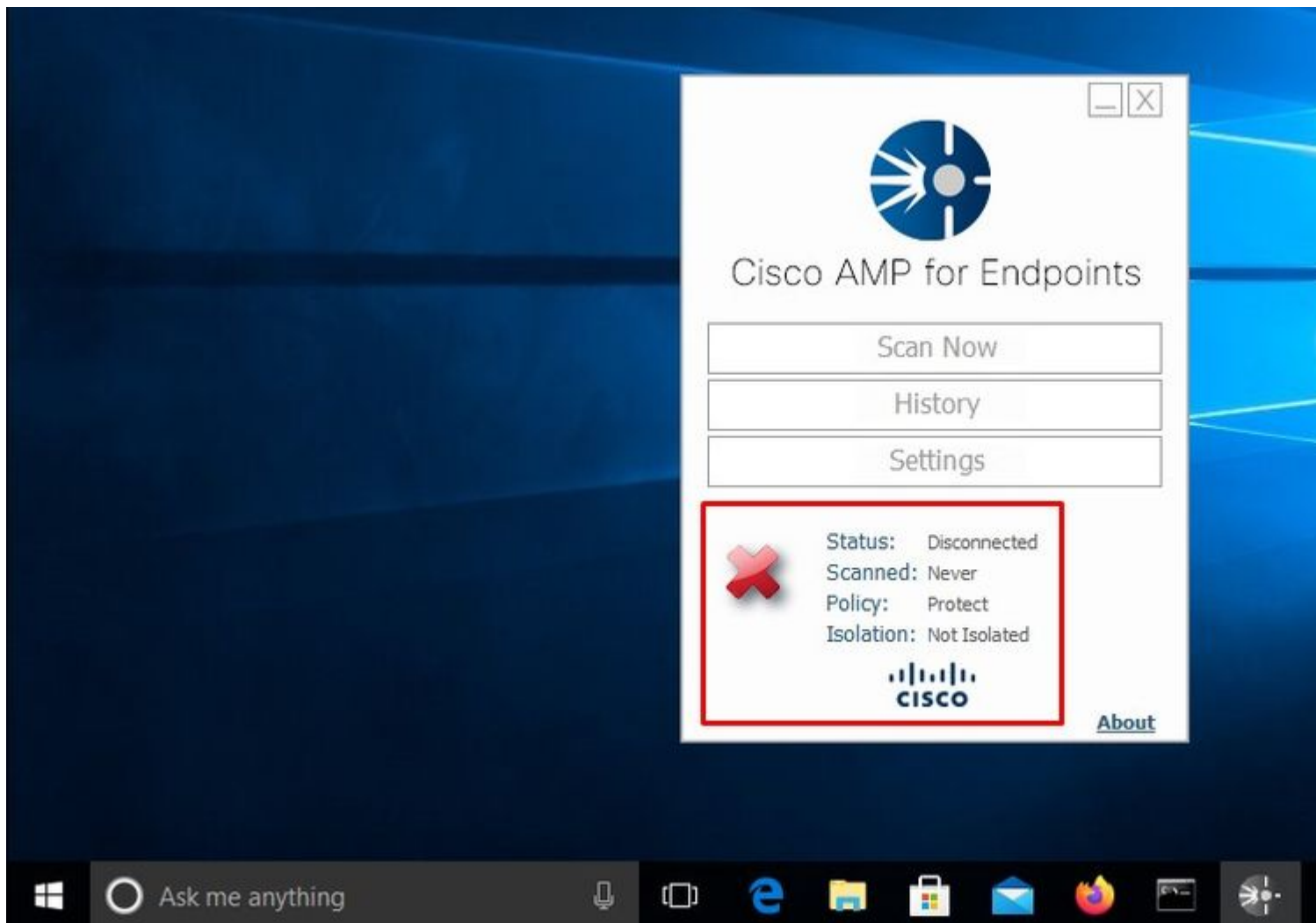
Step 4: Verify, Contain, and Protect

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.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
```

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 AMP for Endpoints

Scan Now

History

Settings

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

 [About](#)

Certificate

General Details Certifi

 **Certificate**

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

Issued to: All

Issued by: All

Valid from: 4/





Cisco AMP for Endpoints

Scan Now

History

Settings

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



[About](#)

Certificate Import Wizard

Welcome to the Certificate Import Wizard

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

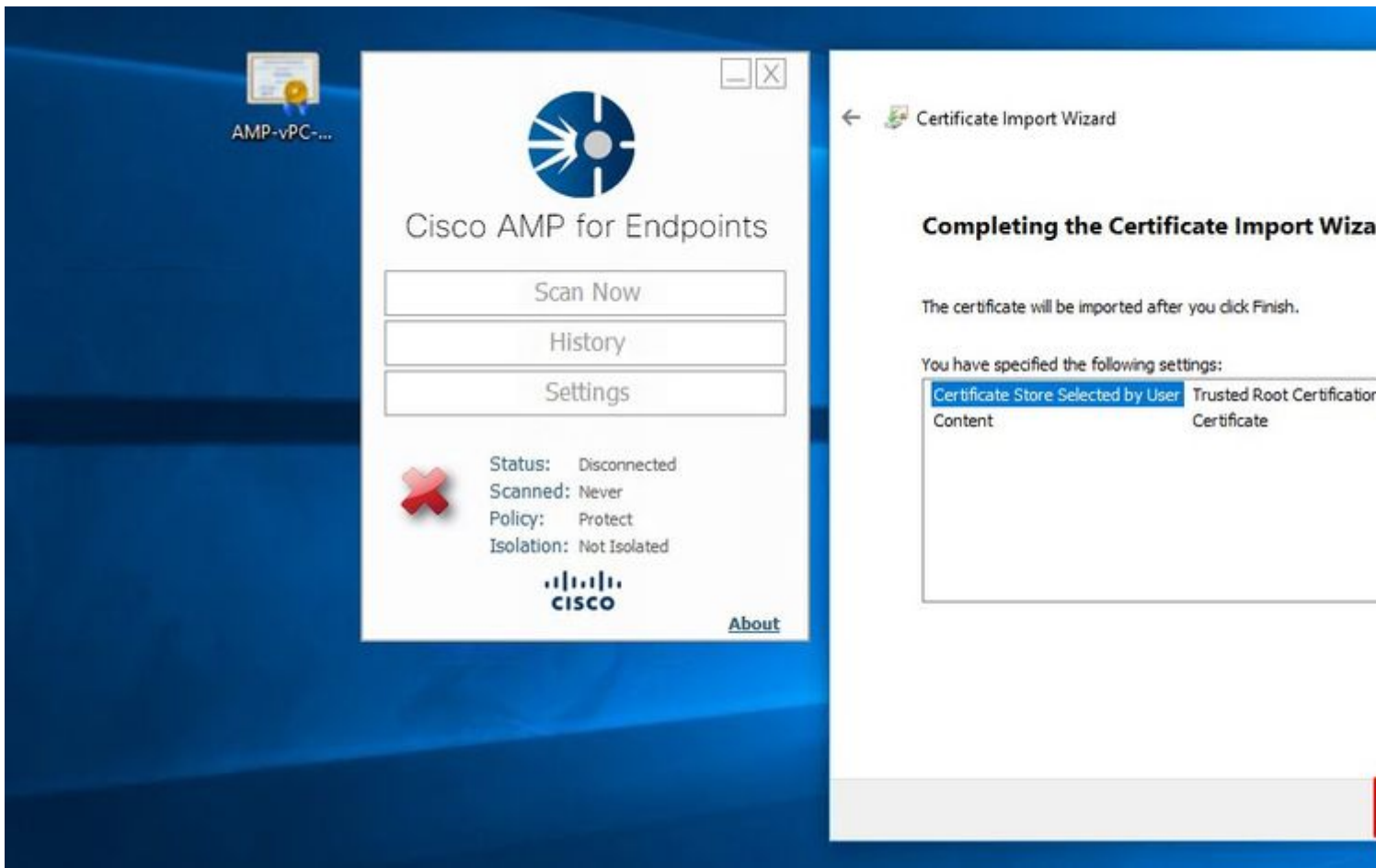
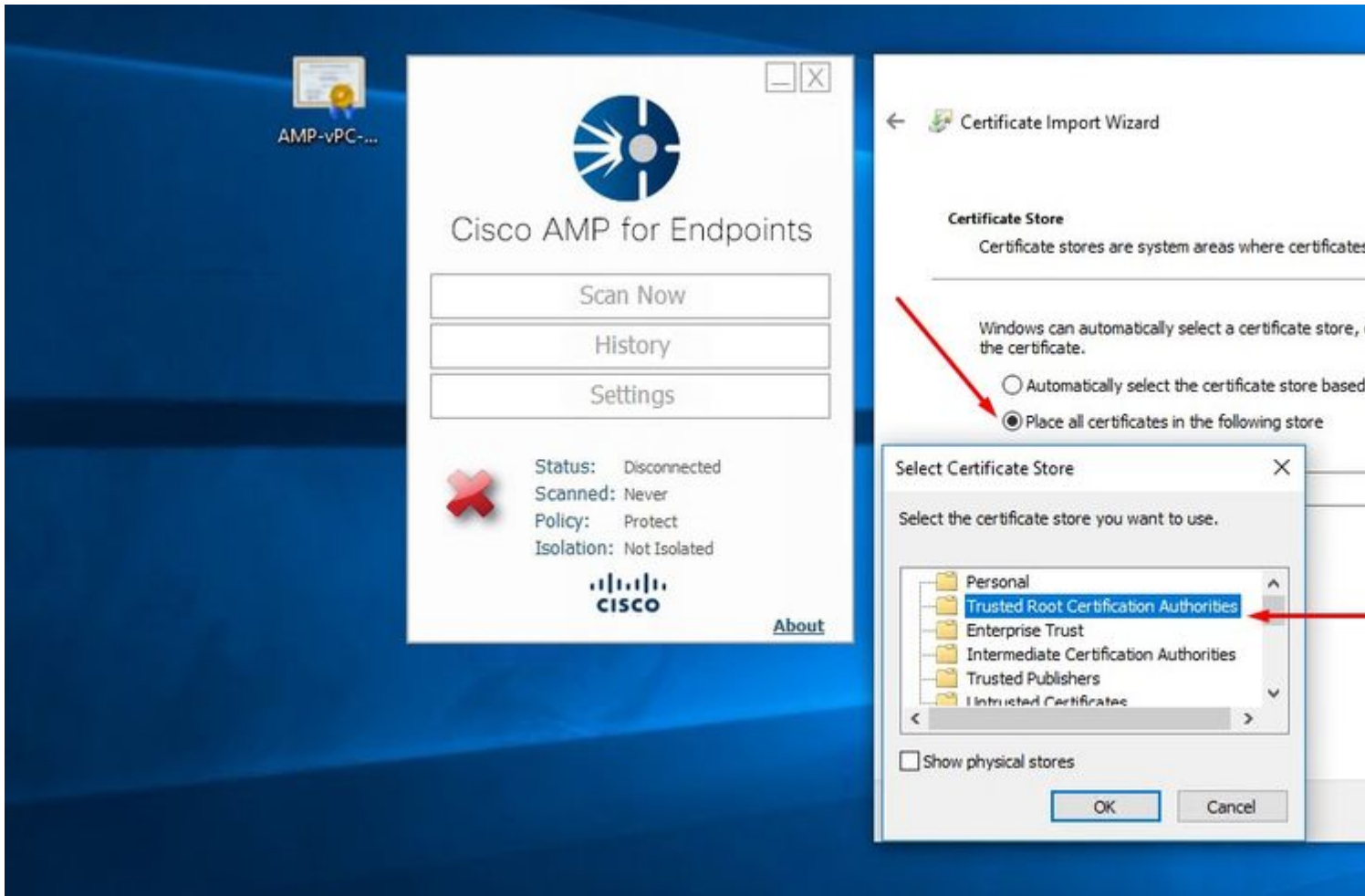
A certificate, which is issued by a certification authority and contains information used to protect data or to establish connections. A certificate store is the system area where certificates are stored.

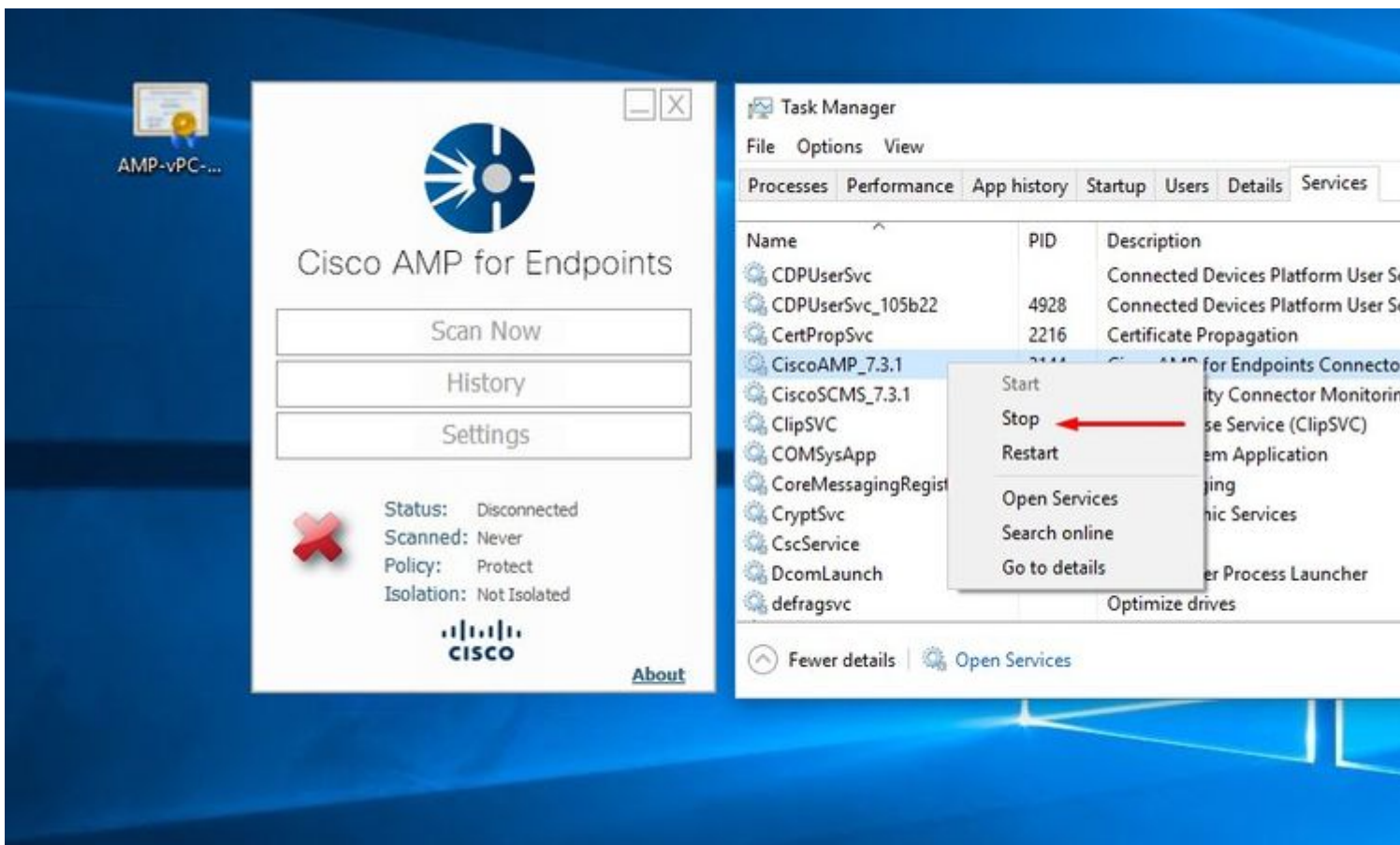
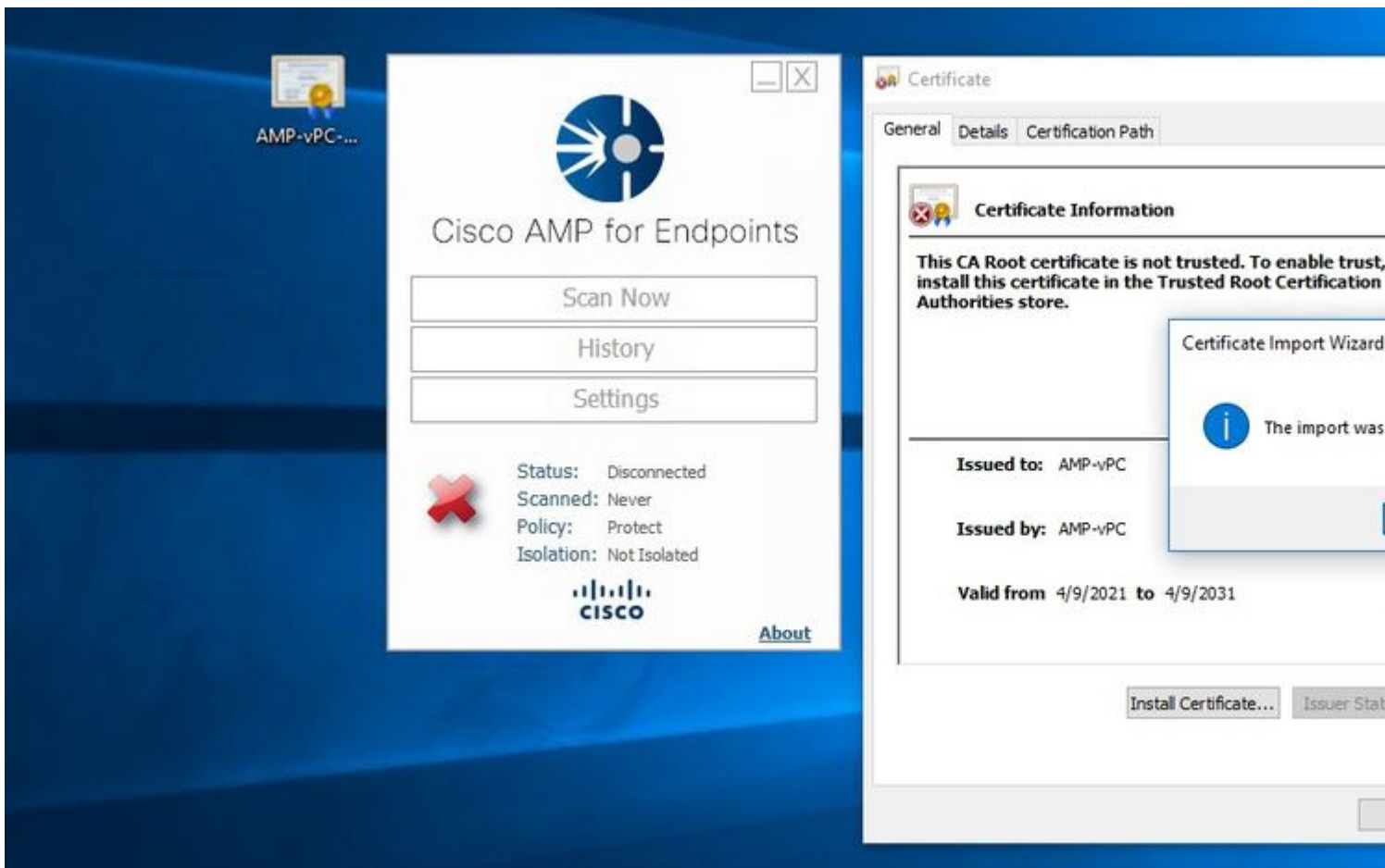
Store Location

Current User

Local Machine

To continue, click Next.





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





Cisco AMP for Endpoints


Scan Now

History

Settings



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



CISCO

[About](#)

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

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

Fewer details | Open Services

AMP for Endpoints Private Cloud A X Dashboard X +

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

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

Dashboard

Dashboard **Inbox** Overview Events

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

0% compromised ⓘ

Compromises ⓘ Inbox

Top 0 / 1

Protect

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

Quarantined Detections ⓘ Quarantine Events

Top 0 / 1

Protect

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

Significant Compromise Artifacts ⓘ

No artifacts

Compromise Event Types ⓘ

No event types

â€f

Tested malicious activity

AMP for Endpoints

Dashboard Analysis Outbreak Control Management Accounts

Dashboard

Dashboard **Inbox** Overview Events

Refresh All Auto-Refresh

Reset New Filter

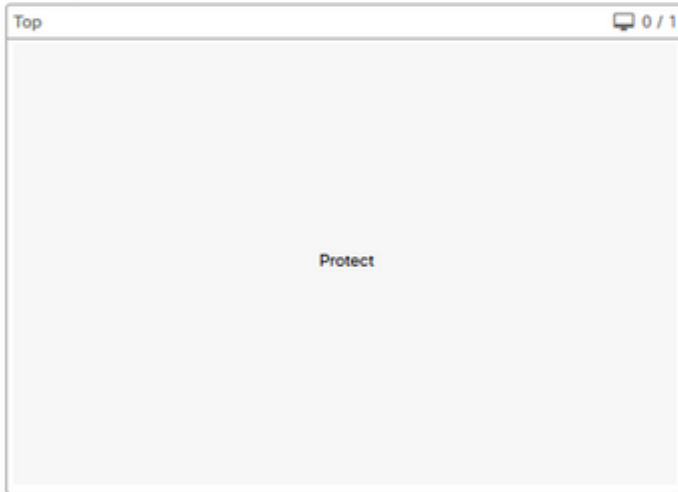
0% compromised

Inbox Status

0 Require Attention 0 In Progress 0 Resolved

Compromises

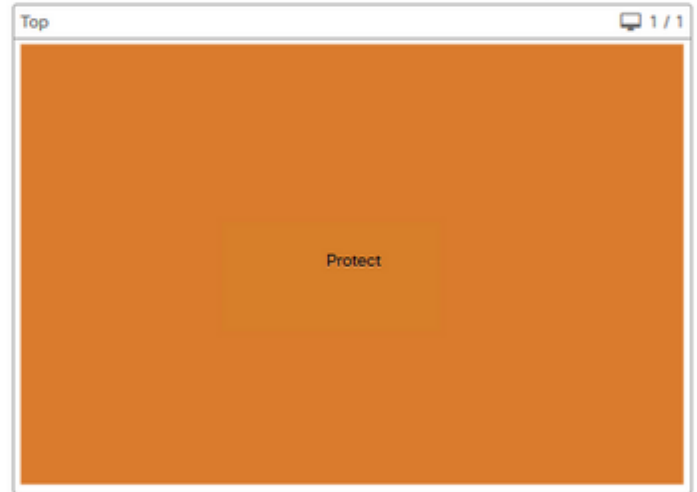
Inbox



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

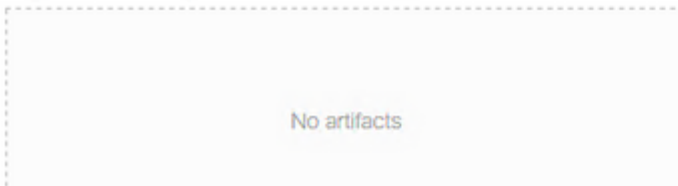
Quarantined Detections

Quarantine Events

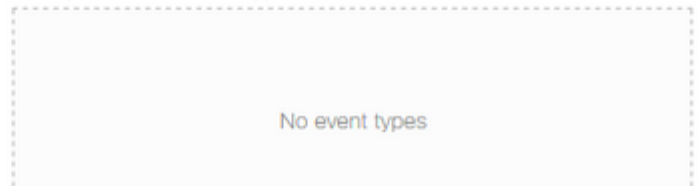


13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12
MAR APR

Significant Compromise Artifacts



Compromise Event Types



â€f