FireAMP Private Cloud 3.0.1 upgrade procedure

Contents

Introduction

This document describes how to upgrade a FireAMP Private Cloud (vPC) version 2.4.4 to version 3.0.1. Please note that upgrade procedure requires a new Virtual Machine instance for 3.0.1 version.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Installation an Open Virtual Appliance (OVA) Template in the VMWare ESXi
- Basic knowledge of how Virtual AMP Cloud works and operates

Hardware Requirements

Below are the minimum hardware requirements for the FireAMP Private Cloud:

- vSphere ESX 5 or higher

- 8 CPUs
- 64 GB RAM
- 1 TB free disk space on the VMWare datastore
- Type of drives: SSD required
- RAID Type: One RAID 10 group (stripe of mirrors)
- Minimum VMware data store size: 1TB
- Minimum Data Store Random Reads for the RAID 10 Group (4K): 60K IOPS
- Minimum Data Store Random Writes for the RAID 10 Group (4K): 30K IOPS

> **Caution**: The Private Cloud OVA creates the drive partitions, so there is no need to specify them in VMWare.

> **Note**: Refer to the FireAMP Private Cloud User Guide for more information about Hardware Requirements.

Components Used

The information in this document is based on these hardware and software versions:

- FireAMP Private Cloud 2.4.4
- FireAMP Private Cloud 3.0.1
- VMWare ESXi 5.0 or greater

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, make sure that you understand the potential impact of any command.

Upgrade process

This section provides step by step instructions on how to collect the backup from the FireAMP Private Cloud 2.4.4 version and how to properly restore it on FireAMP Private Cloud 3.0.1 version.

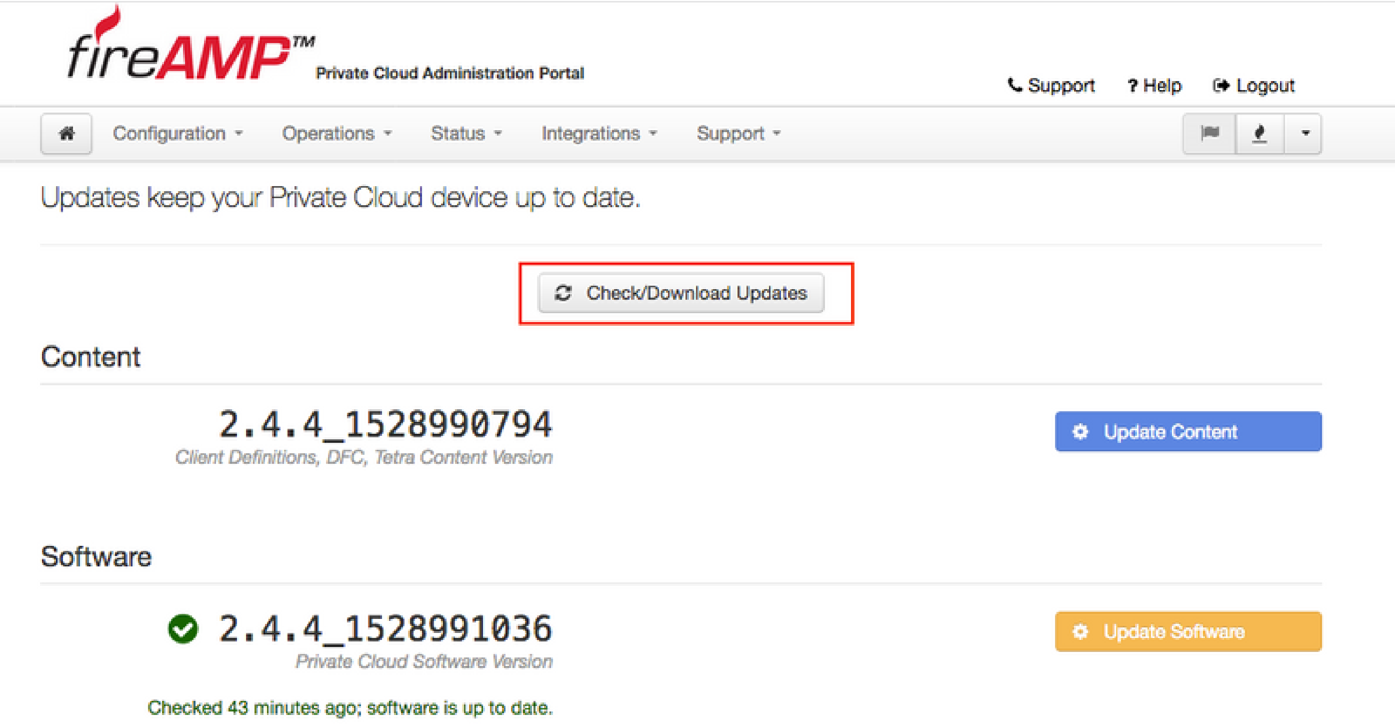
> **Caution**: Upgrade process can introduce a downtime in your environment. Connectors (includes AMP for Networks connected to your Virtual Private Cloud) which use Private Cloud can lose connectivity to the Virtual Cloud and they can have impaired functionality because of that.

1. Update download and installation

Make sure that your FireAMP Virtual Private Cloud 2.4.4 is up to date.

Step 1. Navigate to **Operations** -> **Update Device** in Administrator Portal.

Step 2. Click **Check/Download Updates** button, as shown in the image, to make sure that your FireAMP Virtual Private Cloud, from where backup collection takes place, is up to date (Content and Software wise).



Updates keep your Private Cloud device up to date.

Content

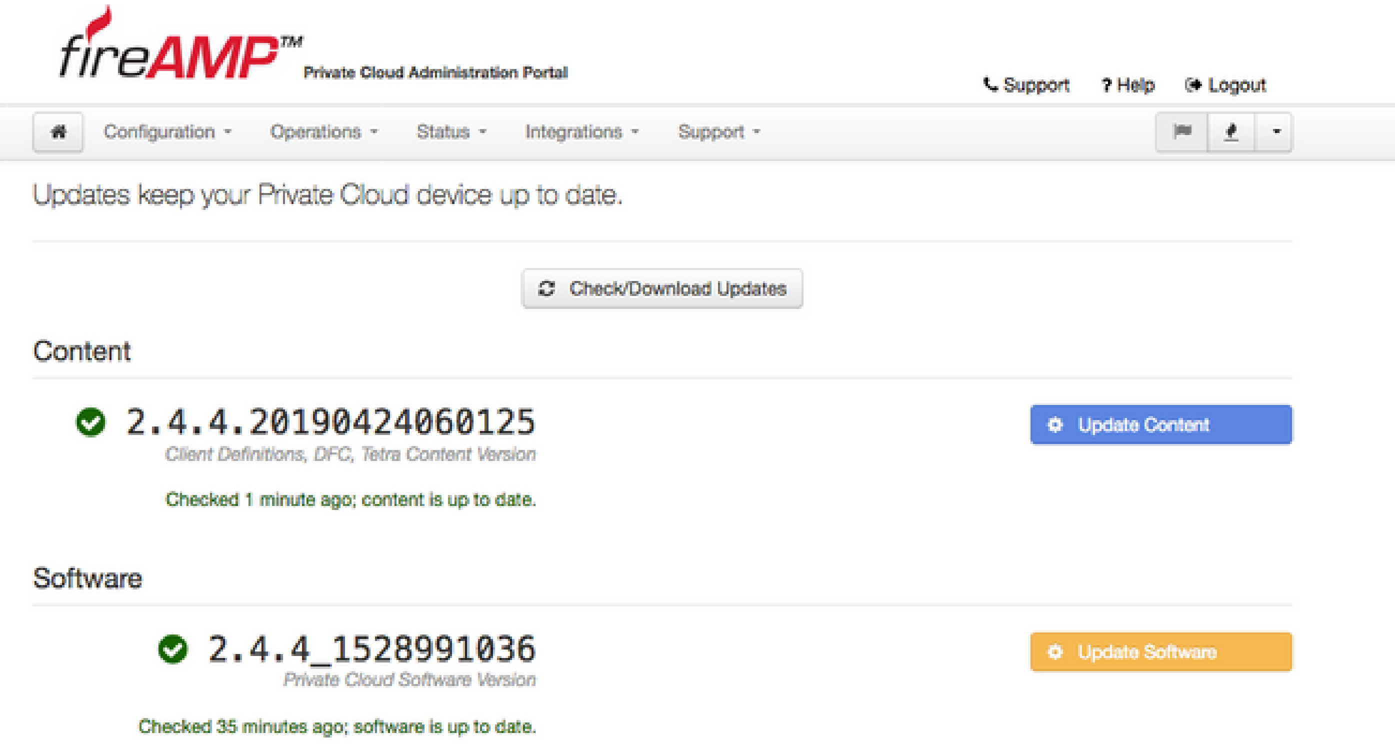
2.4.4_1528990794
Client Definitions, DFC, Tetra Content Version

Software

2.4.4_1528991036
Private Cloud Software Version

Checked 43 minutes ago; software is up to date.

Step 3. Once Content and Software updates are installed, the update page shows the information that the device is up to date, as shown in the image.



Updates keep your Private Cloud device up to date.

Content

2.4.4.20190424060125
Client Definitions, DFC, Tetra Content Version

Checked 1 minute ago; content is up to date.

Software

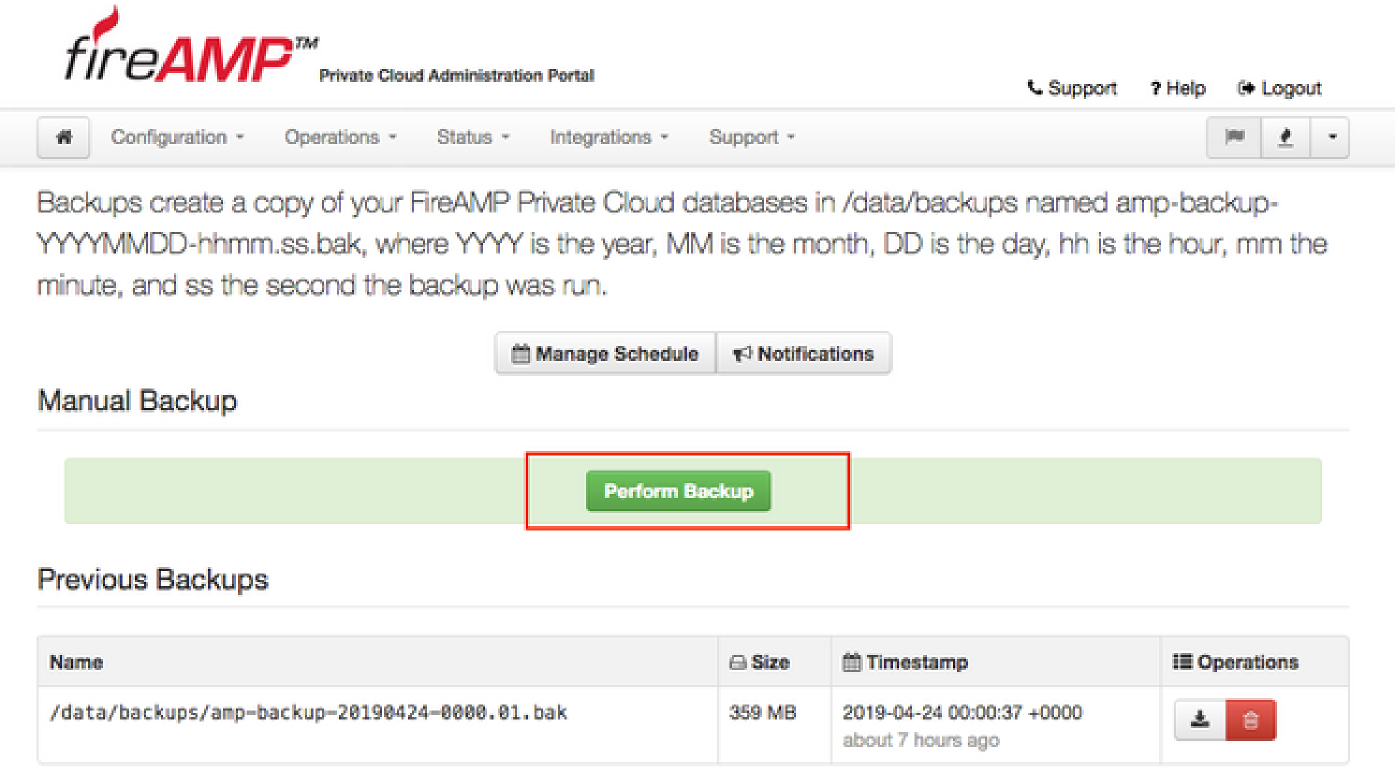
2.4.4_1528991036
Private Cloud Software Version

Checked 35 minutes ago; software is up to date.

2. Backup collection and shutdown

Step 1. Navigate to **Operations** -> **Backups.**

Step 2. In the Manual Backup section, click **Perform Backup** button. The procedure starts a backup creation.



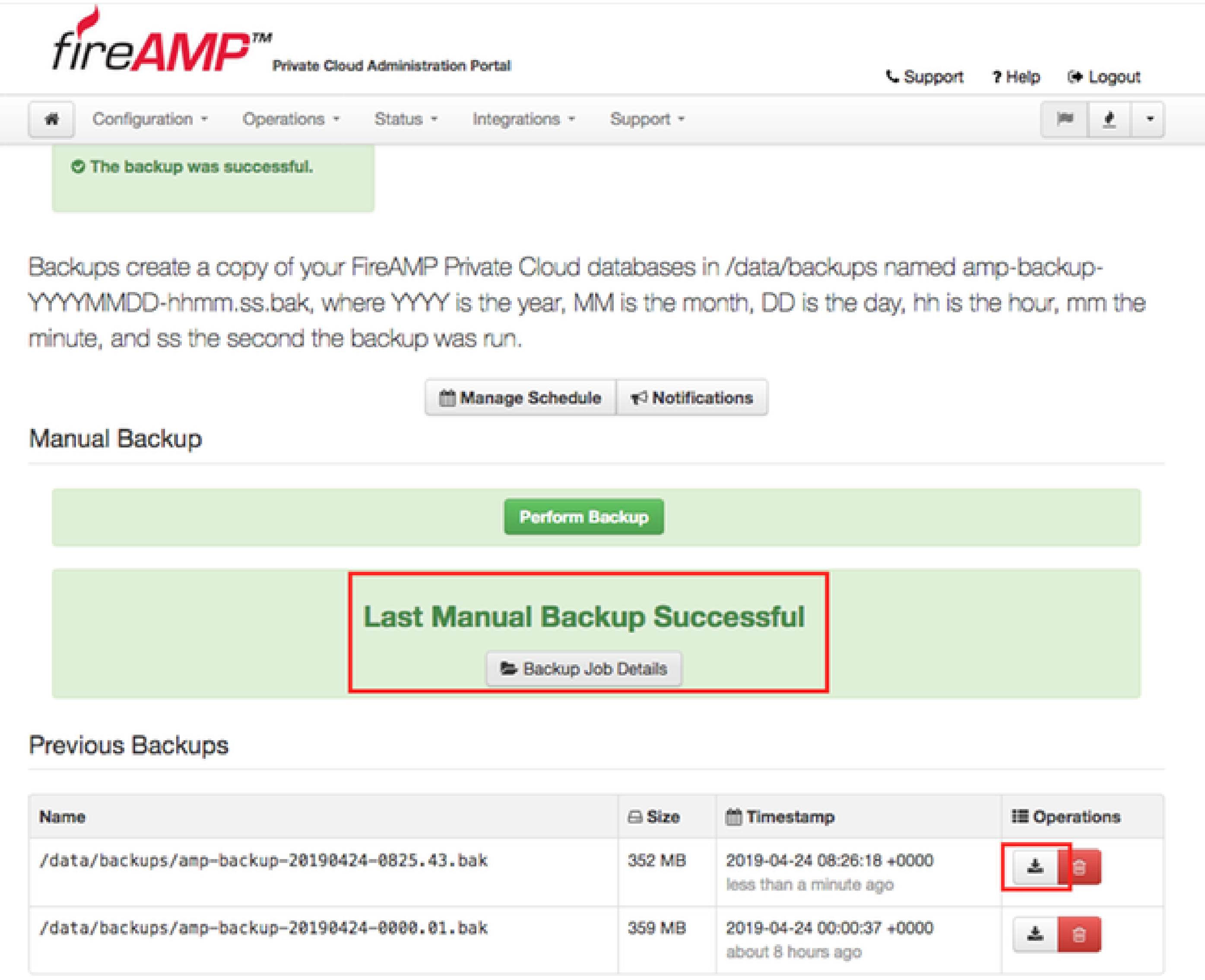
Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manual Backup

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 7 hours ago	

Step 3. When the process finishes successfully, the successful notification appears, as shown in the image.



The backup was successful.

Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manual Backup

Last Manual Backup Successful

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0825.43.bak	352 MB	2019-04-24 08:26:18 +0000 less than a minute ago	
/data/backups/amp-backup-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 8 hours ago	

Step 4. Click ⬇ button. Make sure that the backup is properly downloaded and saved in a safe location.

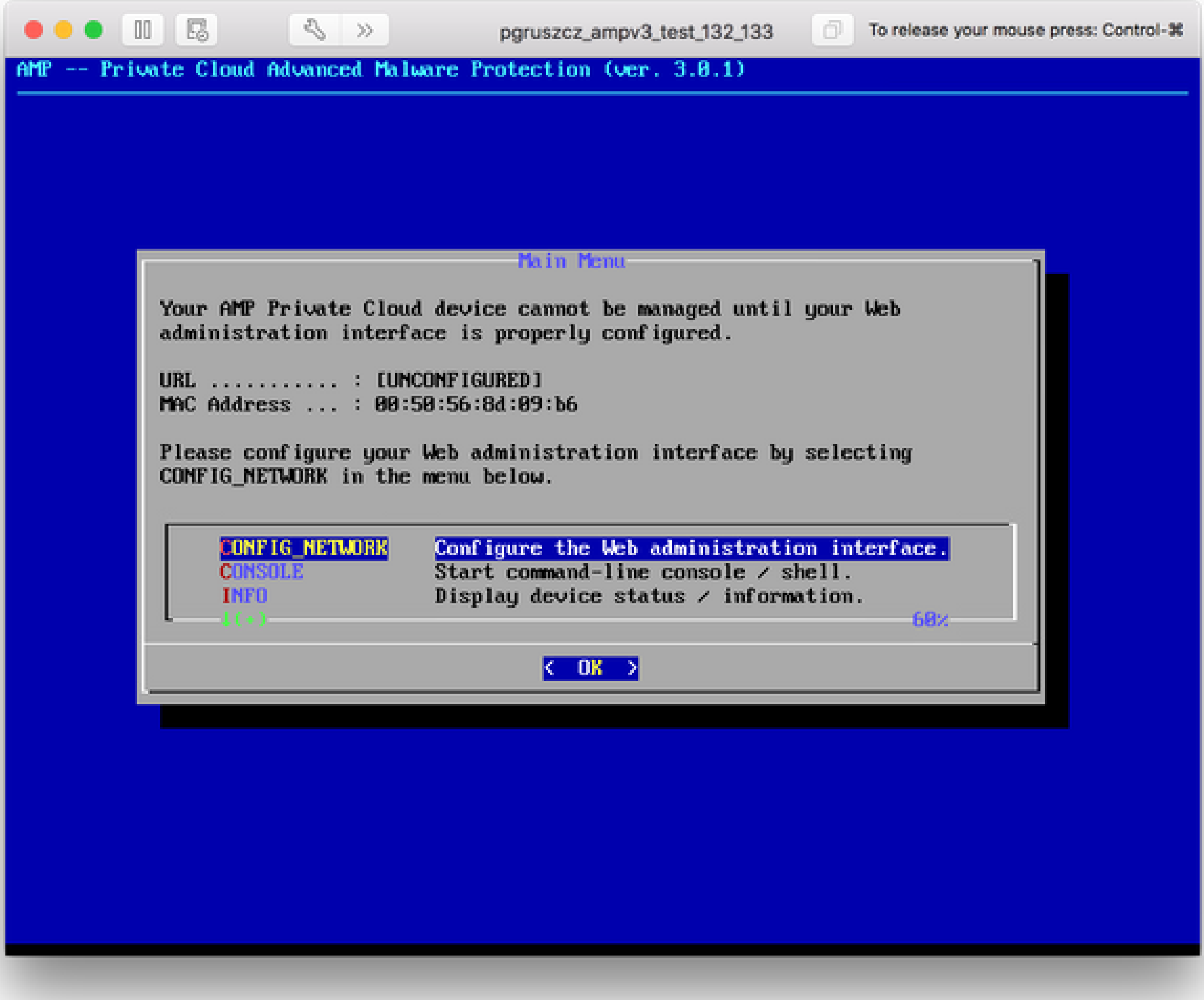
3. New version installation

This section assumes that Virtual Machine for 3.0.1 FireAMP Virtual Private Cloud is already deployed. Install procedure in regards of Virtual Machine for 3.0.1 OVA on VMWare ESXi can be found under the link: Deploy an OVA File on an ESX Server.

> **Note**: Procedure presented in the article uses exactly the same hostnames and IP addresses for FireAMP Virtual Private Cloud 2.4.4 and 3.0.1. When you follow this guide, you must shutdown FireAMP Virtual Private Cloud 2.4.4 after backup is collected.

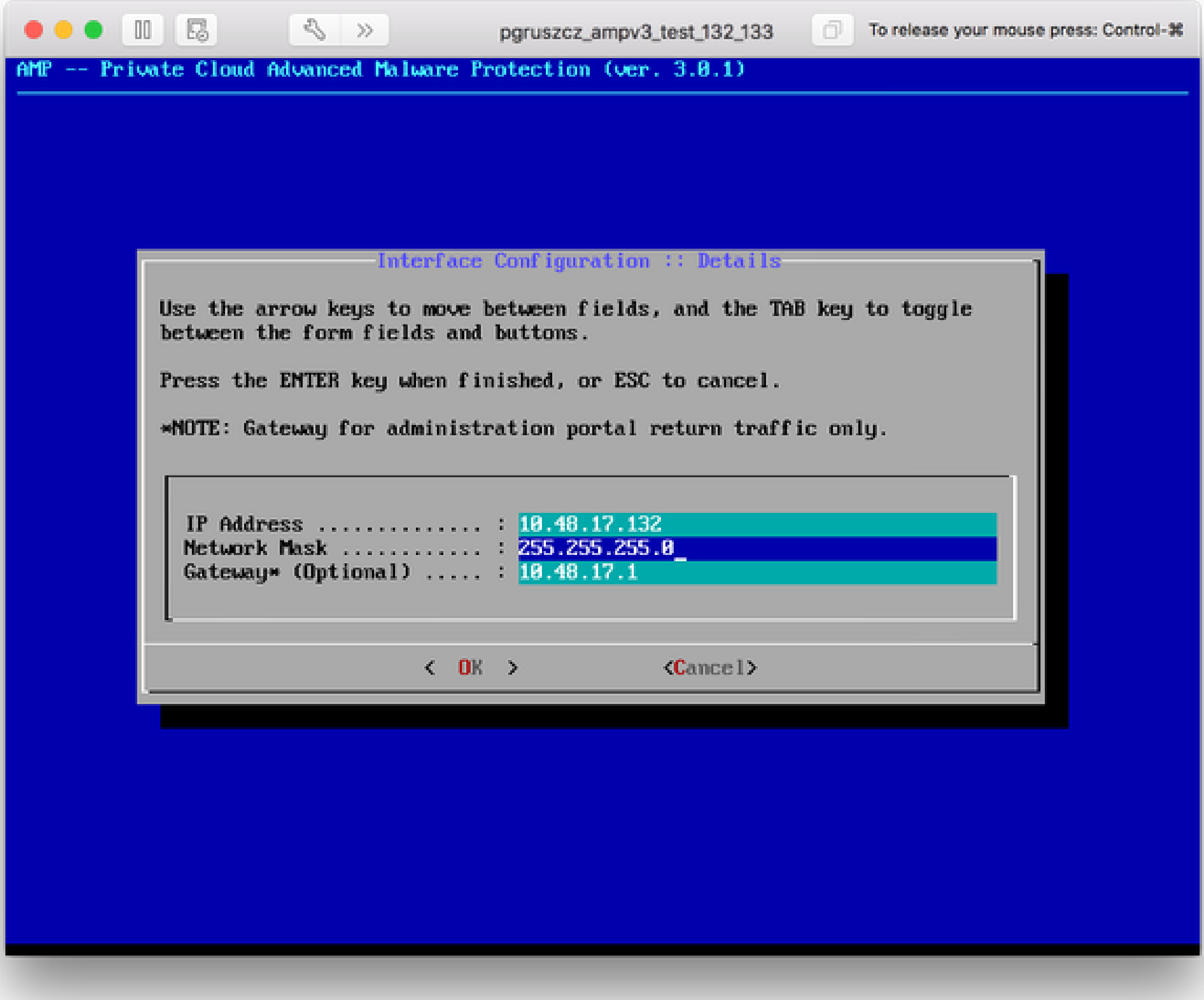
Step 1. Open console terminal for newly created Virtual Machine instance with 3.0.1 version installed. You can navigate through **Tab**, **Enter** and **arrow** keys.

Step 2. Navigate to **CONFIG_NETWORK** and click the **Enter** key on your keyboard to begin the configuration of the management IP address for the FireAMP Private Cloud. If you do not want to use DHCP, select **No** and press **Enter**.


pgruszcz_ampv3_test_132_133
To release your mouse press: Control-⌘

```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.0.1)

                              Main Menu
 Your AMP Private Cloud device cannot be managed until your Web
 administration interface is properly configured.

 URL ........... : [UNCONFIGURED]
 MAC Address ... : 00:50:56:8d:09:b6

 Please configure your Web administration interface by selecting
 CONFIG_NETWORK in the menu below.

     CONFIG_NETWORK   Configure the Web administration interface.
     CONSOLE          Start command-line console / shell.
     INFO             Display device status / information.
     ↓(+)                                                    60%

                               < OK >
```

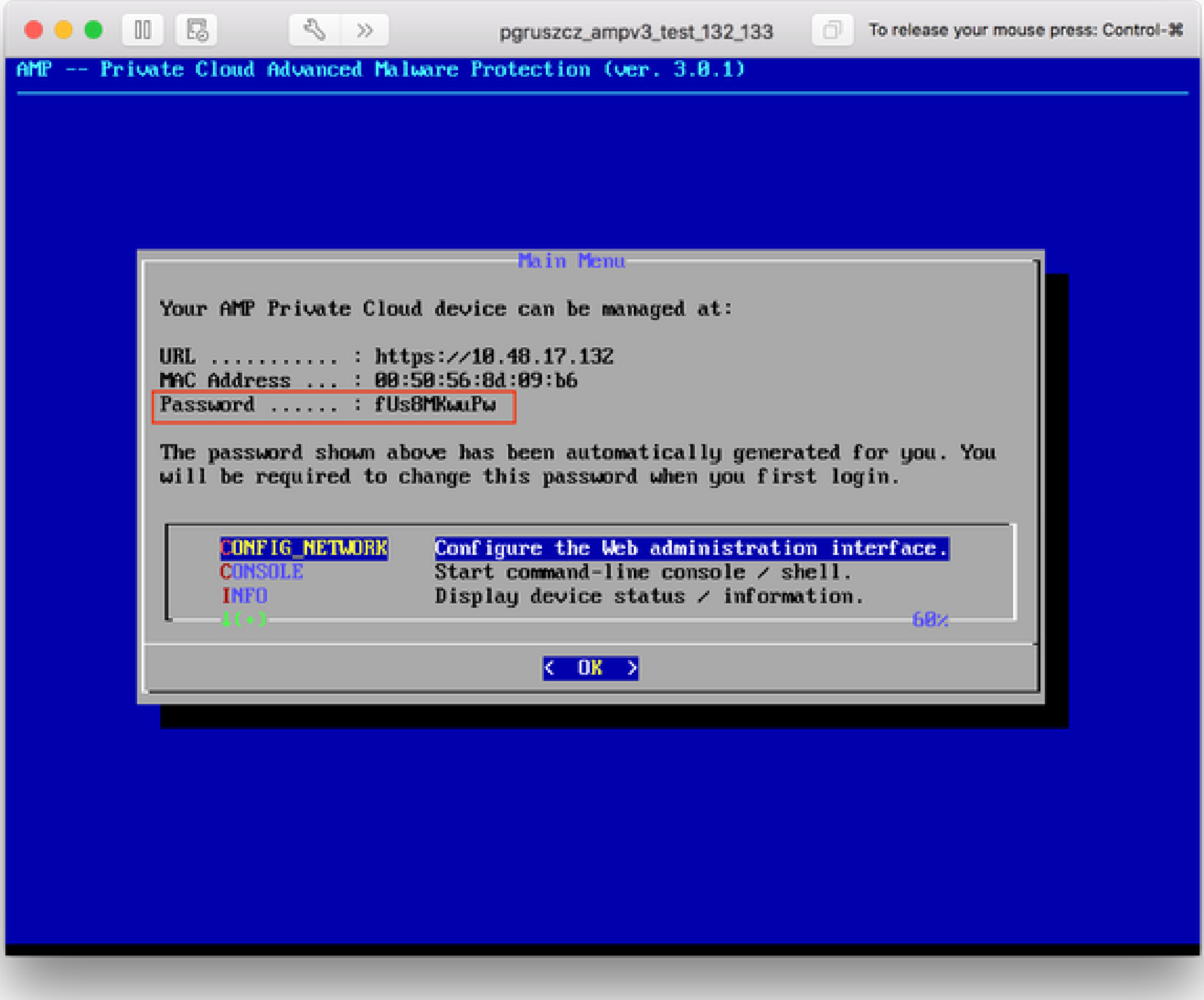
Step 3. Enter the **IP address**, **Network Mask** and **Default Gateway**. Navigate to **OK**, as shown in the image. Press **Enter** key.



pgruszcz_ampv3_test_132_133
To release your mouse press: Control-⌘

```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.0.1)

                    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 .............. : 10.48.17.132
   Network Mask ............ : 255.255.255.0_
   Gateway* (Optional) ..... : 10.48.17.1

                    <  OK  >              <Cancel>
```

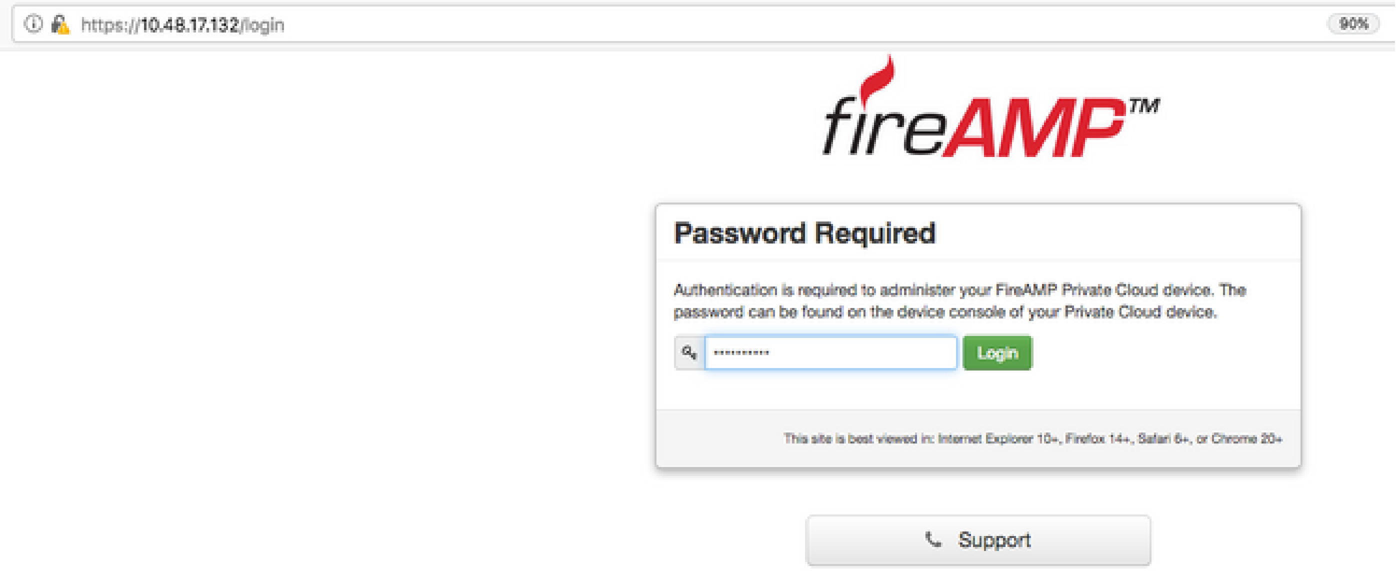
Step 4. Network configuration change requires a restart of the interface. After the restart, main console menu reappears, as shown in the image. This time you see an IP address on the URL line. Also, note that the initial **Password** is displayed. This is a one-time password (later referenced as **initial password**) which is used in the web-based setup.


pgruszcz_ampv3_test_132_133
To release your mouse press: Control-⌘

```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.0.1)

                              Main Menu

  Your AMP Private Cloud device can be managed at:

  URL ........... : https://10.48.17.132
  MAC Address ... : 00:50:56:8d:09:b6
  Password ...... : fUs8MKwuPw

  The password shown above has been automatically generated for you. You
  will be required to change this password when you first login.

       CONFIG_NETWORK     Configure the Web administration interface.
       CONSOLE            Start command-line console / shell.
       INFO               Display device status / information.
       ↓(+)                                                      60%

                               <  OK  >
```

Step 5. Open a web browser and navigate to the management IP address of the appliance. You receive a certificate error as the FireAMP Private Cloud initially generates its own HTTPS certificate. Configure your browser to temporarily trust the self-signed certificate of the FireAMP Private Cloud.

Step 6. You get a screen to enter a password, as shown in the image. Use the **initial password** from the console. Click on **Login**.



https://10.48.17.132/login

90%

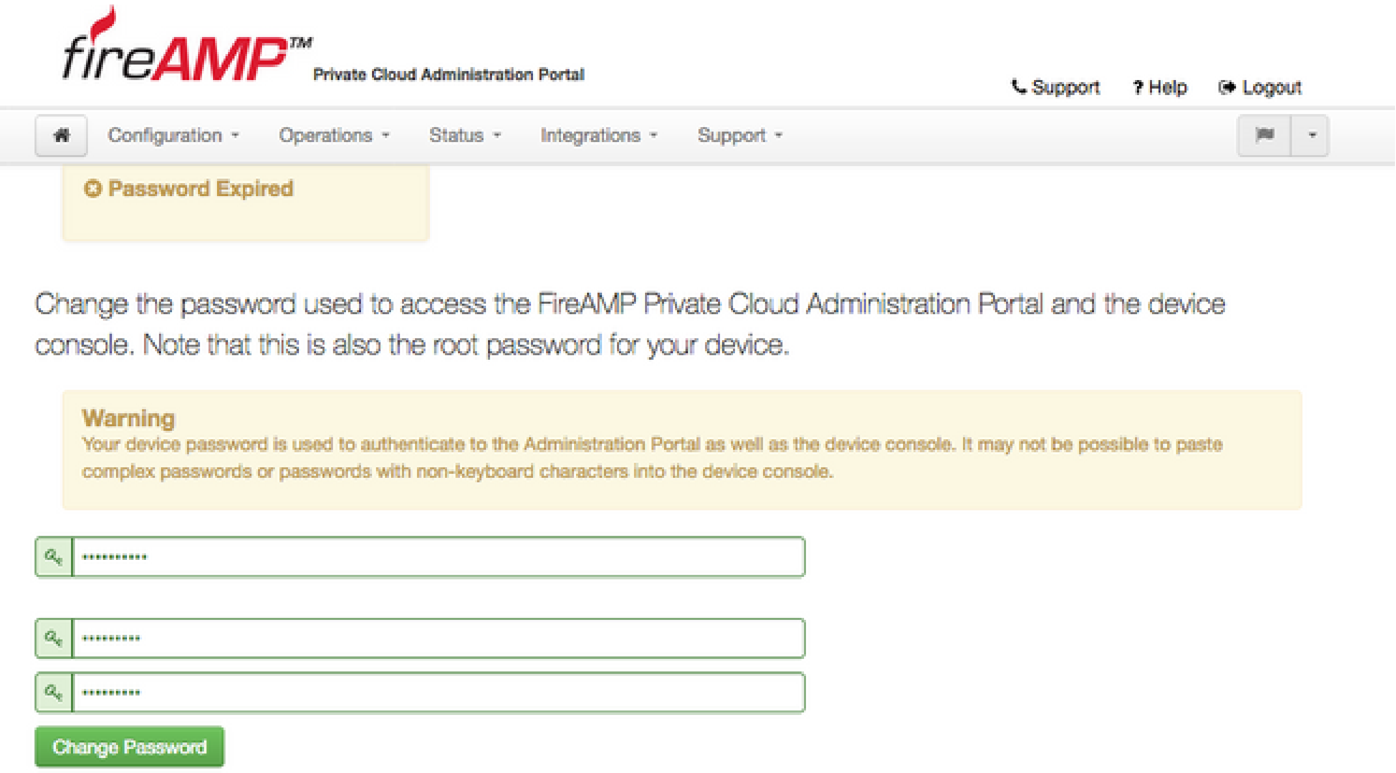
fireAMP™

Password Required

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

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

Step 7. After successful login, you are required to change the password. Use the **initial password** from the console in the **Old Password** field. Use your new password twice in the **New Password** fields. Click **Change Password**.



fireAMP™ Private Cloud Administration Portal

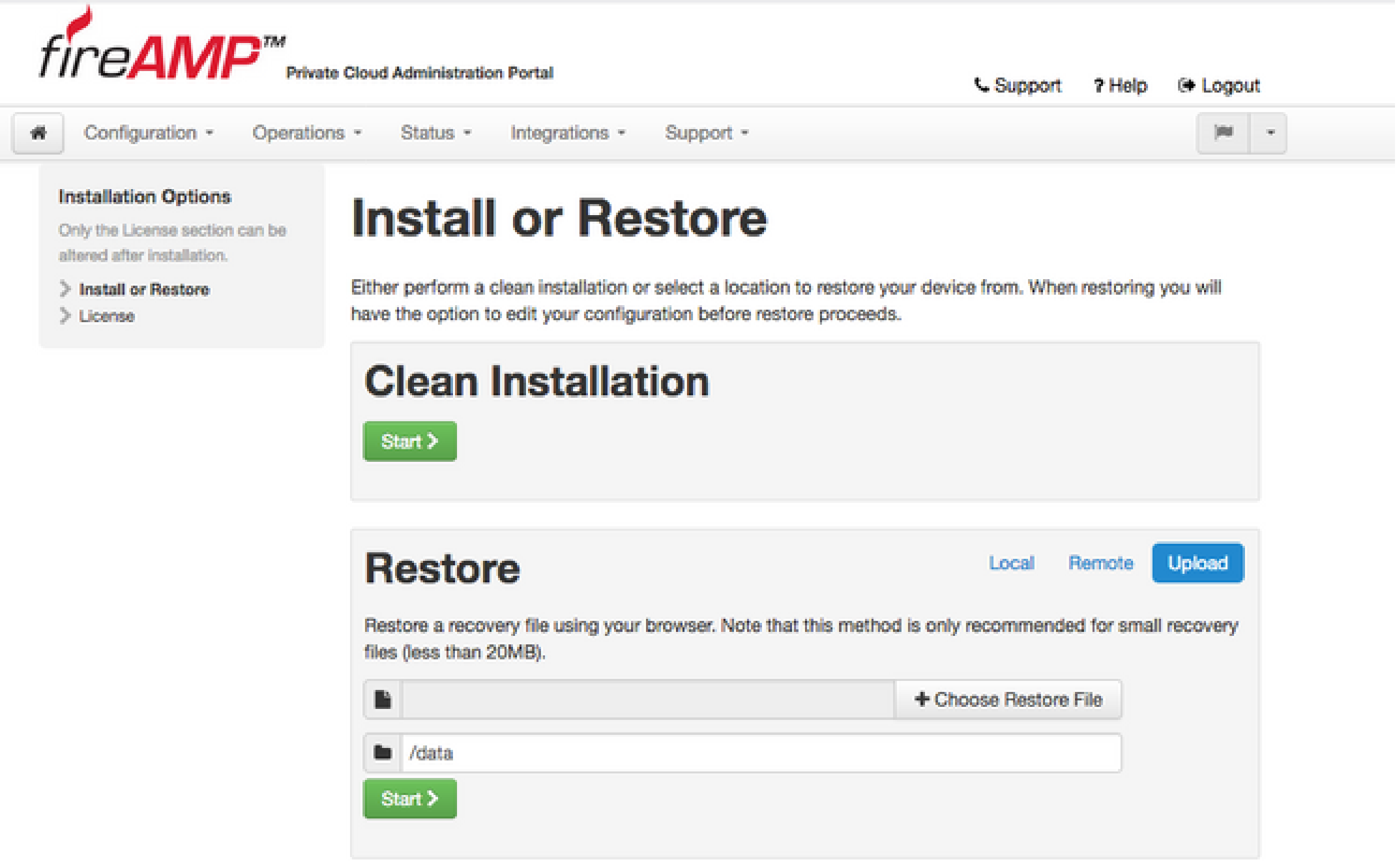
Password Expired

Change the password used to access the FireAMP Private Cloud Administration Portal and the device console. 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 paste complex passwords or passwords with non-keyboard characters into the device console.

4. Backup restore

Step 1. Welcome page of Admin portal presents two ways of 3.0.1 FireAMP Virtual Cloud installation, as shown in the image.



Install or Restore

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

Clean Installation

Restore

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

/data

Step 2. You can choose one of three different methods to upload the backup file to the newly created FireAMP Virtual Private Cloud instance:

Local - Restores the configuration from a backup file already presented on the device (you must put the file on the appliance via SFTP or SCP). Files are extracted to the correct directory once the restore process begins. For this reason, recommended is `/data` directory.

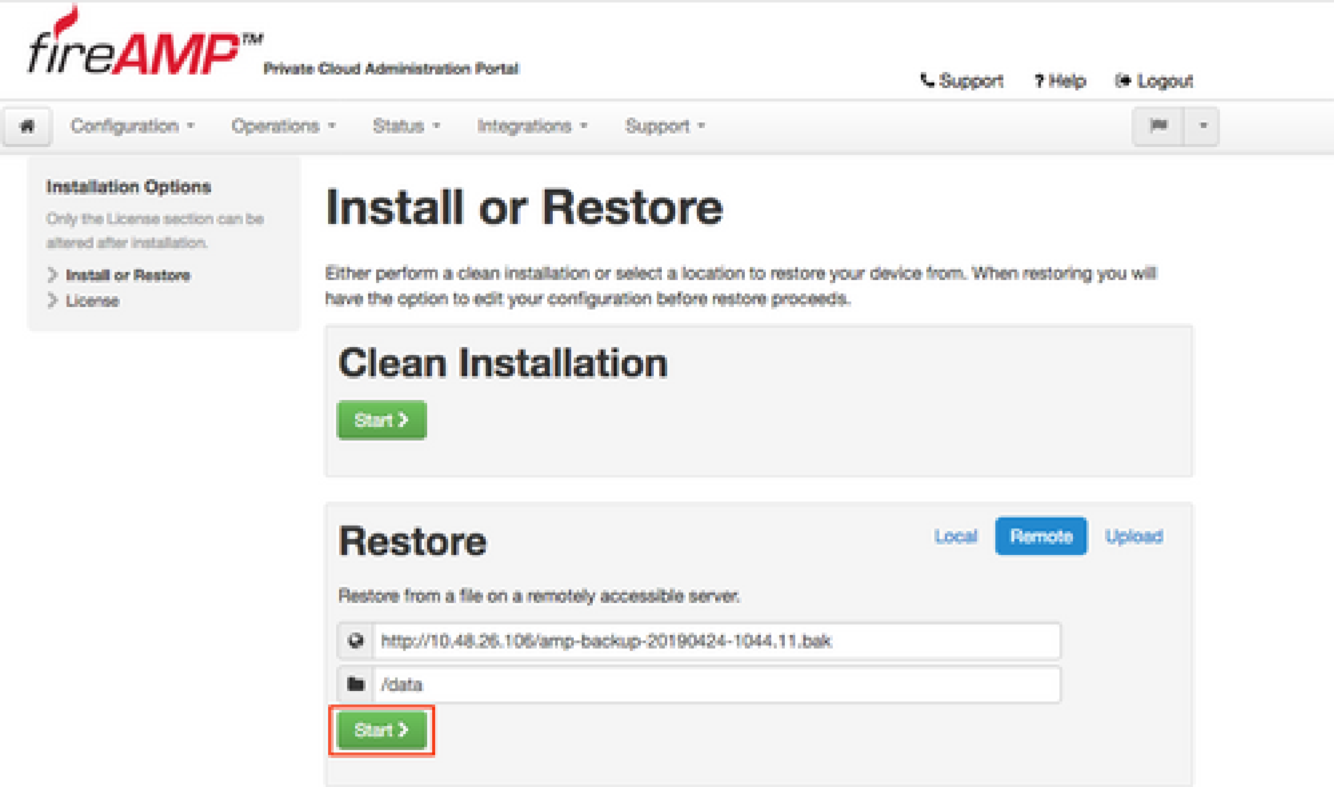
Remote - Restore from a file on a remotely accessible HTTP server.

Upload - Restore from the file uploaded by your browser. Works only if your backup file is smaller than 20MB.

In this example, the remote option was chosen.

> **Note**: Proper connectivity must be allowed for the HTTP server. Backup file needs to be accessible from the Private Cloud perspective.

Click **Start** button to proceed with the restore, as shown in the image.



Only the License section can be altered after installation.

Install or Restore

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

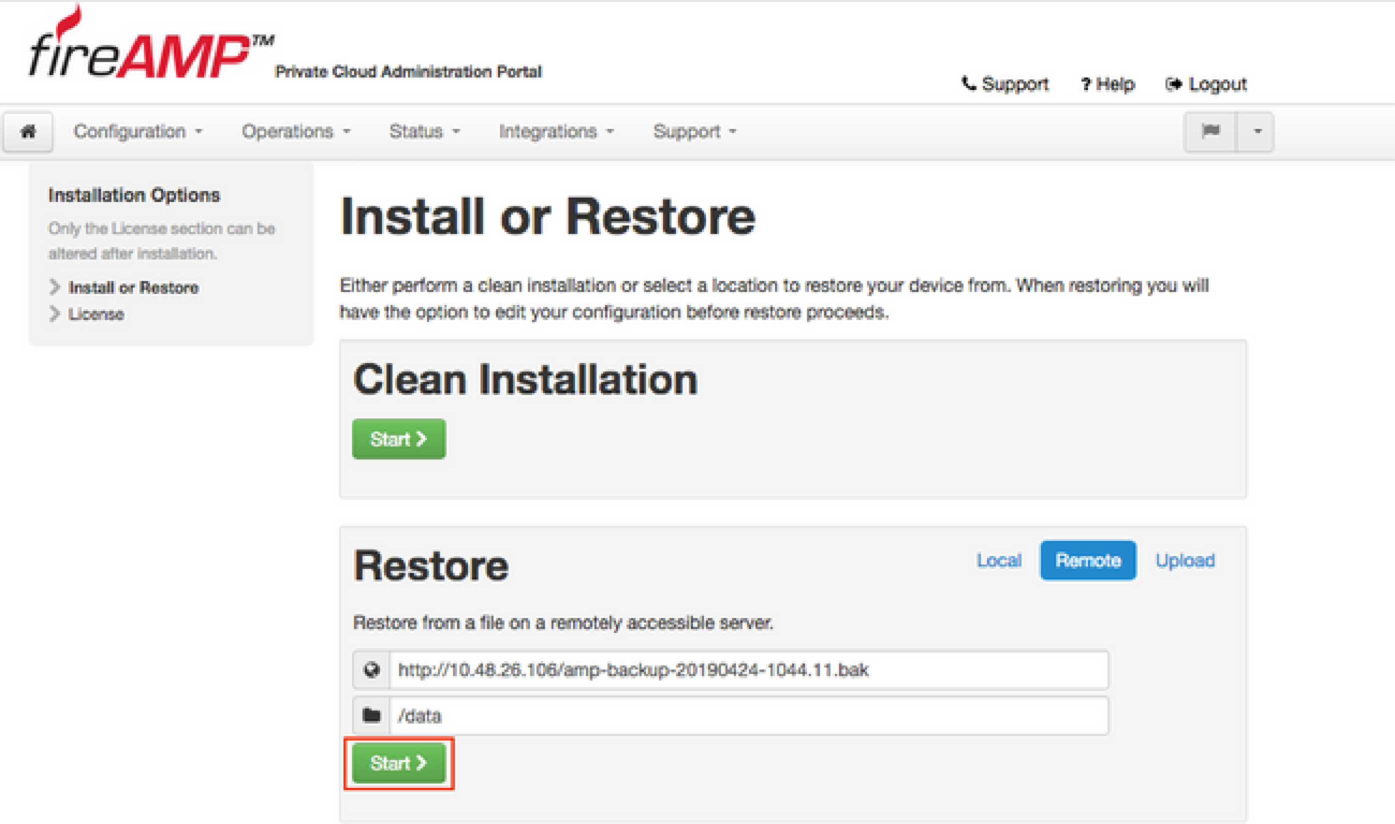
Clean Installation

Restore

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data



Only the License section can be altered after installation.

Install or Restore

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

Clean Installation

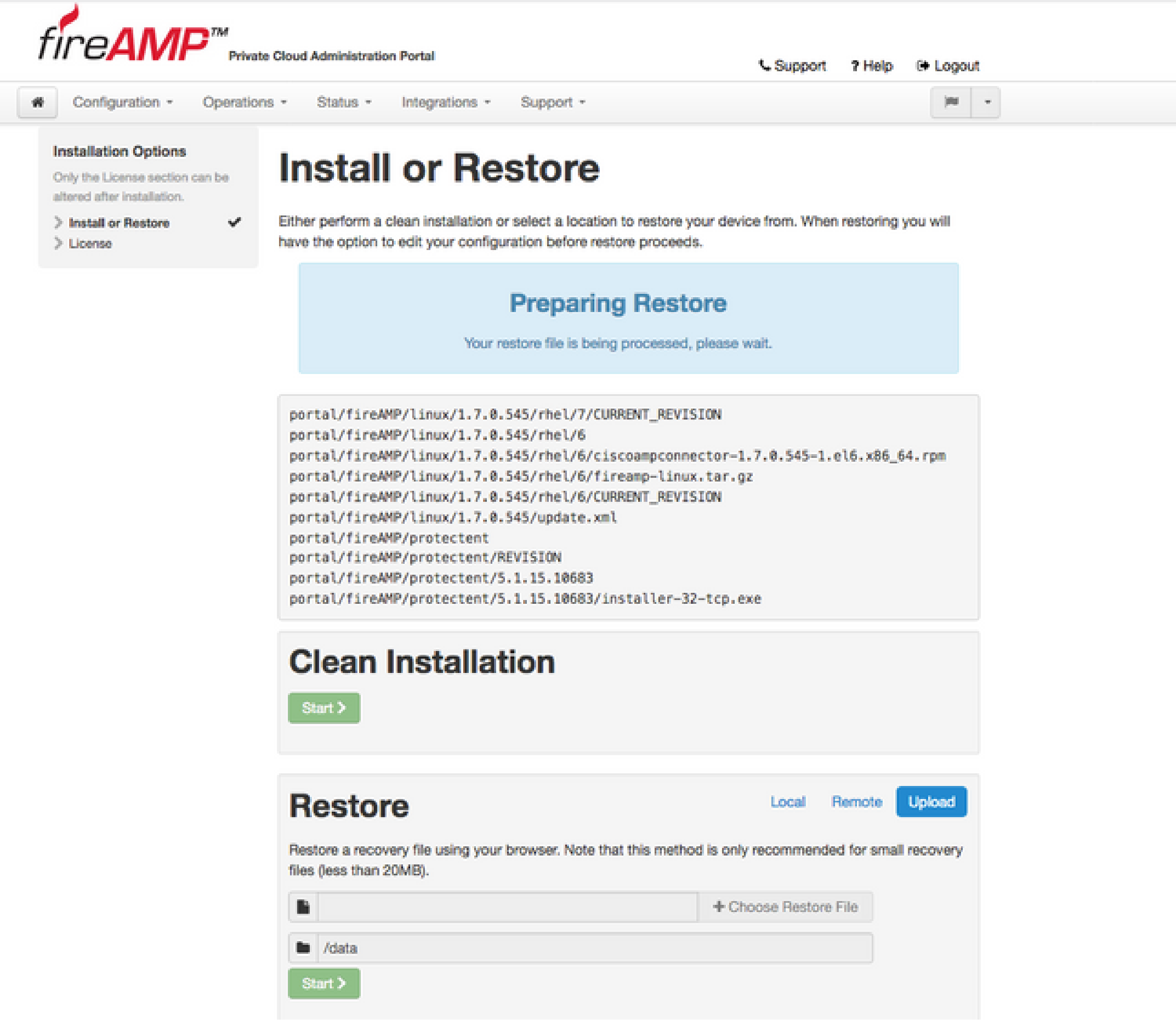
Restore

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Step 3. Restore procedure from a backup replaces your current configuration. Your device's SSH host keys and Administration Portal password are replaced. You can review parts of your configuration in regards of installation.



Only the License section can be altered after installation.

Install or Restore

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

Preparing Restore

Your restore file is being processed, please wait.

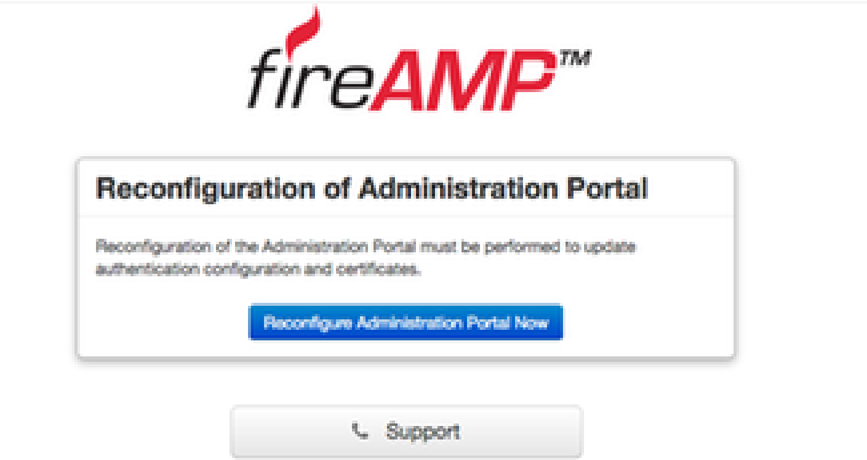
```
portal/fireAMP/linux/1.7.0.545/rhel/7/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/rhel/6
portal/fireAMP/linux/1.7.0.545/rhel/6/ciscoampconnector-1.7.0.545-1.el6.x86_64.rpm
portal/fireAMP/linux/1.7.0.545/rhel/6/fireamp-linux.tar.gz
portal/fireAMP/linux/1.7.0.545/rhel/6/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/update.xml
portal/fireAMP/protectent
portal/fireAMP/protectent/REVISION
portal/fireAMP/protectent/5.1.15.10683
portal/fireAMP/protectent/5.1.15.10683/installer-32-tcp.exe
```

Clean Installation

Restore

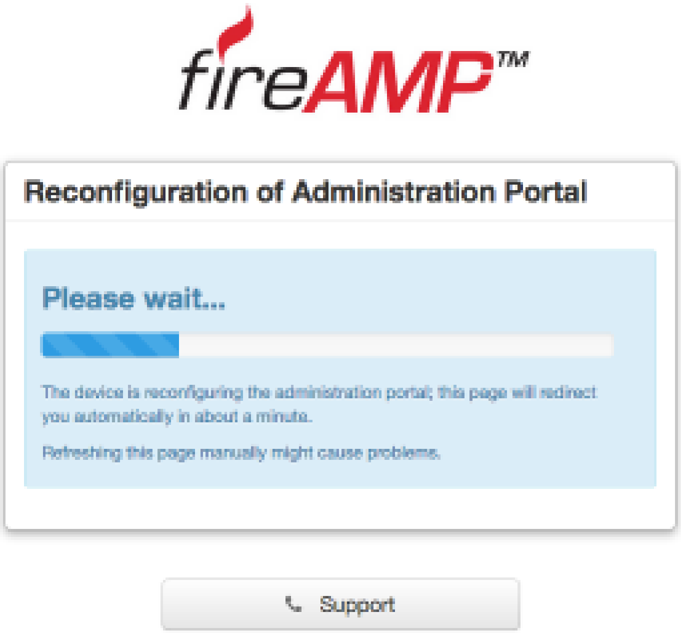
Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

Step 4. After a successful copy of the backup file, restore page presents pop-up message as shown on the image. Click **Reconfigure Administration Portal Now** button to finish the restore procedure.



Reconfiguration of Administration Portal

Reconfiguration of the Administration Portal must be performed to update authentication configuration and certificates.



Reconfiguration of Administration Portal

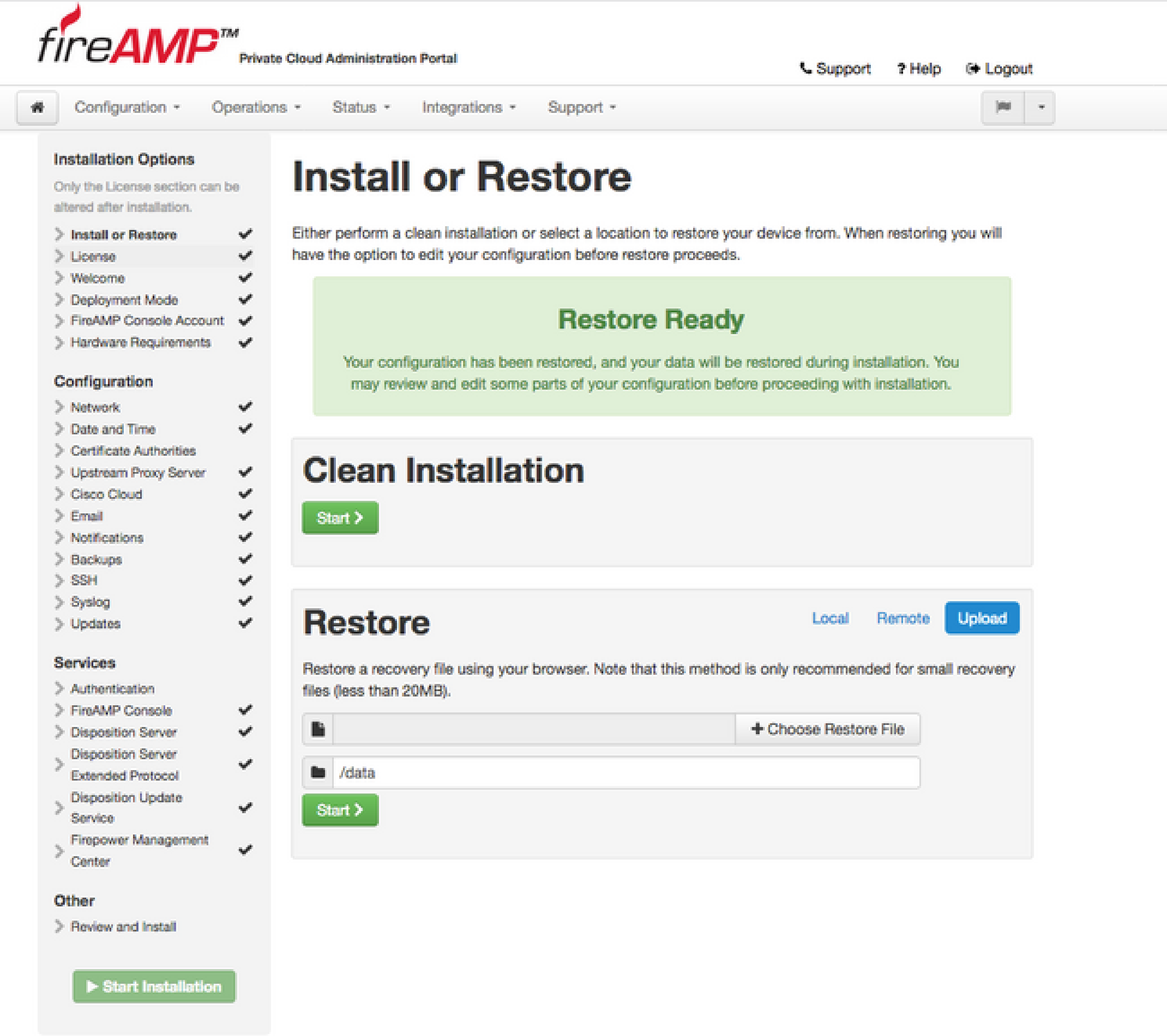
Please wait...

The device is reconfiguring the administration portal; this page will redirect you automatically in about a minute.

Refreshing this page manually might cause problems.

Step 5. Once reconfiguration is finished, the Administration portal page is displayed again, as shown in the image. From now on, to login you must use the password from 2.4.4 FireAMP Virtual Private Cloud backup.

Image shows most of the work for the proper installation as already done (checkpoint marks). It is expected since backup restores the configuration from FireAMP Virtual Private Cloud 2.4.4.



Install or Restore

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

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Clean Installation

Restore

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

/data

5. Certificate Authorities

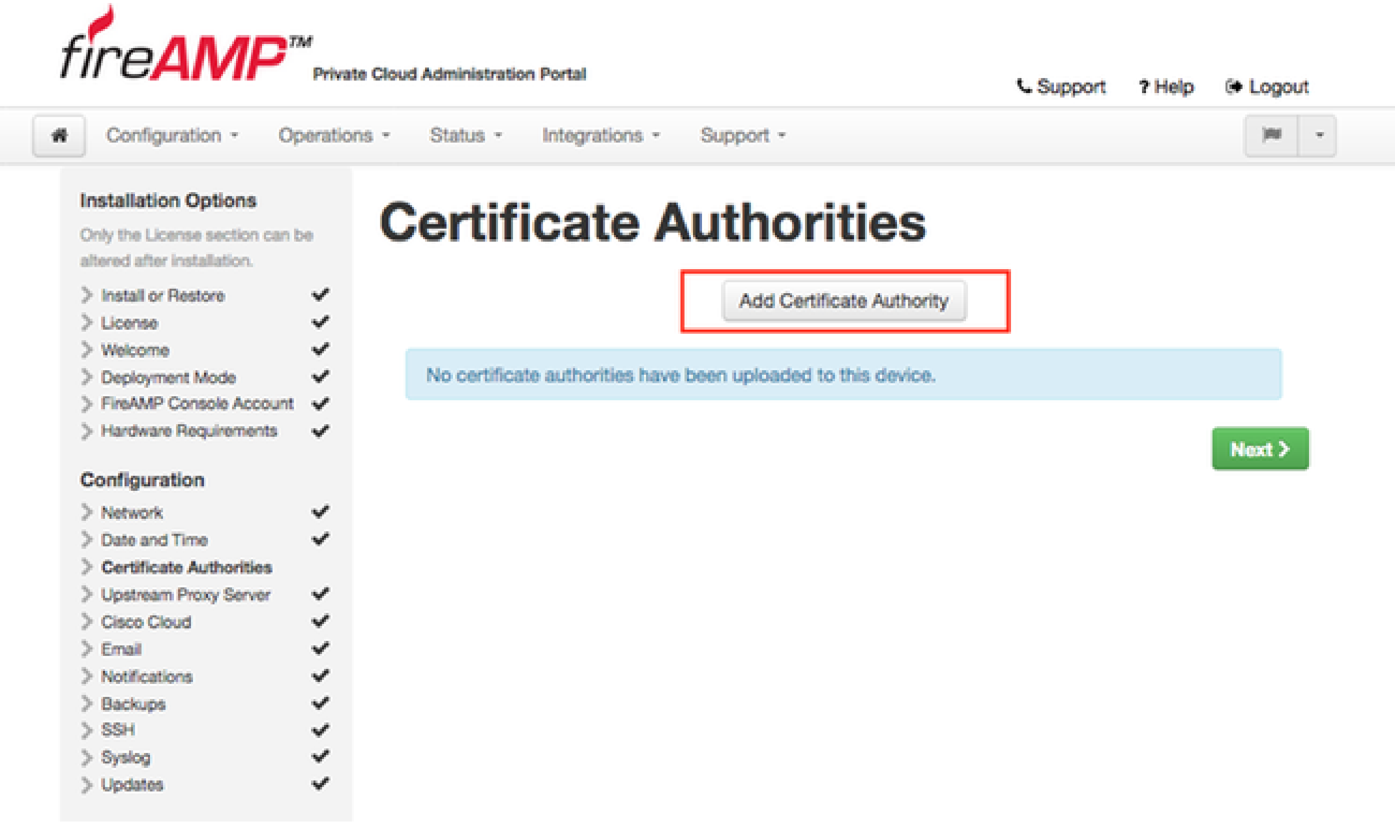
Version 3.0.1 of FireAMP Virtual Private Cloud introduces new features and behaviors in terms of how the system operates. Those need to be configured and completed before you can begin the installation.

The first component which is new and was not present in the earlier release is **Certificate Authorities**.

Certificate Authorities page allows you to manage root certificates for your services if you want to use a custom certificate authority. You can download or delete your root certificate if needed.

> **Note**: Certificate Authorities trusted store is used only for Virtual Cloud services (to build and validate the proper certificate chain). It is not used for various vPC integrations, like ThreatGrid.

Step 1. Navigate to **Configuration** -> **Certificate Authorities** section in **Installation Options** panel. Click **Add Certificate Authority** button, as shown in the image.

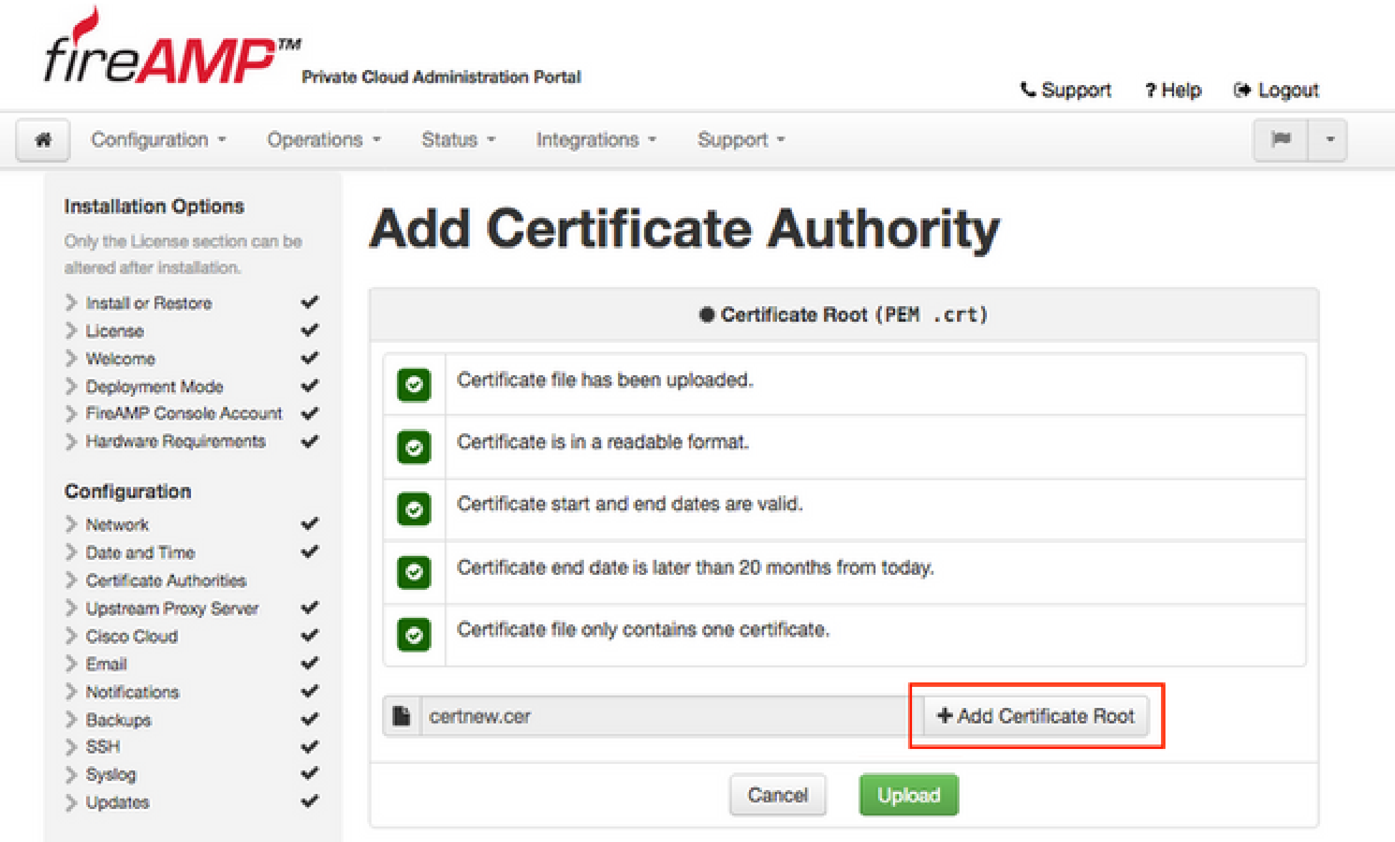


Certificate Authorities

No certificate authorities have been uploaded to this device.

Step 2. Click **Add Certificate Root,** as shown in the image, to upload the certificate. All listed requirements need to be met for Virtual Private Cloud to accept the certificate.

> **Note**: During the upgrade procedure, you must add **root certificate** used to sign the **Authentication** service certificate, explained in the next section.



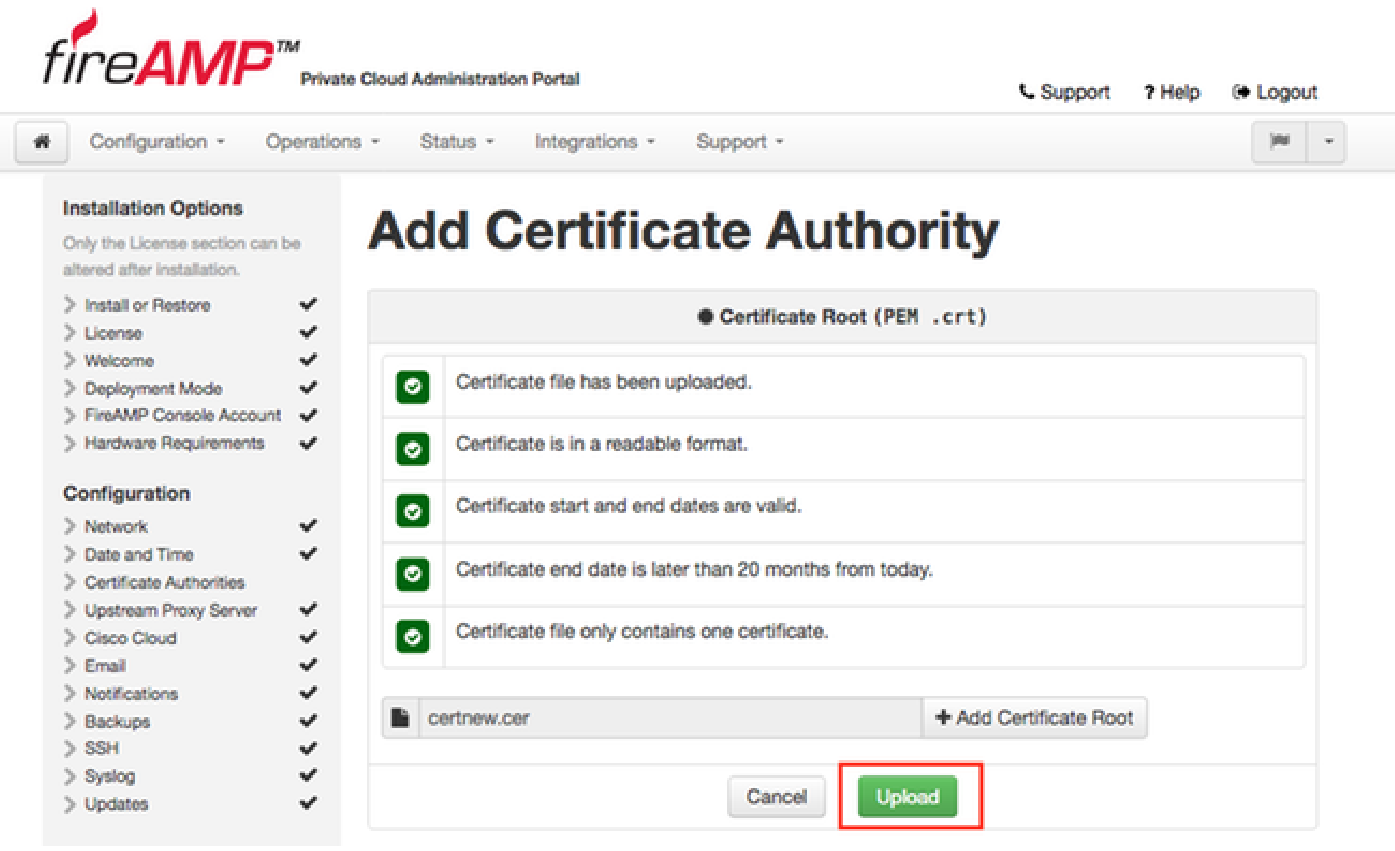
Add Certificate Authority

● Certificate Root (PEM .crt)

- ✓ 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.

certnew.cer

Step 3. Once the certificate is updated, click **Upload** button, as shown in the image, to upload the certificate.



Add Certificate Authority

● Certificate Root (PEM .crt)

✓ 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.

certnew.cer

If you use any subordinate certificates authority to sign any service certificates, upload them in this section as well.

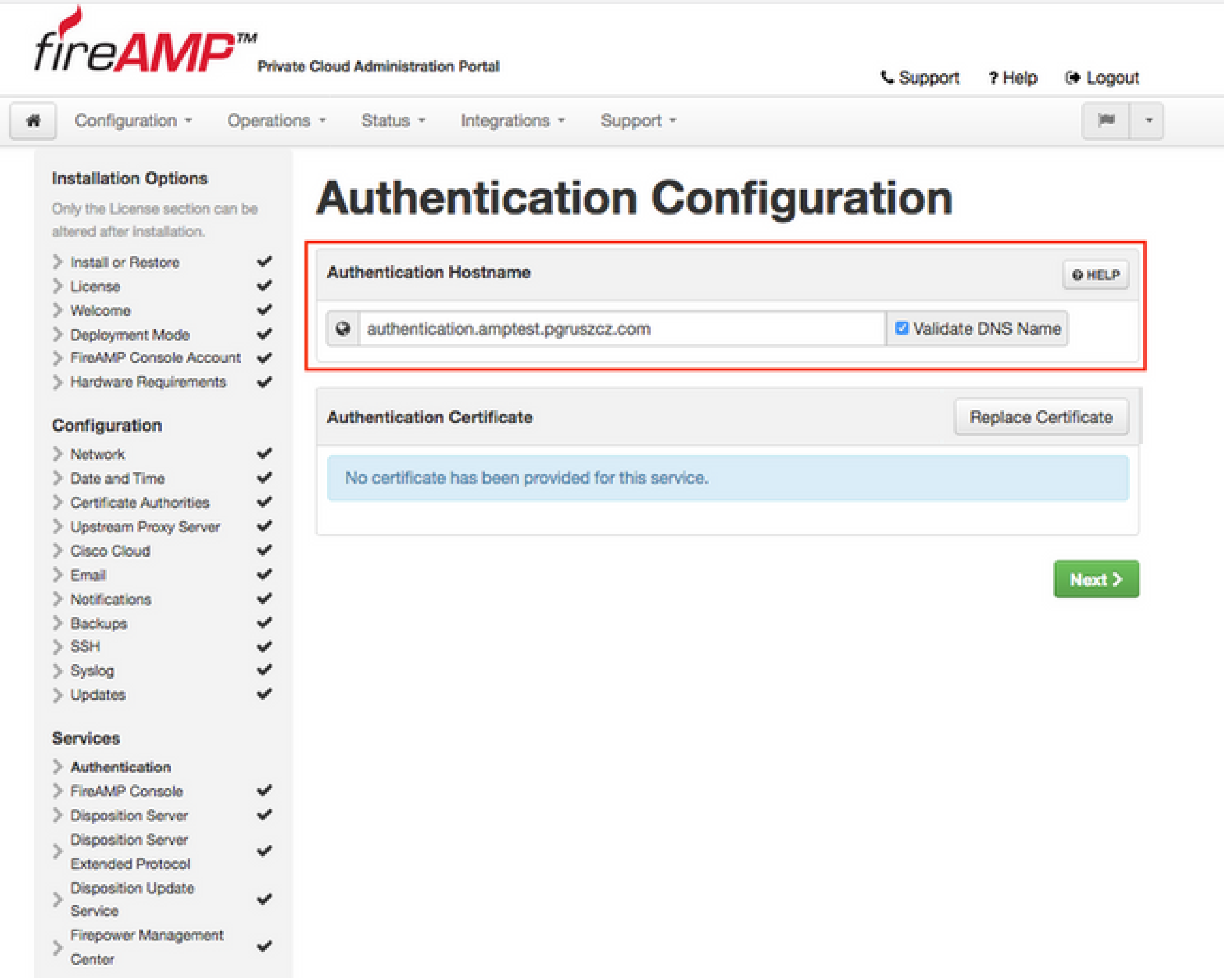
> **Caution**: Even if you generate a self-signed certificate for the Authentication Service, make sure that it is uploaded in the Certificate Authority section before you go to the next steps.

6. Authentication Service

The second component which is added in 3.0.1 version, and not imported from the backup, is **Authentication** under the Services section.

Authentication service will be used in future versions of Private Cloud to handle user authentication requests. It is added in 3.0.1 version for future compatibility.

Step 1. Navigate to **Services** -> **Authentication** section in the **Installation Options** panel. Enter unique **Authentication Hostname**, DNS entry specified in the hostname section must be correctly configured on the DNS server and points to the Virtual Private Cloud console interface IP address.



Authentication Configuration

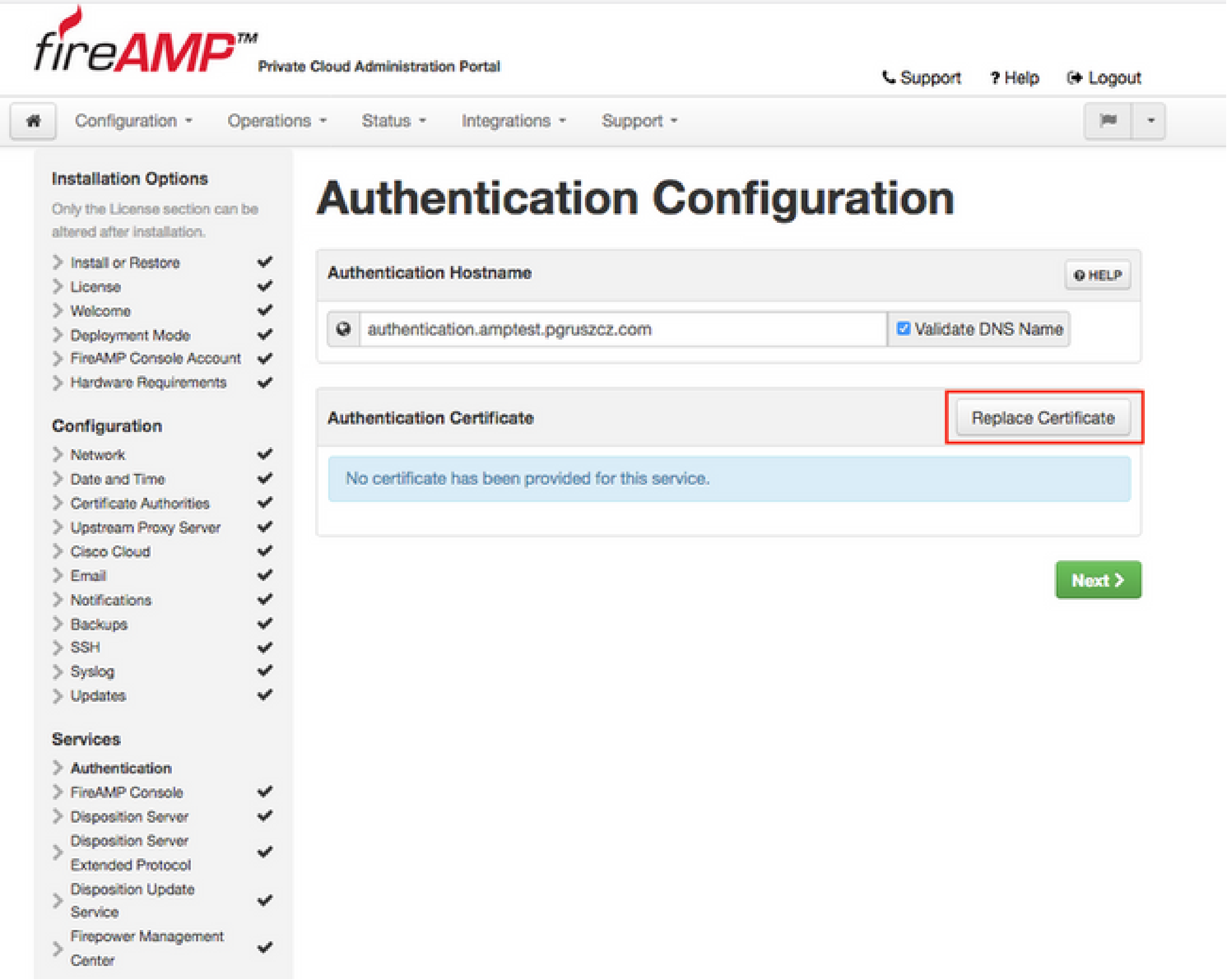
Authentication Hostname

authentication.amptest.pgruszcz.com ☑ Validate DNS Name

Authentication Certificate

No certificate has been provided for this service.

Step 2. Once the hostname is specified and properly resolvable, click **Replace Certificate** button, as showed in image.



Authentication Configuration

Authentication Hostname

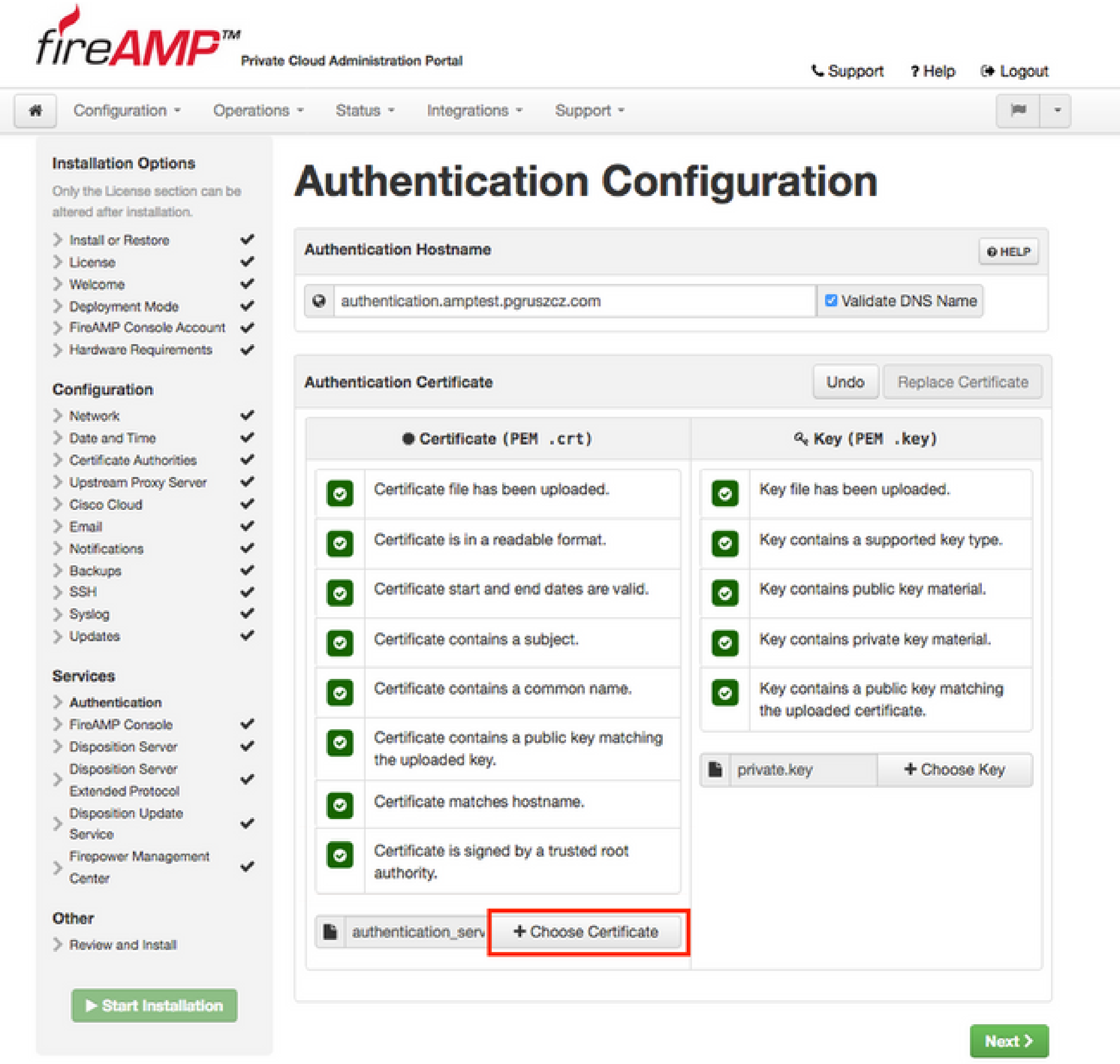
authentication.amptest.pgruszcz.com ☑ Validate DNS Name

Authentication Certificate

No certificate has been provided for this service.

Note: If you need help with the Certificate generation, please visit the article: How to Generate and Add Certificates that are Required for Installation of AMP VPC 3.x Onwards for more information about Hardware Requirements.

Step 3. Click **Choose Certificate** button to upload the Authentication Service certificate, as showed in image.



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- FireAMP Console Account ✓
- Hardware Requirements ✓

Configuration

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

Services

- Authentication
- FireAMP Console ✓
- Disposition Server ✓
- Disposition Server Extended Protocol ✓
- Disposition Update Service ✓
- Firepower Management Center ✓

Other

- Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

authentication.amptest.pgruszcz.com ☑ Validate DNS Name

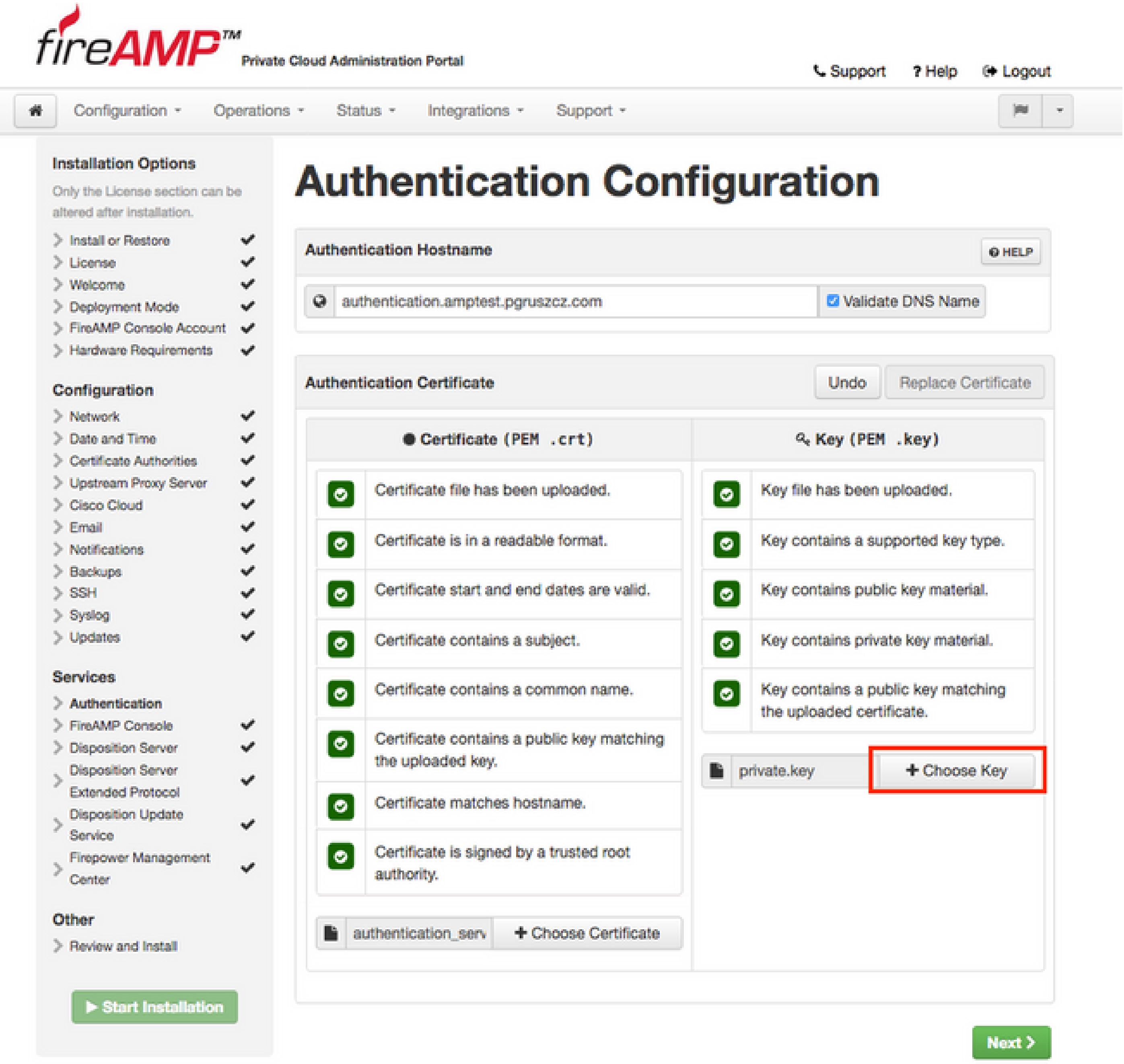
Authentication Certificate

Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
✓ Certificate file has been uploaded.	✓ Key file has been uploaded.
✓ Certificate is in a readable format.	✓ Key contains a supported key type.
✓ Certificate start and end dates are valid.	✓ Key contains public key material.
✓ Certificate contains a subject.	✓ Key contains private key material.
✓ Certificate contains a common name.	✓ Key contains a public key matching the uploaded certificate.
✓ Certificate contains a public key matching the uploaded key.	private.key + Choose Key
✓ Certificate matches hostname.	
✓ Certificate is signed by a trusted root authority.	
authentication_serv + Choose Certificate	

Next ›

Step 4. Next step is to upload the private key file for the certificate. To add it, click **Choose Key** button.



Authentication Configuration

Authentication Hostname

authentication.amptest.pgruszcz.com ☑ Validate DNS Name

Authentication Certificate

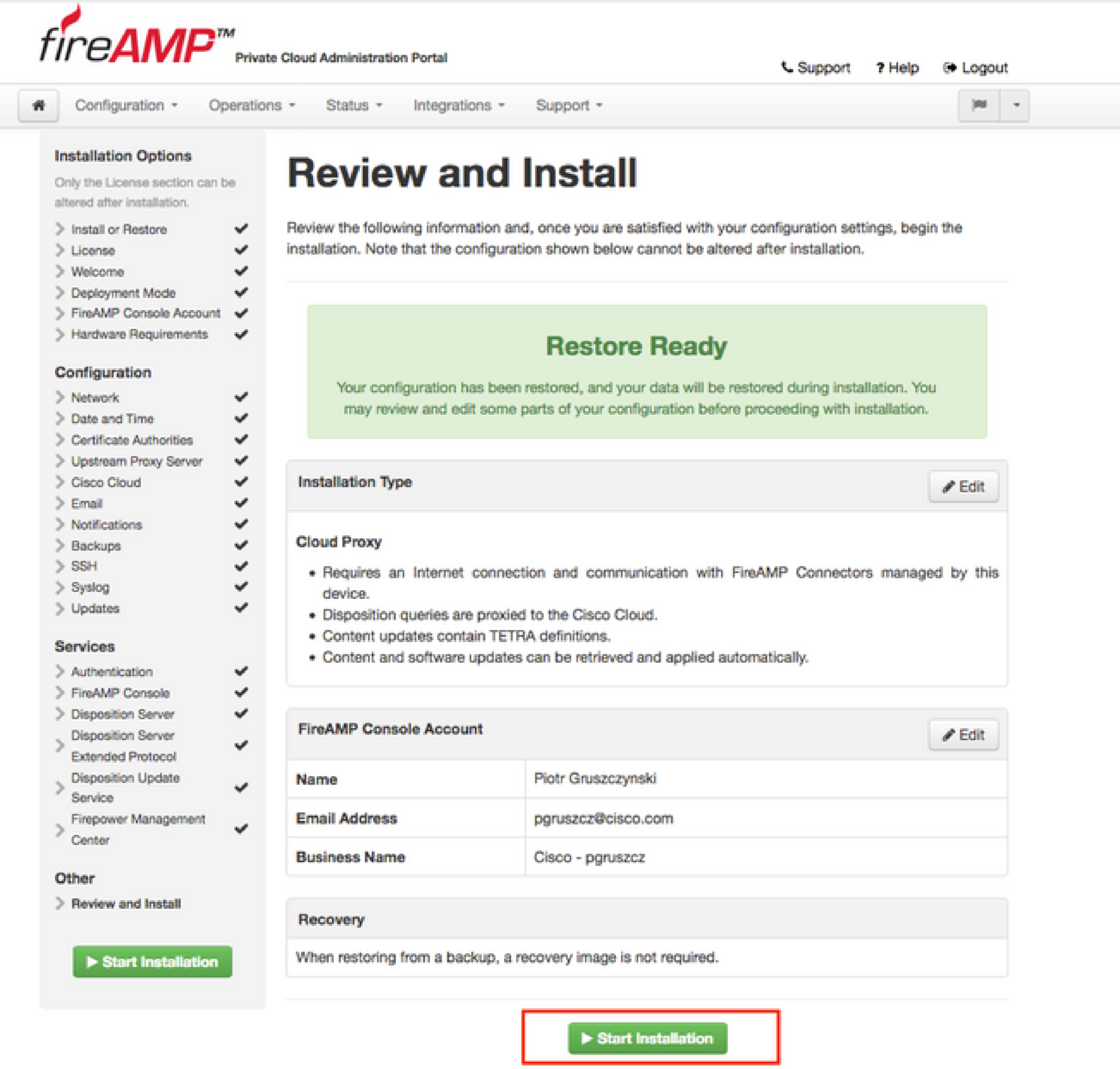
● Certificate (PEM .crt)	Key (PEM .key)
✓ Certificate file has been uploaded.	✓ Key file has been uploaded.
✓ Certificate is in a readable format.	✓ Key contains a supported key type.
✓ Certificate start and end dates are valid.	✓ Key contains public key material.
✓ Certificate contains a subject.	✓ Key contains private key material.
✓ Certificate contains a common name.	✓ Key contains a public key matching the uploaded certificate.
✓ Certificate contains a public key matching the uploaded key.	private.key
✓ Certificate matches hostname.	
✓ Certificate is signed by a trusted root authority.	
authentication_serv	

Step 5. You need to make sure all of the requirements are met before you can proceed to the next step. Highlighted requirements are met if the root certificate used to sign the **Authentication** service is correctly placed in the **Certificate Authorities** store.

> **Caution**: You can change the hostnames for all other Services at this stage only. Once the installation is finished, hostname for the services cannot be changed. Later you can change certificates only. You need to make sure you understand the risk of such operation. If you change the hostnames of the services used by the Connectors or AMP for Network devices, they can have problems to communicate with the cloud once upgrade is completed.

7. Installation

Step 1. Once every section is completed and marked as valid, you begin the installation. Navigate to **Review and Install** section and click **Start Installation** button, as shown in the image.



Installation Options

Only the License section can be altered after installation.

- Install or Restore ✓
- License ✓
- Welcome ✓
- Deployment Mode ✓
- FireAMP Console Account ✓
- Hardware Requirements ✓

Configuration

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

Services

- Authentication ✓
- FireAMP Console ✓
- Disposition Server ✓
- Disposition Server Extended Protocol ✓
- Disposition Update Service ✓
- Firepower Management Center ✓

Other

- 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.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type Edit

Cloud Proxy

- Requires an Internet connection and communication with FireAMP 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.

FireAMP Console Account Edit

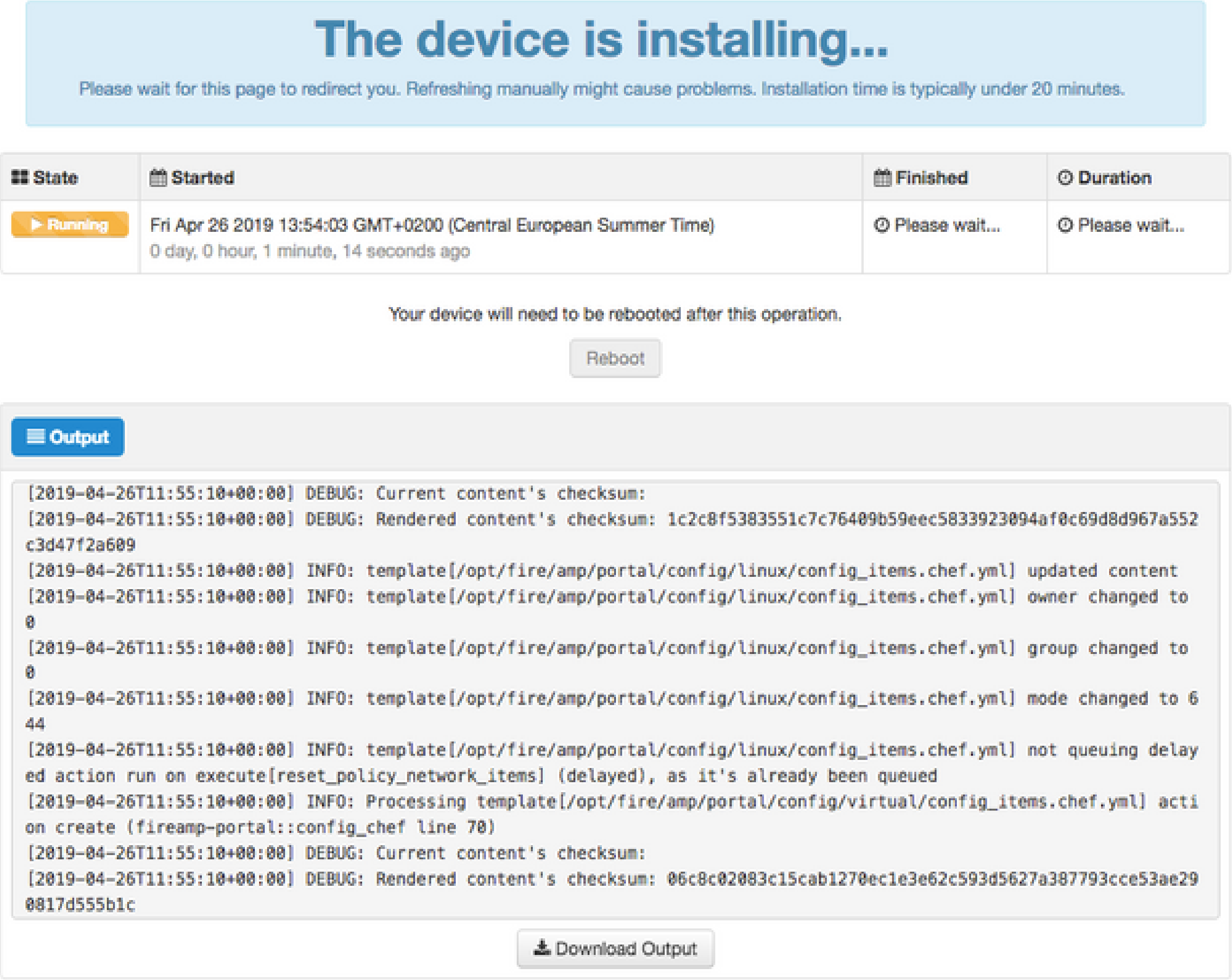
Name	Piotr Gruszczynski
Email Address	pgruszcz@cisco.com
Business Name	Cisco - pgruszcz

Recovery

When restoring from a backup, a recovery image is not required.

▶ Start Installation

Step 2. Administrator portal presents you the current state, start date and logs. If you encounter any errors or problems which needs support attention, collect the logs by click **Download Output** button, as shown in the image, and attach them to the TAC case.



The device is installing...

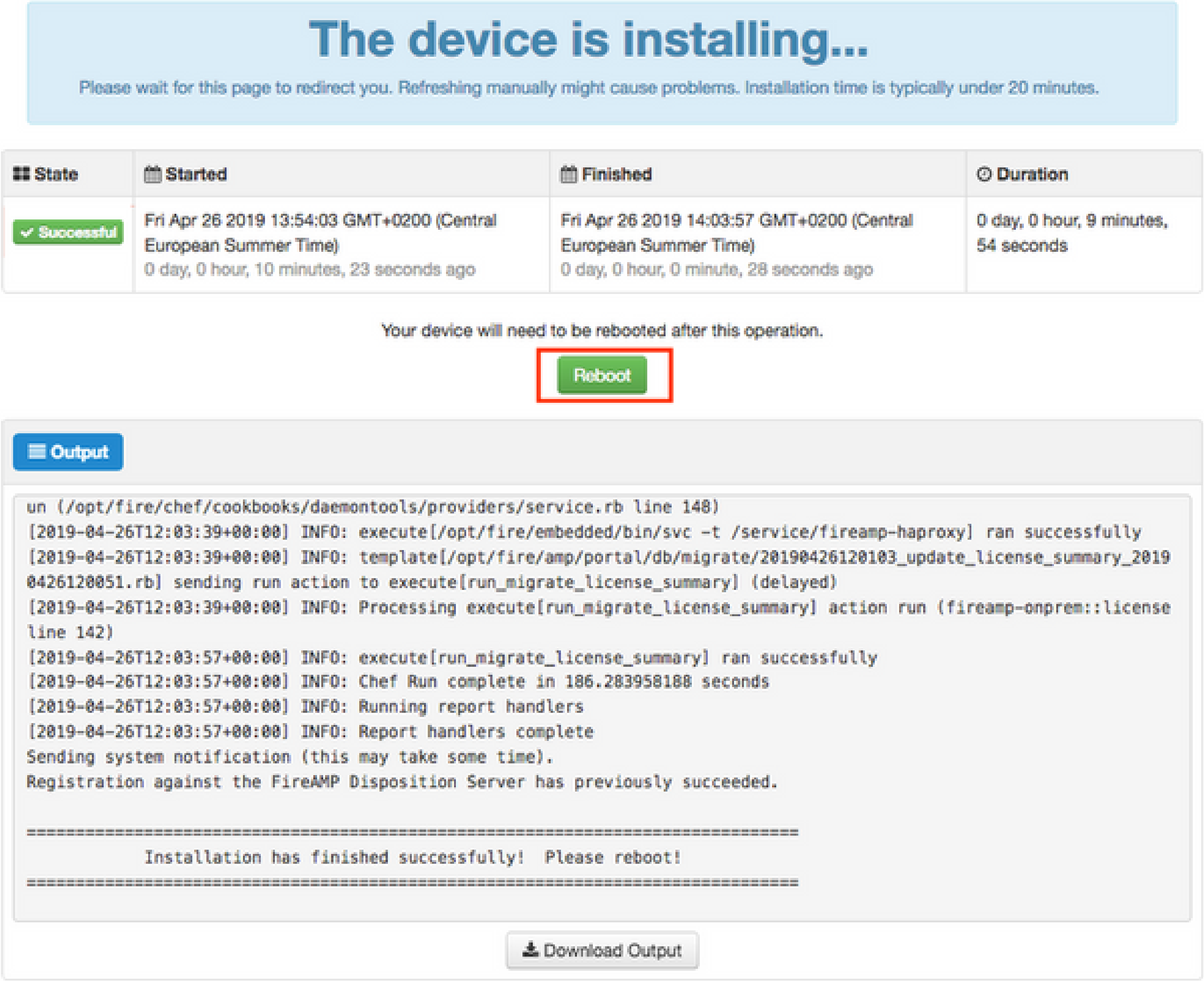
Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 1 minute, 14 seconds ago	Please wait...	Please wait...

Your device will need to be rebooted after this operation.

```
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 1c2c8f5383551c7c76409b59eec5833923094af0c69d8d967a552
c3d47f2a609
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] updated content
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] owner changed to
0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] group changed to
0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] mode changed to 6
44
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] not queuing delay
ed action run on execute[reset_policy_network_items] (delayed), as it's already been queued
[2019-04-26T11:55:10+00:00] INFO: Processing template[/opt/fire/amp/portal/config/virtual/config_items.chef.yml] acti
on create (fireamp-portal::config_chef line 70)
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 06c8c02083c15cab1270ec1e3e62c593d5627a387793cce53ae29
0817d555b1c
```

Step 3. When the installation is successful, you must reboot the device to finish the process. Click **Reboot** button to proceed with the restart procedure, as shown in the image.



The device is installing...

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

State	Started	Finished	Duration
✓ Successful	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 10 minutes, 23 seconds ago	Fri Apr 26 2019 14:03:57 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 28 seconds ago	0 day, 0 hour, 9 minutes, 54 seconds

Your device will need to be rebooted after this operation.

```
un (/opt/fire/chef/cookbooks/daemontools/providers/service.rb line 148)
[2019-04-26T12:03:39+00:00] INFO: execute[/opt/fire/embedded/bin/svc -t /service/fireamp-haproxy] ran successfully
[2019-04-26T12:03:39+00:00] INFO: template[/opt/fire/amp/portal/db/migrate/20190426120103_update_license_summary_2019
0426120051.rb] sending run action to execute[run_migrate_license_summary] (delayed)
[2019-04-26T12:03:39+00:00] INFO: Processing execute[run_migrate_license_summary] action run (fireamp-onprem::license
line 142)
[2019-04-26T12:03:57+00:00] INFO: execute[run_migrate_license_summary] ran successfully
[2019-04-26T12:03:57+00:00] INFO: Chef Run complete in 186.283958188 seconds
[2019-04-26T12:03:57+00:00] INFO: Running report handlers
[2019-04-26T12:03:57+00:00] INFO: Report handlers complete
Sending system notification (this may take some time).
Registration against the FireAMP Disposition Server has previously succeeded.

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

Step 4. After the reboot procedure, you can login to the **Administrator** Portal and **Console** Portal. The upgrade procedure is finished.

8. Post upgrade checks

Once the device is rebooted, please make sure that restore was completed successfully:

Step 1. Check if connectors are able to communicate to the newly installed virtual appliance 3.0.1.

Step 2. Make sure that Events, Device Trajectory and Computers object are correctly restored and presented in the console portal.

Step 3. If you have any AMP for Network integrations like FMC, ESA, WSA make sure they can communicate to the File Disposition server.

Step 4. Check for any Content/Software (Operations -> Update Device) updates and proceed with the installation of such.

It is highly suggested to perform tests to assure a successful upgrade.

Changes in Virtual Private Cloud 3.0.1

1. Windows Connector version 6.1.7

Private Cloud 3.0.1 is shipped with the support for 6.1.7 Windows Connector version, you can find the documentation about it under the link: Release notes for 6.1.7

> **Caution**: If you have made any change in certificates, make sure that before an upgrade or installation to version 6.1.7 of Windows Connector, certificates used for private cloud services are trusted on the endpoint itself. Trust needs to be on the machine level, not user. If this condition is not met, connectors do not trust the certificate presented by Private Cloud which keeps them in a disconnected state.

2. Certificate Authorities and Authentication service

Changes were thoroughly described in the user guide for 3.0: Private Cloud User Guide.

Certificate Authorities allows you to manage root certificates for your Services if you want to use a custom certificate authority. You can download or delete your root certificate if needed.

Authentication service will be used in future versions of Private Cloud to handle user authentication requests. It is added in 3.0.1 version for future compatibility.