Re-Image the AMP Private Cloud PC3000 and Restore the Backup

Contents

Introduction

This document describes how to re-image Advanced Malware Protection (AMP) Private Cloud hardware appliance to the factory state and then restore the backup. If you want to just revert the appliance to the factory state, skip step 8 and follow the regular installation.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AMP Private Cloud PC3000
- Kernel-based Virtual Machine (KVM) access via Cisco Integrated Management Controller (CIMC)

Components Used

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

- Cisco AMP Private Cloud PC3000 3.1.1
- Chrome browser to access the KVM console

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.

Configure

Step 1. Log in to CIMC. Open the KVM console.

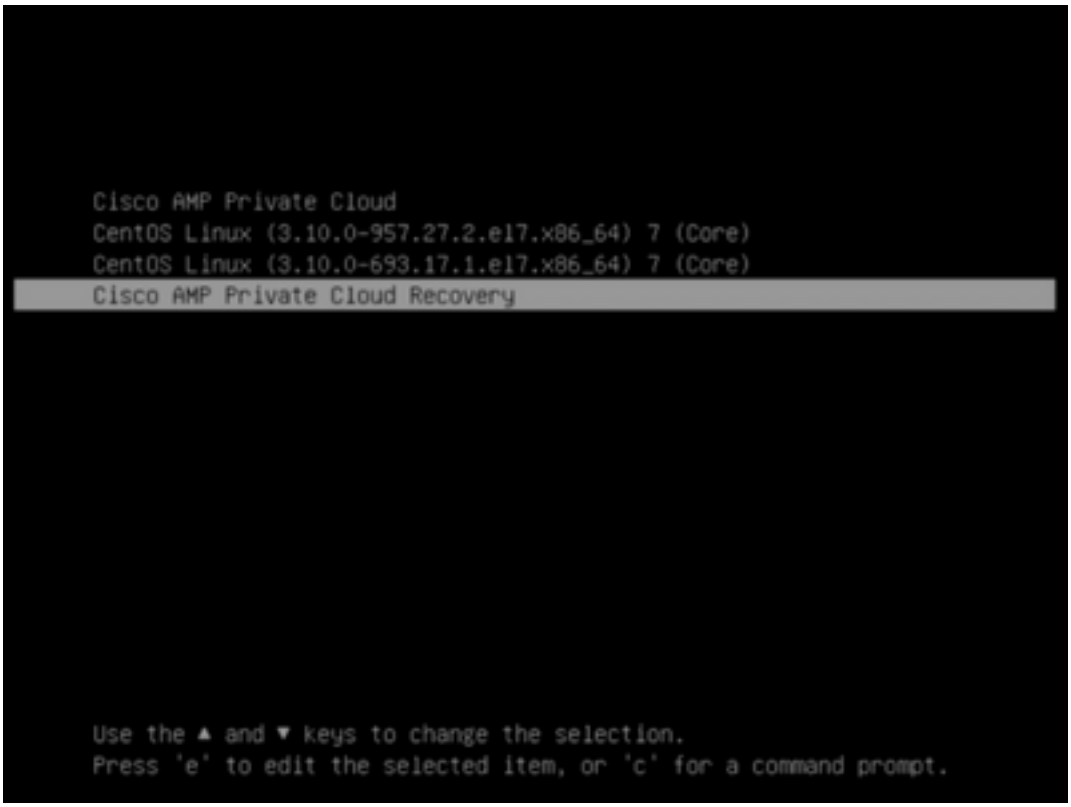
Ensure pop-ups are enabled for that page in the browser.

Step 2. Reload the appliance.

You can reboot the appliance either via the admin portal, Secure Shell (SSH), or CIMC KVM.

Step 3. After the Basic Input Output System (BIOS) Power-on self-test (POST) finishes, GNU GRand Unified Bootloader (GRUB) menu shows up:

Select **Cisco AMP Private Cloud Recovery > Appliance Reinstall Options > Appliance Reinstall**.

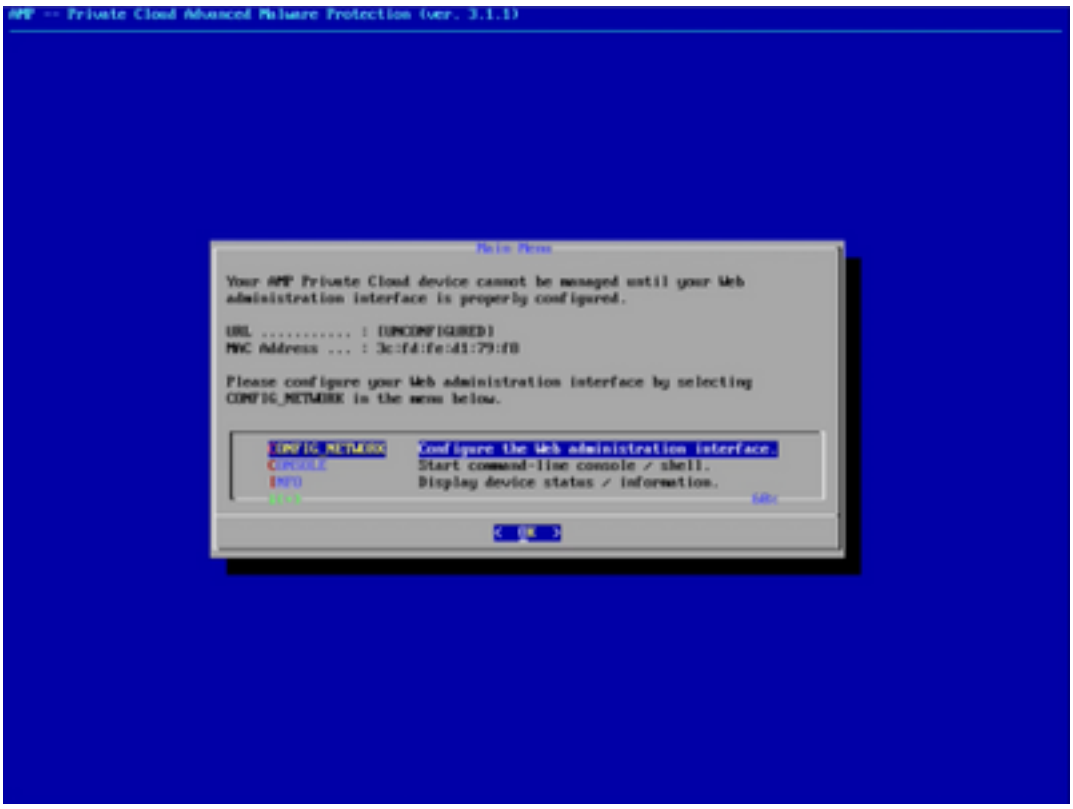


Step 4. Enter username and password.

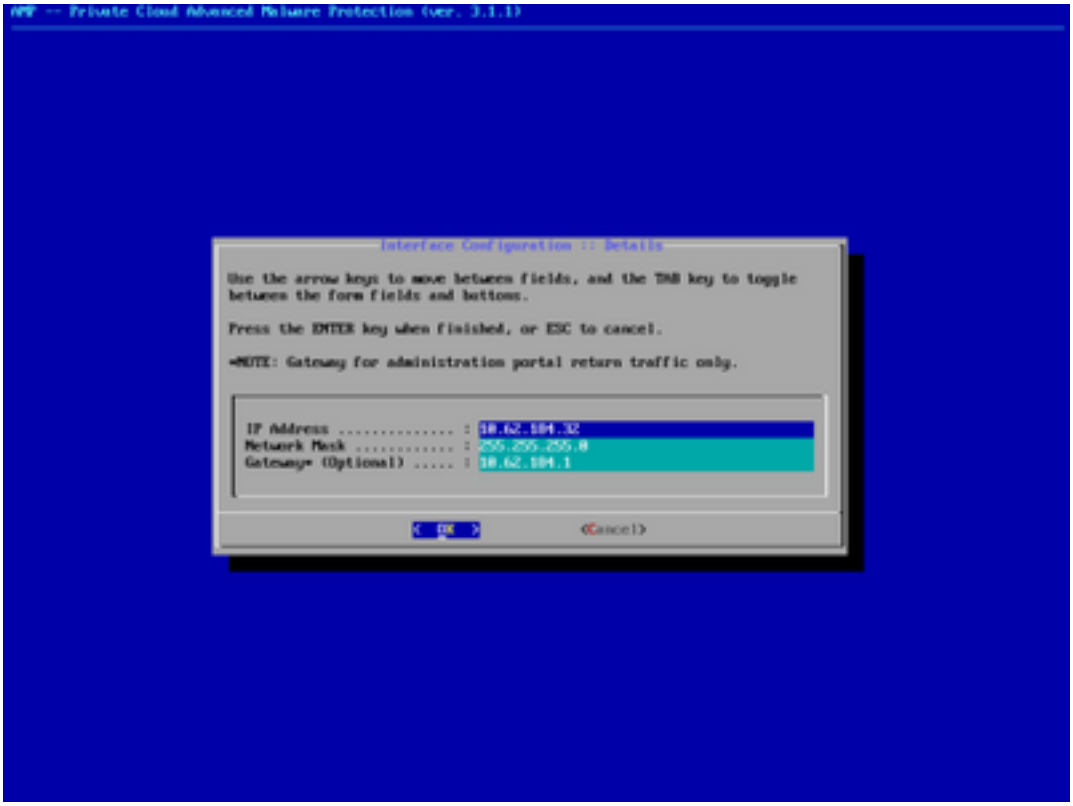
Username: **reinstall**

Password: **yes**

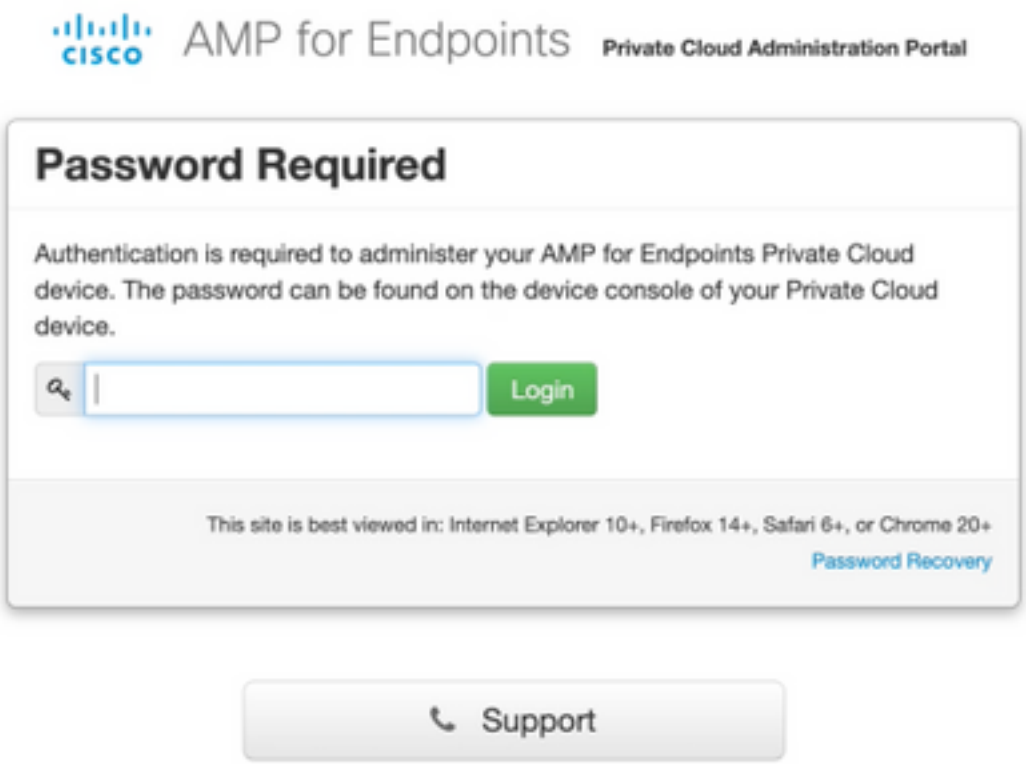
Step 5. Reimage starts and after reload you are presented with the initial menu.



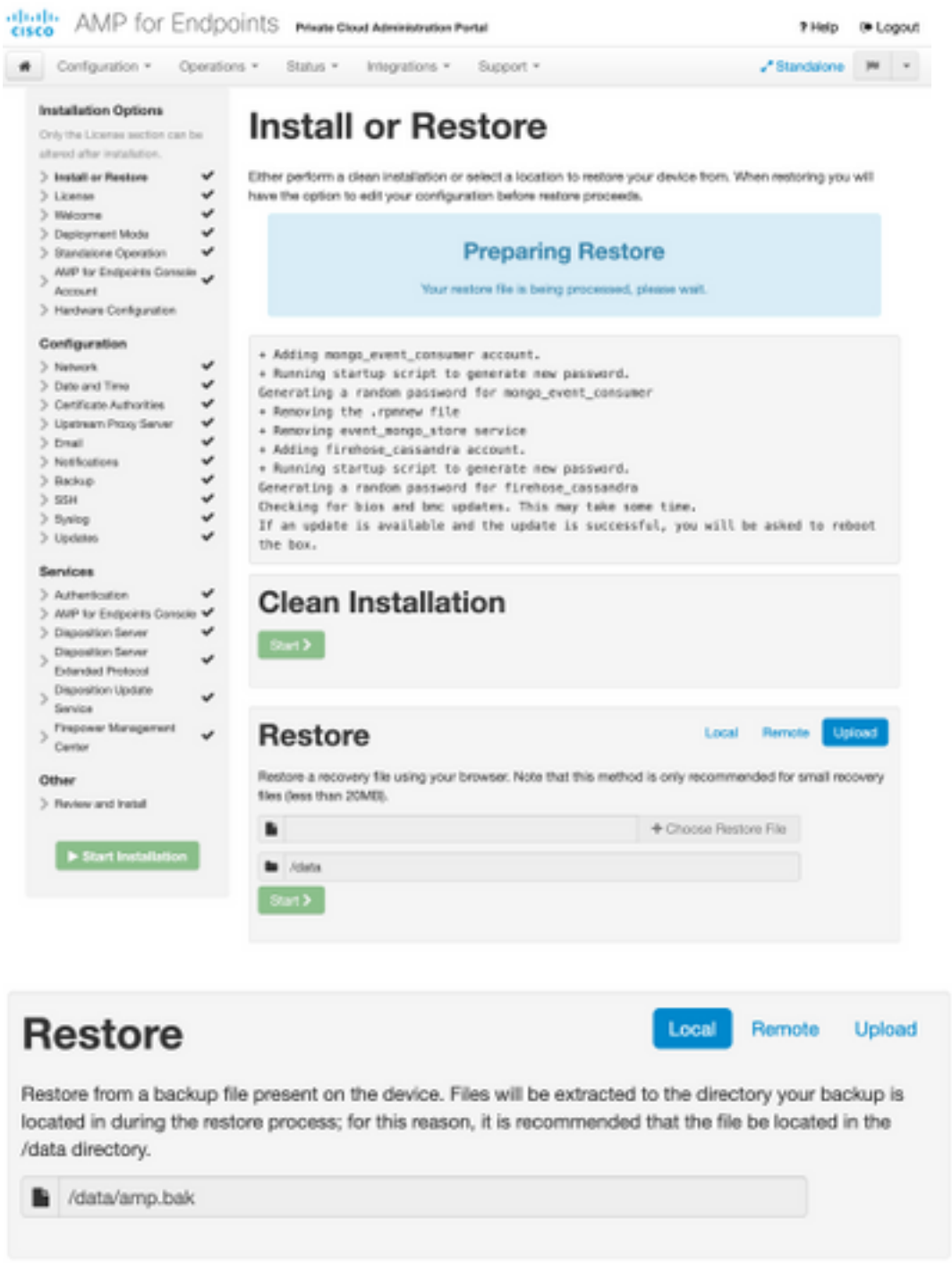
Step 6. Configure the network in CONFIG_NETWORK sub-menu.



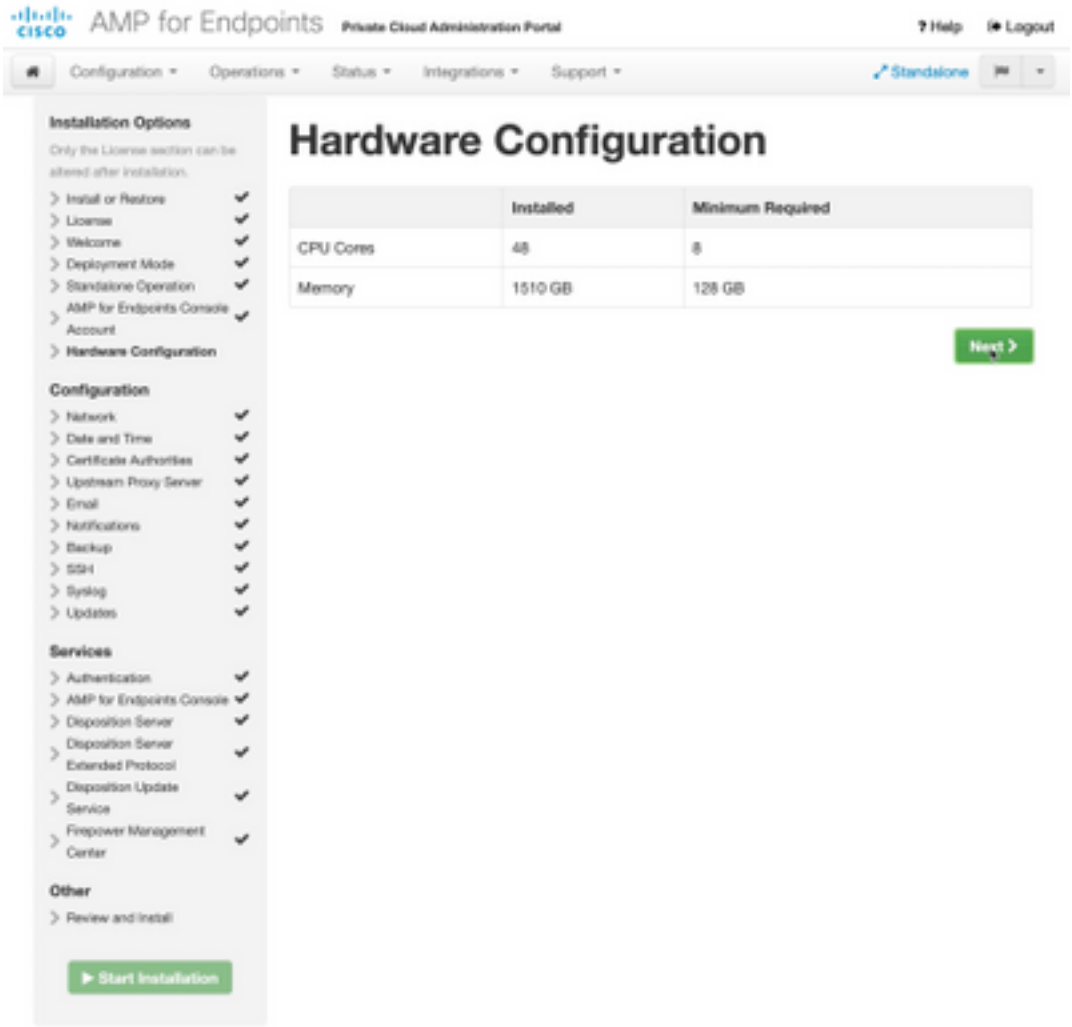
Step 7. Log in to AMP OPadmin portal with password from step 5.

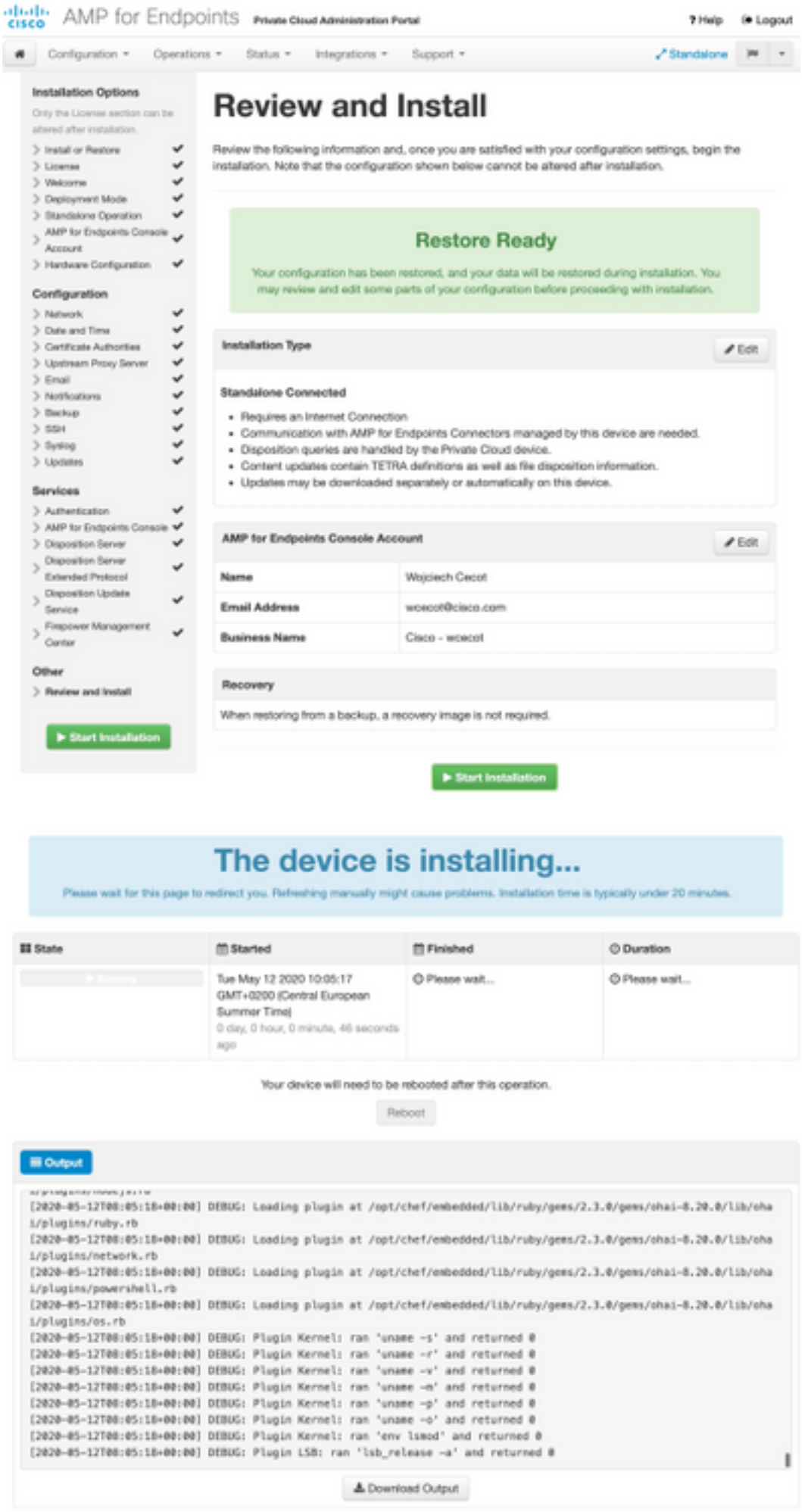


Step 8. Use SFTP or SCP to download backup from remote server to /data/.

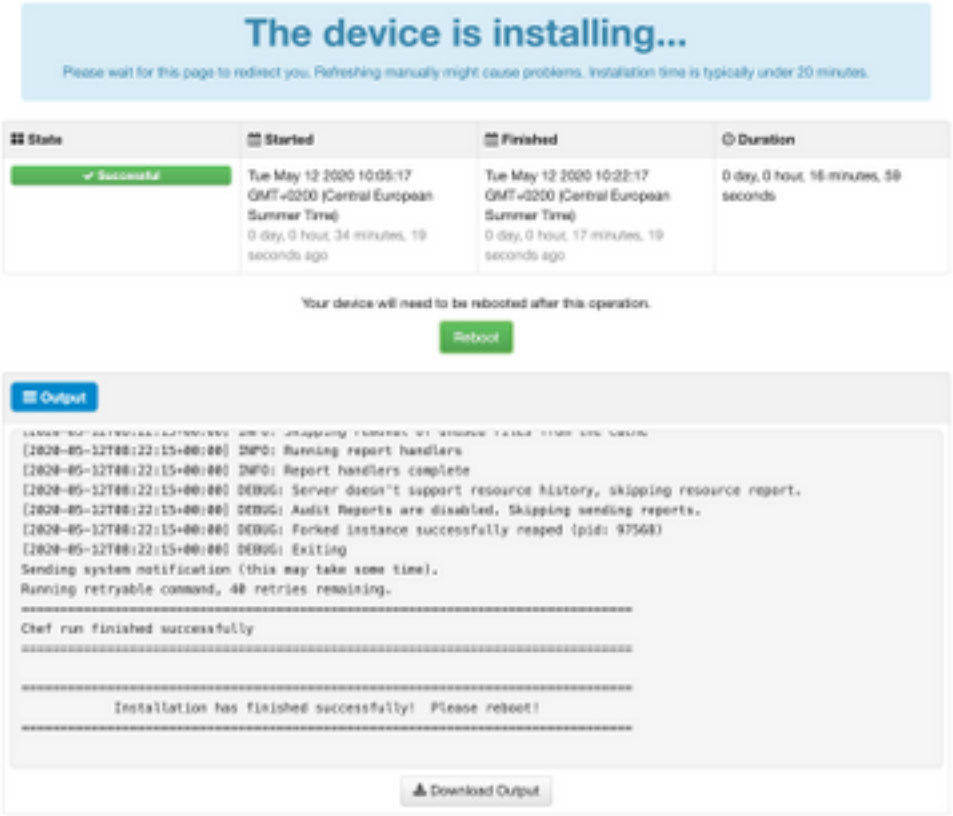


Step 9. Confirm Hardware Configuration, click **Next > Start Installation**.


AMP for Endpoints
Private Cloud Administration Portal
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
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 Configuration
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
Review and Install
Start Installation
Hardware Configuration
Installed
Minimum Required
CPU Cores
48
8
Memory
1510 GB
128 GB
Next


AMP for Endpoints
Private Cloud Administration Portal
Help
Logout
Configuration
Operations
Status
Integrations
Support
Standalone
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 Configuration
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
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
Standalone Connected
Requires an Internet Connection
Communication with AMP for Endpoints Connectors managed by this device are needed.
Disposition queries are handled by the Private Cloud device.
Content updates contain TETRA definitions as well as file disposition information.
Updates may be downloaded separately or automatically on this device.
AMP for Endpoints Console Account
Edit
Name
Wojciech Cecot
Email Address
wcecot@cisco.com
Business Name
Cisco - wcecot
Recovery
When restoring from a backup, a recovery image is not required.
Start Installation
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
Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time)
0 day, 0 hour, 0 minute, 46 seconds ago
Please wait...
Please wait...
Your device will need to be rebooted after this operation.
Reboot
Output
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/ohai/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/ohai/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/ohai/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/ohai-8.20.0/lib/ohai/plugins/os.rb
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -s' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -r' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -v' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -m' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -p' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'uname -o' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin Kernel: ran 'env lsmod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0
Download Output

Step 10. Reboot is required after successful restore.



Verify

After the appliance is rebooted, check if both portals work fine. Try to open OPadmin and Console portal in the web browser. It takes few minutes for both portals to be accessible.

Troubleshoot

In case backup restore process, password for OPadmin and Console portals are the same as before. Otherwise, you need to use what you have set in the wizard.