Re-Image the Secure Endpoint Private Cloud PC3000 or PC4000 and Restore the Backup

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

Verify

Troubleshoot

Introduction

This document describes how to re-image Secure Endpoint Private Cloud hardware appliance to the factory state and then restore the backup.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Endpoint Private Cloud PC3000 or PC4000
- 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 Secure Endpoint Private Cloud PC4000 4.2.2
- 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.

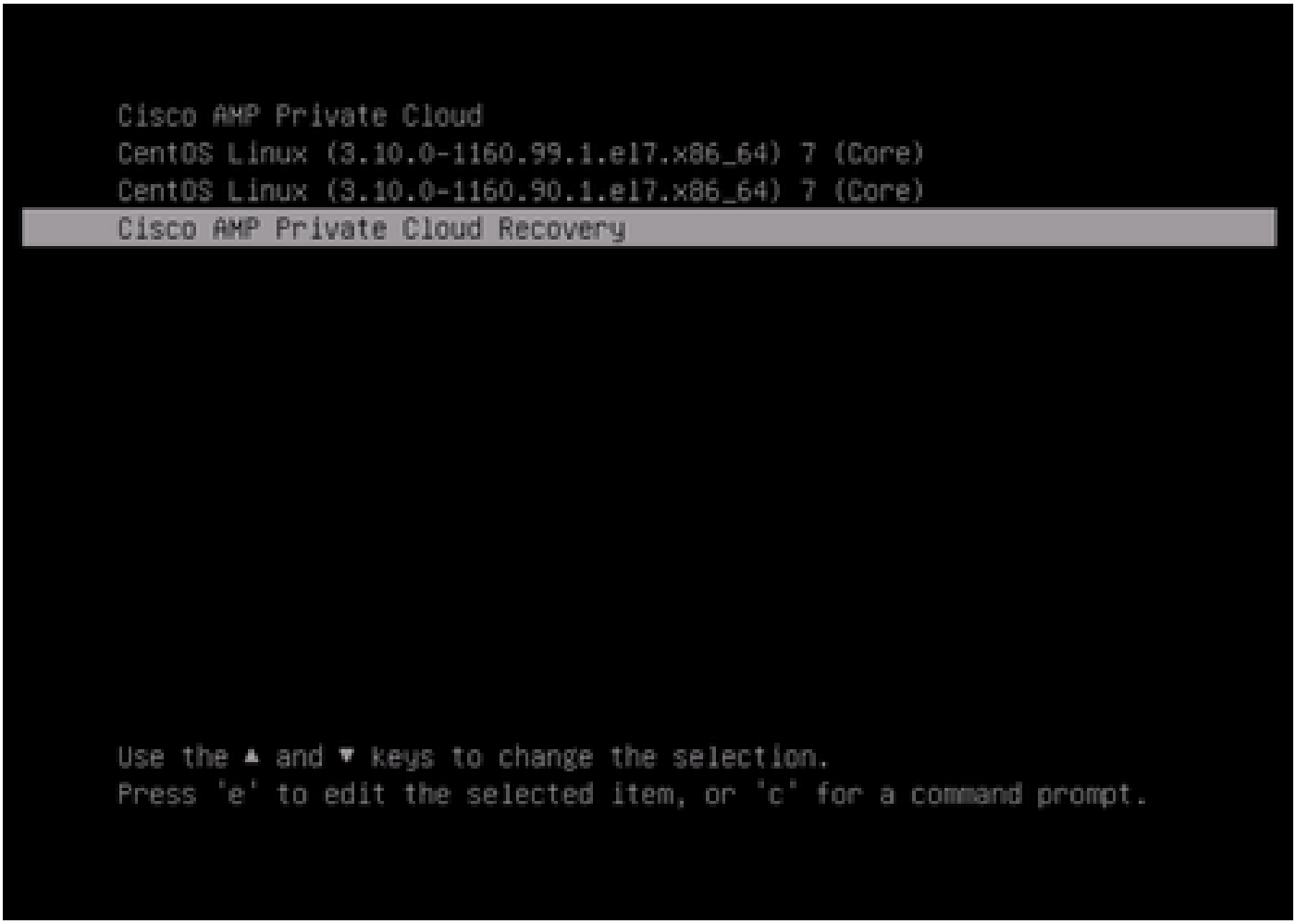
Ensure pop-ups are enabled for that page in the browser.

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**.




Attempt Regular Boot
Recovery Boot
Appliance Reinstall Options
Wipe Appliance Options
Boot previous Recovery Boot version
CISCO
Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.



Step 4. Enter username and password.

Username: **reinstall**

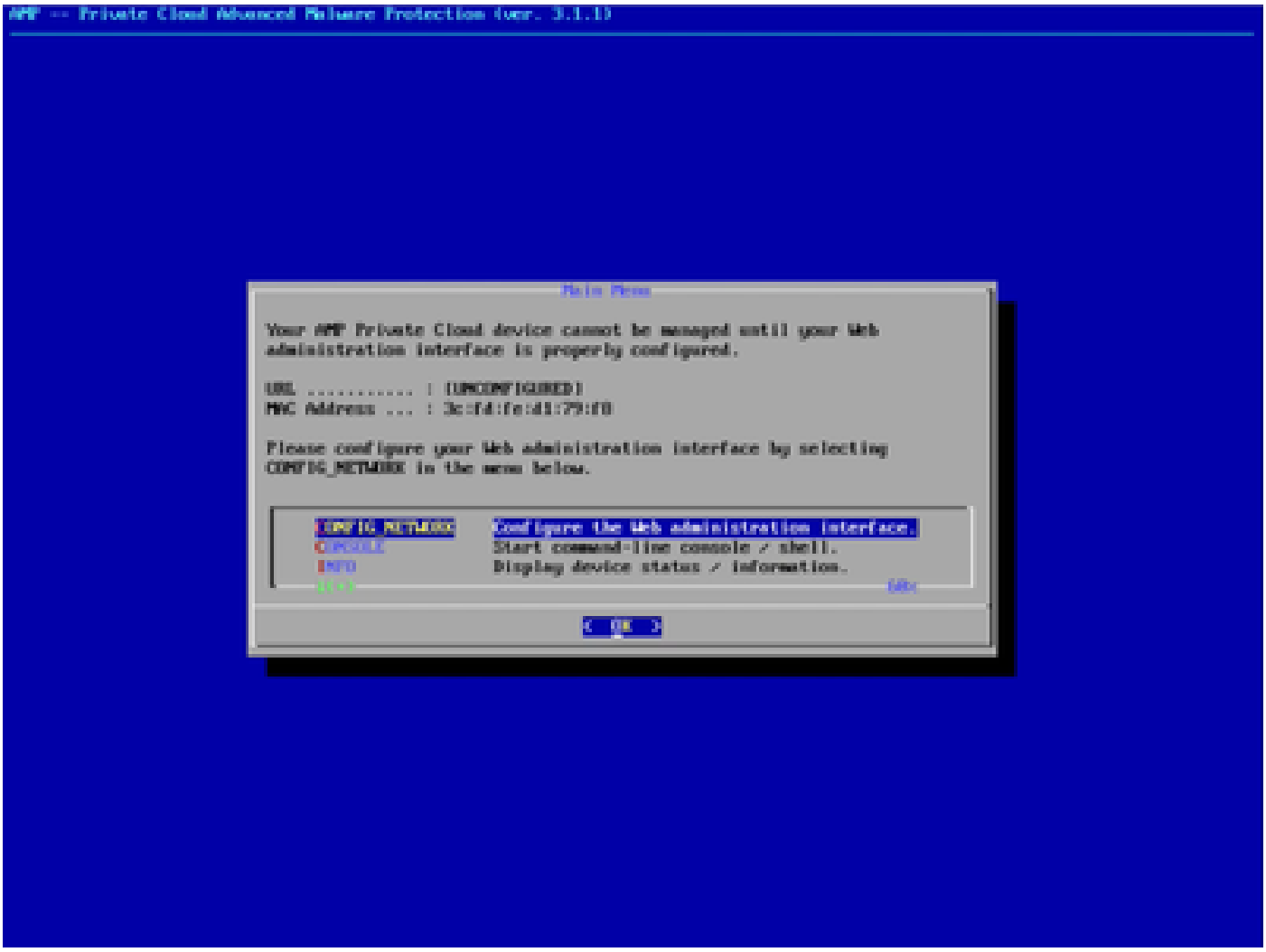
Password: **yes**



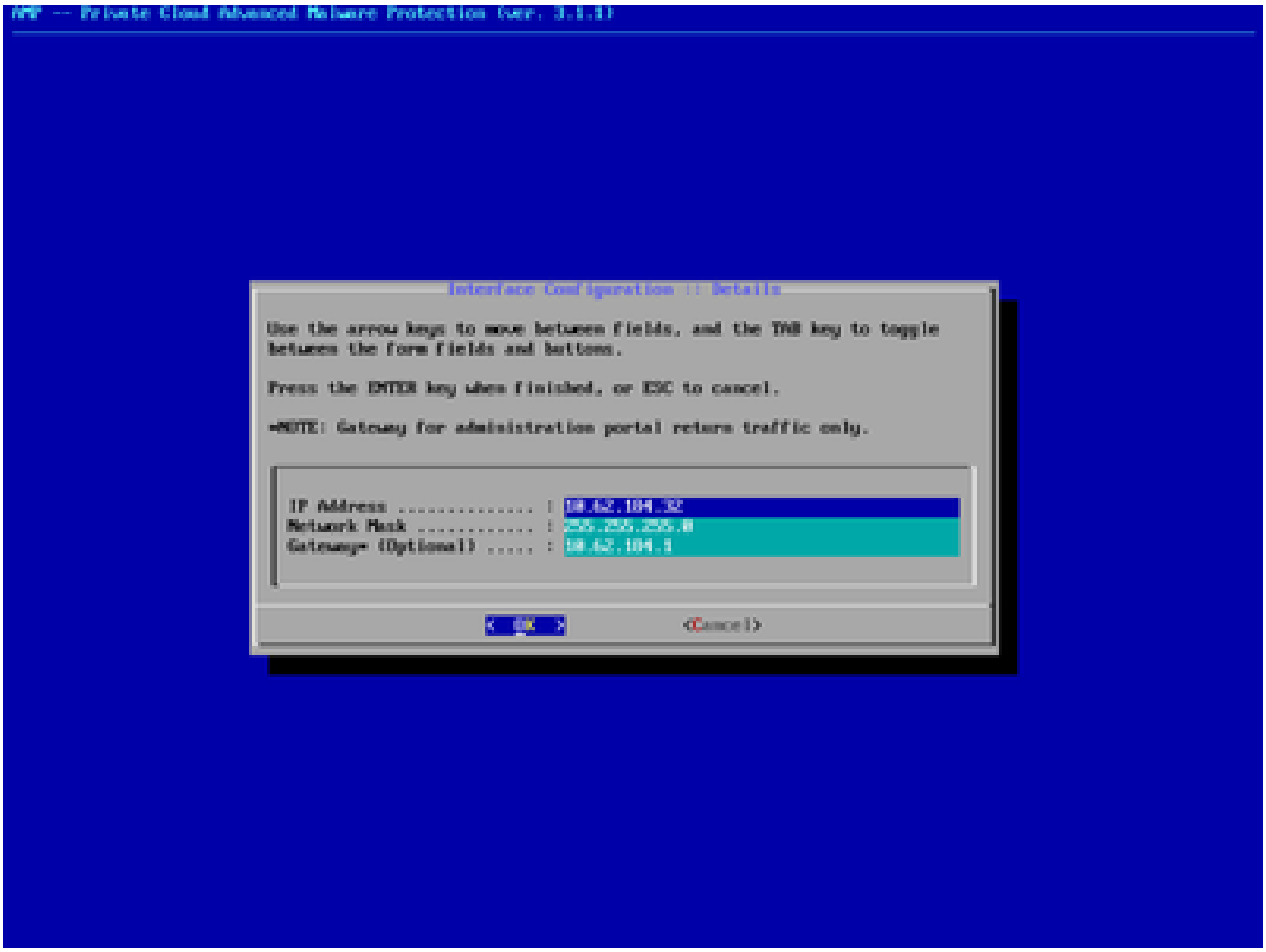
Step 5. Reimage starts and after reload you are presented with the initial menu.



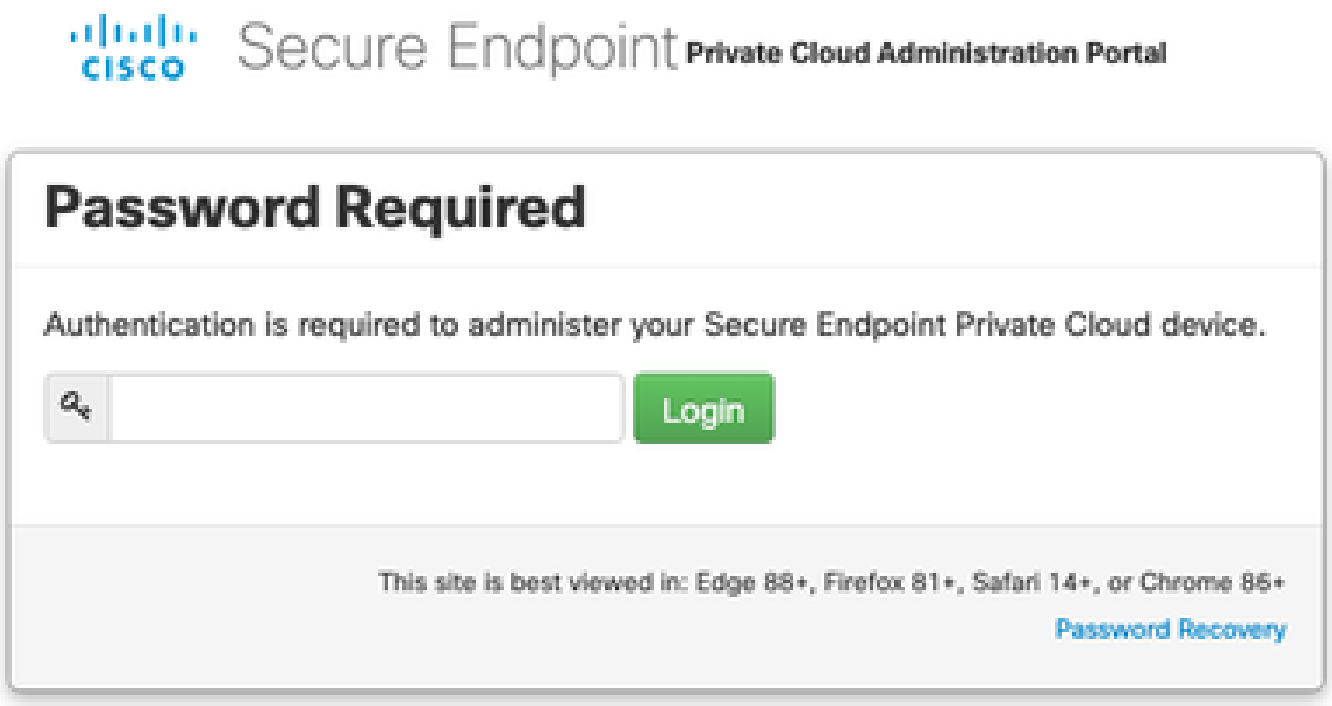
```
[    0.737008] usbcore: registered new interface driver usbserial_generic
[    0.744808] usbserial: USB Serial support registered for generic
[    0.753899] i8042: PNP: No PS/2 controller found. Probing ports directly.
[    0.905203] usb 1-6: new high-speed USB device number 2 using xhci_hcd
[    0.938201] usb 1-6: New USB device found, idVendor=2e8a, idProduct=0400
[    0.123103] usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[    0.130530] usb 1-6: Product: Raspberry Pi Pico
[    0.136013] usb 1-6: Manufacturer: Raspberry Pi
[    0.140912] usb 1-6: SerialNumber: 0xBADFACE
[    0.146133] hub 1-6:1.0: USB hub found
[    0.150658] hub 1-6:1.0: 7 ports detected
[    0.267503] usb 1-7: new high-speed USB device number 3 using xhci_hcd
[    0.239535] i8042: Can't read CTR while initializing i8042
[    0.303622] i8042: probe of i8042 failed with error -5
[    0.308705] mousedev: PS/2 mouse device common for all mice
[    0.315268] rtc_cmos 00:00: RTC can wake from S4
[    0.336427] rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0
[    0.320818] rtc_cmos 00:00: alarms up to one month, y3k, 114 bytes nvram, hpet ir
[    0.325435] intel_pstate: Intel P-state driver initializing
[    0.332253] intel_pstate: HWP enabled
[    0.335208] cpuidle: using governor menu
[    0.340827] EFI Variables Facility v0.08 2004-May-17
[    0.338265] tsc: Refined TSC clocksource calibration: 2593.906 MHz
[    0.384193] Switched to clocksource tsc
[    0.485753] hidraw: raw HID events driver (C) Jiri Kosina
[    0.490874] usbhid: USB HID core driver
[    0.411948] usb 1-7: New USB device found, idVendor=0424, idProduct=4570
[    0.411952] usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
[    0.411955] usb 1-7: Product: USB2.0 Hub
[    0.413591] hub 1-7:1.0: USB hub found
[    0.417942] hub 1-7:1.0: 4 ports detected
[    0.441224] Detected 1 PCC Subspaces
[    0.445423] Registering PCC driver as Mailbox controller
[    0.451900] drop_monitor: Initializing network drop monitor service
[    0.456236] TCP: cubic registered
[    0.462456] Initializing XFRM netlink socket
[    0.466642] NET: Registered protocol family 10
[    0.472026] NET: Registered protocol family 17
[    0.479948] usb 1-6.1: new high-speed USB device number 4 using xhci_hcd
[    0.481000] mpls_gso: MPLS GSO support
[    0.495395] intel_rdt: Intel RDT MB allocation detected
[    0.505606] microcode: sig=0x50654, pf=0x80, revision=0x2000064
```



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

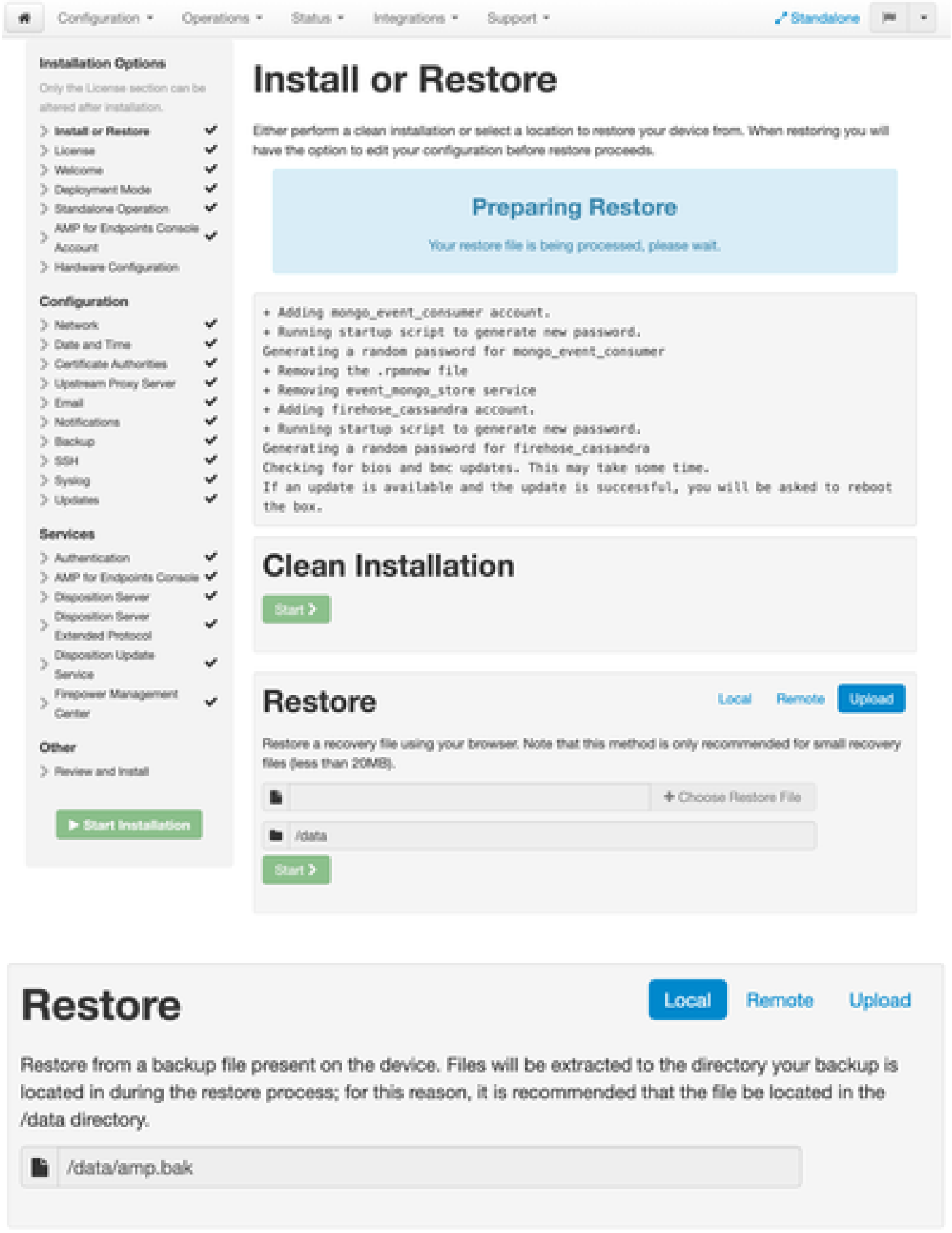


Step 7. Log in to AMP OPadmin portal with password from step 5.

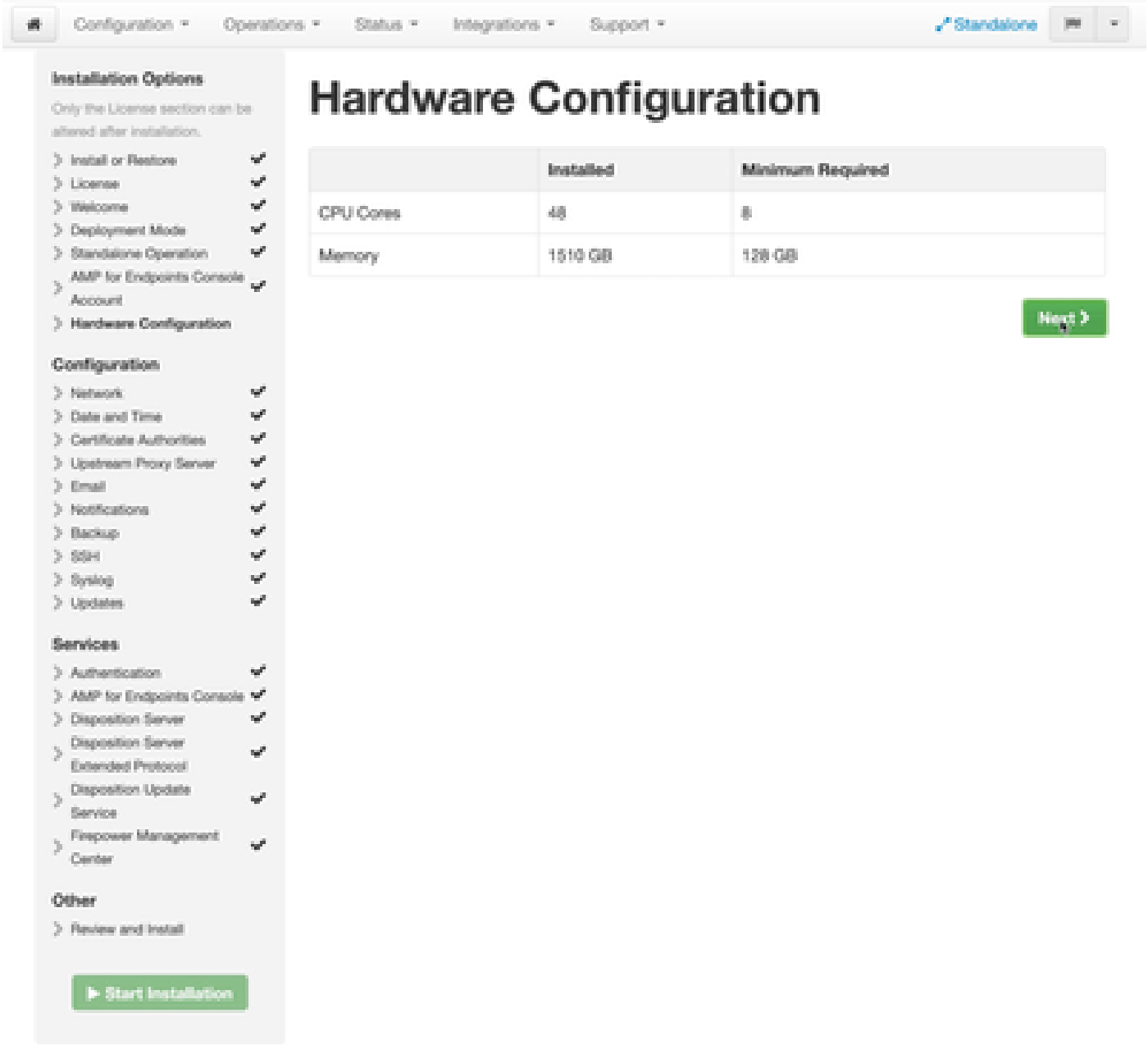


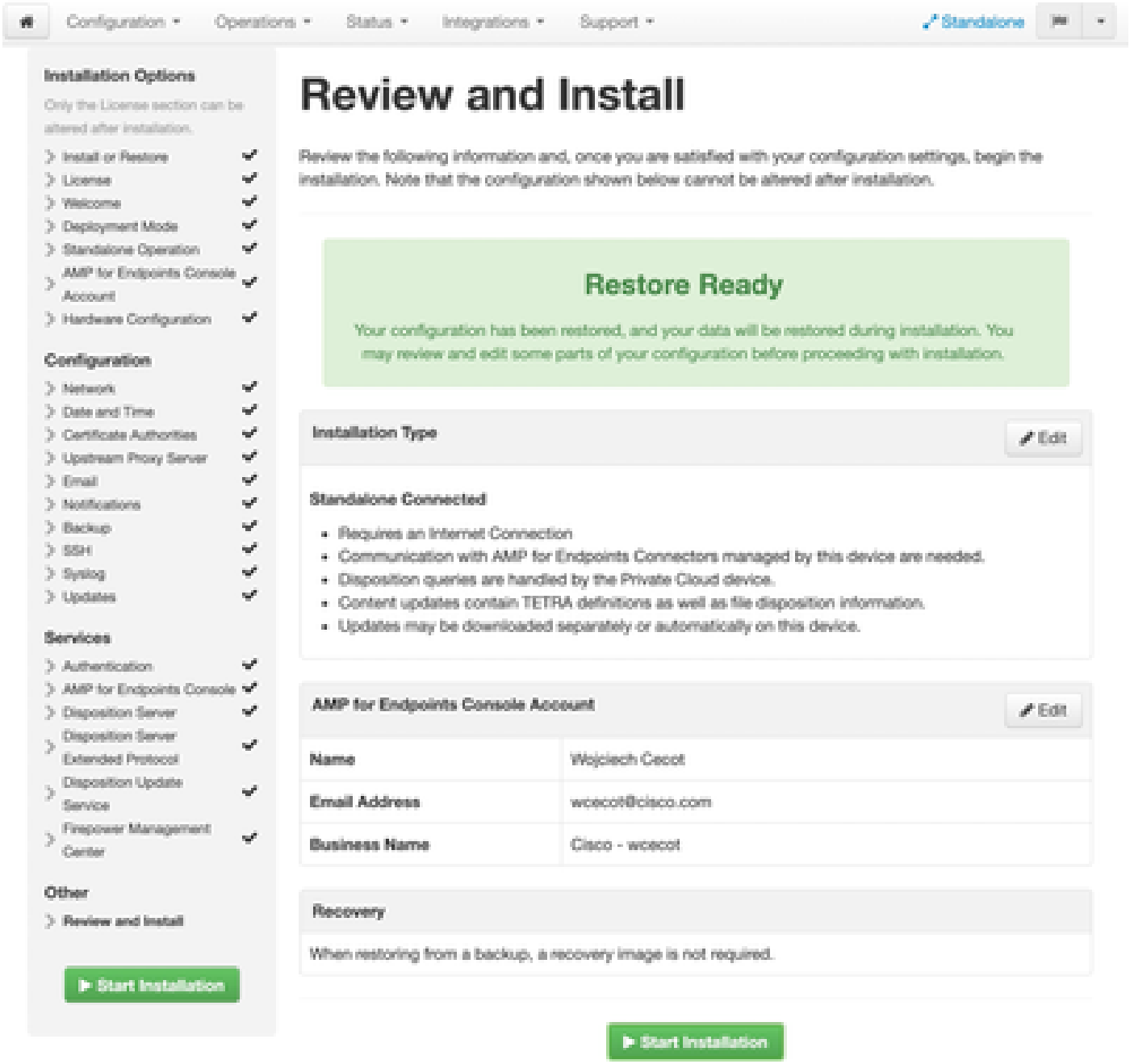
Step 8. Use SFTP or SCP to download backup from remote server to /data/.

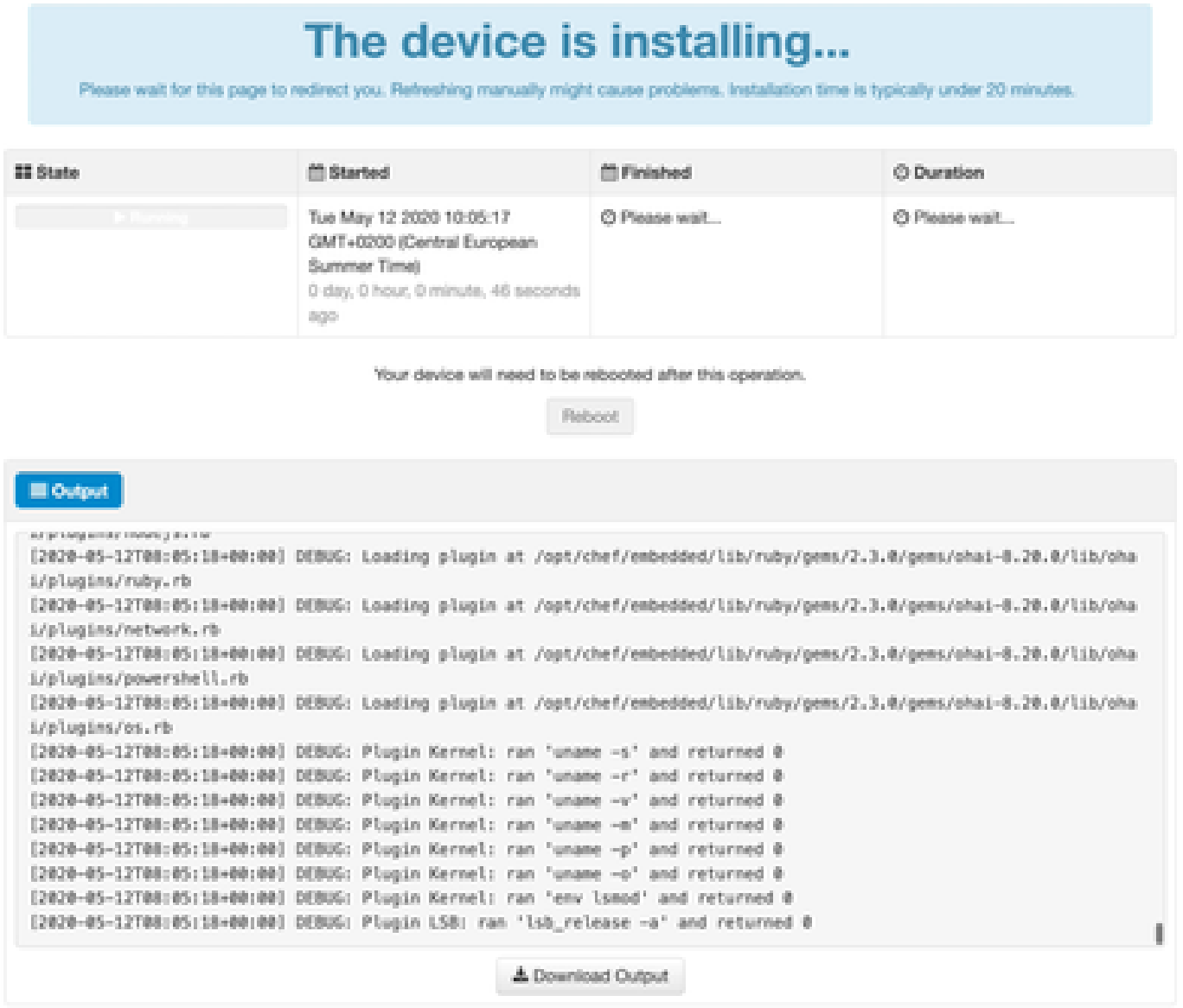
⚠ **Caution**: If you want to just revert the appliance to the factory state, skip this step and continue the regular installation.



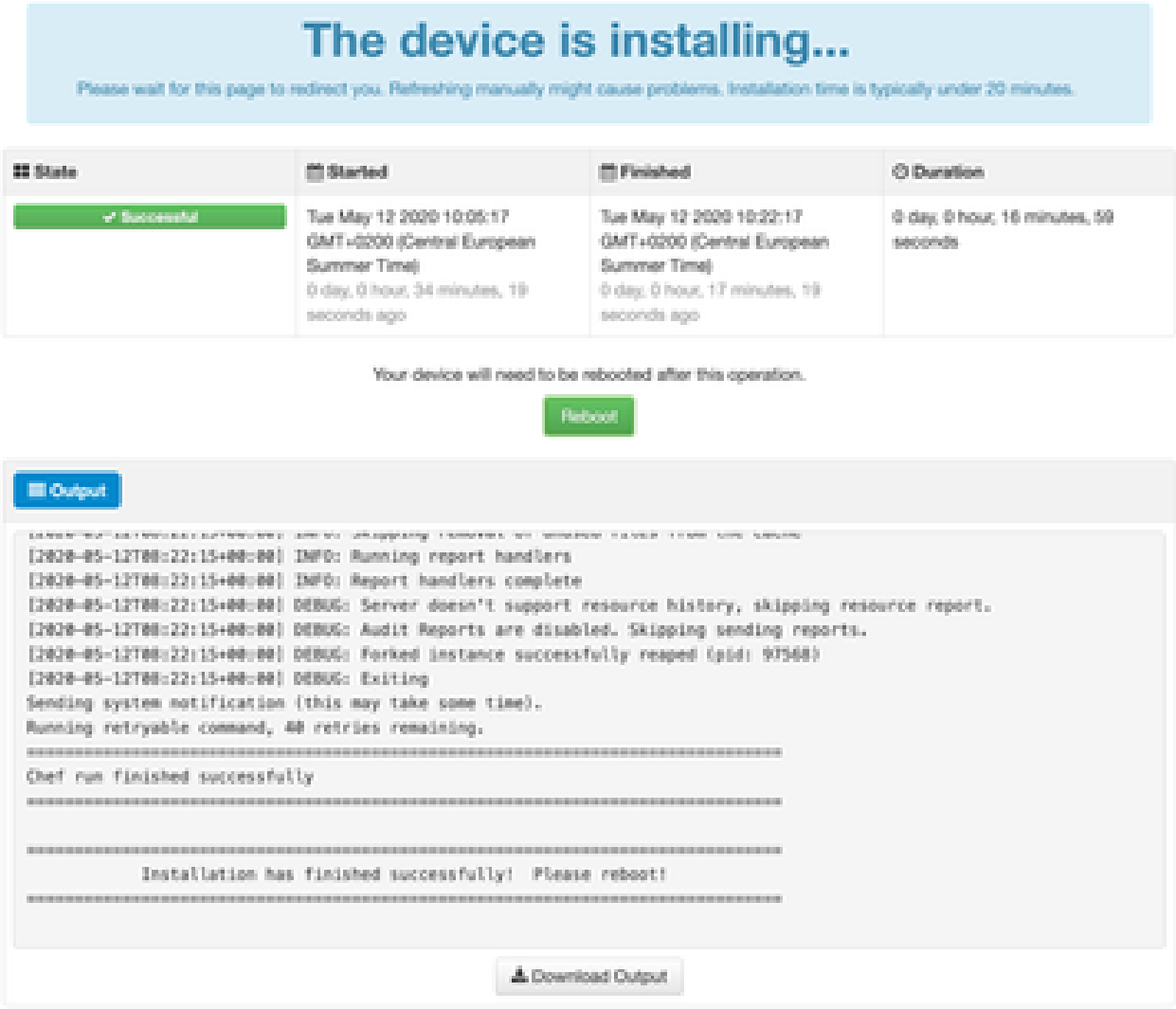
Step 9. Confirm Hardware Configuration, click **Next > Start Installation**.


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


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



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 used previously, before backup restore. Otherwise, you need to use what you have set in the wizard.