

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

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

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.

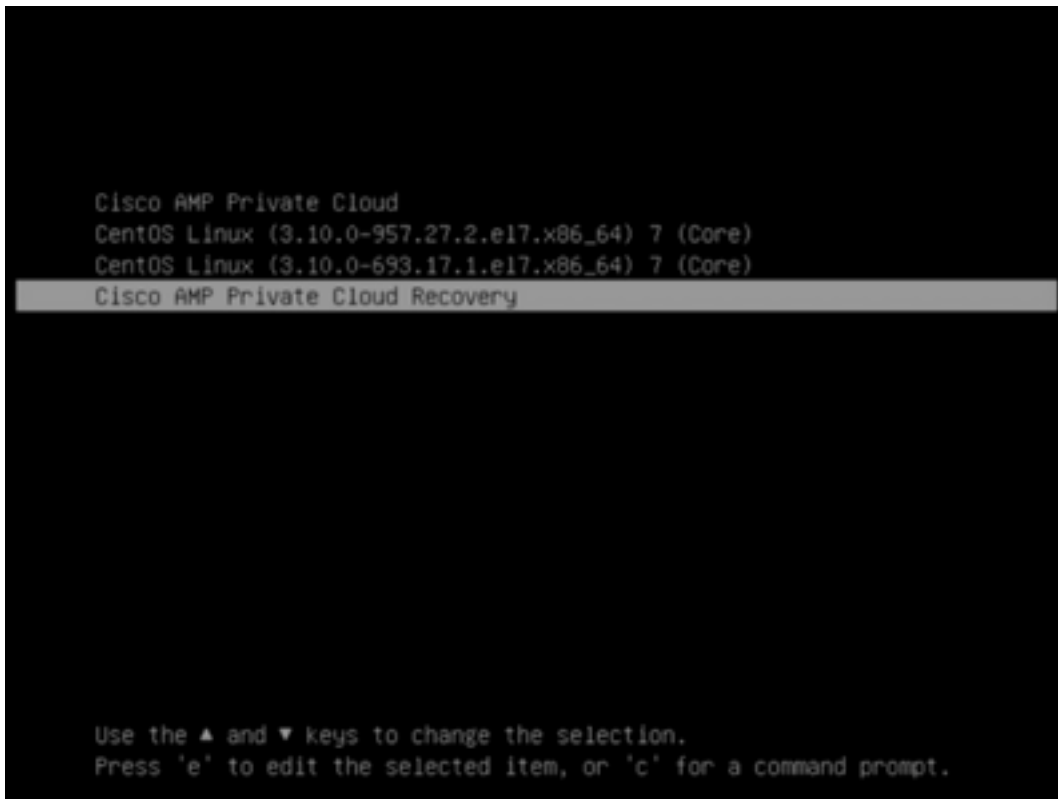
Ensure pop-ups are enabled for that page in the browser.

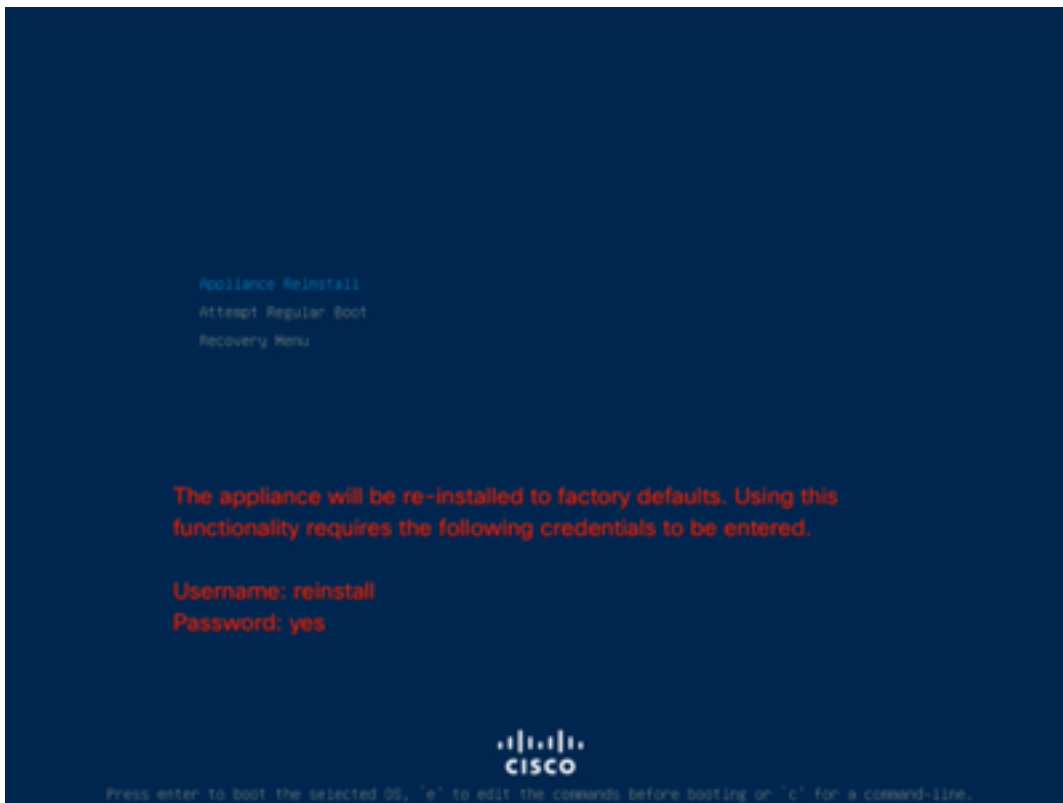
Step 2. Reload the appliance.

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**

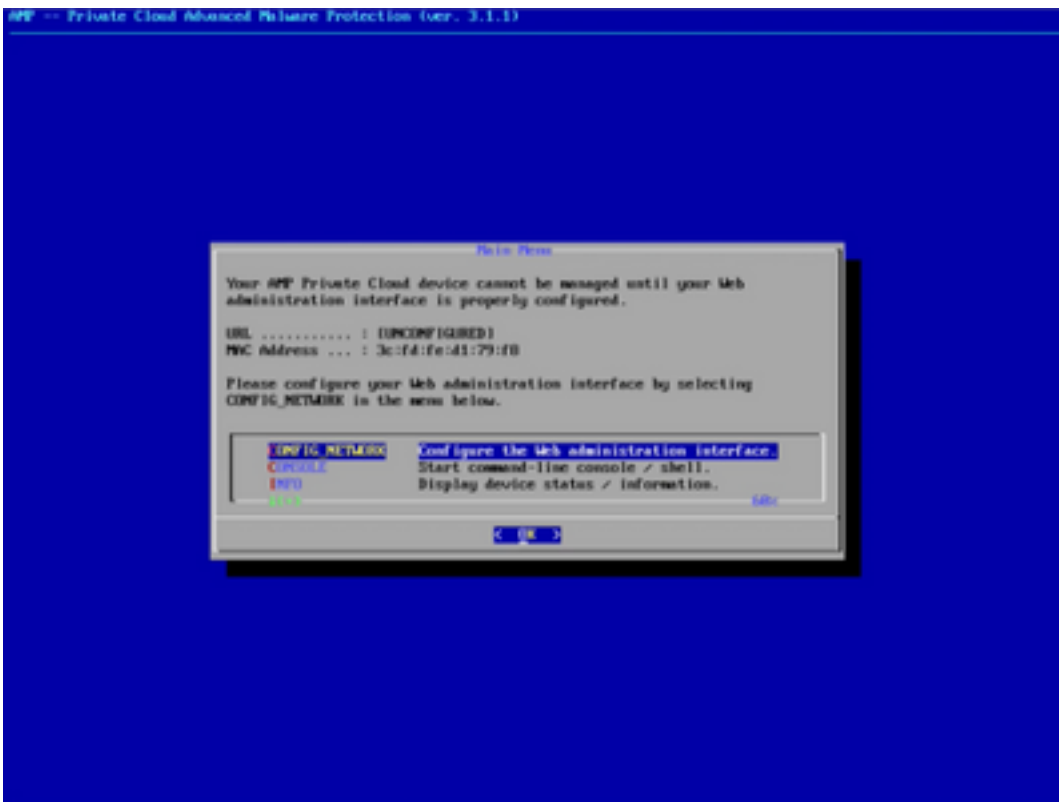


Step 5. Reimage starts and after reload you are presented with the initial menu.

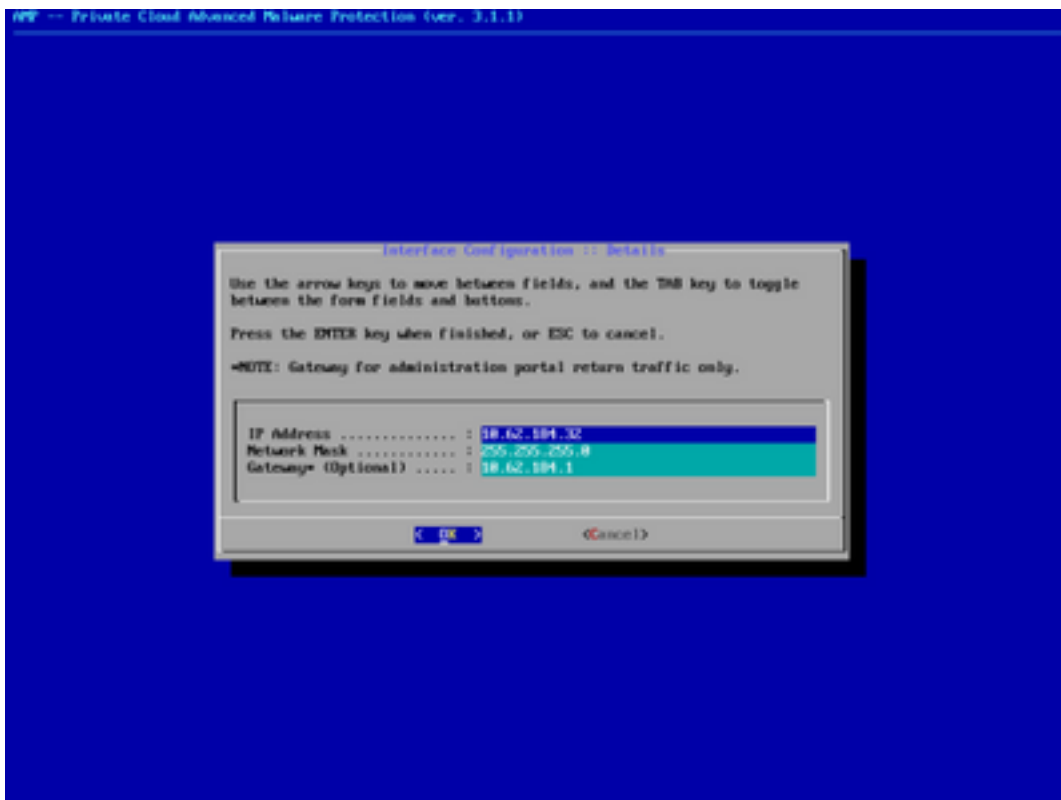
```

[ 11.717638] sdhci: registered new interface driver sdhci-omap
[ 11.744818] sdhci-omap: USB Serial support registered for omap
[ 11.753899] HSD2: PHY: No PS/2 controller found. Probing ports directly.
[ 11.793227] usb 1-6: new high-speed USB device number 2 using xhci_hcd
[ 12.103241] usb 1-6: New USB device found, idVendor=0a1b, idProduct=0400
[ 12.123183] usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 12.130536] usb 1-6: Product: Emulex F1004 HighSpeed HSB
[ 12.136513] usb 1-6: Manufacturer: Emulex Communications
[ 12.140912] usb 1-6: SerialNumber: 0x00000000
[ 12.146133] hub 1-6:1.0: USB hub found
[ 12.150658] hub 1-6:1.0: 7 ports detected
[ 12.267327] usb 1-7: new high-speed USB device number 3 using xhci_hcd
[ 12.275353] HSD2: Can't read CRB while initializing HSD2
[ 12.365623] HSD2: probe of HSD2 failed with error -5
[ 12.396905] omap_hwmod: PS/2 mouse device comes from all wires
[ 12.391040] rtc_omap 00:00: RTC can wake from S4
[ 12.396477] rtc_omap 00:00: rtc core: registered rtc_omap as rtc0
[ 12.398010] rtc_omap 00:00: alarm up to use month, yM, 114 bytes alarm, 16pt 1r
[ 12.325435] intel_pstate: Intel P-state driver initializing
[ 12.332253] intel_pstate: HWP enabled
[ 12.373288] cpuidle: using governor menu
[ 12.344827] EFI Variables Facility v0.00 2004-Aug-17
[ 12.338253] iuc: Refined TIC clocksource calibration: 2593.766 MHz
[ 12.391373] Switched to clocksource iuc
[ 12.401793] hidraw: raw HID events driver (C) Jiri Kosina...
[ 12.493674] usbhid: USB HID core driver
[ 12.431948] usb 1-7: New USB device found, idVendor=0914, idProduct=0578
[ 12.431962] usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
[ 12.431953] usb 1-7: Product: USB2.0 Hub
[ 12.433741] hub 1-7:1.0: USB hub found
[ 12.433942] hub 1-7:1.0: 4 ports detected
[ 12.445243] Detected 1 PCI Subspaces
[ 12.445433] Registering PCI driver as Mellanox controller
[ 12.451988] drop_monitor: Initializing network drop monitor service
[ 12.456753] TUN: tunix registered
[ 12.462953] Initializing RDM netlink socket
[ 12.466623] NET: Registered protocol family 18
[ 12.470676] NET: Registered protocol family 17
[ 12.470848] usb 1-6:1: new high-speed USB device number 4 using xhci_hcd
[ 12.481888] nfil_x_tables: NFIS OSH support
[ 12.471775] intel_rdt: Intel RDT RR allocation detected
[ 12.505676] microcode: sig=0x00054, pf=0x00, revision=0x200004d
[ 12.513488] microcode: Microcode Update Driver: v2.01 (13years@linux.ibm.com), Peter Oruba

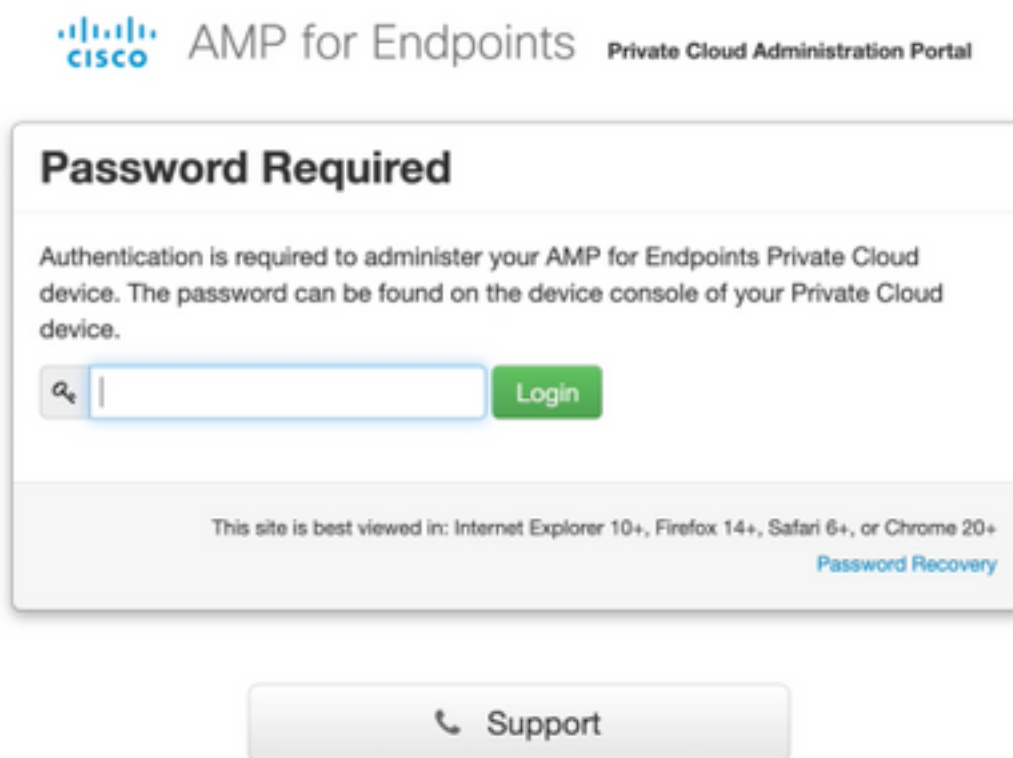
```



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



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



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

- 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 ✓
 - > Firewall Management Center ✓
- Other**
- > Review and Install
- [Start 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.

- + Adding mongo_event_consumer account.
 - + Running startup script to generate new password.
Generating a random password for mongo_event_consumer
 - + Removing the .rpmnew file
 - + Removing event_mongo_store service
 - + Adding firehose_cassandra account.
 - + Running startup script to generate new password.
Generating a random password for firehose_cassandra
 - Checking for bios and lmc updates. This may take some time.
- If an update is available and the update is successful, you will be asked to reboot the box.

Clean Installation

[Start >](#)

Restore

Local Remote **Upload**

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 >](#)

Restore

Local Remote **Upload**

Restore from a backup file present on the device. Files will be extracted to the directory your backup is located in during the restore process; for this reason, it is recommended that the file be located in the /data directory.

📁 /data/amp.bak

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



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 ✓
- > Finpower Management Center ✓

Other

- > Review and Install

Start Installation

Hardware Configuration

	Installed	Minimum Required
CPU Cores	48	8
Memory	1510 GB	128 GB

Next >



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 ✓
- > Firewall 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
▶ Pending	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/shai-8.20.0/lib/shai/plugins/ruby.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/network.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/plugins/powershell.rb
[2020-05-12T08:05:18+00:00] DEBUG: Loading plugin at /opt/chef/embedded/lib/ruby/gems/2.3.0/gems/shai-8.20.0/lib/shai/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 lsofd' 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.

The device is installing...

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

State	Started	Finished	Duration
✔ Successful	Tue May 12 2020 10:05:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 34 minutes, 19 seconds ago	Tue May 12 2020 10:22:17 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 17 minutes, 19 seconds ago	0 day, 0 hour, 16 minutes, 59 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2020-05-12T00:22:15+00:00] INFO: Skipping cleanup of resource table files and links
[2020-05-12T00:22:15+00:00] INFO: Running report handlers
[2020-05-12T00:22:15+00:00] INFO: Report handlers complete
[2020-05-12T00:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T00:22:15+00:00] DEBUG: Audit Reports are disabled, skipping sending reports.
[2020-05-12T00:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T00:22:15+00:00] DEBUG: Exiting
Sending system notification (this may take some time).
Running retryable command, 40 retries remaining.

=====
Chef run finished successfully
=====

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

Download Output

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.