重新映像AMP私有云PC3000并恢复备份

目录

简介

本文档介绍如何将高级恶意软件防护(AMP)私有云硬件设备重新映像到出厂状态，然后恢复备份。如果只想将设备恢复为出厂状态，请跳过步骤8并执行常规安装。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科AMP私有云PC3000
- 通过思科集成管理控制器(CIMC)进行基于内核的虚拟机(KVM)访问

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科AMP私有云PC3000 3.1.1
- 访问KVM控制台的Chrome浏览器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

步骤1.登录CIMC。打开KVM控制台。

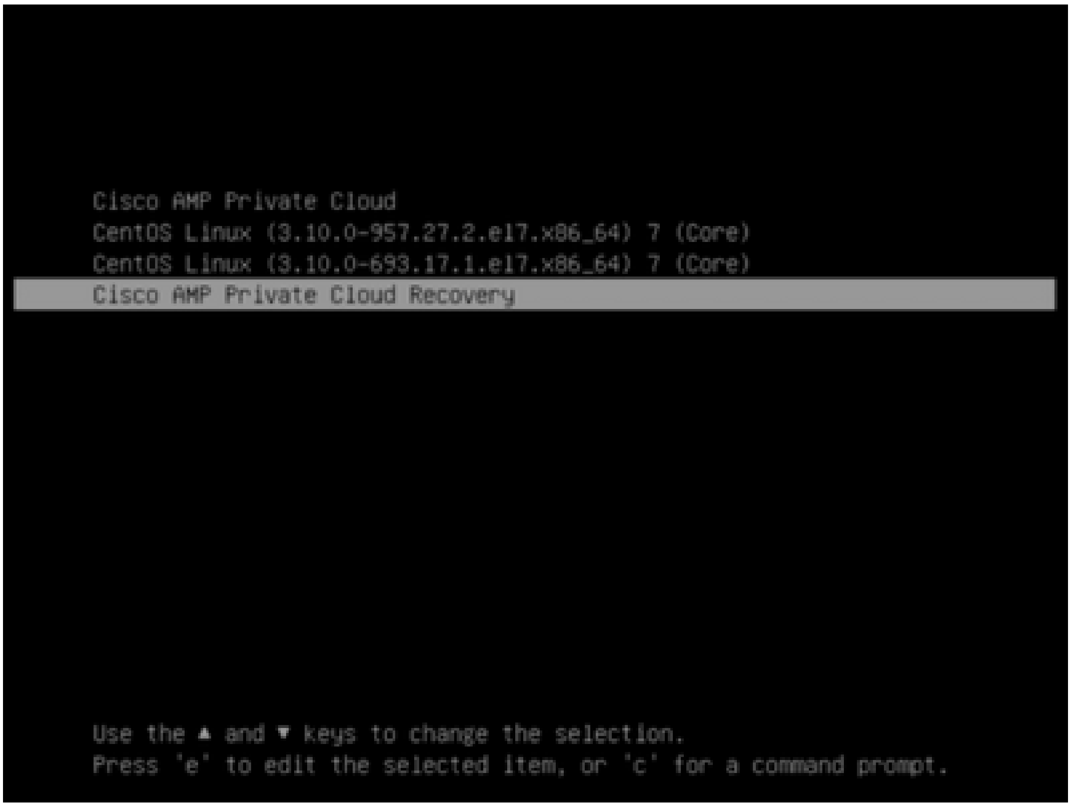
确保在浏览器中为该页面启用弹出窗口。

步骤2.重新加载设备。

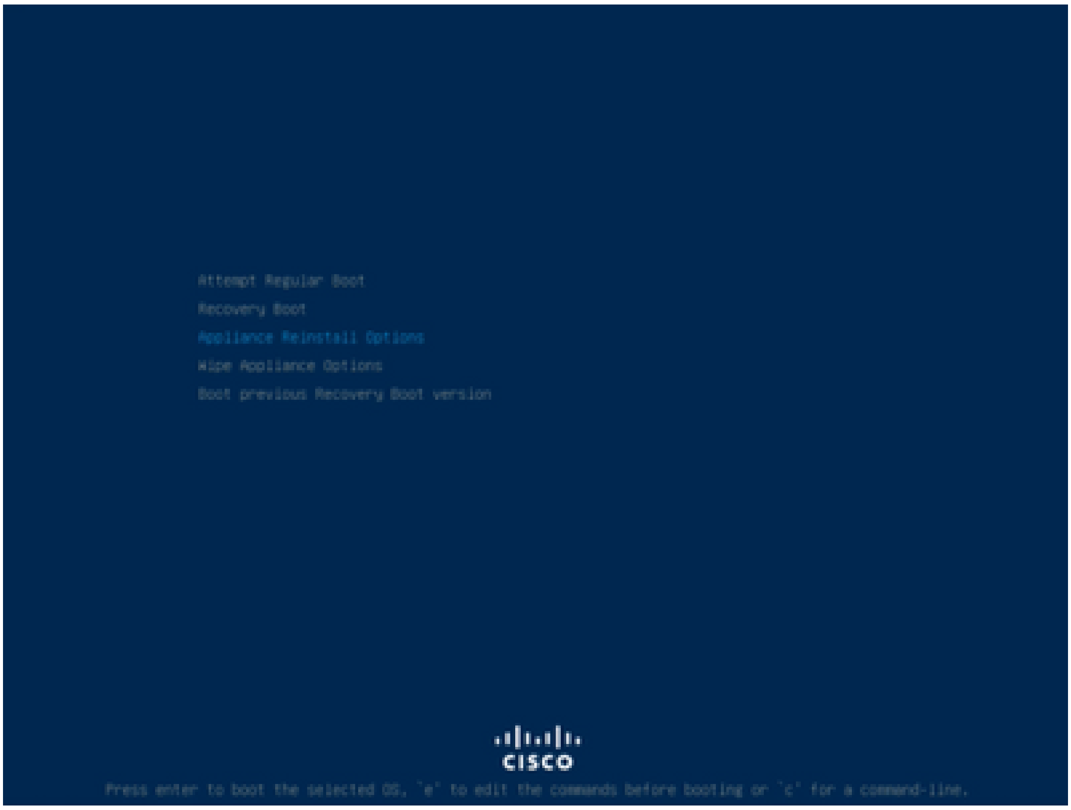
您可以通过管理员门户、安全外壳(SSH)或CIMC KVM重新启动设备。

步骤3.在基本输入输出系统(BIOS)加电自检(POST)完成后，GNU GR和Unified Bootloader(GRUB)菜单显示：

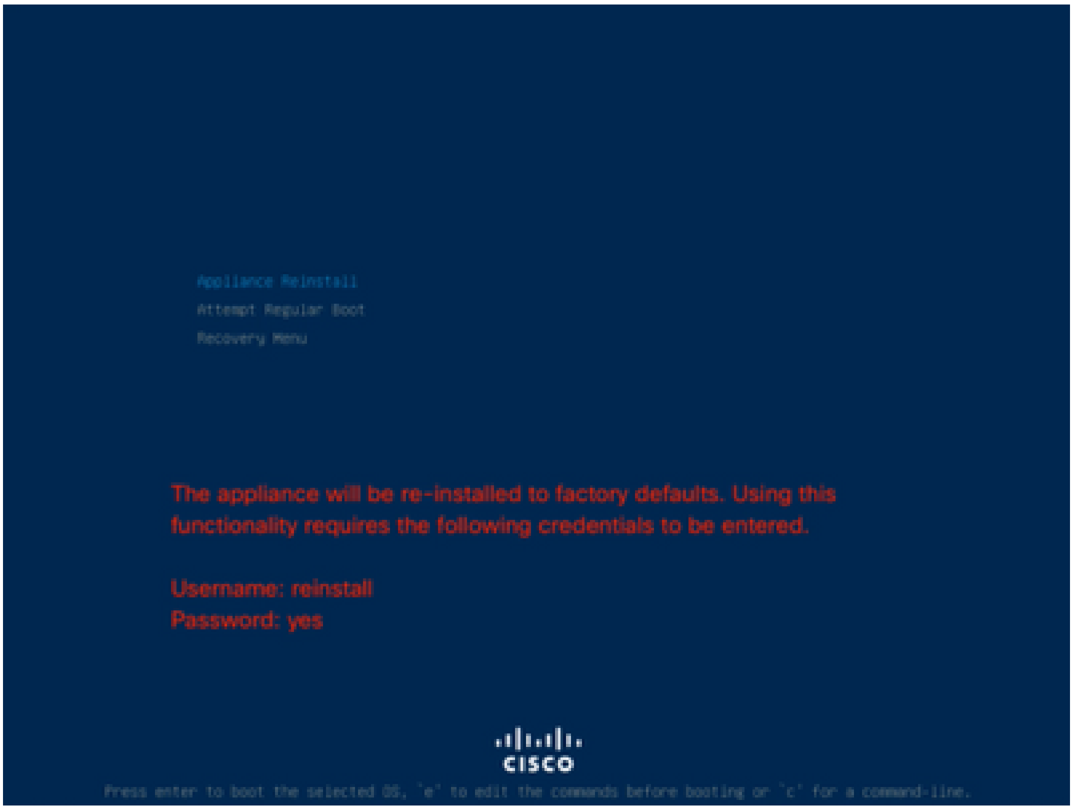
选择**Cisco AMP私有云恢复>设备重新安装选项>设备重新安装。**



```
Cisco AMP Private Cloud
CentOS Linux (3.10.0-957.27.2.el7.x86_64) 7 (Core)
CentOS Linux (3.10.0-693.17.1.el7.x86_64) 7 (Core)
Cisco AMP Private Cloud Recovery




Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```



```
Attempt Regular Boot
Recovery Boot
Appliance Reinstall Options
Wipe Appliance Options
Boot previous Recovery Boot version




Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
```



The appliance will be re-installed to factory defaults. Using this functionality requires the following credentials to be entered.

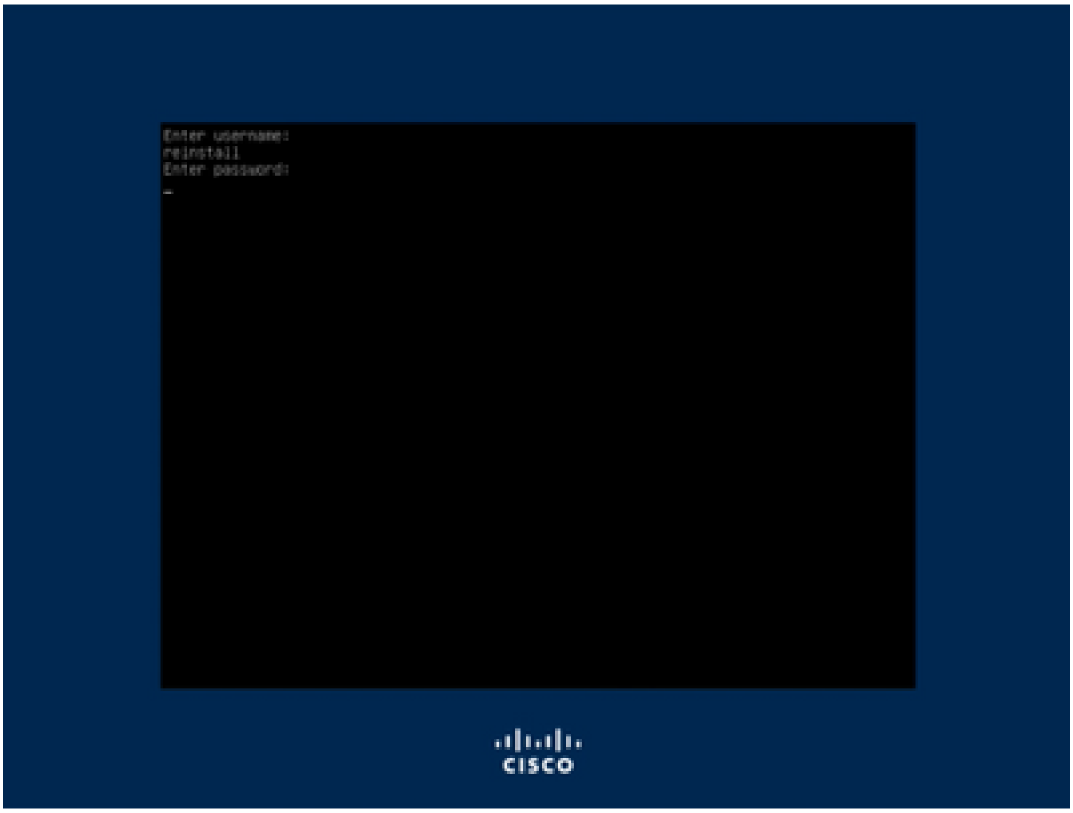
Username: reinstall
Password: yes

Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.

步骤4.输入用户名和密码。

username：**重新安装**

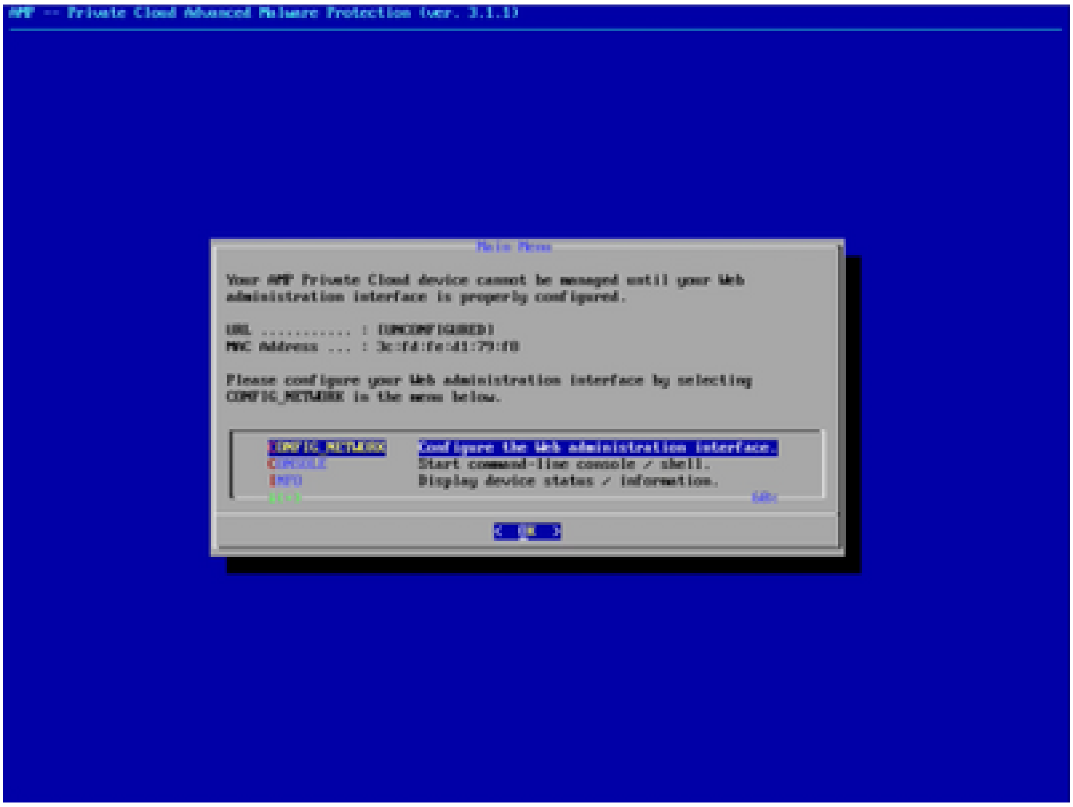
密码：**是**



```
Enter username:
reinstall
Enter password:
_
```

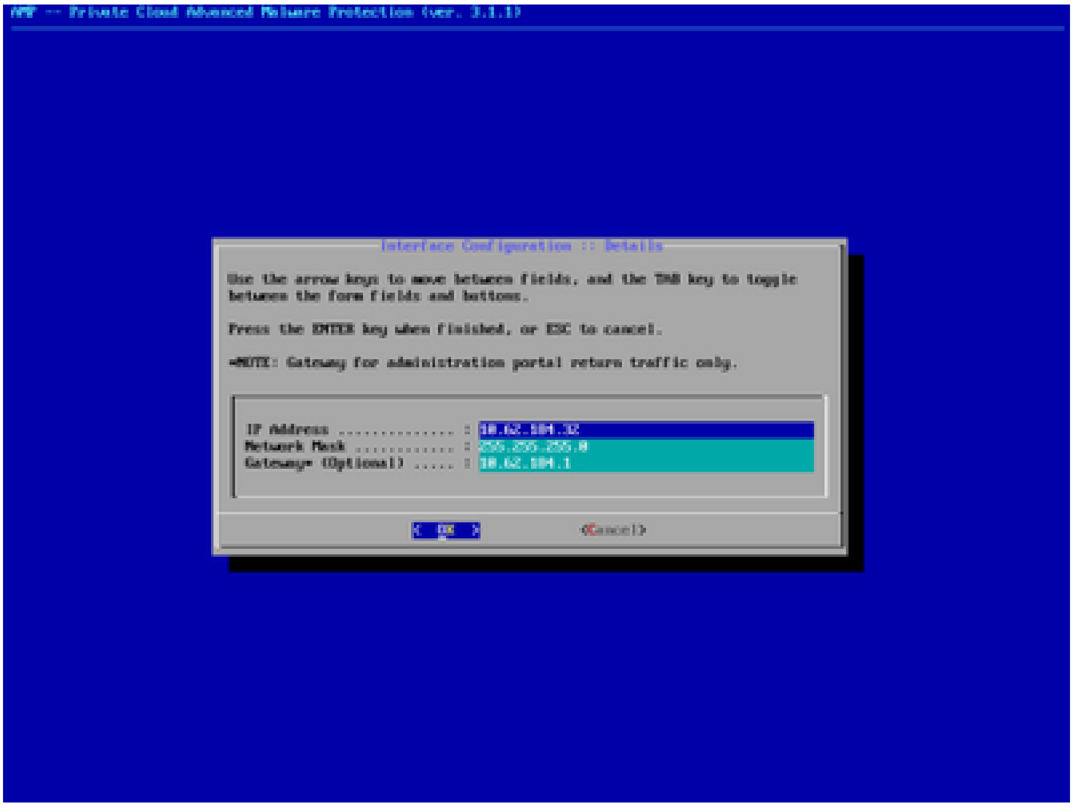
步骤5.重新映像启动后，系统会显示初始菜单。

```
[   11.737838] usbcore: registered new interface driver usbserial_generic
[   11.744818] usbserial: USB Serial support registered for generic
[   11.753899] i8042: PNP: No PS/2 controller found. Probing ports directly.
[   11.985287] usb 1-6: new high-speed USB device number 2 using xhci_hcd
[   12.118281] usb 1-6: New USB device found, idVendor=2a4b, idProduct=0400
[   12.123183] usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[   12.130530] usb 1-6: Product: Emulex Pilot4 HighSpeed HUB
[   12.136513] usb 1-6: Manufacturer: Emulex Communications
[   12.140912] usb 1-6: SerialNumber: 0xDADEFACE
[   12.146133] hub 1-6:1.0: USB hub found
[   12.150658] hub 1-6:1.0: 7 ports detected
[   12.267537] usb 1-7: new high-speed USB device number 3 using xhci_hcd
[   12.297535] i8042: Can't read CTR while initializing i8042
[   12.302622] i8042: probe of i8042 failed with error -5
[   12.306905] mousedev: PS/2 mouse device common for all mice
[   12.311284] rtc_cmos 00:00: RTC can wake from S4
[   12.316427] rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0
[   12.320810] rtc_cmos 00:00: alarms up to one month, y3k, 114 bytes nvram, hpet ir
[   12.325435] intel_pstate: Intel P-state driver initializing
[   12.332225] intel_pstate: HWP enabled
[   12.379208] cpuidle: using governor menu
[   12.344827] EFI Variables Facility v0.08 2004-May-17
[   12.378265] tsc: Refined TSC clocksource calibration: 2593.906 MHz
[   12.384193] Switched to clocksource tsc
[   12.405792] hidraw: raw HID events driver (C) Jiri Kosina
[   12.409874] usbhid: USB HID core driver
[   12.411948] usb 1-7: New USB device found, idVendor=04b4, idProduct=6570
[   12.411952] usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0
[   12.411955] usb 1-7: Product: USB2.0 Hub
[   12.413574] hub 1-7:1.0: USB hub found
[   12.413942] hub 1-7:1.0: 4 ports detected
[   12.441224] Detected 1 PCC Subspaces
[   12.445423] Registering PCC driver as Mailbox controller
[   12.451900] drop_monitor: Initializing network drop monitor service
[   12.456276] TCP: cubic registered
[   12.462456] Initializing XFRM netlink socket
[   12.466662] NET: Registered protocol family 10
[   12.472626] NET: Registered protocol family 17
[   12.472848] usb 1-6.1: new high-speed USB device number 4 using xhci_hcd
[   12.481500] mpls_gso: MPLS GSO support
[   12.491295] intel_rdt: Intel RDT L3 allocation detected
[   12.505676] microcode: sig=0x50654, pf=0x80, revision=0x200004d
[   12.513408] microcode: Microcode Update Driver: v2.01 <tigran@aivazian.fsnet.co.uk>, Peter Oruba
```



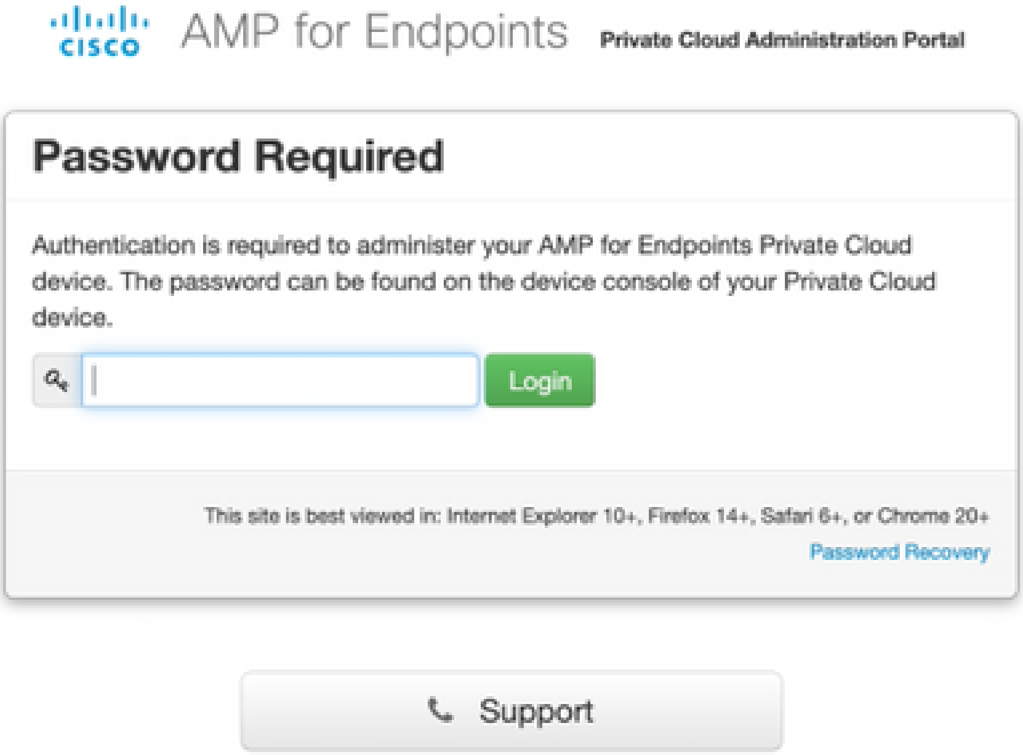
```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.1.1)

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

URL ............ : [UNCONFIGURED]
MAC Address ... : 3c:fd:fe:d1:79:f8

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.
    ↓(+)                                                    68%

                           < OK >
```

步骤6.在CONFIG_NETWORK子菜单中配置网络。



```
AMP -- Private Cloud Advanced Malware Protection (ver. 3.1.1)

              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 ............... : 10.62.104.32
  Network Mask ............. : 255.255.255.0
  Gateway* (Optional) ...... : 10.62.104.1

              <  OK  >            <Cancel>
```

步骤7.使用步骤5中的密码登录AMP OPadmin门户。



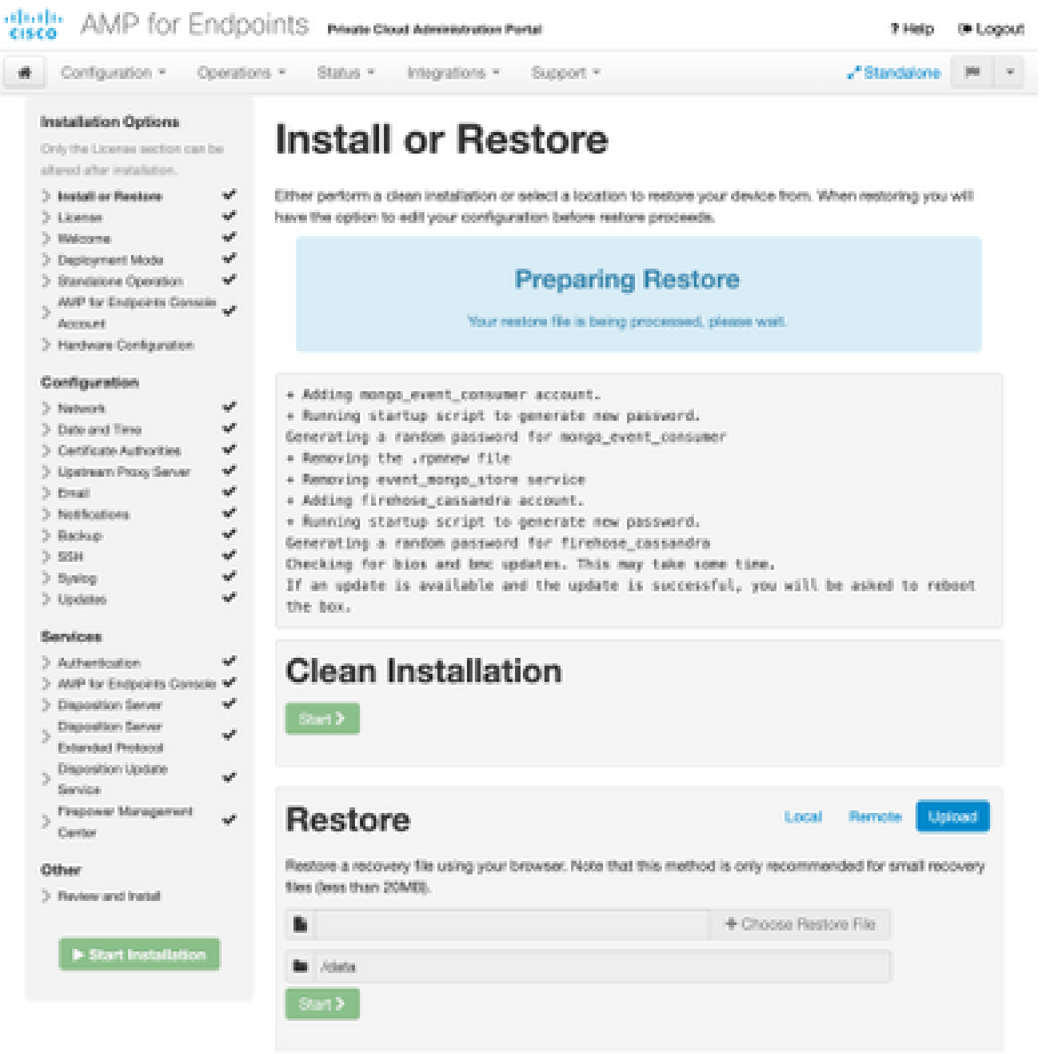
cisco
AMP for Endpoints
Private Cloud Administration Portal

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.

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

步骤8.使用SFTP或SCP将备份从远程服务器下载到/data/。



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.

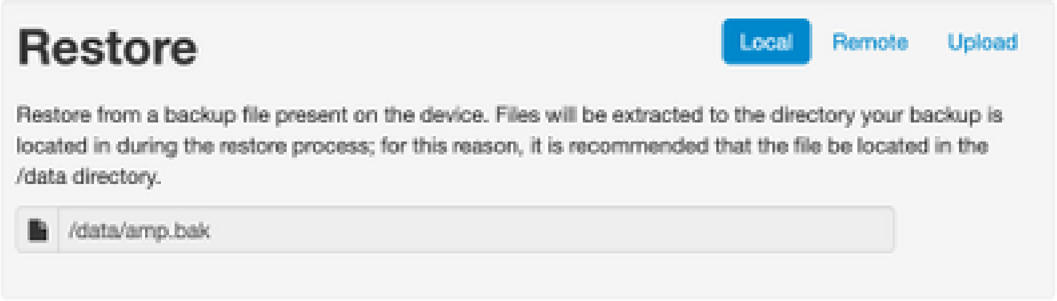
```
* Adding mongo_event_consumer account.
* Running startup script to generate new password.
Generating a random password for mongo_event_consumer
* Removing the .rpmnew file
* Removing event_mongo_store service
* Adding firehose_cassandra account.
* Running startup script to generate new password.
Generating a random password for firehose_cassandra
Checking for bios and bmc 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

Restore

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

/data

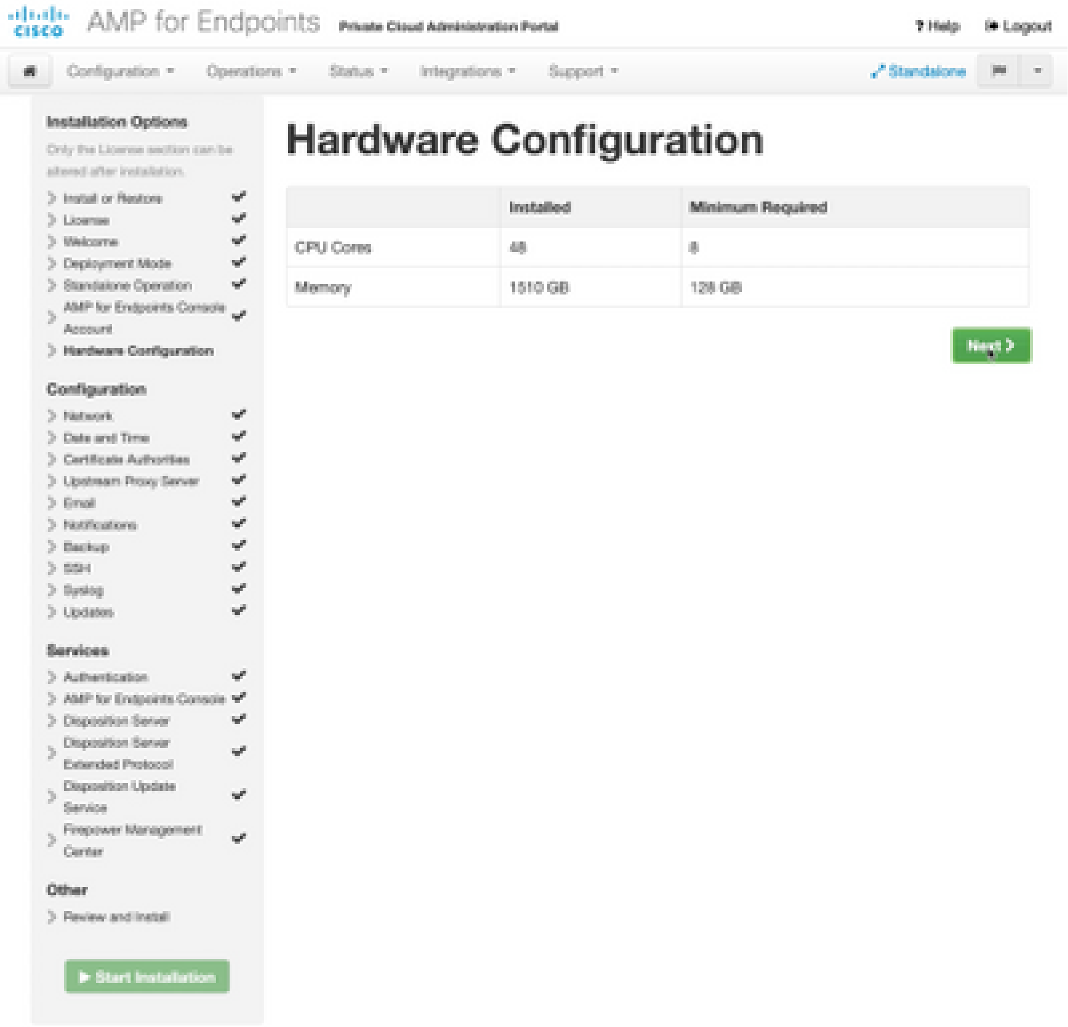


Restore

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

步骤9.确认硬件配置，单击“下一步**”>“开始安装**”。



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

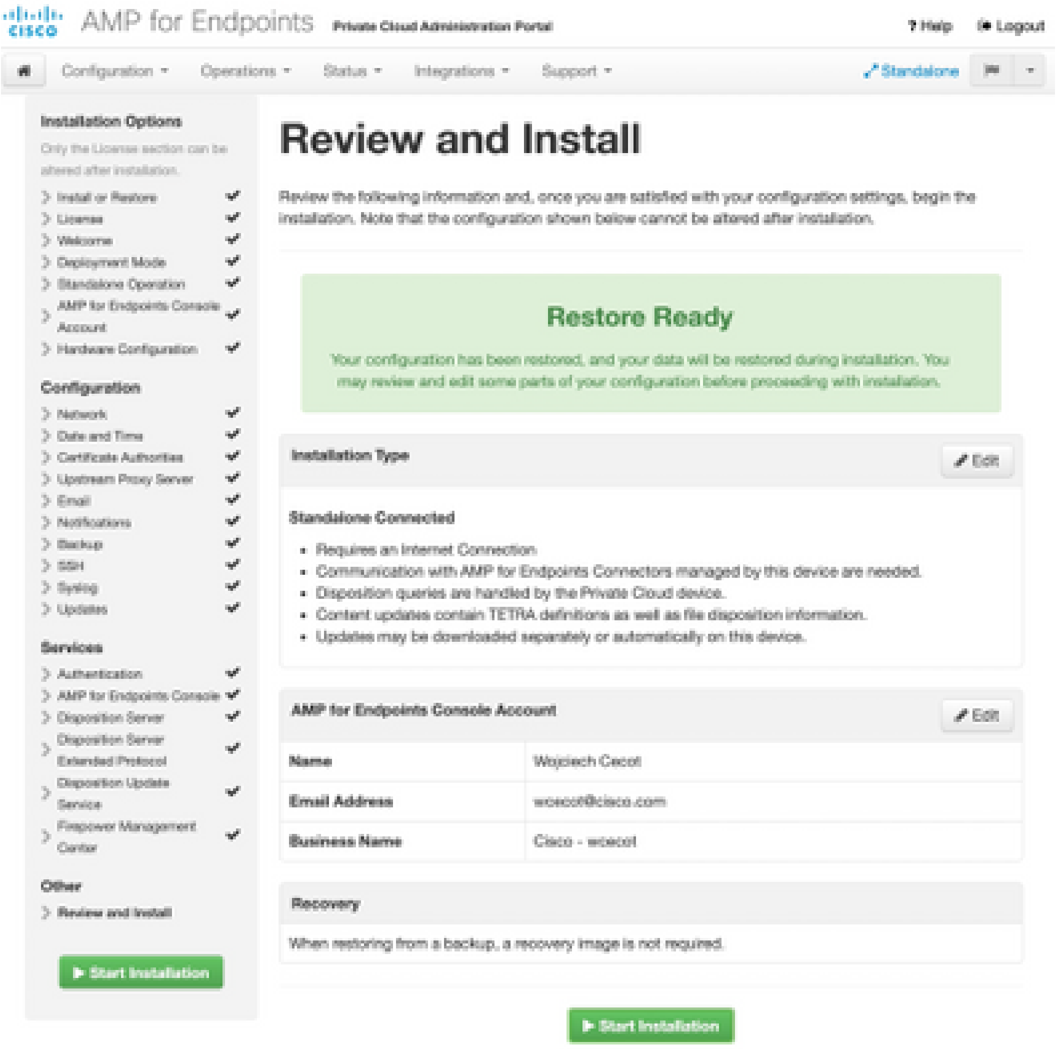
- Review and Install

Start Installation

Hardware Configuration

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

Next



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.

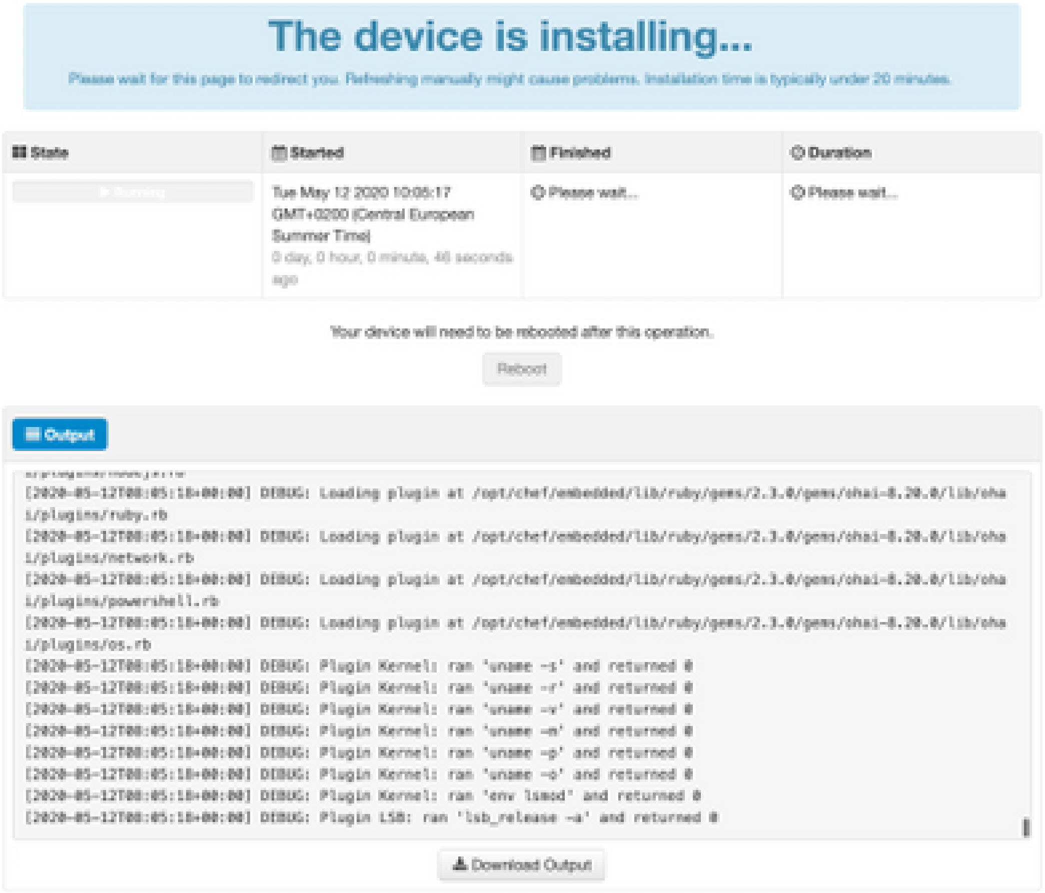
AMP for Endpoints Console Account ✎ Edit

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.

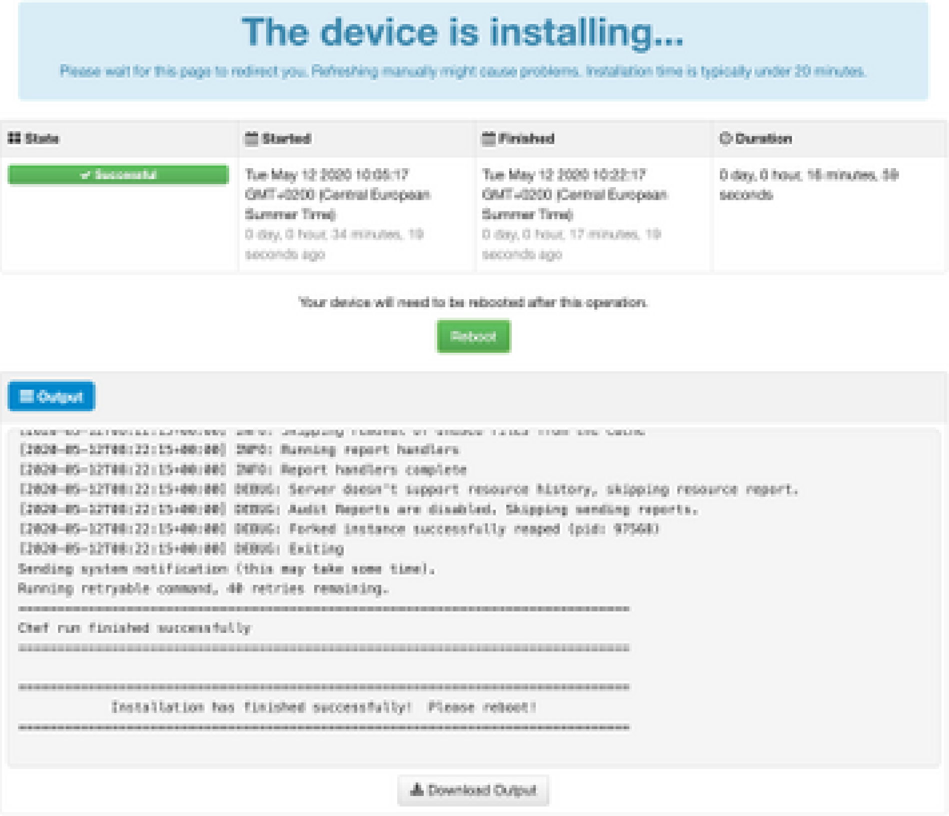
Reboot

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/oha
i/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/oha
i/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/oha
i/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/oha
i/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

步骤10.成功恢复后需要重新启动。



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.

```
[2020-05-12T08:22:15+00:00] INFO: Skipping removal of unused files from the cache
[2020-05-12T08:22:15+00:00] INFO: Running report handlers
[2020-05-12T08:22:15+00:00] INFO: Report handlers complete
[2020-05-12T08:22:15+00:00] DEBUG: Server doesn't support resource history, skipping resource report.
[2020-05-12T08:22:15+00:00] DEBUG: Audit Reports are disabled. Skipping sending reports.
[2020-05-12T08:22:15+00:00] DEBUG: Forked instance successfully reaped (pid: 97568)
[2020-05-12T08:22:15+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!
================================================================================
```

验证

重新启动设备后，检查两个门户是否工作正常。尝试在Web浏览器中打开OPadmin和控制台门户。访问两个门户需要几分钟。

故障排除

在备份还原过程中，OPadmin和控制台门户的密码与之前相同。否则，您需要使用在向导中设置的内容。