

# Fehlerbehebung und Neustrukturierung des AMP Private Cloud PC3000 und Wiederherstellen der Sicherung

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie die AMP-Hardware-Appliance (Advanced Malware Protection) für die Private Cloud auf den Werkzustand umgestellt und anschließend die Sicherung wiederhergestellt wird. Wenn Sie die Einheit auf den Werkzustand zurücksetzen möchten, überspringen Sie Schritt 8 und folgen Sie der normalen Installation.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco AMP Private Cloud PC3000
- Kernel-basierter KVM-Zugriff über Cisco Integrated Management Controller (CIMC)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco AMP Private Cloud PC3000 3.1.1
- Chrome-Browser für den Zugriff auf die KVM-Konsole

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfigurieren

Schritt 1: Melden Sie sich beim CIMC an. Öffnen Sie die KVM-Konsole.

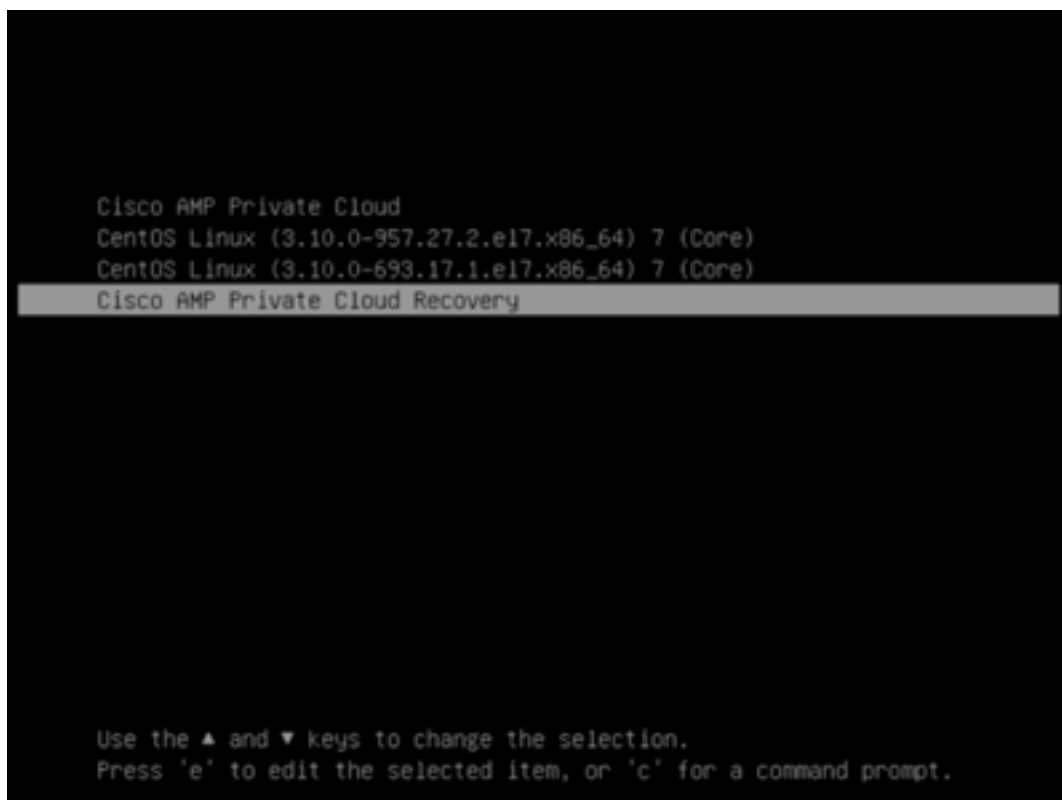
Stellen Sie sicher, dass Popups für diese Seite im Browser aktiviert sind.

Schritt 2: Laden Sie die Appliance neu.

Sie können die Einheit entweder über das Admin-Portal, Secure Shell (SSH) oder CIMC KVM neu starten.

Schritt 3: Nach Abschluss des Power-On Self-Tests (POST) des Basic Input Output System (BIOS) werden im Menü GNU GR und Unified Bootloader (GRUB) Folgendes angezeigt:

Wählen Sie **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



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

Appliance Reinstall  
Attempt Regular Boot  
Recovery Menu

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.

Schritt 4: Geben Sie Benutzername und Kennwort ein.

Benutzername: neu installieren

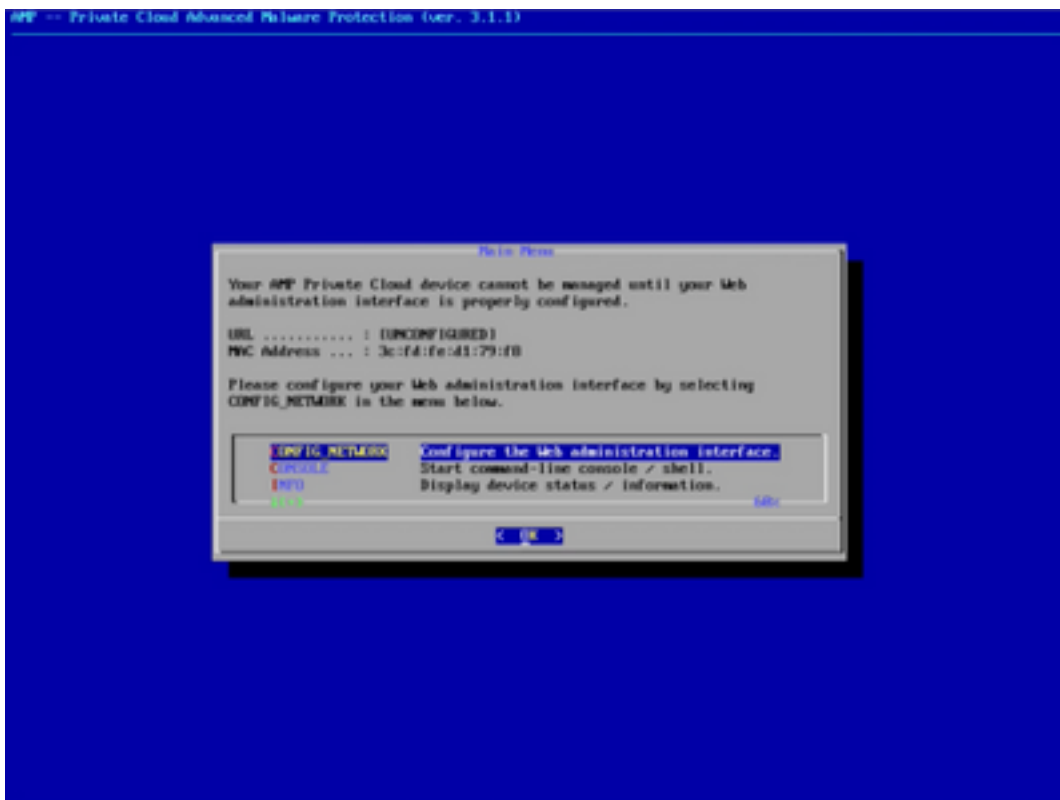
Kennwort: ja

```
Enter username:  
reinstall  
Enter password:  
-
```

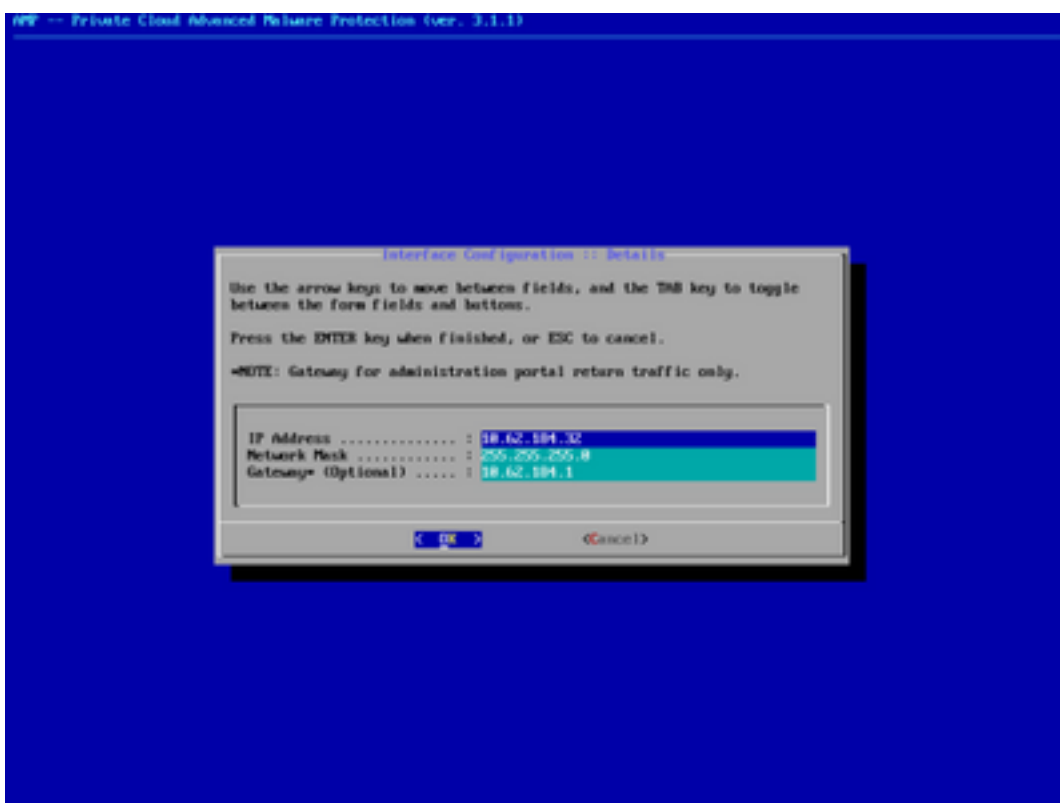


Schritt 5: Das neue Image wird gestartet, und nach dem erneuten Laden wird das Startmenü angezeigt.

```
 | 11.779380| usbcore: registered new interface driver usbserial_generic  
 | 11.749180| usbserial: USB Serial support registered for generic  
 | 11.753899| USB: FW: No USB2 controller found. Probing ports directly.  
 | 11.793227| usb 1-6: new high-speed USB device number 2 using ohci_hcd  
 | 12.182811| usb 1-6: New USB device found, idVendor=0a1b, idProduct=0400  
 | 12.123810| usb 1-6: New USB device strings: Mfr=1, Product=2, SerialNumber=3  
 | 12.1305380| usb 1-6: Product: Emulex Fibre4 HighSpeed HB  
 | 12.1305330| usb 1-6: Manufacturer: Emulex Communications  
 | 12.1409123| usb 1-6: SerialNumber: 8d9882f9ce  
 | 12.1461333| hub 1-6:1.0: USB hub found  
 | 12.1506580| hub 1-6:1.0: 7 ports detected  
 | 12.2675373| usb 1-7: new high-speed USB device number 3 using ohci_hcd  
 | 12.2705363| USB: Can't read CTR while initializing 80942  
 | 12.3026223| USB: probe of 80942 failed with error -5  
 | 12.3869953| usbcore: FS-C mass device common for all w/ot  
 | 12.3813883| rtc_cmos 00:00: RTC can wake from S4  
 | 12.3284273| rtc_cmos 00:00: rtc core: registered rtc_cmos as rtc0  
 | 12.3284180| rtc_cmos 00:00: alarms up to one month, y1k, 114 bytes nrwsk, 1ppm irq  
 | 12.3254253| intel_pstate: intel P-state driver initializing  
 | 12.3322253| intel_pstate: HWP enabled  
 | 12.3732880| cpuidle: using governor menu  
 | 12.3448273| EFI Variables Facility v0.00 2009-Sep-17  
 | 12.3782853| tsc: refined TSC clocksource calibration: 2593.766 MHz  
 | 12.3841930| Switched to clocksource tsc  
 | 12.4057920| hidraw: *usb,virtio,virtio-blank,OC) J161 Device...  
 | 12.4996243| usbhid: USB HID core driver  
 | 12.4319480| usb 1-7: New USB device found, idVendor=0418, idProduct=5578  
 | 12.4319523| usb 1-7: New USB device strings: Mfr=0, Product=1, SerialNumber=0  
 | 12.4319553| usb 1-7: Product: USB2.0 Hub  
 | 12.4320443| hub 1-7:1.0: USB hub found  
 | 12.4329423| hub 1-7:1.0: 4 ports detected  
 | 12.4452243| Detected 1 PCC Subspaces  
 | 12.4454230| Registering PCC driver as Mailbox controller  
 | 12.4519880| drop_monitor: Initializing network drop monitor service  
 | 12.4562793| TUN: tunlt registered  
 | 12.4624583| Initializing IPVS netlink socket  
 | 12.4666623| NET: Registered protocol family 18  
 | 12.4728623| NET: Registered protocol family 17  
 | 12.4729480| usb 1-8:1: new high-speed USB device number 4 using ohci_hcd  
 | 12.4818880| nfs_gss: RTLS GSS support  
 | 12.4737753| intel_rdt: Intel RDT MM allocation detected  
 | 12.5056263| sdcmcode: s1p-0x50054, pf-0x00, revision-0x2000044  
 | 12.5134880| sdcmcode: M100000 Update Driver: v2.01 (Copyright 2010-2011, Peter Grech)
```



Schritt 6: Konfigurieren Sie das Netzwerk im Untermenü CONFIG\_NETWORK.



Schritt 7: Melden Sie sich mit einem Kennwort aus Schritt 5 beim AMP OPadmin-Portal an.



## 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.

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

[Password Recovery](#)

Support

Schritt 8: Laden Sie mit SFTP oder SCP eine Sicherung vom Remote-Server auf /data/ herunter.



### Installation Options

Only the Licenses section can be altered after installation.

- Install or Restore ✓
- Licenses ✓
- 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 ✓
- Preprocessor 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

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

Schritt 9: Hardwarekonfiguration bestätigen, auf **Weiter > Installation starten** klicken.

CISCO AMP for Endpoints Private Cloud Administration Portal Help Logout

Configuration Operations Status Integrations Support Standalone

## Hardware Configuration

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

Next >

Start Installation

- Installation Options
  - 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 ✓
  - Synlog ✓
  - Updates ✓
- Services
  - Authentication ✓
  - AMP for Endpoints Console ✓
  - Disposition Server ✓
  - Disposition Server ✓
  - Extended Protocol ✓
  - Disposition Update ✓
  - Service ✓
  - Firepower Management Center ✓
- Other
  - Review and Install



## 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 lscod' and returned 0
[2020-05-12T08:05:18+00:00] DEBUG: Plugin LSB: ran 'lsb_release -a' and returned 0

```

Download Output



Schritt 10: Nach erfolgreicher Wiederherstellung ist ein Neustart erforderlich.

### 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](#)

## Überprüfung

Überprüfen Sie nach dem Neustart der Appliance, ob beide Portale einwandfrei funktionieren. Versuchen Sie, das OAdmin- und Konsolenportal im Webbrowser zu öffnen. Der Zugriff auf beide Portale dauert nur wenige Minuten.

## Fehlerbehebung

Im Falle eines Backup-Wiederherstellungsprozesses sind das Kennwort für die OAdmin- und Konsolenportale das gleiche wie zuvor. Andernfalls müssen Sie die im Assistenten festgelegten Einstellungen verwenden.