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

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die AMP-Hardware-Appliance (Advanced Malware Protection) für die Private Cloud auf den Werkszustand umgestellt und anschließend die Sicherung wiederhergestellt wird. Wenn Sie die Einheit auf den Werkszustand 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.

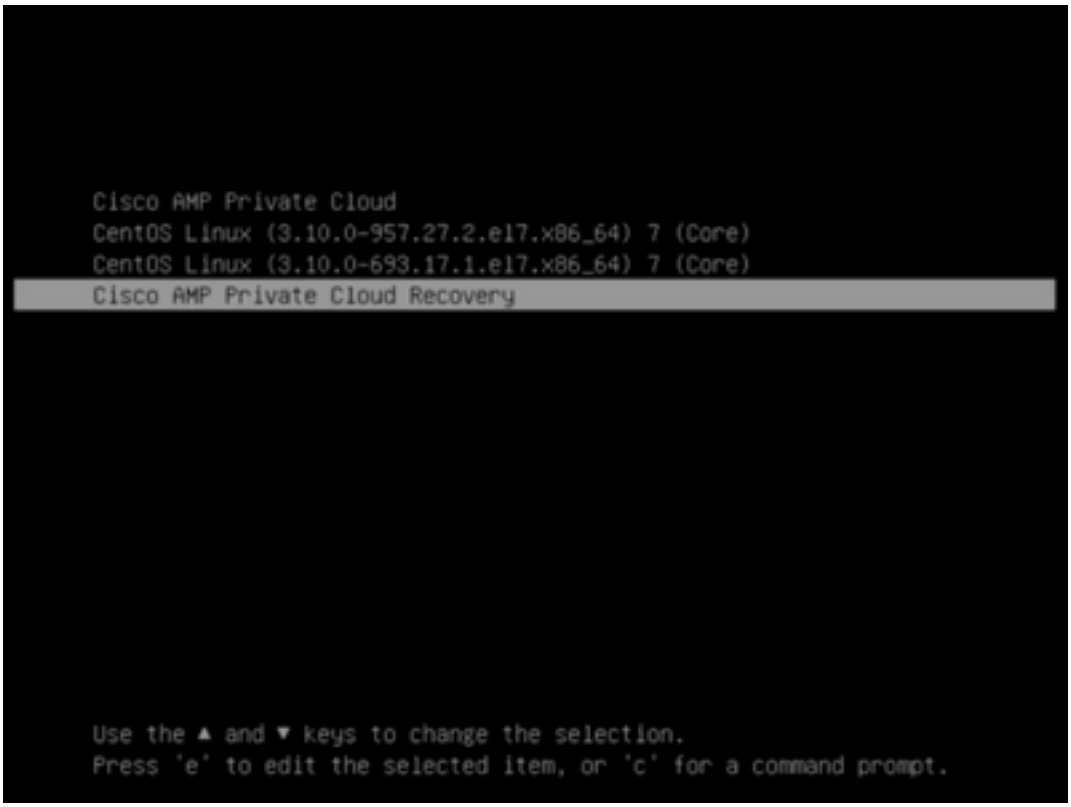
Stellen Sie sicher, dass Popups für diese Seite im Browser aktiviert sind.

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**.

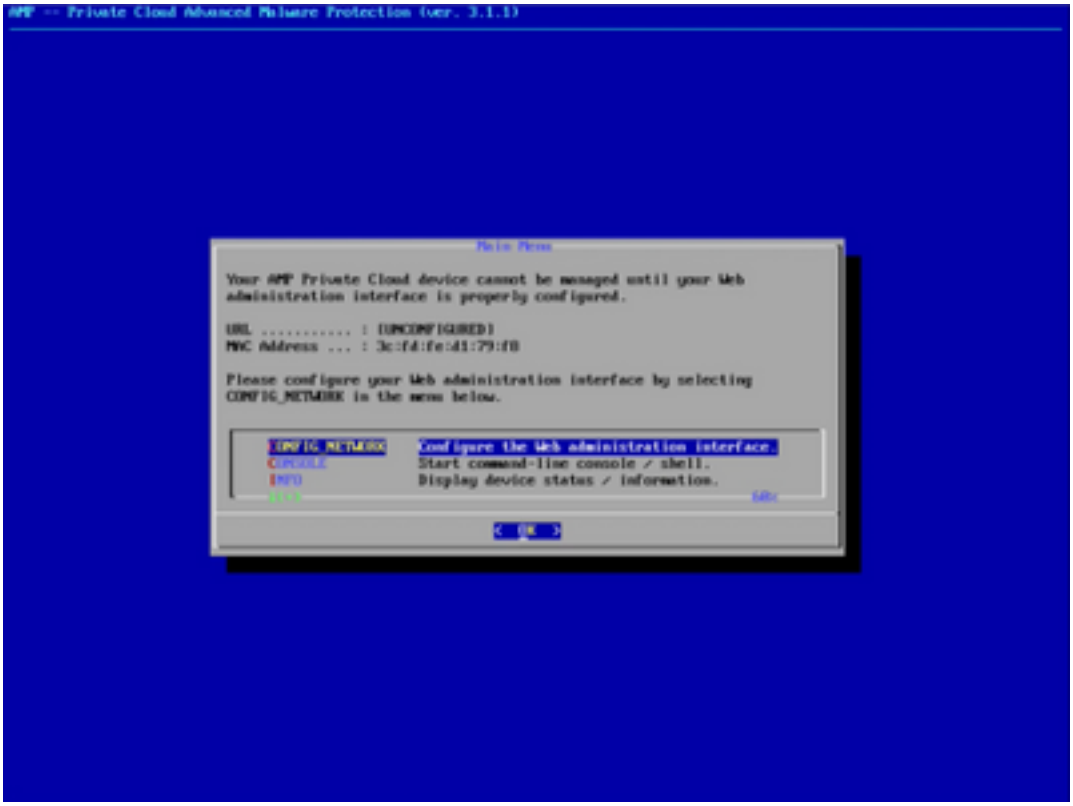


Schritt 4: Geben Sie Benutzername und Kennwort ein.

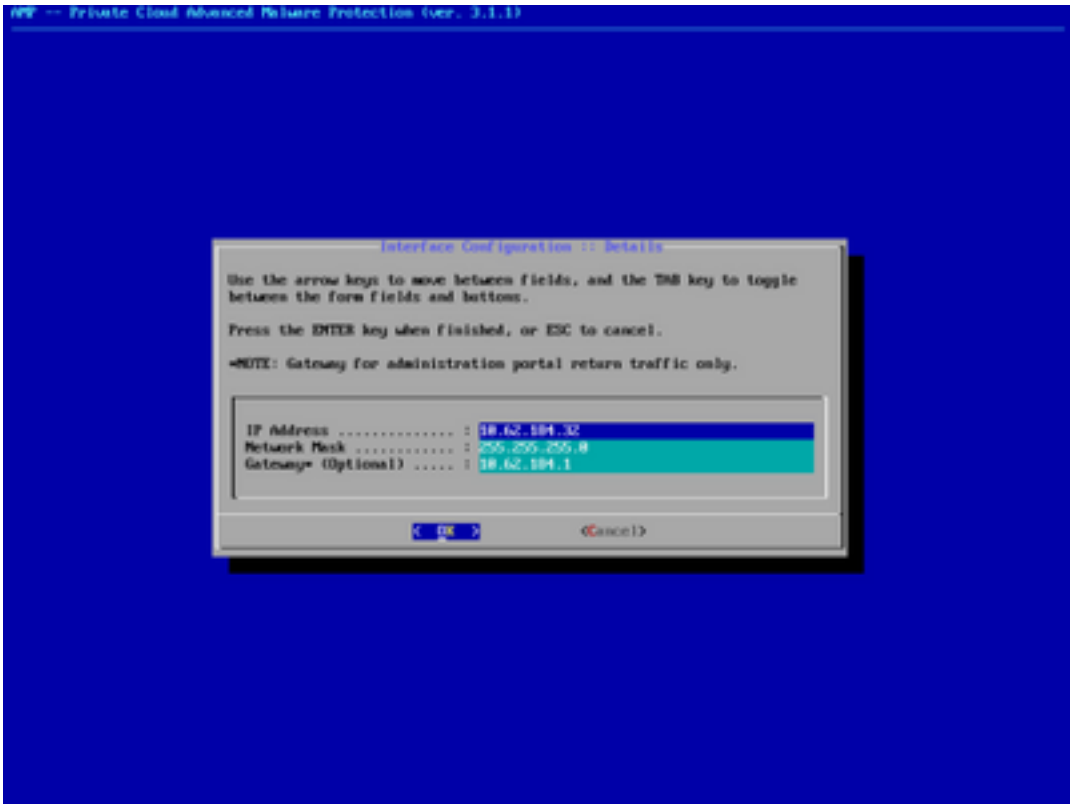
Benutzername: **neu installieren**

Kennwort: **ja**

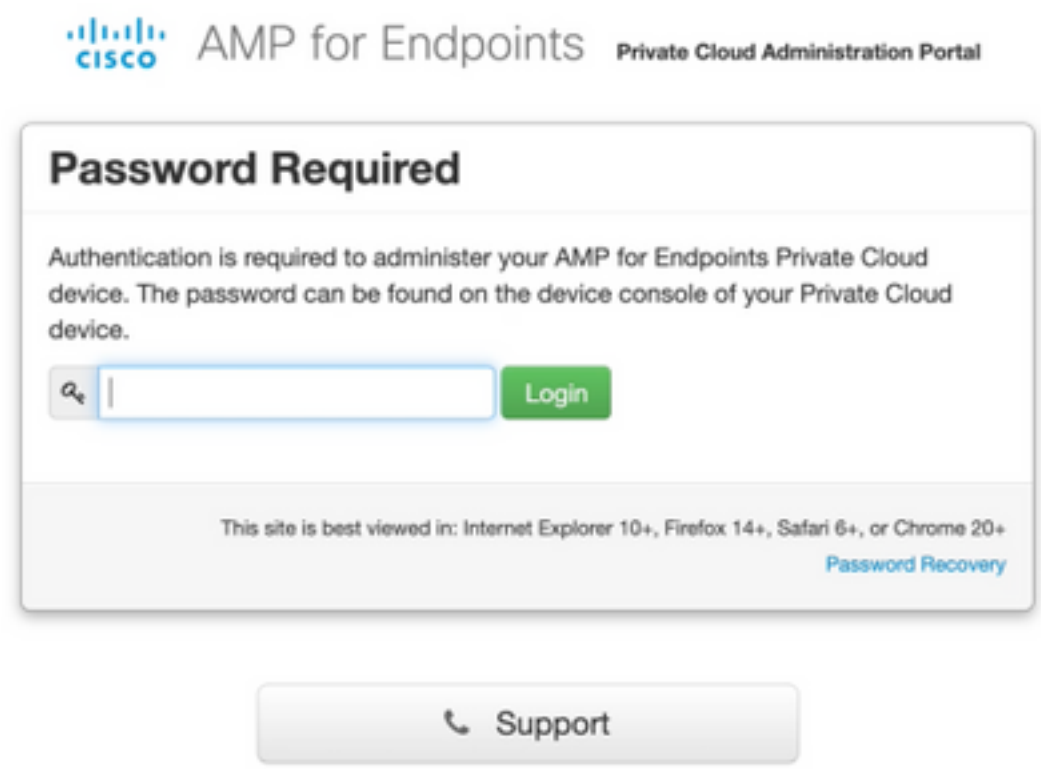
Schritt 5: Das neue Image wird gestartet, und nach dem erneuten Laden wird das Startmenü angezeigt.



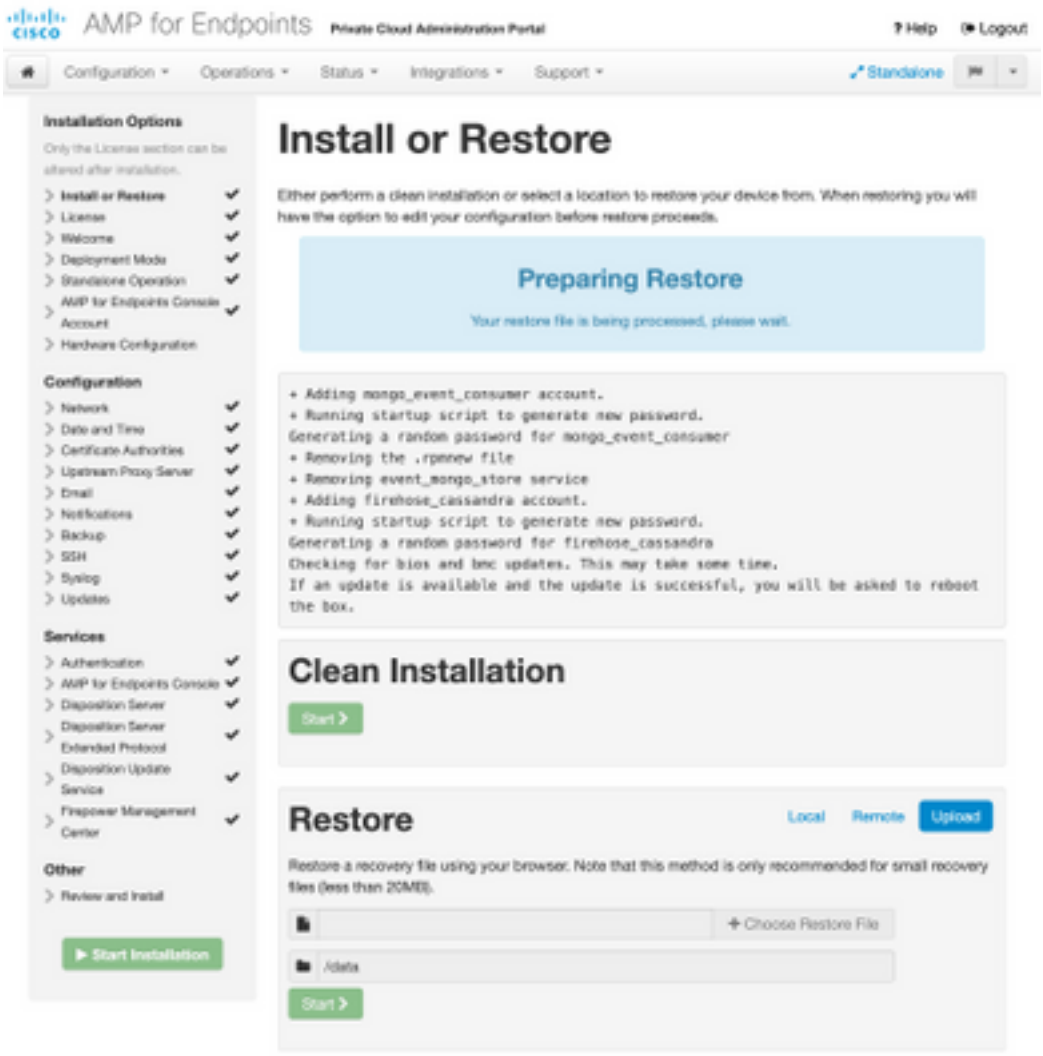
Schritt 6: Konfigurieren Sie das Netzwerk im Untermenü CONFIG_NETWORK.



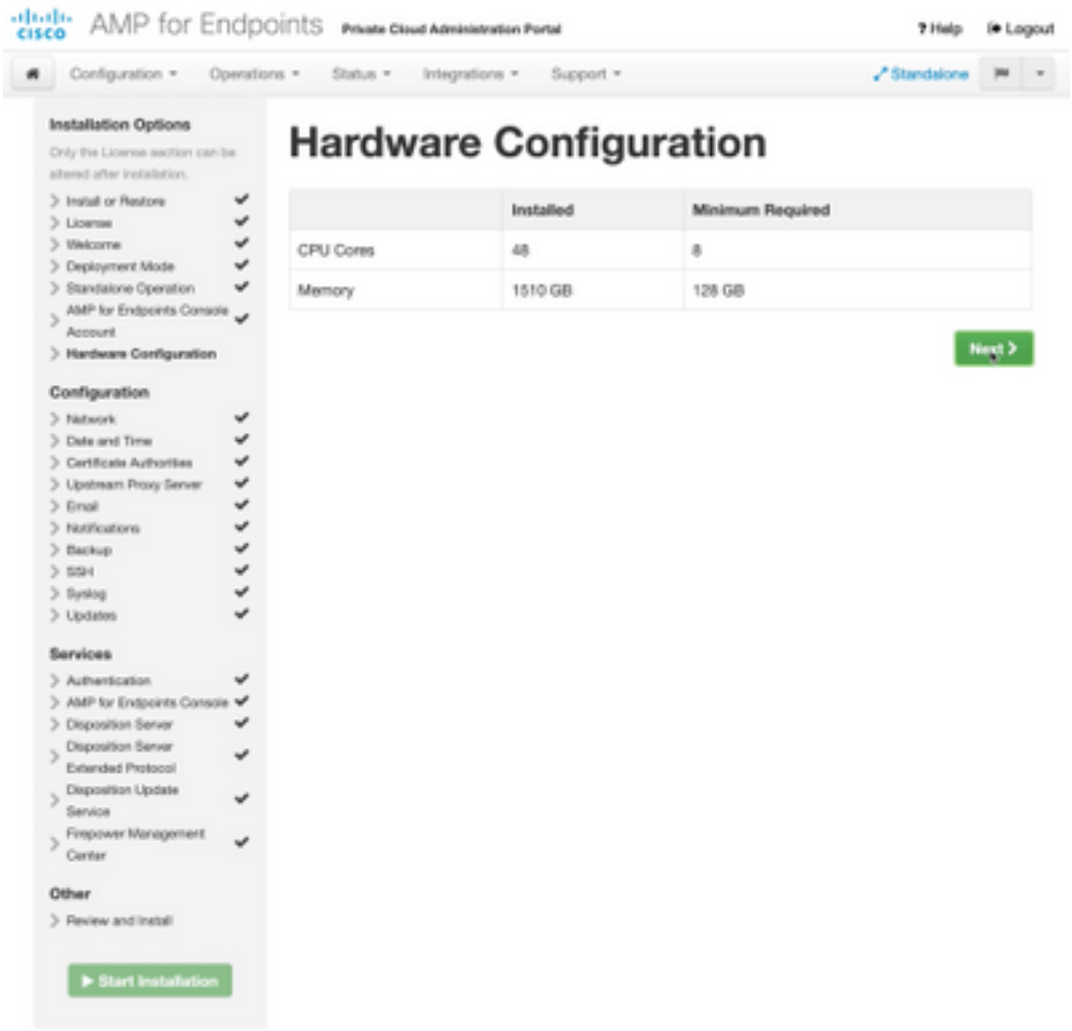
Schritt 7: Melden Sie sich mit einem Kennwort aus Schritt 5 beim AMP OPadmin-Portal an.

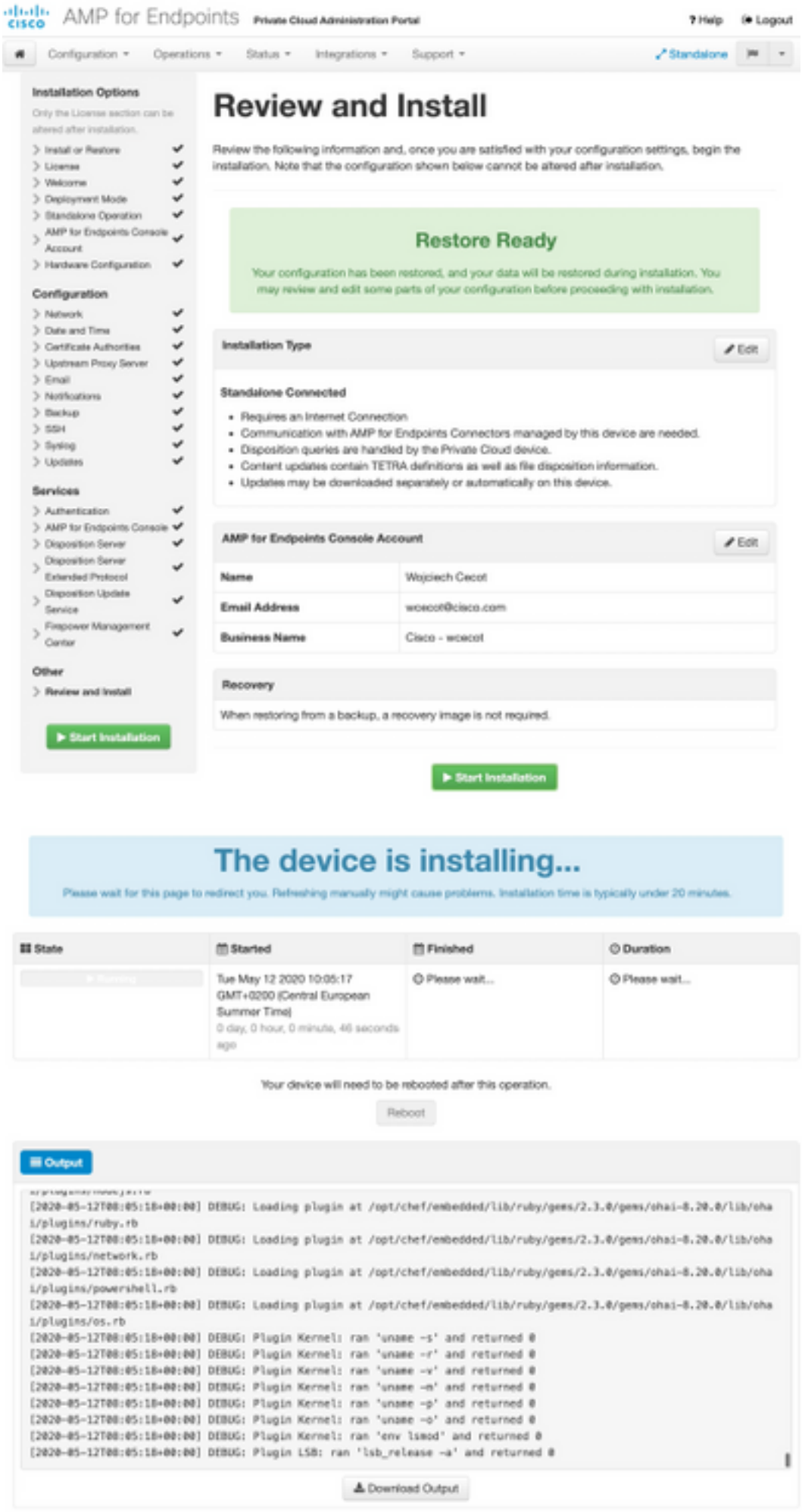


Schritt 8: Laden Sie mit SFTP oder SCP eine Sicherung vom Remote-Server auf /data/ herunter.

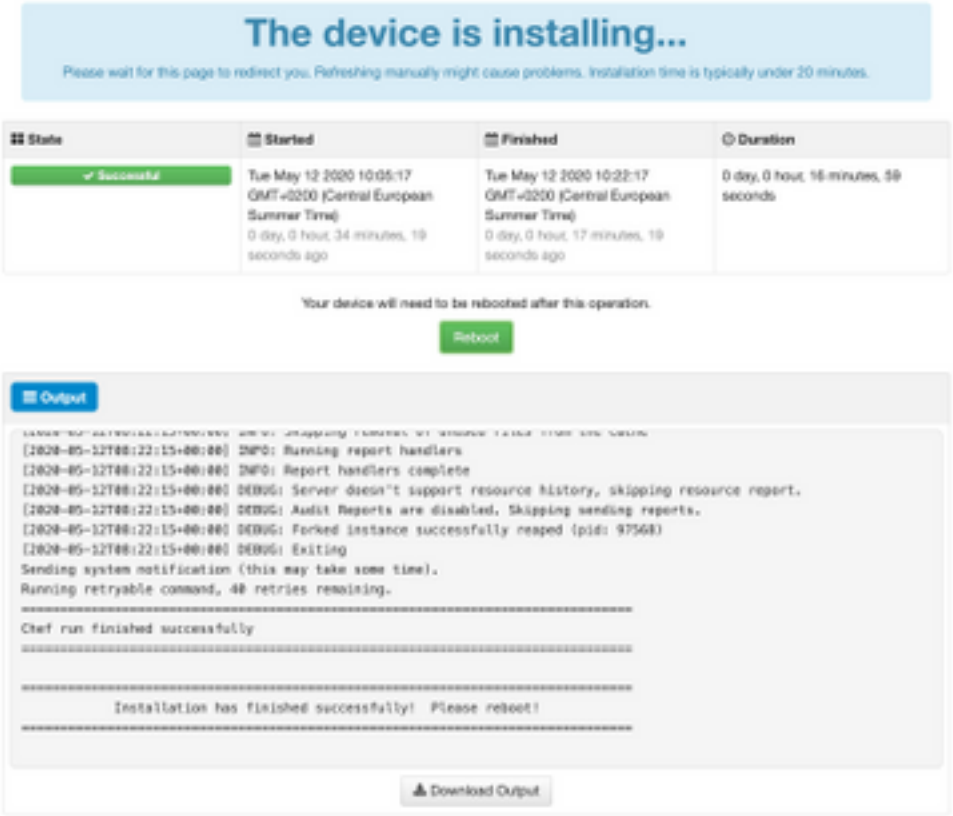


Schritt 9: Hardwarekonfiguration bestätigen, auf **Weiter > Installation starten** klicken.




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

Schritt 10: Nach erfolgreicher Wiederherstellung ist ein Neustart erforderlich.



Überprüfung

Überprüfen Sie nach dem Neustart der Appliance, ob beide Portale einwandfrei funktionieren. Versuchen Sie, das OPadmin- 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 OPadmin- und Konsolenportale das gleiche wie zuvor. Andernfalls müssen Sie die im Assistenten festgelegten Einstellungen verwenden.