Vuelva a crear la imagen de AMP Private Cloud PC3000 y restaure la copia de seguridad

Contenido

Introducción

Este documento describe cómo recrear la imagen del dispositivo de hardware de protección frente a malware avanzado (AMP) de la nube privada en el estado de fábrica y, a continuación, restaurar la copia de seguridad. Si sólo desea volver al estado de fábrica del dispositivo, omita el paso 8 y siga la instalación normal.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- PC3000 de nube privada de Cisco AMP
- Acceso de máquina virtual (KVM) basado en el núcleo a través de Cisco Integrated Management Controller (CIMC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco AMP para PC3000 3.1.1
- Navegador cromado para acceder a la consola KVM

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Paso 1. Inicie sesión en CIMC. Abra la consola KVM.

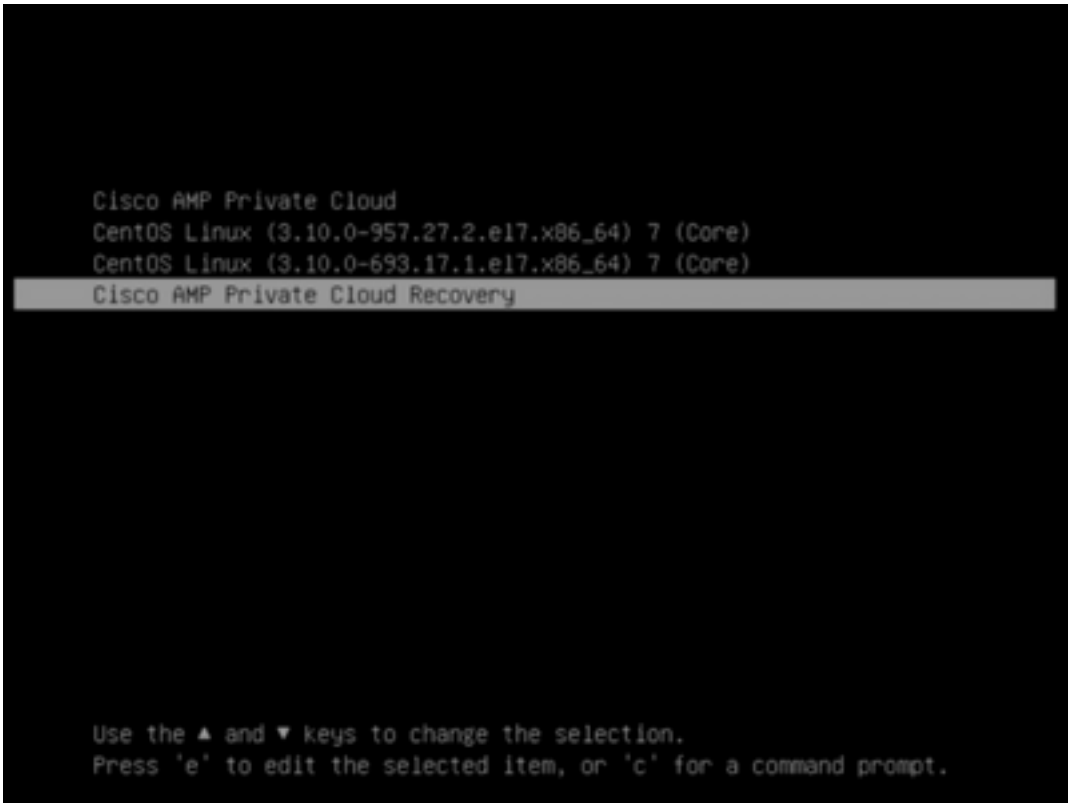
Asegúrese de que las ventanas emergentes están habilitadas para esa página en el explorador.

Paso 2. Recargue el dispositivo.

Puede reiniciar el dispositivo mediante el portal de administración, Secure Shell (SSH) o CIMC KVM.

Paso 3. Una vez finalizada la prueba automática de encendido (POST) del sistema de salida de entrada básico (BIOS), aparece el menú GRy cargador de arranque unificado (GRUB) de GNU:

Seleccione **Cisco AMP Private Cloud Recovery > Appliance Reinstall Options > Appliance Reinstall**.

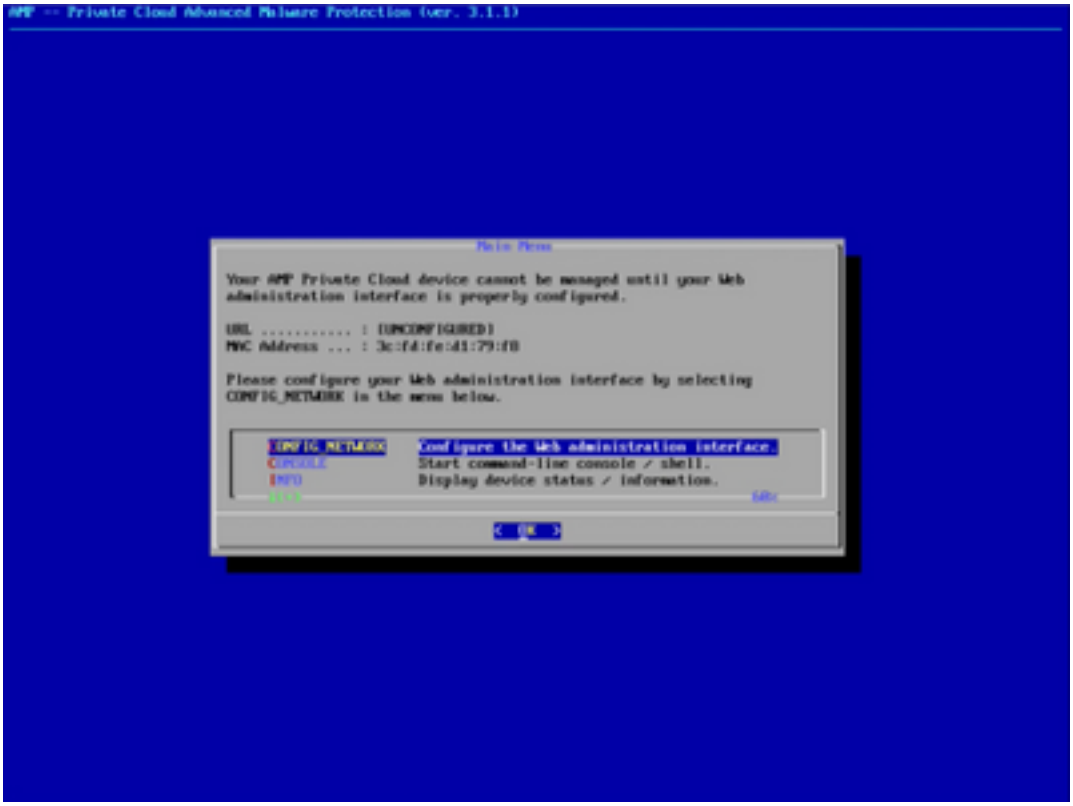


Paso 4. Introduzca el nombre de usuario y la contraseña.

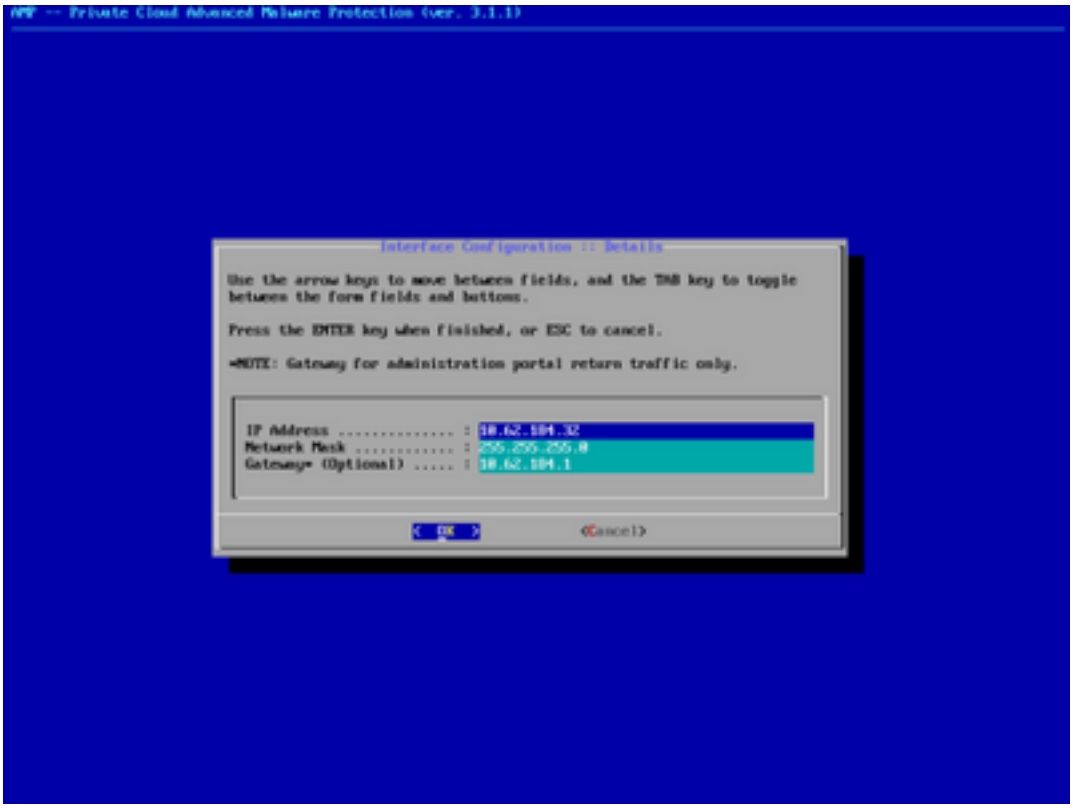
Nombre de usuario: **reinstalar**

Contraseña **sí**

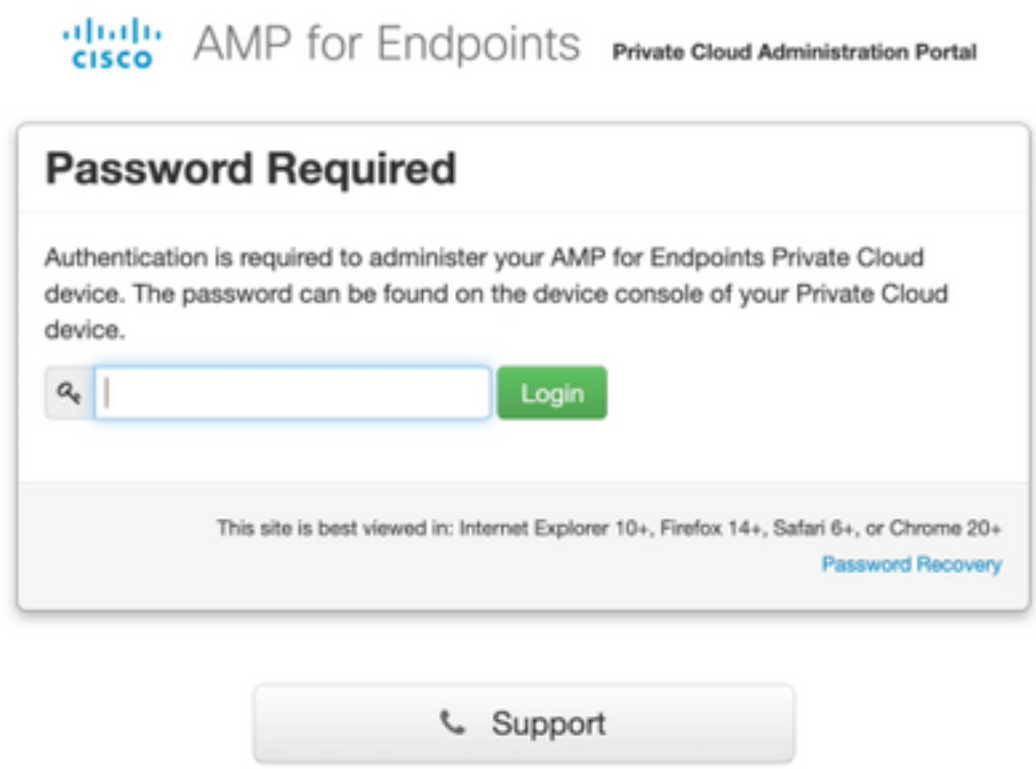
Paso 5. Se inicia la recreación de imágenes y después de la recarga se le presenta el menú inicial.



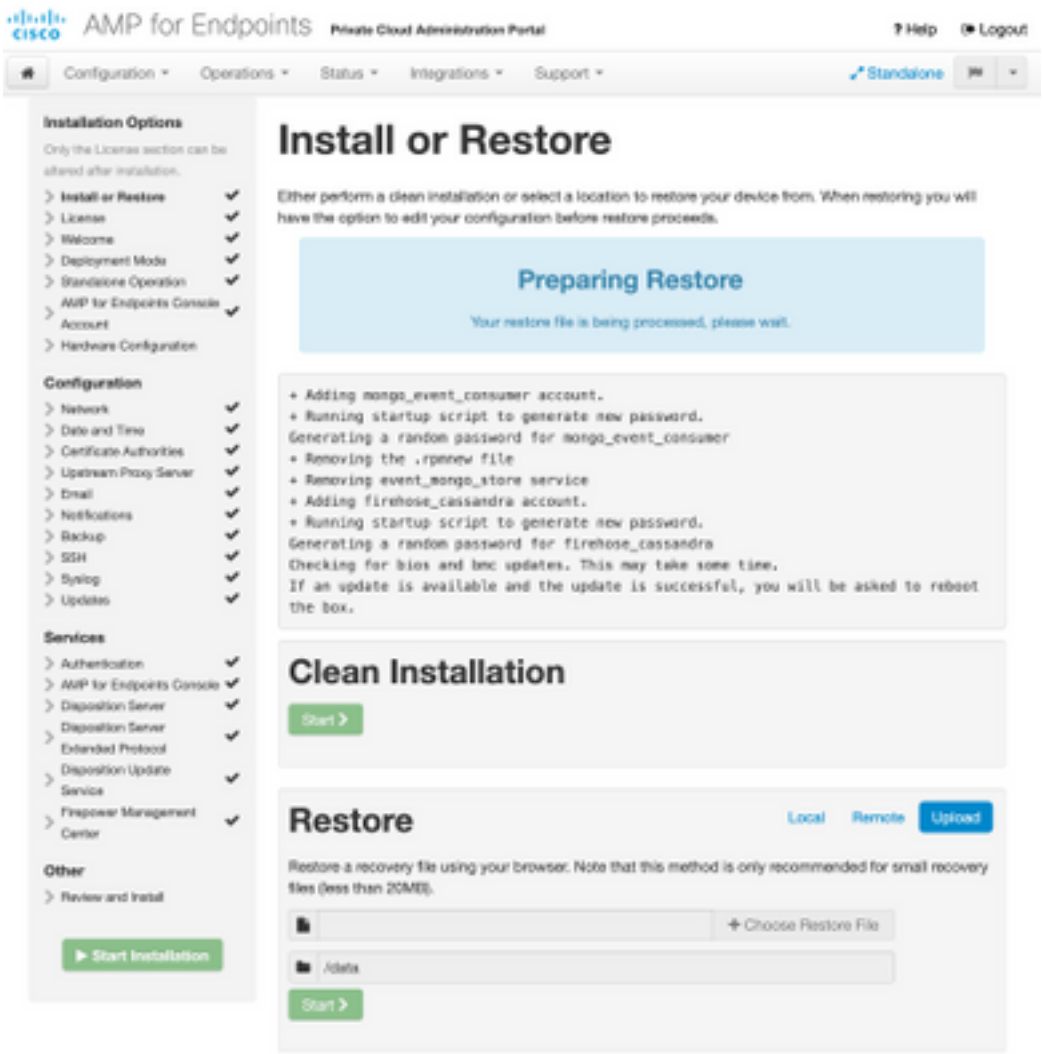
Paso 6. Configure la red en el submenú CONFIG_NETWORK.



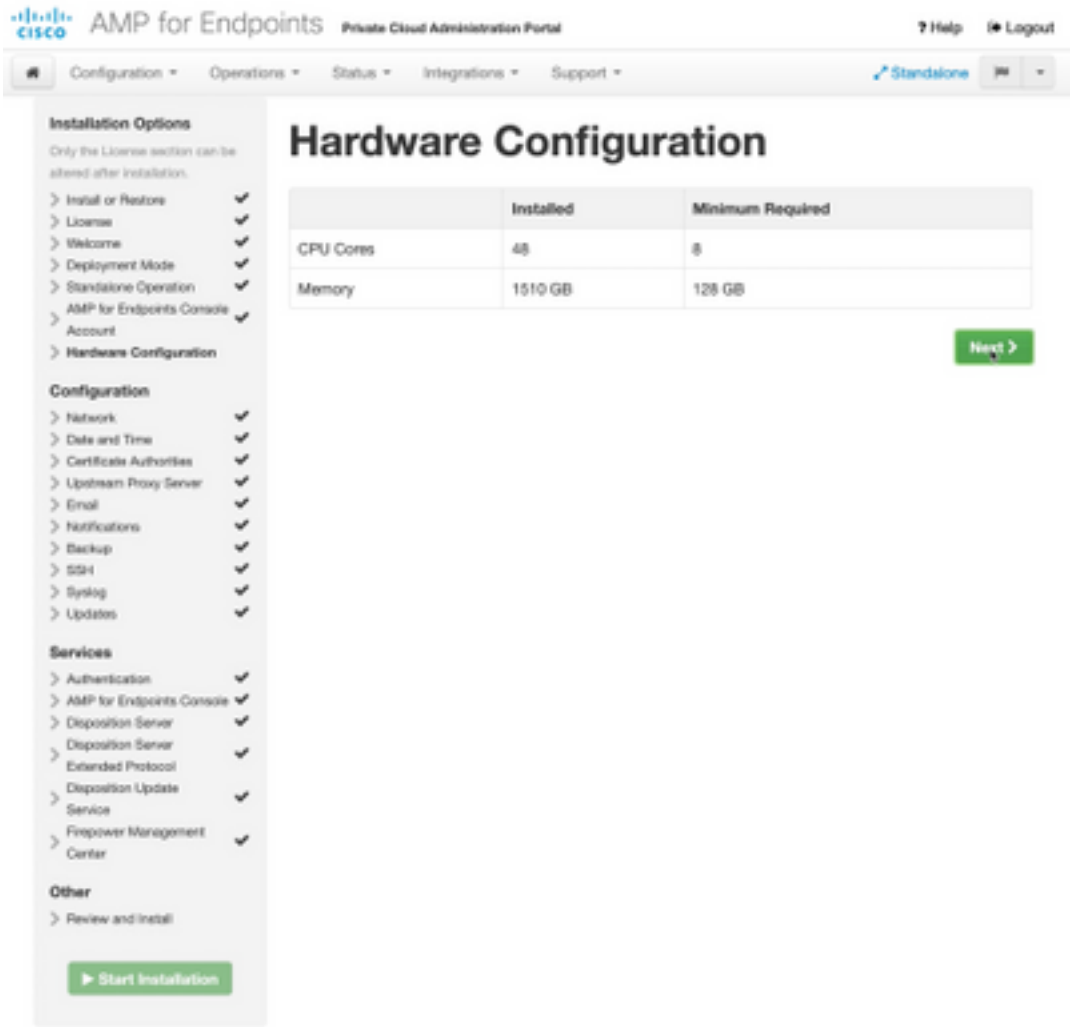
Paso 7. Inicie sesión en el portal OPadmin de AMP con la contraseña del paso 5.

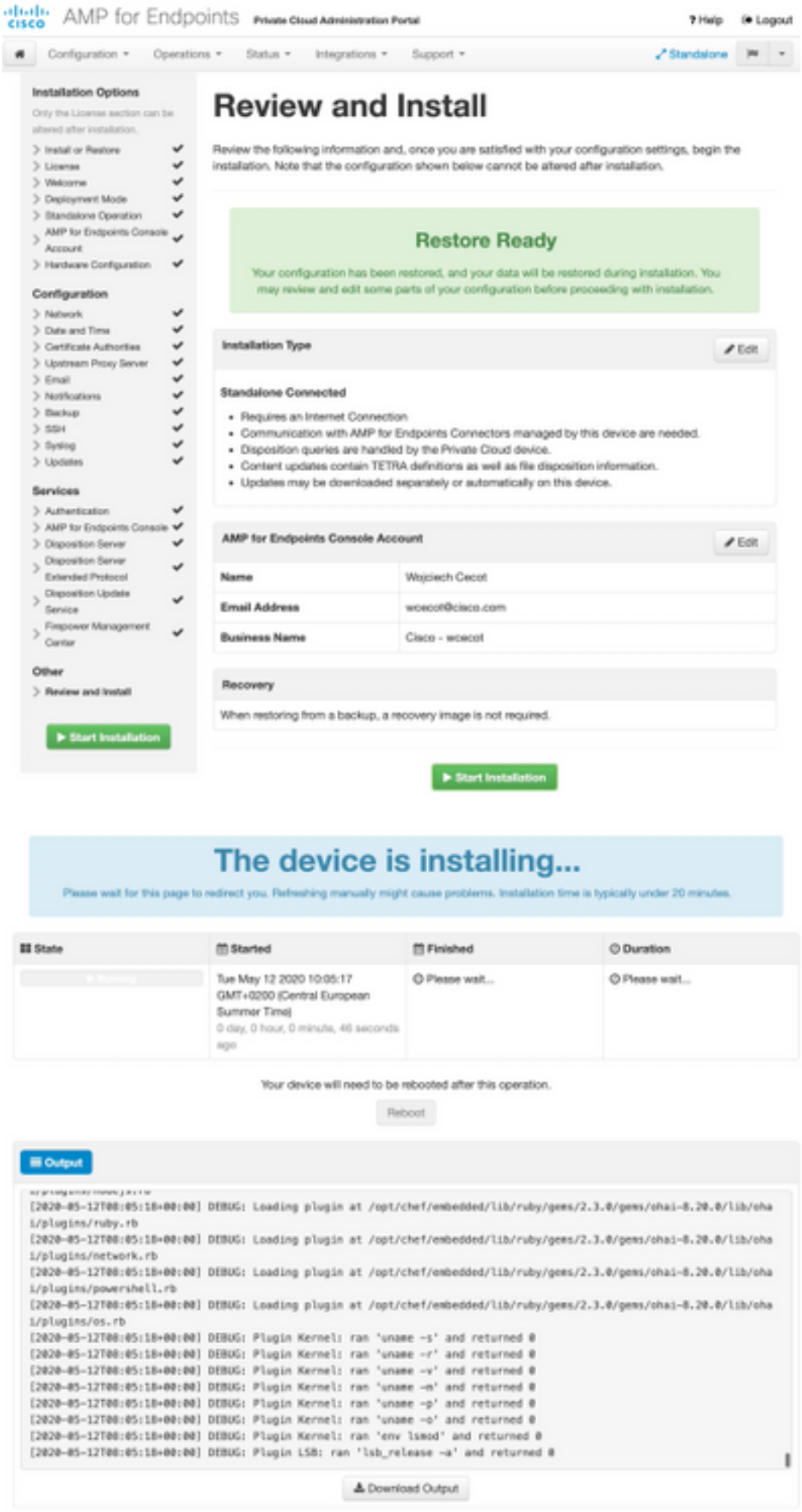


Paso 8. Utilice SFTP o SCP para descargar la copia de seguridad desde el servidor remoto a /data/.

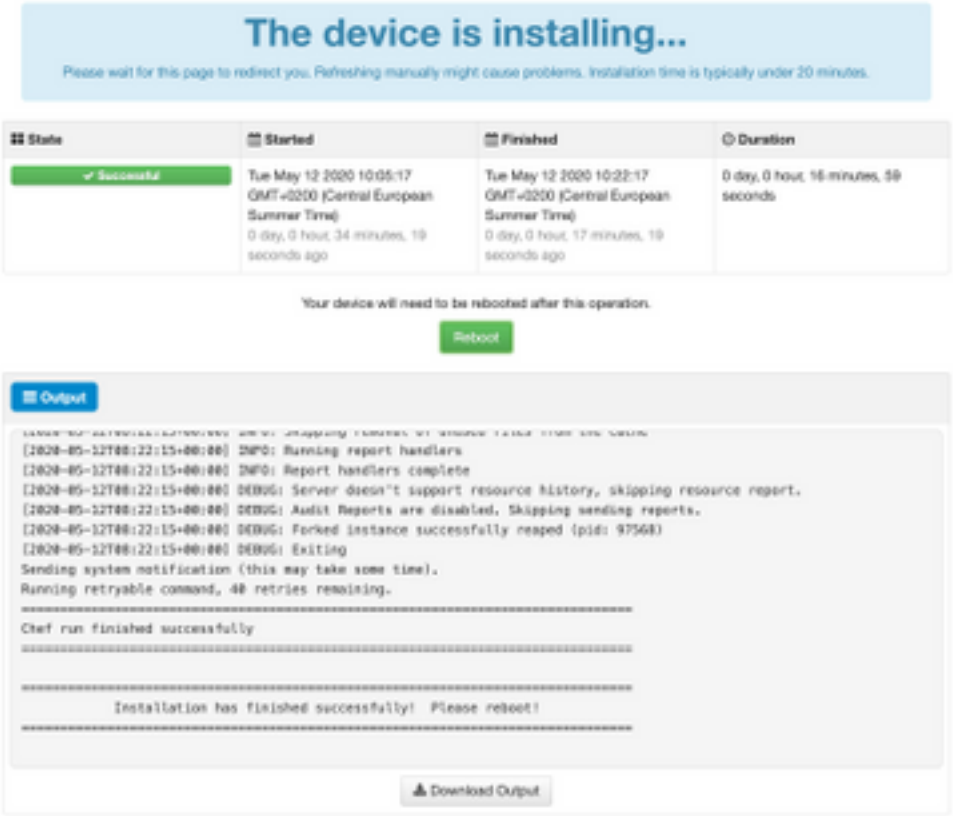


Paso 9. Confirm Hardware Configuration (Confirmar configuración de hardware), haga clic en **Next (Siguiente) > Start Installation (Iniciar instalación)**.




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

Paso 10. El reinicio es obligatorio después de la restauración correcta.



Verificación

Después de reiniciar el dispositivo, verifique si ambos portales funcionan correctamente. Intente abrir OPadmin y el portal de consola en el navegador web. Ambos portales tardan unos minutos en ser accesibles.

Troubleshoot

En caso de proceso de restauración de respaldo, la contraseña para los portales OPadmin y Console es la misma que antes. De lo contrario, debe utilizar lo que ha configurado en el asistente.