FORCEPOINT
POWERED BY Raytheon

Installation Guide

Advanced Malware Detection On-Premises Manager

v1.1

©2019 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Published 2019

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this documentation is subject to change without notice.

Last modified 20-May-2019

Contents

1 Introduction

Installation Guide | AMD OP Manager | v1.1

This guide describes the process to install the Advanced Malware Detection On-Premises Manager component on hardware provided by the customer.

The Advanced Malware Detection On-Premises Manager is offered as part of the on-premises deployment configuration to customers with stringent privacy and policy constraints. In this configuration, the Advanced Malware Detection On-Premises Manager stores, within the customer's data center, all the information regarding the detection of infected hosts and the analysis of software artifacts.

The Advanced Malware Detection On-Premises Manager collects information from Forcepoint appliances, processes it, and presents it to the user. More precisely, the Advanced Malware Detection On-Premises Manager receives artifacts (i.e., executables and documents) that are received or downloaded by the users and passes them to an Analysis Engine. The results of the analysis are collected and presented to the user via a web portal using an incident-centered approach in which evidence from run-time analysis, network monitoring, and anomaly detection are correlated to provide prioritized and actionable threat intelligence.

The Advanced Malware Detection On-Premises Manager provides a dashboard to manage appliances. It is also responsible for downloading the latest network behavior models that are associated with malware activity.

2 Prerequisites

Installation Guide | AMD OP Manager | v1.1

Hardware

The Advanced Malware Detection On-Premises Manager is a software solution that leverages your existing hardware. The following system requirements provide the minimum specifications for optimal performance and effectiveness.

- 1x Intel Xeon E5 6-core CPU
- 48 GB RAM
- 4x 2TB 7.2K RPM SATA disks (RAID 10)
- Dual PSU (highly recommended)
- ILO/LOM/DRAC (highly recommended)

Forcepoint also offers an option of purchasing dedicated hardware that is suitable for hosting the Advanced Malware Detection On-Premises Manager. Forcepoint delivers the server with the Advanced Malware Detection On-Premises Manager software already installed.

Network connectivity

The Advanced Malware Detection On-Premises Manager requires the following connections:

- log.lastline.com to TCP port 443
- update.lastline.com to TCP port 443 and optionally to UDP port 123 for time synchronization

  The latter can be replaced with a local NTP server.
- management.lastline.com to TCP port 443
- user.lastline.com to TCP port 443
- anonvpn.lastline.com to UDP port 1194

This is not mandatory, but highly recommended, as the lack of it can negatively impact the performance and malware detection capability of the analysis engine.

The domain names above may resolve to any IP addresses in the following ranges:

- 38.95.226.0/24
- 38.142.33.16/28
- 199.91.71.80/28
- 46.244.5.64/28

All connections can be optionally routed through an explicit HTTP proxy, but proxy authentication is not supported.

License

Before starting the installation, you need to contact Forcepoint Sales to purchase a license for the software.

If you have already purchased the product, your license information can be found under the **Products** tab after you log on to the Forcepoint Support Portal. The following license information is provided:

- AMD Portal Username
- API Key
- FQDN

Furthermore, you need your Lastline Portal password. To retrieve this password:

1. Navigate to the Lastline Portal.
2. Click **Forgot your password?**
3. Follow the instructions provided on the Portal. You need your Lastline Account Username.

License extensions

To renew an expired license, contact Forcepoint Sales. After your request has been processed, your license expiration date will automatically be extended.

3 Installation Process

Installation Guide | AMD OP Manager | v1.1

The installation process for the Advanced Malware Detection On-Premises Manager consists of the following steps:

1. Install the base system.
2. Collect and apply the basic configuration information to the system.

If you purchased dedicated hardware from Forcepoint with the Advanced Malware Detection On-Premises Manager software already installed, skip to *Registration and configuration*, page 6.

Base system installation

Preparing hardware

Before starting the installation of the Advanced Malware Detection On-Premises Manager software, the RAID controller must be configured in RAID10. If you purchased dedicated hardware directly from Dell, the RAID controller is likely not configured appropriately. Please see *RAID Configuration*, page 23 for configuration instructions.

Important

Before you install the software, wire the Advanced Malware Detection On-Premises Manager as shown in the *Quick Start Guide* (included with your Advanced Malware Detection On-Premises server). It is important that the E port (2nd interface/bottom port) be connected to either an Advanced Malware Detection On-Premises Engine or network switch that is powered ON. Software installation should take approximately 30 minutes.

Software installation

The Advanced Malware Detection On-Premises Manager uses CentOS 7 as the underlying operating system. It uses an automated text-based installation process, eliminating the need for user input or a graphical user interface.

Before starting the installation, you must obtain an official copy of the latest Advanced Malware Detection On-Premises Manager ISO from Forcepoint. The image may be burned onto a bootable DVD, or simply mounted using the Dell iDRAC interface, if available.

To install the Advanced Malware Detection On-Premises Manager, boot the system from the selected medium and let it run to completion. The installation is automatic and only stops if it encounters a hardware error. The system reboots twice, then presents you with a log on prompt.

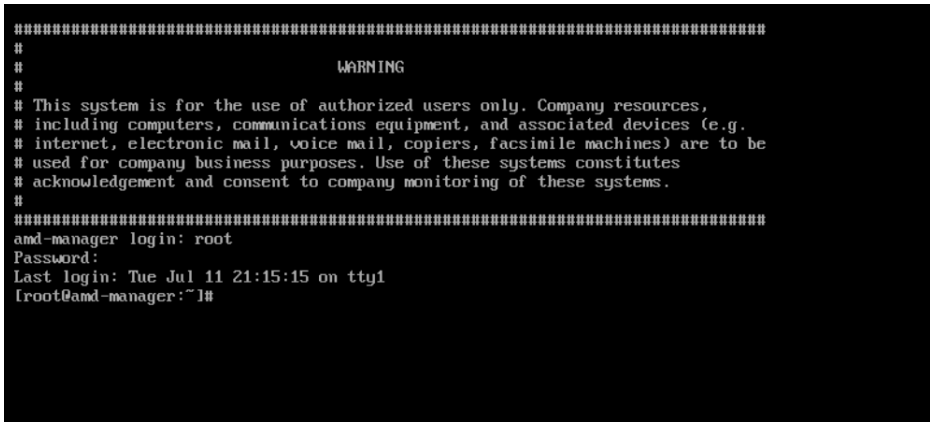
Registration and configuration

To register and apply the software configuration to the Advanced Malware Detection On-Premises Manager, complete the following procedure:

1. Log on to the console using the following credentials:
   - username: **root**
   - password: **P!L)TP@ssw0rd**

   Note, you can log on with this username and password only from a console.

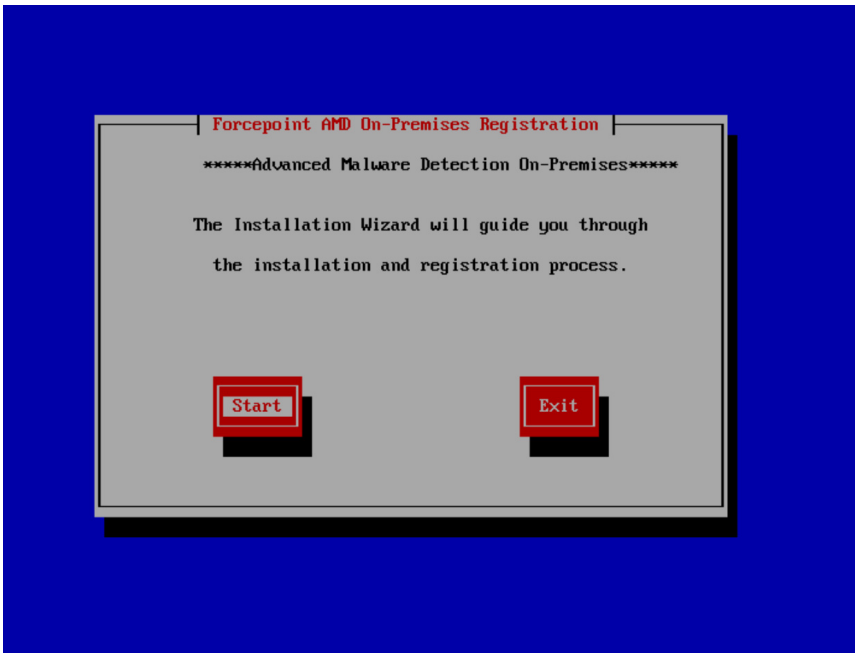
> **Important**
> This is a default password that is available for all Advanced Malware Detection On-Premises Manager installations. Change the default password to a password that is unique to your organization.



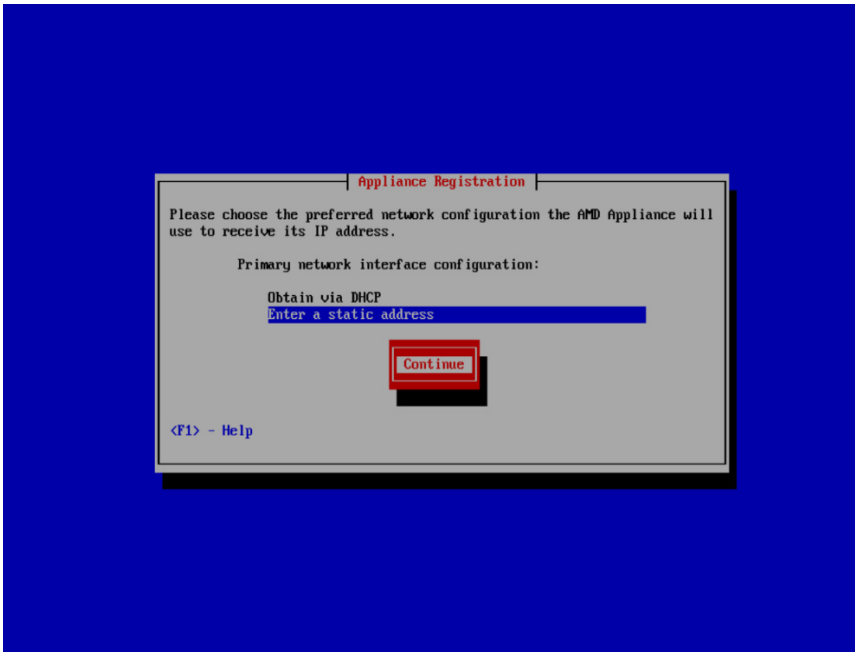
2. Execute **amd_register** to start the guided configuration and installation process.

If asked what interface to use as the primary network interface, select **eth0**. If a different interface is selected, some components may not work properly.

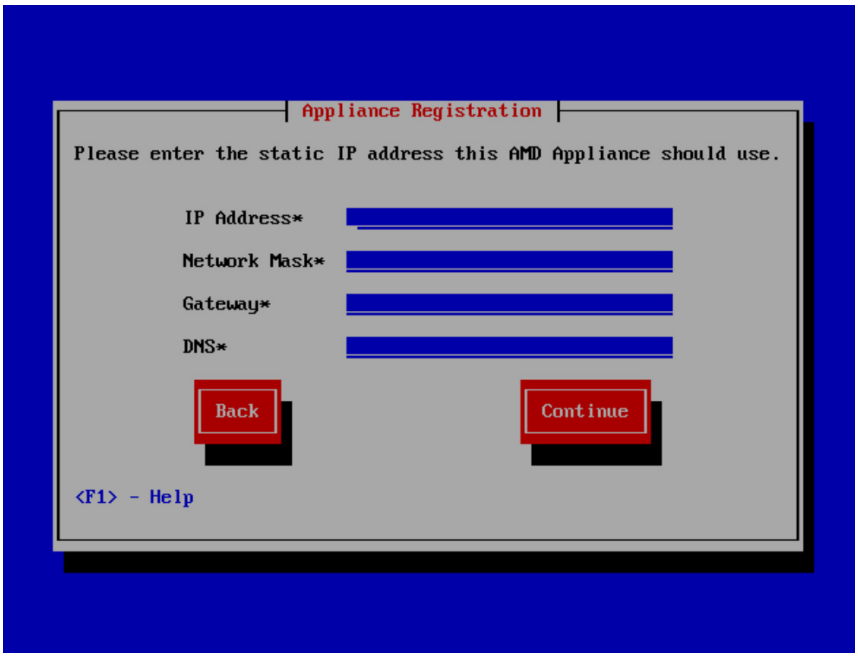
3. The installation process starts at the Welcome screen. When you are ready to begin the installation process, select **Start**.



4. You can configure the network via DHCP (**Obtain via DHCP**) or a static IP address (**Enter a static address**). Select your option, then select **Continue**.



5. If you selected **Enter static address** on the previous screen, type the **IP Address** to be assigned to the interface, the **Network Mask**, **Gateway** address, and **DNS** address, then select **Continue**.



6. You then have the option of configuring an HTTP proxy for connecting to the update servers.

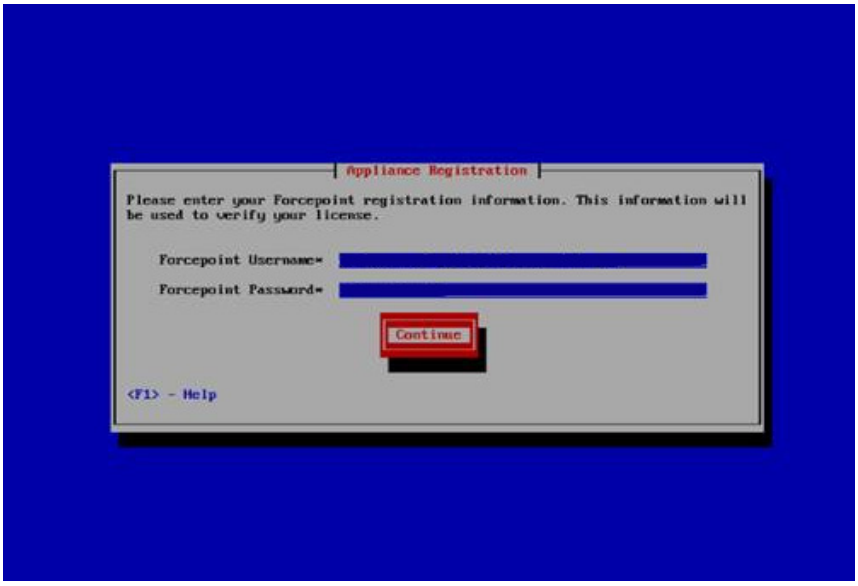
If no proxy configuration is required to access the Internet via HTTPS, this field should be left empty. Otherwise, if all HTTPS connections need to go through an HTTP proxy, the address of the proxy must be entered here. Optionally, a non-default port of the proxy server can be specified. Valid proxy configuration examples are: **my_proxy.my_domain.com:3128** and **192.168.0.1:8080**.

Select **Continue**. At this point, the network configuration is applied.

7. Configure the NTP server, then select **Configure Network**.

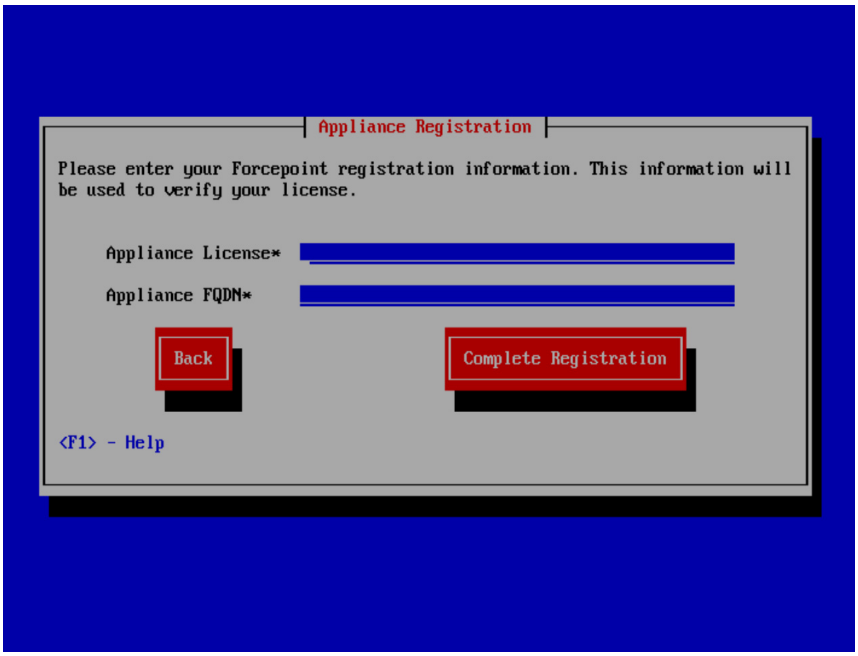
Unless the use of a different NTP server is needed, keep the default value. The system must be able to reach the chosen NTP server over UDP port 123.

8. Type the **Forcepoint Username** and **Forcepoint Password** provided with the license, then select **Continue**.

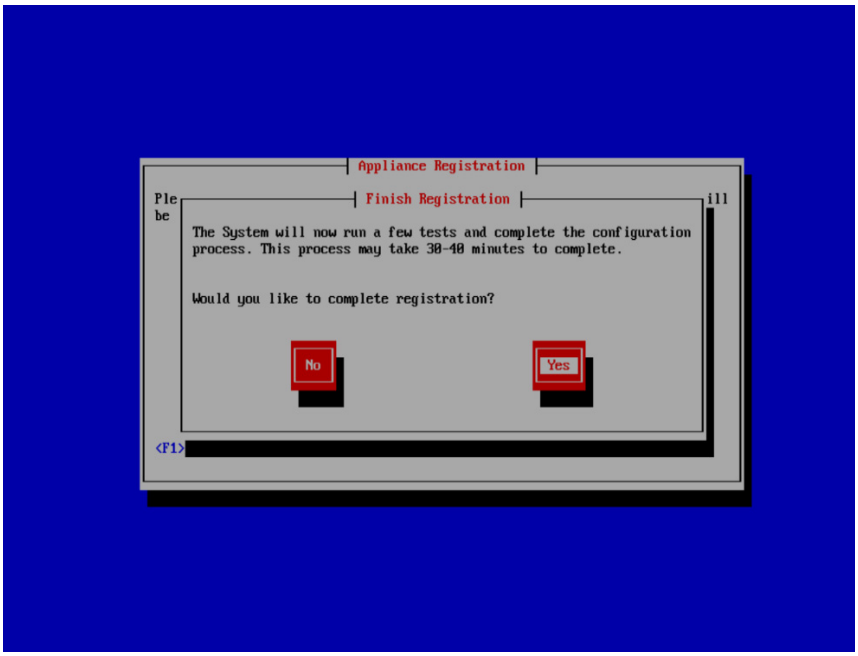


9. Enter the license key and assigned FQDN associated with the purchased license, then select **Complete Registration**.

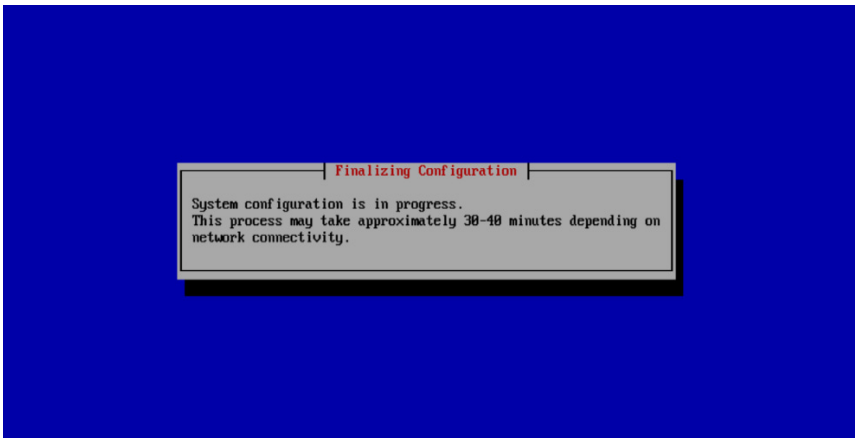
   See *License*, page 4 for details on acquiring your license information.



10. You are prompted to verify your readiness to complete the configuration process. Select **Yes** to begin the system configuration and product registration. Internet access is required throughout this portion of the registration process.



11. After system configuration is complete, the remaining process (testing, applying configurations, and registering the Advanced Malware Detection On-Premises Manager) starts. This process may take up to 30 – 40 minutes to complete depending on network connectivity and system characteristics.



12. After the installation process completes, select **OK** to exit the installation wizard.

Users can access the user portal:

https://<<*IP address of AMD Manager*>> or https://<<*assigned FQDN*>>

If any error message is shown, please refer to *Error handling*, page 14.

4 System Administration

Installation Guide | AMD OP Manager | v1.1

The Advanced Malware Detection On-Premises Manager is developed to require as little maintenance and administration as possible. The only action that might be required is to change the system's network configuration, as discussed below.

See the Advanced Malware Detection On-Premises Troubleshooting Guide for additional information.

Advanced Malware Detection On-Premises Manager installation wizard

The easiest way to modify the system configuration is by re-running the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

Then, you can change the configuration values provided the last time the installation wizard ran.

Advanced Malware Detection On-Premises configuration tool

The system comes with the Advanced Malware Detection On-Premises configuration tool, **amd_setup**, which provides an interface to administrate and manage the Advanced Malware Detection On-Premises Manager. The tool can be started by logging on to the Manager virtual machine:

1. To connect to the Manager through SSH, run the following command from the command line:

   ```
   ssh <<IP address of AMD appliance>>
   ```

   a. SSH credentials:

      - username: **admin**

- password: **D#FP@ssw0rd**

2. Run the following command from the command line:

```
amd_setup <action> <arguments>
```

Important
The password provided in this procedure is the default password that is available for all Advanced Malware Detection On-Premises Engine SSH connections. Change the default password to a password that is unique to your organization.

Error handling

If any error message is shown when using **amd_setup**, please contact Forcepoint Support.

Network configuration

The Advanced Malware Detection On-Premises server connects to 2 networks:

- The primary (external) network
- The private analysis network

Primary network

The primary (external) network connects to **eno1** and must be able to provide NTP and DNS services. It must also be able to connect to the Internet, which is required for product registration and for downloading images required by the Advanced Malware Detection On-Premises Engine appliances.

The Advanced Malware Detection On-Premises Manager can also receive network configuration via DHCP over this interface. This can be configured using the amd_register utility described in *Advanced Malware Detection On-Premises Manager installation wizard* above.

Use the IP address assigned to this interface to access the Advanced Malware Detection On-Premises user interface.

Analysis network

The Advanced Malware Detection On-Premises Manager connects to the analysis network using the **eno2** interface, which is reserved for connecting the Advanced Malware Detection On-Premises Engine appliances with the Advanced Malware Detection On-Premises Manager. Additionally, the Advanced Malware Detection On-Premises Manager provides network configuration via DHCP to all Advanced Malware Detection On-Premises Engines connected to this network.

The Advanced Malware Detection On-Premises Manager uses the static IP address 10.0.0.10 for this network. This is not configurable.

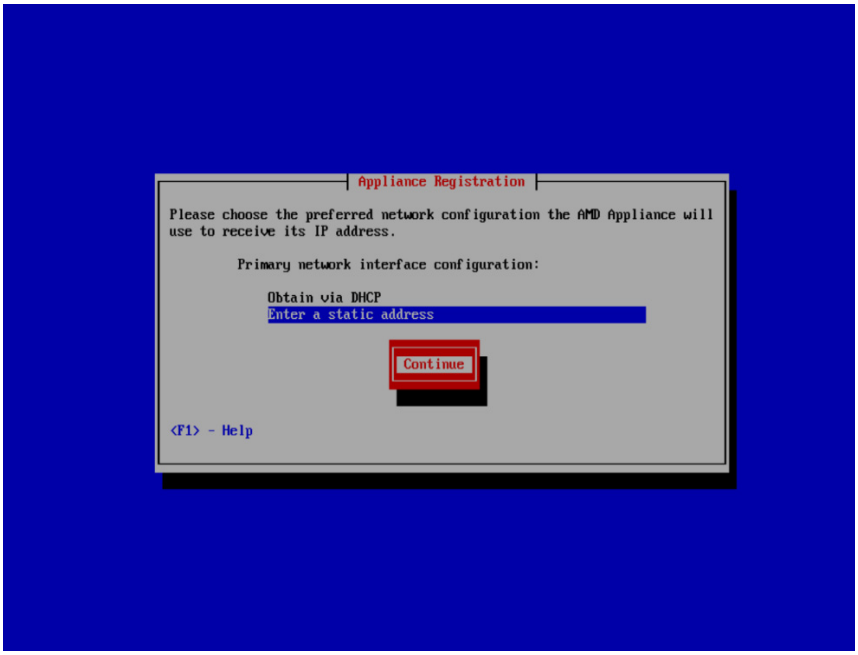
Reconfiguring the network address: static to DHCP

If you selected a static IP-based network configuration during the initial installation, you can switch this to a DHCP-based network configuration at a later time. To switch to a DHCP-based network configuration, run the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

The following installation wizard screen displays.

Select **Start** to begin. As you go through the wizard, the screens show the configuration as last entered. For example, if you selected **Enter Static Address** the last time the wizard ran, the following screen displays.



From this screen, you may select the alternate option of how the IP is configured. Select **Obtain via DHCP** to have Advanced Malware Detection On-Premises automatically be configured with DHCP. At this point, no configuration changes have yet been applied. Select **Continue** and go through the remaining screens to apply the configuration changes. Select **Complete Registration**, and then select **Yes** to complete the registration and apply the changes.

Reconfiguring the network address: DHCP to static

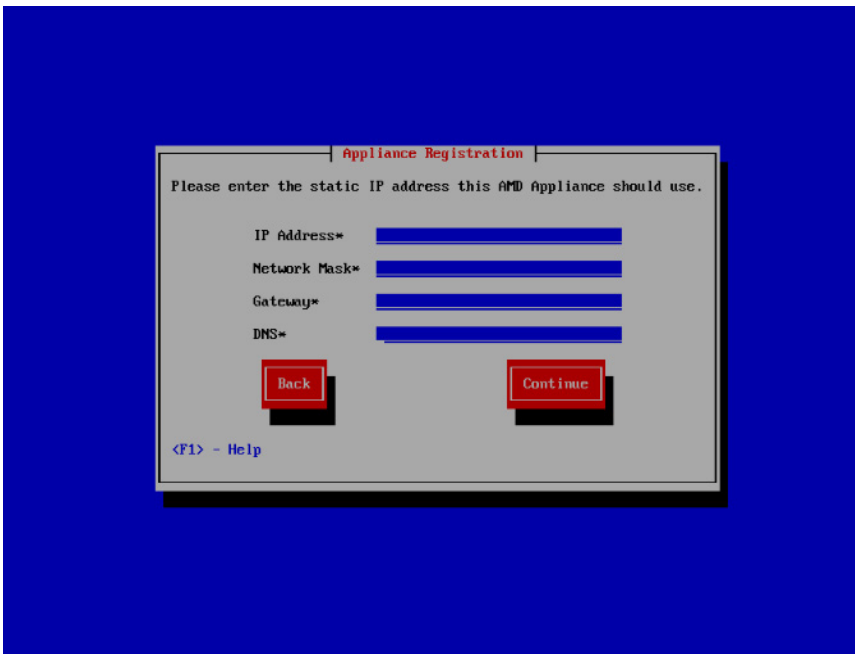
If you selected a DHCP-based network configuration during the initial installation, you can switch this to a static IP-based network configuration at a later time. To switch to a static IP-based network configuration, run the Advanced Malware Detection On-Premises Manager installation wizard tool using the following command:

```
amd_register
```

The following installation wizard screen displays.

Select **Start** to begin. As you go through the wizard, the screens show the configuration as last entered. For example, if you selected **Obtain via DHCP** the last time the wizard ran, that option is highlighted.

From this screen, you may select the alternate option of how the IP is configured. Select **Enter a static address** to have Advanced Malware Detection On-Premises automatically be configured with a static IP address. At this point, no configuration changes have yet been applied. Select **Continue** and type the **IP Address**, **Network Mask**, **Gateway**, and **DNS** to configure the static IP address.



Select **Continue** to go through the remaining screens to apply the configuration changes. Select **Complete Registration**, and then select **Yes** to complete the registration and apply the changes.

Configuration update after a network DHCP change

After a new network address has been assigned to the host (e.g., after the DHCP server hands out a new network address), the new configuration needs be applied to all software on the host. To do so, log on to the console of the host and run the following command (for default password, see *Registration and configuration*, page 6):

```
lastline_apply_config
```

Storing Forcepoint Email Security or Forcepoint Web Security artifacts after analysis

The Advanced Malware Detection On-Premises Manager is configured by default to delete all submitted artifacts after analysis is complete. An optional setting is provided to enable storage of artifacts submitted by your Forcepoint Email Security or Forcepoint Web Security products locally on your Advanced Malware Detection On-Premises Manager.

To enable the setting:

1. Connect to the Advanced Malware Detection On-Premises Manager through SSH by running the following command from the command line:

   ```
   ssh <<IP address of the AMD appliance>>
   ```

2. To edit the properties file, run the following command:

   ```
   vi /etc/lastline/amd-llmgr.ini
   ```

3. Make sure the **delete_after_analysis** option is set to **False**:

   ```
   delete_after_analysis = False
   ```

4. Save the properties file.
5. Stop and restart the SHIM service:

   ```
   sh /usr/local/amd/shim/bin/stop_shim.sh
   sh /usr/local/amd/shim/bin/start_shim.sh
   ```

Configuring the memcache timeout

Starting in Advanced Malware Detection On-Premises v1.1, the memcache timeout value can be adjusted:

1. Open the **wsgi.py** file on the Advanced Malware Detection On-Premises Manager at the following location:

   `/usr/local/amd/shim/app/wsgi.py`

2. Change the **<<timeout value>>** in the following string:

   `amc = amd.Memcache("127.0.0.1",11211,<<timeout value>>)`

   The <<timeout value>> must be in seconds. For example, the following string has a timeout value of 25 minutes (1500 seconds):

   `amc = amd.Memcache("127.0.0.1",11211,1500)`

3. Save the **wsgi.py** file.

5 Software Upgrades

Forcepoint periodically releases appliance and software upgrades or hotfixes. If you plan to upgrade from v1.0 to v1.1, see the Advanced Malware Detection On-Premises v1.1 Upgrade Guide.

If the software has automatic updates enabled, these updates are transparently applied.

Automatic software updates are enabled by default upon installation. To disable automatic upgrades, or to manually upgrade an appliance with automatic updates disabled, log on to the web interface of the appliance itself and access the appliance configuration page from the Appliances tab.

System appliance updates released by Forcepoint are communicated through email. To manually check for system updates, log on to the appliance as an administrator and run the following commands:

```
cd /usr/local/amd/shim/bin/
./check_for_updates
```

If updates are available, you are shown the version available and instructed to run the following command to install the appliance updates:

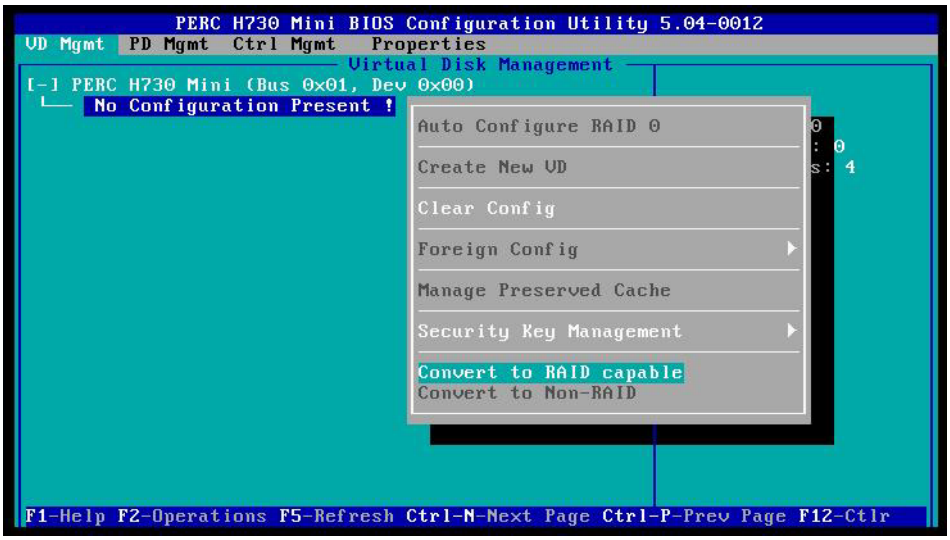
```
./update_amd
```

6 RAID Configuration

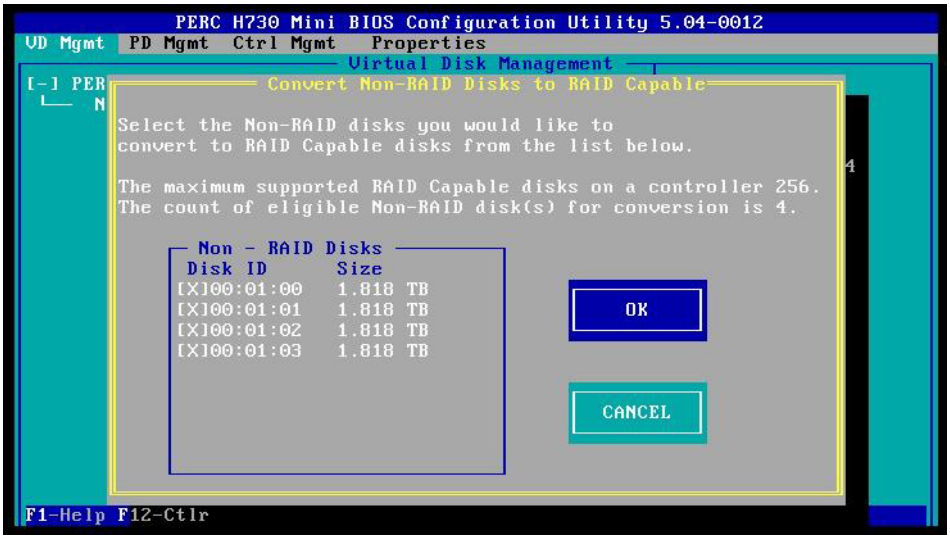
Complete the following procedure to configure RAID on the Advanced Malware Detection On-Premises Manager.

1. Launch the PERC Configuration Utility by pressing **<Ctrl>+R** during the server boot sequence:

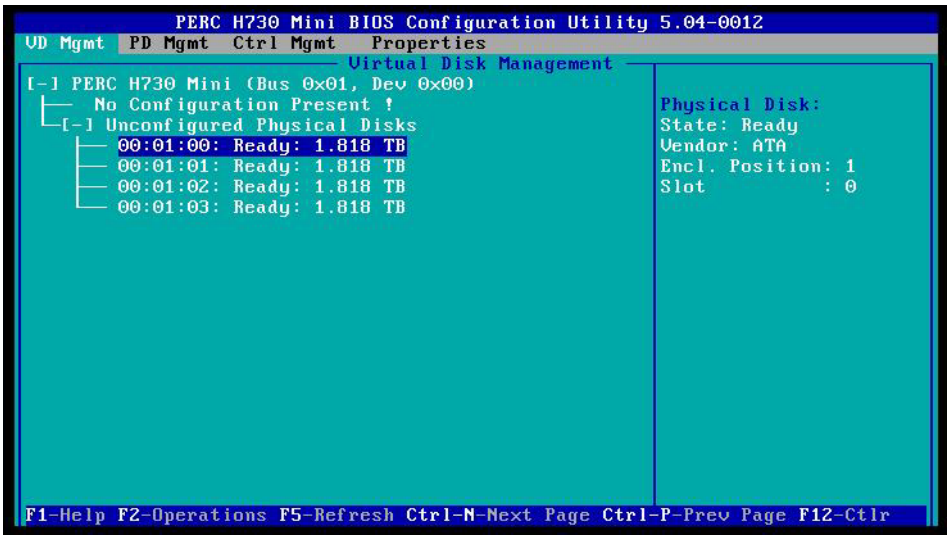
2. After the configuration utility starts, press **F2** on your keyboard and select **Convert to RAID Capable**.



3. Select all 4 disks and select **OK**.

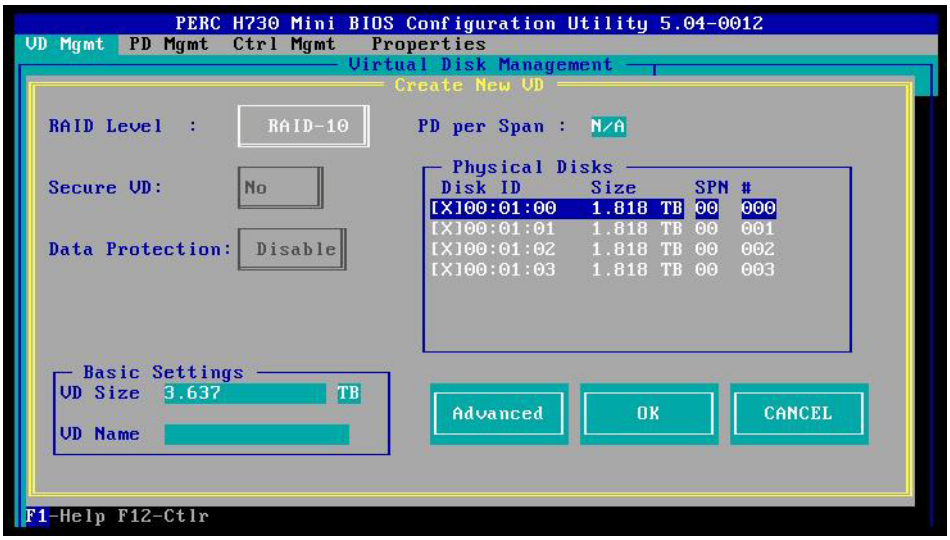


You should see the 4 disks on this screen:

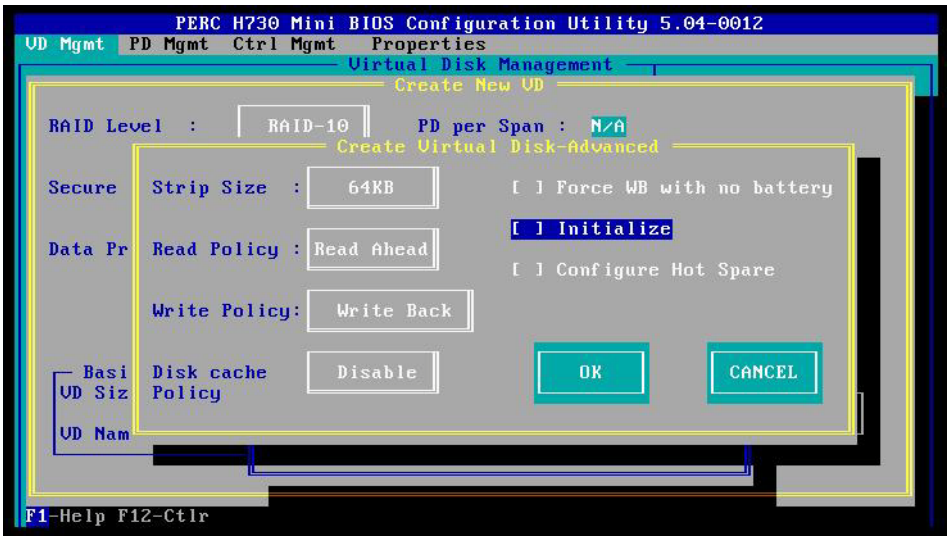


4. Press **F2** on your keyboard and select **Create New VD**.

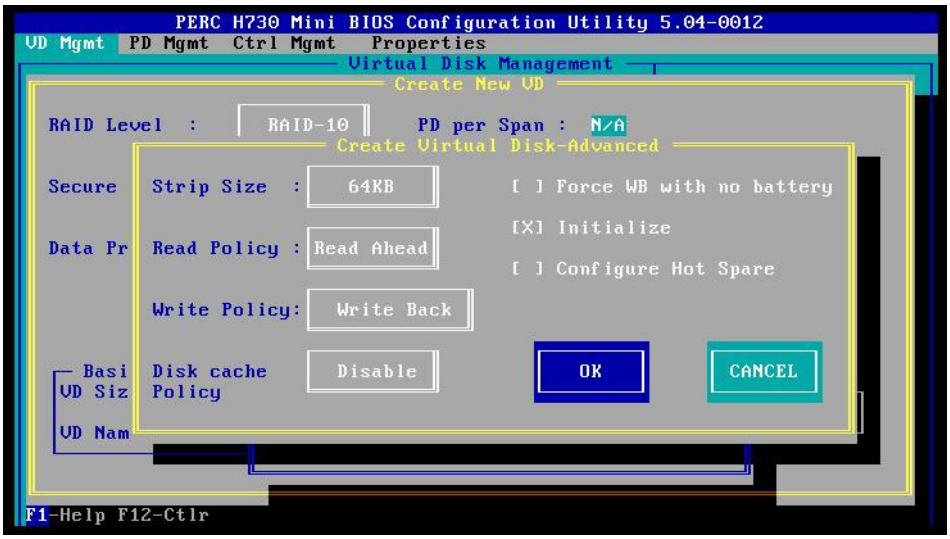
5. Select all 4 disks, make sure **RAID Level** is set to **RAID-10**, then select **Advanced**.



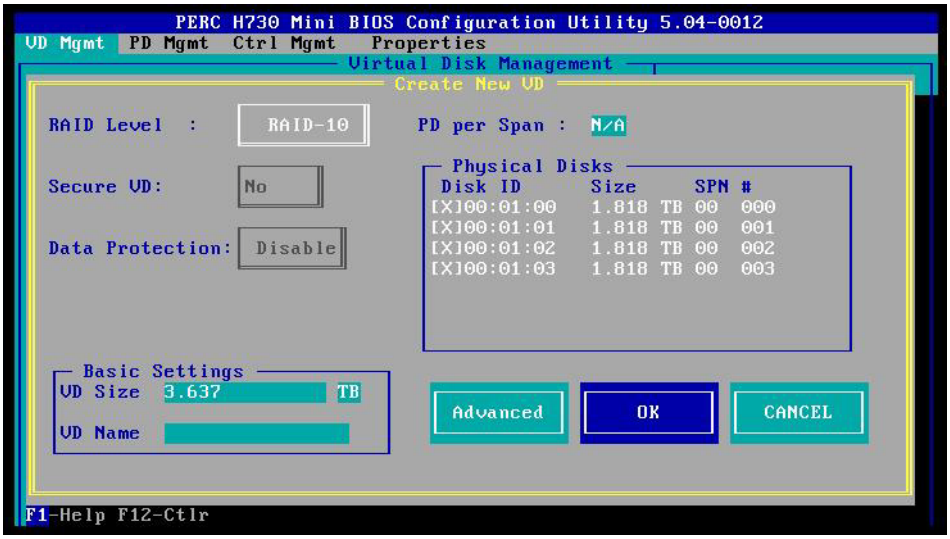
6. Make sure **Write Policy** is set to **Write Back**, **Disk cache policy** is set to **Disable** and **Force WB with no battery** is not select. Then select the **Initialize** option (select **OK** if the utility shows an initialization confirmation pop-up).



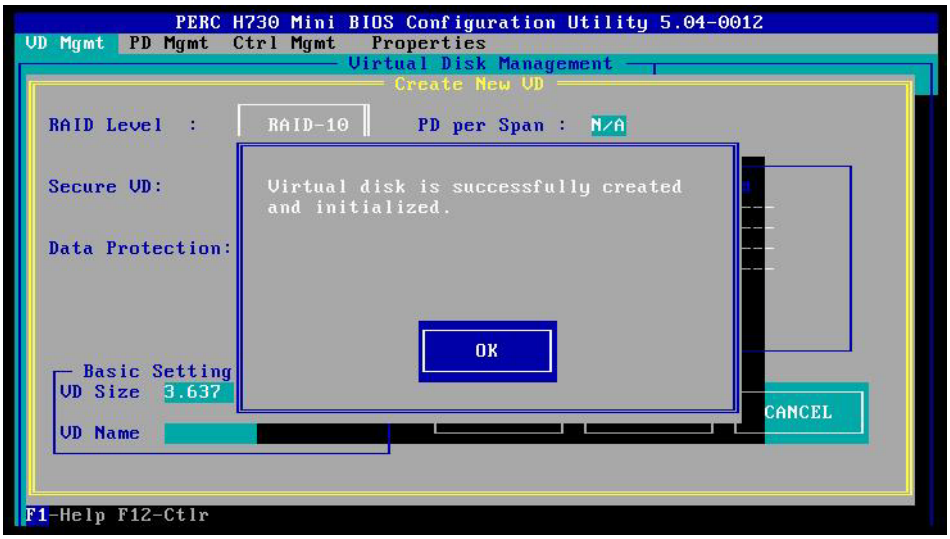
7. After initialization is complete, select **OK** to save the advanced settings.



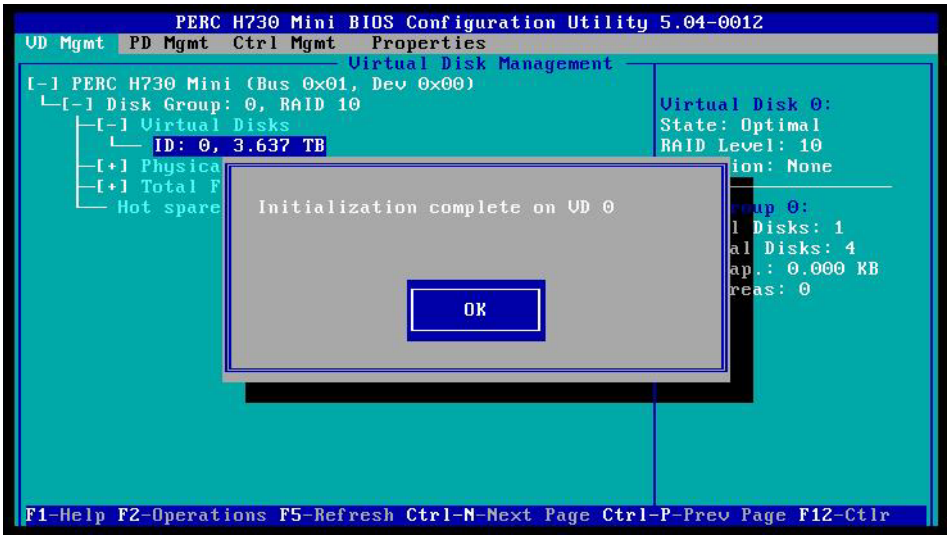
8. Select **OK** to create the virtual drive.



9. Select **OK** to confirm.

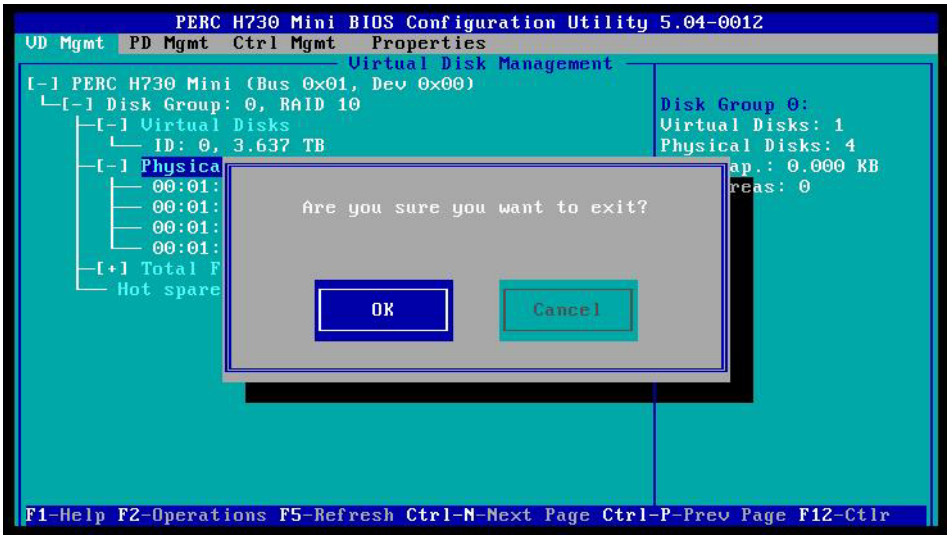


10. Select **OK** to confirm the initialization.



This is what the virtual and physical disks should look like.

11. Press **ESC** on your keyboard, then select **OK** to exit.



7 Copyrights and Trademarks

Installation Guide | AMD OP Manager | v1.1

Published 2019
Printed in the United States of America

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Copyrights and trademarks

© 2019 Forcepoint. This document may not, in whole or in part, be reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint.

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Other acknowledgments

This Forcepoint product uses the third-party software listed in this file. In addition, this Advanced Malware Detection On-Premises product includes or may include the following open source components:

NGINX 1.10.3, © 2002-2017 Igor Sysoev, © 2011-2017 Nginx, Inc., is distributed under the BSD 2-Clause License (opensource.org/licenses/BSD-2-Clause) ▪ PYTHON 2.7.5, © 2001-2017 Python Software Foundation, is distributed under the Python License (docs.python.org/3/license.html) ▪ UWSGI V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html) ▪ UWSGI-PLUGIN-COMMON V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html) ▪ UWSGI-PLUGIN-PYTHON V2.0.14, © 2016 anthon, unbit, is distributed under the GNU General Public License, version 2 with Classpath Exception (gnu.org/software/classpath/license.html)

Some third-party software included in Forcepoint Advanced Malware Detection On-Premises is licensed under the following open source license(s):

GNU General Public License with Classpath Exception

If you would like a copy of the source code for such third-party software included in Forcepoint Advanced Malware Detection On-Premises, you may email your request to opensource@forcepoint.com.