Installation Guide

Advanced Malware Detection On-Premises Engine

v1.1

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 Engine | v1.1

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

The Advanced Malware Detection On-Premises Engine component receives artifacts (i.e., executables and documents) from the Advanced Malware Detection On-Premises Manager. It runs these artifacts, then returns analysis results back to the Advanced Malware Detection On-Premises Manager, which then displays results to the users.

The Engine is managed by the Manager. However, as an important part of the installation process, the Engine must be made known to the Manager.

2 Prerequisites

Installation Guide | AMD OP Engine | v1.1

Hardware

The Advanced Malware Detection On-Premises Engine 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
- 2x 1TB 7.2K RPM SATA disks (RAID 1)
- 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 Engine. Forcepoint delivers the server with the Advanced Malware Detection On-Premises Engine software already installed.

Network connectivity

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

- log.<<*MANAGER*>> to TCP port 443
- update.<<*MANAGER*>> to TCP port 443 and 8443
- update.<<*MANAGER*>> to UDP port 1194
- update.<<*MANAGER*>> to UDP port 123 for time synchronization
- user.<<*MANAGER*>> to TCP port 443.

  This can be replaced with a local NTP server.

Replace <<*MANAGER*>> with the Advanced Malware Detection On-Premises Manager’s Fully Qualified Domain Name (FQDN).

All HTTPS connections (port 443) can be optionally routed though an explicit HTTP proxy.

License

Before starting the installation, 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 will need your Lastline Account Username.

License extensions

To renew an expired license, contact Forcepoint Sales. After your request is processed, your license expiration date is automatically extended.

3 Installation Process

Installation Guide | AMD OP Engine | v1.1

The installation process for the Advanced Malware Detection On-Premises Engine consists of two 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 Engine software already installed, skip to *Registration and configuration*, page 5. The base system has already been installed.

Base system installation

The Advanced Malware Detection On-Premises Engine uses Ubuntu 14.04.5 LTS as the underlying operating system. It uses an automated text-based installation process that eliminates 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 Engine 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 Engine, 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

The Advanced Malware Detection On-Premises Engine appliance should be connected to the Advanced Malware Detection On-Premises Manager server’s **eth1** port (2nd NIC). If there are multiple Advanced Malware Detection On-Premises Engines, a switch or private VLAN should be used to create a private network that connects to the Advanced Malware Detection On-Premises Manager’s 2nd NIC. For more information, see the Advanced Malware Detection On-Premises Quick Start Guide.

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

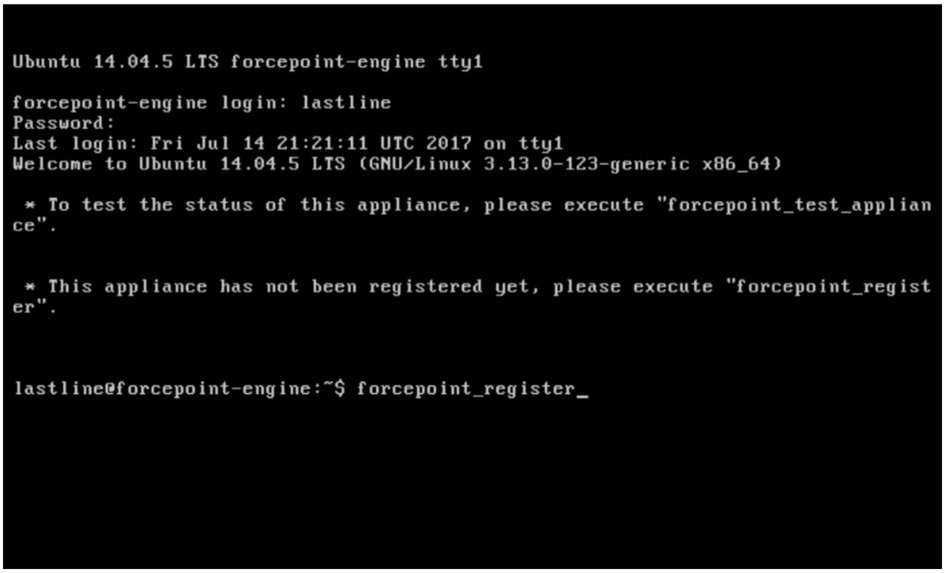
1. Log on to the console using the following credentials:
   - username: **lastline**
   - password: **lastline**

   Note, it is possible to log on with the username and password only from a console.

   Important

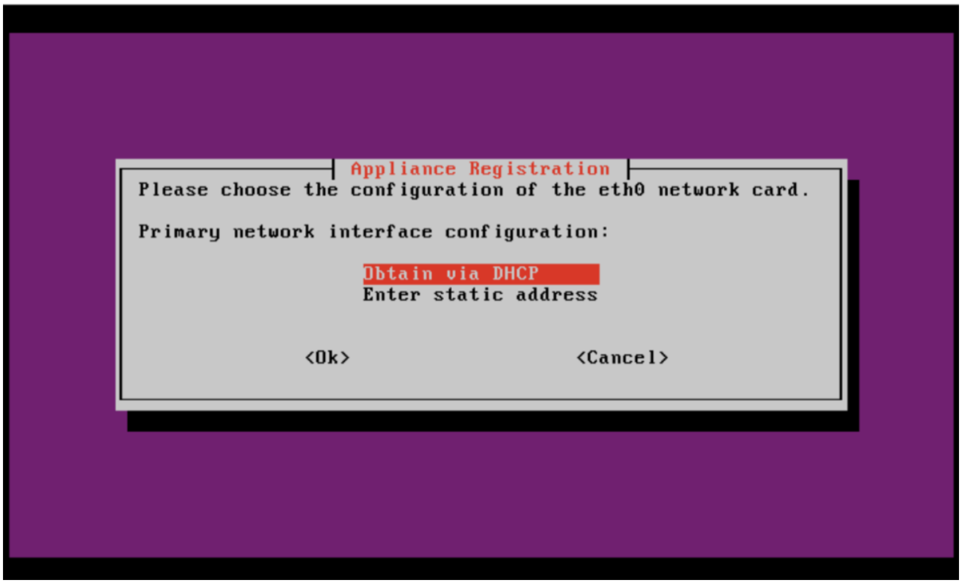
   This is a default password that is available for all Advanced Malware Detection On-Premises Engine installations. Change the default password to a password that is unique to your organization.

2. Execute **forcepoint_register** to start the guided registration and configuration process.



```
Ubuntu 14.04.5 LTS forcepoint-engine tty1

forcepoint-engine login: lastline
Password:
Last login: Fri Jul 14 21:21:11 UTC 2017 on tty1
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-123-generic x86_64)

 * To test the status of this appliance, please execute "forcepoint_test_applian
ce".


 * This appliance has not been registered yet, please execute "forcepoint_regist
er".



lastline@forcepoint-engine:~$ forcepoint_register_
```

3. You can configure the network via DHCP (**Obtain via DHCP**) or with a static IP address (**Enter static address**).



```
Appliance Registration
Please choose the configuration of the eth0 network card.

Primary network interface configuration:

          Obtain via DHCP
          Enter static address

     <Ok>                <Cancel>
```

Forcepoint strongly recommends the use of DHCP. An IP in the range of 10.0.0.200-254 will be assigned to each Advanced Malware Detection On-Premises Engine on the private engine network. The Advanced Malware Detection On-Premises Engines will obtain IPs via DHCP from the Advanced Malware Detection On-Premises Manager over the engine network.

If static IPs are issued, use the 10.0.0.11-199 range.

If an Advanced Malware Detection On-Premises Manager has been installed in the network, the user has to specify its domain name. For example, if the domain name of the Advanced Malware Detection On-Premises Manager is **amd-manager.mycompany.com**, then this name should be provided.

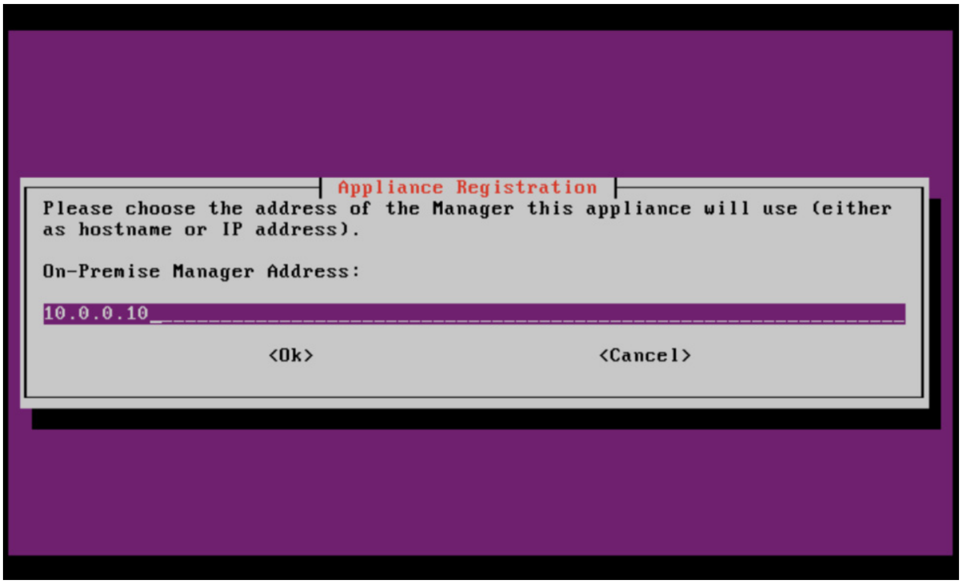
Note that, as part of the installation of the Advanced Malware Detection On-Premises Manager, the names

- update.amd-manager.mycompany.com
- log.amd-manager.mycompany.com
- user.amd-manager.company.com

should have also been registered as aliases of **amd-manager.mycompany.com**.

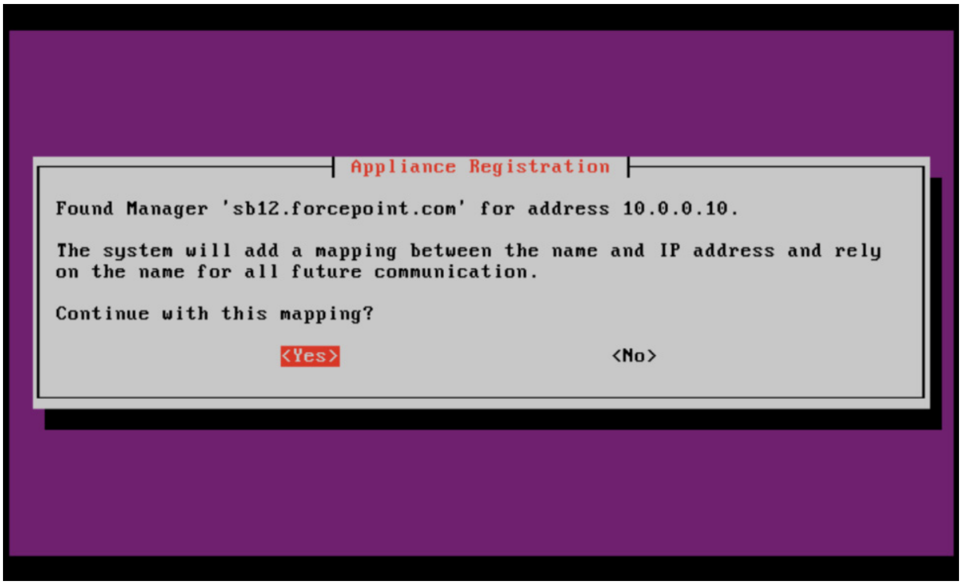
In case an Advanced Malware Detection On-Premises Manager has been installed in the network, but no FQDN has been assigned to it (or the DNS server is not able to resolve its domain name), then the IP address of the Manager can be provided to the installer, as shown below.

4. The Advanced Malware Detection On-Premises Manager's IP address has automatically been assigned to **10.0.0.10**. Type this address when prompted for the On-Premises Manager Address.



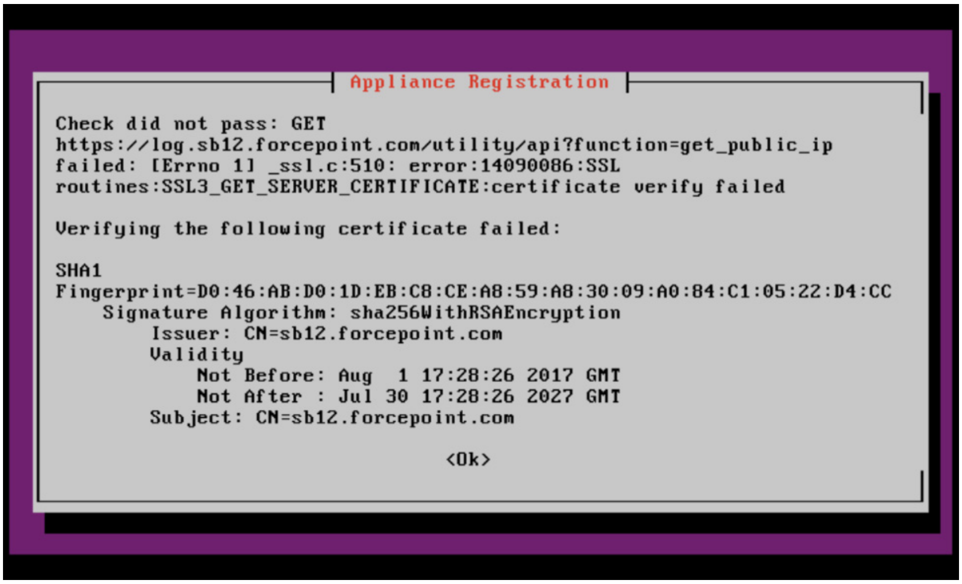
```
Appliance Registration
Please choose the address of the Manager this appliance will use (either
as hostname or IP address).

On-Premise Manager Address:

10.0.0.10_

        <Ok>                        <Cancel>
```

5. Select **Yes** to configure the Advanced Malware Detection On-Premises Engine by using the IP address of the Advanced Malware Detection On-Premises Manager.



```
Appliance Registration

Found Manager 'sb12.forcepoint.com' for address 10.0.0.10.

The system will add a mapping between the name and IP address and rely
on the name for all future communication.

Continue with this mapping?

        <Yes>                        <No>
```

6. You may see a certificate error page similar to the screen below:

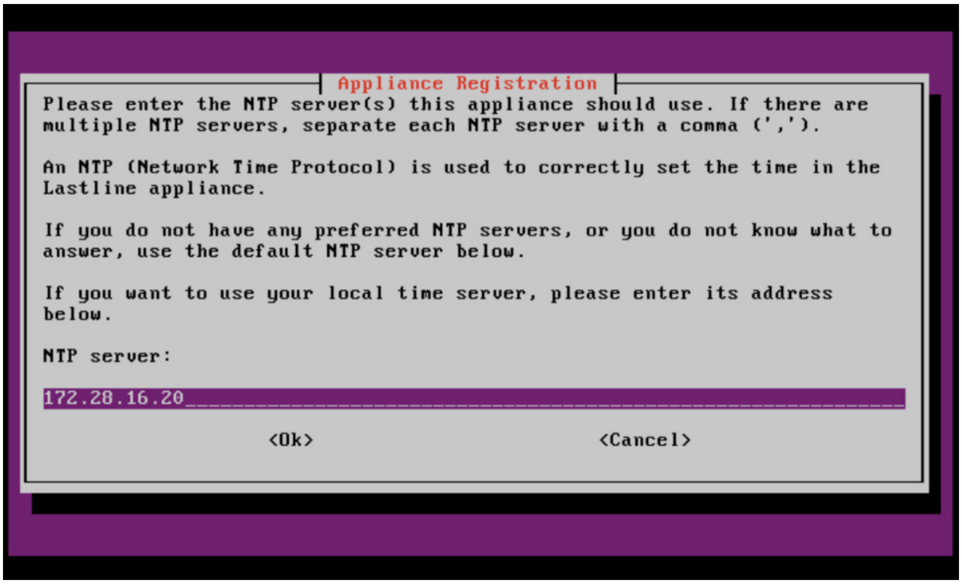


```
Appliance Registration

Check did not pass: GET
https://log.sb12.forcepoint.com/utility/api?function=get_public_ip
failed: [Errno 1] _ssl.c:510: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

Verifying the following certificate failed:

SHA1
Fingerprint=D0:46:AB:D0:1D:EB:C8:CE:A8:59:A8:30:09:A0:84:C1:05:22:D4:CC
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=sb12.forcepoint.com
        Validity
            Not Before: Aug  1 17:28:26 2017 GMT
            Not After : Jul 30 17:28:26 2027 GMT
        Subject: CN=sb12.forcepoint.com

                              <Ok>
```

Select **Ok** on this screen, then **Yes** on the next screen when asked to trust the certification. Verifying that the certificate failed does not negatively impact the Advanced Malware Detection On-Premises Engine registration process.

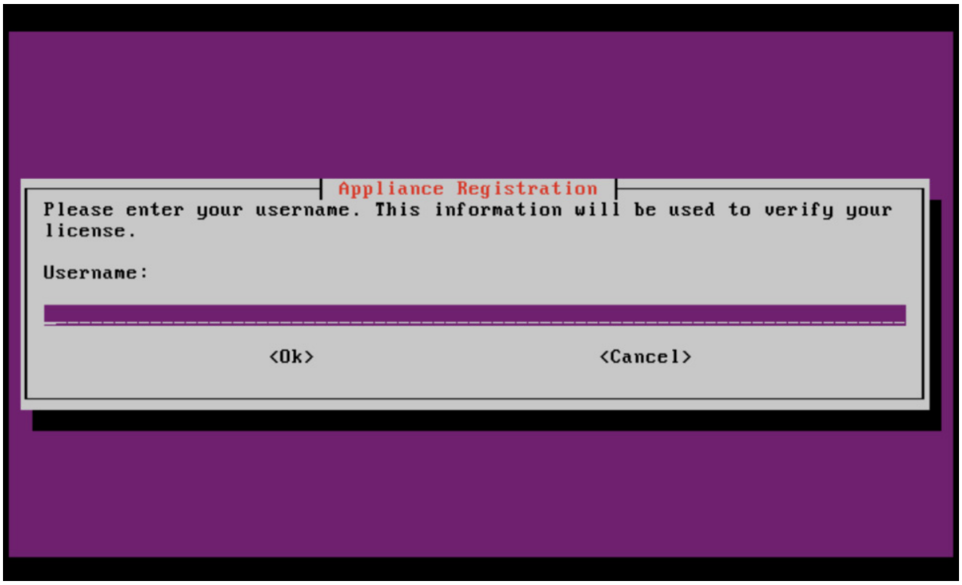
7. Type the IP address for the NTP server, then select **Ok**.

   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.

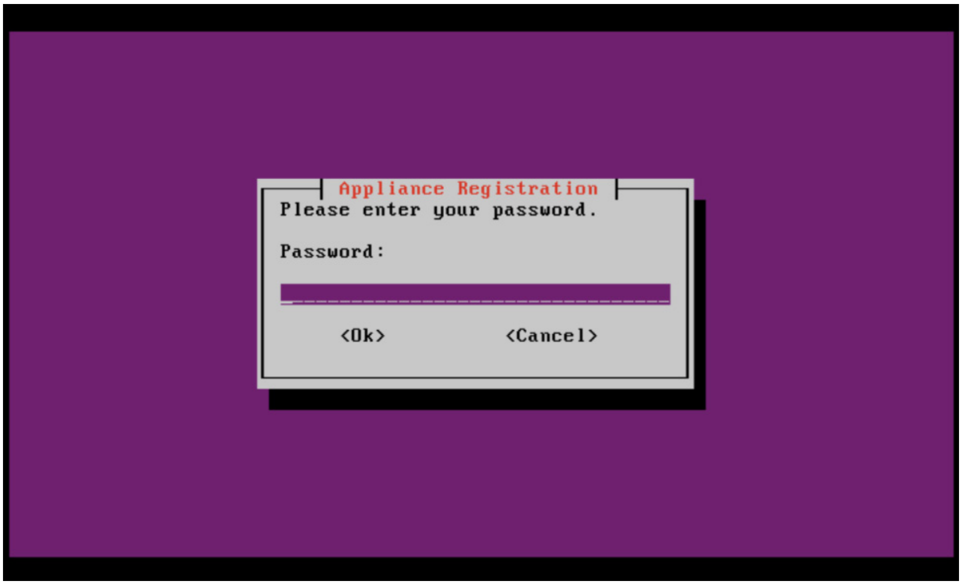


```
Appliance Registration
Please enter the NTP server(s) this appliance should use. If there are
multiple NTP servers, separate each NTP server with a comma (',').

An NTP (Network Time Protocol) is used to correctly set the time in the
Lastline appliance.

If you do not have any preferred NTP servers, or you do not know what to
answer, use the default NTP server below.

If you want to use your local time server, please enter its address
below.

NTP server:

172.28.16.20_________________________________________________________

                <Ok>                          <Cancel>
```

8. Verify your readiness to complete the configuration process. Select **Yes** to begin the system configuration and product registration. Internet access is required to complete the rest of the registration process.
9. Type the username and password provided during registration. Click **Ok**.

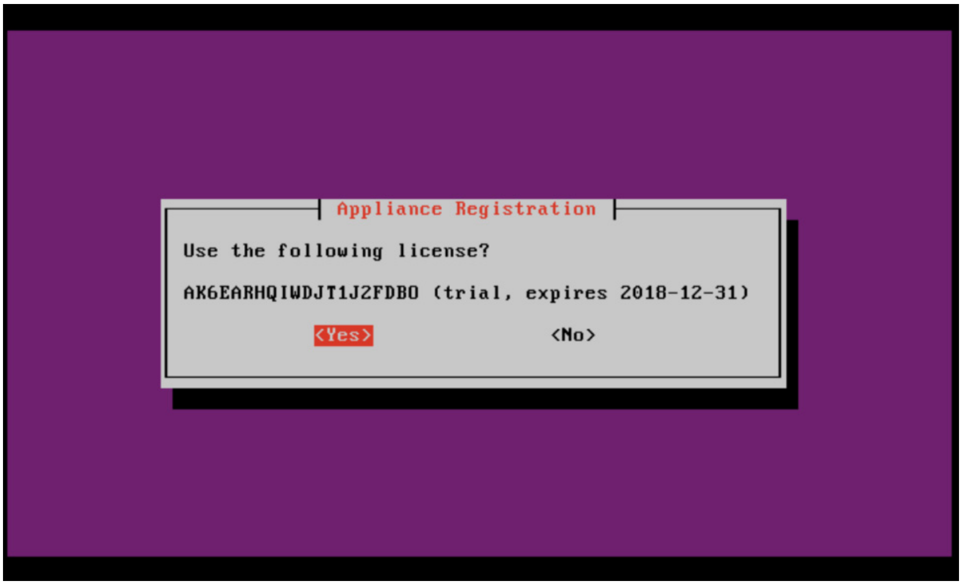


```
Appliance Registration
Please enter your username. This information will be used to verify your
license.

Username:

              <Ok>                              <Cancel>
```



```
Appliance Registration
Please enter your password.

Password:

    <Ok>              <Cancel>
```

10. If the provided credentials are valid, you are shown the available license keys. If the list of license keys is not retrieved correctly, please contact Forcepoint Support, mentioning the corresponding error message.

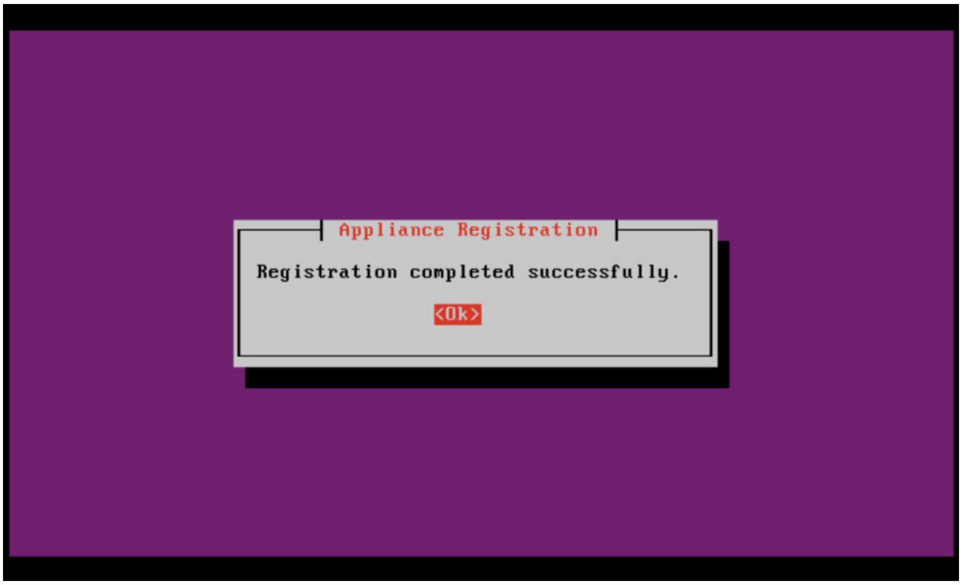


```
Use the following license?

AK6EARHQIWDJT1J2FDBO (trial, expires 2018-12-31)
```

If the license information is correct, select **Yes**.

If you select **No**, you are asked if you want to restart the configuration process. Select **Yes** to restart the configuration, or **No** to stop the configuration process.

11. The setup program applies the configuration to the machine. This process may take several minutes (20 – 40) depending on network connectivity and system characteristics.



```
Registration completed successfully.
```

The registration is complete. At this point, users can access the user portal:

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

If any error message is displayed, please refer to *Error handling*, page 13.

4 System Administration

The Advanced Malware Detection On-Premises Engine 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 Engine installation wizard

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

```
forcepoint_register
```

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

Error handling

If any error message is shown, please contact Forcepoint Support.

5 Software Upgrades

Installation Guide | AMD OP Engine | v1.1

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.

6 Copyrights and Trademarks

Installation Guide | AMD OP Engine | 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

Other acknowledgments

This Forcepoint product uses the third-party software listed in this file.