Advanced Malware Detection and Protection

2.1

On-Premises Deployment Guide

Revision A

Contents

- Introduction on page 2
- Deployment prerequisites on page 4
- Licensing Forcepoint AMDP on page 5
- Downloading installation file on page 6
- Software installation on page 6
- Manager configuration on page 27
- Engine configuration on page 28
- Software updates on page 32
- Backup and Restore on page 35
- Microsoft Office licensing on page 36
- Web Security licensing and configuration on page 41
- Configuring AMDP on Secure SD-WAN via SMC GUI on page 43
- Admin Web Portal on page 46

Introduction

Forcepoint Advanced Malware Detection and Protection (AMDP) is an advanced file sandbox, sometimes referred to as a “Network Sandbox”, designed to detect zero-day malicious files currently not detectable via traditional signature based solutions and static analysis alone.

AMDP is integrated into Forcepoint’s Web Security and Secure SD-WAN products for fast and easy setup.

This guide describes the process to install the AMDP On-Premises Manager and Engine components on hardware provided by the customer.

The AMDP 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 AMDP On-Premises Manager stores, within the customer's data center, all the information regarding the detection of infected hosts and the analysis of software files.

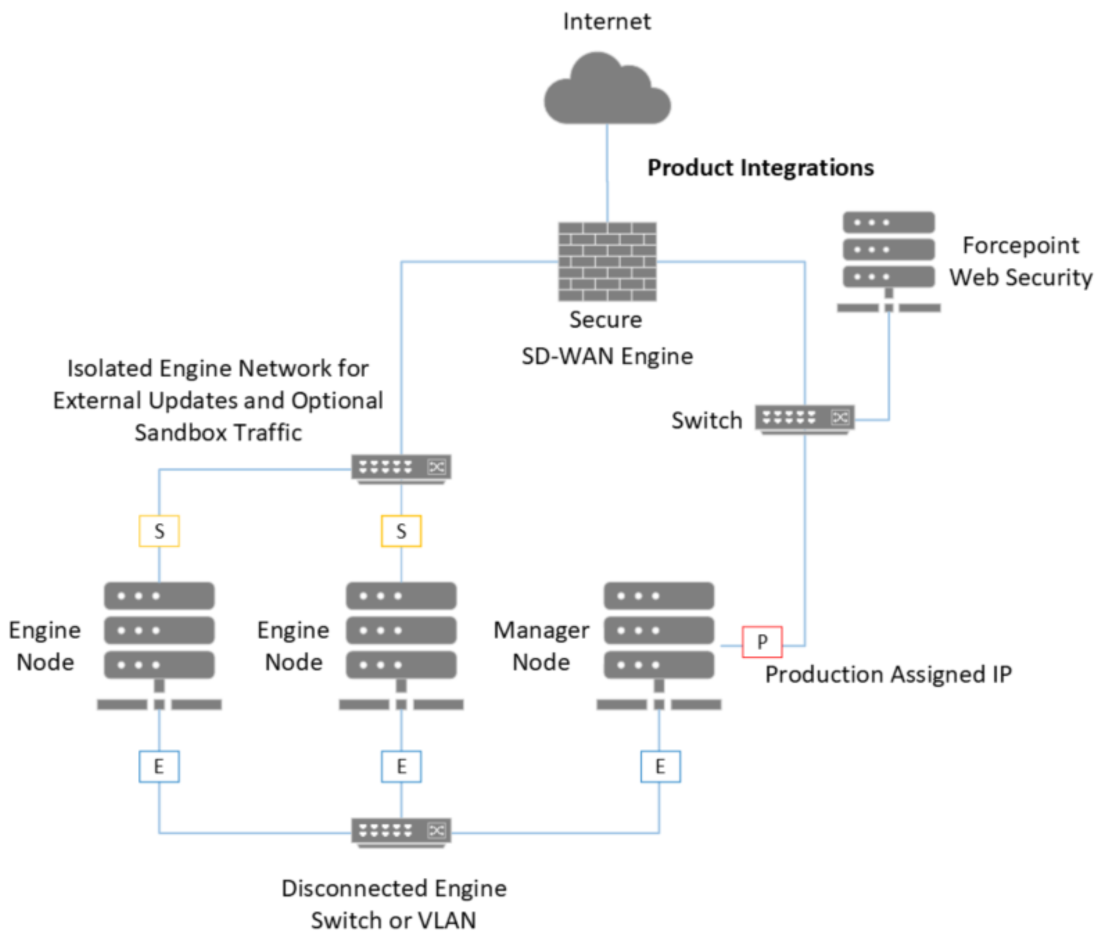
The AMDP On-Premises Manager collects information from Forcepoint appliances, processes it, and presents it to the End User. More precisely, the AMDP On-Premises Manager receives files (i.e., executables and documents) that are received or downloaded by the users and passes them to an Analysis Engine. The results of the analysis are collected and presented to the Admin 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 AMDP On-Premises Engine component receives files (i.e., executables and documents) from the AMDP On-Premises Manager. It runs these files, then returns analysis results back to SWG and Secure SD-WAN. Alerts can be configured to notify when AMDP detects an issue.

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.

Network topology

Integrating AMDP with Secure SD-WAN Engine

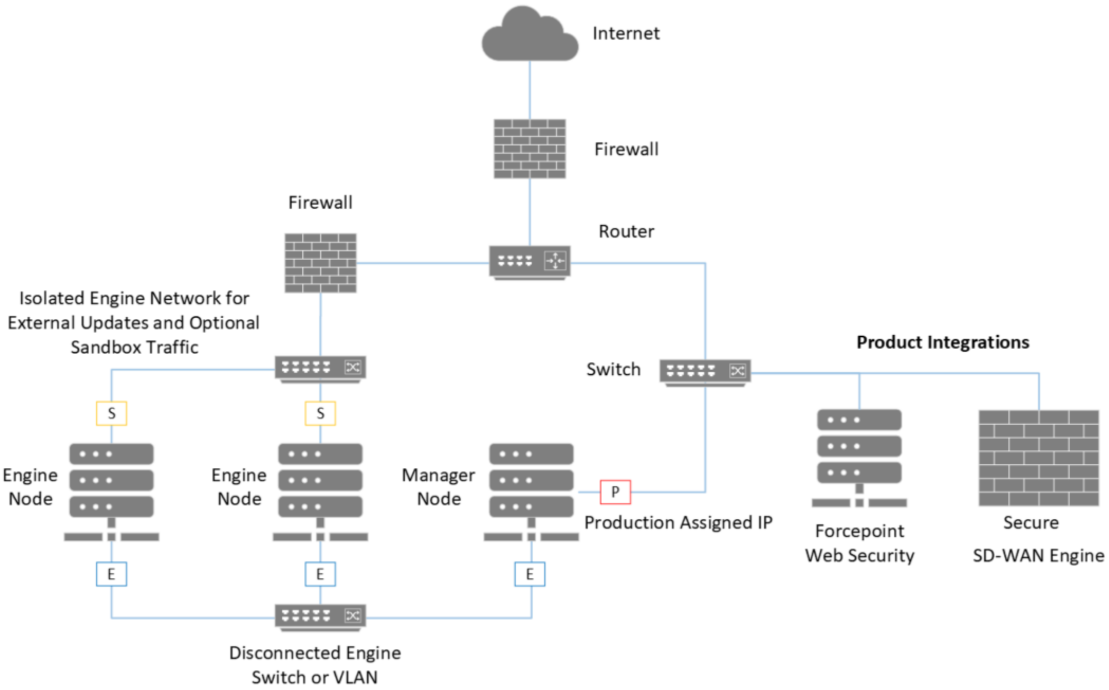


P - Primary / Production Network

E- Engine Network

S- Sandbox Network

Integrating AMDP with third party router and firewall



P - Primary / Production Network

E- Engine Network

S- Sandbox Network

Note

The Engine network should be isolated as the sandbox machines execute here.

Deployment prerequisites

The following system requirements provide the minimum specifications for optimal performance and effectiveness.

Manager

- CPU: 10 cores (20 threads) Intel Xeon, Broadwell or newer.
  For example: Xeon Silver 4114
- RAM: 64 GB
- NIC: 2
- Storage: 256 GB SSD, RAID 10 recommended

Engine

- CPU: 18 cores (36 threads) Intel Xeon, Broadwell or newer.
  For example: Xeon E5-2686 v4, or 2x Xeon Silver 4114
- RAM: 96 GB

- NIC: 2
- Storage: 256 GB SSD, RAID 10 recommended

> **Note**
>
> Engine cannot be installed on a VM.

Firewall Rules

If a firewall is being used, make sure it allows (permits) the following domain names.

- app.recordedfuture.com
- sandbox.recordedfuture.com
- recordedfuture.zendesk.com
- support.recordedfuture.com
- securitytrails.com
- private.tria.ge
- recordedfuture.phishfort.com
- admin.recordedfuture.com/enterprise-admin/
- api.recordedfuture.com (162.159.128.62 and 162.159.129.62)
- forcepoint.com
- hatching.dev
- 1.1.1.1 (Cloudfare DNS used as DNS Resolver)
- 8.8.8.8, 8.8.4.4 (Google DNS used as DNS Resolver)

Remember

AMDP requires at least NGFW and SMC version 7.1.1.

Licensing Forcepoint AMDP

Forcepoint AMDP requires a valid License Key. The License Key may be entered on installation but this step can be skipped and entered post-installation.

If an installation skips the License Key entry, the product defaults to running in an evaluation mode for a limited time and will function for a short evaluation period.

> **Note**
>
> Installations without a valid License Key will not receive updates.

Both the AMDP Manager and AMDP Engine require a valid License Key. Your AMDP On-Premises License Key can be found in the Support Hub Account License section.

Evaluation License

When installed without a License Key, AMDP On-Premises will automatically switch to an Evaluation License. After 60 days of evaluation, the service will no longer accept file submissions. Automatic updates are disabled in AMDP On-Premises Evaluation mode.

The service will enable automatic updates once a legitimate License Key is entered. Your AMDP On-Premises License Key can be found in the Support Hub Account License section.

> **Note**
>
> A valid Microsoft Office License Key is required for AMDP Engine. As Forcepoint is not a reseller of Microsoft Office License Keys, please use your organization's existing Microsoft License Keys or point AMD to your KMS. AMDP also supports O365 Licenses. This is needed to scan MS Office document types. If MS documents are not needed then this step can be skipped.

Downloading installation file

Steps

1) Go to Forcepoint Customer Hub

2) Log in using your existing user account.

3) Download the Forcepoint AMDP installation (`.iso`) file from **Downloads** > **AMDP On-Premises** section of Forcepoint Customer Hub.

Software installation

The Advanced Malware Detection and Protection software provisions the base system from an ISO image using an automated installation process. This is a combined installation media for both the Manager and Engines. The choice of system role is configured from the console after the base system is installed during registration. Before starting the installation, you must download an official copy of the latest Advanced Malware Detection and Protection 2.1 `.iso` file from **Downloads** > **AMDP On-Premises** section of Forcepoint Customer Hub. The image may be burned onto a bootable DVD, or otherwise mounted to the system to be installed.

To install the Advanced Malware Detection and Protection software, 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, and then presents you with a login prompt at the system console.

Installing Manager

1) Log into the console of the host using the following credentials:

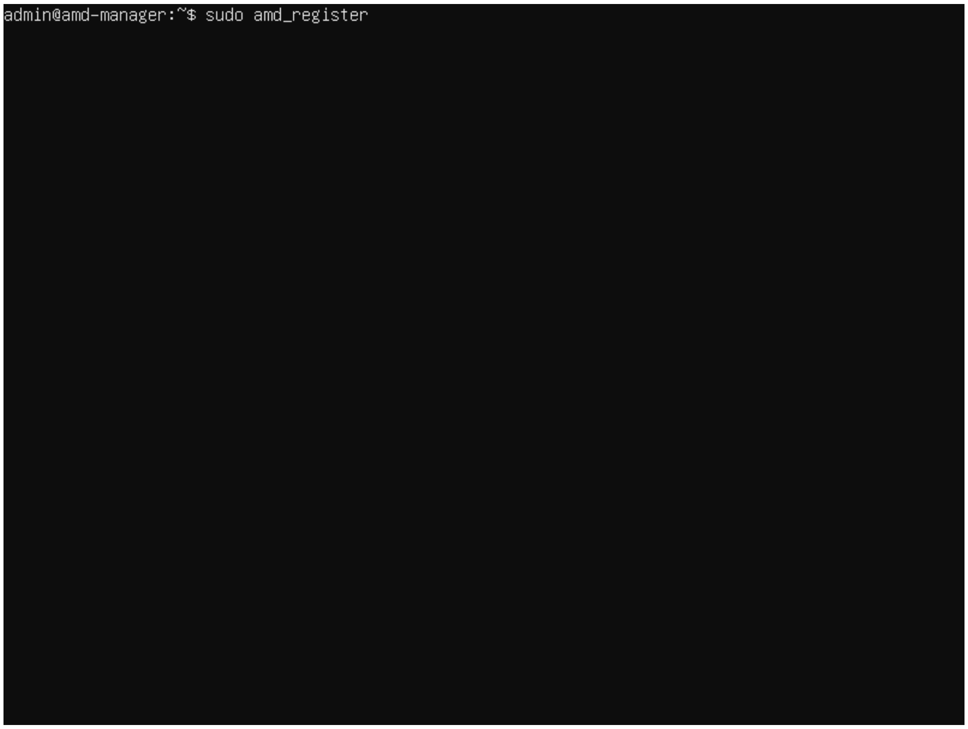
   a) username: admin

   b) password: **P!L)TP@ssw0rd**

Important

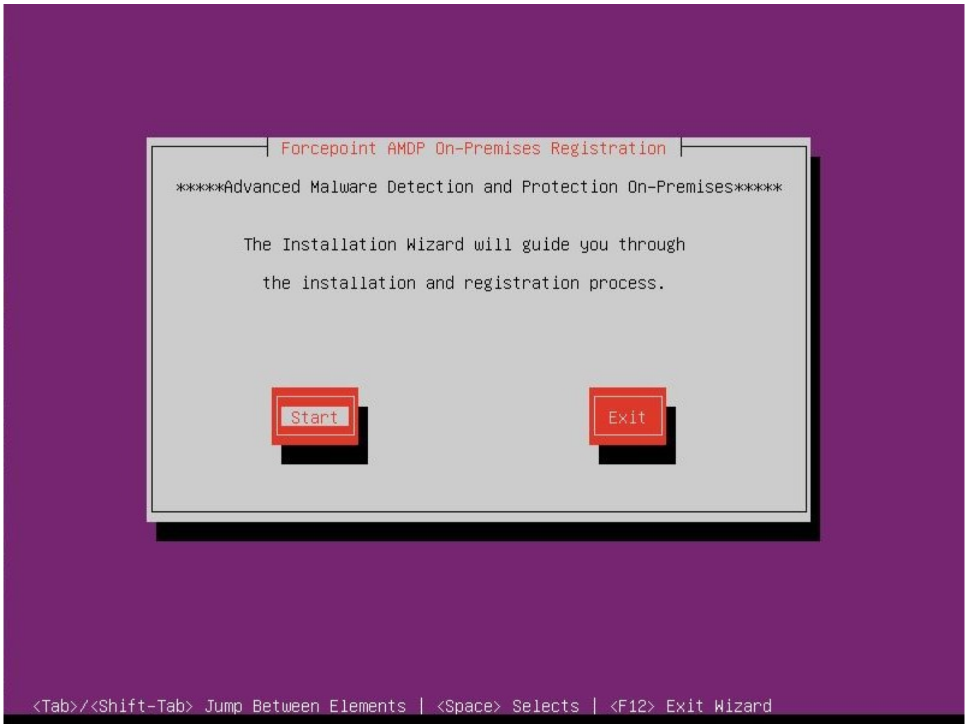
This is the default admin login credentials for AMDP console. Change the default password to a password that is unique to your organization.

2) Run the **sudo amd_register** command to start the guided installation and registration process.



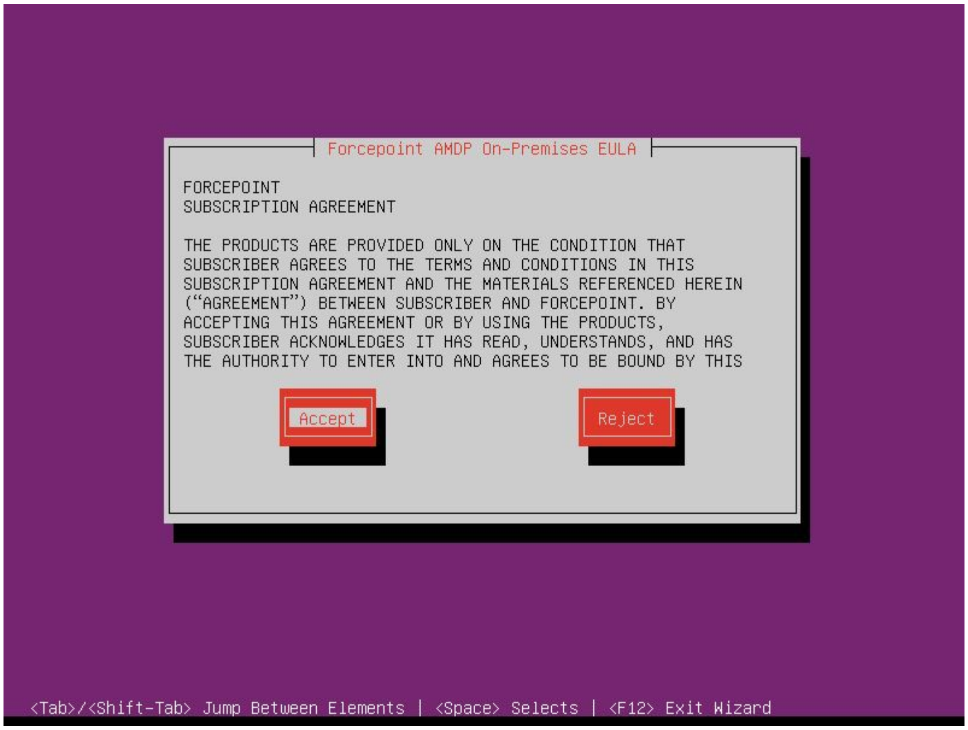
```
admin@amd-manager:~$ sudo amd_register
```

3) The installation process starts at the **Welcome** screen. When you are ready to begin the installation process, select **Start**. This wizard will gather information about the system role and install the appropriate components. The wizard provides the initial system configuration which is then further tailored with the **amd_setup** utility.



```
Forcepoint AMDP On-Premises Registration

*****Advanced Malware Detection and Protection On-Premises*****

The Installation Wizard will guide you through

the installation and registration process.

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

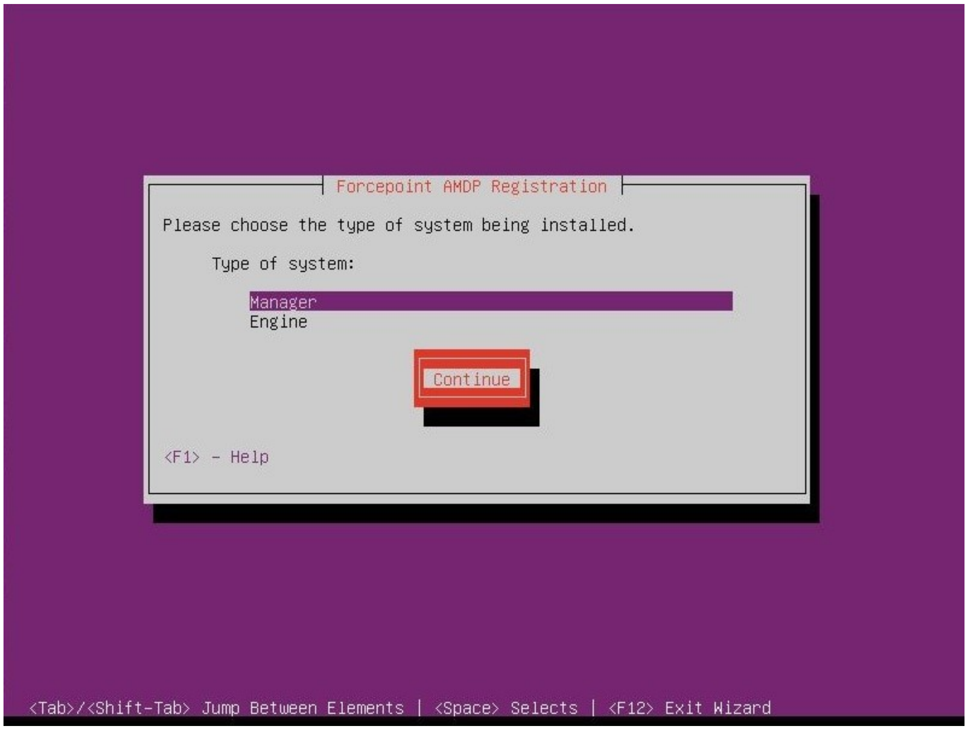
4) Read the Forcepoint Subscription Agreement and select **Accept** to proceed with the installation.



```
Forcepoint AMDP On-Premises EULA

FORCEPOINT
SUBSCRIPTION AGREEMENT

THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT
SUBSCRIBER AGREES TO THE TERMS AND CONDITIONS IN THIS
SUBSCRIPTION AGREEMENT AND THE MATERIALS REFERENCED HEREIN
(“AGREEMENT”) BETWEEN SUBSCRIBER AND FORCEPOINT. BY
ACCEPTING THIS AGREEMENT OR BY USING THE PRODUCTS,
SUBSCRIBER ACKNOWLEDGES IT HAS READ, UNDERSTANDS, AND HAS
THE AUTHORITY TO ENTER INTO AND AGREES TO BE BOUND BY THIS

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

5) Choose the type of system to install. Select **Manager**, and select **Continue** to install and configure the **Manager**.

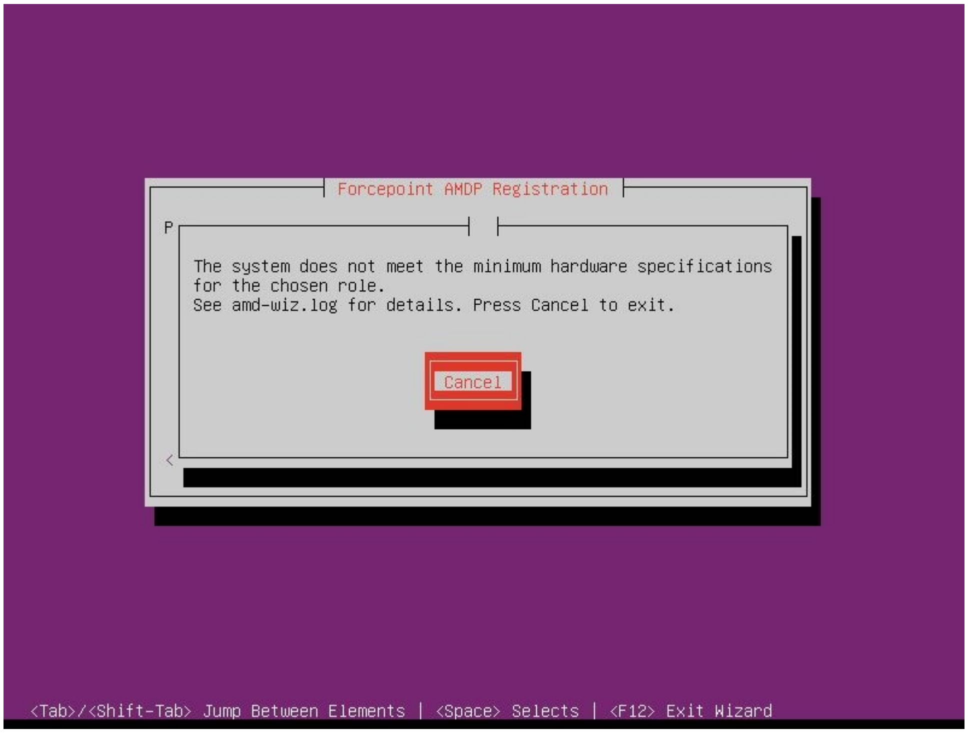
5(a)



```
Forcepoint AMDP Registration

Please choose the type of system being installed.

    Type of system:

        Manager
        Engine

                    <Continue>

<F1> - Help

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

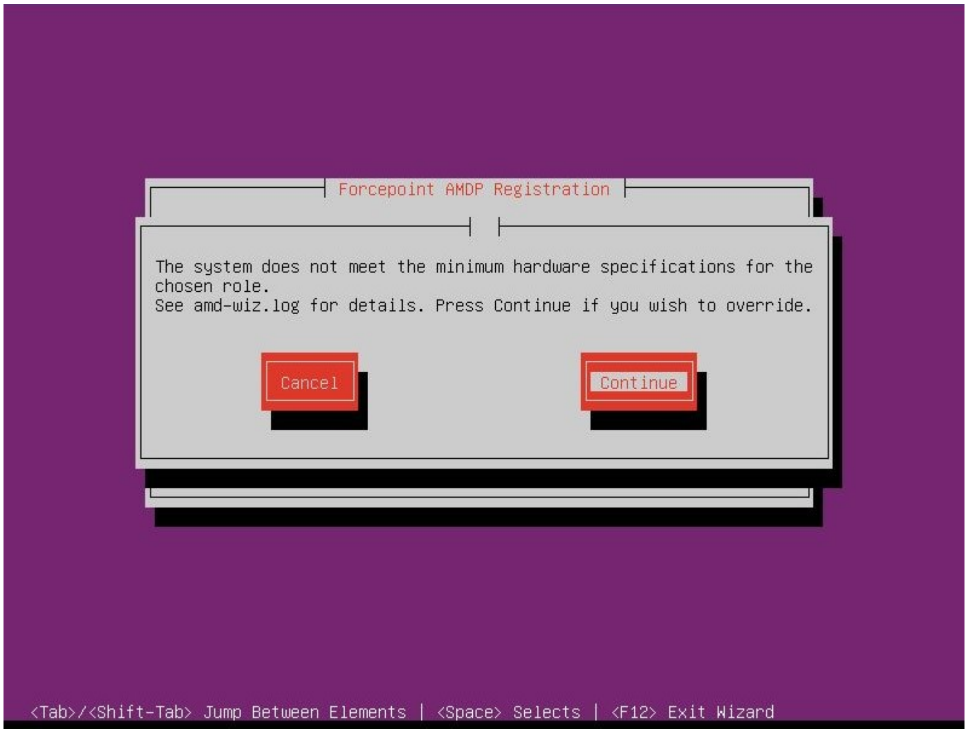
The below wizard checks the server for minimum hardware requirements. If the server does not meet the minimum requirements, either **5(b)** or **5(c)** will appear, depending on the severity of the requirement that is not met. **5(b)** forces the user to cancel the wizard and address the issue, while **5(c)** will allow the user to continue.

5(b)



```
Forcepoint AMDP Registration

The system does not meet the minimum hardware specifications
for the chosen role.
See amd-wiz.log for details. Press Cancel to exit.

                    <Cancel>

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

5(c)

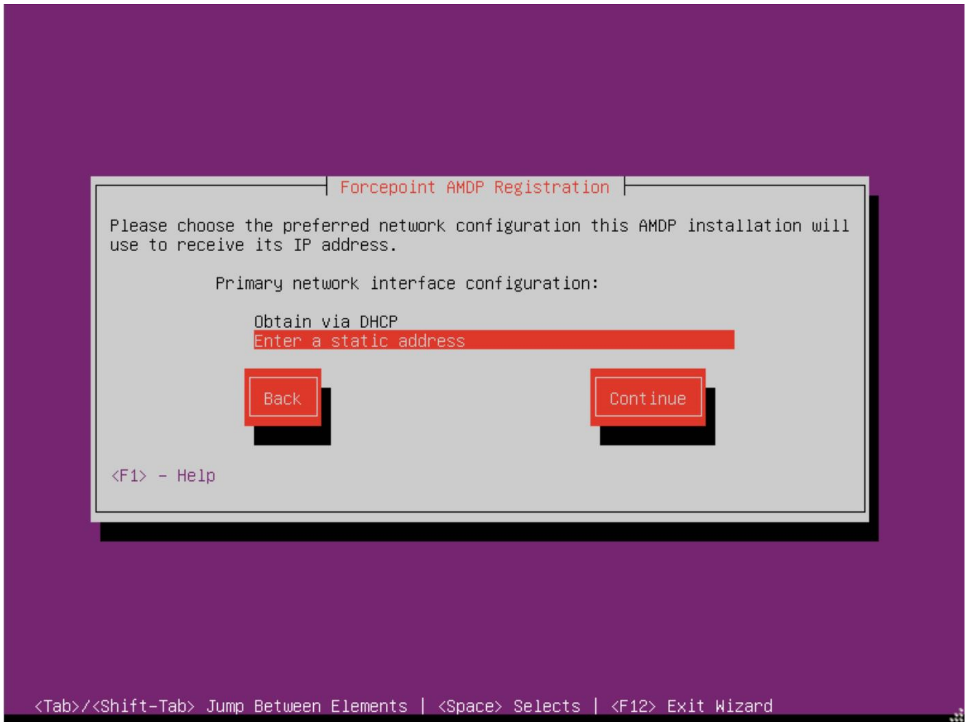


Forcepoint AMDP Registration

The system does not meet the minimum hardware specifications for the chosen role.
See amd-wiz.log for details. Press Continue if you wish to override.

Cancel
Continue
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

6) Choose the preferred network configuration and select **Continue**.



Forcepoint AMDP Registration

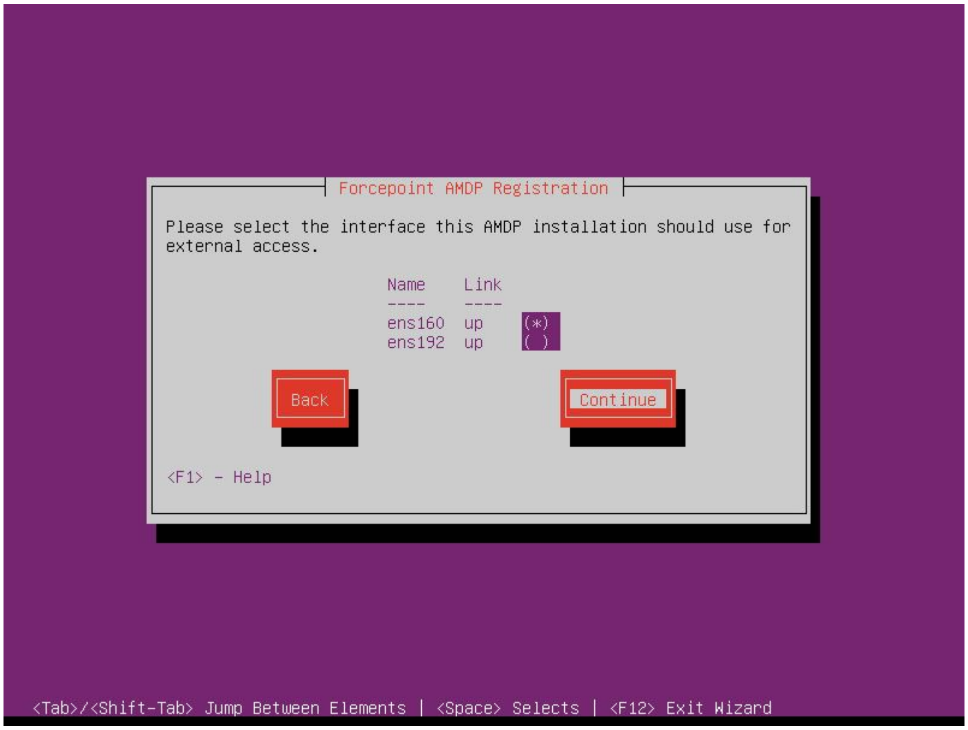
Please choose the preferred network configuration this AMDP installation will use to receive its IP address.

Primary network interface configuration:

Obtain via DHCP
Enter a static address

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

7) Choose the interface for external access and select **Continue**.



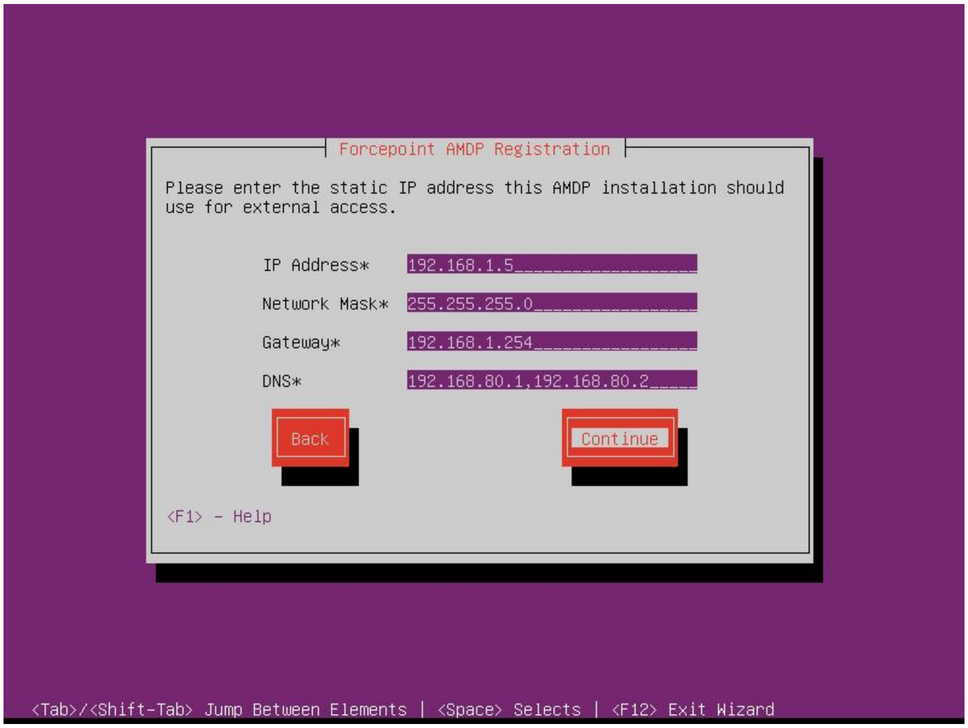
```
Forcepoint AMDP Registration

Please select the interface this AMDP installation should use for
external access.

          Name    Link
          ----    ----
          ens160  up    (*)
          ens192  up    ( )
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

8) On the Primary network interface, enter the static **IP Address**, **Network Mask/CIDR**, **Gateway**, and **DNS** entries. Select **Continue**.

Note

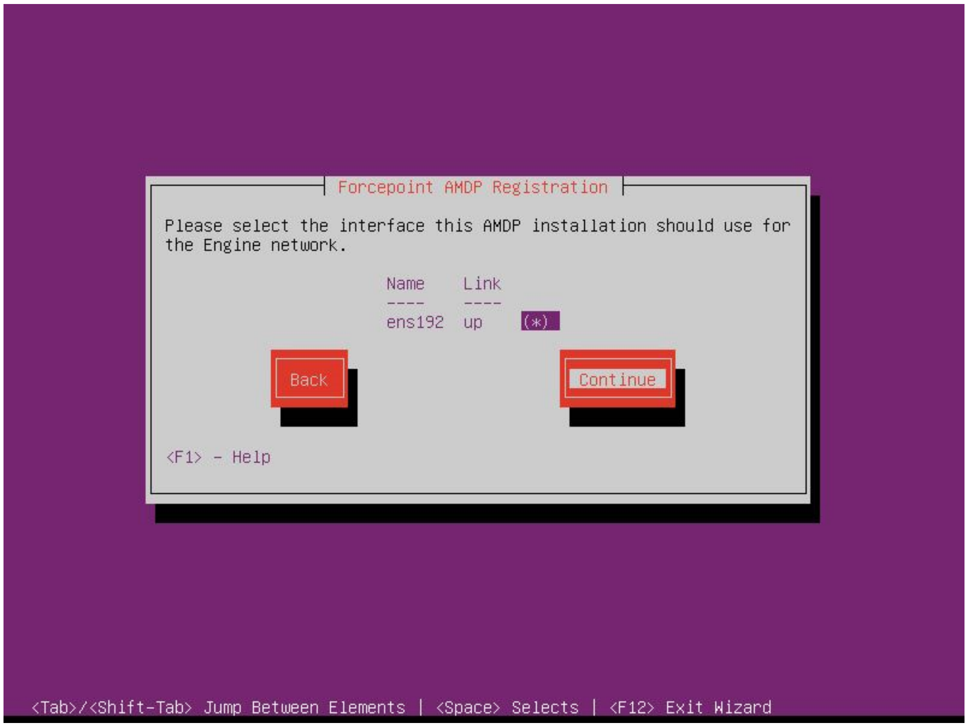
Multiple DNS servers should be comma separated.



```
Forcepoint AMDP Registration

Please enter the static IP address this AMDP installation should
use for external access.

      IP Address*     192.168.1.5
      Network Mask*   255.255.255.0
      Gateway*        192.168.1.254
      DNS*            192.168.80.1,192.168.80.2
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

9) Select the interface for the Engine network and **Continue**.

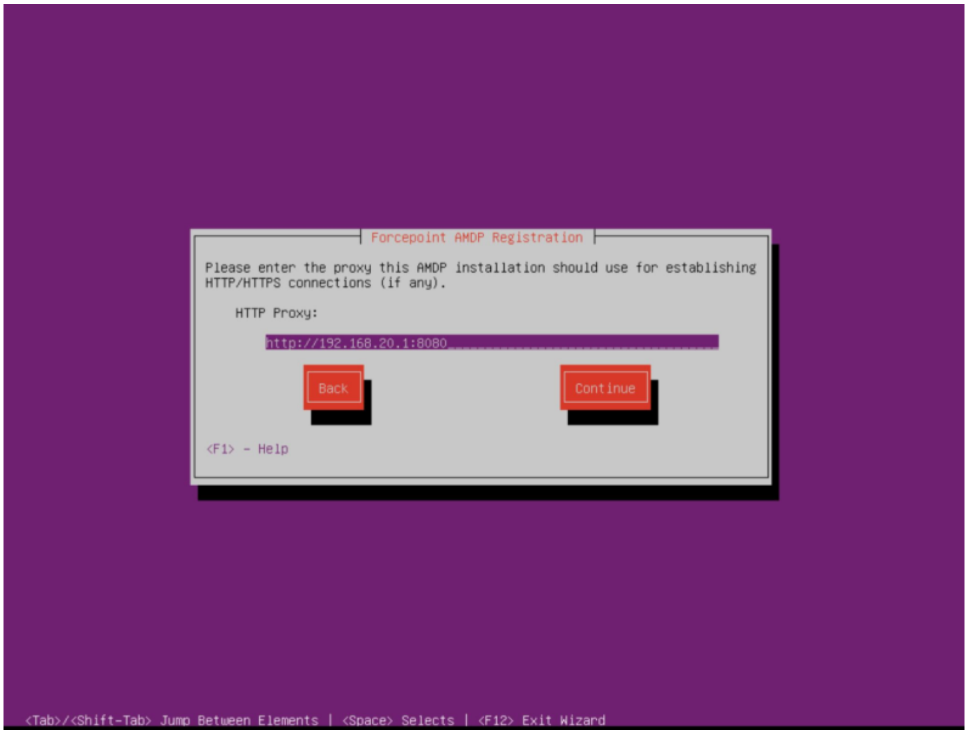


```
Forcepoint AMDP Registration

Please select the interface this AMDP installation should use for
the Engine network.

              Name    Link
              ----    ----
              ens192  up    (*)
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

10) Enter the **HTTP Proxy** address for establishing connection with the update servers. Select **Continue**.

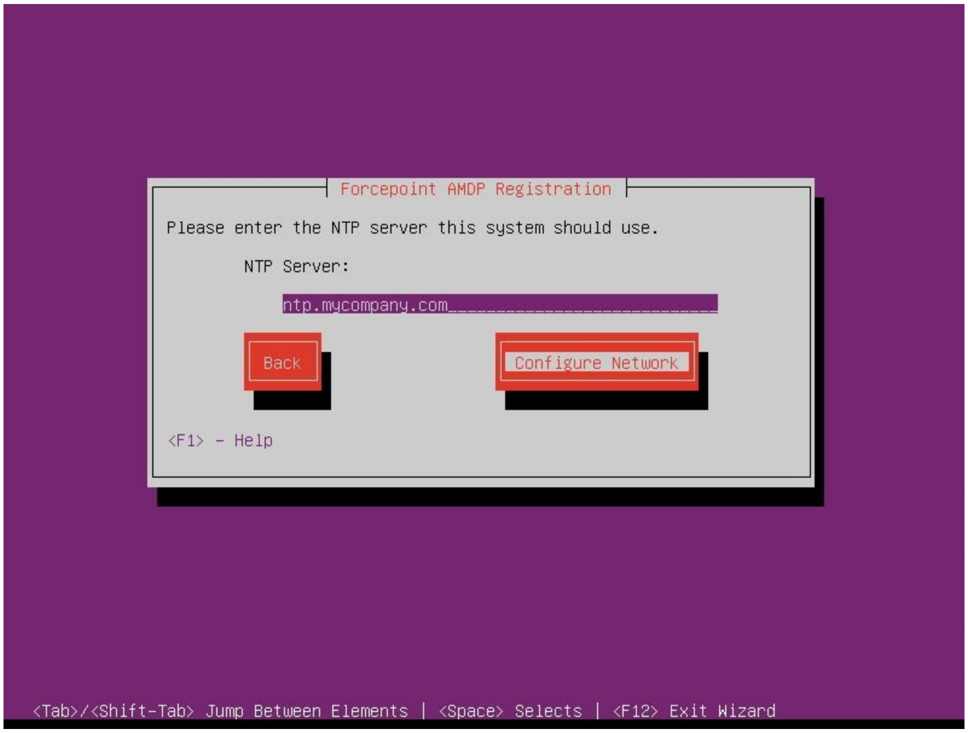
> **Note**
>
> Port 9091 needs to be reachable through the proxy for license verification.



```
Forcepoint AMDP Registration

Please enter the proxy this AMDP installation should use for establishing
HTTP/HTTPS connections (if any).

    HTTP Proxy:

        http://192.168.20.1:8080
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

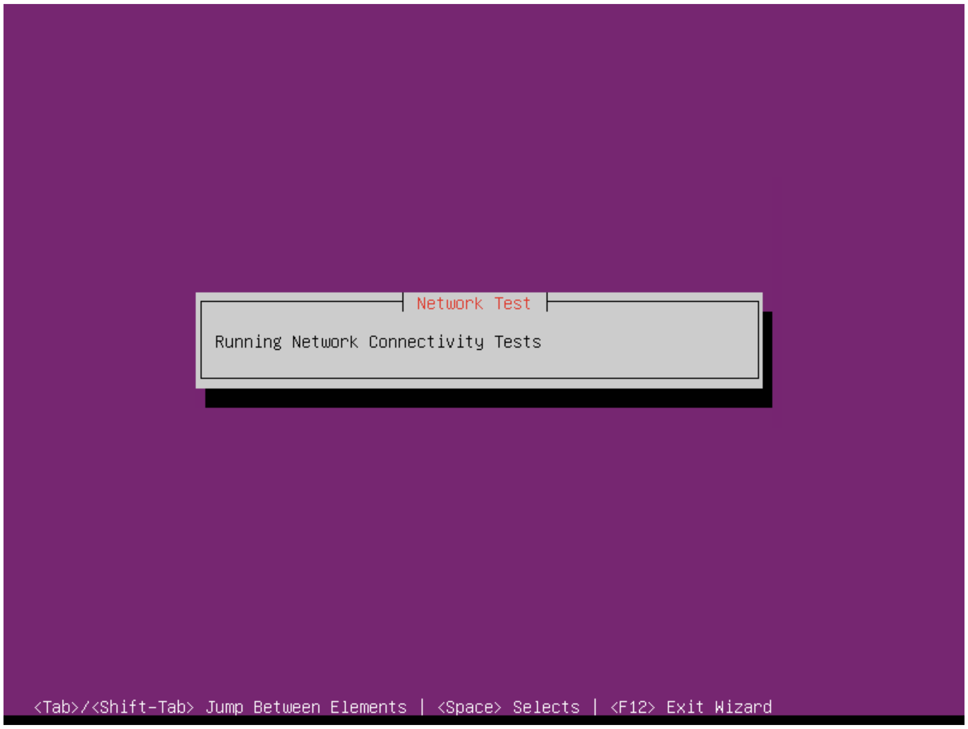
11) Enter the **NTP Server** address and select **Configure Network**.



```
Forcepoint AMDP Registration
Please enter the NTP server this system should use.

        NTP Server:

            ntp.mycompany.com_______________________________
```

Back
Configure Network
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

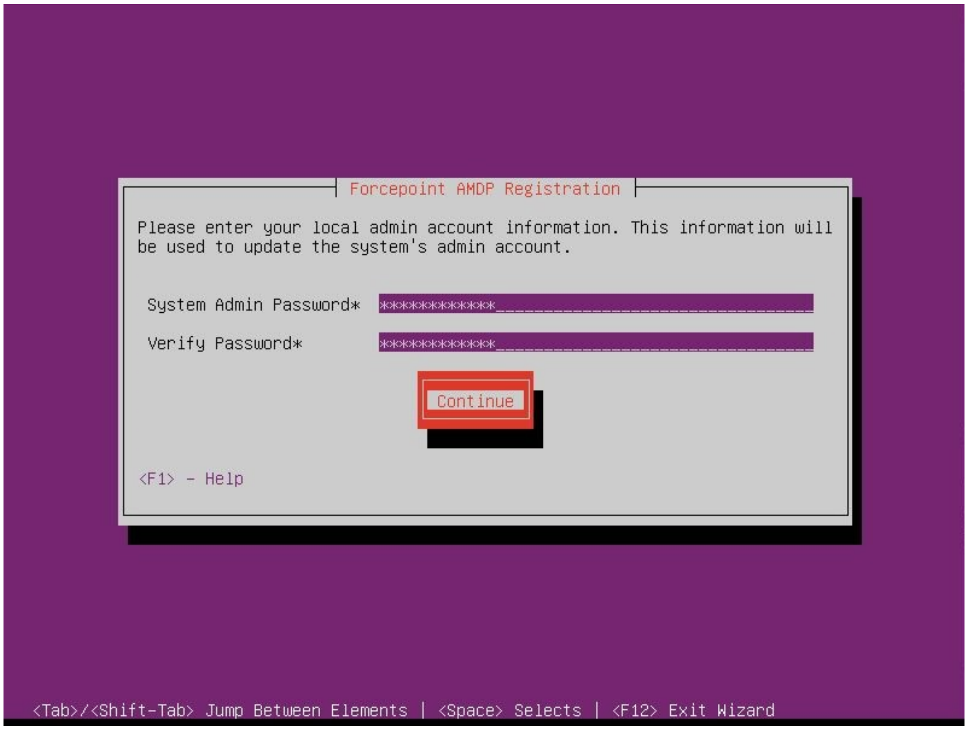
Network connectivity test runs.



```
Network Test
Running Network Connectivity Tests
```

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

12) Update the password for the local admin user to be used for console and ssh access. Select **Continue**.



Forcepoint AMDP Registration

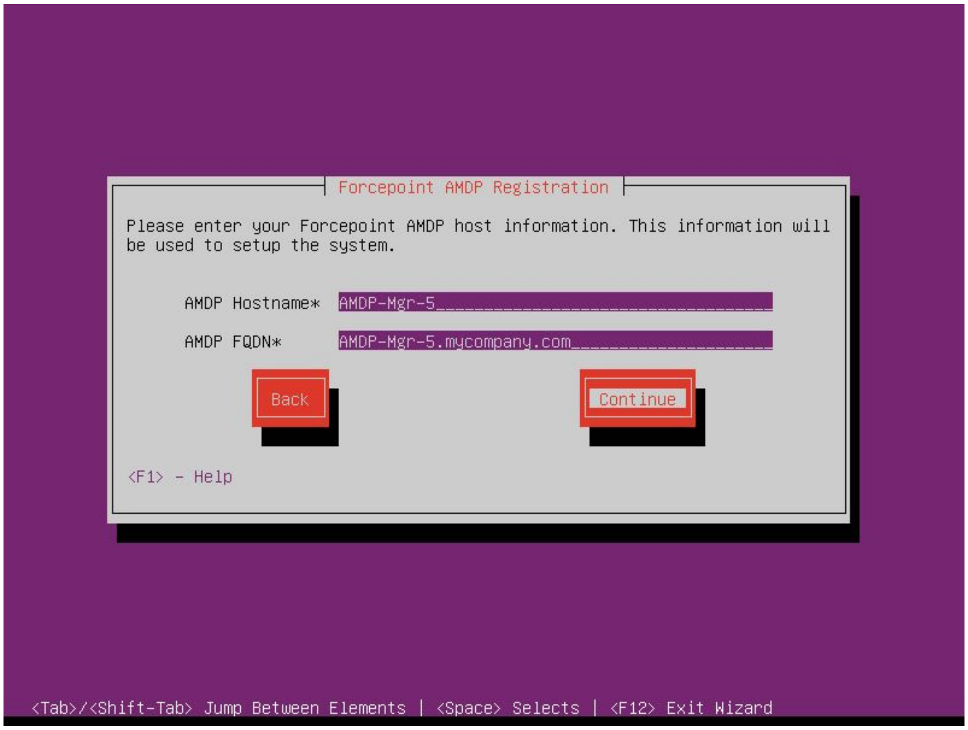
Please enter your local admin account information. This information will be used to update the system's admin account.

System Admin Password* *************

Verify Password* *************

Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

13) Enter your Forcepoint Manager host information and select **Continue**.



Forcepoint AMDP Registration

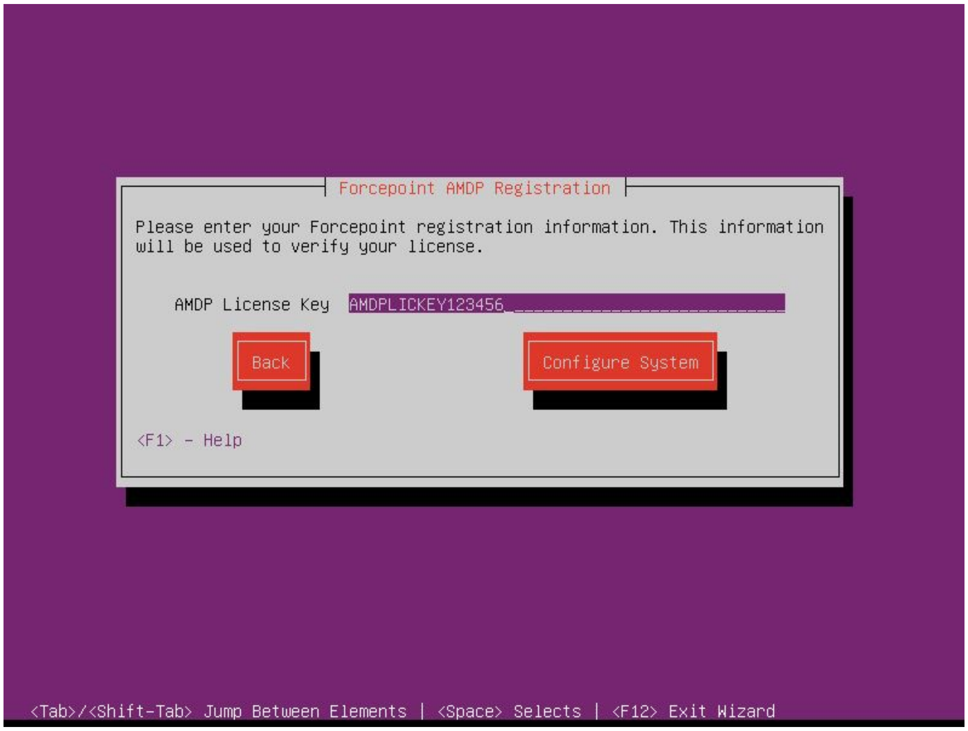
Please enter your Forcepoint AMDP host information. This information will be used to setup the system.

AMDP Hostname* AMDP-Mgr-5

AMDP FQDN* AMDP-Mgr-5.mycompany.com

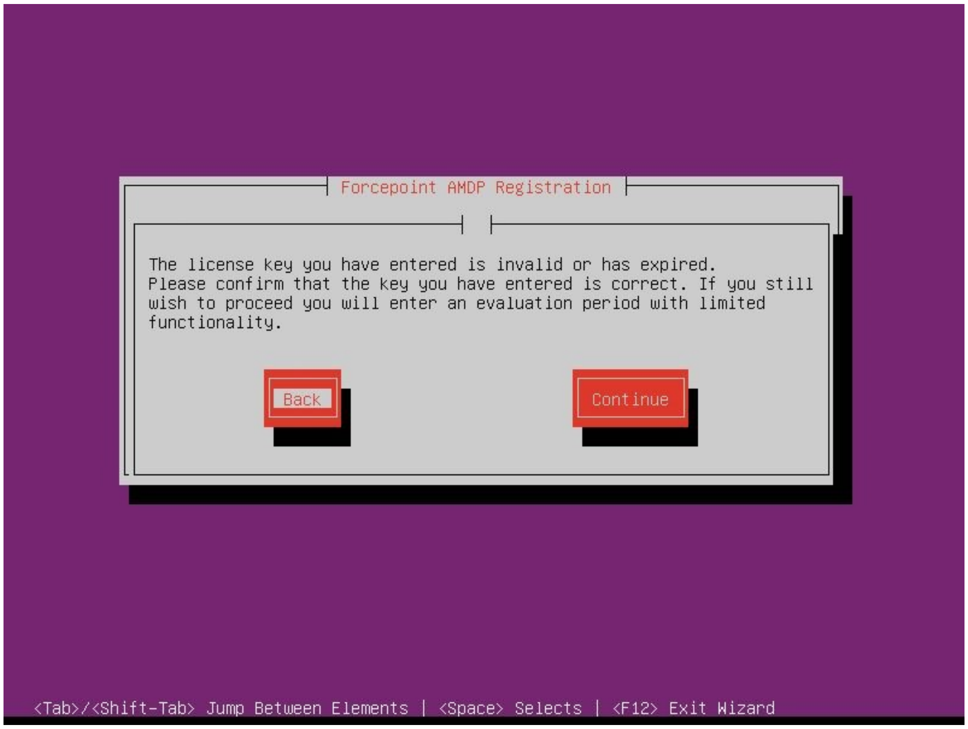
Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

14) Enter your Forcepoint Manager License Key and select **Configure System**.



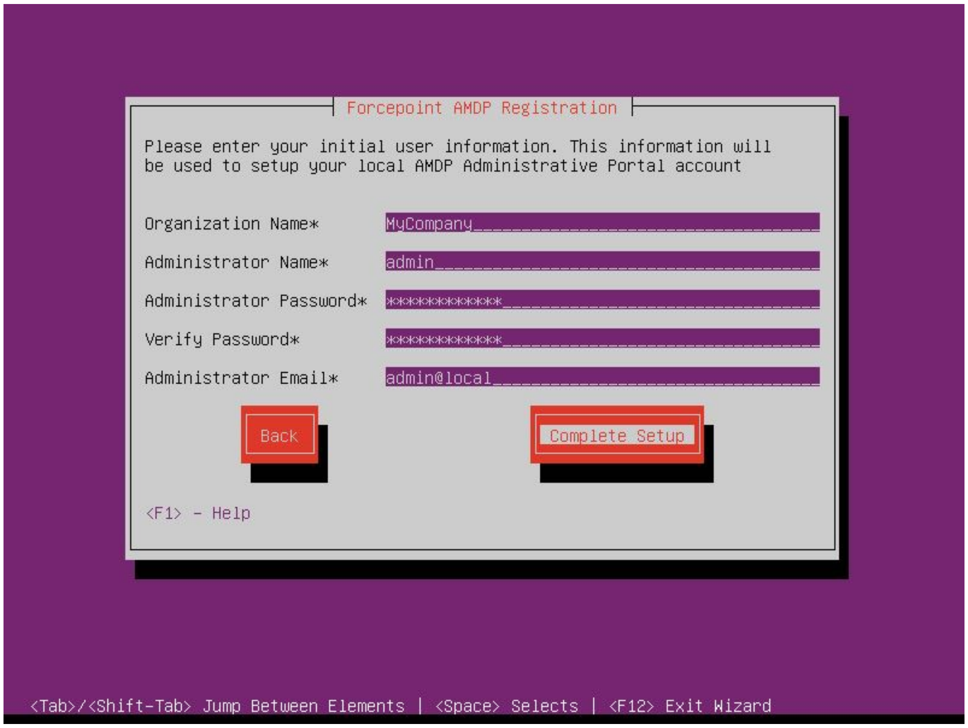
```
Forcepoint AMDP Registration

Please enter your Forcepoint registration information. This information
will be used to verify your license.

   AMDP License Key  AMDPLICKEY123456_

<F1> - Help

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

If the license key is invalid or has expired, you will enter an evaluation period with reduced functionality if you decide to **Continue**. Enter a valid license key to ensure the AMDP solution receives the necessary updates to function correctly.



```
Forcepoint AMDP Registration

The license key you have entered is invalid or has expired.
Please confirm that the key you have entered is correct. If you still
wish to proceed you will enter an evaluation period with limited
functionality.

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

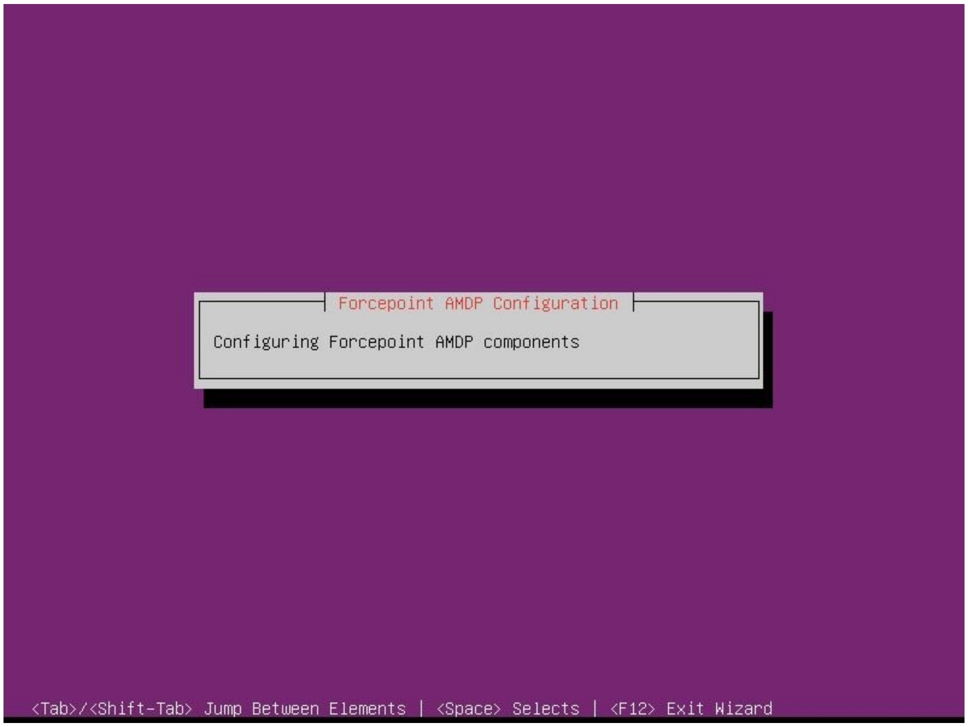
15) To configure the AMDP administrative portal and login account for the portal administrator, enter **Organization Name**, **Administrator Name**, **Administrator Password**, and **Administrator Email**. Select **Complete Setup**.



```
Forcepoint AMDP Registration

Please enter your initial user information. This information will
be used to setup your local AMDP Administrative Portal account

Organization Name*          MyCompany
Administrator Name*         admin
Administrator Password*     ************
Verify Password*            ************
Administrator Email*        admin@local
```

Back
Complete Setup
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

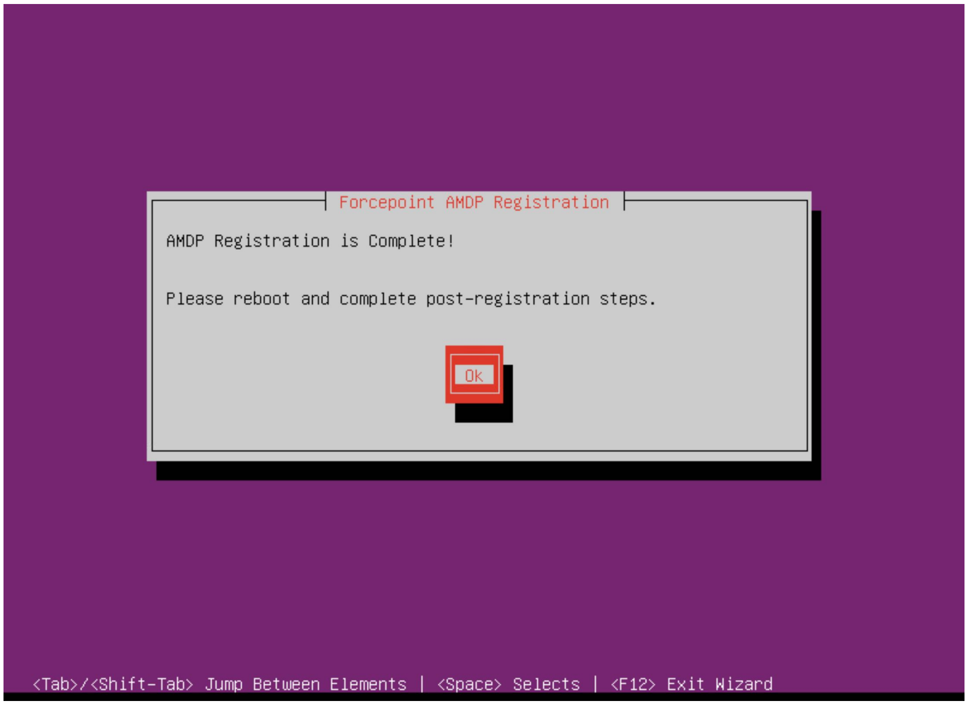
This will configure Forcepoint AMDP components. This step may take a while to complete.



```
Forcepoint AMDP Configuration

Configuring Forcepoint AMDP components
```

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

16) Select **Ok** to exit the Manager Registration wizard. Upon exiting the Manager Registration wizard, you are taken back to the command line.



Forcepoint AMDP Registration

AMDP Registration is Complete!

Please reboot and complete post-registration steps.

Ok
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

Using a Custom Certificate check for AMDP Manager:

As part of installation, a self-signed certificate is generated for the manager. If your organization is able to generate a certificate from a trusted authority, it is possible to install it manually.

Generating a trusted certificate is outside the scope of this document. The primary requirements are three files:

- The signing Certificate Authority's public key in PEM format.
- The signed certificate of the server in PEM format.
- The private key of the server in PEM format.

1) Copy the certificates to the Manager.

   In these examples, the files are uploaded to the home directory of the "**admin**" user, and are named:

   a) Server Cert: `amd-manager-crt.pem`

   b) Server PK: `amd-manager-key.pem`

   c) Signing CA: `ca-cert.pem`

2) Copy the certificate and key files to the correct locations.

```
root@amd-manager:/etc/nginx/ssl# cp ~admin/amd-manager-crt.pem tts.pem
root@amd-manager:/etc/nginx/ssl# cp ~admin/amd-manager-key.pem tts.key
```

3) Add the Signing Certificate to the web server certificate chain by concatenating files.

```
root@amd-manager:/etc/nginx/ssl# cat ~admin/ca-cert.pem >> tts.pem
```

4) Verify the certificate installation was successful.

```
root@amd-manager:/etc/nginx/ssl# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

5) Restart the nginx web server.

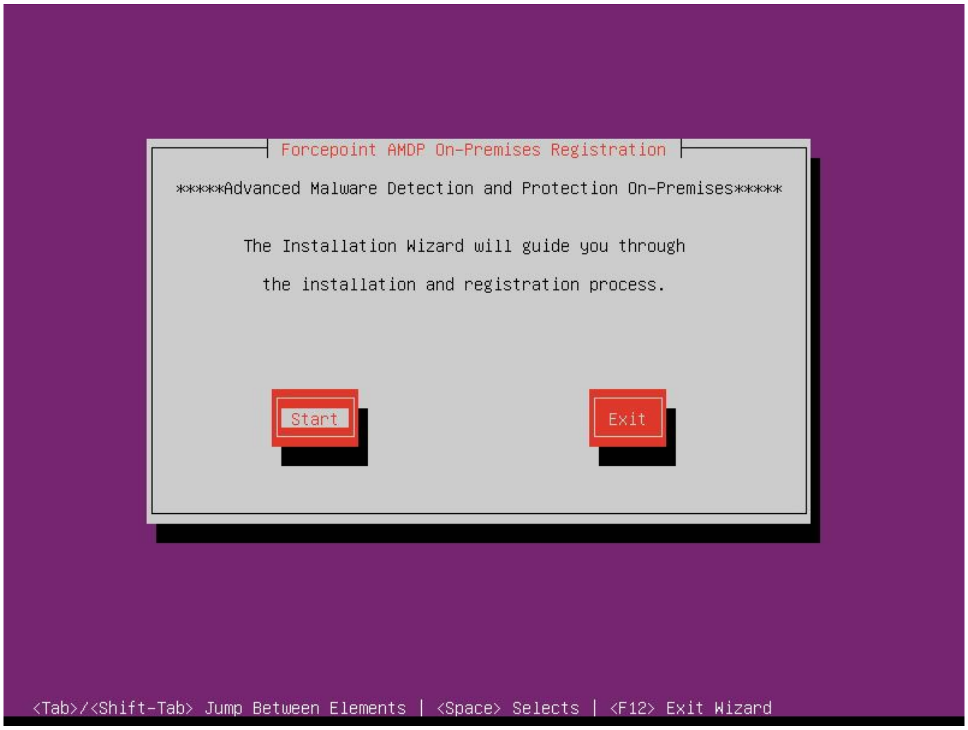
```
root@amd-manager:/home/admin# systemctl restart nginx
```

Installing Engine

1) Run the **sudo amd_register** command to start the guided installation and registration process.

```
admin@amd-manager:~$ sudo amd_register
```

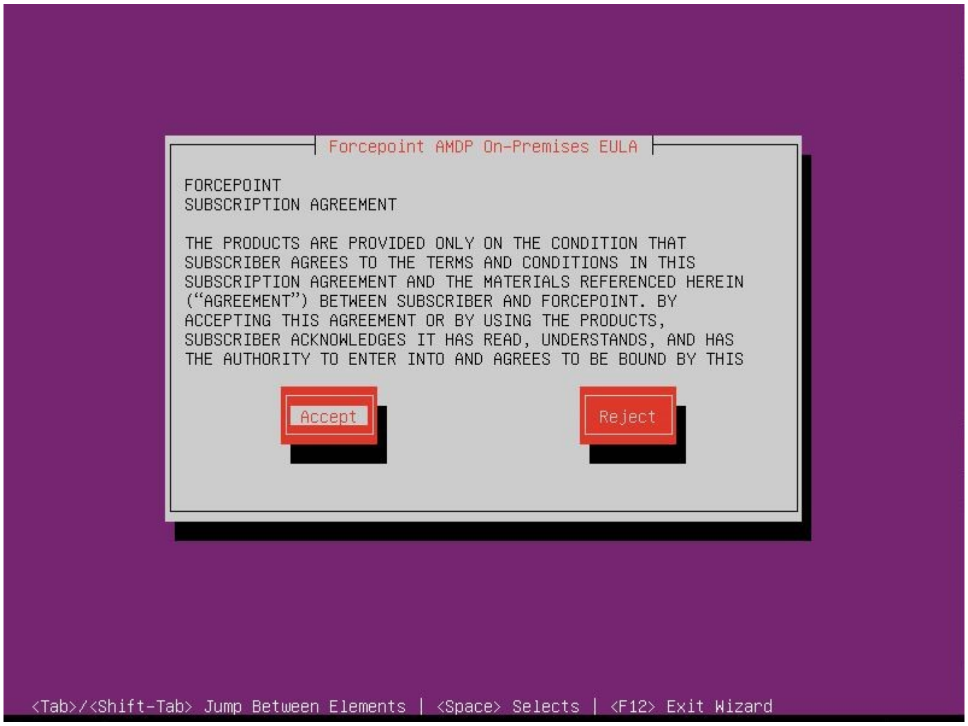
2) The installation process starts at the **Welcome** screen. When you are ready to begin the installation process, select **Start**. This wizard will gather information about the system role and install the appropriate components. The wizard provides the initial system configuration which is then further tailored with the **amd_setup** utility.



```
Forcepoint AMDP On-Premises Registration

*****Advanced Malware Detection and Protection On-Premises*****

The Installation Wizard will guide you through

the installation and registration process.
```

Start
Exit
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

3) Read the Forcepoint Subscription Agreement and select **Accept** to proceed with the installation.

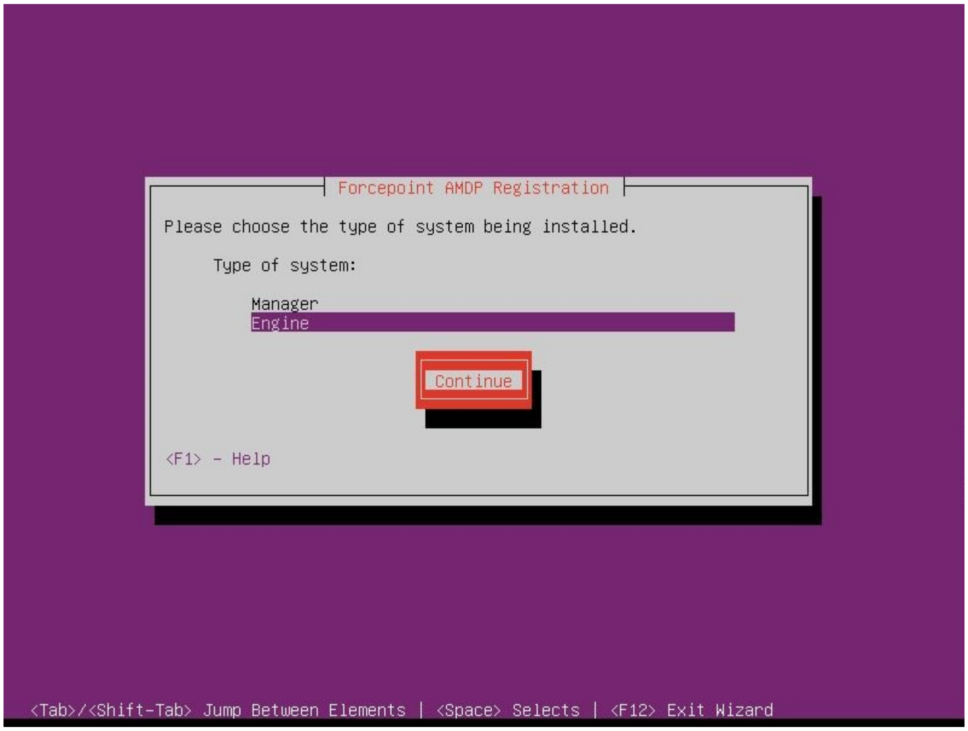


```
Forcepoint AMDP On-Premises EULA

FORCEPOINT
SUBSCRIPTION AGREEMENT

THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT
SUBSCRIBER AGREES TO THE TERMS AND CONDITIONS IN THIS
SUBSCRIPTION AGREEMENT AND THE MATERIALS REFERENCED HEREIN
(“AGREEMENT”) BETWEEN SUBSCRIBER AND FORCEPOINT. BY
ACCEPTING THIS AGREEMENT OR BY USING THE PRODUCTS,
SUBSCRIBER ACKNOWLEDGES IT HAS READ, UNDERSTANDS, AND HAS
THE AUTHORITY TO ENTER INTO AND AGREES TO BE BOUND BY THIS
```

Accept
Reject
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

4) To install the Engine, choose **Engine** and select **Continue**.

4(a)

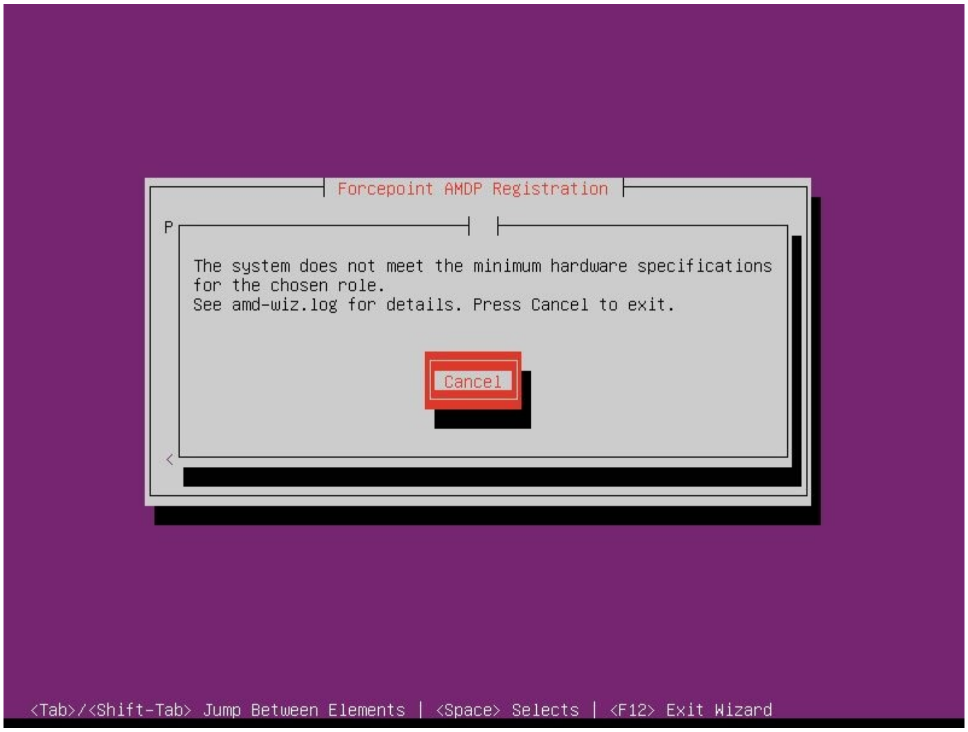


```
Forcepoint AMDP Registration

Please choose the type of system being installed.

     Type of system:

         Manager
         Engine

                    <Continue>

<F1> - Help
```

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

The below wizard checks the server for minimum hardware requirements. If the server does not meet the minimum requirements, either **4(b)** or **4(c)** will appear, depending on the severity of the requirement that is not met. **4(b)** forces the user to cancel the wizard and address the issue, while **4(c)** will allow the user to continue.

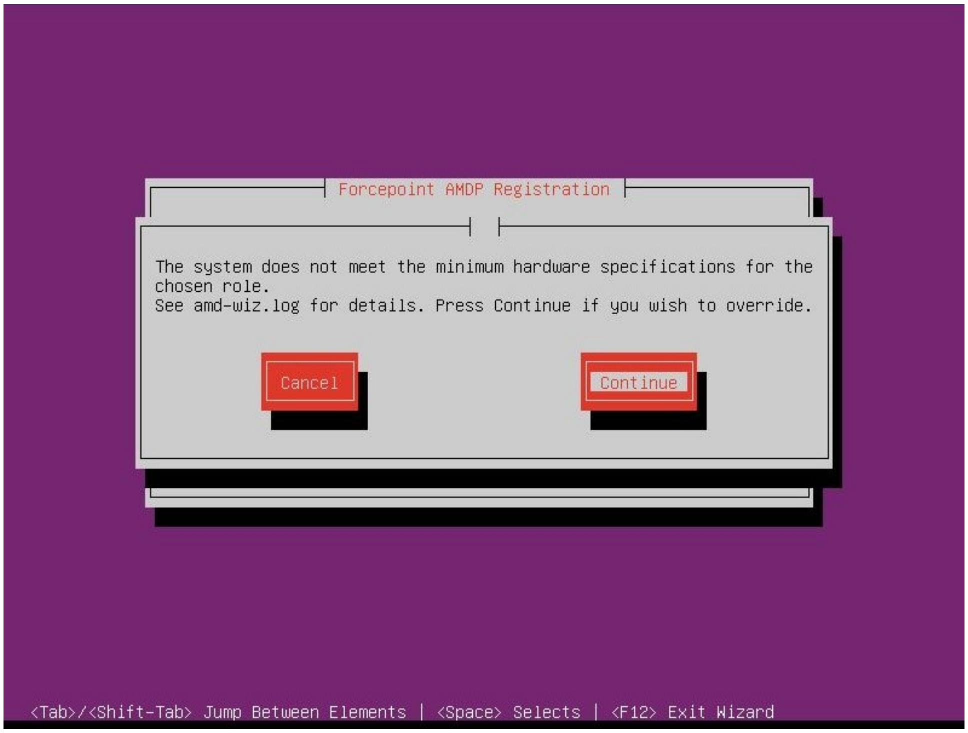
4(b)



```
Forcepoint AMDP Registration

The system does not meet the minimum hardware specifications
for the chosen role.
See amd-wiz.log for details. Press Cancel to exit.

                    <Cancel>
```

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

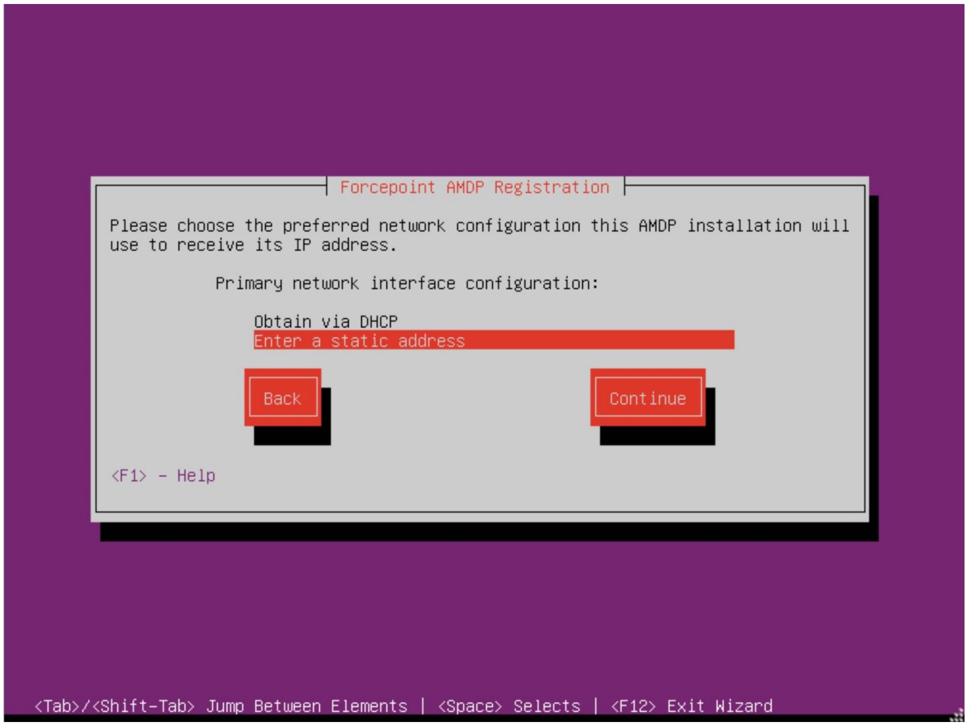
4(c)



```
Forcepoint AMDP Registration

The system does not meet the minimum hardware specifications for the
chosen role.
See amd-wiz.log for details. Press Continue if you wish to override.
```

Cancel
Continue
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

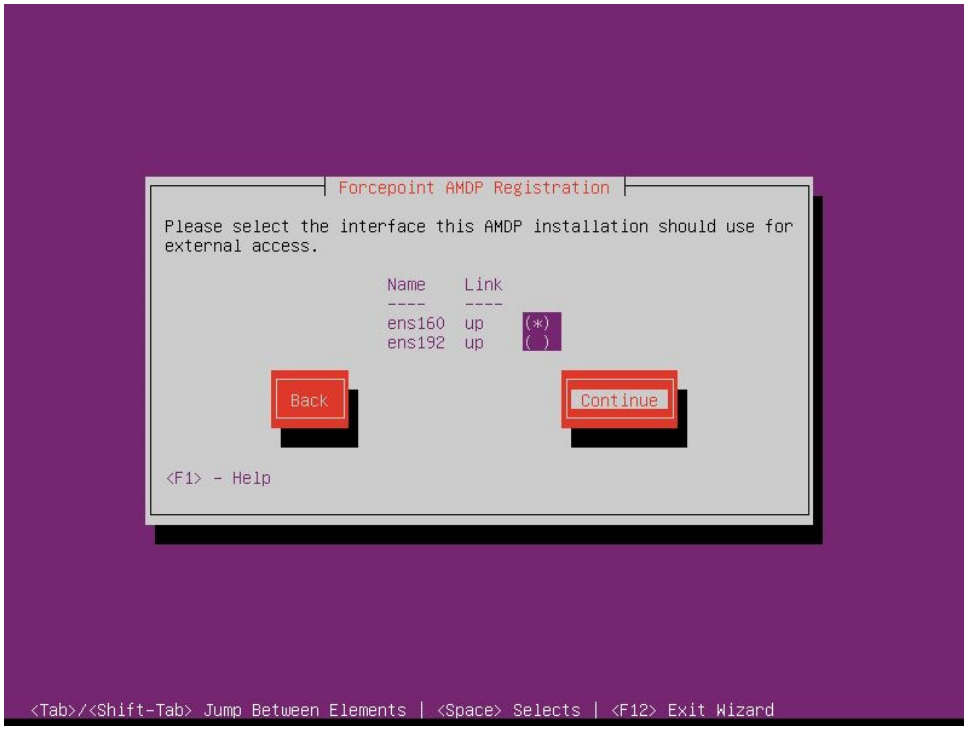
5) Choose the preferred network configuration and select **Continue**.



```
Forcepoint AMDP Registration

Please choose the preferred network configuration this AMDP installation will
use to receive its IP address.

           Primary network interface configuration:

               Obtain via DHCP
               Enter a static address
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

6) Choose the interface for external access and select **Continue**.



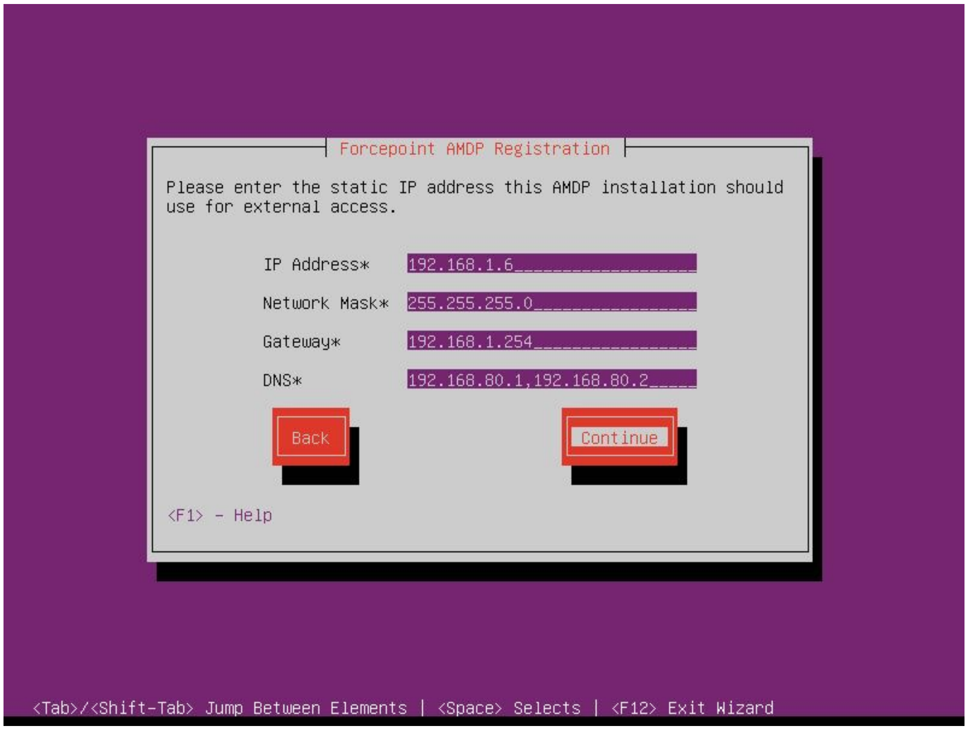
```
Forcepoint AMDP Registration

Please select the interface this AMDP installation should use for
external access.

                    Name    Link
                    ----    ----
                    ens160  up    (*)
                    ens192  up    ( )
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

7) On the Engine network interface, enter the static **IP Address**, **Network Mask/CIDR**, **Gateway**, and **DNS** entries. Select **Continue**.

Note

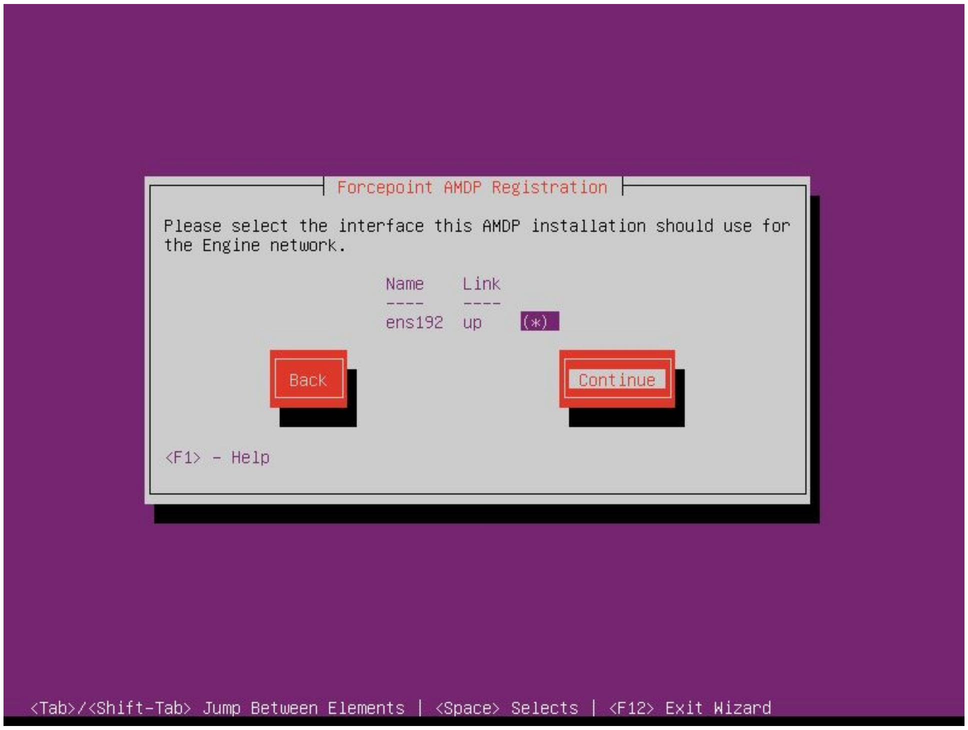
Multiple DNS entries should be comma separated.



```
Forcepoint AMDP Registration

Please enter the static IP address this AMDP installation should
use for external access.

          IP Address*     192.168.1.6__________________
          Network Mask*   255.255.255.0________________
          Gateway*        192.168.1.254________________
          DNS*            192.168.80.1,192.168.80.2____
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

8) Select the interface for the Engine network and **Continue**.



Forcepoint AMDP Registration

Please select the interface this AMDP installation should use for the Engine network.

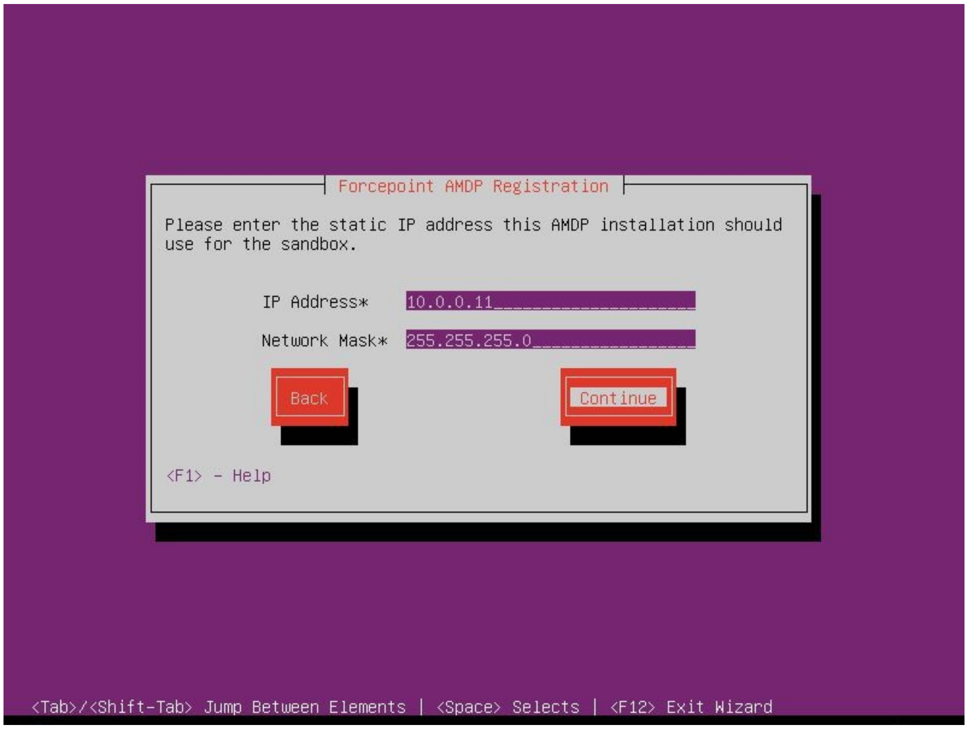
```
Name    Link
----    ----
ens192  up    (*)
```

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

9) Enter the static **IP Address** and select **Continue**.

Note

Select an unused IP address in the 10.0.0.0/24 subnet to communicate with the Manager. The Manager is assigned with the fixed (reserved) IP address 10.0.0.10 on the Engine network (E).



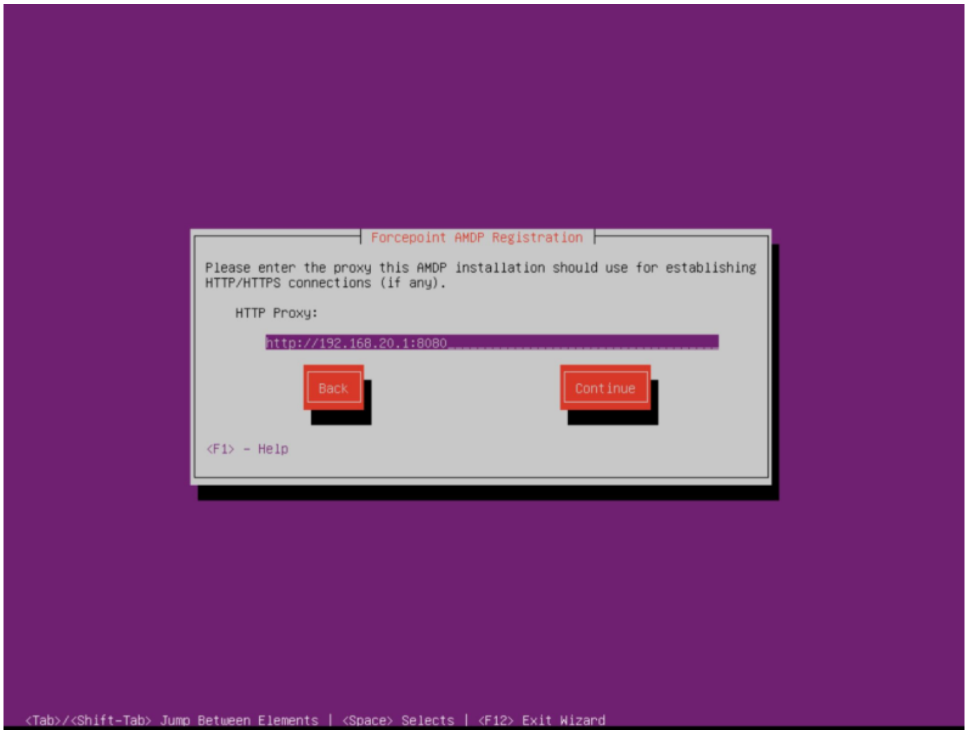
Forcepoint AMDP Registration

Please enter the static IP address this AMDP installation should use for the sandbox.

```
IP Address*     10.0.0.11____________________
Network Mask*   255.255.255.0________________
```

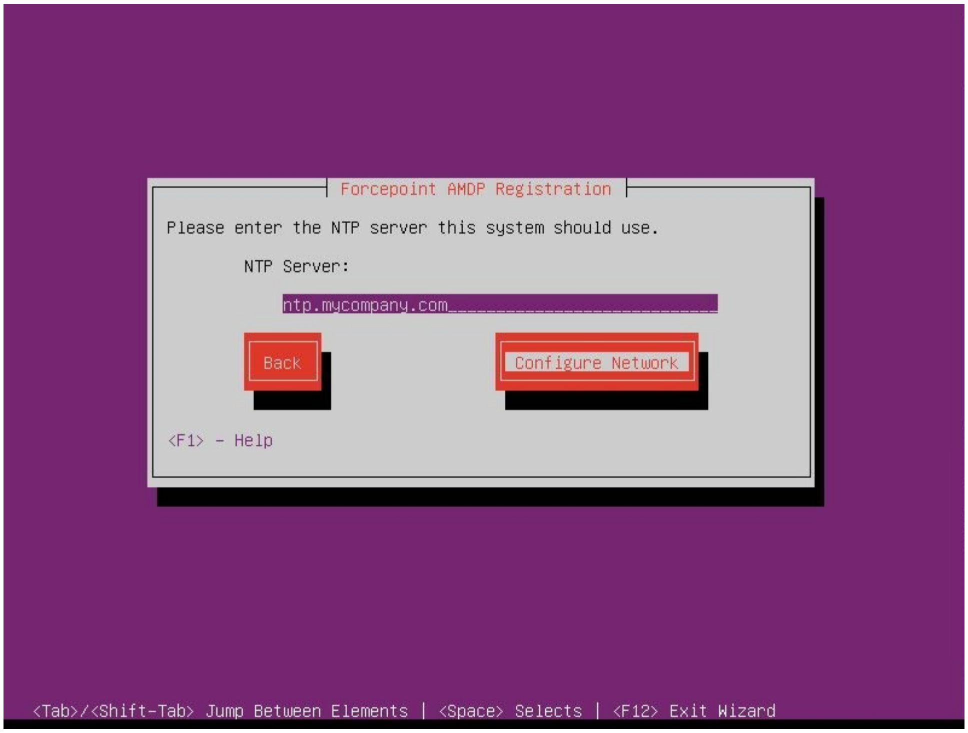
Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

10) Enter the **HTTP Proxy** address for establishing connection with the update servers else leave it blank. Select **Continue**.



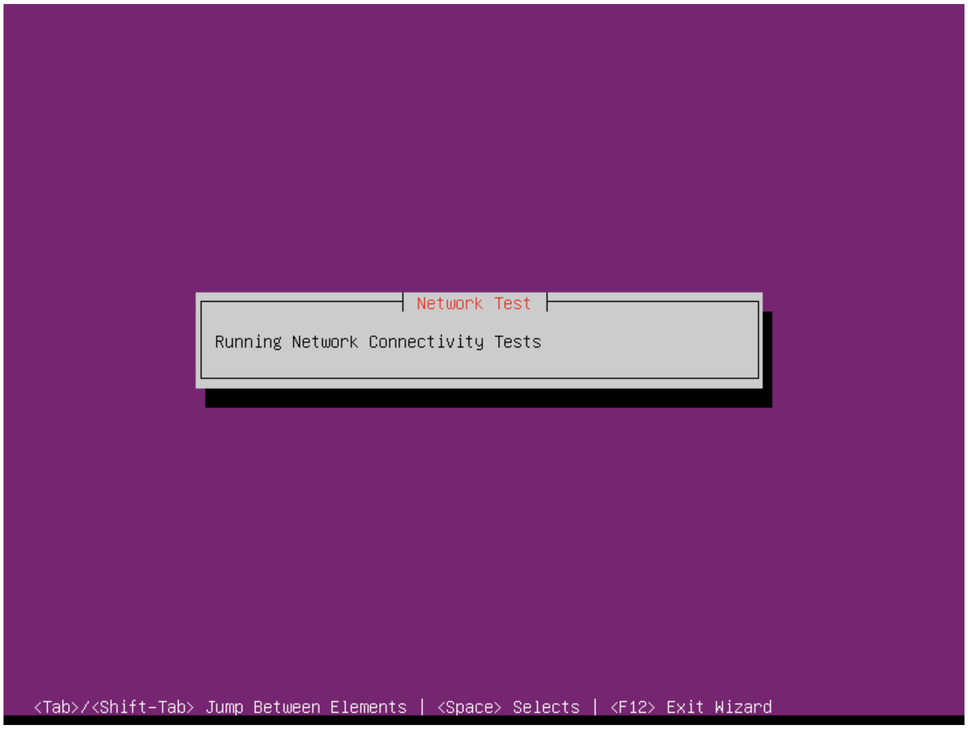
```
Forcepoint AMDP Registration

Please enter the proxy this AMDP installation should use for establishing
HTTP/HTTPS connections (if any).

    HTTP Proxy:

        http://192.168.20.1:8080

<F1> - Help

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

11) Enter the **NTP Server** address and select **Configure Network**.



```
Forcepoint AMDP Registration

Please enter the NTP server this system should use.

        NTP Server:

            ntp.mycompany.com

<F1> - Help

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard
```

Network connectivity test runs.….

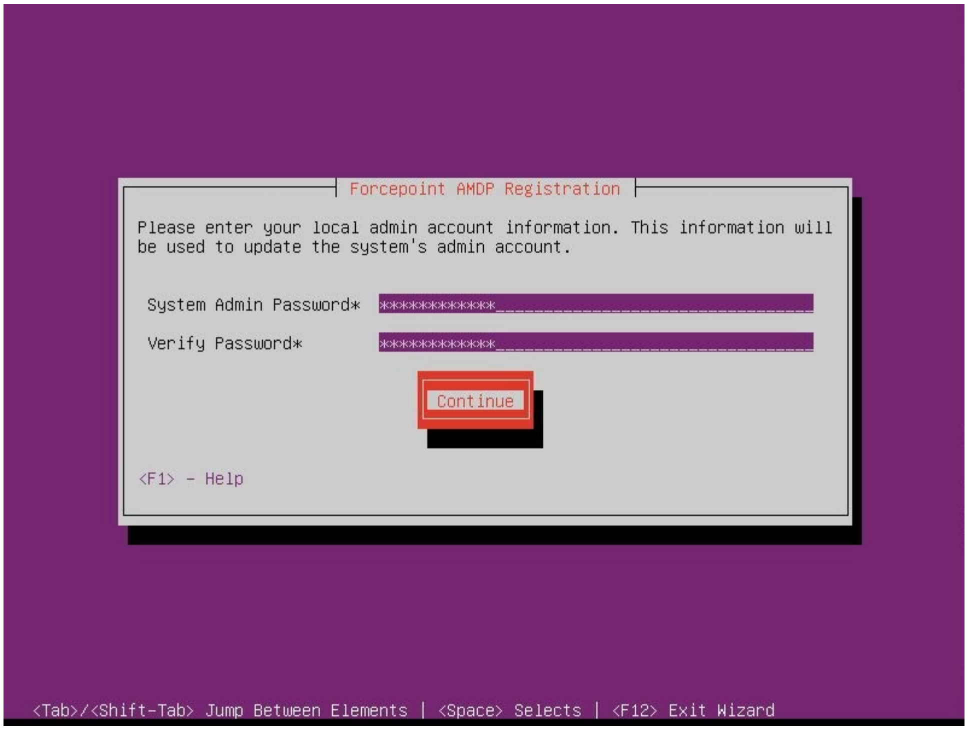


Network Test

Running Network Connectivity Tests

<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

12) Update the password for the local admin user to be used for console and ssh access. Select **Continue**.



Forcepoint AMDP Registration

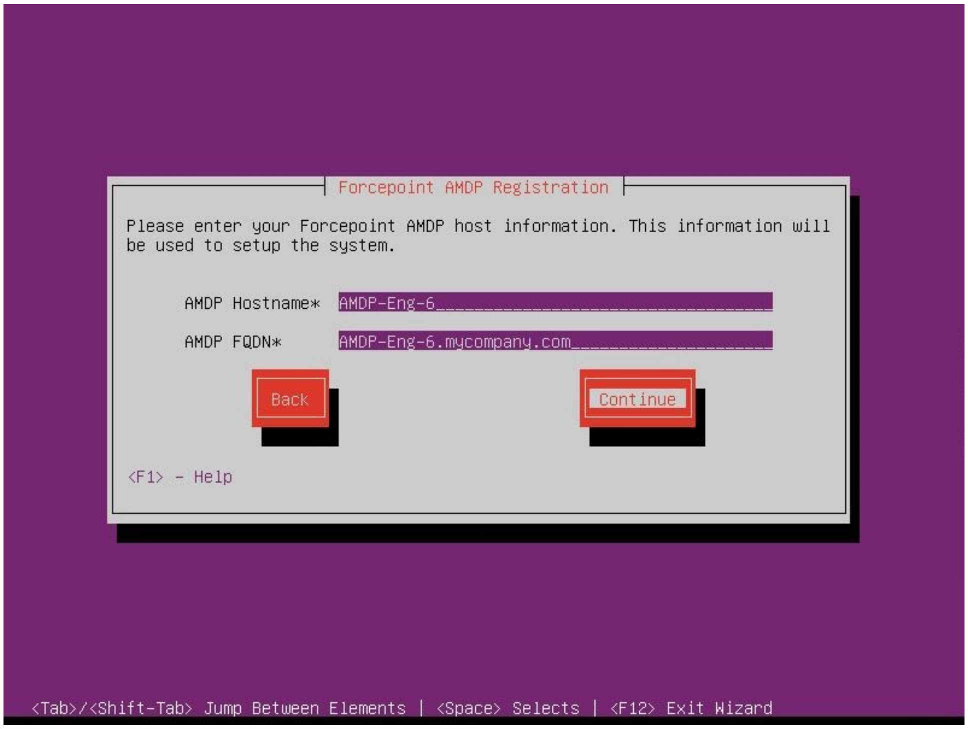
Please enter your local admin account information. This information will be used to update the system's admin account.

System Admin Password* ************

Verify Password* ************

Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

13) Enter your Forcepoint Engine host information and select **Continue**.



Forcepoint AMDP Registration

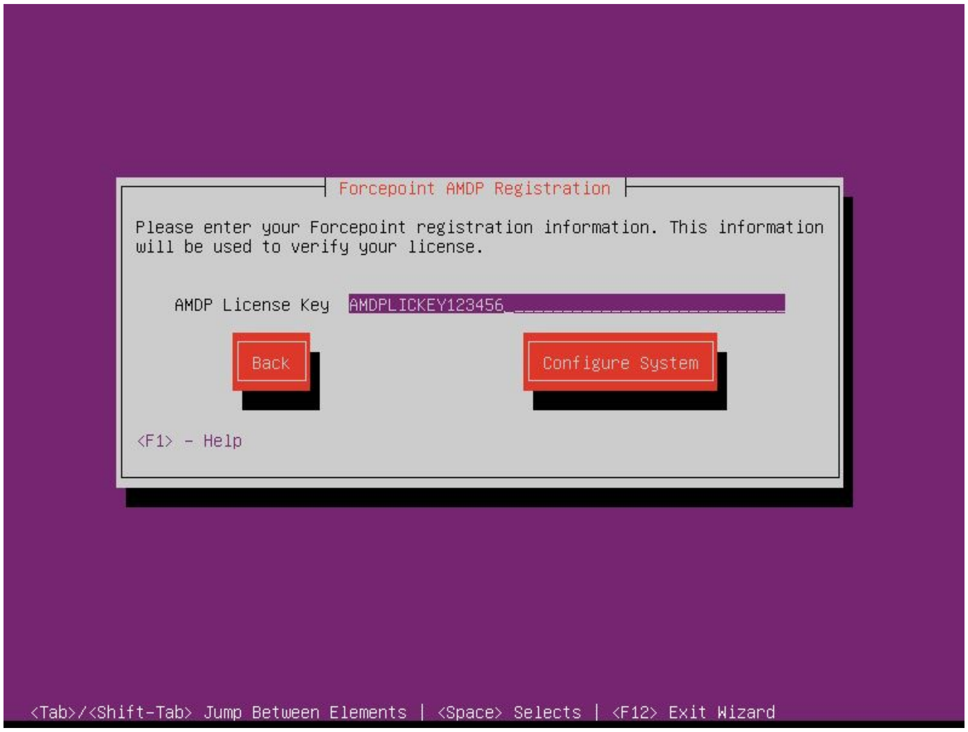
Please enter your Forcepoint AMDP host information. This information will be used to setup the system.

AMDP Hostname* AMDP-Eng-6

AMDP FQDN* AMDP-Eng-6.mycompany.com

Back
Continue
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

14) Enter your Forcepoint Engine License Key and select **Configure System**.



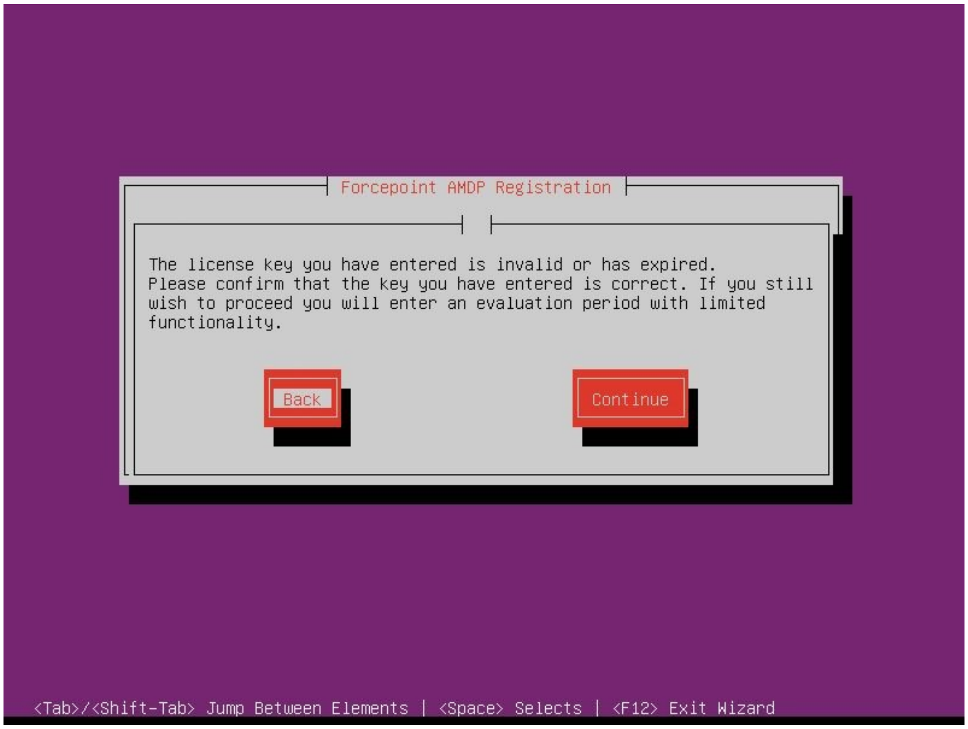
Forcepoint AMDP Registration

Please enter your Forcepoint registration information. This information will be used to verify your license.

AMDP License Key AMDPLICKEY123456

Back
Configure System
<F1> - Help
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

If the license key is invalid or has expired, you will enter an evaluation period with reduced functionality if you decide to **Continue**. Since installations without a valid key will not receive updates, provide a valid, non-expired license key.

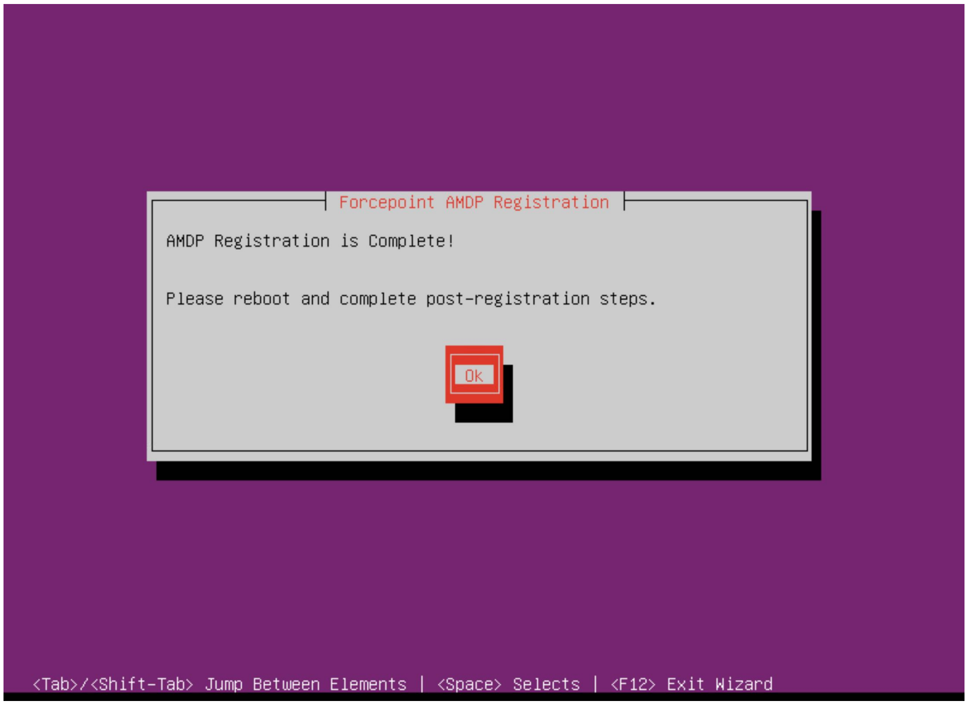


Forcepoint AMDP Registration

The license key you have entered is invalid or has expired.
Please confirm that the key you have entered is correct. If you still
wish to proceed you will enter an evaluation period with limited
functionality.

Back
Continue
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

15) Select **Ok** to exit the Engine Registration wizard.



Forcepoint AMDP Registration

AMDP Registration is Complete!

Please reboot and complete post-registration steps.

Ok
<Tab>/<Shift-Tab> Jump Between Elements | <Space> Selects | <F12> Exit Wizard

Manager configuration

This section focusses on the **amd_setup** command.

Note

All CLI commands must be executed either using sudo or logged in as root.

The Manager CLI is primarily concerned with Engine management. The **amd_setup** utility supports the **engines** command.

```
root@amd-mgr:~# amd_setup engines -h
usage: amd_setup engine [-h] [-l] [-a ENGINE] [-r ENGINE] [-u ENGINE] [-i IP]

optional arguments:
  -h, --help            show this help message and exit
  -l, --list-engines
  -a ENGINE, --add-engine ENGINE
  -r ENGINE, --remove-engine ENGINE
  -u ENGINE, --update-engine ENGINE
  -i IP, --ip IP, --ipv4 IP
root@amd-mgr:~#
```

- Adding an Engine

  ```
  amd_setup engine -a sandbox1 -i 10.0.0.11
  ```

- Listing Engines

  ```
  amd_setup engines -l
  ```

- Removing an Engine

  ```
  amd_setup engine -r sandbox1
  ```

Engine configuration

This section focusses on the `amd_setup` command.

Note

All CLI commands must be executed either using sudo or logged in as root.

The Engine CLI is primarily concerned with sandbox management. Sandbox environments are instantiated to detonate samples for particular machine types. The `amd_setup` utility supports the `sandbox` command.

> **Note**
>
> - Support for Windows 11 version 21H2 '--win11v21h2' and `--vmdelete` require **python3-amd-config** version 2.0.4 or newer.
> - Support for Windows 7 --win7 has been removed starting from **python3-amd-config** version 2.0.5 and newer.

```
root@amd-mgr:~# amd_setup sandbox -h
usage: amd_setup sandbox [-h] [--vms] [--vmbuild] [--vmstatus] [--fetch]
                         [--win10] [--win10v2004] [--win11v21h2][--linux] [--android]
                         [--instances INSTANCES] [--autosize]
                         [--msofficekey MSOFFICEKEY | --office365] [--kms KMS] [--vmtimezone
 TIMEZONE] [--vmdelete VM_TYPE]


optional arguments:
  -h, --help            show this help message and exit
  --vms
  --vmbuild
  --vmstatus
  --fetch
  --win10
  --win10v2004
  --win11v21h2
  --linux
  --android
  --instances INSTANCES
  --autosize
  --msofficekey MSOFFICEKEY
  --office365
  --kms KMS
  --vmtimezone TIMEZONE timezone for the sandbox virtual machine (e.g. America/Chicago ; see
 tzselect(8))
  --vmdelete VM_TYPE    Delete both VM resources and configuration for the specified VM type
```

- Configuring Windows VMs

  ```
  amd_setup sandbox --win10v2004
  amd_setup sandbox --win11v21h2
  ```

- Configuring Linux VMs

  ```
  amd_setup sandbox --linux
  ```

- Configuring Android VMs

  ```
  amd_setup sandbox --android
  ```

- Sandbox engine capacity:
  The Engine is capable of running a number of sandbox virtual machine environments in parallel. This capacity is determined primarily by the number of CPUs on the engine and was automatically configured by `amd_register`. Each virtual machine environment is called an *instance*.
- Tailoring the instance count:
  You can specify an explicit instance count for a machine type (For example: win10v2004) by supplying the **--instances** parameter. In the following example, the Linux machine templates will be instantiated specifying 4 instances per machine type (Ubuntu, Debian, etc.).

  Alternatively, you can specify the **--autosize** parameter to consider all the machines listed on the command line and balance the available resource among them.

Note

Machines not listed in the command are not considered.

```
amd_setup sandbox --linux --instances 4
```

- Autosize option:
  The **--autosize** sandbox option can be used to balance the available parallel instance capacity among the machine types listed on the command line.

  Note

  --autosize will overwrite any existing sandbox machine configurations, so is best used during initial provisioning of the engine.

  For example, to create a balanced configuration for all the available sandbox types use the following commands. First we check the status; the status will indicate the parallel instance capacity of the engine.

  ```
  root@amd-eng:~# amd_setup sandbox --vmstatus
  Instance capacity: 8
  Total instances: 0
  VM status:
  No desired VMs configured.
  ```

  Next, we create the basic configuration for each desired sandbox environment:

  ```
  root@amd-eng:~# amd_setup sandbox --win10 --win10v2004 --win11v21h2 --linux --android --autosize
  Instance capacity: 8
  Added instances:
          win10:      1
          win10v2004: 1
          win11v21h2: 1
          android9:   1
          android10:  1
          android11:  1
          ubuntu1804: 1
  Total instances: 8
  Warning: Windows options require a Microsoft Office license to ensure efficacy for analysis
  of Office documents; supply --msofficekey (supported for win10, win10v2004,
  win11v21h2) or --office365 (only supported for win10v2004)
  Warning: Windows options require a Microsoft Office license to ensure efficacy for analysis
  of Office documents; supply --msofficekey (supported for win10, win10v2004,
  win11v21h2) or --office365 (only supported for win10v2004)
  Warning: Windows options require a Microsoft Office license to ensure efficacy for analysis
  of Office documents; supply --msofficekey (supported for win10, win10v2004,
  win11v21h2) or --office365 (only supported for win10v2004)
  ```

  For any sandbox environment requiring additional options such as a license or office, take note of the instance count for that machine type and reissue the setup command with an explicit instance count observed from the `--autosize` command (1 in this example):

  ```
  root@amd-eng:~# amd_setup sandbox --win10v2004 --office365 --vmtimezone America/Chicago --
  instances 1
  Instance capacity: 7
  Added instances:
  win10v2004: 1
  Total instances: 7
  ```

- Building VMs:
  To initiate a build of the configured sandbox VM types, use the `--vmbuild` option for the sandbox command. The build will create the VM environments for each newly configured or modified machine type. The build will also update sandbox VM environments if there has been a software update applied.

Note

Building sandbox VMs can be a time consuming operation and may take several hours to complete. Once the build has started, check the status with **--vmstatus** option to see if it has completed.

```
# amd_setup sandbox --vmbuild --vmstatus
```

- Checking VM build status:
  After allocating a virtual machine type (For example: --win10v2004), the corresponding virtual machine environment will need to be built. You can test the status of the build with the `--vmstatus` option. If the environment has not yet been built for that type or has changes pending due to a software update, the status will indicate "Build action recommended". The version will indicate "UNAVAILABLE" until the build action has completed (see Building VMs section above).

```
# amd_setup sandbox --vmstatus
Instance capacity: 7
Total instances: 1
VM status:
VM: win10v2004
Latest version: UNAVAILABLE
Latest version is not up to date with current config
# Build action recommended
```

Note

If the build status indicates "UNAVAILABLE" the VM has not been built yet. Whenever a VM configuration has been changed or the base ISO has been updated, a build action is indicated. To start the build, run **amd_setup sandbox** with a **--vmbuild** option.

- Deleting a VM (requires **python3-amd-config** version 2.0.4 or newer):
  Once a VM is either configured to be built or is successfully built or its build has failed, if there is a need to delete it to change its configuration, like the number of instances or the office license or to build another type of VM, use the `--vmdelete` option. This option frees up the resources being used by the specified VM and its configuration as well. This option cannot be used on a VM during build.

Note

VM_TYPE arguments supported for `--vmdelete` option are: win10, win10v2004, win11v21h2, linux, android.

For example, consider that a Linux VM is successfully built:

```
# amd_setup sandbox --vmstatus
Instance capacity: 15
Total instances: 1
VM status:
VM: ubuntu1804-amd64
Latest version: 20250714
Resource: ubuntu1804-amd64-20250714-en
```

To delete it, use the `--vmdelete` option as below:

```
# amd_setup sandbox --vmdelete linux
Instance capacity: 15
Total instances: 1
Successfully deleted VM resources & configuration for: ubuntu1804-amd64
```

Check the VM build status to confirm deletion:

```
# amd_setup sandbox --vmstatus
Instance capacity: 15
Total instances: 0
VM status:

No desired VMs configured.
```

For a VM during the build, the `--vmdelete` option cannot be used.

```
# amd_setup sandbox --vmstatus
Instance capacity: 15
Total instances: 1
VM status:

VM: ubuntu1804-amd64
Latest version: UNAVAILABLE
Latest version is not up to date with current config
Undesired resource: ubuntu1804-amd64-20250723-en
# Build active

# amd_setup sandbox --vmdelete linux
Instance capacity: 15
Total instances: 1
ERROR:root:Failed to delete VM resources for ubuntu1804-amd64: Error: HTTP 500 (INTERNAL):
 Cannot modify VM during build
```

Software updates

The base operating system for AMDP is currently Ubuntu Noble 24.04 LTS and uses standard Ubuntu software update facilities and package management tools.

The system installation from the ISO includes baseline packages for AMDP and Ubuntu, as well as configuration for the related update repositories and the digital signatures for validating updates. The primary tool for managing updates is the standard Linux Advanced Packaging Tool (APT).

As part of the initial setup and registration, the **amd_register** tool invokes **apt** to update the system and AMDP software to the latest versions available from the update repositories.

After the system has been installed and registered, the update behavior can be changed. By default, the repositories are checked daily to see if there are available updates, and any updates which are eligible for **automatic installation** are applied. To change this behavior, use the **amd_setup updates** command.

To enable automatic updates for both AMDP and the system, use the following command:

```
amd_setup updates --system --amdp enable
```

or to disable automatic updates:

```
amd_setup updates --system --amdp disable
```

If either **--system** or **--amdp** are omitted, only the specified updates are affected by the command, so for example

```
amd_setup updates --amdp enable
```

enables updates for AMDP but doesn't change the setting for system updates.

Run **amd_setup updates -h** to see the available options for the command:

```
root@amd-mgr:~# amd_setup updates -h
usage: amd_setup updates [-h] [--system] [--amdp] {enable,disable}

positional arguments:
  {enable,disable}  Choose whether to enable or disable automatic updates

optional arguments:
  -h, --help        show this help message and exit
  --system          base system software updates
  --amdp            AMDP software updates
```

Automatic updates

The following package types are eligible for automatic update:

- Security updates for system packages
- AMDP administrative tools (wizard, cli)
- AMDP services and health monitors
- Threat Detection and Malware signatures (manager); (autoinstalled, but need to reload)
- Sandbox VM monitors (engine); (autoinstalled, but VMs may need be rebuilt)

Manual updates

For updates which are not automatically applied, the following CLI command will upgrade all available packages to the most recent version.

> **Note**
>
> Some AMDP packages require special handling prior to upgrade (see *Upgrade Special Handling Steps* below).

```
apt update  # updates the information about available updates

apt list --upgradeable  # lists packages eligible for update

apt upgrade  # upgrade and install all eligible packages
```

or

```
apt install package(s) #  upgrade and install a particular package (or packages)
```

> **Note**
>
> The **apt upgrade** command will install non-security related system packages as well as the AMDP packages.

Check for available updates on the manager once a week for signature updates, and every few weeks for other updates.

Upgrade special handling steps

Some packages require special handling prior to and/or after upgrading, so we strongly recommend to use the **apt list** command to see what changes will be affected prior to deciding to use the apt upgrade command.

Static analysis service (Manager)

Prior to upgrading the hatching-triage package, it's desirable to quiesce the processing of new samples and finish ones in progress. Use the following command:

```
killall -TERM triage; while pidof triage >/dev/null; do echo -n .; sleep 1; done
```

After updating the hatching-triage package, restart the service as below:

```
systemctl restart hatching-triage
```

> **CAUTION**
>
> Avoid restarting the hatching-triage service until the signatures have been reloaded if there are active analysis in progress.

Frontend service (Manager)

After updating the hatching-frontend package, restart the service as below:

```
systemctl restart triage-frontend
```

VM monitors and services (Engine)

Virtual machine monitors include some components which are installed in the virtual machine environments for the sandbox. While the monitor packages are automatically installed, the corresponding VMs may need to be rebuilt. When checking for general updates, run the following command to check if the VMs need to be rebuilt:

```
amd_setup sandbox --vmstatus
```

See *Engine configuration* for additional information on building VMs.

Sandbox manager and services (Engine)

After upgrading the hatching-sandbox-node and/or hatching-sandbox-allos-node package, it is recommended to safely stop sandbox and wait for tasks to complete. Use the following command:

```
pidof sandbox | xargs kill -s INT 2>/dev/null && while $(pidof sandbox >/dev/null); do echo
 "Waiting for exit.." && sleep 2; done
```

Then restart the services as below:

```
systemctl restart hatching-sandbox-net
systemctl restart hatching-sandbox
systemctl restart hatching-vms
```

> **Note**
>
> Do not restart this service if there is an active VM build (see **amd_setup sandbox --vmstatus**).

Packages requiring reboot

Some updates require the system to be rebooted to complete the installation, typically associated with a new kernel or core service. Generally, AMDP updates do not require a reboot, but a reboot is the easiest way to ensure all the associated services have been restarted following an upgrade.

General notes about package naming

AMDP package names start with "**amd**", "**python3-amd**", "**hatching**" or "**tts**".

Related concepts
Engine configuration on page 28

Backup and Restore

The **amd_backup** tool creates a backup of the AMDP configuration files and log files that can be restored through the **amd_restore** command on a freshly installed machine that has gone through the initial registration.

Usage and options for the backup command are as follows:

```
root@amd-mgr# amd_backup -h
usage: amd_backup [-h] [--logs-only] [--no-sql-backup] [--template TEMPLATE] [--list] [--dry-run]

optional arguments:
  -h, --help           show this help message and exit
  --logs-only          Only backup logs
  --no-sql-backup      Don't backup the Triage database
  --template TEMPLATE  Provide a custom backup template
  --list               List available backup files
  --dry-run            Do a dry-run backup
```

Usage and options for the restore command are as follows:

```
root@amd-mgr# amd_restore -h
usage: amd_restore [-h] -f FILE

optional arguments:
  -h, --help            show this help message and exit
  -f FILE, --file FILE  Backup file to restore
```

Usage

To provide the backup logs to Forcepoint Support, you may wish to use the **--logs-only** option to exclude samples.

```
root@amd-mgr:# amd_backup --logs-only
Space required for backup: 54369 KB
Available Space: 38294704 KB
Creating backup
Created backup at /var/spool/amd/backups/amdp-backup_20231129-160139-logs.tar.gz
root@amd-mgr:# amd_backup --list
Available backups:
/var/spool/amd/backups/amdp-backup_20231129-160139-logs.tar.gz

----

root@amd-mgr:~# amd_backup --list
Available backups:
/var/spool/amd/backups/amdp-backup_20231129-160139-logs.tar.gz
root@amd-mgr:~# amd_restore -f /var/spool/amd/backups/amdp-backup_20231129-160139-logs.tar.gz
Extracting /var/spool/amd/backups/amdp-backup_20231129-160139-logs.tar.gz
Validating backup compatibility
Stopping services
Restoring backup
Cleaning up temp directory
Initial restore complete. Restart the system to finish the restore operation.
root@amd-mgr:~#
```

Microsoft Office licensing

Note

- Windows **10** and Windows **11** VMs require **Microsoft Office 2019**

There are 2 options for Microsoft Office licensing:

1) `root@amd-eng:~# amd_setup sandbox --[vm type][--msofficekey MSOFFICEKEY]`
   where MSOFFICEKEY is a license key for Microsoft Office.

   For example: `amd_setup sandbox --win10 --msofficekey XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX`

2) `root@amd-eng:~# amd_setup sandbox --[vm type][--msofficekey MSOFFICEKEY][--kms KMS]`
   where KMS is an optional key management server.

If you want to specify **--instances** to tailor the instance count that must be supplied with the Windows VM type and the license key then,

```
root@amd-eng:~# amd_setup sandbox --[vm type][--msofficekey MSOFFICEKEY][--instances count]
```

For example: `root@amd-eng:~# amd_setup sandbox --win10 --msofficekey XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX --instances 24`

Below warning message is displayed if MS license key is **not** supplied: `root@amd-eng:~# amd_setup sandbox --win10`

Warning

Windows options require a Microsoft Office license to ensure efficacy for analysis of Office documents; supply --msofficekey (supported for win10, win10v2004, win11v21h2) or --office365 (only supported for win10v2004).

Office 365 configuration

Steps

1) Add a Windows 10 Build 2004 sandbox with Office 365 support with following command. Make sure to insert the correct timezone for your location.

```
sudo amd_setup sandbox --win10v2004 --office365 --vmtimezone <tzselect style>
```

A `<tzselect style>` would be in this format: America/New_York or Europe/London for example.

```
admin@bt-amdp-eng-159:~$ sudo amd_setup sandbox --win10v2004 --office365 --vmtimezone
 America/Denver
[sudo] password for admin:
Instance capacity:15
No instance count specified, defaulting to 8
Added instances:
    win10v2004: 8
Total instances: 8
```

2) Run `sudo amd_setup sandbox --vmbuild` to start building the sandbox VM.

```
admin@bt-amdp-eng-159:~$ sudo amd_setup sandbox --vmbuild
Instance capacity:15
Total instances: 8
VM build:

Building all desired VMs
{}
```

Waiting for Office to be ready for manual action...

a) When the Office 365 script is ran, the `hatching-vms` logs will log the used host and port. This log message looks like:

```
The current script may need manual interaction. VNC is enabled. script=office365new
 vnc_host=0.0.0.0 vnc_port=29023 ..
```

b) Find it by running:

```
journalctl -u hatching-vms | grep "script may need manual" | tail -1
```

c) The Office 365 script will first install Office 365. When it is ready to be activated, the following log messages will appear:

```
script=office365new script-message="Waiting for manual activation of Office 365. Connect
 with VNC and manually activate.\n" ..
```

d) Find it by running:

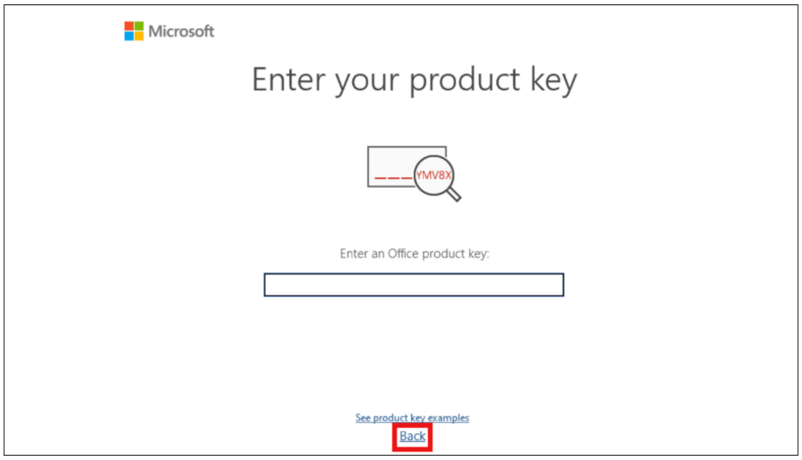
```
journalctl -u hatching-vms | grep "Waiting for manual activation of Office 365" | tail -1
```

Note

The **vnc_port** is listed in the first log message.

3) On a separate host, use a VNC client to connect to the IP of the engine on the port listed previously.

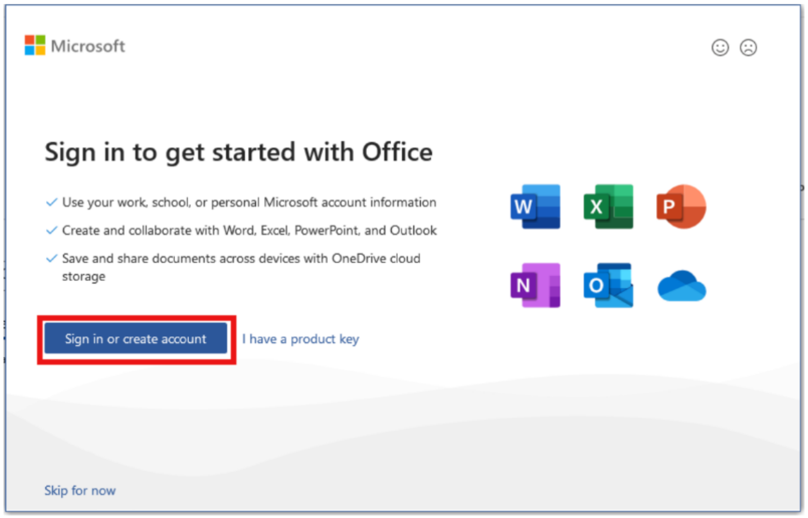
4) Once connected via VNC, you will be presented with a prompt to enter a product key for Office. Select **Back** on this menu.



Enter your product key

Enter an Office product key:

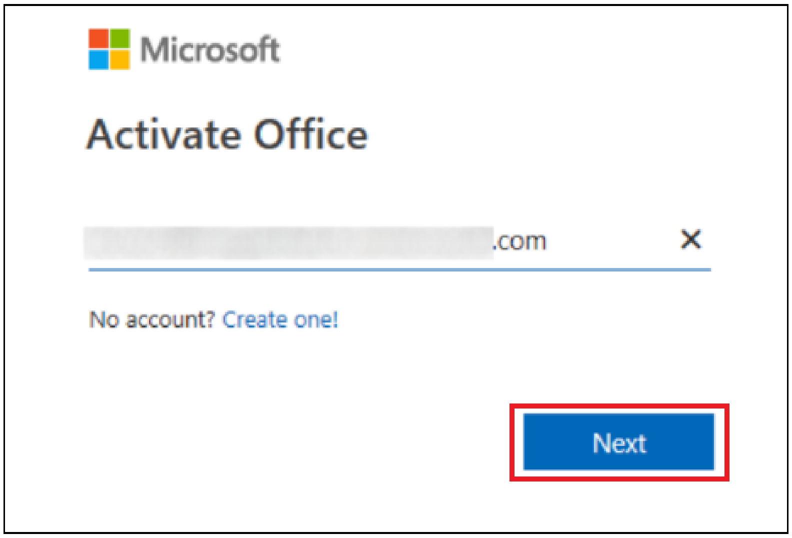
5) A new pop-up appears asking to **Sign in to get started with Office**. Select **Sign in or create account**.



Sign in to get started with Office

- ✓ Use your work, school, or personal Microsoft account information
- ✓ Create and collaborate with Word, Excel, PowerPoint, and Outlook
- ✓ Save and share documents across devices with OneDrive cloud storage

6) Enter the email address of the user that will be used with the sandboxes and select **Next**.



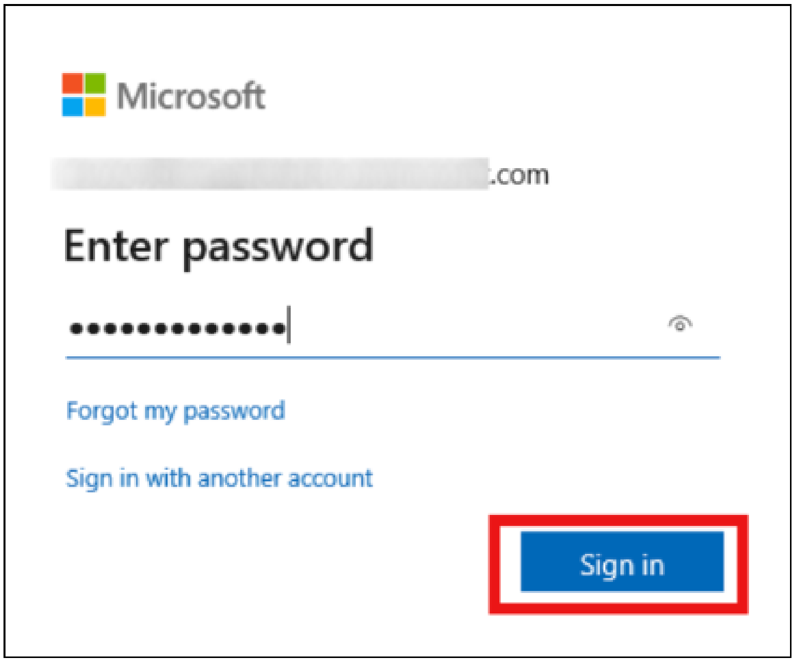
Microsoft

Activate Office

[redacted].com

No account? Create one!

7) Enter the password for the user entered previously.



Microsoft

[redacted].com

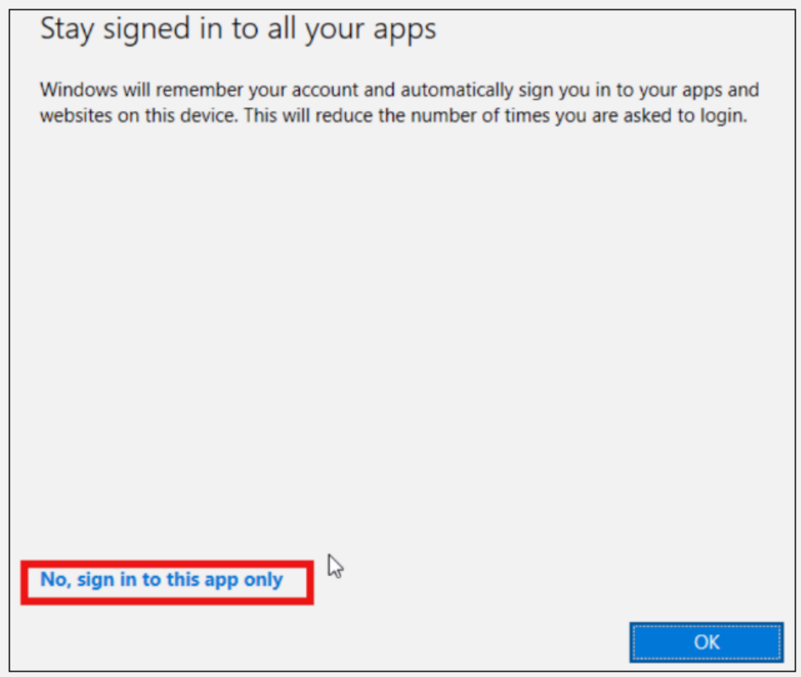
Enter password

•••••••••••••

Forgot my password

Sign in with another account

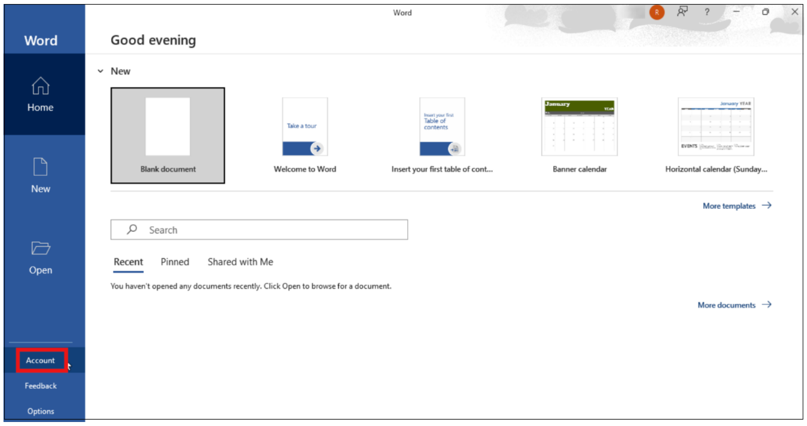
8) Once signed in, select **No, sign in to this app only** on the pop-up that says **Stay signed in to all your apps**.



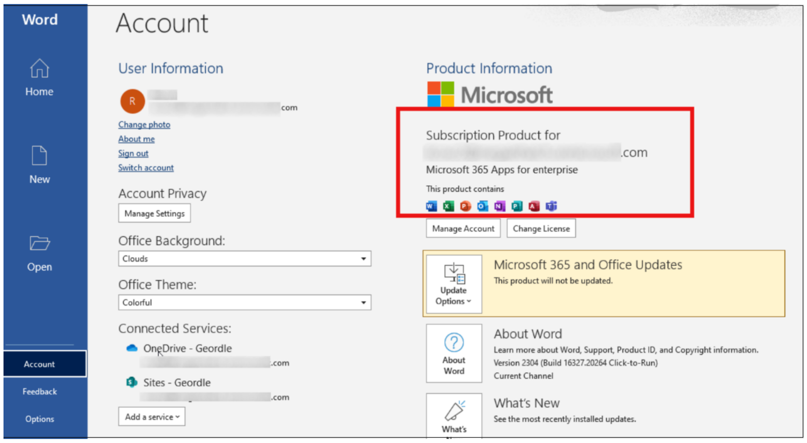
Stay signed in to all your apps

Windows will remember your account and automatically sign you in to your apps and websites on this device. This will reduce the number of times you are asked to login.

9) Select **Account** in the Microsoft Word menu and verify that Office is activated. You should see a section related to your subscription on the right side of the screen.



You haven't opened any documents recently. Click Open to browse for a document.



User Information

[redacted]
[redacted]com

Product Information

Subscription Product for
[redacted].com
Microsoft 365 Apps for enterprise
This product contains

Microsoft 365 and Office Updates
This product will not be updated.

About Word
Learn more about Word, Support, Product ID, and Copyright information.
Version 2304 (Build 16327.20264 Click-to-Run)
Current Channel

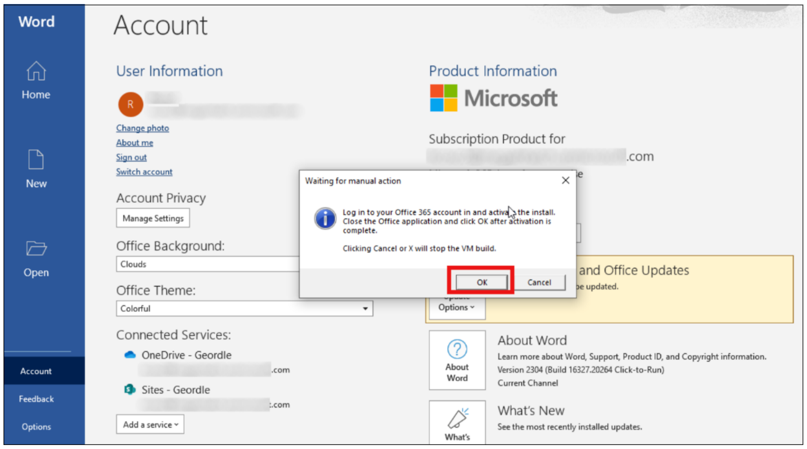
What's New
See the most recently installed updates.

Office Background: Clouds

Office Theme: Colorful

Connected Services:
OneDrive - Geordle
[redacted].com
Sites - Geordle
[redacted].com

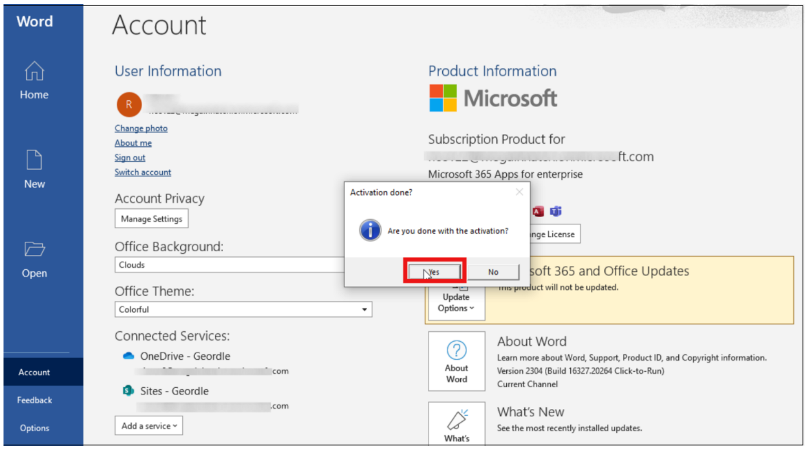
10) In the taskbar, find the window that has **Waiting for manual action** in the text field and select **OK**. Select **Yes** on the next pop-up to confirm that the activation is complete.



Waiting for manual action

Log in to your Office 365 account in and activa the install. Close the Office application and click OK after activation is complete.

Clicking Cancel or X will stop the VM build.



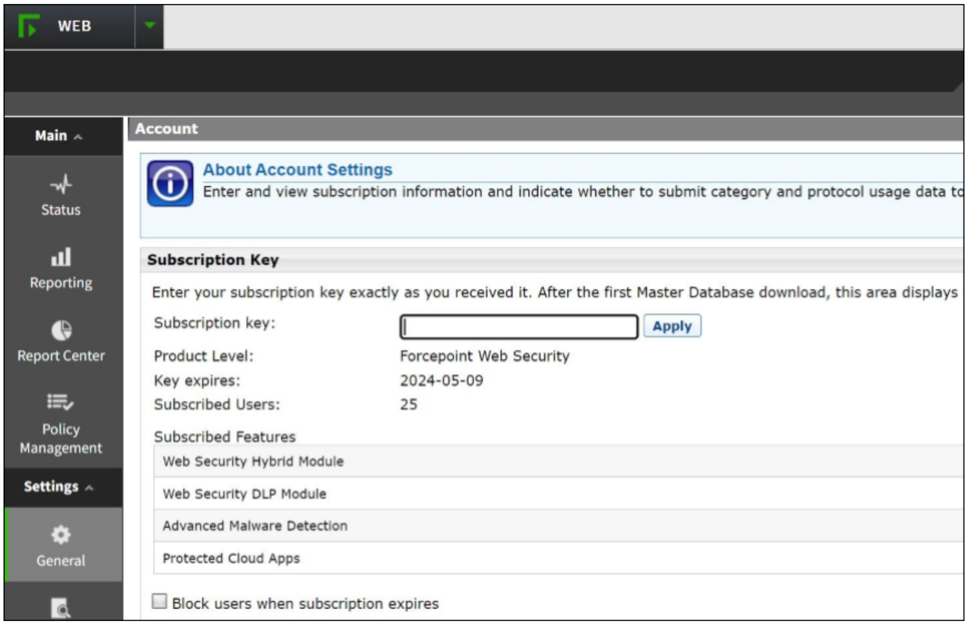
Activation done?

Are you done with the activation?

11) Close the VNC session and wait for the VM to finish building.

Web Security licensing and configuration

The Web Security License Key is entered in the Web section of Forcepoint Security Manager (FSM) under **Settings** > **General** > **Account** > **Subscription Key**.



About Account Settings
Enter and view subscription information and indicate whether to submit category and protocol usage data to

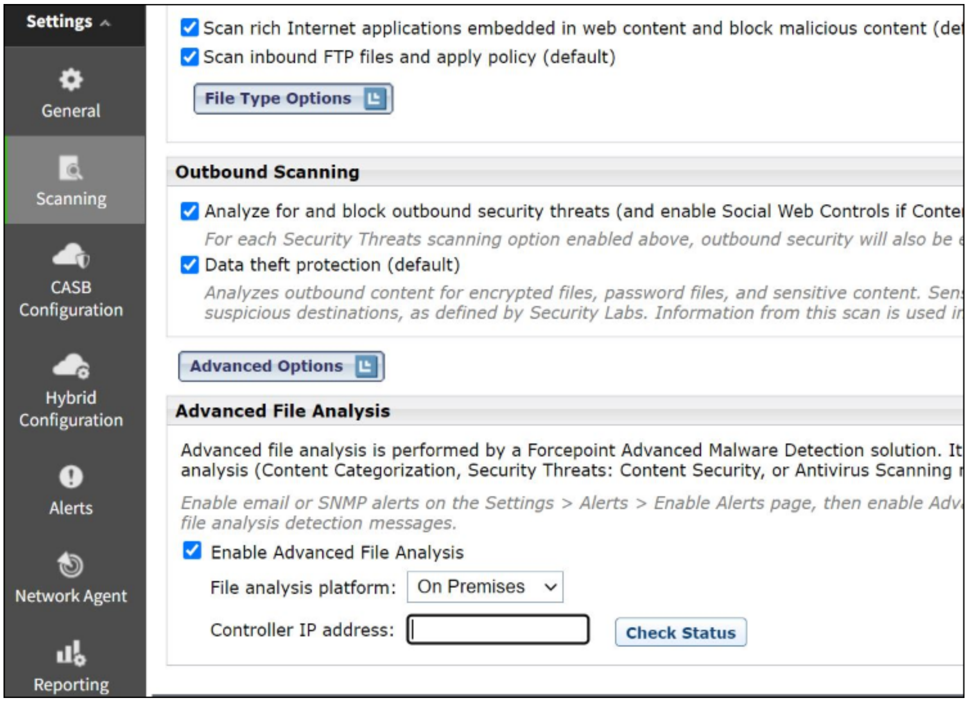
Subscription Key
Enter your subscription key exactly as you received it. After the first Master Database download, this area displays

Subscription key:
Product Level: Forcepoint Web Security
Key expires: 2024-05-09
Subscribed Users: 25

Subscribed Features
- Web Security Hybrid Module
- Web Security DLP Module
- Advanced Malware Detection
- Protected Cloud Apps

□ Block users when subscription expires

AMDP configuration for Web Security is done in the Web section of Forcepoint Security Manager under **Settings** > **Scanning** > **Scanning Options** > **Advanced File Analysis**. The only configuration needed, is the IP address of the AMDP Manager.



☑ Scan rich Internet applications embedded in web content and block malicious content (de
☑ Scan inbound FTP files and apply policy (default)

Outbound Scanning
☑ Analyze for and block outbound security threats (and enable Social Web Controls if Conte
For each Security Threats scanning option enabled above, outbound security will also be
☑ Data theft protection (default)
Analyzes outbound content for encrypted files, password files, and sensitive content. Sen suspicious destinations, as defined by Security Labs. Information from this scan is used i

Advanced File Analysis
Advanced file analysis is performed by a Forcepoint Advanced Malware Detection solution. It analysis (Content Categorization, Security Threats: Content Security, or Antivirus Scanning
Enable email or SNMP alerts on the Settings > Alerts > Enable Alerts page, then enable Adv file analysis detection messages.
☑ Enable Advanced File Analysis
File analysis platform: On Premises
Controller IP address:

For detailed information, refer to Advanced File Analysis section and Configuring your account information section in Forcepoint Web Security Administrator Help.

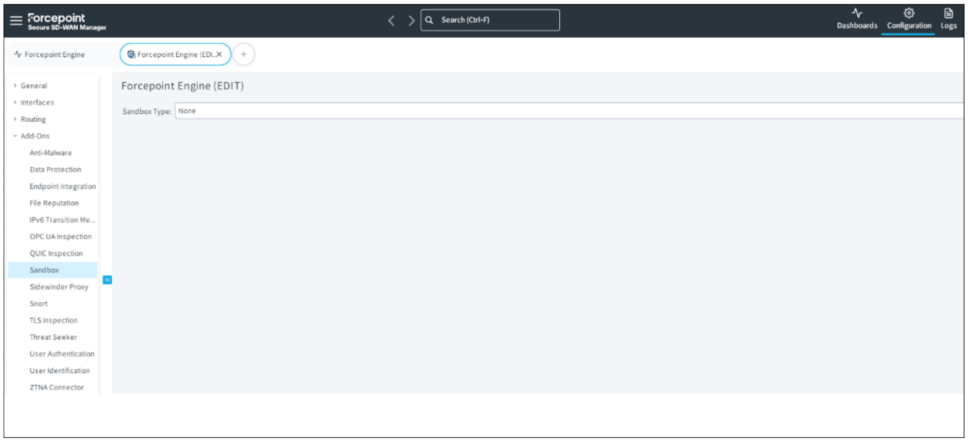
Configuring AMDP on Secure SD-WAN via SMC GUI

Follow the instructions listed below to configure AMDP on the Secure SD-WAN using the SMC GUI:

Note

The menu options described in the numbered list below are only present on SMC version 7.1.1 and above.

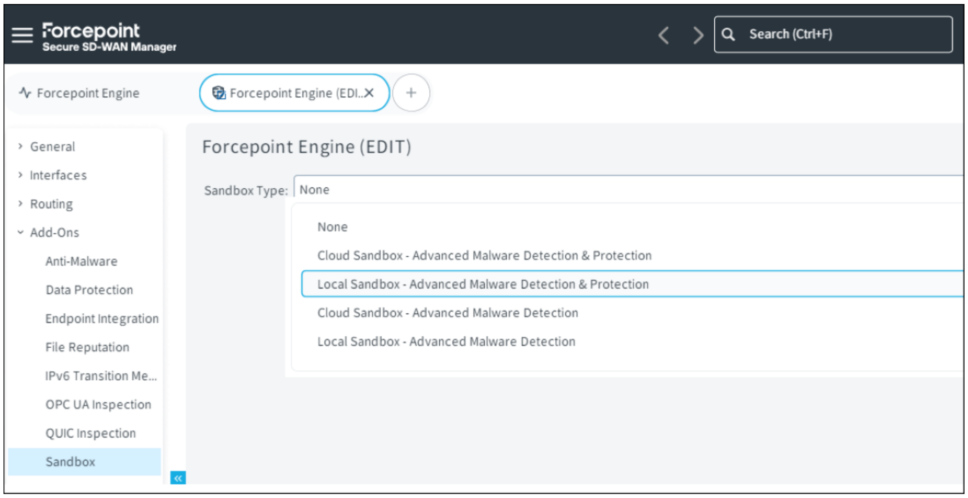
1) Open the engine editor for a firewall and navigate to **Add-Ons** > **Sandbox**.



Forcepoint Engine (EDIT)

Sandbox Type: None

2) Under **Sandbox Type** select **Local Sandbox - Advanced Malware Detection & Protection**.

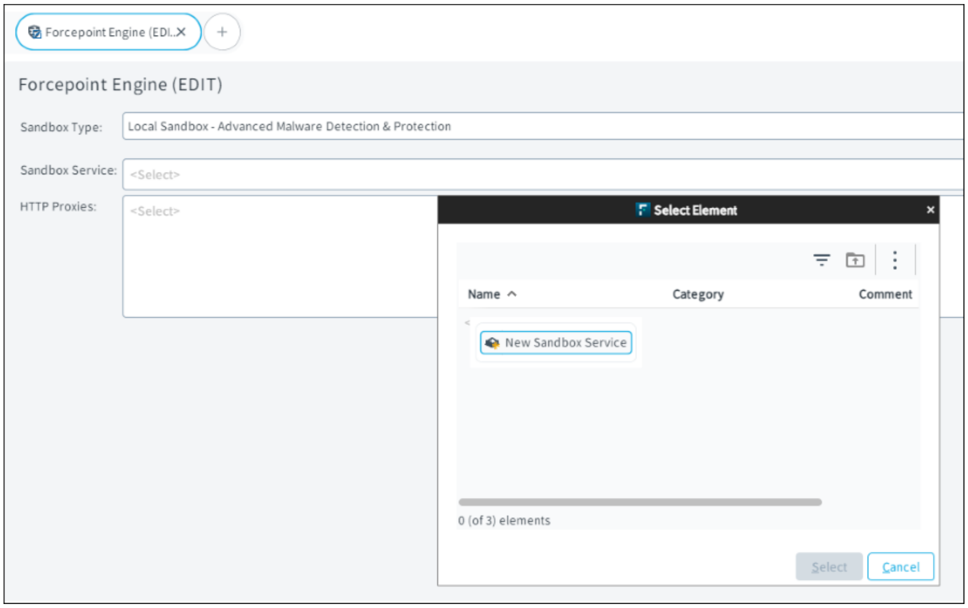


Forcepoint Engine (EDIT)

Sandbox Type: None

None
Cloud Sandbox - Advanced Malware Detection & Protection
Local Sandbox - Advanced Malware Detection & Protection
Cloud Sandbox - Advanced Malware Detection
Local Sandbox - Advanced Malware Detection

3) Select the **Sandbox Service** field and create a **New Sandbox Service** element in the pop-up that appears.



Forcepoint Engine (EDIT)

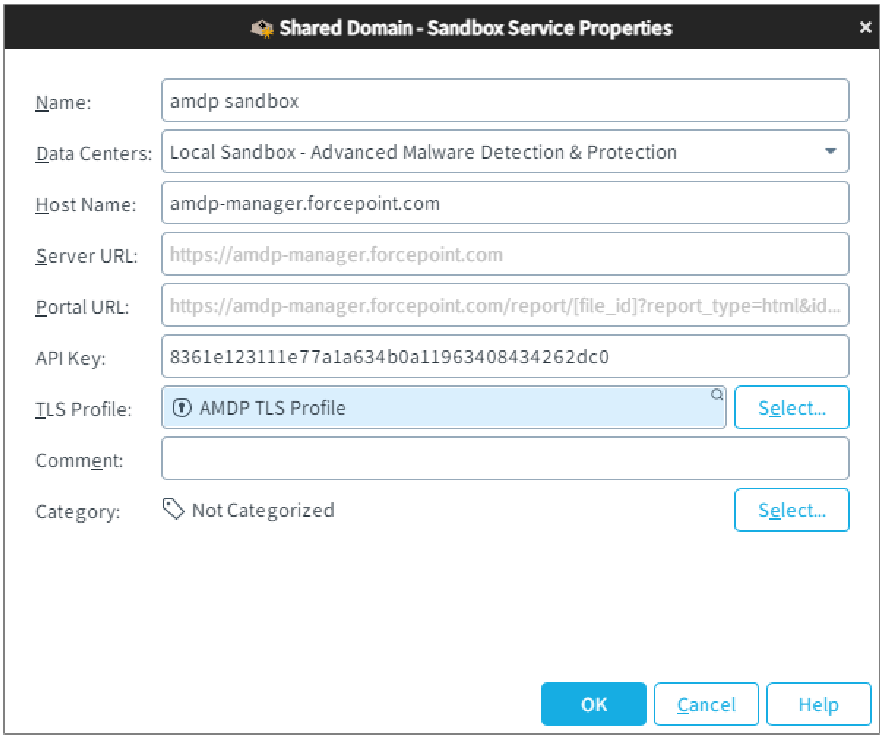
Sandbox Type: Local Sandbox - Advanced Malware Detection & Protection

Sandbox Service: <Select>

HTTP Proxies: <Select>

0 (of 3) elements

4) Under **Host Name** field add the domain name or IP address of the AMDP Manager and under **API Key** field, enter your AMDP License. Under **TLS Profile**, click **Select** and create a new TLS Profile.



Name: amdp sandbox

Data Centers: Local Sandbox - Advanced Malware Detection & Protection

Host Name: amdp-manager.forcepoint.com

Server URL: https://amdp-manager.forcepoint.com

Portal URL: https://amdp-manager.forcepoint.com/report/[file_id]?report_type=html&id...

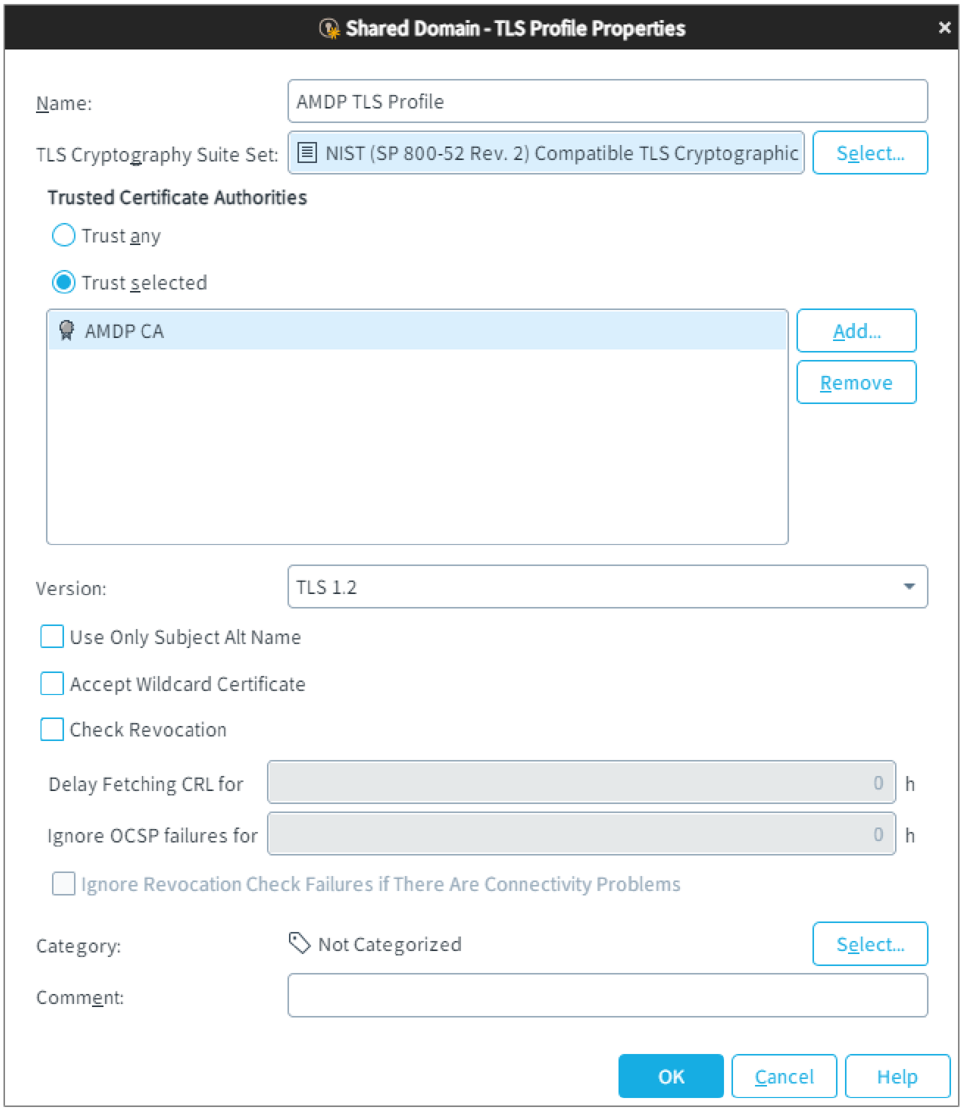
API Key: 8361e123111e77a1a634b0a11963408434262dc0

TLS Profile: AMDP TLS Profile

Comment:

Category: Not Categorized

5) Select an appropriate Cryptographic Suite such as **NIST (SP 800-52 Rev. 2)**. Either use **Trust any** under **Trusted Certificate Authorities** or upload the AMDP Manager certificate to the SMC and add that to the trusted CA list. Select **OK** to finish creating the Sandbox Service element.



Name: AMDP TLS Profile

TLS Cryptography Suite Set: NIST (SP 800-52 Rev. 2) Compatible TLS Cryptographic

Trusted Certificate Authorities

○ Trust any

● Trust selected

AMDP CA

Version: TLS 1.2

□ Use Only Subject Alt Name

□ Accept Wildcard Certificate

□ Check Revocation

Delay Fetching CRL for 0 h

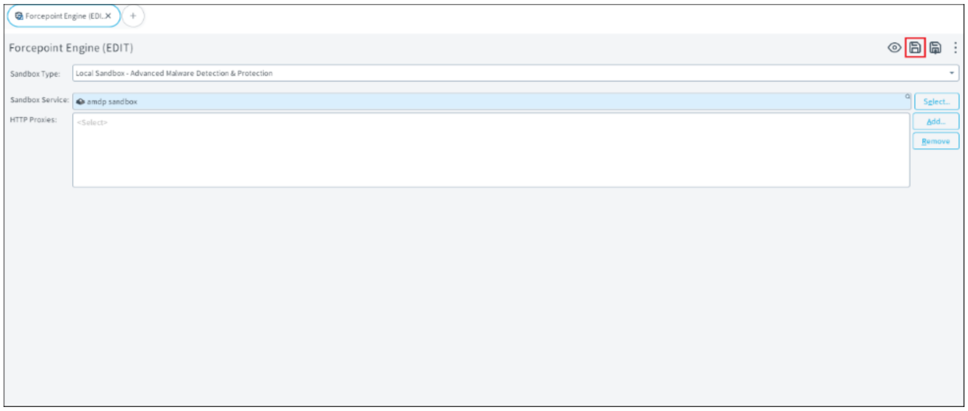
Ignore OCSP failures for 0 h

□ Ignore Revocation Check Failures if There Are Connectivity Problems

Category: Not Categorized

Comment:

6) Select the newly created Sandbox Service element from the list and save your engine configuration.



Forcepoint Engine (EDIT)

Sandbox Type: Local Sandbox - Advanced Malware Detection & Protection

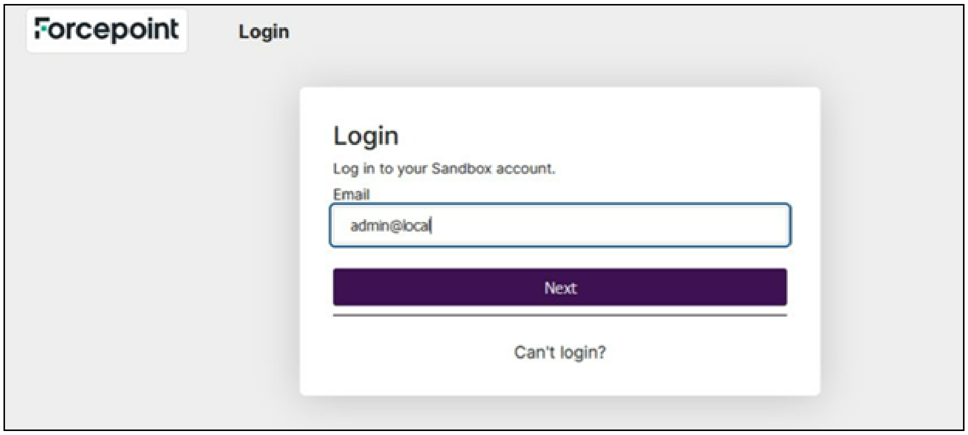
Sandbox Service: amdp sandbox

HTTP Proxies: <Select>

Admin Web Portal

The Admin Web Portal user interface allows you to verify the state of the sandbox machine availability, to manually submit samples (useful for troubleshooting), to view and edit the default analysis profile, to view reports, and to administer the Admin account (add/remove other accounts).

- Log into the Admin Web Portal with the email address and password of the user you added on the Manager in the Organization screen of the wizard.

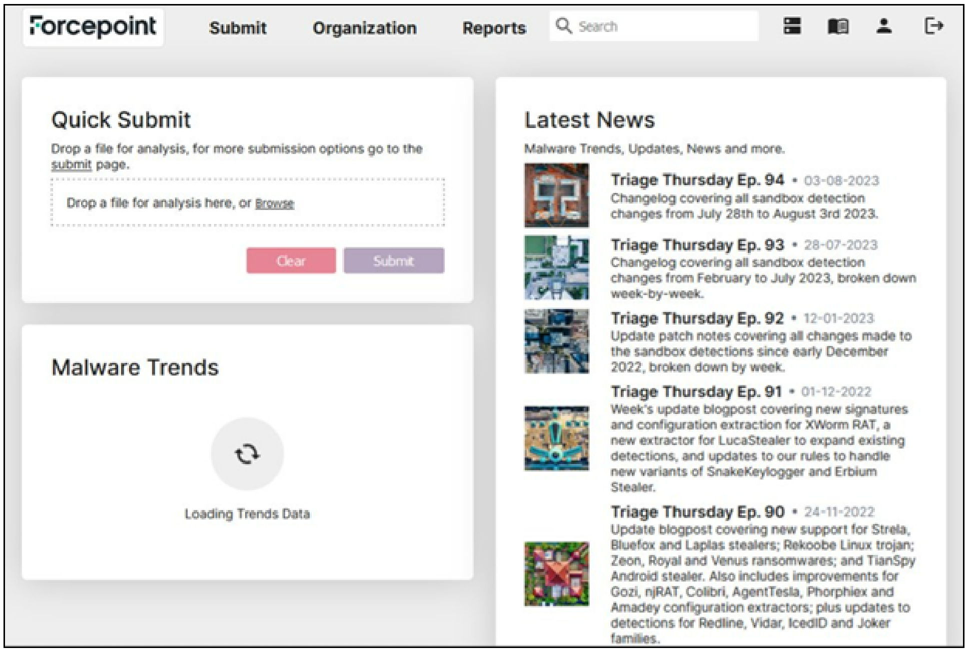


Login

Log in to your Sandbox account.

Email: admin@local

The dashboard is the initial view when logging into the portal.



Quick Submit

Drop a file for analysis, for more submission options go to the submit page.

Drop a file for analysis here, or Browse

Malware Trends

Loading Trends Data

Latest News

Malware Trends, Updates, News and more.

Triage Thursday Ep. 94 • 03-08-2023
Changelog covering all sandbox detection changes from July 28th to August 3rd 2023.

Triage Thursday Ep. 93 • 28-07-2023
Changelog covering all sandbox detection changes from February to July 2023, broken down week-by-week.

Triage Thursday Ep. 92 • 12-01-2023
Update patch notes covering all changes made to the sandbox detections since early December 2022, broken down by week.

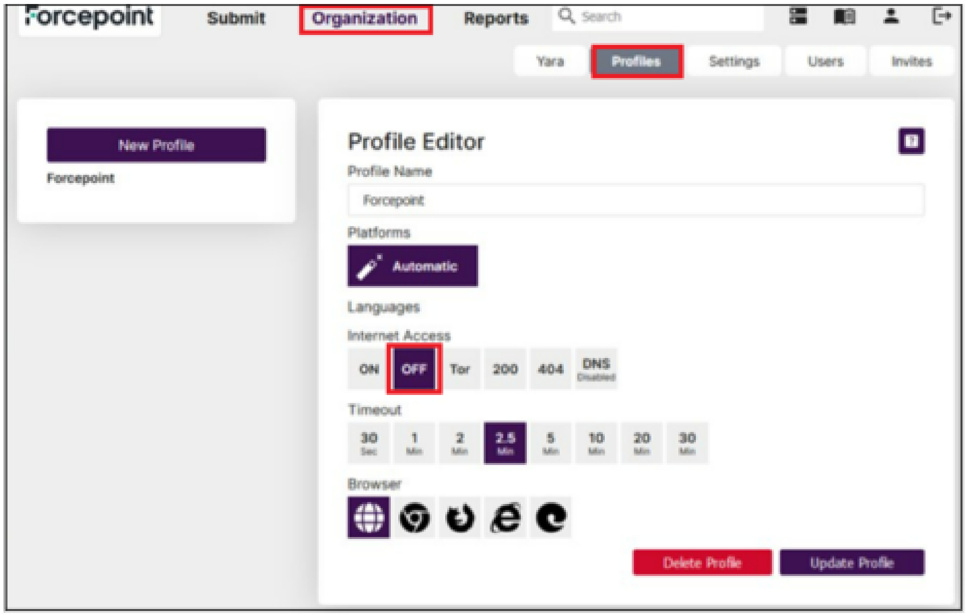
Triage Thursday Ep. 91 • 01-12-2022
Week's update blogpost covering new signatures and configuration extraction for XWorm RAT, a new extractor for LucaStealer to expand existing detections, and updates to our rules to handle new variants of SnakeKeylogger and Erbium Stealer.

Triage Thursday Ep. 90 • 24-11-2022
Update blogpost covering new support for Strela, Bluefox and Laplas stealers; Rekoobe Linux trojan; Zeon, Royal and Venus ransomwares; and TianSpy Android stealer. Also includes improvements for Gozi, njRAT, Colibri, AgentTesla, Phorphiex and Amadey configuration extractors; plus updates to detections for Redline, Vidar, IcedID and Joker families.

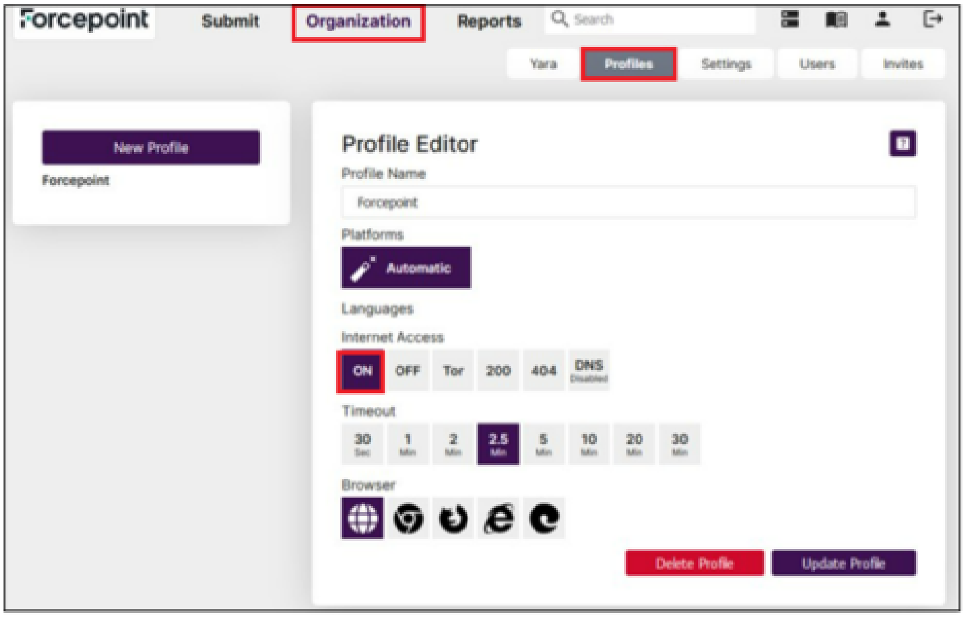
- Profiles control various aspects for control of the sandbox detonation. Select the **Organization** tab, then select **Profiles**. The default profile used for sample analysis is called “Forcepoint”. The default for **Internet access** is **OFF** to enhance the security of the system. There is a trade off in setting internet access to off in a loss of efficacy and each customer should determine what best suites their needs.

CAUTION

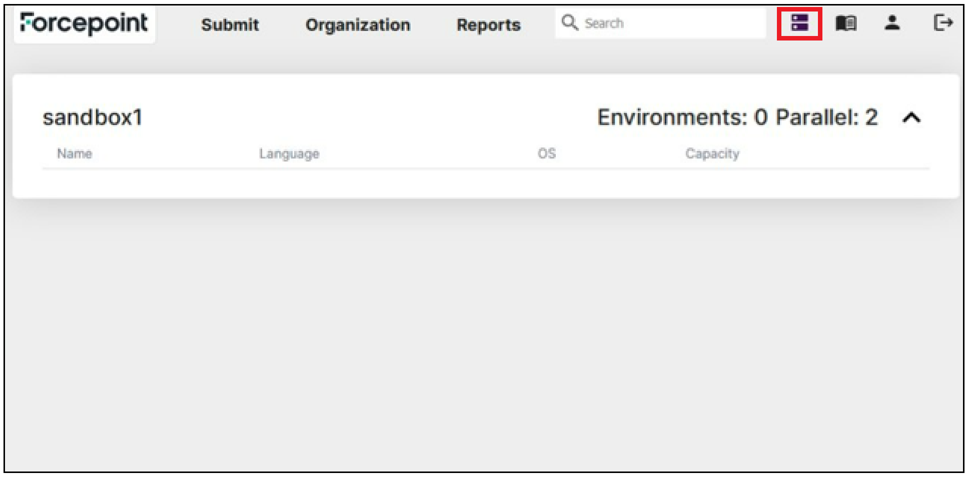
The default profile (Forcepoint) should not be deleted.



Here we modify the **Forcepoint** profile to enable **Internet access** (setting changed to ON).



- The **Machines** tab is selected via the icon highlighted in red below (just left of the docs/help icon). Here is the initial configuration after an Engine has been configured and added to the Manager. The Environments count reflects the total of the instance counts for each configured virtual machine. The Parallel count is the number of environments which can be executed simultaneously. That value is set when the Engine is initially configured and based on the number of CPUs in the Engine.

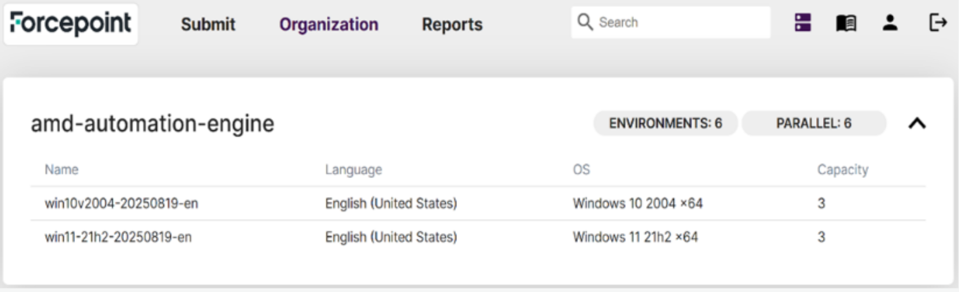


sandbox1

Environments: 0 Parallel: 2

Name	Language	OS	Capacity

Once the VMs have been built, the available machine types are shown on the **Machines** tab. Note for this example, there are 6 environments available (3 windows 10, 3 windows 11), and 2 VMs can operate in parallel. If an analysis requires a machine type but all the parallel slots are in use, the analysis will be queued until a parallel slot becomes available.

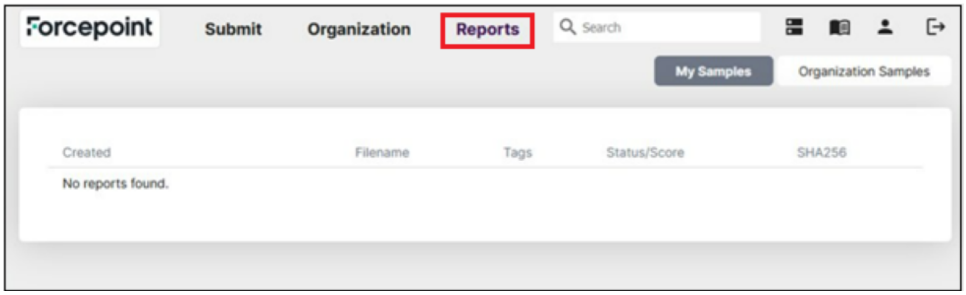


amd-automation-engine

ENVIRONMENTS: 6 PARALLEL: 6

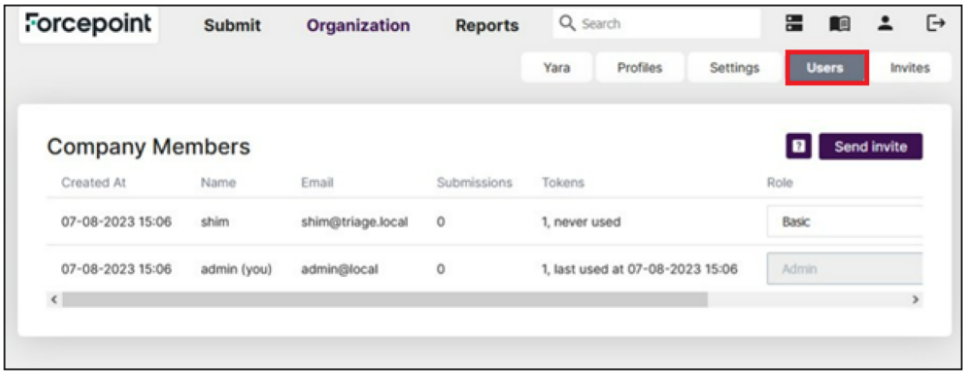
Name	Language	OS	Capacity
win10v2004-20250819-en	English (United States)	Windows 10 2004 x64	3
win11-21h2-20250819-en	English (United States)	Windows 11 21h2 x64	3

- Selecting the **Reports** tab shows the samples which have been submitted and the associated analysis. **My Samples** only shows samples for the user logged into the portal. To see samples/reports which were submitted to the Manager, select the **Organization Samples** tab.



Created	Filename	Tags	Status/Score	SHA256
No reports found.				

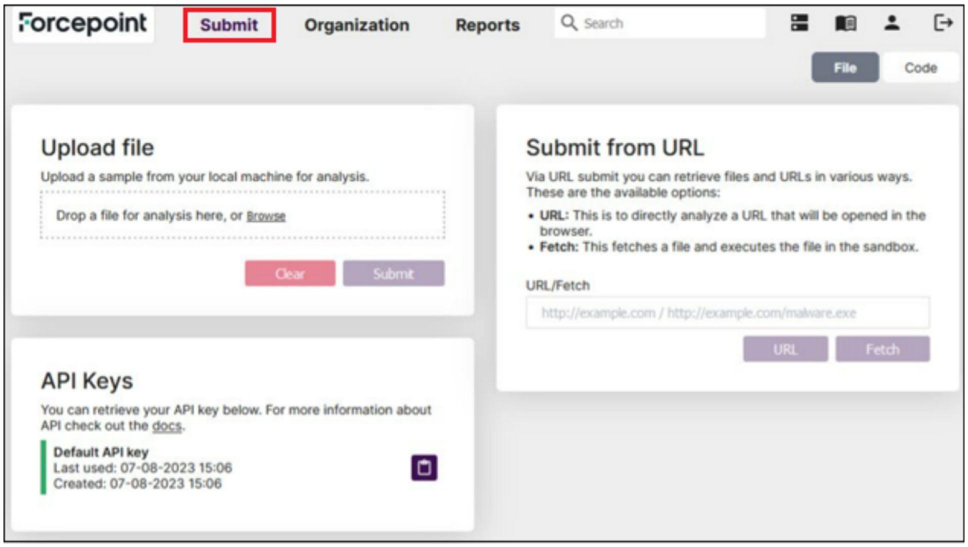
- Selecting the **Users** tab allows you to view the configured Users for the system. There is a reserved user “**shim@triage.local**” which is used to relay the samples received by the Manager. You should not modify or delete this user.The user with (you) indicates the currently logged in user, which is the user created in the registration wizard on the Organization (web portal) screen for the Manager.



Company Members

Created At	Name	Email	Submissions	Tokens	Role
07-08-2023 15:06	shim	shim@triage.local	0	1, never used	Basic
07-08-2023 15:06	admin (you)	admin@local	0	1, last used at 07-08-2023 15:06	Admin

- The **Submit** tab allows for manual upload and analysis of files.



Upload file

Upload a sample from your local machine for analysis.

Drop a file for analysis here, or Browse

Submit from URL

Via URL submit you can retrieve files and URLs in various ways. These are the available options:

- **URL:** This is to directly analyze a URL that will be opened in the browser.
- **Fetch:** This fetches a file and executes the file in the sandbox.

URL/Fetch

http://example.com / http://example.com/malware.exe

API Keys

You can retrieve your API key below. For more information about API check out the docs.

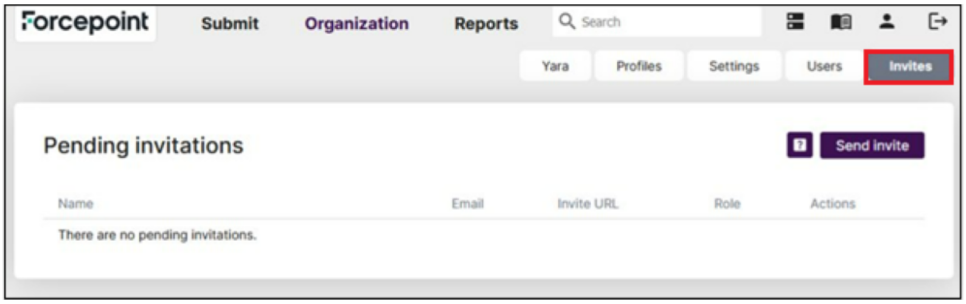
Default API key
Last used: 07-08-2023 15:06
Created: 07-08-2023 15:06

Note

Files submitted through the Admin Web Portal will not generate a score visible to other products integrating with AMDP.

- The **Invites** tab is used to craft an invitation with initial login details for a newly created user. The primary use case is to add other Portal Administrator accounts.
  Delivering invitations via the email channel is not supported. An Admin should select a pending invitation and click the clipboard icon to copy the invite URL. The Admin should then send the invite URL to the intended new user using their email application or some other method.

  The new user then follows the link provided in the invite to setup their new account.



Pending invitations

Name	Email	Invite URL	Role	Actions
There are no pending invitations.				

Published 17 December 2025