ENDPOINT PROTECTOR | 4

User Manual Version 1.0.0.0

AWS / Amazon Web Services EC2 for Endpoint Protector User Manual

COSOSYS

Table of Contents

1. Getting Started 1
1.1. Introduction 1
1.2. Locate AMI of Endpoint Protector 4 on AWS Marketplace or AWS Management Console 1
1.3. Licensing for Endpoint Protector with AWS 2
1.4. Setting up an EC2 Instance 3
1.5. Accessing Endpoint Protector Web Interface 12
2. What Endpoint Protector does 14
3. Support 17
4. Important Notice / Disclaimer 18

1. Getting Started

1.1. Introduction

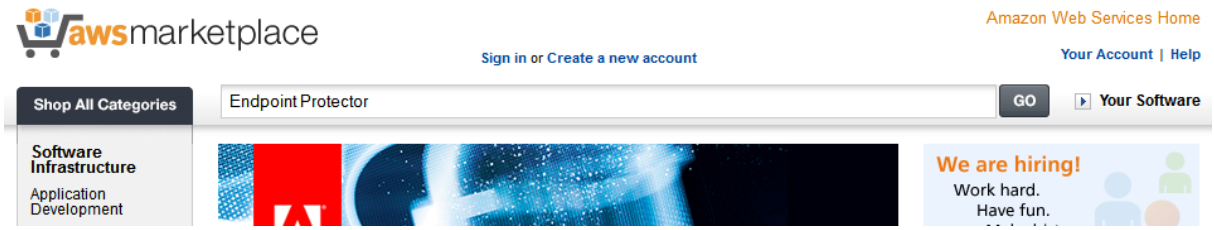
This manual gives a short guidance on how to use an Endpoint Protector 4 (server part) AMI with Amazon Web Services (short AWS).

It shows you the steps in order to run the Endpoint Protector 4 server part as an Amazon EC2 instance.

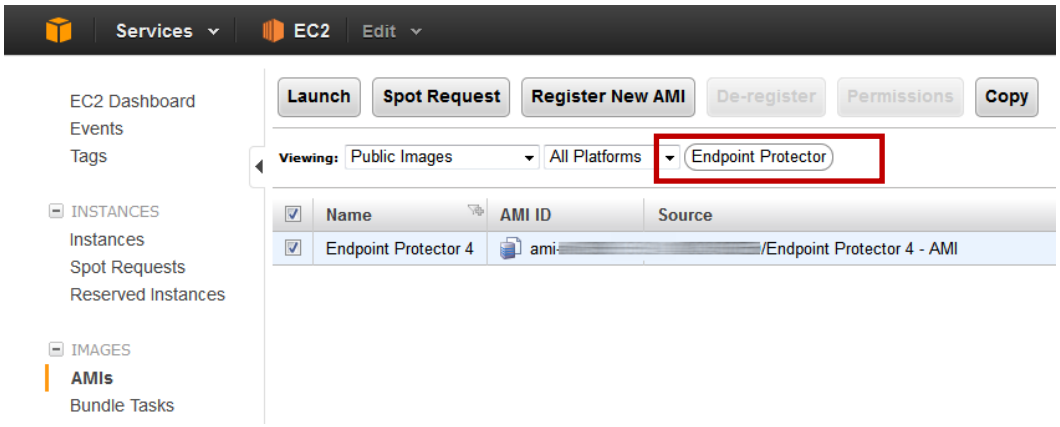
For information about general use of Endpoint Protector 4 and its features please consult the Endpoint Protector 4 User Manual.

1.2. Locate AMI of Endpoint Protector 4 on AWS Marketplace or AWS Management Console

Endpoint Protector 4 is available as an AMI on the AWS Marketplace, to find it search for Endpoint Protector on the AWS Marketplace:



or after logging in your AWS account in the AWS Management Console:

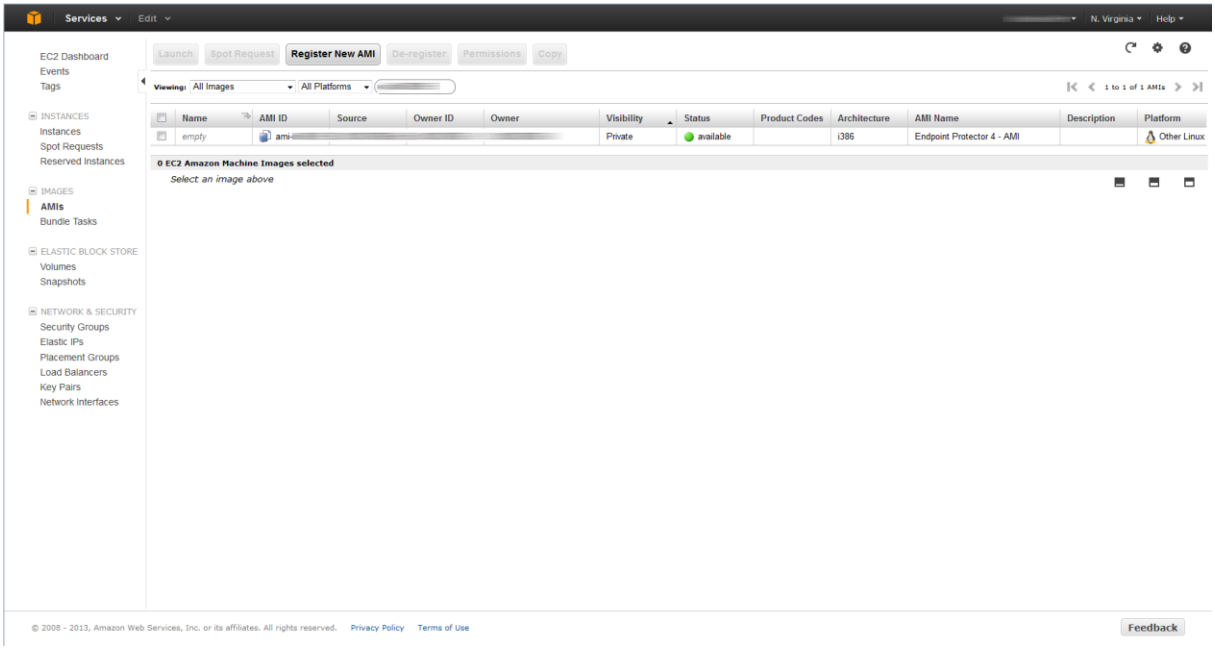


1.3. Licensing for Endpoint Protector with AWS

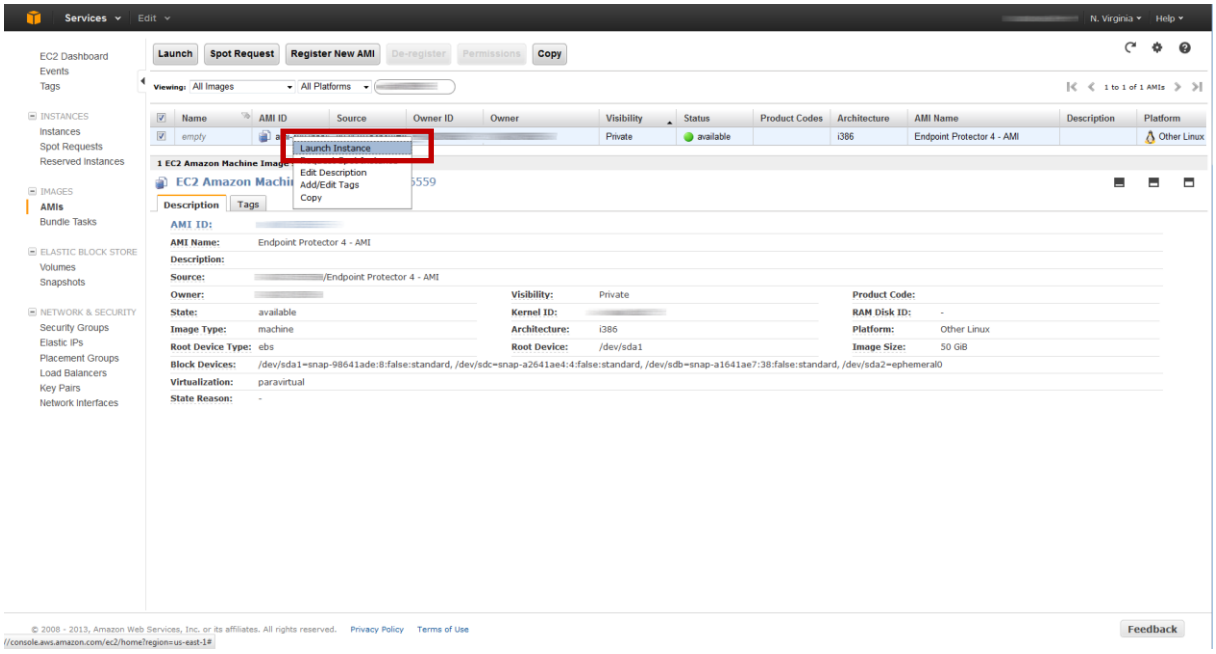
Endpoint Protector 4 is a Bring your Own License (BYOL) Instance. It means you are paying Amazon for running the instance and you import your license file that you have purchased from CoSoSys or any CoSoSys Partner. The license fee for using Endpoint Protector with AWS is the same as for licensing Endpoint Protector 4 as a Virtual Appliance. To purchase a license please contact your CoSoSys Distribution Partner or sales@cososys.com.

1.4. Setting up an EC2 Instance

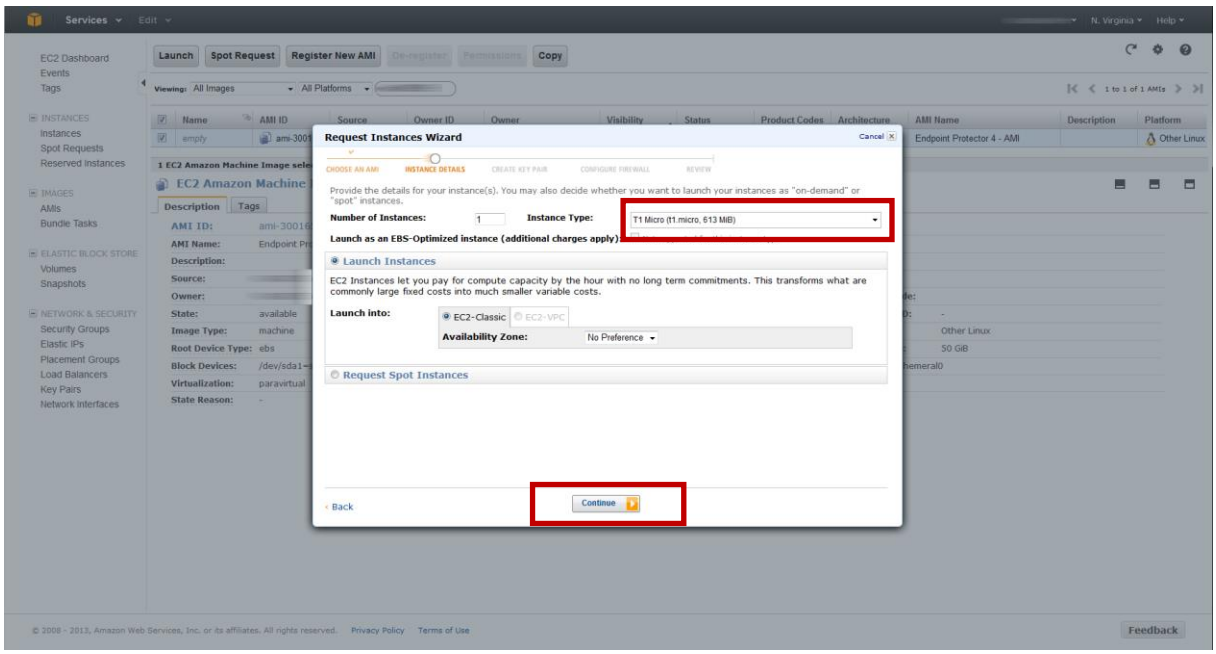
After finding the Endpoint Protector 4 AMI in your AWS Management Console, select it,



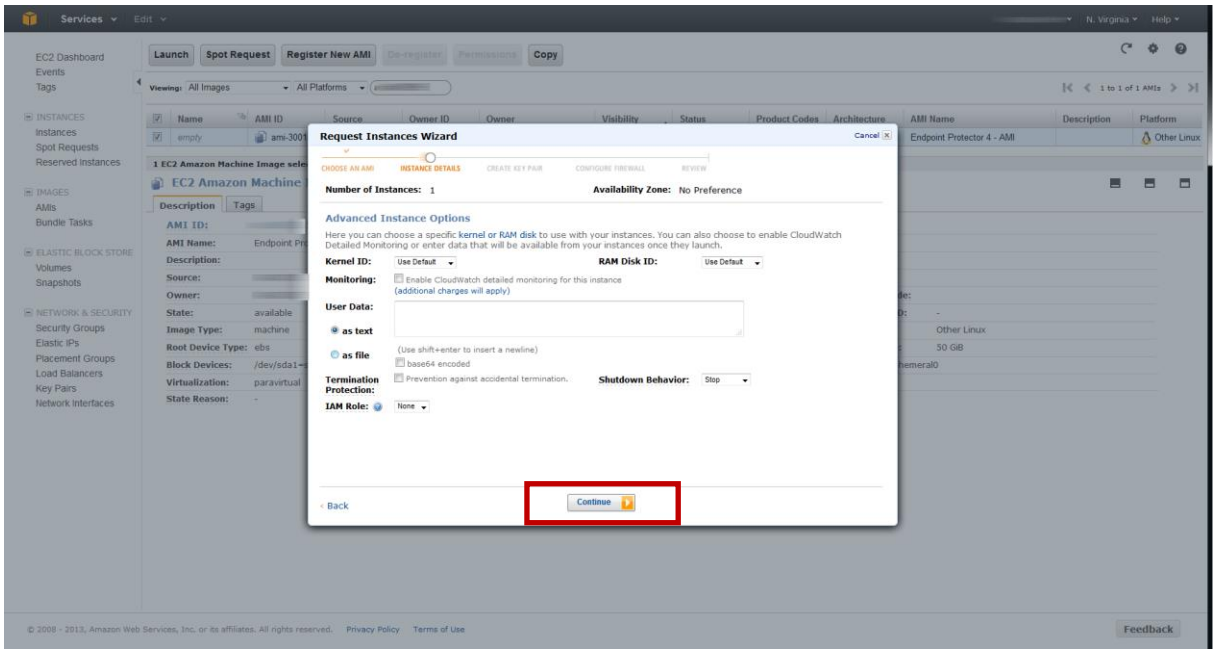
Choose "Launch Instance" from the right click menu which will launch the "Request Instance Wizard".



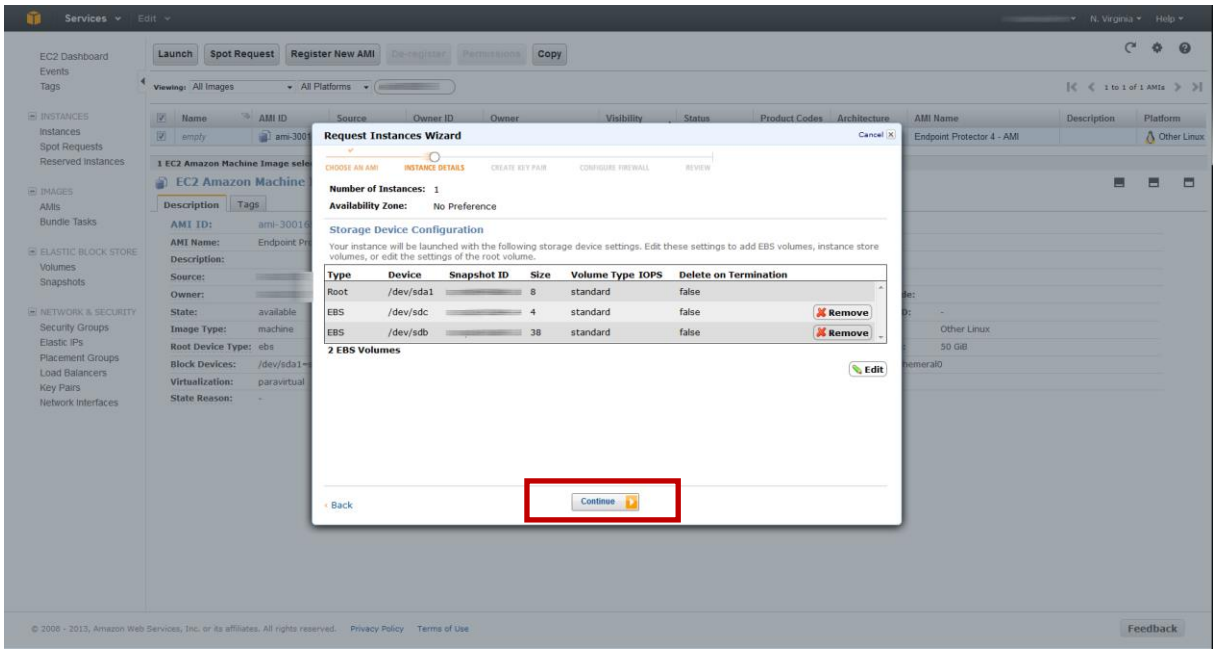
Choose an Instance Type and "Region/Availability Zone" and click "Continue". The default Endpoint Protector 4 AMI you are using is optimized to be run as a small T1 Micro instance. It is the optimal size to support deployment with 50 protected Endpoints and 50 mobile iOS/Android mobile devices. To support larger deployment of Endpoint Protector please contact support@endpointprotector.com to have your instance adjusted for greater performance with one of our experts.



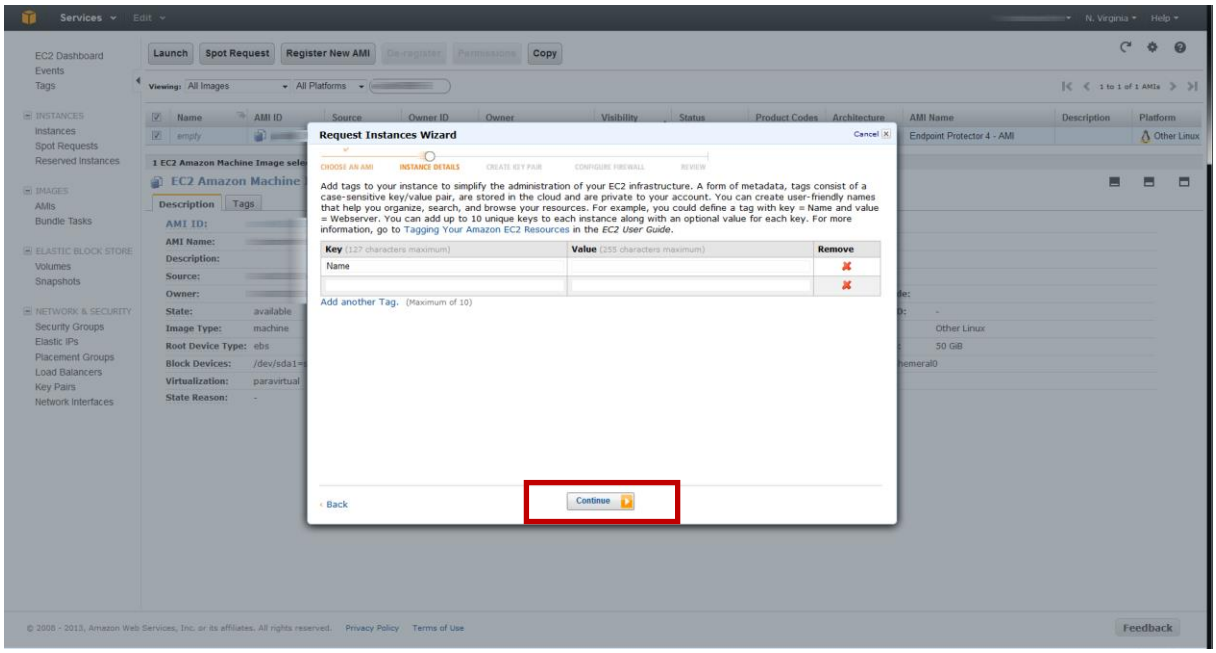
Instance Details do not require any adjustments, click “Continue”.



Storage Device Configuration does not require any changes, click “Continue”. If you remove any of the assigned EBS Volumes the Instance will fail to start.

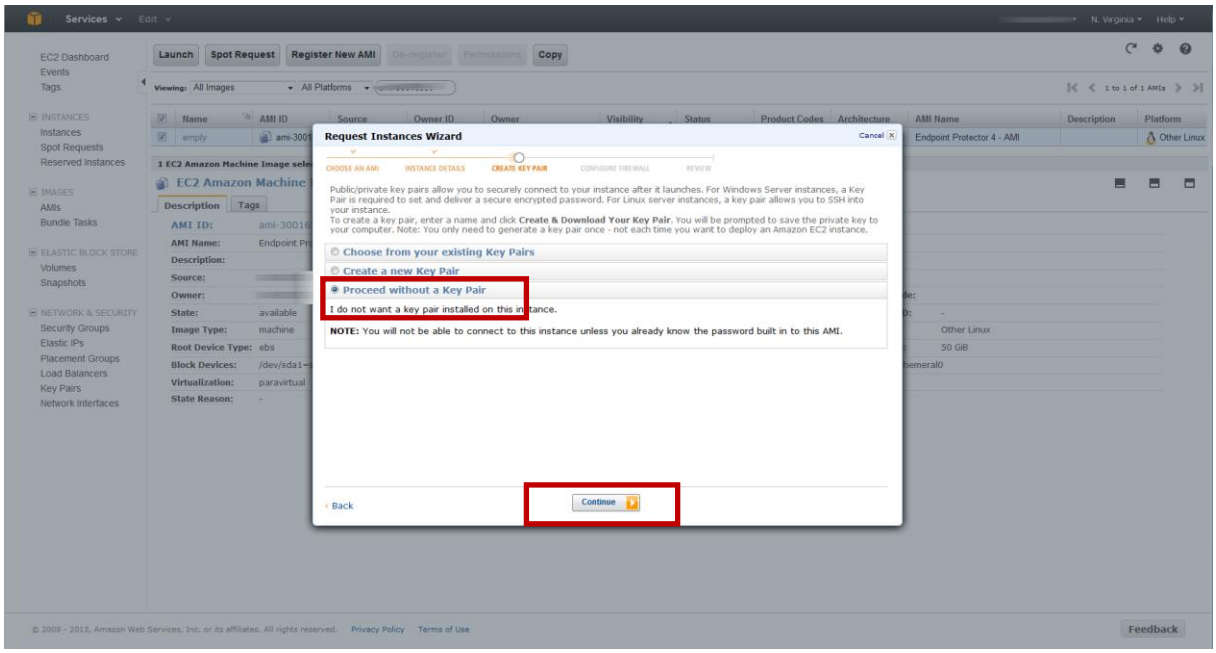


Adding Tags is your own choice. Click "Continue".



In the step "Create Key Pair" we recommend you to choose the option "Proceed without a Key Pair".

If you choose to use a key pair you might have to share it with our support team for support requests. If you choose to use Key Pair make sure it is only used for this instance. Click "Continue".



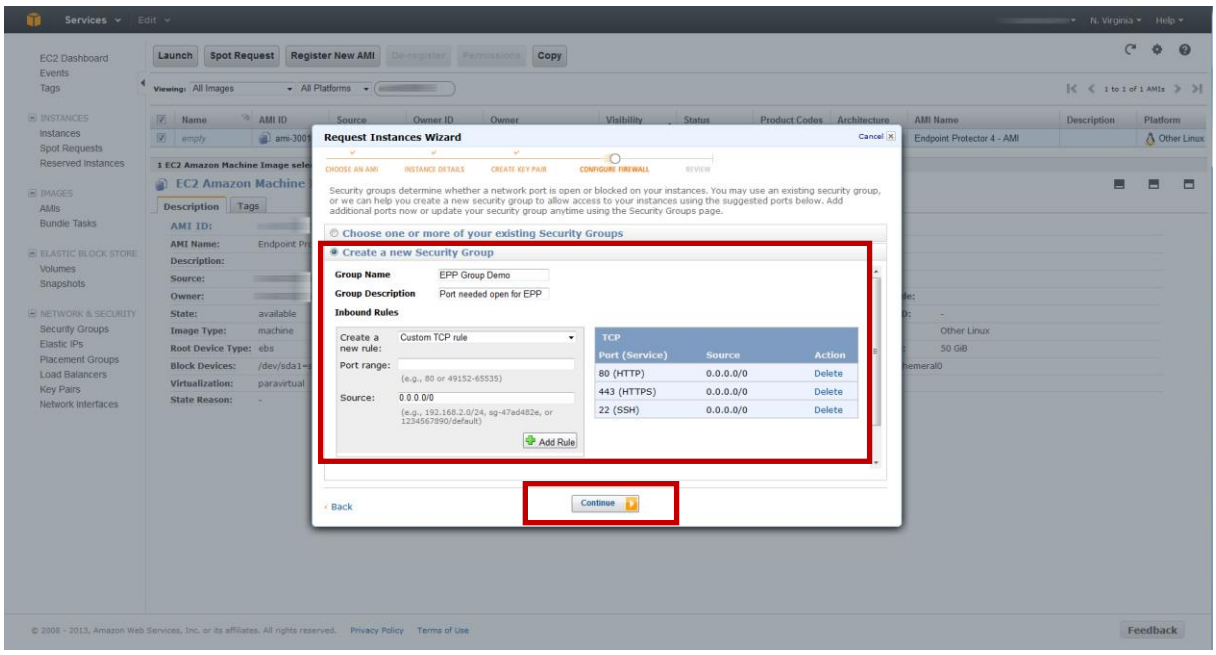
In the step "Configure Firewall" we recommend you to make the following settings. Choose the option "Create a new Security Group".

Give the Group a Name and a Description.

For Inbound Rules choose "Create a new Rule" choose "Custom TCP rule" from the dropdown.

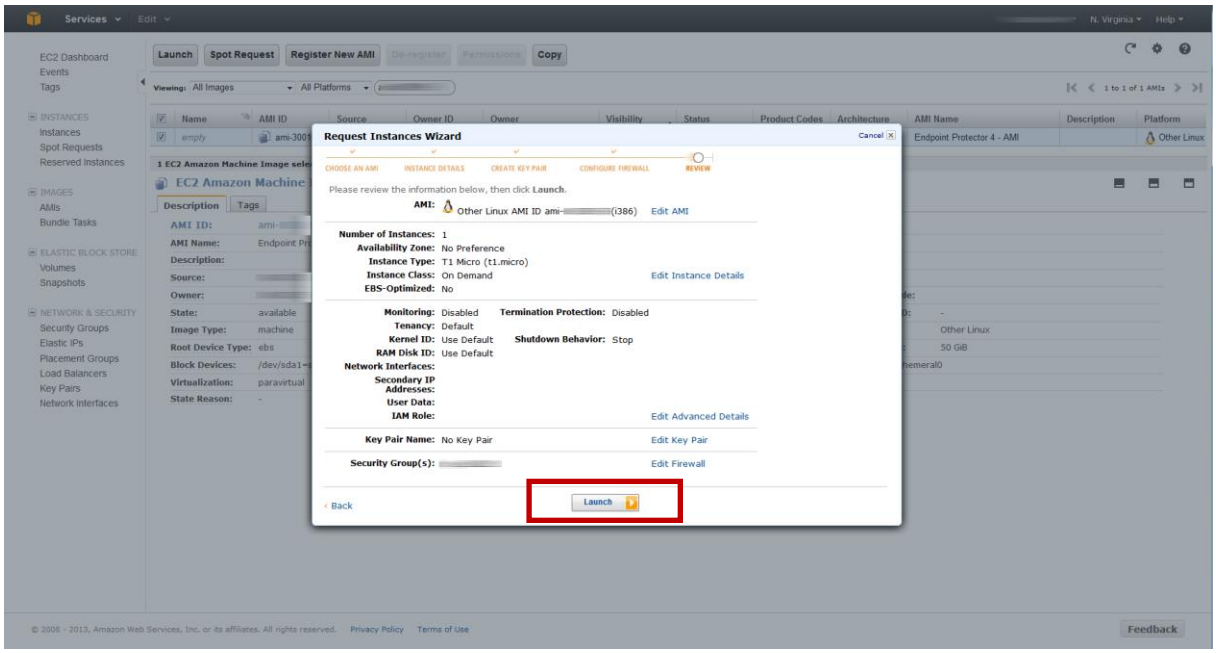
Add port 80 and click "+Add Rule",
add port 443 and click "+Add Rule",
add port 22 and click "+Add Rule".

Click "Continue".

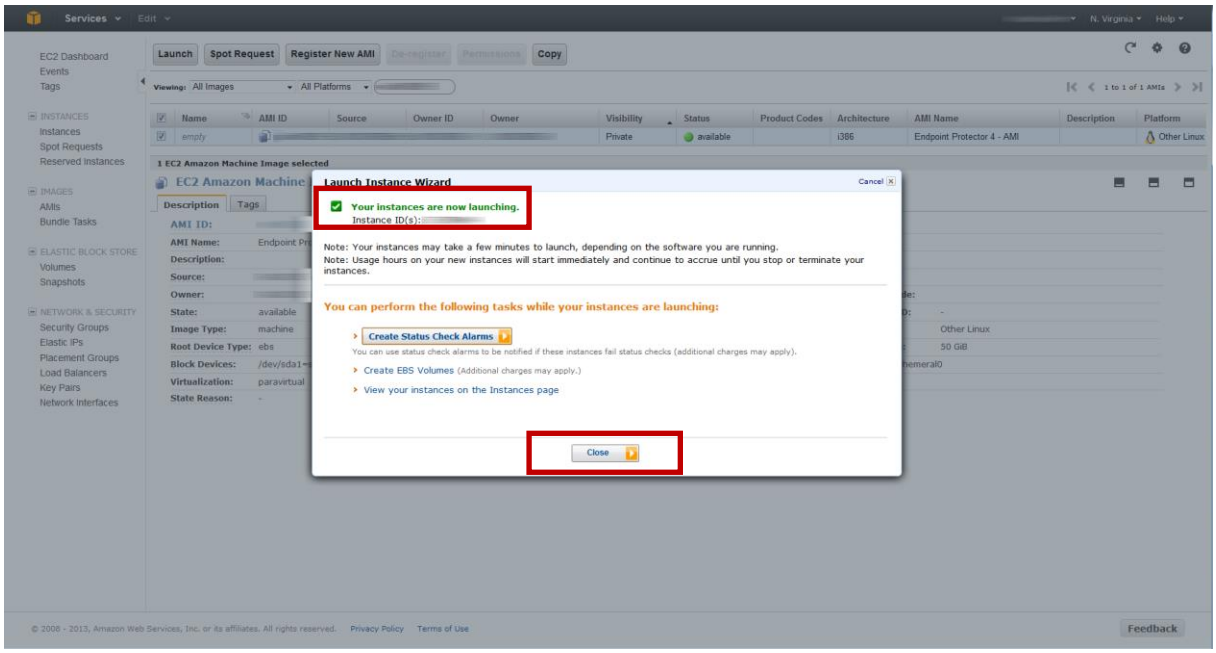


The ports are required as follows, port 22 for support, 80 for http access and 443 for interface access and client – server communication.

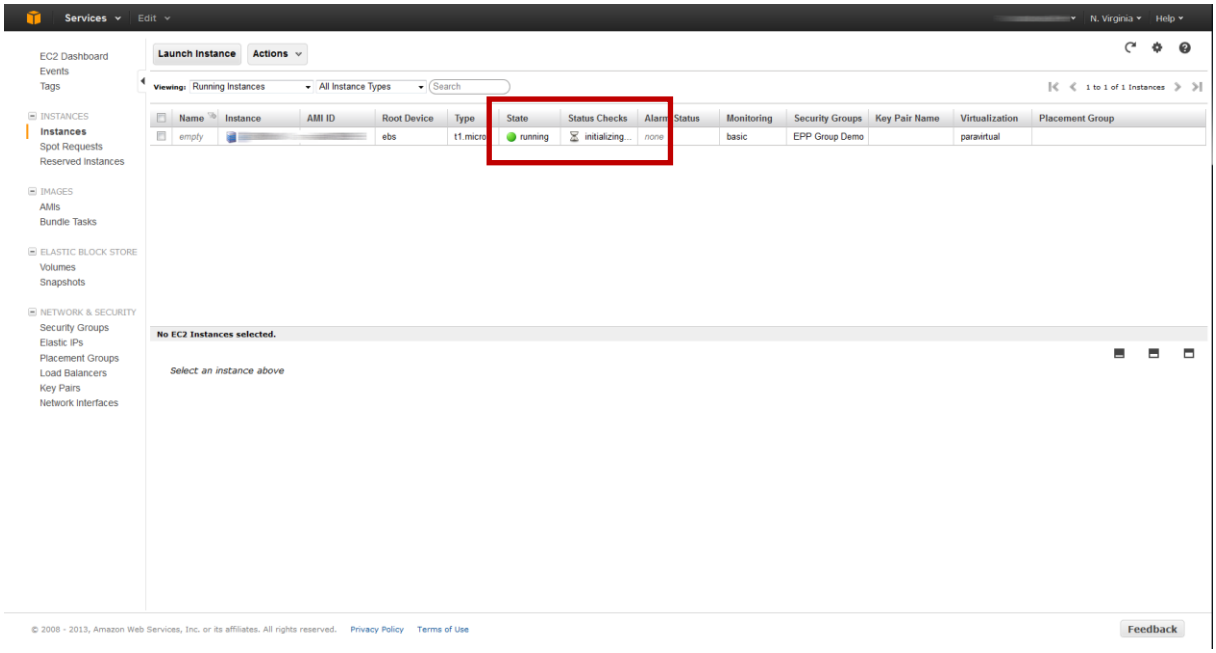
Review your settings and click "Launch" your instance.



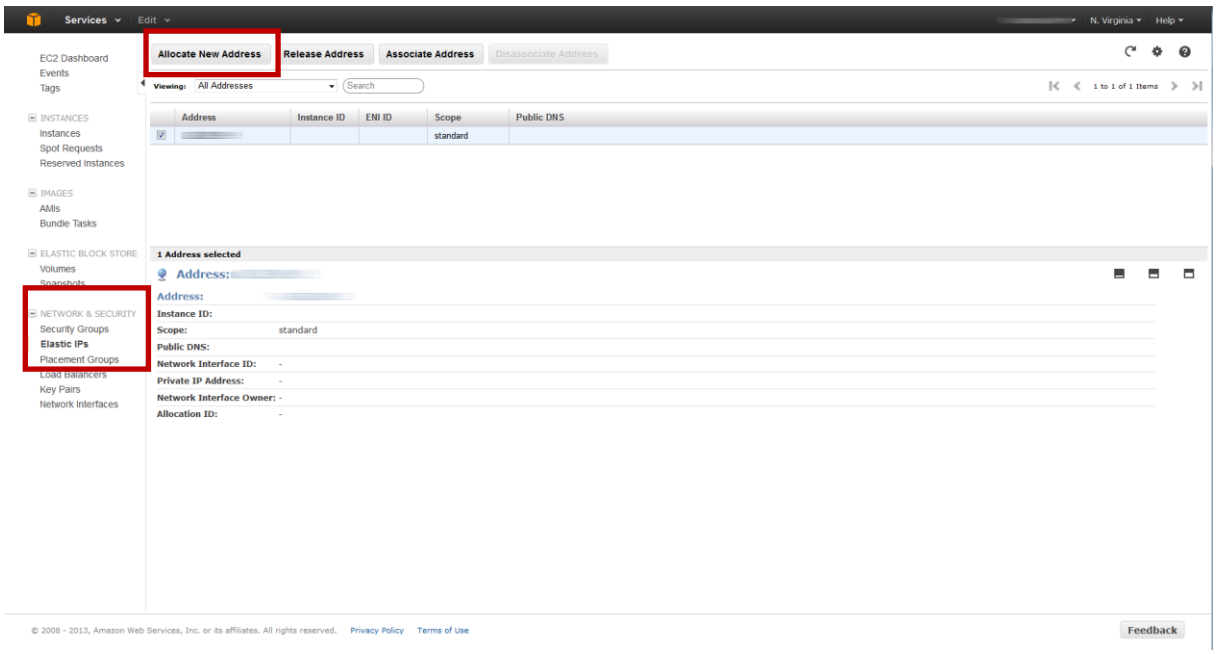
You see the message that "your instance is launching". Choose "Close" to finish the Launch Instance Wizard.



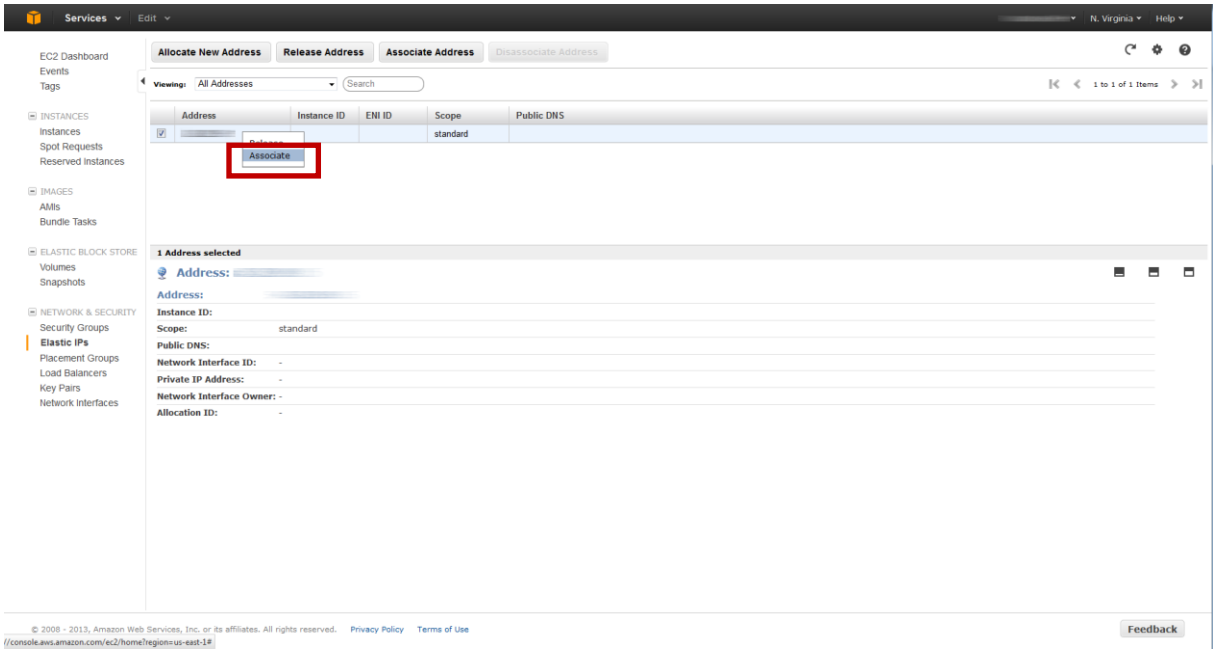
Wait for the instance to start. This might take a few minutes while the "Status Checks" appears as "Initializing".



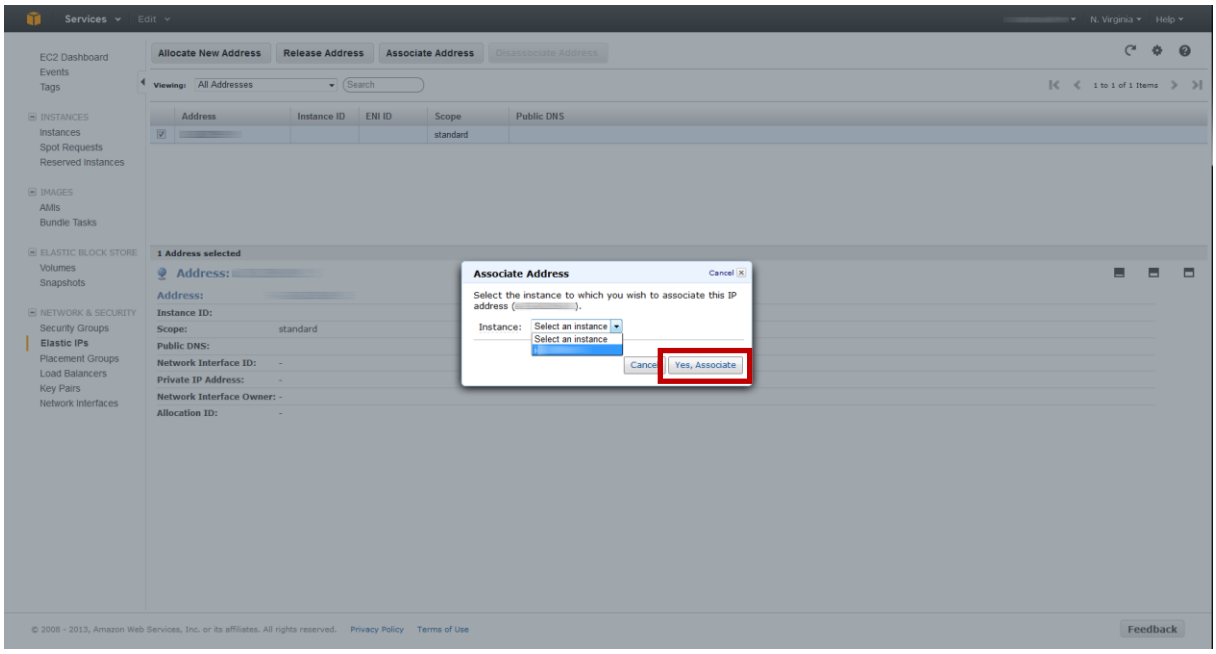
As a next step we recommend you to request an Elastic IP. This is required so the Endpoint Protector Clients can communicate with the same IP Address in case the instance is restarted. Without an Elastic IP (Static IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled. To request an Elastic IP go in the AWS Management Console to the option Network & Security > Elastic IPs and click "Allocate New Address".



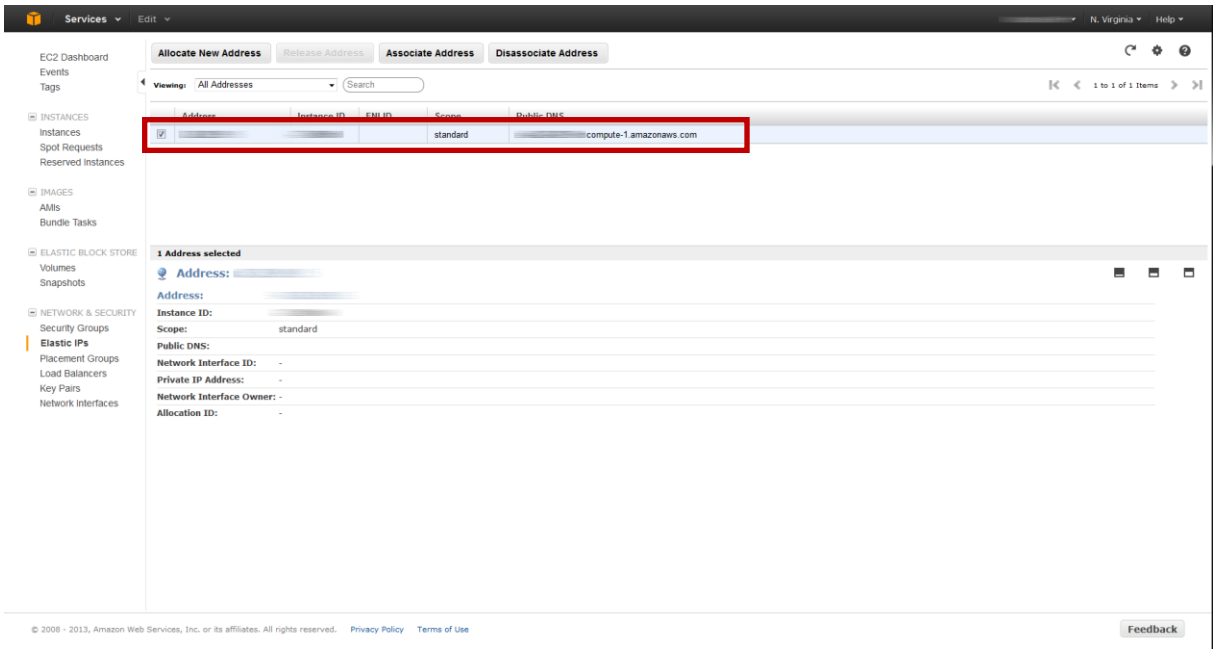
Now associate the Elastic IP with your Endpoint Protector Instance. For that select the IP Address and click “Associate”.



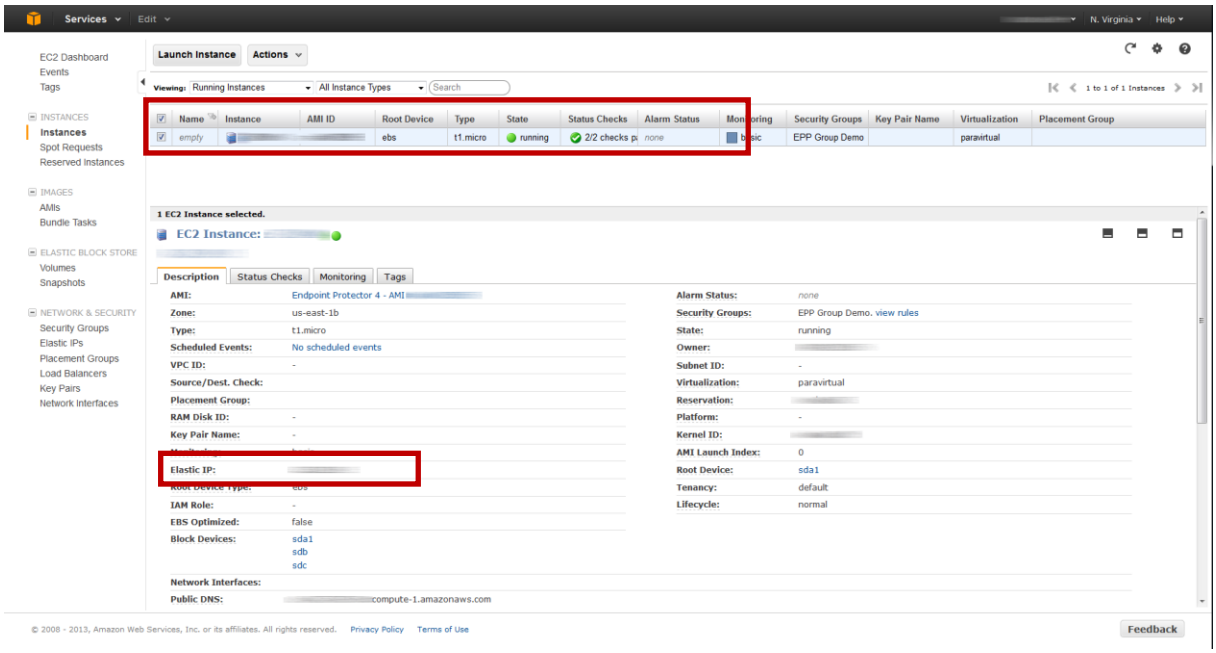
Select the Endpoint Protector Instance from the dropdown list and click “Yes, Associate”.



The Elastic IP is now associated with your Endpoint Protector Instance.



After a few minutes the Endpoint Protector Instance is running and is associated with the Elastic IP.



1.5. Accessing Endpoint Protector Web Interface

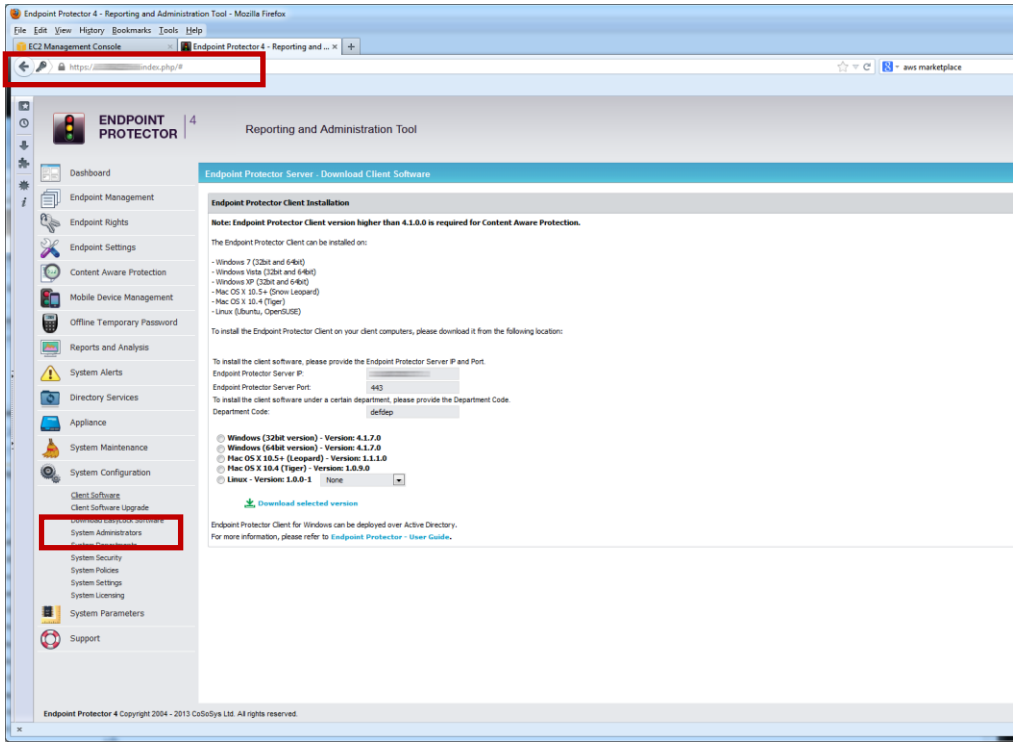
As a next step you can now access your Endpoint Protector through a web-browser to continue and finalize the setup.

Login to interface through **httpS://Elastic IP** using the Elastic IP you have assigned in the previous step.

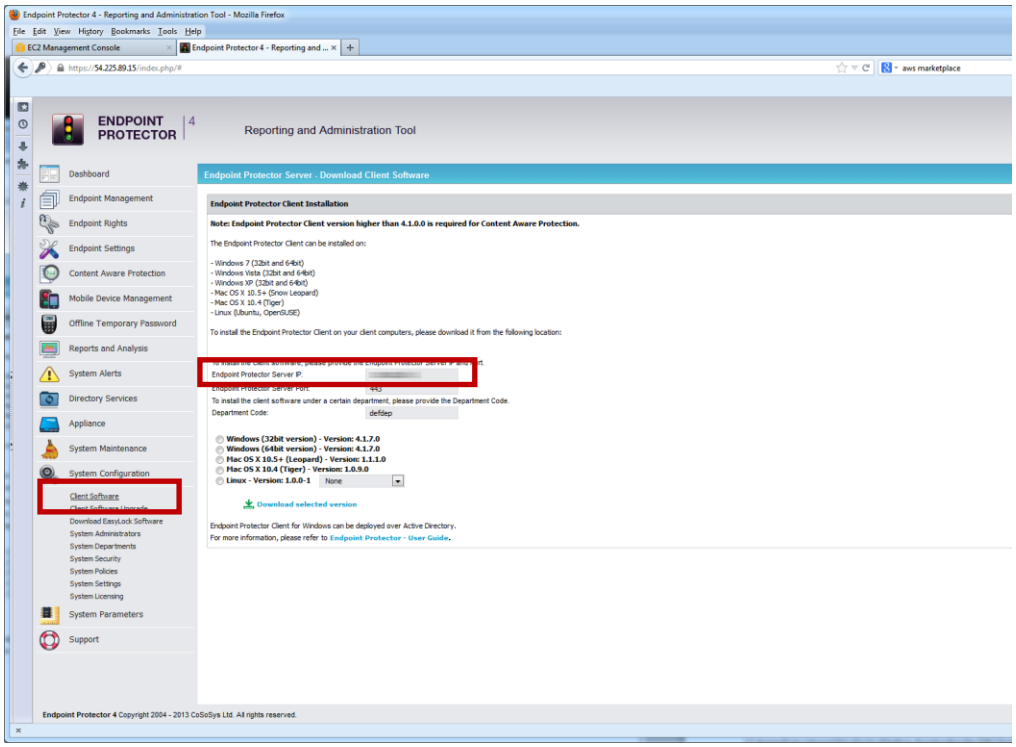
Click "continue/trust or add exception" when your web-browser shows you a warning regarding the certificate of the accessed website.

The default user name to login the Endpoint Protector interface is: **root** and the password is: **epp2011**

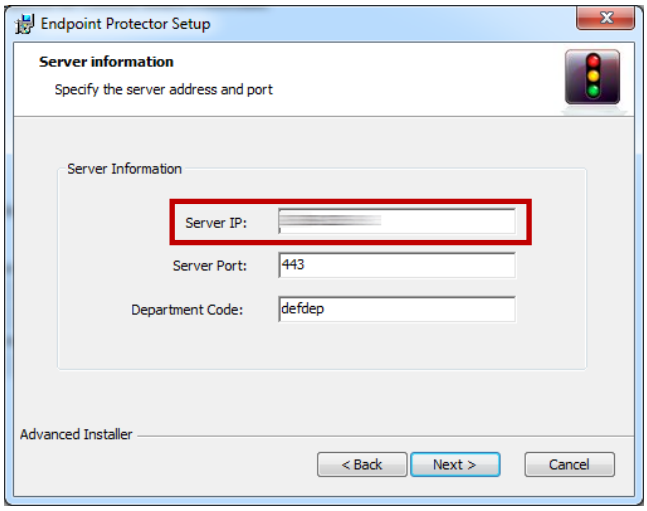
First we recommend you to change the root account password to login in Endpoint Protector in order to secure your EPP instance from unauthorized access. Change the root password under System Configuration > System Administrators.



Now go to System Configuration > Client Software and change the IP Address written in the field "Endpoint Protector Server IP" and change the IP in this field to the Elastic IP you have assigned to the Endpoint Protector Instance.

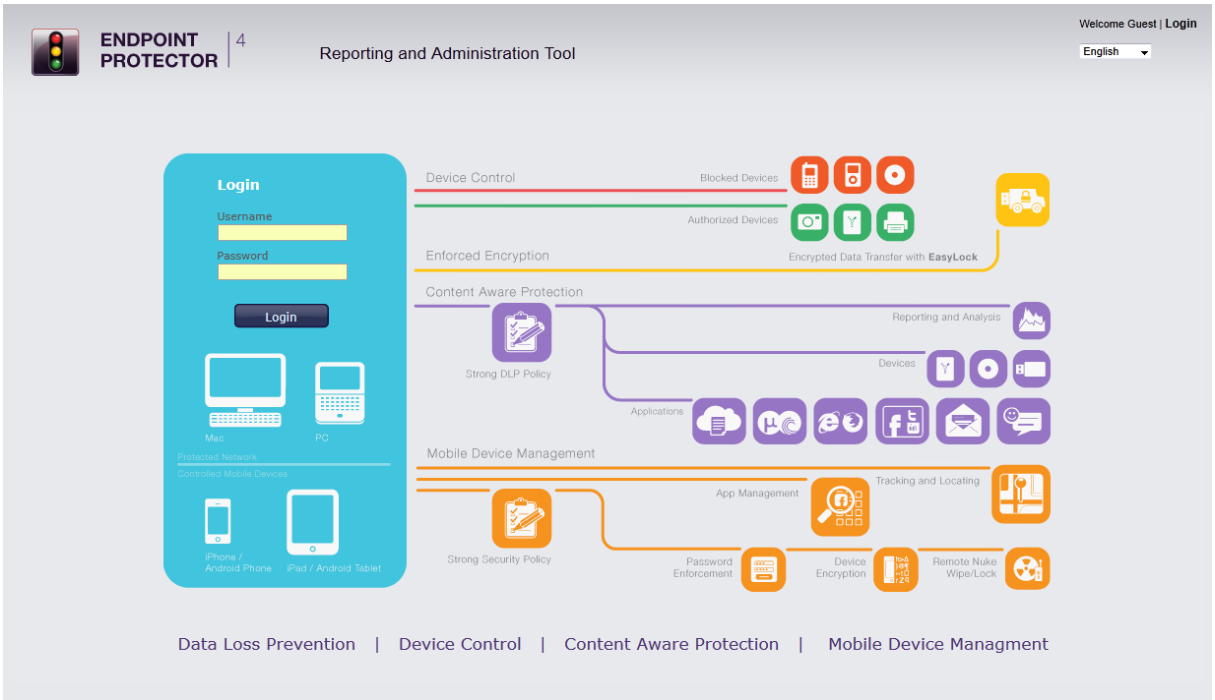


Now you can download the Endpoint Protector Client Software that has the Elastic IP Address already included. Start an Endpoint Protector Client MSI and check in the field Server IP if it corresponds to the Elastic IP. If this is the case you can start deploying your Clients to protect your Windows and Mac OS X endpoints.



2. What Endpoint Protector does

Endpoint Protector is a complete Data Loss Prevention solution for companies' networks of all sizes, enabling a detailed control over removable, mobile storage media and mobile devices both inside and outside the companies' walls.



Endpoint Protector comprises three separate modules, which used together ensures the next generation security of your endpoints:

- **Mobile Device Management**: closely controls and monitors the entire mobile device fleet through dedicated MDM policies, protecting sensitive company data, while permitting a degree of freedom on what concerns the stored personal information. Once integrated in a company or enterprise network, it ensures a highly secure working environment for companies adopting and using the BYOD model.

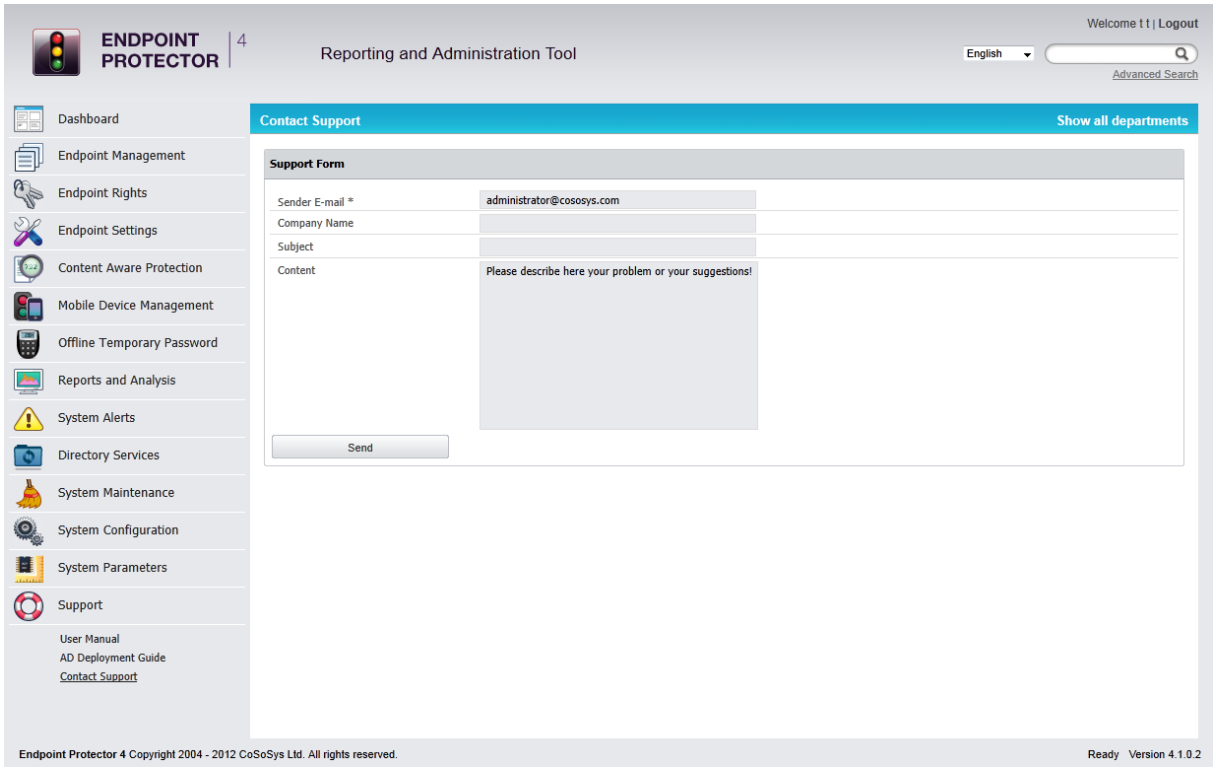
- **Device Control**: enforces strong security policies for controlling and closely monitoring all portable storage device use inside the company network. Once deployed inside companies networks, the Device Control modules reduces the risks of data loss and data theft through unauthorized use of removable and mobile devices through USB, etc..

- **Content Aware Protection**: allows defining custom content aware policies for a detailed inspection, detection and reporting of all sensitive content transfers outside the secured network. Once enabled, the Content Aware Protection module scans all possible exit points and ensures that no critical data leaves the company network either by transfers to removable media or directly via e-mail, file sharing applications or to the cloud.

3. Support

In case additional help, such as the FAQs or e-mail support is required, please visit our support website directly at http://www.endpointprotector.com/support/.

You can also write an e-mail to our Support Department under the Contact Us tab from the Support module.



One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

4. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.