ENDPOINT PROTECTOR

User Manual Version 1.0.0.2

AWS / Amazon Web Services EC2 for Endpoint Protector User Manual

COSOSYS

Table of Contents

1. Getting Started

1.1. Introduction

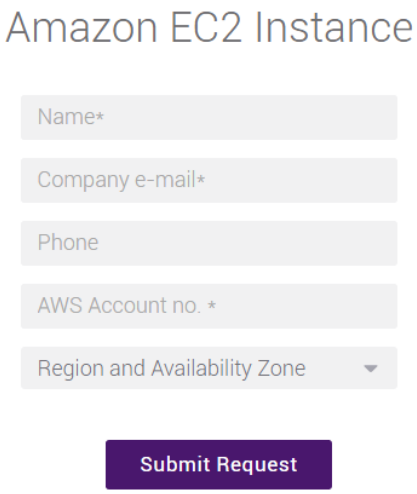
This manual gives a short guidance for using Endpoint Protector Server AMI with AWS, as an Amazon EC2 instance.

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

1.2. Obtaining the EPP AMI on AWS

Endpoint Protector is not generally available in the AWS Marketplace. In order to obtain the AMI, follow the below steps:

1. Fill in the Amazon EC2 Instance request from our website.

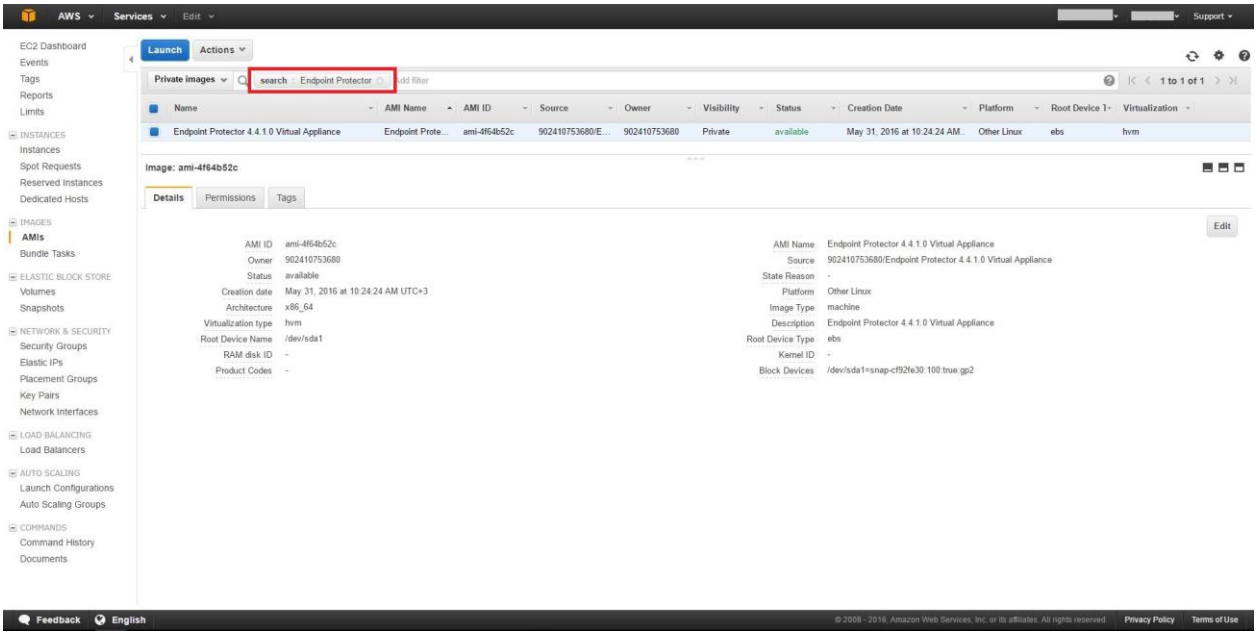


2. After receiving a replay from an Endpoint Protector Representative, log into your AWS account.

3. Go to **Services: EC2** > Select your **region**.

4. Go to **Images: AMIs** > Choose the **Private images** type and enter in the search field: **Endpoint Protector**.

These steps will display the Endpoint Protector AMI as seen in the below screenshot.



1.3. Licensing the Endpoint Protector AMI for AWS

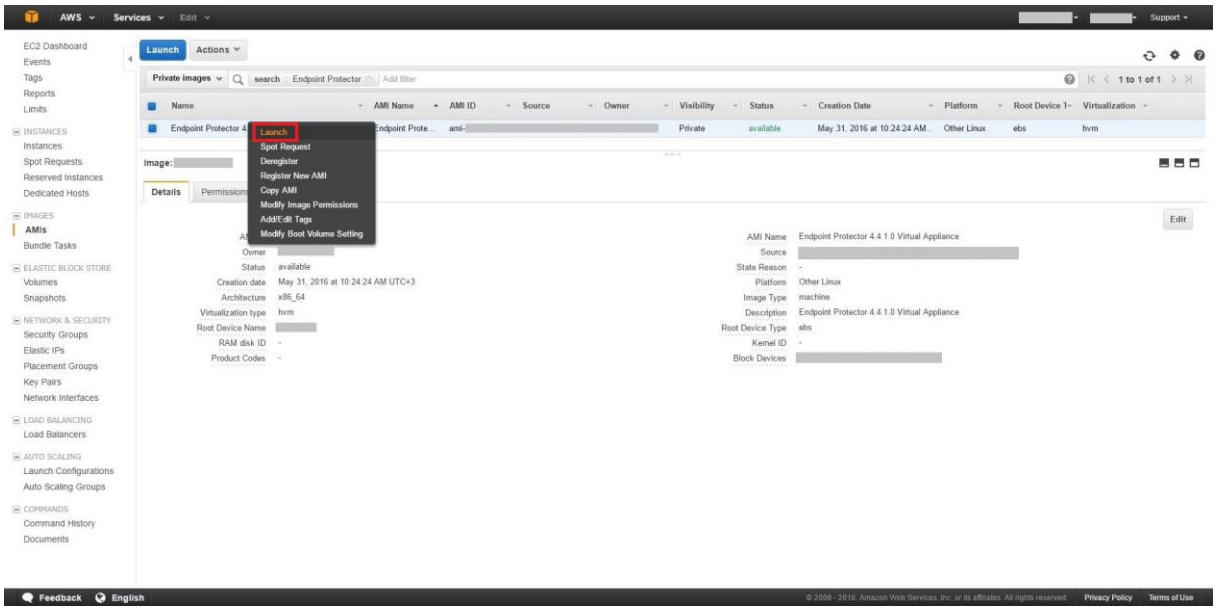
Endpoint Protector is a Bring your Own License (BYOL) Instance. This means that you are paying Amazon for running the instance and then import the license previously purchased from CoSoSys or from any CoSoSys Partner.

Licensing Endpoint Protector with AWS has the same fee as licensing the Endpoint Protector Virtual Appliance. To purchase a license please contact your CoSoSys Distribution Partner or sales@cososys.com.

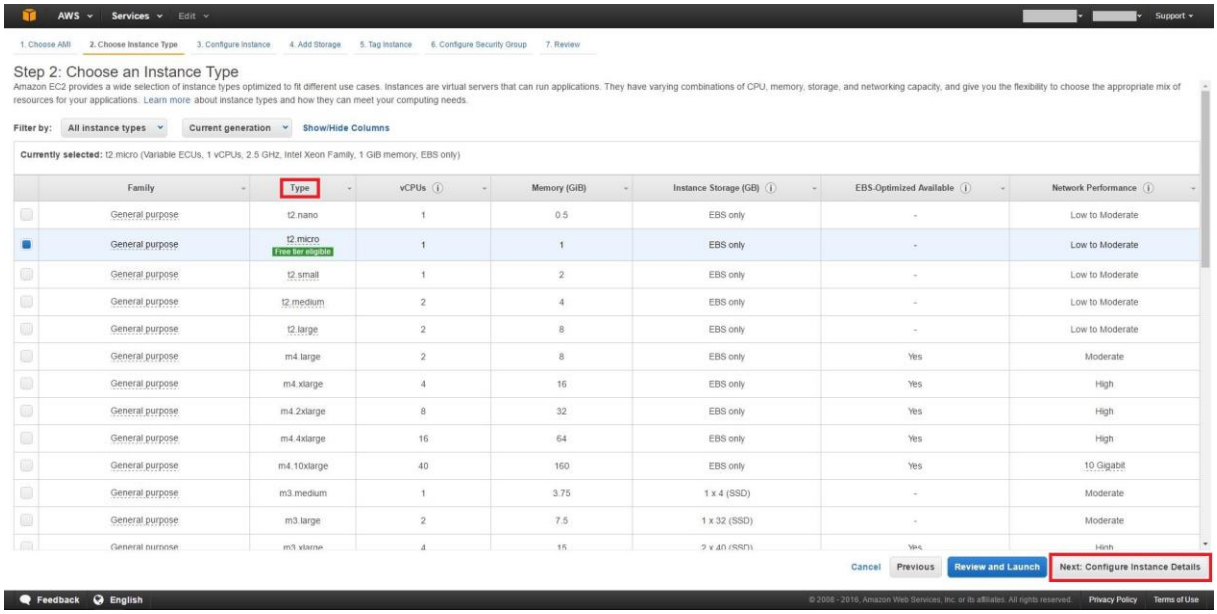
1.4. Setting up the EPP4 EC2 Instance

Please follow the below steps for setting up the EPP4 EC2 instance.

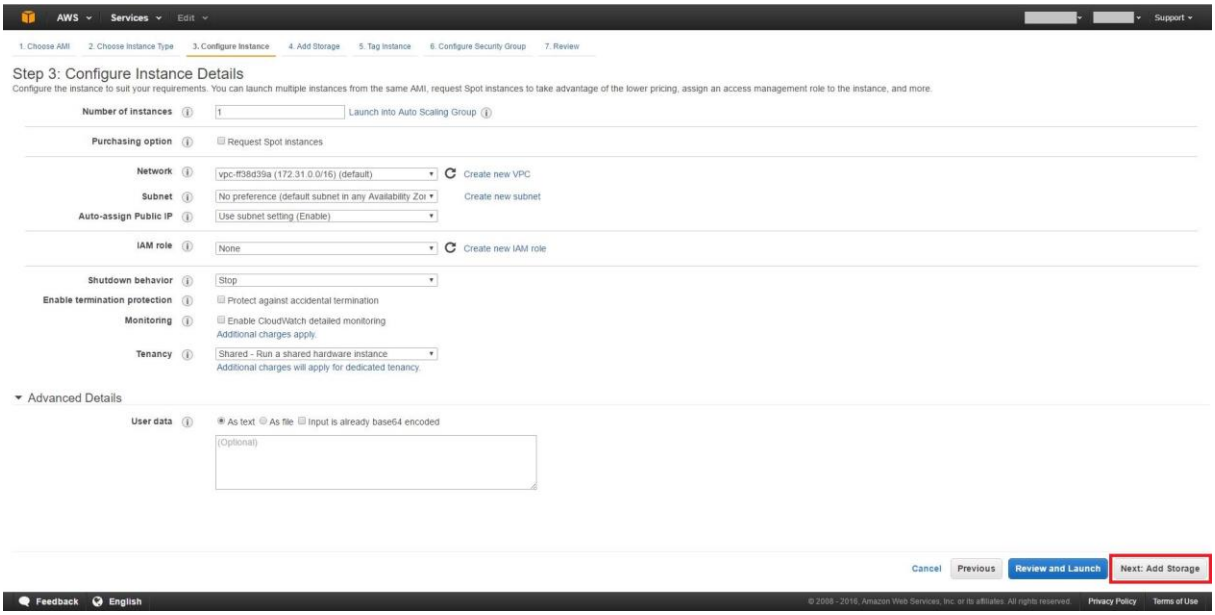
1. After finding the EPP4 AMI, select it, right-click on it and choose "Launch Instance" from the menu. This will launch the "Request Instance Wizard".



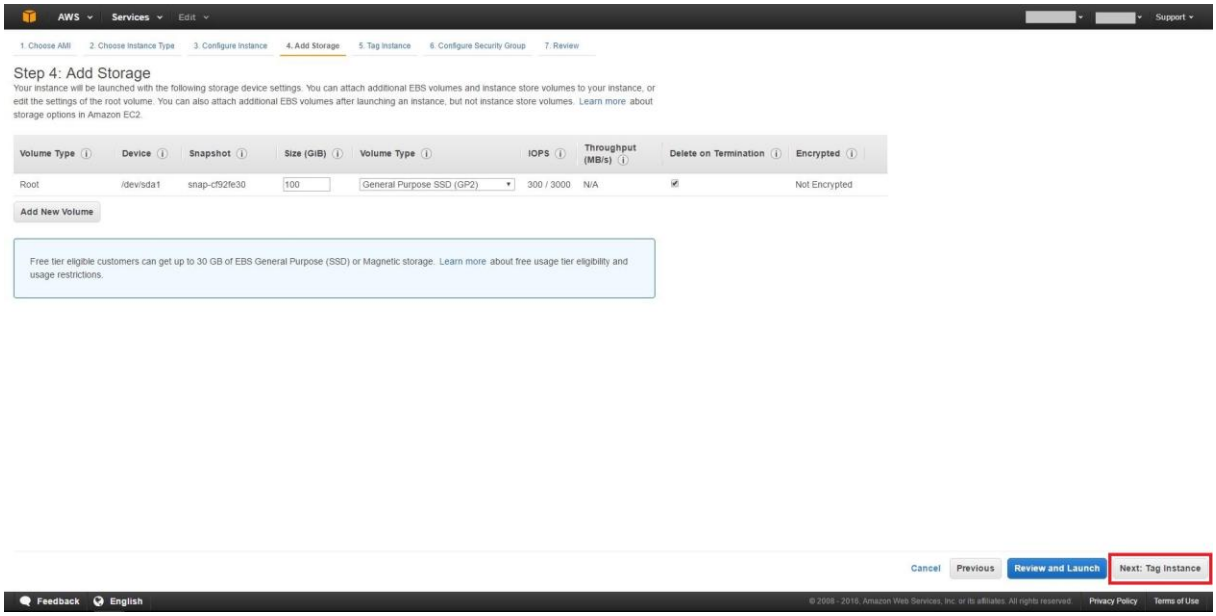
2. Choose an instance type, the region (the availability zone) and click "Next". For any question that you have in choosing the instance type best fitted for your needs, please contact support@endpointprotector.com.



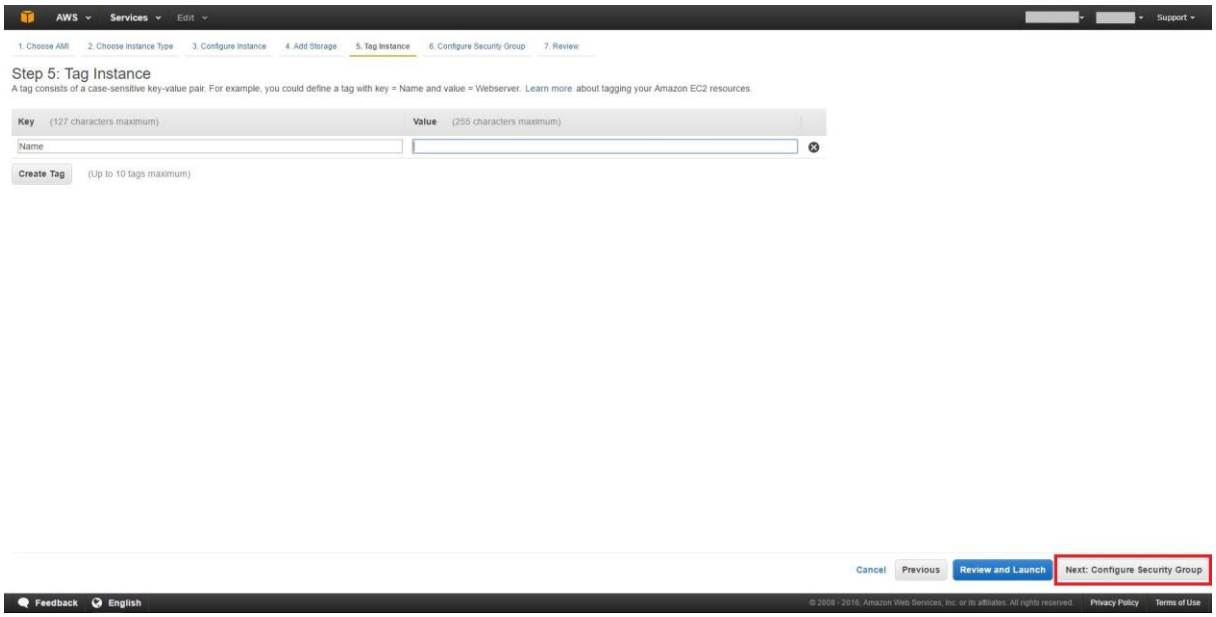
3. The instance details do not require any adjustments. Simply click “Next”.



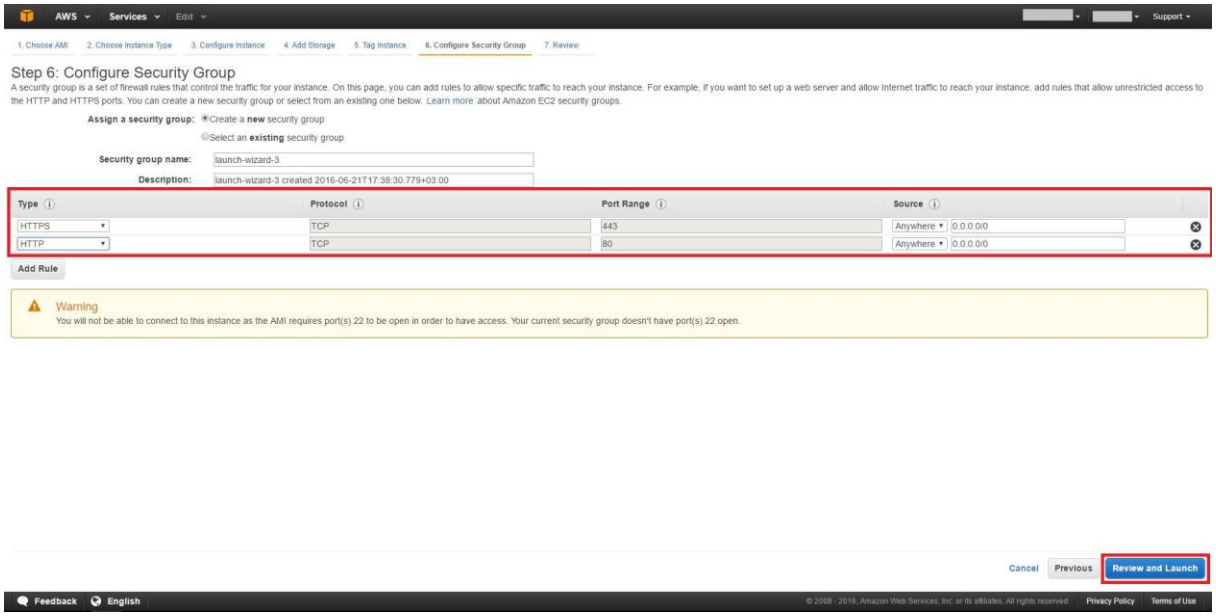
4. The Storage Device Configuration does not require any changes. Continue by clicking “Next”.



5. After adding the tags as you consider, click “Next”.

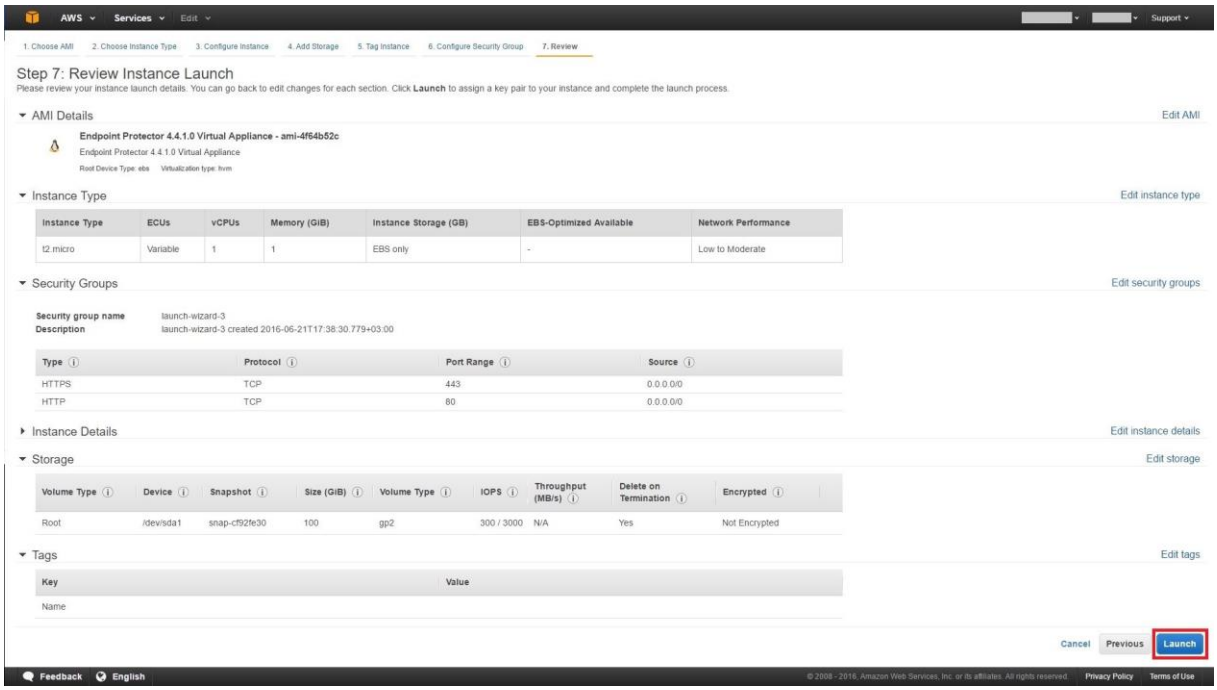


6. To Configure the Firewall, we recommend you the following settings:
6.1. Check “Create a new Security Group”.
6.2. Specify the Group Name and a Description.
6.3. Under Inbound Rules choose from the dropdown menu to create a new rule as “Custom TCP rule”. Add the port 443 (mandatory) and 80 (not mandatory). Each of them will have the source set for: Anywhere, 0.0.0.0. When you are done, click “Review and Launch”.

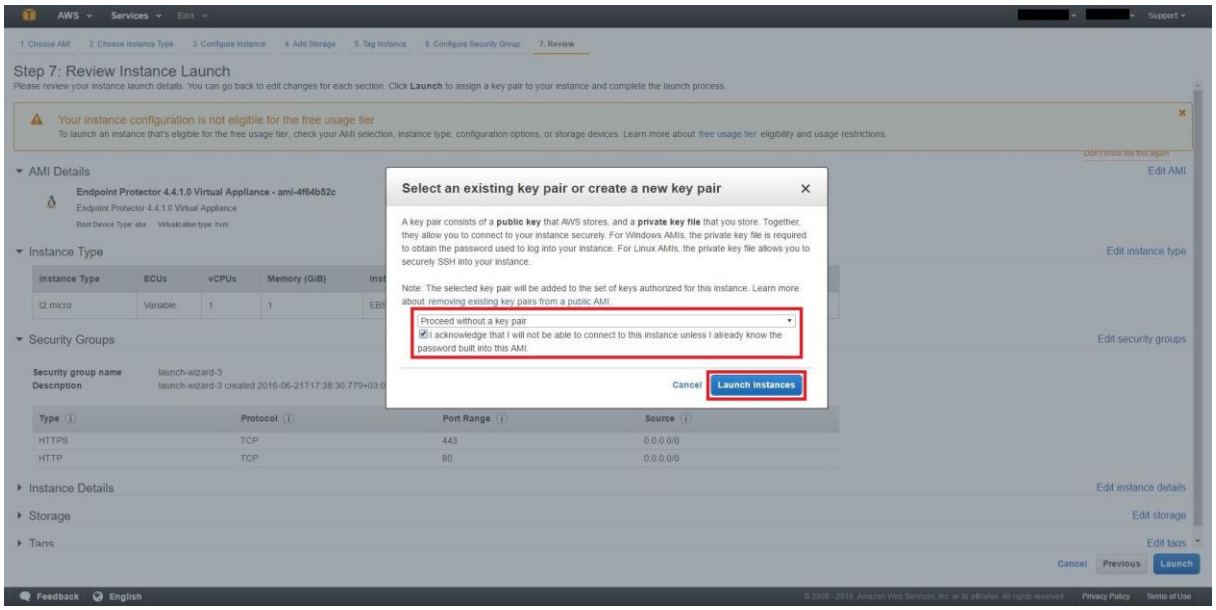


The port 443 is for the client-server communication and the port 80 is for the web interface access. In case you need a remote intervention of the Endpoint Protector Support Team, temporary opening one more port would be required.

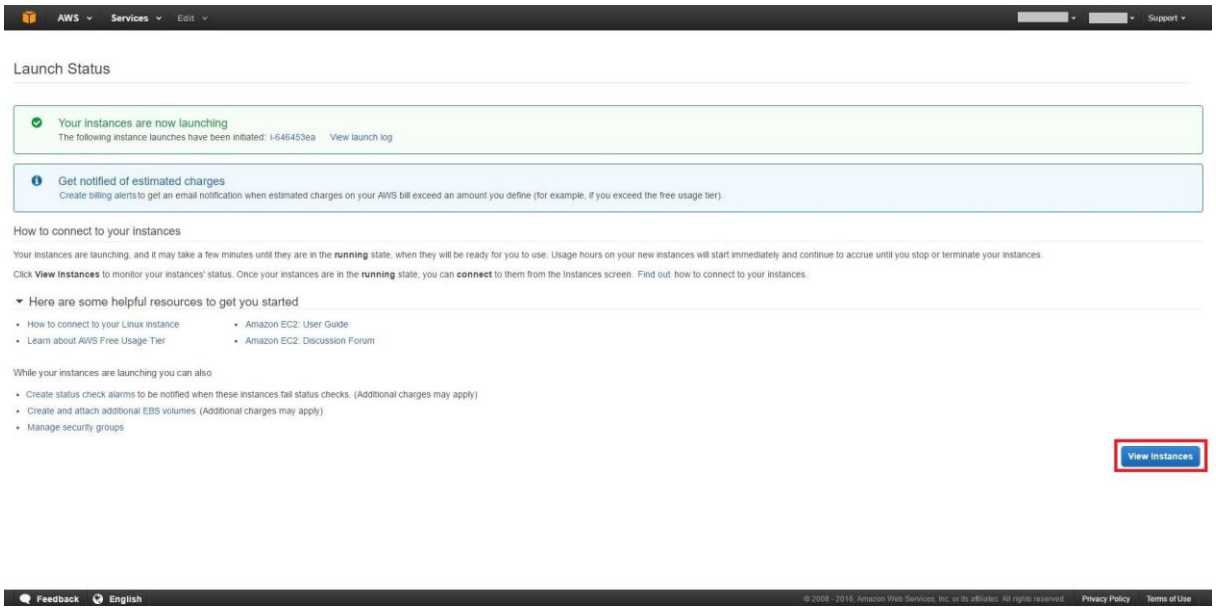
7. Review the settings of the instance and click "Launch".



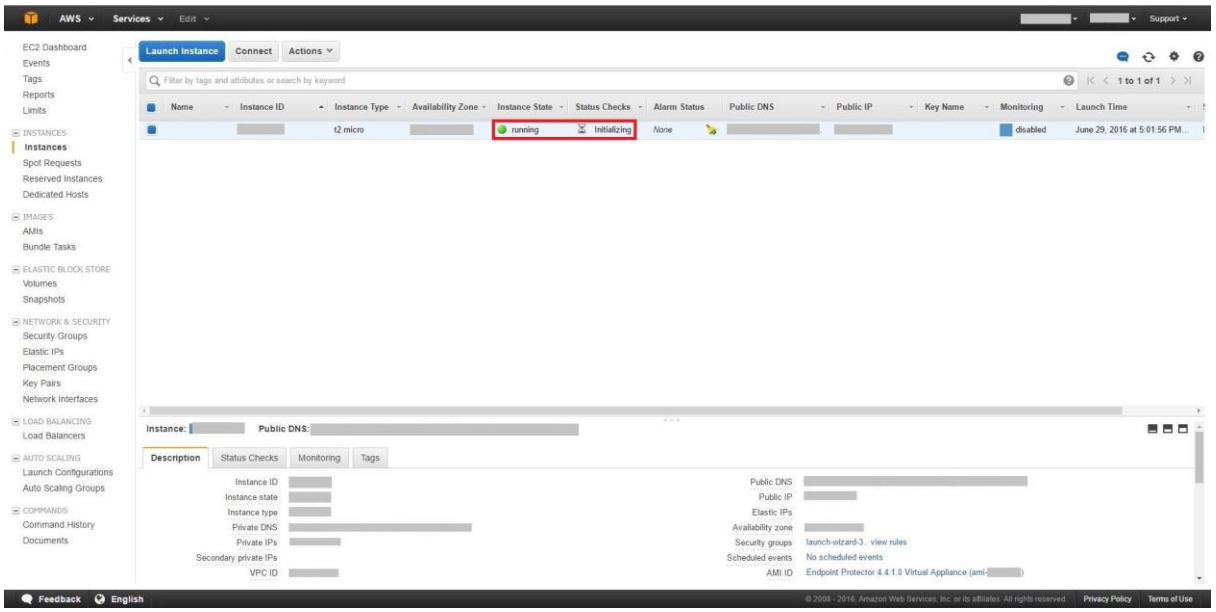
8. A pop-up window will ask you to "Select an existing key pair or create a new key pair". If you choose to use a key pair you might have to share it with our Support Team for support requests. In this case, ensure it is used only for this instance. We would recommend choosing the option "Proceed without a Key Pair". Then click "Launch Instances".



9. The message "Your instance is now launching" shows up. Finish the process by pressing "View Instances".

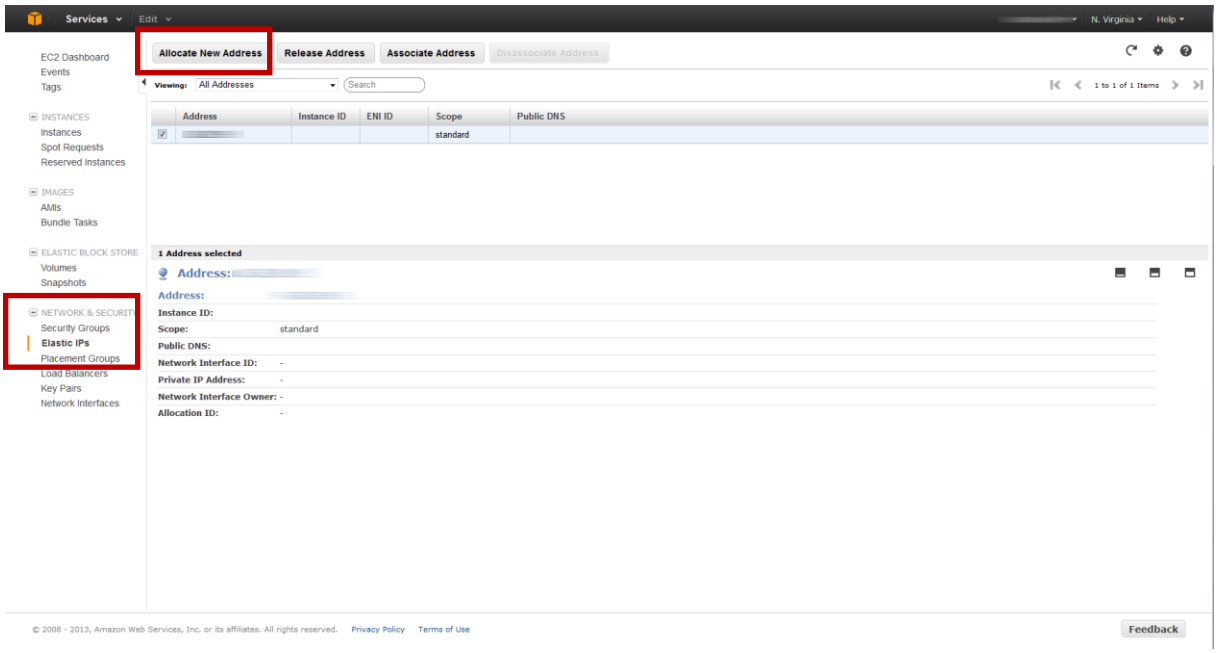


10. Wait for the instance to start. This might take a few minutes while the "Status Checks" appears as "Initializing".

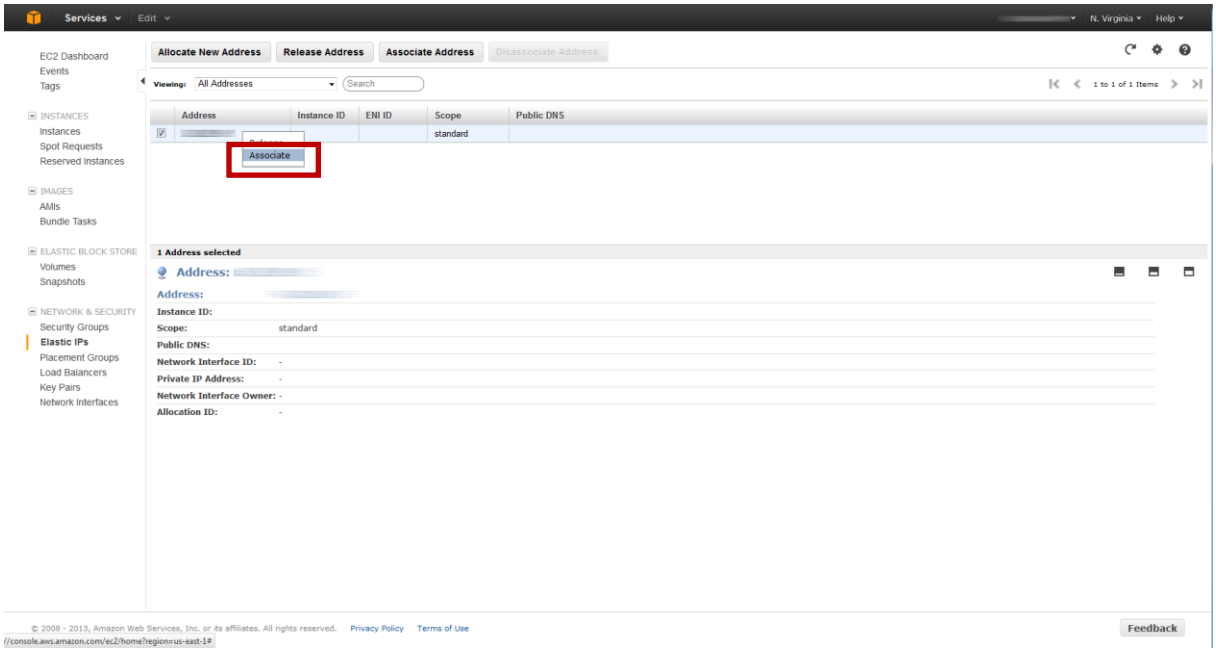


11. As a next step, we recommend you to request an Elastic IP. This is required so the Endpoint Protector Clients can communicate with the same IP Address in case of an instance restart. Without an Elastic IP (Static IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled. To request an Elastic IP go in the AWS

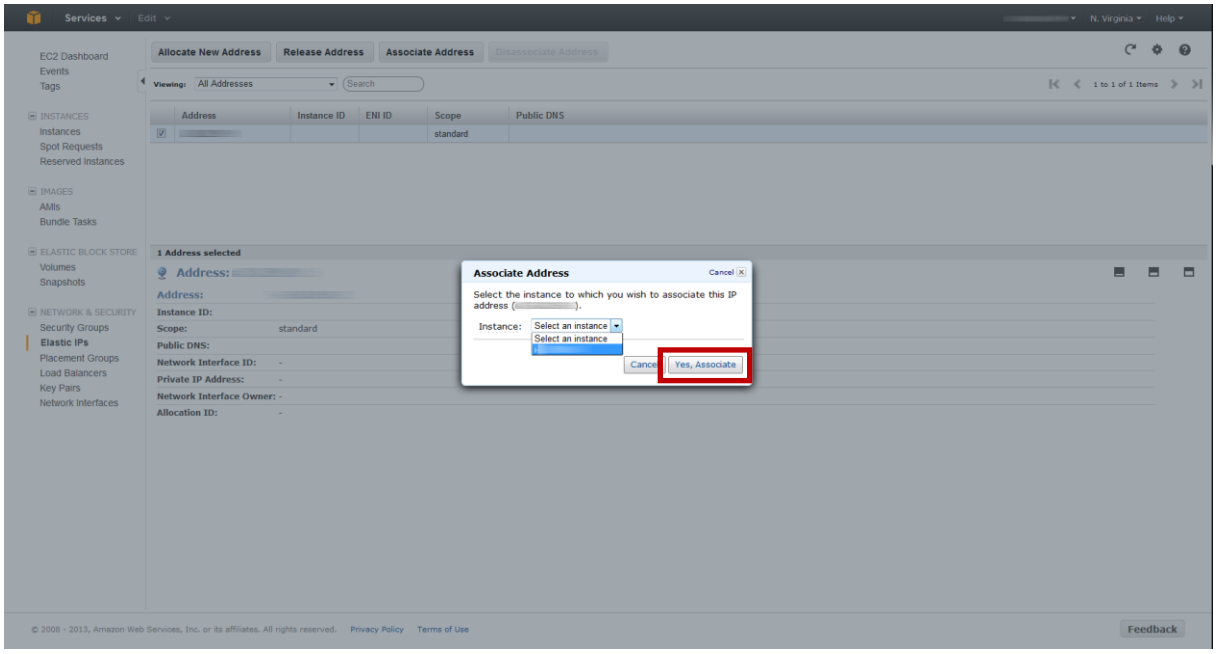
Management Console to the option Network & Security > Elastic IPs and click on "Allocate New Address".



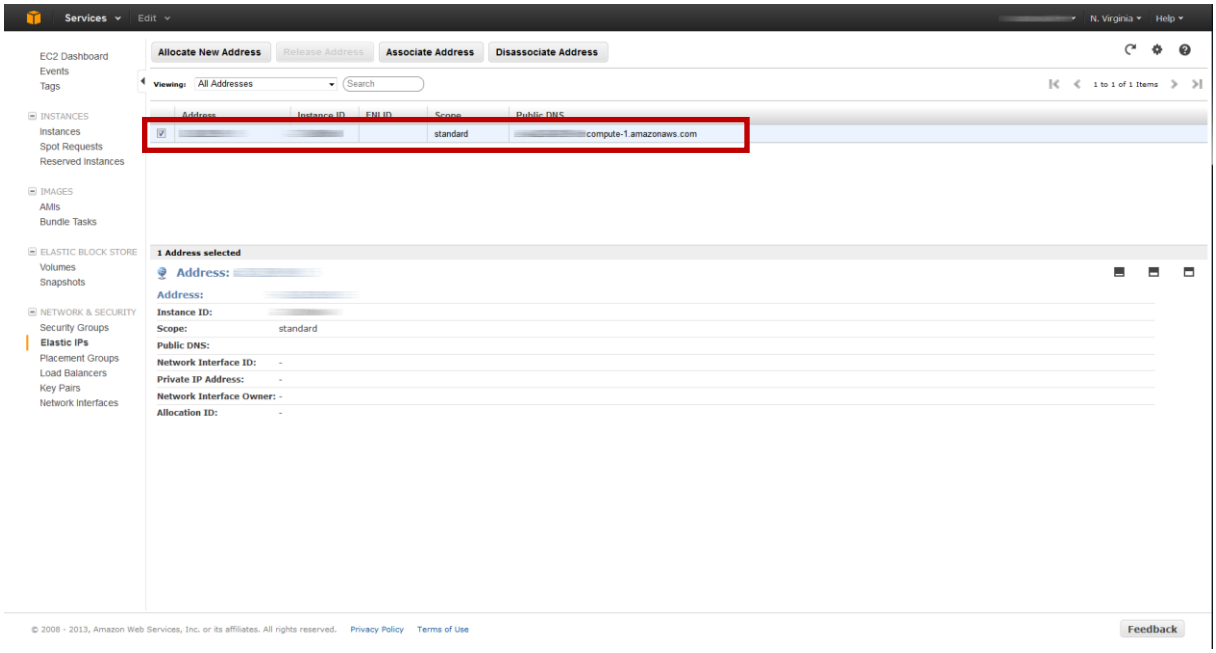
12. Associate the Elastic IP with your Endpoint Protector Instance. Select the IP Address and click "Associate".



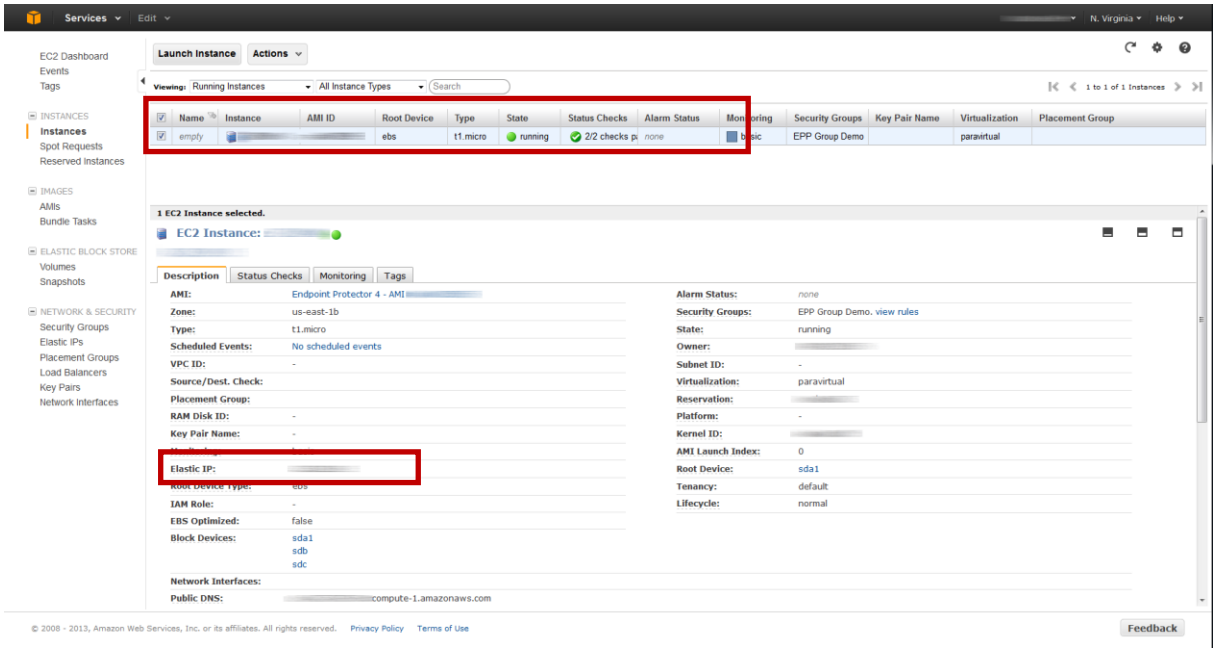
13. Select the Endpoint Protector Instance from the dropdown list and click "Yes, Associate".



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



After a few minutes, the Endpoint Protector Instance will be running associated with the Elastic IP.


Services
Edit
N. Virginia
Help
EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces
Launch Instance
Actions
Viewing: Running Instances
All Instance Types
Search
1 to 1 of 1 Instances
Name
Instance
AMI ID
Root Device
Type
State
Status Checks
Alarm Status
Monitoring
Security Groups
Key Pair Name
Virtualization
Placement Group
empty
ebs
t1.micro
running
2/2 checks p
none
basic
EPP Group Demo
paravirtual
1 EC2 Instance selected.
EC2 Instance:
Description
Status Checks
Monitoring
Tags
AMI:
Endpoint Protector 4 - AMI
Zone:
us-east-1b
Type:
t1.micro
Scheduled Events:
No scheduled events
VPC ID:
Source/Dest. Check:
Placement Group:
RAM Disk ID:
Key Pair Name:
Elastic IP:
IAM Role:
EBS Optimized:
false
Block Devices:
sda1
sdb
sdc
Network Interfaces:
Public DNS:
compute-1.amazonaws.com
Alarm Status:
none
Security Groups:
EPP Group Demo. view rules
State:
running
Owner:
Subnet ID:
Virtualization:
paravirtual
Reservation:
Platform:
Kernel ID:
AMI Launch Index:
0
Root Device:
sda1
Tenancy:
default
Lifecycle:
normal
© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

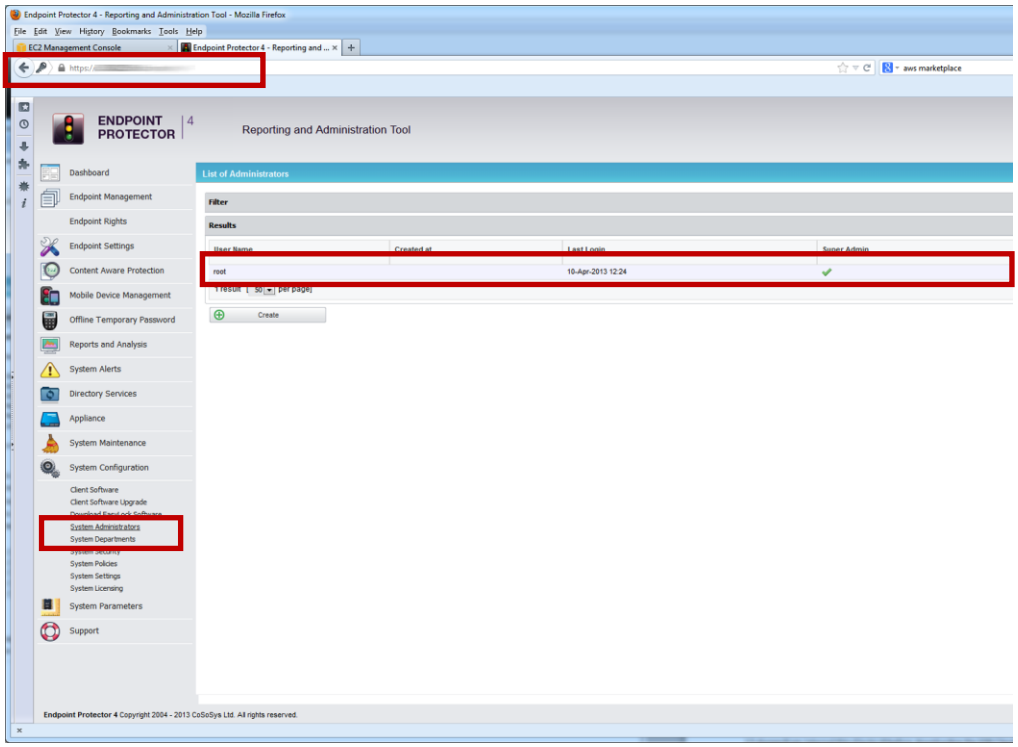
1.5. Accessing the Endpoint Protector Web Interface

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

Click "Continue/Trust or Add exception" when the browser displays a warning regarding the certificate of this webpage.

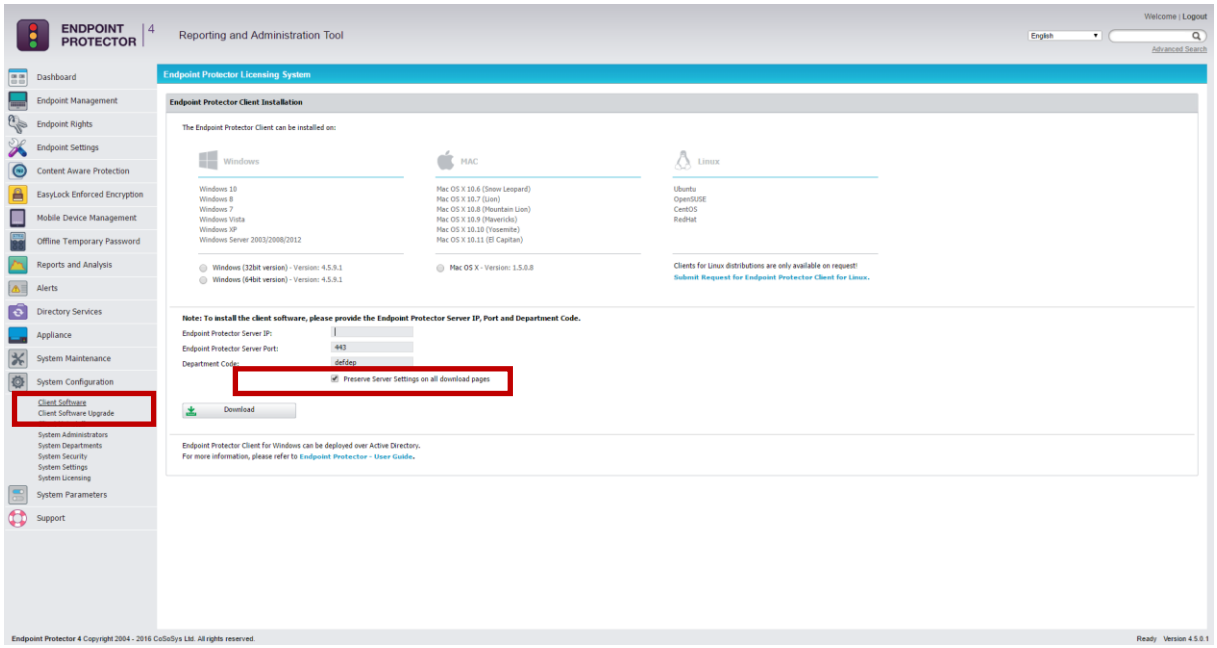
The default user name to login the Endpoint Protector interface is: **root** and the password is: **epp2011**

We recommend changing the root account password to login in Endpoint Protector in order to secure your EPP instance from unauthorized access. This can be done from System Configuration > System Administrators.

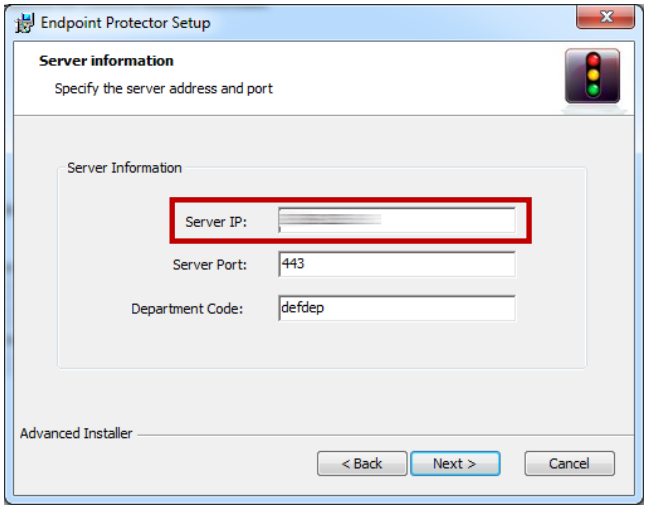


Now go to System Configuration > Client Software and change the IP Address written in the field "Endpoint Protector Server IP" and change the IP in this field to the Elastic IP you have assigned to the Endpoint Protector Instance.

To avoid known issues like navigating away from this page and having the Client IP switch back to the internal IP of the EC2 Instance, the "Preserve Server Settings on all download pages" needs to be checked.



Now you can download the Endpoint Protector Client Software that has the Elastic IP Address already included. In order to double check it, start an Endpoint Protector Client MSI and check in the field Server IP if it corresponds to the Elastic IP. Then, you can start installing the EPP4 Client or deploying it.

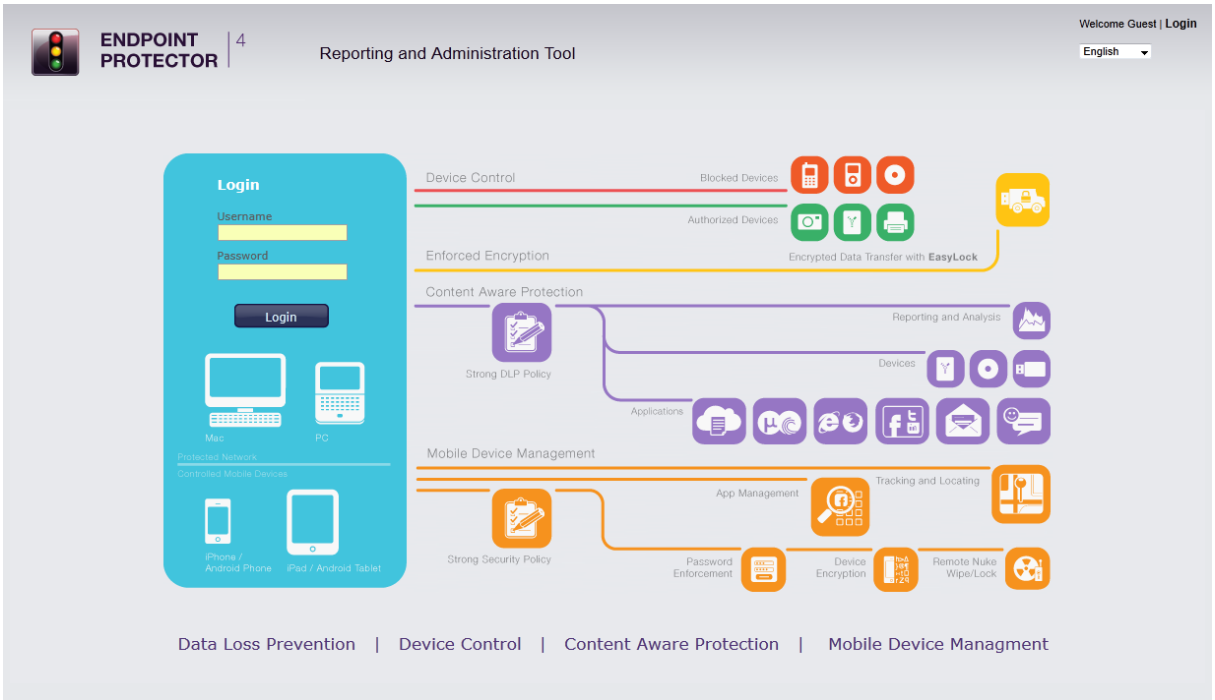


1.6. Securing your Instance

We recommend further securing your Instance by making all possible settings in the AWS Interface under the option "Security Groups".

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, that used together ensure 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.

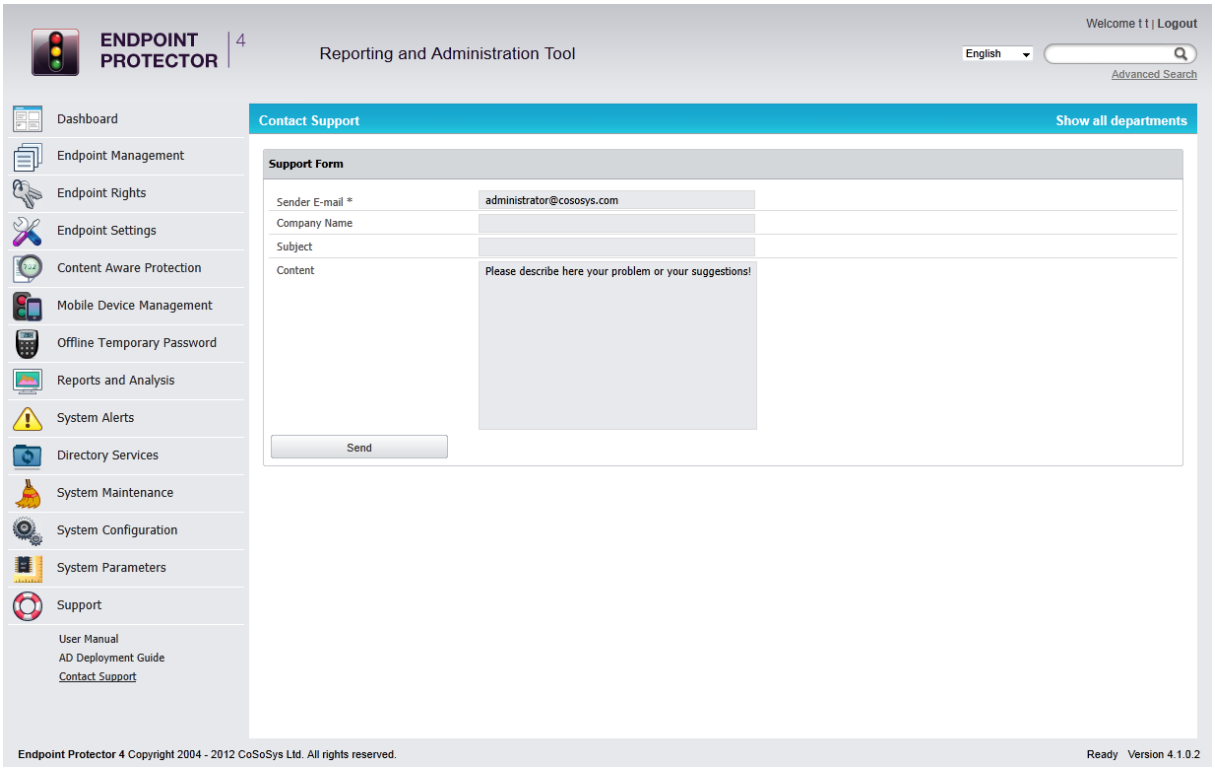
- **Device Control**: enforces strong security policies for controlling and closely monitoring all portable storage device use inside the company network. Once deployed inside companies networks, the Device Control modules reduces the risks of data loss and data theft through unauthorized use of removable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

- **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 by transfers either 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/.

To log a Support ticket, please send a message from the menu Support > Contact Support.



We appreciate all feedback from our customers' side.

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.