

User Manual Version 1.0.0.2

AWS / Amazon Web Services EC2 for Endpoint Protector User Manual



Table of Contents

1. Getting Started	1
1.1. Introduction	1
1.2. Obtaining the EPP AMI on AWS	1
1.3. Licensing the Endpoint Protector AMI for AWS	2
1.4. Setting up the EPP4 EC2 Instance	3
1.5. Accessing the Endpoint Protector Web Interface	11
1.6. Securing your Instance	
2. What Endpoint Protector does	13
3.Support	15
4.Important Notice / Disclaimer	16

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.

A	mazon EC2 Insta	ance	2
	Name*		
	Company e-mail*		
	Phone		
	AWS Account no. *		
	Region and Availability Zone	~	
	Submit Request		

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 <u>CoSoSys Distribution Partner</u> or <u>sales@cososys.com</u>.

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 <u>support@endpointprotector.com</u>.

p 2: 0	2. Choose Instance Type 3. Centigure	Instance 4. Add Storage 5.	Tag Instance 6. Configure Security	Group 7. Review			
n EC2 ces for	provides a wide selection of instance types your applications. Learn more about insta	optimized to fit different use ca nce types and how they can me	ses. Instances are virtual servers et your computing needs.	that can run applications. They	ave varying combinations of CPU, memory, st	orage, and networking capacity, and give you the	flexibility to choose the appropriate m
y:	All instance types 👻 Current gen	eration 👻 Show/Hide Col	umns				
ntly s	elected: t2 micro (Variable ECUs, 1 vCPUs	s, 2.5 GHz, Intel Xeon Family, 1	GIB memory, EBS only)				
	Family	- Туре -	vCPUs (j) +	Memory (GiB) -	Instance Storage (GB) (j) -	EBS-Optimized Available (j) -	Network Performance (j)
	General purpose	t2.nano	1	0.5	EBS only	*	Low to Moderate
	General purpose	12 micro Free tier eligible	1	1	EBS only		Low to Moderate
	General purpose	t2.small	1	2	EBS only	,	Low to Moderate
	General purpose	t2.medium	2	4	EBS only	2	Low to Moderate
	General purpose	12 large	2	8	EBS only		Low to Moderate
	General purpose	m4.large	2	8	EBS only	Yes	Moderate
	General purpose	m4.xlarge	4	16	EBS only	Yes	High
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
	General purpose	m4.4xlarge	16	64	EBS only	Yes	High
	General purpose	m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	*	Moderate
	General purpose	m3.large	2	7.5	1 x 32 (SSD)	X	Moderate
	General purpose	m3 xlarne	4	15	2 x 40 (SSD)	yp.c.	Hinh

- 4 | Endpoint Protector Amazon Web Services EC2 for Endpoint Protector | User Manual
- 3. The instance details do not require any adjustments. Simply click "Next".

AWS - Services -	Edit v	2									✓ Support ✓
											N. Citti i anti C
1. Choose AMI 2. Choose Instance Type	3.0	configure Instance 4. Add Storage 5. Tag Instance 6.	Configure Security Group 7. F	Review							
Step 3: Configure Instan	ce D	Details									
Configure the instance to suit your requir	ements	. You can launch multiple instances from the same AMI, re	quest Spot instances to take	advantage of the	e lower pricing, assi	gn an access managen	ient role to the instance	, and more.			
Number of instances	(1)	1 Launch Into Auto Scali	ig Group 🕧								
Purchasing option		Request Spot Instances									
Network	۲	vpc-ff38d39a (172.31.0.0/16) (default)	C Create new VPC								
Subnet	1	No preference (default subnet in any Availability Zor •	Create new subnet								
Auto-assign Public IP		Use subnet setting (Enable)									
IAM role	0	None •	Create new IAM role								
Shutdown behavior	(j)	Stop •									
Enable termination protection	1	Protect against accidental termination									
Monitoring	1	Enable CloudWatch detailed monitoring Additional charges apply.									
Tenancy	۲	Shared - Run a shared hardware instance *									
		Additional charges will apply for dedicated tenancy.									
 Advanced Details 											
User data											
		(Optional)									
								Cancel	Previous	Review and Launch	Next: Add Storage
🗨 Feedback 🥥 English							@ 2008 - 2016, Amazo	n Web Services, I	nc. or its affiliates	All rights reserved. Prive	cy Policy Terms of Use

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

🧊 AWS 🖌 Services 🗸 Edit 🗸					_	• Support •
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage	5. Tag Instance 6. Configure Security Group	7. Review				
Step 4: Add Storage Your instance will be launched with the following storage device settings. You can att edit the settings of the root volume. You can also attach additional EBS volumes afte storage options in Amazon EC2.	ach additional EBS volumes and instance store r launching an instance, but not instance store v	e volumes to your instance, or volumes, Learn more about				
Volume Type () Device () Snapshot () Size (GIB) ()	Volume Type () IOF	PS () Throughput (MB/s) ()	Delete on Termination (j)	Encrypted ()		
Root /dev/sda1 snap-cf92fe30 100	General Purpose SSD (GP2) * 300	00 / 3000 N/A	×	Not Encrypted		
Add New Volume						
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) usage restrictions.	or Magnetic storage. Learn more about free us	usage tier eligibility and				

	Cancel	Previous	Review and Laund	h Next:	Tag Instance
				-	
Eastback Q English	it 2018 - 2016 Amaron Web Services In		All rights reserved.	rivary Policy	Terms of tise

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".

🎁 AWS - Services - Edit	v				✓ Support ✓
1. Choose AMI 2. Choose Instance Type 3.	Configure Instance 4. Add Storage 5. Tag Instance	6. Configure Security Group 7. Review	π.		
Step 6: Configure Security C security group is a set of frewall rules that co ne HTTP and HTTP8 ports. You can create a r Assign a security group: Security group name: Description:	Aroup nitor the traffic for your instance. On this page, you can be security group or select from an existing one below *Create a new security group Select an existing security group launch-watcad-3. created 2016.06-27137.283.03.77	add rules to allow specific traffic to rea . Learn more about Amazon EC2 second	ch your instance. For example, if you want to r rifly groups.	set up a web server and allow internet traffic to reach your instance, add rules that allo	ow unrestricted access to
Туре ()	Protocol (j)		Port Range (i)	Source ①	E
HTTPS *	TCP		443	Anywhere • 0.0.0.0/0	e
HTTP *	TCP		80	Anywhere * 0.0.0.0/0	8
				Cancel Previous	Review and Launch
Feedback Q English				45 2028 - 2018 Jamman Web Survivas for at its affinites All rights towards d	

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".

🚺 AWS 🗸	Services - Ed	fit v						v Support v
1. Choose AMI 2.	Choose Instance Type	3. Configure Instance	4. Add Storage 5.	Tag Instance 6. Configure Se	curity Group 7. Revie	w		
Step 7: Revie Please review your in	ew Instance L	aunch You can go back to	edit changes for each se	ction. Click Launch to assign	a key pair to your ins	tance and complete the launch	process.	
▼ AMI Details								Edit AMI
A Endp Endpo Root D	point Protector 4.4.1. Dint Protector 4.4.1.0 Virt evice Type: ebs Virtualizat	0 Virtual Appliance tual Appliance tion type: itvm	e - ami-4f64b52c					
 Instance Type 	e							Edit instance type
Instance Type	ECUs	vCPUs	Memory (GIB)	Instance Storage (GB)	EBS-Optin	nized Available	Network Performance	
12.micro	Variable	1	1	EBS only			Low to Moderate	
 Security Group 	ups							Edit security groups
Type ()	launch	Protoc	col (j)	Port Ran	ge ()	Source ()		
HTTPS		TCP		443		0.0.0.0/0		
HILP		TCP		80		0.0.0.0/0		
Instance Deta	ails							Edit instance details
 Storage 								Edit storage
Volume Type	() Device ()	Snapshot 🕕	Size (GiB) (j)	Volume Type 🕕 🛛	OPS (i) Through (MB/s) (put Delete on Termination ()	Encrypted (j)	
Root	/dev/sda1	snap-cf92fe30	100	gp2 3	00/3000 N/A	Yes	Not Encrypted	
▼ Tags								Edit tags
Kev				Value				
Name								
								Cancel Previous Launch
Eedback	English							2016, Amazon Web Services, Inc. or its attiliates. All rights reserved. Privacy Policy Terms of Use

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".

<form> 1 Case Add 2 Case Randow 2 1 Cade Randow 2 Randow 2</form>	AWS - Serv	vices 🛩 Edi	t. *					 Support +
Your instance configuration is not eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will searce to prove the usage let eligible for the free usage let, should will be usage let eligible for the free usage let, should will be usage let eligible for the free usage let, should will be usage let eligible for the free usage let, should will be usage let eligible for the free usage eligible for the free usage let eligible for the free usage eligible for the free usa	1 Choose AMI 2 Choose In Step 7: Review In Please review your instance 1	nstance Type Instance L Jaunch details	3 Configure insta aunch fou can go bacl	ance 4 Add Storage	5 Tag Ins	ance 6. Configure Security Group 7. Rev Click Launch to assign a key pair to your in	ww	
• AMI Details Endpoint Protector 4.1.0 Virtual Appliance - ami-dt64502c Edd instance Type Image: Control to fire applied by the fire applied by the state of the protector 4.1.0 Virtual Appliance - ami-dt64502c Edd instance Type Edd instance Type Instance Type Edd is to control to your status et by the protector 4.1.0 Virtual Appliance - ami-dt64502c Edd instance Type Edd instance Type Edd instance Type Variable Variable Variable Variable Variable Variable Variable Variable Edd instance Type Security Groups Basench visitanci 3 Basench visitanci 3 Edd instance Up of variable Concert Law Mitter Board Edd instance Type Edd instance Type Ype Protector 1 Protector 4.43 0.00.0.00 Edd instance of the state of	Your instance To launch an insta	configuration ince that's eligit	n is not eligit ble for the free u	Die for the free usag usage tier, check your A	<mark>ge tier</mark> MI selectio	n, instance type, configuration options, or st	orage devices. Learn more about free usage tier eligibility and usage restrictions	×
Control Durants <td>× AMI Details</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>DON'TSYOW WE THE SQUIN</td>	× AMI Details							DON'TSYOW WE THE SQUIN
Instance Type Instanc	AMI Details Endpoint Prote Rost Device Type	rotector 4.4.1.0 actor 4.4.1.0 Virtu e: ethe Vetoakzati	Virtual Applia aal Appliance on type: hym	ance - ami-4164b52c		Select an existing key pair A key pair consists of a public key that they allow you to connect to your instan to obtain the paragraduated to ke prior.	r or create a new key pair ×	Edit Anti
Instance Type ECUs vcPUs Memory (GIB) Instance Type 12 mice Variable 1 1 EB Note: The selected key pair will be added to the set of keys authorized for this instance. Leam more about removing existing key pair mo	 Instance Type 				_	securely SSH into your instance.	our instance. For Linux Anna, the private sety the allows you to	Edit instance type
Security Groups S	Instance Type	ECUs Variable	VCPUs	Memory (GiB)	EBS	Note: The selected key pair will be adde about removing existing key pairs from	d to the set of keys authorized for this instance. Learn more public AMI.	
Security group name basinch-wizzer53 created 2016-66-2117 73.83 0779-030 Cancel Lunch Instances Type () Protocol () Port Range () Source () HTTPS TCP 443 0.00.00 HTTP TCP 80 0.00.00 Instance Details Edd instance details Edd instance details Storage Edd instance details Edd instance details	✓ Security Groups					Proceed without a key pair I acknowledge that I will not be all password built into this AMI.	Edit security groups	
Type () Protocol () Petr Range () Source () HTTPS TCP 443 0.00.00 HTTP TCP 80 0.00.00 Instance Details Edit instance details Edit instance details Storage Edit instance details Edit instance details	Security group name Description	launch-i	wizard-3 wizard-3 create	d 2016-06-21717:38-30	779+03:0		Cancel Launch Instances	
HTTPS TCP 443 0.00.00 HTTP TCP 80 0.00.00 Instance Details Edit instance details Instance Details Edit instance details Storage Edit instance details	Туре		Pr	otocol (j)	4	Port Range (1)	Source (i)	
HTTP TCP 80 0.0.0.0 Instance Details Edit instance details Instance Details Edit instance details Storage Edit instance details Tans Edit instance details	HTTPS			P		443	0.0.0.0/0	
Instance Details Edit instance details Storage Tans Concel Previous Concel Previous	HTTP		TC	P		80	0.0.0.0/0	
Storage Editoriage Tans Concel Previous Lanch	Instance Details							Edit instance details
Tans Editions Concel Previous Launch	Storage							Edit storage
Concel Previous Launch	▶ Tags							Edit taos *
								Cancel Previous Launch

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".

🚺 AWS 🗸 Ser	vices 🖌 Edit 🗸	- Support -
EC2 Dashboard Events Tags	Launch Instance Connect Actions * Q, Filter by tage and attributes or search by keyword	
Reports Limits	Name - Instance ID - Instance Type - Availability Zone	Instance State + Status Checks + Alarm Status Public DNS + Public IP + Key Name + Monitoring + Launch Time +
INSTANCES Instances Spot Requests Reserved Instances Dedicated Hosts	12 micro	numing Z Initializing Alone Source Lange Lang
 IMAGES AMIs Bundle Tasks 		
ELASTIC BLOCK STORE Volumes Snapshots		
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces		
LOAD BALANCING	Instance: Public DNS:	
AUTO SCALING Launch Configurations Auto Scaling Groups COMMANDS Command History Documents	Description Status Checks Monitoring Tags Instance ID Instance State Instance State Private DNS Private DNS Private IPs Secondary private IPs	Public DNS Public IP Elastic IP Availability zone Security grane Scheduled events

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".

🧊 Services 🛩 E	idit 🗸				(N. Virginia 👻	Help	• •
EC2 Dashboard	Allocate New Address	Release Addres	ss Associate A	Address		C	٥	0
Events Tags	Viewing: All Addresses	• (Se	earch		K <	1 to 1 of 1 Ite	ims)	> >1
INSTANCES Instances Spot Requests Reserved instances IMAGES AMIS Bundie Tasks	Address	Instance ID	ENI ID Si	Scope standard	Public DNS			
 ELASTIC PLOCK STORE Volumes Snapshots NETWORK & SECURITY Security Groups Elastic IPs Piacement Groups Load Balancers Key Pars Network Interfaces 	1 Address selected Address: Instance ID: Scope: Public DNS: Network Interface ID: Private IP Address: Network Interface Owner Allocation ID:	standard - - - -				8		
© 2008 - 2013, Amszon Web	Services, Inc. or its affiliates. Al	II rights reserved. P	Privacy Policy Terms	is of Use		Fee	dbac	k

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

🎁 Services 🗸 E					• N. Virginia	✓ Hel	
EC2 Dashboard	Allocate New Address	Release Address Associa	te Address		C	٥	0
Tags	Viewing: All Addresses	Search)		≪ ≪ 1 to 1 of 1	Items	> >
INSTANCES Instances Spot Requests Reserved Instances IMAGES AMIs	Address	Instance ID ENI ID	Scope standard	Public DNS			
Bundle Tasks ELASTIC BLOCK STORE Volumes	1 Address selected					-	-
Snapshots Intervente & Security Security Groups	Address: Address: Instance ID:	standard					
Elastic IPs Placement Groups Load Balancers	Public DNS: Network Interface ID:	standard -					
Key Pairs Network Interfaces	Network Interface Owne Allocation ID:	er: -					
© 2008 - 2013, Amazon Web //console.aws.amazon.com/ec2/home	Services, Inc. or its affiliates. A Pregion=us-east-1#	All rights reserved. Privacy Policy T	erms of Use		F	eedbac	k

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

👔 Services v Edit v										
EC2 Dashboard	Allocate New Address Release Address Associate Address Disassociate Address									
Tags	Viewing: All Addresses									
INSTANCES Instances Spot Requests Reserved instances IMAGES AMIs Bundle Tasks	Address Instance ID ENI ID Scope Public DN S									
ELASTIC BLOCK STORE	1 Address selected									
 ELASTIC IRLOCK STORE Volumes Bnapshots NETWORK & SECURITY Security Groups Elastic IPs Pacement Groups Load Balancers Key Pars Hetwork Interfaces 	Address: Cance K Address: Scope: Istance D: Scope: Scope: standard Public (NS: Select hin intance Private IP Address: - Allocation ID: -		-							
© 2008 - 2013, Amazon Web	Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Like		Fe	edbac	k					

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

pard	Allocate New Address Release Address Associate Address Disassociate Address	C ·
•	Viewing: All Addresses	尾 < 1 to 1 of 1 Item
	Address Instance ID FNI ID Scope Public DNS	
_ [standard compute-1.amazonaws.com	
ances		
IS .		
DCK STORE	1 Address selected	
	Address:	
	Address:	
SECURITY	Instance ID: Scone: standard	
pa	Public DNS:	
ups	Network Interface ID: -	
s	Private IP Address: -	
	Network Interface Owner: -	
erfaces	Allocation ID: -	

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

Dashboard	Launch Instance Actio	ns v												C.
s •	Viewing: Running Instances - All Instance Types - (Search)										to 1 of 1 Instance			
TANCES	🕑 Name 🖗 Instance	AMI ID	Root Device	Туре	State	Status Checks	Alarm State	is Mo	on oring	Security Groups	Key Pair Name	Virtualization	Placement Gro	up
t Requests	🗹 empty 🍯		ebs	t1.micro	running	2/2 checks p	none		b sic	EPP Group Demo	1	paravirtual		
erved Instances														
GES dia Tanka	1 EC2 Instance selected.													
die Tasks	EC2 Instance:												1	
STIC BLOCK STORE														
imes	Description Status C	hecks Monitoring	Tags											
panota	AMI:	Endpoint Protecto	r 4 - AMI				Ala	m Status:		none				
WORK & SECURITY	Zone:	us-east-1b					Sec	urity Grou	ips:	EPP Group Den	10. view rules			
urity Groups	Туре:	t1.micro					Sta	te:		running				
tic IPs	Scheduled Events:	No scheduled ever			Ow	ner:								
1 Balancers	VPC ID:	-						net ID:		-				
Pairs	Source/Dest. Check:			Virt	ualization	4	paravirtual							
vork Interfaces	Placement Group:			Res	ervation:									
	RAM Disk ID:	•						form:		-				
	Key Pair Name:						Ker	nel ID:						
	11						AM)	Launch I	ndex:	0				
	Elastic IP:						Roo	t Device:		sda1				
	ROOT DEVICE Type:	ebs					Ten	ancy:		default				
	IAM Role:	-					Life	cycle:		normal				
	EBS Optimized:	false												
	Block Devices:	sda1												
		sdc												
	Network Interfaces:													
	Public DNS:		compute-1.amaz	onaws.com										

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.

	Reporting and Administration Tool			English •) Q Advanced Search
Dashboard	Endpoint Protector Licensing System			
Endpoint Management	Endpoint Protector Client Installation			
Endpoint Rights	The Endpoint Protector Client can be installed on:			
Endpoint Settings		4	A	
Content Aware Protect	n Windows	MAC	A Linux	
EasyLock Enforced Enc	ption Windows 10 Windows 8	Mac OS X 10.6 (Snow Leopard) Mac OS X 10.7 (Lion)	Ubuntu OpenSUSE	
Mobile Device Manager	ent Windows 7 Windows Vista Windows Vista	Mac OS X 10.8 (Mountain Lion) Mac OS X 10.9 (Mavericks) Mac OS X 10.10 (Movernita)	CentOS RedHat	
Offline Temporary Pas	word Windows Server 2003/2008/2012	Mac OS X 10.11 (El Capitan)		
Reports and Analysis	Windows (32bit version) - Version: 4.5.9.1	Mac OS X - Version: 1.5.0.8	Clients for Linux distributions are only available on request!	
Alerts	 Windows (64bit version) - Version: 4.5.9.1 		amount request for Empount Protector Caent for Landa.	
Directory Services	Note: To install the client software, please provide the End	point Protector Server IP, Port and Department Code.		
Appliance	Endpoint Protector Server IP: 442			
System Maintenance	Department Code: defdep			
System Configuration	Preserve Server	r Settings on all download pages		
Client Software Client Software Upgrade	📩 Download			
System Administrators System Departments System Security System Settings System Licensing	Endpoint Protector Client for Windows can be deployed over Active For more information, please refer to Endpoint Protector - User	Directory. - Guide.		
System Parameters				
Support				
Endpoint Protector 4 Copyright 2	34 - 2016 CoSoSys Ltd. All rights reserved.			Ready Version 4.5.0.1

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.

	B Endpoint Protector Setup
	Server information Specify the server address and port
	Server Information
1	Server IP:
	Server Port: 443
	Department Code: defdep
1	
	Advanced Installer

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	4 Reporting a	nd Administration Tool		Welcome Guest Login English →
	Login	Device Control	Blocked Devices	
	Username Password	Enforced Encryption	Authorized Devices	
	Login c PC Nativary	Content Aware Protection	Reporting and Analysis	
Controller Production	e Mobile Devices	Strong Security Policy	App Management Facking and Locating	
Data	Loss Prevention D	Device Control Cont	tent Aware Protection Mobile Device Managment	

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 <u>http://www.endpointprotector.com/support/</u>.

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

	ENDPOINT PROTECTOR 4	Reporting and Admi	nistration Tool	English	Welcome t t Logout
	Dashboard	Contact Support			Show all departments
Í	Endpoint Management	Support Form			
Ca	Endpoint Rights	Sender E-mail *	administrator@cososys.com		
X	Endpoint Settings	Company Name			
Ø	Content Aware Protection	Subject Content	Please describe here your problem or your suggestions!		
	Mobile Device Management				
	Offline Temporary Password				
	Reports and Analysis				
	System Alerts				
\$	Directory Services	Send			
٨	System Maintenance				
0	System Configuration				
	System Parameters				
\bigcirc	Support				
	User Manual AD Deployment Guide <u>Contact Support</u>				
Endpo	sint Protector 4 Copyright 2004 - 2012 Co	SoSys Ltd. All rights reserved.			Ready Version 4.1.0.2

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.

© 2004 – 2016 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Android is registered trademark of Google Inc. Macintosh, Mac OS X, iOS, MacBook, are trademarks of Apple Corporation. AWS and Amazon Web Services is a trademark of Amazon. All other names and trademarks are property of their respective owners.