Quick Start Guide for Symantec™ Endpoint Protection for Amazon Web Services

Usage instructions and best practices for Symantec Endpoint Protection Manager on Amazon Web Services (AWS)

When you log on to Symantec Endpoint Protection Manager Amazon Machine Image (AMI) on Amazon Web Services for the first time, you should be aware of the following:

Table 1

Item	Description
Initial logon credentials	When you connect to the instance for the first time, Symantec Endpoint Protection Manager opens automatically and then prompts you to change the password.
LiveUpdate launches after initial logon	When Symantec Endpoint Protection Manager LiveUpdate launches for the first time, it downloads more content than during subsequent LiveUpdate sessions. As a result, the responsiveness of the instance slows down until LiveUpdate completes. This behavior is expected, and only occurs on this initial launch. LiveUpdate launches five minutes after your initial logon to Symantec Endpoint Protection Manager.
Client does not appear immediately in Symantec Endpoint Protection Manager	You may notice that the client that is preinstalled on the instance does not immediately display on the **Home** tab in Symantec Endpoint Protection Manager. This behavior is expected. After the heartbeat into Symantec Endpoint Protection Manager completes, the client appears on the **Home** tab.
Update the email address for **admin**	You must change the default email address for **admin** in Symantec Endpoint Protection Manager. By default, the email address is a@b.com. You can easily change this email address after you log on to Symantec Endpoint Protection Manager in the **Admin** pane, under **Administrators > Edit the administrator**. Since password recovery for Symantec Endpoint Protection Manager requires a valid email address, you should perform this task the first time you log on.
Update the database password	As of version 14, you can change the database password for Symantec Endpoint Protection Manager. You should change this password the first time you log on.

Table 1 *(continued)*

Item	Description
Remote push deployment (optional)	Symantec Endpoint Protection Manager push deployment makes use of the ICMP ping protocol to look up the IP address of an instance on the network. You must explicitly add the **ICMP Echo Request** ingress rule on client instance candidates in order for them to be visible on the Symantec Endpoint Protection Manager Client Deployment Wizard. To successfully deploy the client package from Symantec Endpoint Protection Manager to the client instances, you must enable TCP port 445 on the client instances. See the section Security Groups for more information.
Security Groups	The following tables demonstrate recommended security group firewall rules for AMI instances running Symantec Endpoint Protection: ▪ Table 2 ▪ Table 3 For information on how to work with client instances, see: Amazon EC2 Security Groups for Windows Instances

Table 2 Incoming security group settings for Symantec Endpoint Protection instances

Type / Protocol	Applies to	Port number	Source	Purpose
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8014 443*	0.0.0.0/0	Used for HTTP communication between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection clients. * = Used for the optional HTTPS configuration.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8443	0.0.0.0/0	Used for HTTPS communication between a remote management console and Symantec Endpoint Protection Manager. All logon information and administrative communication takes place using this secure port.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8444	0.0.0.0/0	Used by the Symantec Endpoint Protection Manager web services.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8445	0.0.0.0/0	Used for HTTPS communication for the reporting console.

Table 2 Incoming security group settings for Symantec Endpoint Protection instances *(continued)*

Type / Protocol	Applies to	Port number	Source	Purpose
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8765	0.0.0.0/0	Used for Tomcat shutdown.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	9090	0.0.0.0/0	Used for the initial logon communication between a remote management console and Symantec Endpoint Protection Manager to display the logon screen.
Custom TCP Rule / TCP	Symantec Endpoint Protection client	445	0.0.0.0/0	Used for remote deployment of installation packages from Symantec Endpoint Protection Manager.
Custom ICMP Rule / Echo request	Symantec Endpoint Protection client	N/A	0.0.0.0/0	Used by Remote Push to look up the IP address of an Symantec Endpoint Protection client instance on the network.
RDP / TCP	Symantec Endpoint Protection Manager, Symantec Endpoint Protection client	3389	0.0.0.0/0	Used to remotely connect to the instance.

Table 3 Outgoing security group settings for Symantec Endpoint Protection instances

Type / Protocol	Applies to	Port number	Destination
All traffic / All	Symantec Endpoint Protection Manager Symantec Endpoint Protection client	All	0.0.0.0/0

Requirements to use Symantec Endpoint Protection Manager on Amazon Web Services

Amazon Web Services (AWS) account holders can subscribe to Symantec Endpoint Protection Manager on an Amazon Machine Image (AMI) on Amazon's Elastic Compute Cloud (EC2).

This table highlights prerequisites, supported platforms, and instances to run the Symantec Endpoint Protection Manager AMI.

Table 4

Requirement	Details
Prerequisites	The prerequisites to use Symantec Endpoint Protection Manager AMI for Amazon EC2 are as follows: ■ You must have an AWS Marketplace account. To create an account or to access an existing account, go to: https://aws.amazon.com/marketplace ■ If you use the Bring Your Own License (BYOL) option, you must have a valid license for Symantec Endpoint Protection. To review your licensing status, log on to the Symantec Licensing Portal, which is now part of MySymantec, under My Products: https://licensing.symantec.com/ Alternately, you can contact Symantec customer support for non-technical questions about your license: http://customersupport.symantec.com/
Supported Platforms and Instances	Symantec Endpoint Protection Manager AMI for Amazon EC2 (BYOL and Paid) includes support for: ■ Symantec Endpoint Protection Manager, version 14 MP1 ■ Windows Server 2012 R2 Symantec Endpoint Protection Manager AMI supports the following Amazon EC2 instances of Windows Server 2012 on the AWS Marketplace: ■ 10 client tier: m4.large (2x CPU, 8 GB RAM, EBS disk) ■ 100 client tier: m4.xlarge (4x CPU, 16 GB RAM, EBS disk) ■ 250 client tier: m4.2xlarge (8x CPU, 32 GB RAM, EBS disk) ■ 500 client tier: c4.2xlarge (8x CPU, 15 GB RAM, EBS disk)

Additional reference

The following documentation provides additional information for using Amazon EC2 and Symantec Endpoint Protection AMI:

- Getting Started with AWS
- Symantec Endpoint Protection 14 Installation and Administration Guide