

Quick Start Guide

This guide describes the installation and initial configuration of the IBM Security Access Manager virtual appliance.

National Language Version: To obtain the *Quick Start Guide* in other languages, print the language-specific PDF file from the installation media.

Product overview

The IBM® Security Access Manager virtual appliance helps organizations secure and manage mobile user access and protect mobile applications against fraudulent unauthorized access.

1 Step 1: Access the software and documentation



If you download your product from Passport Advantage®, follow the instructions in the download document at <http://www.ibm.com/support/docview.wss?uid=swg24035706>.

This product includes the following components:

- IBM Security Access Manager virtual appliance firmware. An .iso image is provided to install the virtual appliance.
- Documentation. See the IBM Security Access Manager for Mobile Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html.

2 Step 2: Evaluate the hardware and system configuration



Supported Hypervisors

- ESXi versions 5.0 and 5.1, or later

Supported Browsers

- Mozilla Firefox, versions 17 or later.
- Microsoft Internet Explorer, versions 9.0 or later.
- Google Chrome, versions 27 or later.

For the latest system requirements, click the **Product requirements** link on the Welcome page at http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html.

3 Step 3: Gather network information



You can use either DHCP or a static IP address to manage the appliance for networking. If you are using a static IP address, use this list to record important information for configuring the appliance network:

- Host name
- Management IP address
- Management Subnet Mask
- Management Gateway
- Management DNS server

If your virtual machine is using DHCP, the appliance obtains a dynamically leased IP address from the local DHCP server when it is powered on. You can use DHCP discovery software to locate this IP address, or you can connect directly to the appliance console to manage the Interface Settings.

4 Step 4: Virtual network configuration



It is vital that the VMWare networking is configured correctly before you attempt to install and run the virtual appliance.

The appliance uses up to six network devices. The first two network devices are the management interfaces. These devices are mandatory. The final four network devices are protection interfaces. You must configure at least one of these protection interfaces. That is, for the appliance to function correctly, you must define and enable at least three virtual network devices for the VMWare system.

5 Step 5: Install the appliance



Complete these steps to install the appliance firmware in a virtual machine environment:

1. Create a new virtual machine with the following minimum specifications:
 - VMware disk space requirement: 100 GB
 - VMware memory requirement: 4 GB
 - Virtual network devices: 3 (Maximum 6)
 - Virtual DVD/CD-ROM drive
2. Configure the virtual machine to boot from the supplied .iso file.
3. Start the virtual machine. The firmware installer starts running automatically.
4. Select the language that you want to use from the list of available languages.
5. The system prompts you to install the firmware. Enter yes to proceed.
6. When the firmware installation is complete, the system prompts you to reboot. The virtual machine reboots to the appliance console unconfigured login prompt.

6 Step 6: Get started



1. Access the appliance console or the LMI to start the wizard. To use the LMI, you must browse to the IP address of the appliance. By default, when the virtual image starts, it attempts to obtain an IP address from the local DHCP server. You can use DHCP discovery software to obtain the allocated IP address.
2. Log in as the admin user. The default password is admin. To secure the appliance, change the password immediately when prompted by the wizard.
3. Use the Appliance Setup wizard to complete the initial configuration of the IBM Security Access Manager virtual appliance. Follow the wizard prompts to configure the required details. The following list is a subset of the tasks involved:
 - Read and accept the License Agreement. If you are using the LMI, download and install the license file. You must have a license installed to download the firmware updates.
 - Set the appliance password.
 - Configure the networking, which includes the host name, management interface settings, and DNS configuration.
 - Configure the date and time settings.
4. When you complete the basic configuration, a summary screen displays. If you are using the LMI, review the details on the Completion page and click **Complete Setup**. If you are using the appliance console, follow the prompts to **Accept the configuration**.
5. Download the activation key from your account on Passport Advantage at <https://www.ibm.com/software/howtobuy/softwareandservices/passportadvantage/>.

To continue the setup process, see the “Getting Started” sections in the *Appliance Administration Guide* and *Configuration Guide* in the information center.

More information



For more information, see the following resources:

- The *IBM Security Access Manager for Mobile Administration Guide* walks you through other important tasks for monitoring, securing, and managing the appliance. This guide is available, along with the rest of the documentation, in the IBM Security Access Manager for Mobile Information Center: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.ammob.doc_8.0.0/welcome.html
- IBM Support at http://www.ibm.com/support/entry/portal/overview/software/other_software/ibm_security_access_manager_for_mobile
- IBM User Communities at <http://www.ibm.com/community/>
- IBM Passport Advantage at <http://www.ibm.com/software/howtobuy/passportadvantage/>

