Quick Installation Guide
PineApp Mail-SeCure™ software
as Mail-Relay

This Quick Installation Guide is designed to help you get started quickly and easily install PineApp™ Mail-SeCure™ software. We strongly recommend reading through these instructions carefully before beginning your installation. For more detailed instructions, please refer to the complete User Manual which is adjacent to the documentation CD that accompanies to the installation CD. If you want to set up any advanced features, please refer to the User Manual for further help.

Software Installation

1. Power up your hardware device, and adjust your BIOS to boot from CD-ROM.
2. Insert PineApp Mail-SeCure software's CD, save your settings and reboot your device.
3. Make sure that your system is connected to a network with internet access, and access to port 443 (HTTPS) is permitted by your organization's firewall.
4. The following text will appear on the screen:

If you wish to cancel the installation please remove the CD and reboot your appliance. Otherwise, please type "YES" in order to proceed with the installation.
At this stage – type YES (all capital) and hit the ENTER button.
You will be asked *Do you wish to obtain an IP using DHCP (Y/n)?*
If you would like your device to automatically obtain an IP address using DHCP server, type **Y** (capital letter) and hit the ENTER button and proceed to step 6 below.
If you wish to assign a manual IP address, type **n** (lower case) and hit the ENTER button.
Afterwards, you will be required to configure an IP address for your device manually. Please type in the desired IP address, its corresponding subnet mask & default gateway, and hit the ENTER button in order to proceed with installation.

5. You will be requested to insert your product's license installation key. Carefully type in the key, and hit the ENTER button.
6. The installation process will start. The system will automatically reboot.
7. Upon reboot, make sure to re-adjust your hardware's BIOS to boot from its hard-drive.
8. Remove Mail-SeCure's installation CD, save your settings and reboot.
9. The appliance will now perform another boot process, after which Mail-SeCure system will be installed completely on your device.

Please note: Mail-SeCure can be installed in the DMZ or in the LAN. Please make sure you are familiar with the network topology before beginning the installation and have full access to your Firewall in order to configure it according to the desired topology.

Web Based Installation

1. Connect the workstation that you prepared to the Mail-SeCure unit using a standard network cable. The workstation and the Mail-SeCure unit must be connected to the same network. You may also connect directly from the workstation to the Mail-SeCure™ unit. This will require a crossed network cable.
2. Connect the network cable to your device's network interface card, and assign it with a suitable class C IP address (**192.168.24.x**). No subnet mask assignment is needed.
3. Using your workstation, open the web browser and enter the default URL address of the Mail-SeCure™ unit: https://192.168.24.24:7443 (you can also connect to the system with http://192.168.24.24:7080).
4. A security alert message will appear. Click OK to continue. In IE 7.0, an error page may appear. Click on "Continue to this website (not recommended)" in order to continue.
   Enter the default username and password. The default username is *"pineapp"* and the default password is *"password".*
5. In order to continue you will need to read and accept the User License Agreement.
   Once you have successfully logged in, you will see the status page of the system information.

It is recommended that you change the system password before continuing. To change the password, go to the "**User Management**" tab in the "**System**" menu.
Click on "*pineapp login*", the details of that account will appear on the right column – change the password there (Chapter 2 in the User Manual).

6. Configure your IP, subnet and Gateway addresses. To do this, go to the **"Networking > Interfaces"** tab and enter the information replacing the present configuration or creating new network interfaces. After you have finished, click the "**Save Changes**" button and then click the "**Apply Changes**" button. At this stage you will lose connection to the system. Wait approximately 2 minutes before logging back into the system (Chapter 3 in the User Manual).
7. Set the system clock (**"System > Clock"**) and reboot the system **("System > Advanced > Reboot System"**) to regain access.
8. Repeat steps 3-5 using the IP that you configured in step 8.
9. Define the DNS servers for the system. Go to the **"Networking > General"** tab.

Add the IP's of your DNS. It is recommended that you leave the local host as is (127.0.0.1) and add the DNS servers' IPs in addition to it. After each entry you should hit the "**Save Changes**" button.

IMPORTANT: In order for some of the Anti-Spam engines to work properly, please verify that the system can resolve addresses from external networks.

10. Go to: **"Mail System > General"**, **"Mail Policy > General"** and **"Anti-Virus"** tabs and insert the system administrator's email address in the appropriate text fields. Don't forget to hit the **Save Changes** and the **Apply** buttons respectively.
11. Configure your domains and your destination Mail Server: Go to the **"Mail System > Local domains"** tab. Here you can set your domains and choose a default domain (Delivery method: SMTP). After you have created the list of domains, click on the domain and a table will appear at the bottom of the domain

list. Here you can define the destination Mail Server for each domain. Type the mail server's IP address and hit the "Add" button (Chapter 4 in the User Manual).

12. Update the Anti-Virus. Go to the "Anti-Virus" menu and click the "**Update**" button.

13. Policy Enforcement: Mail-SeCure has two preconfigured rules: **A.** Block all executable files. **B.** Global Spam rule.
We strongly recommend you keep these rules. In order to add / edit rules, go to **"Mail Policy > Policy"** tab (Chapter 5 in the User Manual).

14. Go to **"Anti-Spam > General"** tab and make sure the "Activate Advanced Anti-Spam module" box is checked. Also, we strongly suggest the following modules are activated:

- ✓ Commtouch RPD™ technology
- ✓ Zero-Hour™ Virus protection
- ✓ Deep-Inspection™ engine
- ✓ PineApp ZDS™

The remaining engines can be activated by the administrator.

15. Set User Personal Daily Reports (Chapter 7 in the User Manual).

IMPORTANT: When you finish all configurations, click the "Apply Changes" button or you will lose all of the changes you have made.

Configuring the Firewall

If the Mail-SeCure is located behind a Firewall (in the LAN or in the DMZ), the following ports should be open:

Port	Direction	Protocol	Description
25	In/Out	TCP	SMTP protocol. For incoming and outgoing mail
7022	In	TCP	Remote service and support (by PineApp) - optional
7443	In	TCP	Remote service and support (by PineApp) - optional
53	Out	TCP and UDP	DNS (Domain Name Service)
80	Out	TCP	Anti-Spam Tools, Anti-Virus Updates, Software Updates and Spam updates

* In case the Mail-SeCure is behind a Proxy, refer to chapter 3 in the User Manual.

Please note that if the system acts as a Mail Server, port 110 TCP should be open to the system.

Post Installation Check List

Test Number 1	"Networking" > "Tools & Information" > check if the device can telnet on TCP port 80 with Host: www.pineapp.com
Test Number 2	"Networking" > "Tools & Information" > check if the device can telnet on TCP port 25 to internal Mail Server with Host: xxx.xxx.xxx.xxx
Test Number 3	From your Firewall on all routed ports to Mail-SeCure host (Management Ports & SMTP).

Getting Started

After setting up the system, all email should be routed to the Mail-SeCure™ unit. If an external IP address was assigned to the Mail-SeCure™ unit, the MX record at your Internet Service Provider (ISP) should point to the newly configured IP. Please contact your ISP for assistance with changing the MX record. If you have no free IP addresses or prefer that the Mail-SeCure™ be unexposed behind the Firewall, you will need the Firewall to port forward all incoming mail to the Mail-SeCure™ unit.

Outgoing Mail

In order to route outgoing mail through the Mail-SeCure™ unit, you will need to make sure that:

1. Port 25 TCP and UDP from Mail-SeCure™ to the Internet is open.
2. Configure the smart host on your Mail Server to point to the Mail-SeCure™ unit.
3. Add the internal IP of the Mail Server to the trusted IPs ("Mail System" > "Relay Networks") Please confirm you did NOT add the Firewall's IP in the Relay networks.

Backing up the configuration

Once configured, it is highly recommended that you back up your configuration ("**System**> **Configuration Management**"). Chapter 2 in the User Manual.

Technical support

In case you need any technical support, please contact your reseller or PineApp's technical support center:
North America: +1-877-300-3422
International: +972-4-8212-321
Email: support@PineApp.com
Website: http://www.pineapp.com/