Trend Micro™ Encryption for Email Gateway 5

Secured by Private Post™

Quick Installation Guide

Messaging Security

Document Part No. EEEM54295/100119

Release Date: January 2010

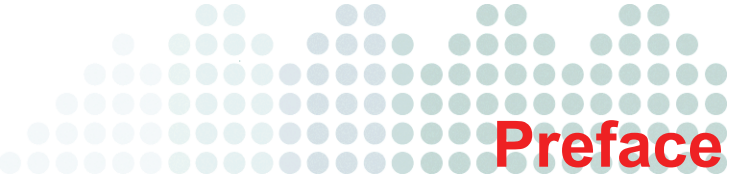
The user documentation of Encryption for Email Gateway is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the Online Help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents



Preface

Welcome to the *Encryption for Email Gateway Quick Installation Guide*. This guide contains information about product settings and service levels.

This preface discusses the following topics:

- *Trend Micro™ Encryption for Email Gateway Documentation*
- *Audience*
- *Document Conventions*

Trend Micro™ Encryption for Email Gateway Documentation

The Trend Micro™ Encryption for Email Gateway documentation consists of the following:

Trend Micro™ Encryption for Email Gateway Administrator's Guide — Helps you plan for deployment and configure all product settings.

Online Help — Helps you configure all features through the user interface. You can access the Online Help by opening the Web console and then clicking the **Help** icon ().

Trend Micro™ Encryption for Email Gateway Quick Installation Guide — Helps you plan for deployment and configure product settings.

Readme File — Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The readme is available at:

http://www.trendmicro.com/download

Audience

This document is intended to be used by new users of the Encryption for Email Gateway Administrator Console, including system administrators, operators, sensitive content contributors, information security staff, executives, and other users with other specific roles.

The audience should have a thorough understanding of the Encryption for Email Gateway system, including general operations and critical concepts. Familiarity with Web browsers and Web-based user interfaces are also required.

Document Conventions

To help you locate and interpret information easily, the Encryption for Email Gateway documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and ScanMail tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Installation

This chapter introduces the *Encryption for Email Gateway Quick Installation Guide*.

Topics include the following:

Overview

Encryption for Email Gateway is a Linux-based software solution providing the ability to perform encryption and decryption of emails at the corporate gateway, regardless of the email client and platform from which it originated.

The encryption and decryption of email on Encryption for Email Gateway is controlled by a Policy Manager that enables an administrator to configure policies based on various parameters, such as sender and recipient email address, keywords or Payment Card Industry (PCI) compliance. Encryption for Email Gateway presents itself as a Simple Mail Transfer Protocol (SMTP) interface and delivers email over SMTP to a configured outbound MTA. This enables easy integration with other email server based products, be them content scanners, mail servers or archiving solutions.

Encryption for Email Gateway documentation is written for IT administrators and email administrators. The documentation assumes that the readers have an in-depth knowledge of email messaging, networks VMware virtual appliances. The document does not assume the reader has any knowledge of email encryption technology.

Terminology

The following list describes acronyms and definitions for terms used throughout this document:

TABLE 1-1. List of Terminology

TERM	DEFINITION
CORBA	Common Object Request Broker Architecture
DLP	Data Loss Prevention
IBE	Identity-based Encryption
MTA	Mail Transport Agent
PCI	Payment Card Industry
SMTP	Simple Mail Transfer Protocol
TMEE	Trend Micro Encryption for Email

TABLE 1-1. List of Terminology (Continued)

TERM	DEFINITION
VT	Virtualization Technology – for hardware assisted virtualization.

Minimum Requirements

For details about the recommended minimum requirements, refer to the readme.

Installation Prerequisites

The installation of Encryption for Email Gateway requires a connection to VMware Infrastructure Client. An installation and configuration of VMware ESX/ESXi needs to be done before you can access an ESX Server host, or a VirtualCenter. The installation and configuration of VMware ESX/ESXi is outside the scope of this guide. See the VMware documentation for this information.

Installing Encryption for Email Gateway

To begin installation:

1. Connect to the VMware Infrastructure Client and enter your login details. To open the VMware Infrastructure Client, select **Start>Programs>VMware>VMware Infrastructure Client**.

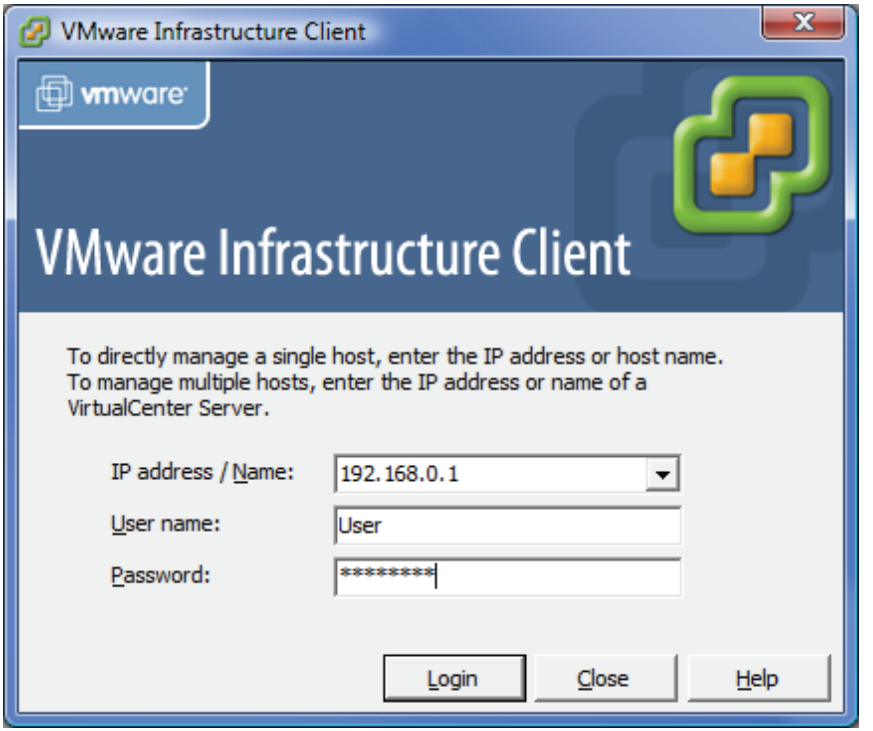


FIGURE 1-1 VMware Infrastructure Client - Login Example

2. Enter the IP address/ Hostname, User name and Password and then click **Login**.

   Note that these details are unique and should have been specified at the time of installation of the ESX/ESXi platform.

3. After logging on, the following screen appears:

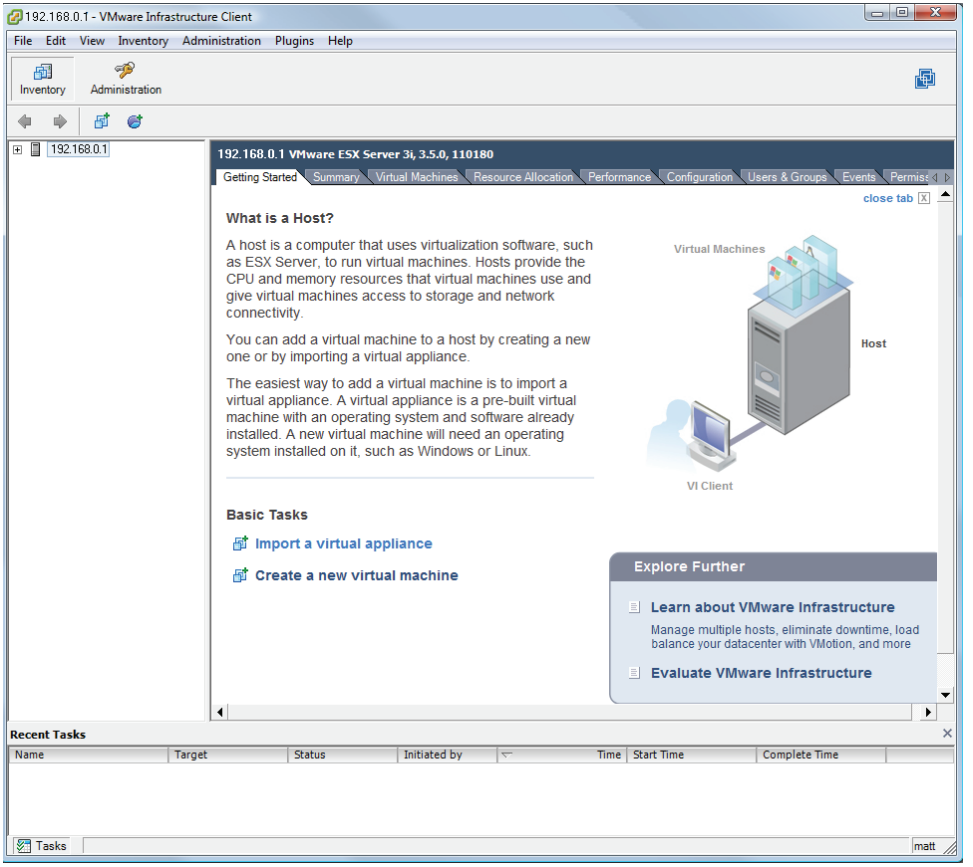


FIGURE 1-2 Import a Virtual Appliance

4. Choose **Import a virtual Appliance** from under "Basic Tasks" to access the Import Virtual Appliance Wizard.
5. Select the **Import from File** radio button and then click **Browse** to locate the `.OVF` file.

   The `.OVF` file is located in the directory where you initially downloaded the Encryption for Email Gateway files.

6. Select **Next** to continue with the import process.

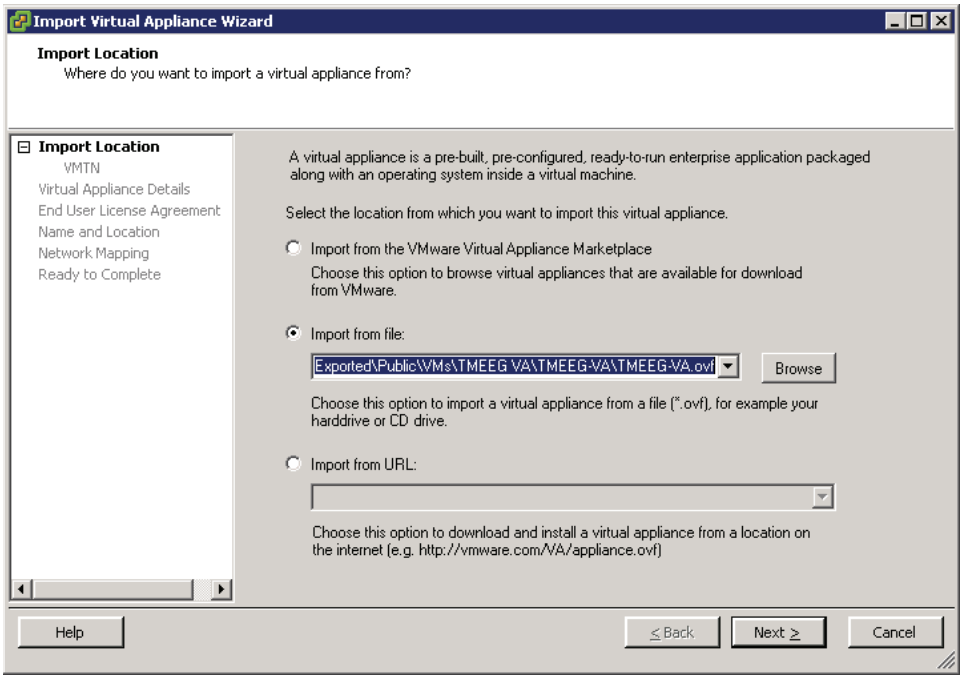


FIGURE 1-3 Import Virtual Appliance Wizard

7. Confirm the details of the OVF file and then select **Next**.

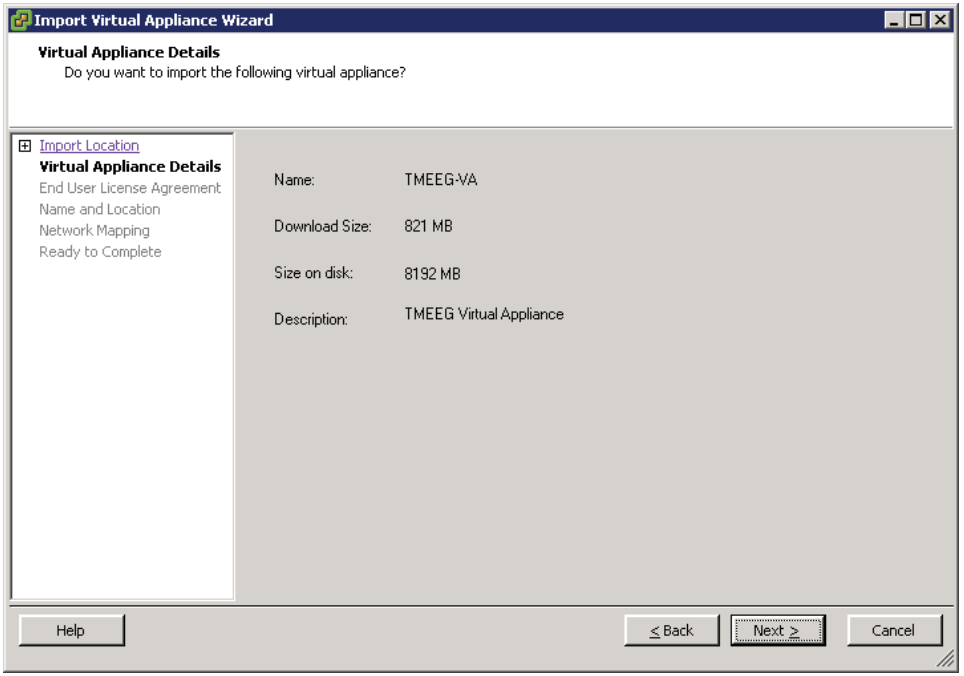


FIGURE 1-4 Virtual Appliance Details

8. Read the Encryption for Email Gateway Licence Agreement first and accept this by choosing the check box **Accept all License agreements**. Select **Next** to proceed to the next step.

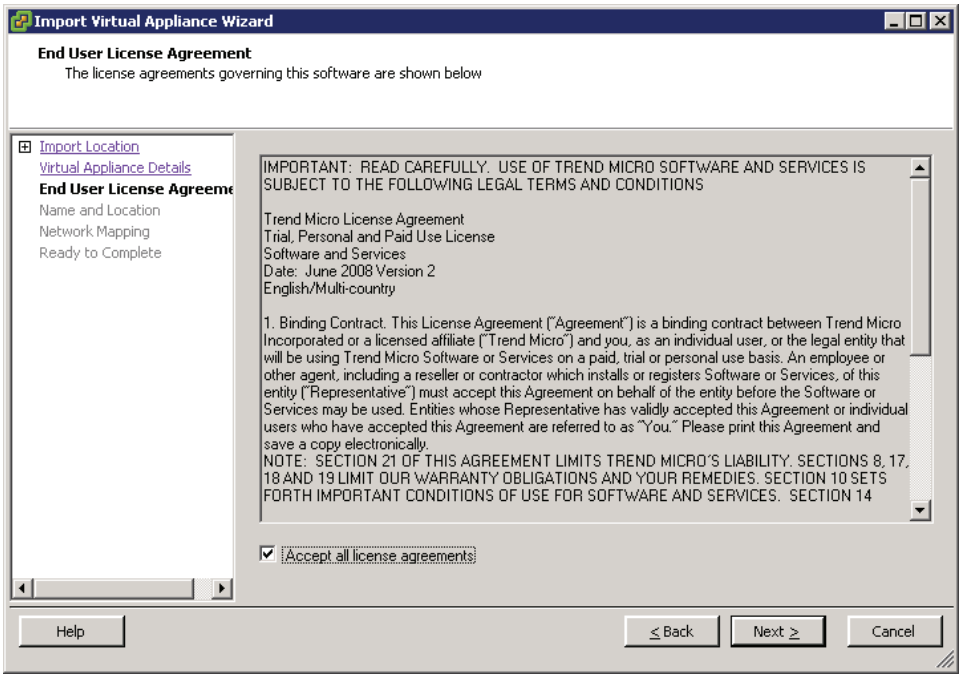


FIGURE 1-5 Encryption for Email Gateway License Agreement

9. Enter a Name for the new virtual appliance and then select **Next**.

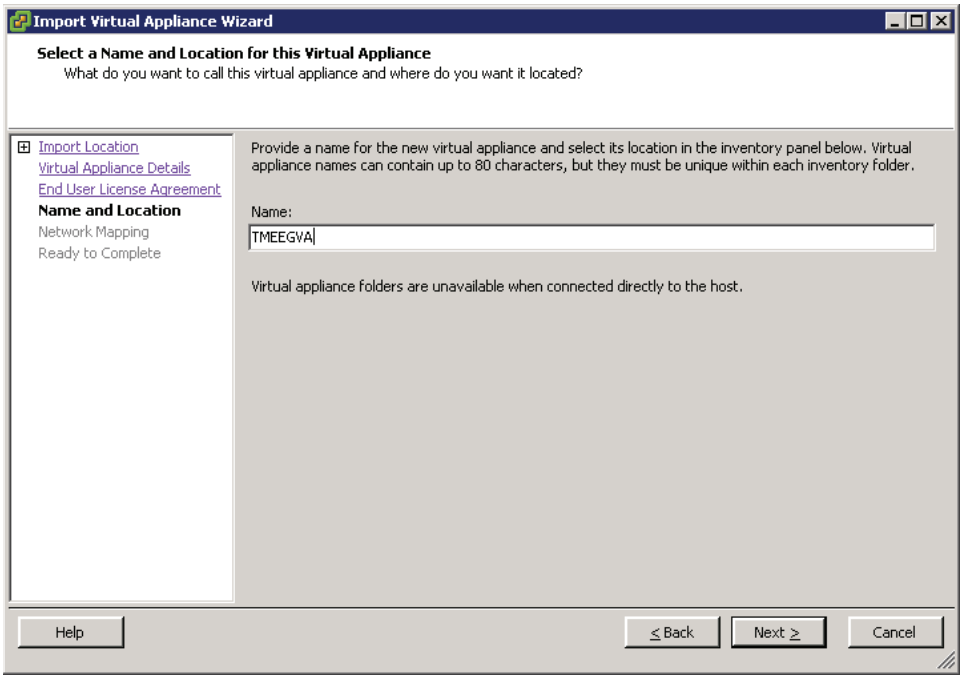


FIGURE 1-6 Name and Location

10. Configure the Network Mapping by selecting the virtual network that you would like to connect to and click on **Next**.

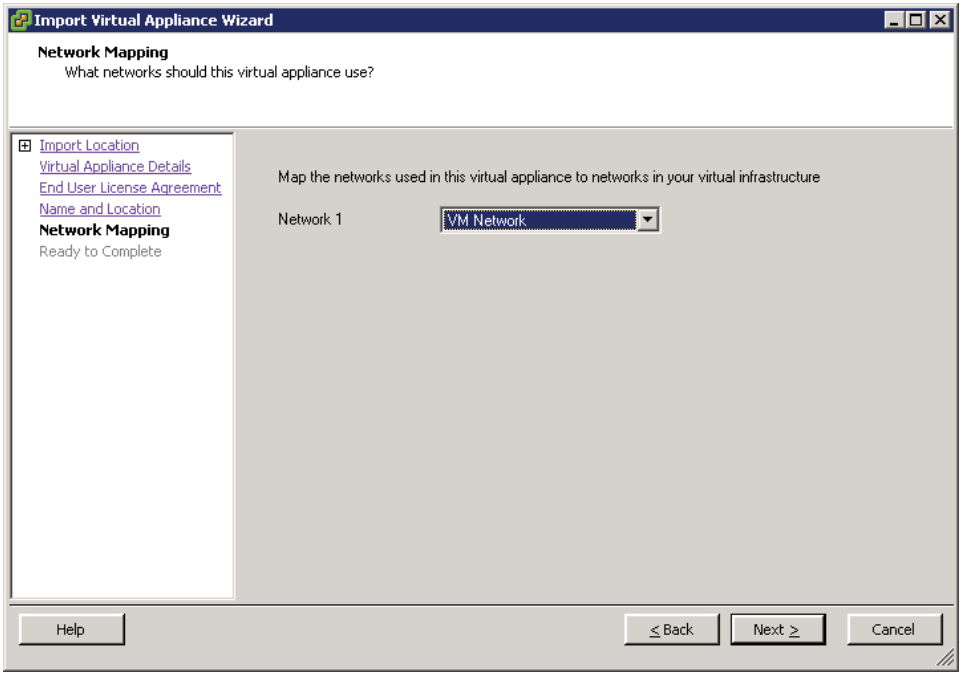


FIGURE 1-7 Network Mapping Example

11. Review the summary and click **Finish**.

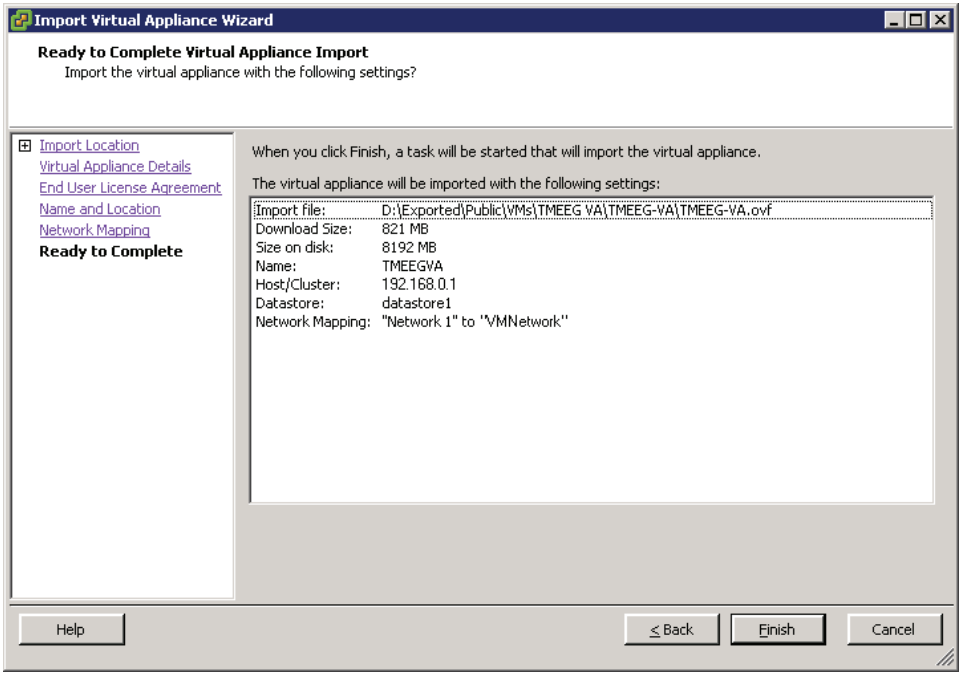


FIGURE 1-8 Ready to Complete Virtual Appliance Import

12. From the Virtual Infrastructure Client screen, select the Virtual Machine that you have just loaded and right-click to display a menu with a list of options.

13. Select **Power On** from the menu to start the virtual appliance.

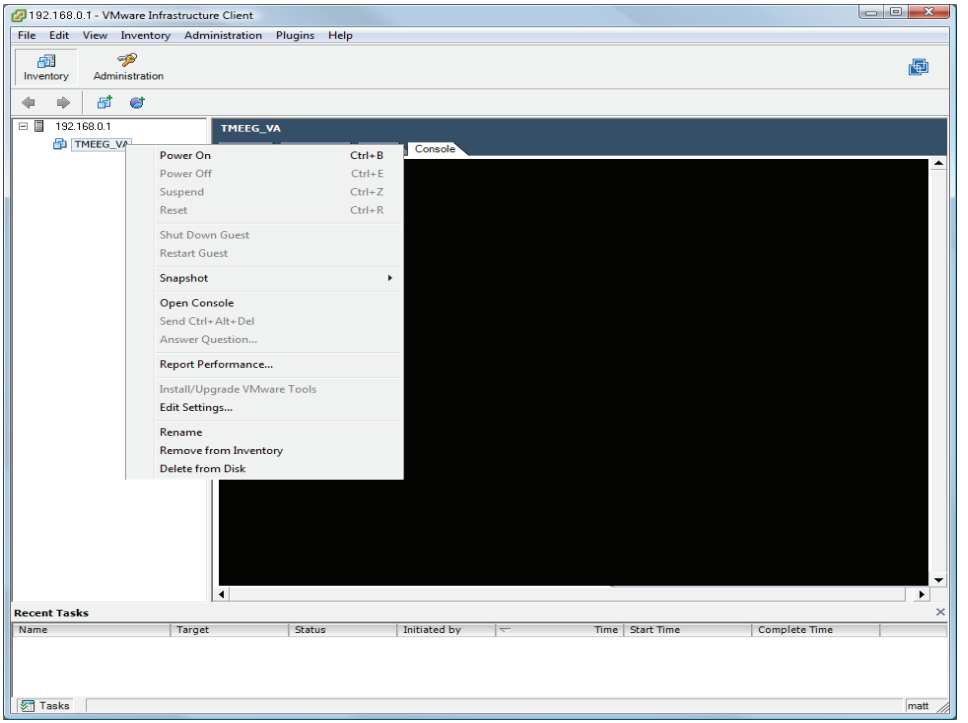


FIGURE 1-9 Virtual Infrastructure Client

14. Allow the boot up sequence to finish and display.
15. Make a note of the address to access the **Virtual Appliance Web Interface**.

    In this example the address is `https://192.168.30.202`. It is important to have this information on hand for the next set of steps.

Note: The virtual appliance is configured to obtain network information via DHCP. It is suggested that either a static address reservation is assigned to the Encryption for Email Gateway MAC address in DHCP, or alternatively configure a static IP address through the command line.

In environments where DHCP is not enabled, or a static IP address is desirable, perform the following steps:

1. Log in to the Encryption for Email Gateway console using the username and password as shown in Figure 1-10.
2. Enter the following command:

   `ifconfig eth0 192.168.1.30 netmask 255.255.255.0`

   (replace `192.168.1.30` and `255.255.255.0` with the proper IP and netmask)

   `route add default gw 192.168.1.1`

   (replace `192.168.1.1` with the correct gateway address)

   `vi /etc/resolv.conf`

   (replace the IP of "nameserver" with the appropriate value)
3. Connect to the Webmin Web console for the static configuration:

   `https://192.168.1.30:10000`

   Log in using the same credentials as mentioned previously.

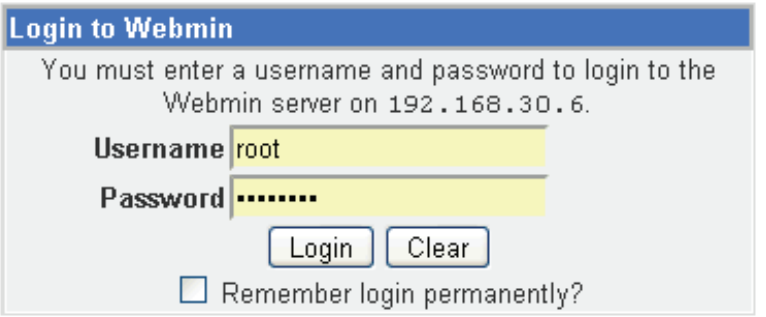


FIGURE 1-10 Webmin Login page

4. To configure the network, choose **Networking > Network Configuration**.

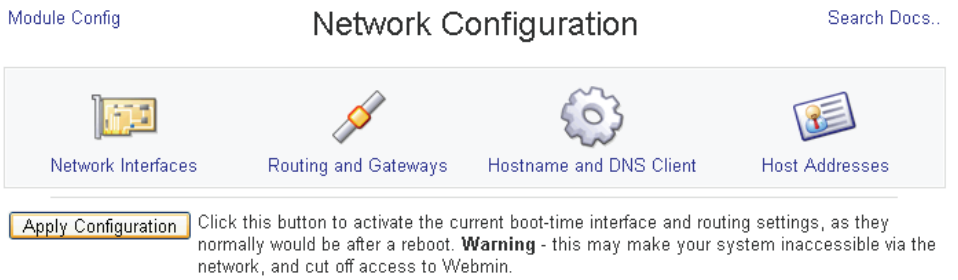


FIGURE 1-11 Network Configuration page

5. Select **Network Interfaces** and then **eth0**.
6. Select **Static**, and define the IP address and netmask.

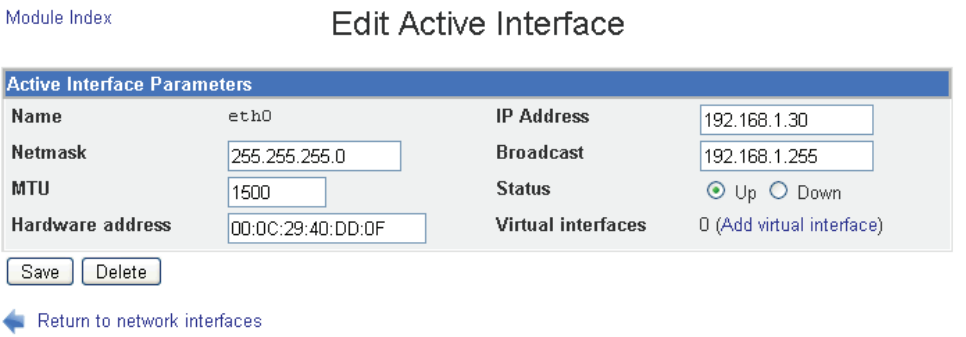


FIGURE 1-12 Active Interface Configuration page

Note: If you do not know your broadcast address, you can get it by typing the following command in the shell:

```
ifconfig eth0 | grep --color Bcast
```

---

7. Click **Save**.
8. Select **Routing and Gateways**.

9. In the **Default routes** dropdown list, select **eth0** as the interface and set the correct gateway.

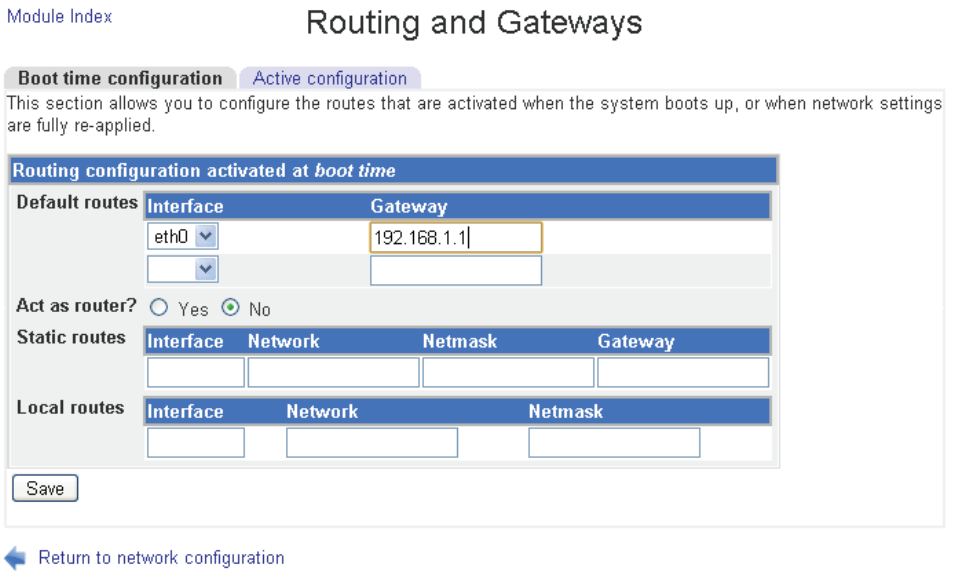


FIGURE 1-13 Routing and Gateways Configuration page

10. Click **Save.**
11. Click **Apply Configuration**.
12. Optionally, reboot Encryption for Email Gateway by entering the `reboot` command in the shell:.
13. Ensure that an open connection to the virtual appliance is established, open a Web browser and enter the server address details:

    For example: `https://192.168.1.30/`

    This will present the Registration page for Encryption for Email Gateway.