

---

# **GUARDIAN DIGITAL ENGARDE SECURE LINUX QUICK START**

This short guide is designed to help you quickly set up EnGarde Secure Linux on your system and get it working on your network. We recommend you read the user manual also. This will discuss how to set up EnGarde, change user passwords and manage certificates.





---

# INSTALLING ENGARDE SECURE LINUX

The installation procedure is mostly automated and required very little interaction to install the operating system.

The installation process is started by booting to the EnGarde Secure Linux CD-ROM. If your system does not support the CD-ROM drive as a boot device or can not boot to the CD for other reasons a boot floppy must be created. If you can boot without difficulty skip the following section.

**NOTE:** The CD will boot from a SCSI CD-ROM drive, if configured to do so in your systems BIOS but it will not install from a SCSI CD-ROM drive. It must be installed via an ATAPI CD-ROM drive.

## Installing EnGarde with a boot floppy

The first step for using a floppy as your boot device is to create your boot floppy. Included on your EnGarde Linux CD are several DOS utilities along with a boot image. The boot image can be found on the CD in /boot/boot.img. There are two ways to create a boot floppy using the boot image.

If you are running in Linux, using a blank floppy, you can type the following:

```
# dd if=./boot/boot.img of=/dev/fd0 bs=1k
```

This will run a disk dump of the boot.img directly to the floppy. If you are in a DOS based system you must use an included program called 'rawrite'. The rawrite program can be found in x:\dosutils\rawrite.exe. 'x' being the drive letter of your CD-ROM.

To create a boot floppy you would enter the following:

```
x:\dosutils\rawrite.exe -f x:\boot\boot.img -d a:
```

You will now have a floppy with the EnGarde Secure Linux installer on it and ready to be booted. Reboot your system with the floppy inserted.

## Boot Menus

When you first boot you will be presented with a prompt and a small menu. You can press return to continue on with a normal installation, press F2 to view more information concerning Rescue Mode or press F3 to view additional information concerning EnGarde and the installation process.

To run a normal installation process simply press enter to start the installation. If you wish to read more about Rescue Mode read the next section, otherwise you can skip over the next section.

---

## Rescue Mode

Rescue mode is designed to be run by an experienced system administrator. Rescue mode is provided in the event your system will not boot. It contains all the necessary tools needed to troubleshoot your system in case of a system failure.

Use Rescue Mode with caution as you in single user mode and always treated as the 'root' user.

## The Installer

Once the Linux kernel finishes booting the installer will load. You will be presented with a “welcome” screen and soon be on your way.

The installer will prompt you for a few simple questions about your hardware and where to install it. Just follow the on-screen instructions.

**NOTE**        The auto partitioner will automatically remove all files systems on /dev/hda, or /dev/sda if SCSI was selected. You will loose all data on that hard disk.

Once EnGarde finishes installing you will configure your network. The default network settings are used to connect to EnGarde from another machine to run the initial configuration portion of the install. These settings are only temporary and will be reconfigured during the initial installation process.

The last step of the installation is to create a new user. A new user can also be created during the initial configuration, so it is not necessary to do so here.

**NOTE**        When creating a new user an SSH key is generated for that user. The passphrase associated with that users key is the password given for the user. You may create a new key for the user from the console or from the WebTool if you wish to change the passphrase.

Once the new user is created you can remove the bootable media and restart your machine.

---

## CONFIGURING ENGARDE SECURE LINUX

EnGarde Secure Linux comes with an easy to use front-end for installing the operating system. Described in the following section are the system requirements to successfully complete the installation and run EnGarde Secure Linux.

EnGarde Secure Linux also provides an easy to use interface for the initial configuration. The initial configuration is ran after installation to configure the software on the machine, as opposed to the installation which configures hardware. This interface requires you to configure it from another PC, via the included cross-over cable to the machine containing EnGarde. The client PC can be any operating system and only requires a browser that supports SSL. Netscape 4+ and Internet Explorer 5+ will be fine for doing this.

The interface you will be using will guide you step-by-step through the set up process. We will also outline the steps in more detail in this manual. The Guardian Digital WebTool will provide the complete ability to configure your EnGarde system.

---

## Configuring the Client Machine

A client machine is required to configure EnGarde. You will need a crossover cable to make the connection from your PC to the EnGarde machine, or you can put them both on a hub. The only drawbacks are while the system is on a hub it is vulnerable from other machines connected to that hub and the default network settings could interfere with other machines connected to that hub.

To configure your client PC you must first start by disconnecting your client PC from the network. You can simply do this by unplugging its network connection. Then change your PC's network settings. Don't forget to write down your old settings to change back to when you are finished setting up EnGarde.

Change your client PC's network settings to the following:

```
IP Address: 192.168.10.110
Subnet:     255.255.255.0
Broadcast:  192.168.10.255
Network:    192.168.10.0
```

Once you have changed your settings and the changes have taken effect, you must make sure all your proxy settings are disabled. To disable your proxy settings in both Netscape Navigator and Internet Explorer please read *Appendix C.2*. Once all changes have been made to the proxy settings you will be ready to connect to EnGarde.

---

## Connecting to EnGarde

At this point you have your client PC's network configuration set up to work with your EnGarde system, and you have it physically connected to your PC via the included cross-over cable. You are now ready to connect to your EnGarde system.

Start by powering up your EnGarde system. There is a rocker switch located on the front panel. Hold the button down until the machine starts to power on.

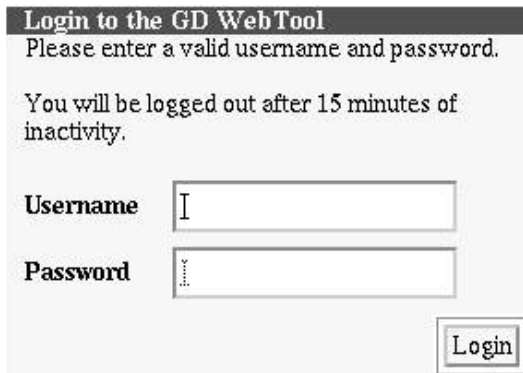
Now load up the browser on your PC. Either Internet Explorer 4+ or Netscape Navigator 4+ is required. First you must make certain that you have proxy servers disabled. You will not be able to successfully connect to EnGarde with proxy servers enabled. Type in the following address:

`https://192.168.10.100:1023`

It will take a few moments to connect. Once the connection is made you will be informed of a new certificate. Guardian Digital distributes EnGarde with a certificate generated by our security team. Since the certificate is not issued by a certificate authority you will be prompted to accept the certificate. Instructions on how to do this and more information concerning certificates can be found in *Appendix D* if necessary.

After accepting the certificate you will be prompted for a login name and password. This information is pre-set to:

Login: admin  
Password: lock&%box



**Login to the GD WebTool**  
Please enter a valid username and password.  
You will be logged out after 15 minutes of inactivity.

**Username**

**Password**

---

The login and password are case sensitive. During step 2 of the initial configuration you will be prompted to change the password. You **MUST** change this password. Otherwise it will remain *lock&%box*.

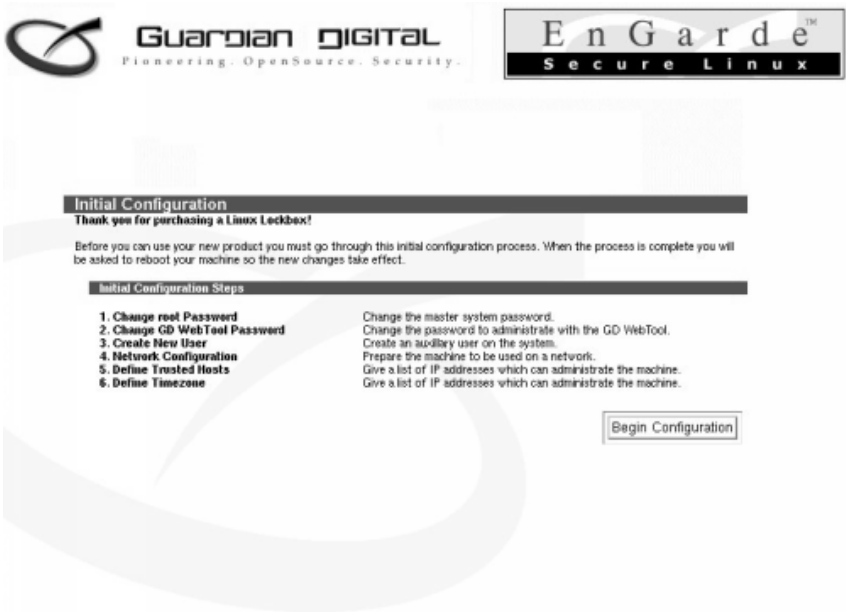


---

# Running the Initial Configuration

Once you enter the login name and password you are in the EnGarde Initial Configuration.

Now we are ready to start the initial configuration of your EnGarde system. Click on the *Begin Configuration* button to start the initial configuration process.



At the main screen you will see a brief outline of the different steps you are about to be going through, each with a brief description.

From here you can start the initial system configuration. It will guide you through step-by-step. You can not skip steps here. The next section covers each step of the configuration process.

## Change the Root Password

This first step in the configuration is to set the root password. The root password will only be used to login to the system from the console. Enter in a password

---

that is at least six characters. Mixing numbers, letters and avoiding whole words is recommended. A few examples would be to take a word like *lockbox* and break it up with some letters and numbers. You can use the following characters as well:

!	@	#	\$	%	^	&	*	(	)
---	---	---	----	---	---	---	---	---	---

So you can end up with something along the lines of:

lock%\$box

Which will be almost impossible to guess even more difficult to crack.

You have to enter the password a second time to verify they match.

**Change root Password** Step 1 of 6

In this section you will change the root password. The root account is the administration account on the Linux machine. Please choose a fairly complicated password that you will remember.

Some example passwords are:

```
lock%#box
m0unt@in!d3w
```

**Password:**

**Password (again):**

## Change the GD WebTool Password

The GD WebTool password will be used every time you login to the WebTool. We suggest making this password different from the root password but still follow the suggestions we offered above.

---

### Change GD WebTool Password

Step 2 of 6

In this section you will change the GD WebTool password. This password is used for all on-line administrative functions. Please choose a fairly complicated password that you will remember.

Password:

Password (again):

## Create a New User

You will now need to create a new user. When you access your system via a Secure Shell (SSH) or from the console you will want to use your regular user account as often as possible. This is recommended for security reasons and also for accidents that can happen when always accessing the system as the root user.

You can select *Enable remote login* so the user has the capability to connect via an SSH secure connection to EnGarde. Before a user can SSH in though, their key will have to be transferred. Information on doing this via the GD WebTool will be covered in *Section 4.4.4 Secure Shell Management*.

### Create a New User

Step 3 of 6

In this section you will create a new user. Please enter the desired username and a password.

Real Name

Username

Enable remote login

Password:

Password (again):

---

## Setup the Network Configuration

Now we are ready to configure the network settings for your EnGarde system. This section is pretty straightforward.

Configure Network		Step 4 of 6
In this section you will configure networking. Please enter all of the default network information here.		
<b>Hostname:</b>	<input type="text" value="lockbox"/>	
<b>Domain Name:</b>	<input type="text" value="guardiandigital.com"/>	
<b>IP Address:</b>	<input type="text" value="192.168.100.100"/>	
<b>Netmask:</b>	<input type="text" value="255.255.255.0"/>	
<b>Gateway:</b>	<input type="text" value="192.168.100.1"/>	
<b>Primary DNS Address:</b>	<input type="text" value="192.168.100.1"/>	
<b>Secondary DNS Address:</b>	<input type="text" value="192.168.100.2"/>	
		<input type="button" value="Change Network Settings"/>

**Hostname** The hostname is another way of labeling your computer. Generally remembering and typing in an IP address for a machine is more difficult than remembering a domain name. For example, remembering `www.guardiandigital.com` is not nearly as difficult as remembering `63.87.101.80`. You can set the hostname to any name you wish, as long as it doesn't conflict with another hostname on the network.

**Domain Name** Here we simply need the Fully-Qualified Domain Name (FQDN) without the hostname. For example `guardiandigital.com` would be entered in for `lockbox.guardiandigital.com`. For more information concerning domain names please see FQDN in the glossary.

**IP Address** An IP address is a unique number used to identify a computer on a network. Generally you can purchase a block of IP addresses you are

---

allowed to use on the Internet or are assigned one or more IP addresses from your service provider. Enter in the IP address you want to assign EnGarde to here.

**Netmask** The standard structure of an IP address can be locally modified by using host address bits as additional network address bits. Essentially, the “dividing line” between network address bits and host address bits is moved, creating additional networks, but reducing the maximum number of hosts that can belong to each network. These newly designated network bits define a network within the larger network, called a subnet. The netmask defines the subnet mask. Enter the appropriate subnet mask for the network, generally 255 . 255 . 255 . 0.

**Gateway** Computers can only talk to other computers that are on the same network. To give a computer the ability to talk to computers on another network they must communicate through a gateway. You must define the IP address of the gateway machine here.

**Primary DNS Address** The primary DNS server, also referred to as the master DNS server, controls the DNS queries for your zone. Enter in the IP address of your primary DNS server. More detailed information regarding primary DNS servers and DNS can be found in *Section 4.4.6 DNS Management*. If this machine is to be configured as the primary DNS for itself, enter it’s own IP address.

**Secondary DNS Address** The secondary DNS server, also referred to as the slave DNS server, is a backup to the primary. If the primary server doesn’t respond or returns no data the secondary DNS server will be queried. This section is optional if no secondary DNS server exists on your network. Enter the IP address of the secondary DNS server if you wish to here.

When registering a domain name on the Internet, through Network Solutions, for example, a secondary server must be provided. Guardian Digital can assist you with this. Contact us should you require assistance.

## Define Trusted Hosts

In this area you will have to supply a list of hosts that are allowed to access the GD WebTool. You can list as many hosts as you want, but we recommend listing only those that are necessary for administration. Ending the IP address with a 0 will specify a network instead of one machine.

---

You can list them by IP address, and use a blank space as the delimiter between IP or hostname.

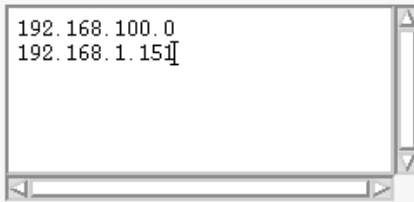
### Define Trusted Hosts

Step 5 of 6

In this section you will define which hosts will have access to the GD Web Tool. You can control access based upon:

- **Hostnames** (for example, mymachine.guardiandigital.com)
- **IP Addresses** (for example, 192.168.10.80)
- **IP Networks** (for example, 192.168.10.0)

You should limit access to trusted addresses, otherwise, anyone who guesses your password will have complete control of your system. Enter one IP address or hostname on each line.



```
192.168.100.0
192.168.1.15
```

Setup Trusted Hosts

## Define Your Time Zone

This section allows you to set your time zone. You have a selection of the four major time zones in the continental U.S. Select *Save Settings* to finish the setup process. This will enable default network time services which can be configured later if necessary.

---

### Setup Timezone

Step 6 of 7

In this section you will be asked to select your timezone. The WebTool will also select three time servers to use based on your time zone. These three time servers will be to sync your system time with the national atomic clock.

Time Zone

East

Save Settings

## Set up Services that are Active at Boot

Here you have a selection of different services that are available during boot time. You can select which ones you wish to turn on and off by selecting the check boxes. It is recommended you only activate services you will be using on this EnGarde system.

### Services Active at Boot

Step 7 of 7

In this section you will be asked to choose what services you want active at boot.

Domain Name Service

Active

Mail Server

Active

Web Server

Active

IMAP Server

Active

POP Server

Active

Save Settings

## Summary

The information you entered during the Initial Configuration will now be displayed back to you for confirmation, as shown in the next screenshot. If everything is correct click the *Confirm* button to complete the configuration process.

Click the *Start Over* button to restart the configuration process.

---

### Configuration Complete!

**Congratulations!** You have successfully configured the Lockbox. After you reboot the Lockbox networking and all services will be enabled.

Below is a summary of your configuration. You should print this out and store it in a safe place.

#### Network Configuration

<b>Hostname</b>	lockbox.linuxseclabs.com
<b>IP Address</b>	63.87.101.8
<b>Netmask</b>	255.255.255.192
<b>Gateway</b>	63.87.101.1
<b>Primary DNS</b>	
<b>Secondary DNS</b>	63.87.101.90

#### Trusted Hosts

<b>Trusted Hosts</b>	63.87.101.195, 24.198.170.251
----------------------	-------------------------------

#### Active Services

<b>Secure Shell Services</b>	Active
<b>Domain Name Service</b>	Active
<b>Mail Server</b>	Active
<b>Web Server</b>	Active
<b>IMAP Server</b>	Active
<b>User Password Changer</b>	Active

Start Over

Reboot

## Reboot

All the information from your configuration is now saved on your EnGarde system. Select the *Reboot* button and the system will be ready to go.



---

**NOTE:** Before the machine reboots you will be returned to the login screen. This is necessary for a successful system logout. You do not need to log back in.

Remove your crossover cable and plug your EnGarde system into the network. You are now ready to start administering your server.

---

## CHANGING A USER'S PASSWORD

As discussed earlier the administrator has the ability to change a users password from the GD WebTool. To increase security, the GD WebTool does not allow any user but the administrator access to those sections of the WebTool. To allow a user to change their own password themselves, a separate URL is provided. By going to:

`https://engarde.guardiandigital.com:1022`

The user can login with their normal login name and password. In the above example replace `engarde.guardiandigital.com` with the FQDN of your server.

**NOTE:** The address is very similar to the regular WebTool but notice the port you are connecting to. The port 1023 is used for the WebTool, while 1022 is the user password utility, as in the example above.

If the default Guardian Digital certificate still remains on the system the user will be prompted to accept it. Instructions on accepting a certificate can be found in *Appendix D*.

Once the user successfully logs in to the system they will be presented with the following screen.

### Change Password

Welcome to the password administration menu. Here you can change your account password. Please enter your old password in the first field and your new password in the next two fields. If the two new passwords match then your password will be changed and you will be logged out of the password changing area.

Old Password:

New Password:

New Password (again):

---

Here they must enter in their old password first, followed by their new password twice. The new password is required twice to double check for typing errors.

When everything is entered in you may click the *Change Password* button for the changes to take effect. These changes take effect immediately. Please note, you can abort this process at any time by clicking the *Abort* button.

---

## QUICK START GUIDE

This section is intended to give an overview of the functions of the Guardian Digital WebTool. After reading this appendix, the reader should be able to perform the steps required to set up a domain to receive mail, configure DNS services, and serve Web pages. If your EnGarde system will not be used to perform all of the functions listed above, it is especially important that you read the User Guide and have a full understanding of each of the services you will be configuring.

Before following the example below, your EnGarde system should have already undergone initial configuration and be plugged in and operating on a network.

To obtain a fast and most accurate setup, follow the steps in the described order. Once you have successfully completed each step, proceed in order to the next step. There are four primary steps required to configure Engarde:

1. Configure the network interface
2. Configure the DNS Server
3. Configure the Mail Server
4. Configure the Web Server to prepare for normal and secure websites

After the initial configuration of your EnGarde system, the basic system and networking functions are operating correctly and is ready to configure a sample store. We will be configuring our example EnGarde system to use the following initial values entered when EnGarde was configured:

**Hostname:** myserver

**Domain Name:** mydomain.com

**IP Address:** 192.168.1.70

**Netmask:** 255.255.255.0

**Gateway:** 192.168.1.1

**Primary DNS Address:** 192.168.1.70

**Secondary DNS Address:** 192.168.1.60

In this example, we will be creating the domain `engardelinux.com` that will be hosting our DNS, routing mail, and serving web pages.

---

## Network Interfaces

Before any interfaces are created you will need to know the following:

- Each SSL-based website requires its own IP address. If more SSL-based websites are to be served, then a new interface must be created on another IP address for each website.
- There can be many normal websites on the same IP address, given there is a *Name Virtual Host* defined in the Web server. See the *Section 4.3 Virtual Host Management* in the *User Guide* for more information on *Name Virtual Hosts*.

### Example:

In the WebTool, click on *System Management*, and then click on *Network Configuration*. There will already be an interface defined as:

	IP Address	Hostname
[ Edit ]	192.168.1.70	myserver.mydomain.com
Add a New Interface		

We want to set up a separate IP address for `www.engardelinux.com`, since we will be creating a *Secure Web Server* on it. Click on *Add a New Interface* to do this. We are now prompted for our information, at which point we enter:

**IP Address:** 192.168.1.71

**Netmask:** 255.255.255.0

After clicking the *Create* button the *Persistent Interfaces* screen will look like:

	IP Address	Hostname
[ Edit ]	192.168.1.70	myserver.mydomain.com
[ Edit ]	192.168.1.71	< Not Yet Defined >
Add a New Interface		

We have now successfully configured our network interface.

---

## DNS Server

The DNS Server is the mechanism that provides name to IP address, and IP address to name mappings. It also provides the information necessary for mail to be properly routed. DNS was created because IP addresses are often hard to remember. DNS is used to map that address to a name, which is much easier to remember.

When typing `http://www.guardiandigital.com` into a Web browser, for example, the DNS server translates the host name (`www.guardiandigital.com`) into the IP address associated with `www.guardiandigital.com`. The browser then sends the request to that IP address and responds with the information available at that address.

DNS contains a number of unique characteristics about each host. Each characteristic forms a 'record' in the database that stores the DNS information. DNS "zones" are regions of IP addresses or names for which a particular organization is responsible.

**Address Records** This is a record that provides a host name to be assigned to an IP address. All host names are associated with an IP address.

**Name Server Records** This is a record that defines what name servers are responsible for the zone. In most cases, this will be the same as the host-name of the machine. Do not alter these records unless you have an explicit reason to.

**Name Alias Records** This is a record which provides an "alias" for a pre-existing host name. There may be multiple aliases for a single host name.

**Mail Server Records** This is a record which provides the information necessary to correctly route mail to correctly deliver electronic mail. Multiple e-mail servers may be defined for the same domain, each with a differing priority. Servers defined with a lower number have a higher priority and mail will be delivered to these hosts first.

### Example:

Because we are creating a new domain (`engardelinux.com`), we must create a new forward zone for it. Before EnGarde can be configured to provide DNS for this domain, it must have been listed among the list of authoritative name servers for this domain.

---

From the *System Management* menu, select *DNS Management*. The next step will be to create a new master zone. Click on the *Create a New Master Zone* link.

Leave the *Forward (Names to Addresses)* button checked since that is the type of zone to be created. Keep the default value of *Master server*. The rest the input looks like:

**Domain name:** engardelinux.com

**Email Address:** administrator@engardelinux.com

Leave the *Allow transfers from...* set to *Allow None*, and the *Allow queries from...* set to *Allow Any*. For more information on these fields please refer to the full manual.

Click on the *Create* button to see the new zone in the zone listing. To add the records for our example, click on the *engardelinux.com* link.

### Address Records

**Hostname:** www.engardelinux.com

**Address:** 192.168.1.71

**Hostname:** mail.engardelinux.com

**Address:** 192.168.1.71

### Name Alias Records

**Alias:** sales.engardelinux.com

**Real Name:** www.engardelinux.com

### Mail Server Records

**Mail Server:** mail.engardelinux.com

**Priority:** 10

At this point we have successfully created *www.engardelinux.com* and *mail.engardelinux.com* to go to *192.168.1.71*.

We have now successfully configured the DNS records for our sample domain.

---

## Mail Server

The mail server provides the mechanism to deliver e-mail to a recipient on the Internet. When an e-mail is sent, the mail server is instructed to deliver the message to the remote mail server responsible for the recipient's domain.

### Example:

To configure e-mail for our new domain, we must create a new Mail Domain. From the *System Management* section select *Mail Server Management*. Then select *Domain Management*.

We want to *Create [a] New Domain* with the following values:

**Domain:** engardelinux.com

**Postmaster:** ryan

This assumes that there is a user named *ryan* on the system. Now EnGarde has been configured to receive mail for `engardelinux.com`. The local user *ryan* has been defined as the Postmaster. More information on the "Postmaster" account is available in *Section 4.4.5 Mail Server Management the User Manual*.

Once the mail domain is created, individual user accounts can be added by clicking on the `engardelinux.com` link:

### Example 1:

**E-Mail Username:** administrator

**Recipient:** christi

### Example 2:

**E-Mail Username:** info

**Recipient:** christi

### Example 3:

**E-Mail Username:** webmaster

**Recipient:** ryan



---

#### Example 4:

**E-Mail Username:** sales

**Recipient:** fred@guardiandigital.com

Here four e-mail addresses are defined. The following table shows the destination of various e-mail addresses according to the examples defined above:

Mail Sent To:	Final Recipient:
administrator@engardelinux.com	christi
info@engardelinux.com	christi
webmaster@engardelinux.com	ryan
sales@engardelinux.com	fred@guardiandigital.com
ryan.maple@engardelinux.com	ryan

We have now successfully configured our Mail Server.

## Web Server

The Web Server is the mechanism for serving websites. There are two types of websites: *normal* and *secure*. Secure websites utilize SSL encryption to provide security for sensitive applications such as e-commerce. Normal websites are simply sites that do not utilize SSL.

Secure websites require two things: a certificate and a key. It can be thought of in the following context: the certificate is what verifies your identity (authentication), and the key is what provides the security (encryption). The certificate and key are also tightly tied into each other; they are a matching pair.

The first time a user connects to a secure site, their browser will store the certificate. Every subsequent time the user connects to the site it verifies that the certificate is the same to ensure a secure connection. This provides the encryption portion of the process.

For more information on certificates please refer to the full User Guide.

#### Example:

To configure the Web server for our new domain, we must set them up in the *Virtual Host Management* section.

---

To create the normal site, go to *Virtual Host Management*, and select *Create a Virtual Host*. We use the following values:

**Address:** 192.168.1.71

**Administrator E-Mail:** webmaster@engardelinux.com

**Server Name:** www.engardelinux.com

**Webmaster:** ryan

For *Group*, we want to first *Create [a] Group* named *engardeweb*, and then select it.

**Group:** engardeweb

If a database is necessary for this site, then we check the *Create a database for this site* box and enter in the values:

**Username:** engardeweb

**Password:** e!nga#rde

We have now successfully created the normal website.

Likewise, to create the secure site, go to *Virtual Host Management*, and select *Create an SSL Virtual Host*. We use the following values:

**Address:** 192.168.1.71

**Administrator E-Mail:** webmaster@engardelinux.com

**Server Name:** www.engardelinux.com

**Webmaster:** ryan

**Group:** engardeweb

We have now successfully created the secure website.

Once this is done, the following directories for the normal site will be created:

---

```
/home/httpd/www.engardelinux.com-80/cgi-bin  
/home/httpd/www.engardelinux.com-80/html  
/home/httpd/www.engardelinux.com-80/logs
```

And the following directories for the secure site:

```
/home/httpd/www.engardelinux.com-443/cgi-bin  
/home/httpd/www.engardelinux.com-443/html  
/home/httpd/www.engardelinux.com-443/logs  
/home/httpd/www.engardelinux.com-443/ssl
```

Once the above steps have been completed, EnGarde is ready to serve webpages for the following sites:

```
http://www.engardelinux.com/  
https://www.engardelinux.com/
```

The next step is to populate your sites with content. For more information on this and the many other aspects of the WebTool, please refer to the User Guide.

---

## ENGARDE CONNECTIVITY

So far the only way we spoke of to connect to your EnGarde system was via the GD WebTool utility. To gain remote access you have another secure alternative. We provide SSH connectivity to your EnGarde system.

Since `telnet` is extremely insecure, it is not provided on your secure EnGarde. SSH uses 1024 bit encryption to protect your connection.

Secure Shell (SSH) is a program for logging into a remote machine, as well as for executing commands on a remote machine. It is intended to replace `rlogin` and `rsh`, and provide secure encrypted communications between two untrusted hosts over an insecure network.

SSH connects and logs into the specified hostname. The user must prove his/her identity to the remote machine using one of several methods depending on the protocol version used. For more information on SSH please visit [www.openssh.com](http://www.openssh.com), the OpenSSH Project home page.

---

## CONNECTING FROM WINDOWS 9x/ME/NT/2000

Windows-based systems only include `telnet` capability. Therefore, we have included a utility to make a secure connection to your EnGarde system from a Windows host. MindTerm is a secure SSH client included on your EnGarde CD-ROM that was shipped with your EnGarde system. It can be found in the `x:\dosutils\mindterm` directory. Replace the "x", in the previous statement with the drive letter of your CD-ROM drive. Installation instructions are in the next section.

MindTerm provides you the ability to make an SSH connection to your EnGarde system. You will be on a secure, 1024 bit encrypted connection. MindTerm performs X-Term emulation. You also have SCP capabilities which allows you to copy files securely over an SSH connection. SCP will be fully explained in the *Menus* section.

### Installing MindTerm

We have included an installer for Windows based systems to use. You can find the installer in `x:/dosutils/mindterm/setup.exe`. You can type in the command by clicking the *Start* button, then selecting *Run*. You can also click on *My Computer*, select you CD-ROM drive, then the *dosutils* folder, followed by the *mindterm* folder and finally selecting the `setup.exe` file. This will start the MindTerm installer.

Once the installer starts, you will have a few options. You will have to choose the directory you wish to install MindTerm into. The default is `c:\Program Files\mindterm`. We suggest leaving the default. You can then select the installer to create an icon on your desktop for MindTerm and/or an icon in your Start Menu. These are both turned on by default.

Once you have made your selection, select *Install*, which will confirm your selections. If you are satisfied with your settings select *Ok* and MindTerm will start installing. You will see all the MindTerm files scrolling in the window as they are installed. When the installation is done a message box will appear saying: "*MindTerm installation successful!*". You can close this box and now use MindTerm. If you selected the option to install the icon on your desktop you will see it there. If you also had the installer create the Start Menu icon you will find *Start Menu->Programs->MindTerm->MindTerm* and *Readme*. The *readme* is detailed information about MindTerm and how to use it. We will be covering a general usage of MindTerm in the next section.

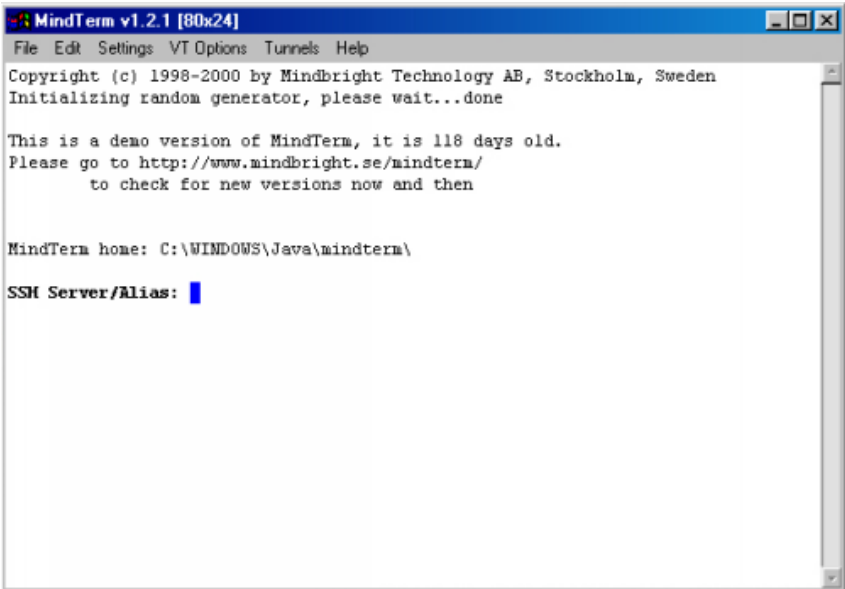
---

**NOTE:** MindTerm is distributed free. There are other programs for Windows such as TeraTerm and Secure-CRT that will also work with your EnGarde system.

## Running MindTerm

MindTerm uses a public/private key cryptography system to connect to your EnGarde system. A public key is a key the user is assigned that can be given out to anyone. At the same time they are also given a private key that no one can have. The public key is then checked against the private key for authenticity. In the case of EnGarde Secure Linux they private key is stored on EnGarde and MindTerm passes the public key to EnGarde for authenticity.

You can start up MindTerm by either double clicking on the MindTerm desktop icon or choosing it from the Start Menu, *Start->Programs->Mindterm->Mindterm*. After a few moments you will be displayed with the MindTerm screen.



When you started up MindTerm you may have noticed a MS-DOS Prompt window appear and it may be located behind your MindTerm window. You may

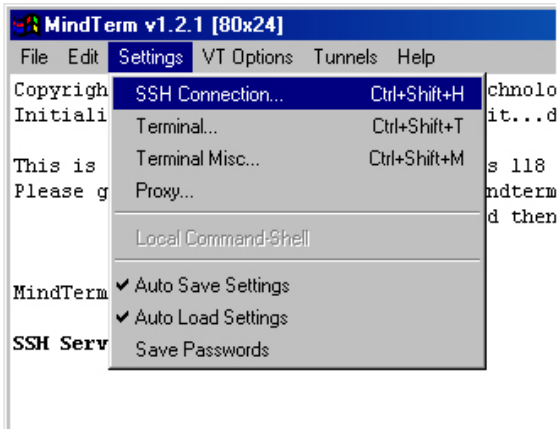
---

minimize this window but do not close it. The MS-DOS Prompt window will close when you shutdown MindTerm.

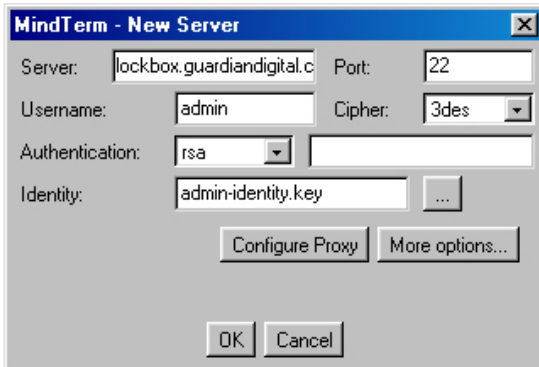
At this point you will need to set up MindTerm so that it knows where to connect to, who you are and what key to use. First you must have a valid user on the system you are trying to connect to. If you do not have a user, are uncertain of the user name or forgot your password then contact your system administrator. To view and/or modify any of the information mentioned please refer to *Section 4.4.1, User Account Administration*.

You are also required to have a key for the system. The key provides the encrypted information MindTerm requires including your password, to authorize you to connect to the remote host. When your account was created by the system administrator, a key should have been given to you. If you do not have this key please contact your system administrator. To generate a new key refer to *Section 4.4.4 Secure Shell Management*.

To enter this information into MindTerm select *Setting->SSH Connection...*



This will pop up a window labeled “MindTerm - New Server”. Here you will need to enter in the information mentioned above. Each field will be described below.



**Server** In this field you will need to enter in either the IP address or the name of the server you are trying to connect to. In our example above we want to connect to `lockbox.guardiandigital.com`. So `lockbox.guardiandigital.com` was entered in to the server field.

**Port** This field should be preset to port 22, the default SSH port. We suggest leaving this as is.

**Username** Here you will need to enter in the user name your system administrator has given you for the server. In our example we are trying to login as user *admin*. This user name will automatically be passed to MindTerm. So you will only need to supply a password when you login. *admin* was entered in to the field.

**Cipher** In this field you will have a pull-down menu giving you a selection of different cipher methods. A cipher is a method of encrypting plain text information into encrypted information. There are several different methods. By default EnGarde is set to use *3DES*. Check with your system administrator to see if they have changed the cipher.

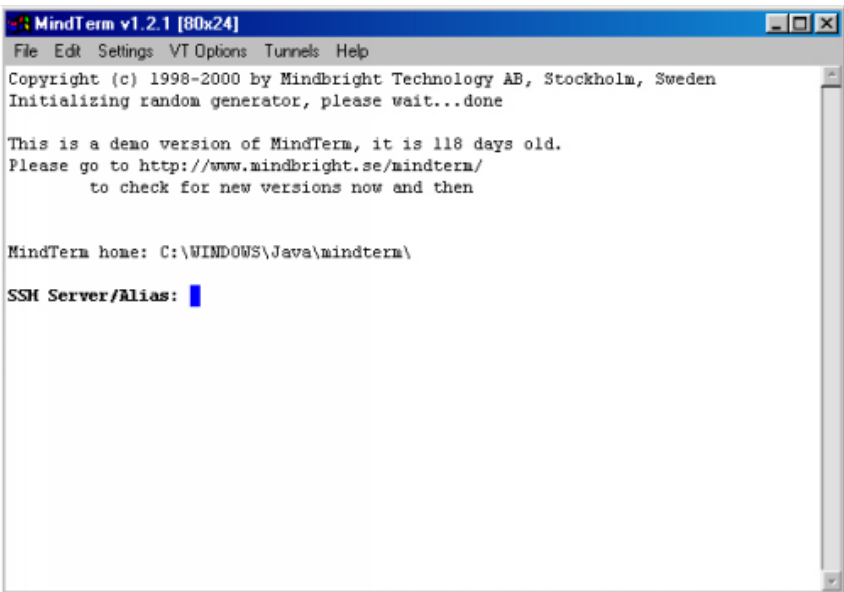
**Authentication** Here you will need to select your authentication type. The authentication type is the method that will be used to authenticate you when you log in. By default *RSA* is used. *RSA* uses a public and private key scheme. When your account was created, you should have been given a key to be used with the server. Forms of authentication other than *RSA* are not supported on EnGarde.



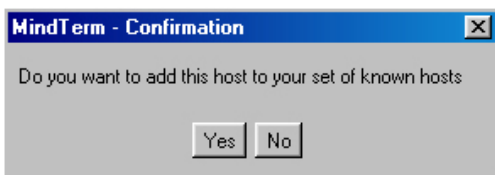
---

**Identity** Here is where you will enter in the path to your key. By default MindTerm will search in `c:\windows\Java\mindterm` for keys. It would be appropriate to place your key in this directory when it is given to you by your system administrator. You can use the “...” button to browse through other directories on your local machine. A key will generally end with `.key`.

Once all the information has been filled in you, can select the *OK* button to continue. You will be brought back to the screen you began on.

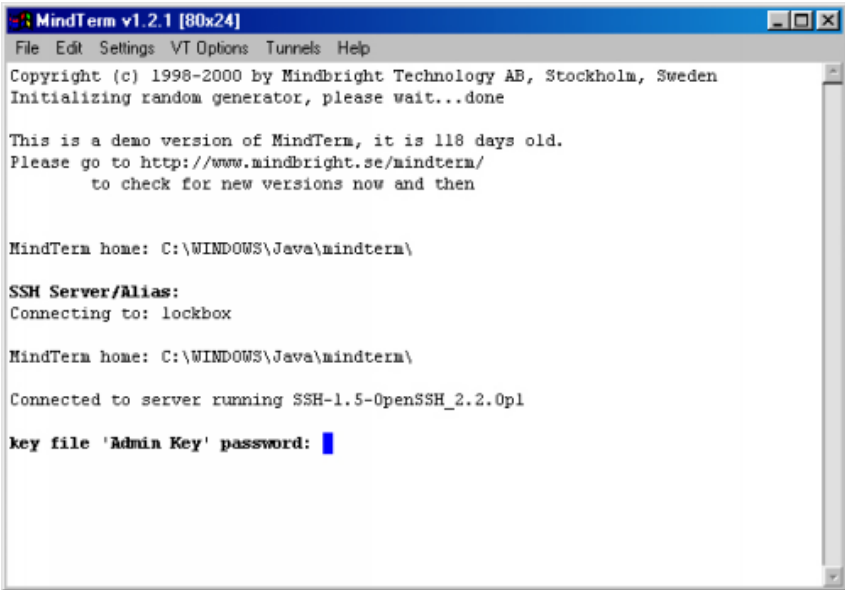


Once you click the *OK* button MindTerm will attempt to make a connection. If you have never connected to the server before you will be asked if you want to add the host to your host key list. Answer *Yes* to this question.



---

Once the dialog box is removed, if the connection was successful you will be prompted for your password.

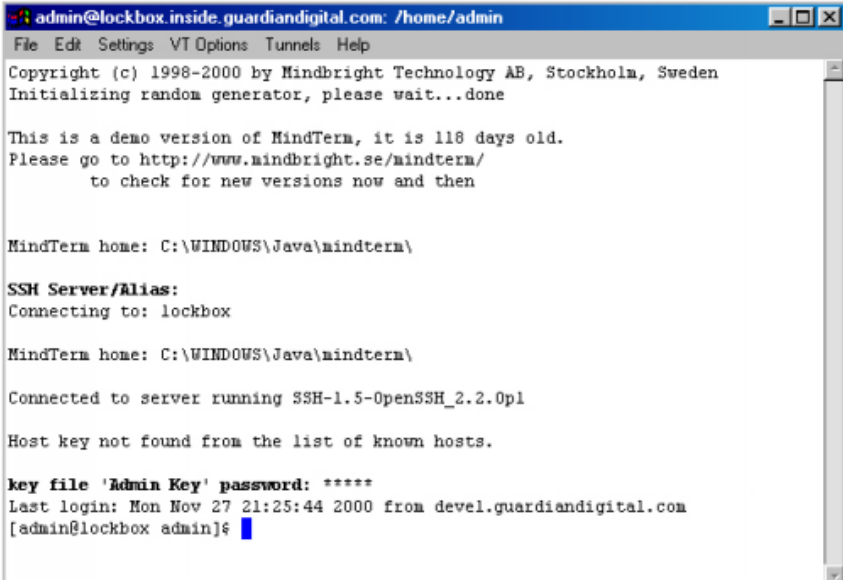


If you do not have the above screen then you most likely received an error. A couple of common errors are:

**Unknown Host:** You will receive this error if the name or IP address of the host was not found or is not responding. Check what you entered in the *SSH Options* screen above.

**Server refused our key** You will receive this error if the key you are using does not correspond to the key on the server. This can be caused if the key on the server has changed, you are pointing MindTerm to the wrong key, or your key is invalid. Double check your settings in the *SSH Options*. If you are certain you are passing the correct key, then a new key may have to be generated. Contact your system administrator if this is the case.

At the password prompt displayed above, enter in your password that was assigned to you by your system administrator. If you entered in the password correctly you will now be logged into the system.



```
admin@lockbox inside.guardiandigital.com: /home/admin
File Edit Settings VT Options Tunnels Help
Copyright (c) 1998-2000 by Mindbright Technology AB, Stockholm, Sweden
Initializing random generator, please wait...done

This is a demo version of MindTerm, it is 118 days old.
Please go to http://www.mindbright.se/mindterm/
to check for new versions now and then

MindTerm home: C:\WINDOWS\Java\mindterm\

SSH Server/Alias:
Connecting to: lockbox

MindTerm home: C:\WINDOWS\Java\mindterm\

Connected to server running SSH-1.5-OpenSSH_2.2.0pl

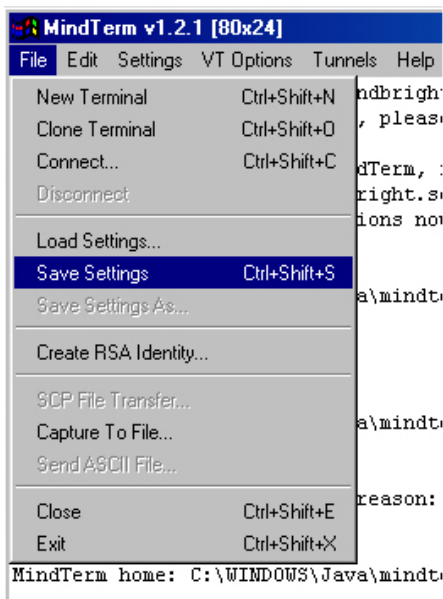
Host key not found from the list of known hosts.

key file 'Admin Key' password: *****
Last login: Mon Nov 27 21:25:44 2000 from devel.guardiandigital.com
[admin@lockbox admin]$
```

At this point you are ready to interact with the system.

By default you will be using a Bash shell interface. Brief information concerning how to use the Bash shell can be found in *Appendix C* of the *User Manual*. There are also numerous books, on-line guides and tutorials concerning Bash usage.

Now would probably be a good time to save your settings. Saving your settings allows MindTerm to store the information you entered into the *SSH Connection...* dialog so you don't have to re-enter the data in every time.



To save your settings select *File->Save Settings*.

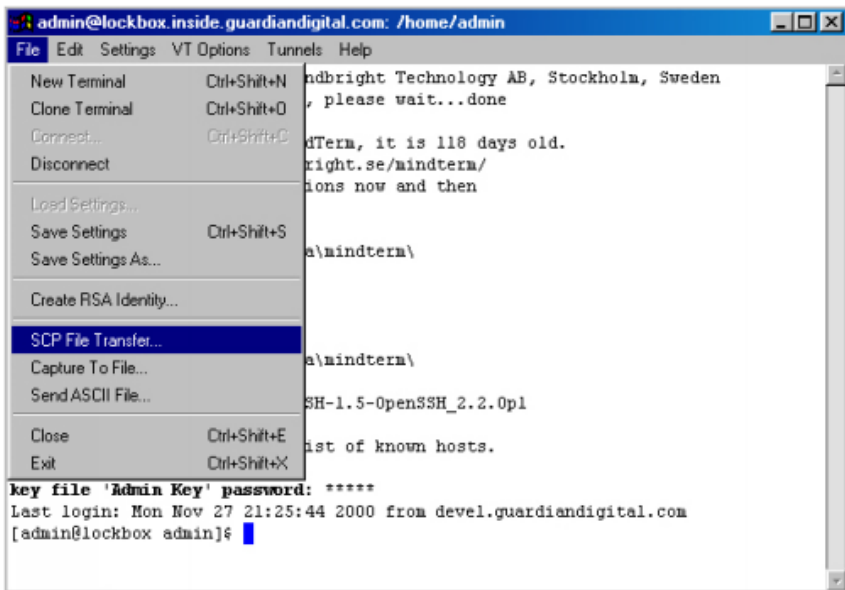
To exit the system type *exit*. You will be brought back to the SSH *Server / Alias :* prompt. At this point you can shutdown MindTerm by clicking the 'X' in the corner or from the menu, *File->Exit*.

It is highly recommended that you log out of the server using the *Exit* command before shutting down MindTerm so you are properly logged out.

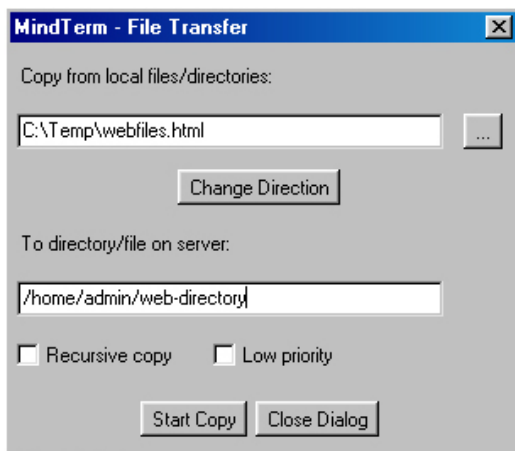
## Secure Copy (SCP)

The Secure Copy (SCP) is a method of copying files over a secured SSH connection. MindTerm supports SCP.

To copy files to and from the server via SCP you will first need to be logged into the system. Read the section above on logging in with MindTerm. You will then have the ability to SCP by selecting *File->SCP File Transfer...*



Selecting the *SCP File Transfer...* option will bring you to the following screen:



Here you can select files and directories to copy to and from. Wildcards are also accepted here.

You have a few options on this screen. The *Change Direction* button will change

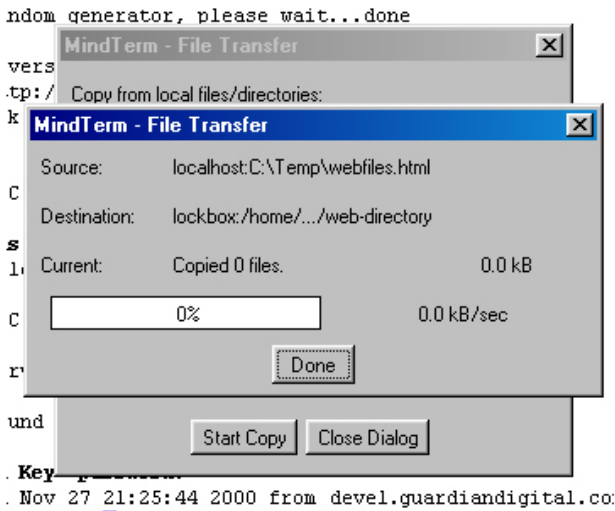
---

whether you are copying files from your local machine to the server, or copying files from the server to your local machine. Clicking on the button will reverse this each time.

You will also notice there is a check-box for *Recursive copy*. This will allow you to enter in a directory in the field you are copying from and it will automatically copy everything in that directory and every directory below it.

Finally you have one last option, *Low priority*. Selecting this will allow the SCP file transfer to take place in the background so you can work while it's copying. It will take longer to copy files using this method but it will also free system resources and bandwidth.

When you are ready to start copying files you can click the *Start Copy* button. MindTerm will then make an SCP connection to the server and start copying the files. You will see the following dialog appear giving you the current status on the file transfer.



Once the copy is finished you can click the *Done* button to close the dialog. If you don't need to transfer any more files at the moment you can click the *Close Dialog* button in the *SCP File Transfer* dialog to close it.

You are now done copying your files and now may work with them.

**NOTE:** More information concerning MindTerm can be found in the *User Guide*.

---

## Connecting from Unix

The first thing you will need to connect to your EnGarde system is an SSH client. For Unix there is OpenSSH. You can download OpenSSH from <http://www.guardiandigital.com/tools>. You will also find OpenSSL, as you will need this too. If you wish to download OpenSSL you can find it at <http://www.guardiandigital.com/tools>. A version of OpenSSL and OpenSSH are included on the EnGarde CD-ROM.

If you are using Windows, use the included MindBright MindTerm software. You can find it on the EnGarde CD-ROM under the *dosutils* directory. Instructions on installation and usage can be found in the previous section.

### USING OPENSSSH

The first thing you will have to do is create a user. This is either done by logging in as root at the console and running *adduser* or adding a user from the GD WebTool utility.

If you use the GD WebTool utility to create the user read *Section 4.4.1 User Account Administration* on how to accomplish this.

If you decide to create the user from the console use the following steps:

As the root user run *adduser* by typing *adduser* at the prompt. *adduser* will prompt you for a user name. Enter the user name you wish to give this user.

Once this is done you will be back at the prompt. You now need to give this user a password for them to use to access their account. Type *passwd username*. In place of *username* will be the user name you assigned to the user. This will prompt you for a password and then prompt you again for the password to confirm it.

Once that is done install OpenSSL and OpenSSH on your client machine.

**NOTE:** You must be root during the installation of OpenSSL and OpenSSH.

On distributions using RPM:

```
$ rpm -Uhv openssl-0.9.4_i386.rpm
$ rpm -Uhv openssh-1.2.3_i386.rpm
```

---

In Debian (or any distribution using DPKG):

```
$ dpkg -i openssl-0.9.4.dpkg
$ dpkg -i openssh-1.2.3.dpkg
```

And from tar files:

```
$ tar zxvf openssl-0.9.4.tgz
$ tar zxvf openssh-1.2.3.tgz
$ cd openssl-0.9.4
$ ./configure
$ make
$ make install
$ cd ../openssh-1.2.3
$ ./configure
$ make
$ make install
```

You now must create a key for yourself. You can create a key with OpenSSH by typing:

```
$ ssh-keygen
Generating RSA keys: .....oooooooo0.....oooooooo0
Key generation complete.
Enter file in which to save the key (/home/nick/.ssh/identity):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

It will prompt you for a filename to save the key in. The default `identity.pub` will be fine. It will then prompt you for a new passphrase. After entering your passphrase twice, your public key will then be generated.

Once you have your key e-mail it to your system administrator and they will insert it in to the system properly. Read *Section 4.4.4 Secure Shell Management* for more information. Once this has been completed you will be able to successfully SSH in to the system.

For more information on SSH and using SSH please read the SSH FAQ which can be found at:

<http://www.linuxsecurity.com/docs>



---

## ACCEPTING AN UNSIGNED CERTIFICATE

During the initial login during the configuration of your EnGarde system and/or when connecting to the GD WebTool you will be prompted with the following screen:



Your browser will ask you if you want to accept the certificate attached to your EnGarde system. The reason for this is Guardian Digital has signed the certificate and is not a Certificate Authority (CA) such as Verisign and Thawte. Having this certificate signed by a CA is not necessary since you can verify that you are connecting to your own EnGarde system.

So you will want to accept this certificate. Click the *Next* button to continue.



This next screen will display brief information concerning the certificate. There is a button you can click, *More Infor...* for detailed information concerning the certificate. Click *Next* to continue.



Now you will be asked in what way you want to accept this certificate. You have three options here. The first option will only accept the certificate for the current session. So when you shut your browser down you will be prompted with the same screens the next time you try to login to the GD WebTool.

The second option will tell your browser to never accept the certificate. This will lock you out of GD WebTool.

Finally the third option will accept the certificate until it expires. When it expires and a new certificate is put in it's place you will be prompted again with these same menus.

If you will be doing your administration via the GD WebTool on the current machine it is recommended you select *Accept this certificate forever (until it expires)* option. Once you have made your decision select the *Next* button.



This fourth screen will inform you of the possibility of fraud and insecurity when using an unsigned certificate. Since you know EnGarde and certificate both came from Guardian Digital you can be certain your connection and data will be secure.



This is the final step and will inform you of your decision to accept the certificate and verify your options. Click *Finish* to fully accept the certificate and enter the GD WebTool.

---