Installation of CentOS 6 for Tenable SecurityCenter Evaluation

These instructions are for the installation of CentOS 6 in preparation for installing Tenable SecurityCenter 4.4 for evaluation purposes. They are not a replacement for CentOS documentation and/or a skilled CentOS professional to perform a production installation of Tenable Network Security software running on CentOS 6. Tenable Network Security provides these procedures as suggested procedures and does not warrant that the instructions are complete and/or correct.

UNDER NO CIRCUMSTANCES WILL TENABLE BE LIABLE TO YOU OR ANY OTHER PERSON OR ENTITY FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES (INCLUDING LOST PROFITS, ANY DAMAGES RESULTING FROM LOSS OF DATA, SECURITY BREACH, PROPERTY DAMAGE, LOSS OF REVENUE, LOSS OF BUSINESS OR LOST SAVINGS), ARISING OUT OF OR IN CONNECTION WITH THESE INSTRUCTIONS, THE PERFORMANCE OF THE SOFTWARE OR TENABLE'S PERFORMANCE OF SERVICES OR OF ANY OTHER OBLIGATIONS RELATING TO THESE INSTRUCTIONS, WHETHER OR NOT TENABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY, AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON.

The instructions are for installing on a 32-bit i386 networked or standalone host, with or without access to the Internet, that can be dedicated to an evaluation of SecurityCenter and whose single hard drive can be wiped clean by a new operating system installation. Please note that if the host does not have access to the Internet these instructions do not cover manually patching and updating CentOS 6 and your installation is unlikely to be up to date with the latest CentOS 6 software revisions.

These instructions will also work on 64-bit x86_64 systems by simply changing references from i386 architecture to x86_64 architecture.

1. Install CentOS 6.x

For the evaluation, you will need a version of CentOS 6 so you can download and burn to DVD the bootable installation ISO image. These directions were tested with CentOS version 6.3.

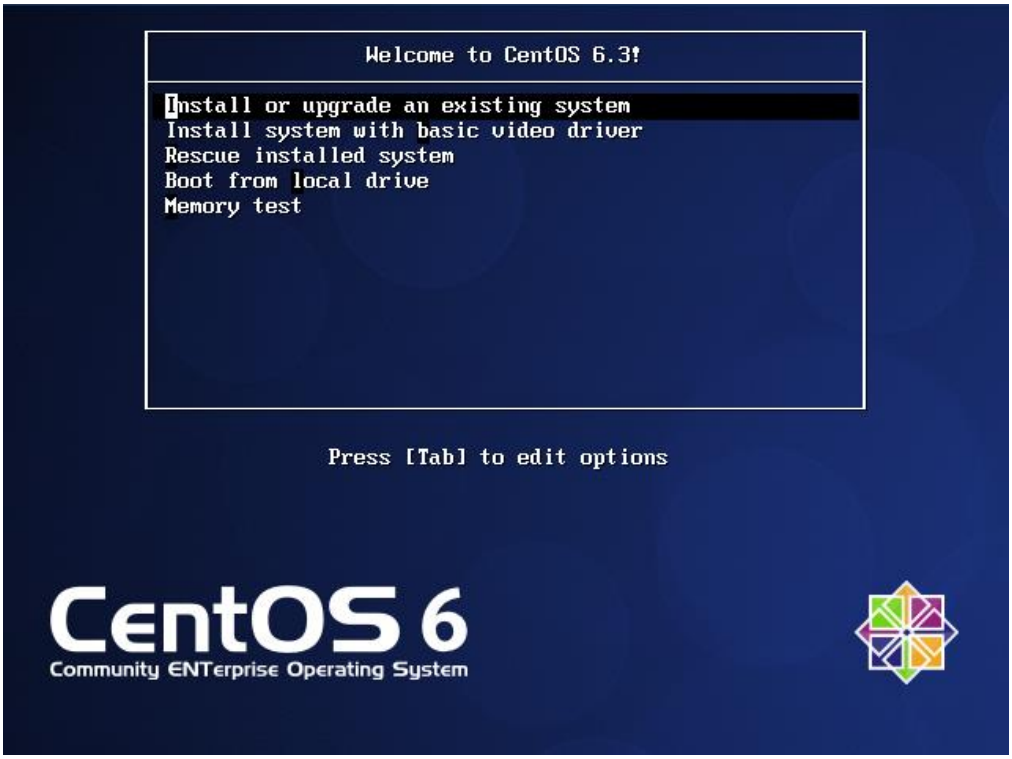
While these instructions are written using a DVD installation, they can be completed with other installation methods. Please note that details for those potential methods are not described as part of this document.

Please note that a production release of Tenable's SecurityCenter 4.4 is only supported on a fully licensed, non-trial version of RHEL with Red Hat Network (RHN) support and software updates or CentOS with the latest patches.

When you are ready to download the ISO from the http://www.centos.org website "downloads" section select a torrent link or mirror site close to you. Choose the CentOS-6.3-i386-bin-DVD1.iso for use with this document. The second DVD image is not needed for these instructions.

If installing on a VMware virtual machine, do not use the "Easy Install" option provided when mounting the DVD ISO image, as it automatically installs additional unnecessary software. Instead choose "I will install the operating system later" and then choose "Customize Hardware" to edit the hardware settings and select the CentOS DVD ISO image.

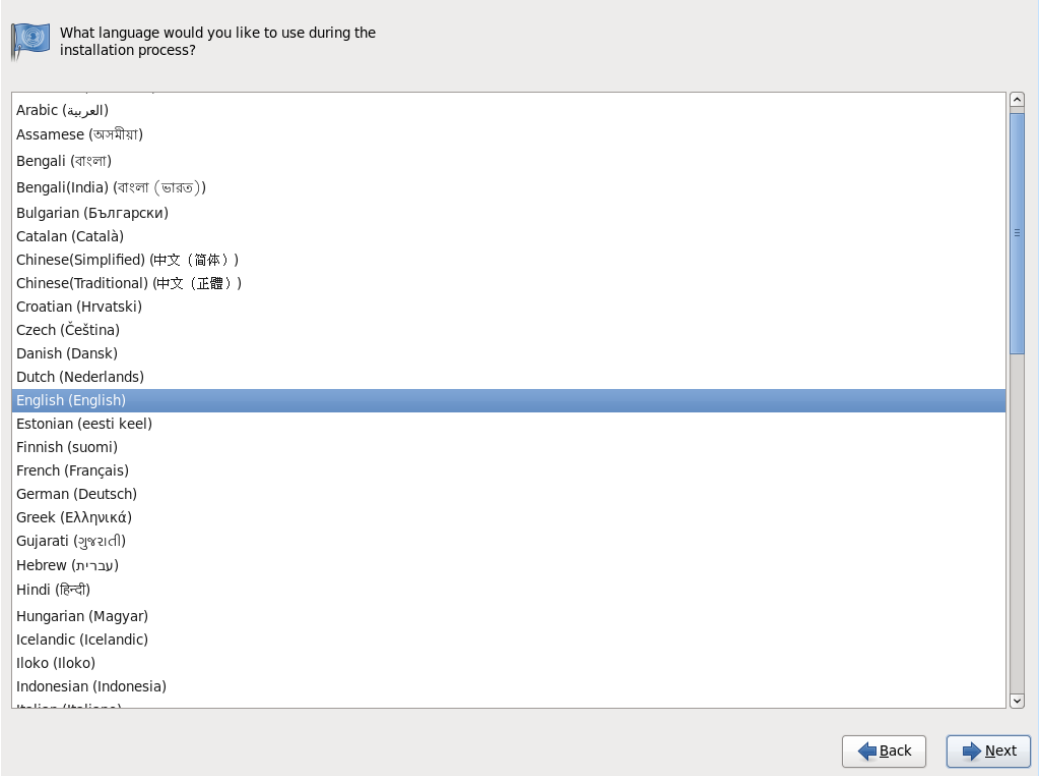
1.1. Insert the CentOS 6 DVD into the DVD-ROM drive and power on the server. At the first installation screen press the "**Enter**" key to select "Install or upgrade an existing system".



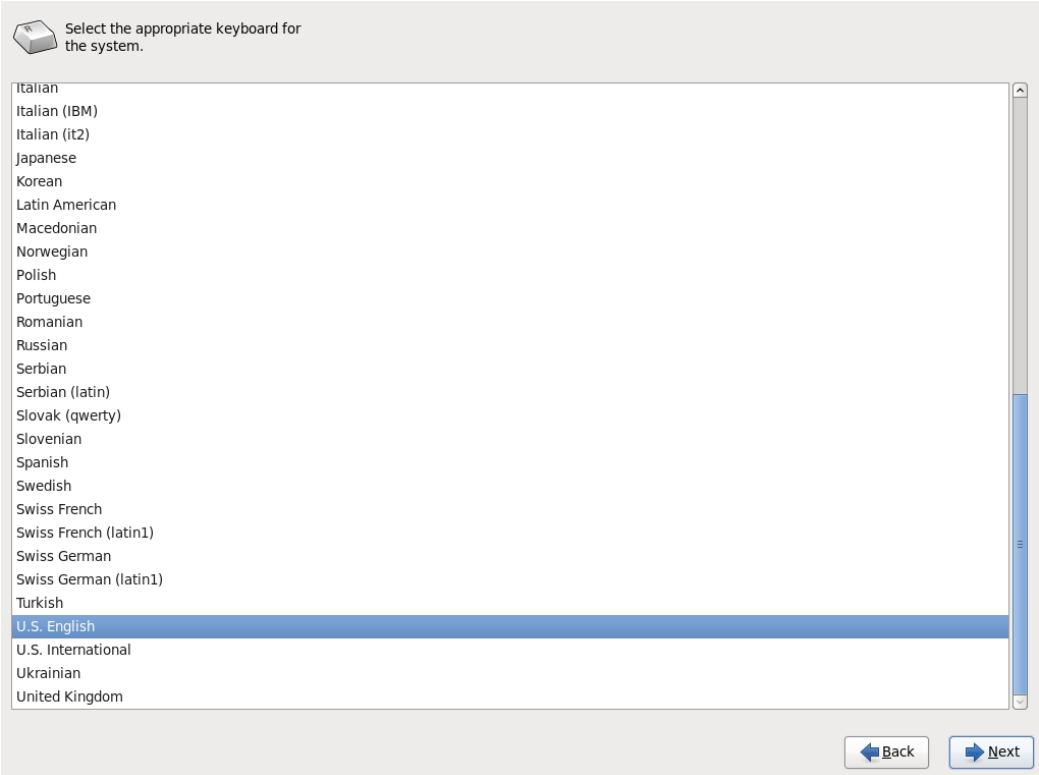
1.2. You can choose to test the installation DVD before beginning installation or skip over the test (e.g., virtual installations from mounted ISO images) by clicking "**Skip**".

1.3. Next, the CentOS 6 installer welcome screen is displayed. Click "**Next**" to proceed.

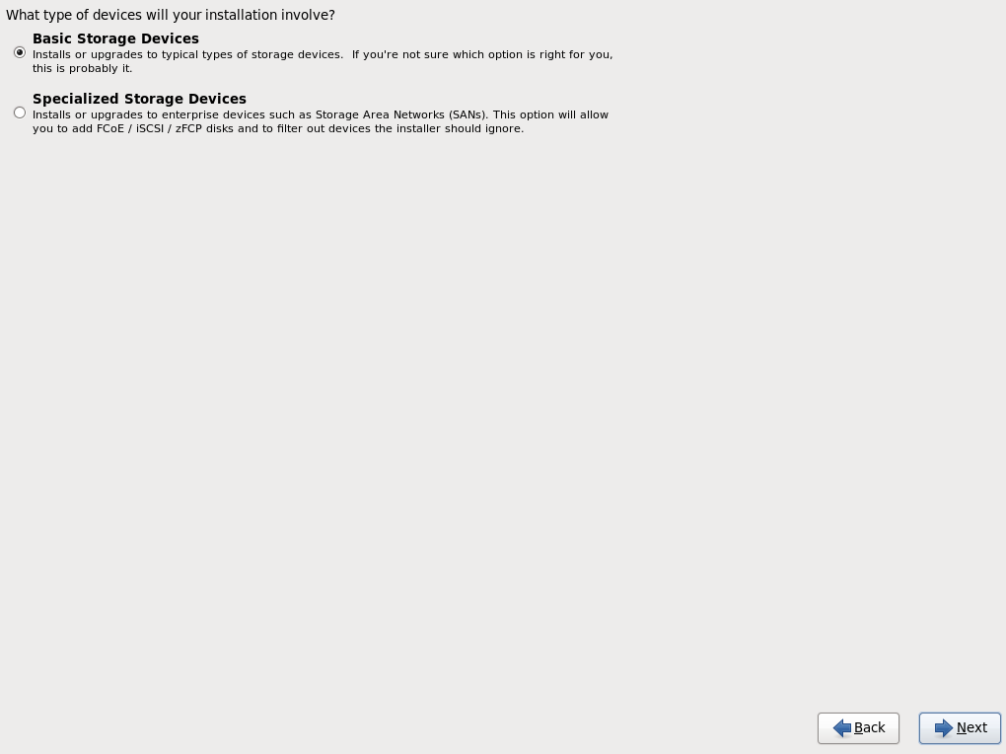
1.4. Choose the desired installation language and click “**Next**”.



1.5. Choose the desired keyboard layout and click “**Next**”.

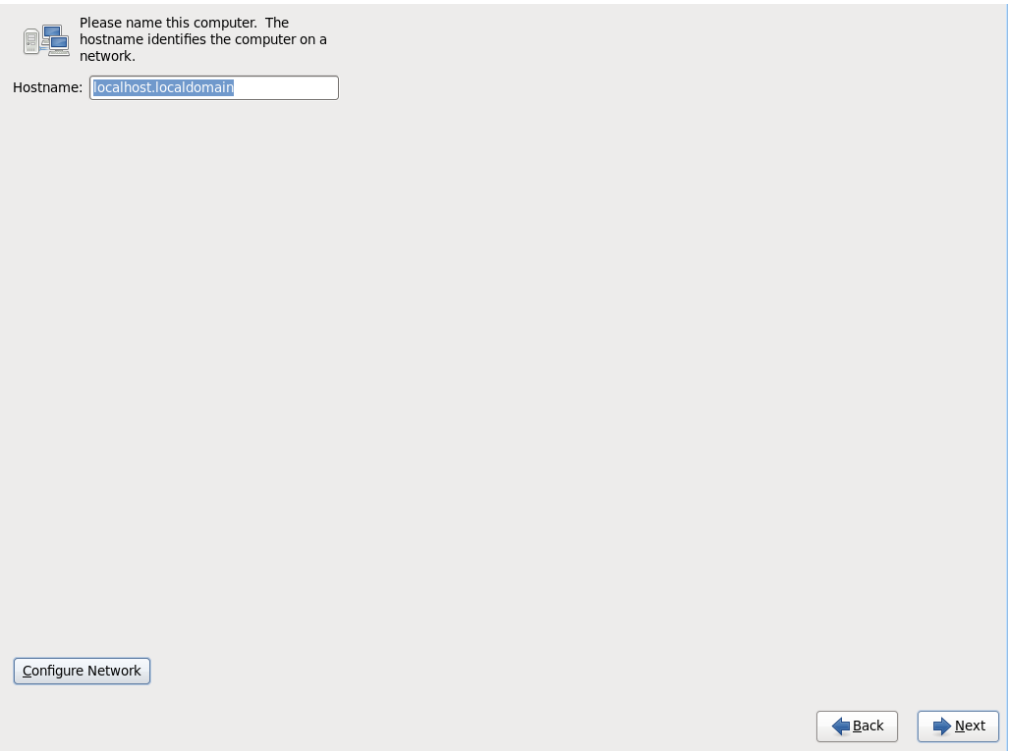


1.6. Select your storage device type. If you are installing to a server with local storage the “Basic Storage Devices” is likely the correct type.

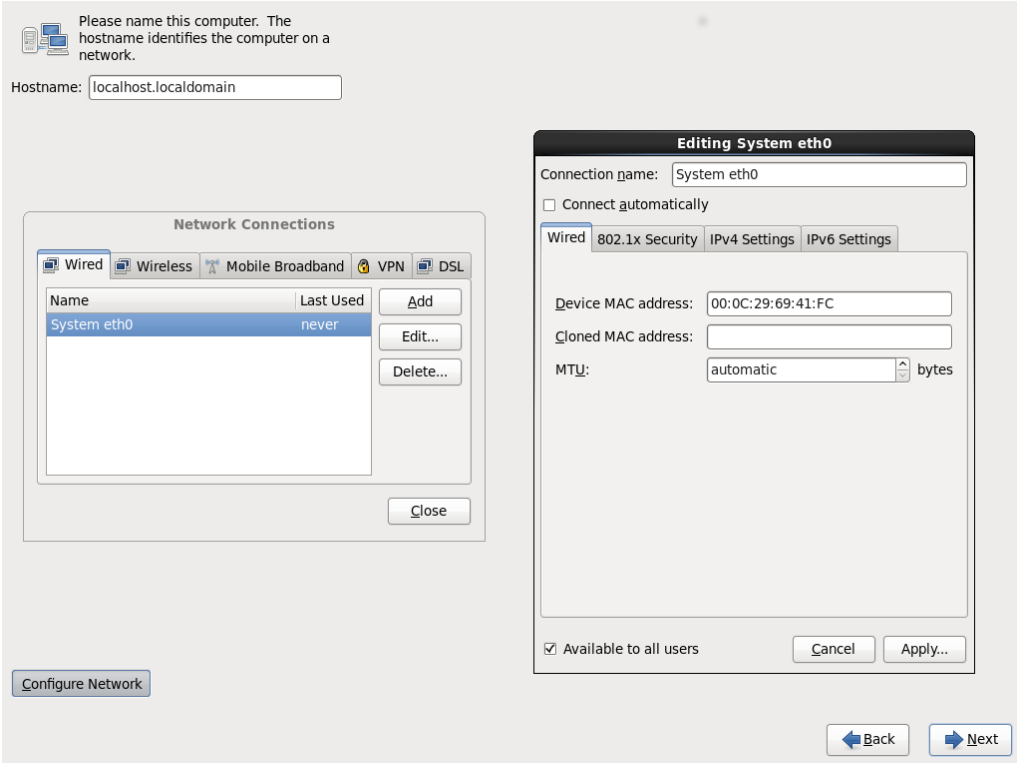


1.7. A storage device warning will be displayed to make it apparent that data will be lost if it contains existing partitions. This guide assumes that the server does not contain any data that needs to be preserved. Select “Yes, discard any data” to allow the installer to initialize the drive.

1.8. Information about the local network may be entered with options from this screen. Enter the hostname for the server (and ensure it is the same one assigned to your SecurityCenter trial key). If this is a simple one NIC server using DHCP, ensure the network cable is plugged into the NIC and accept the defaults.

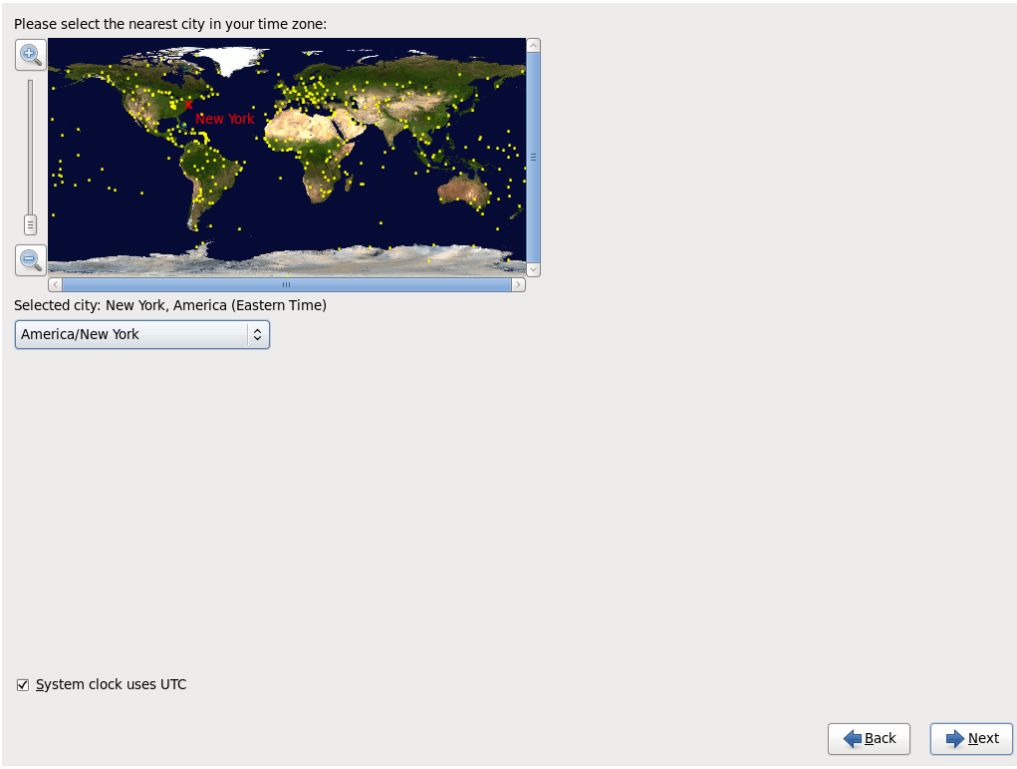


In some system configurations the networking device may not be set to start automatically. To check this, click the “Configure Network” button. On the resulting window select the network interface that will be used and click the “Edit” button. Then ensure the “Connect automatically” check box is selected.

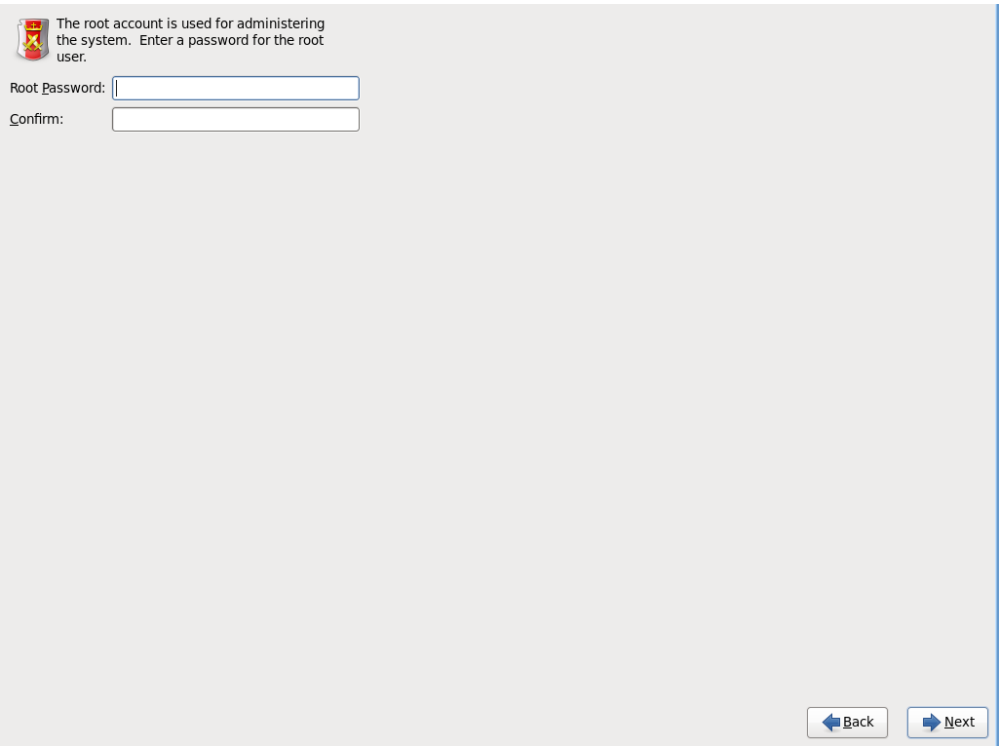


Adjust the steps accordingly based on the available network settings and click "**Next**".

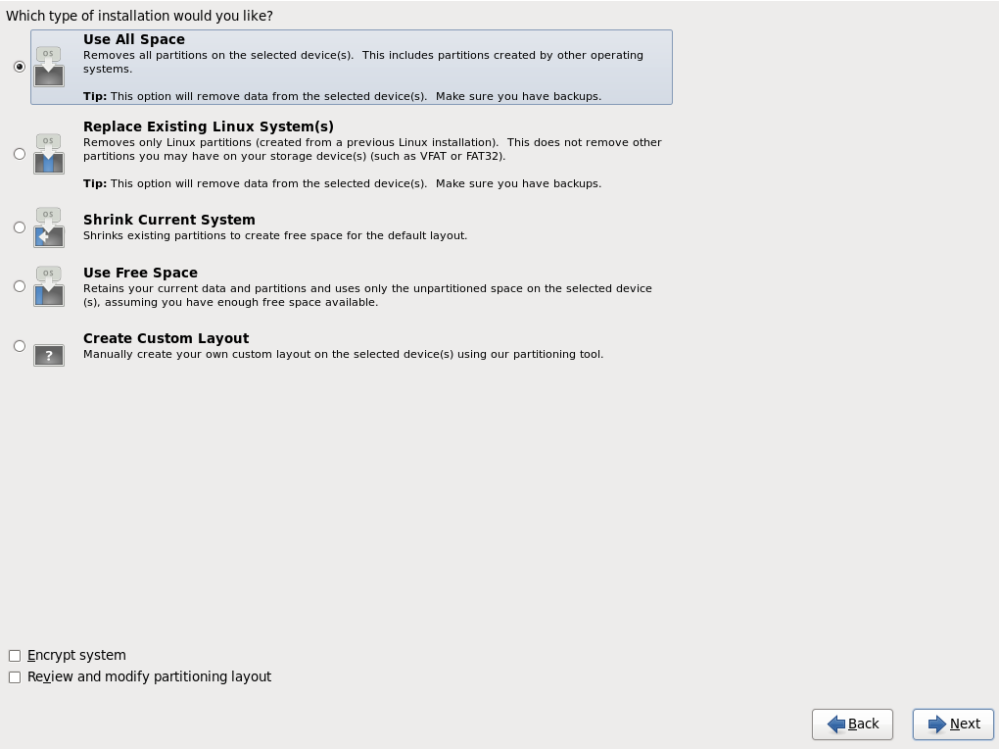
1.9. Select the correct region for the server's time zone and check the box for "System clock uses UTC" if it is true.



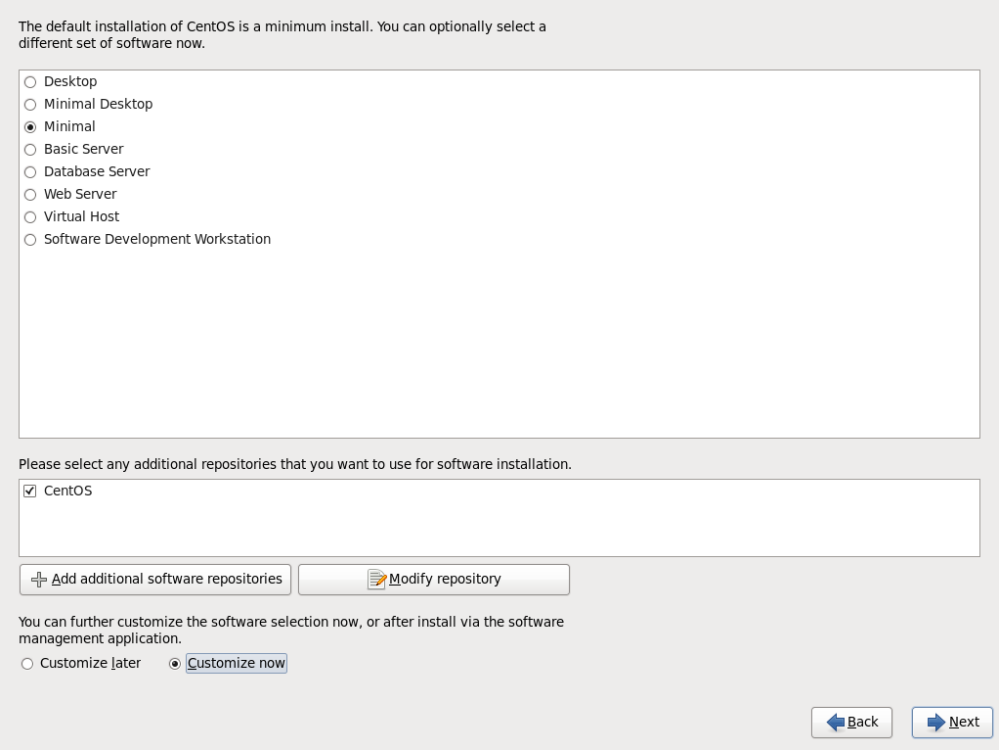
1.10. Set the root user password and click “**Next**”.



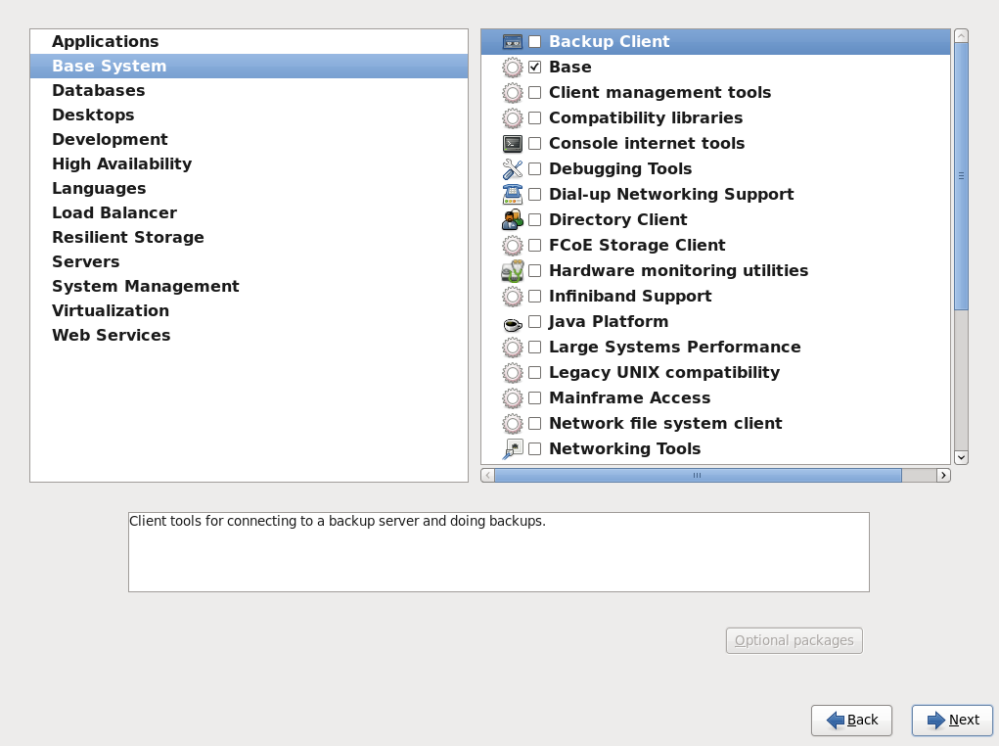
1.11. Select the type of installation to be performed. As this guide assumes a dedicated server, select “Use All Space” and click “Next”. The installer will prompt for a confirmation to write the changes to disk.



1.12. Select the installation type of “Minimal” and “Customize Now” to make appropriate selections for the installation. Leave “CentOS” as the only selected repository. Click “**Next**”.

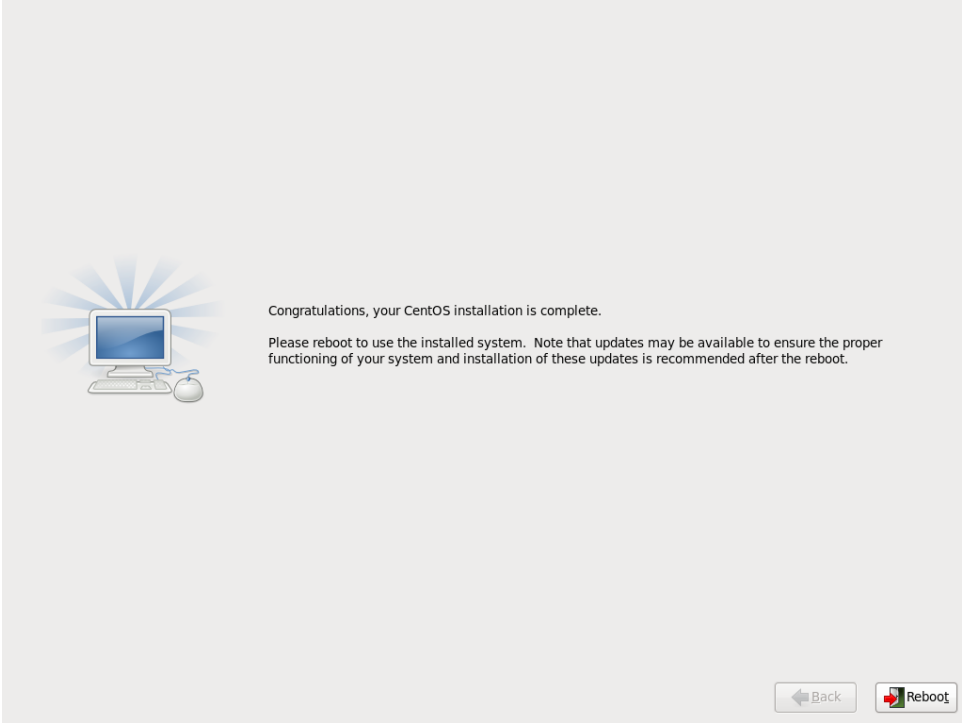


1.13. Ensure that under “Base System” that only the “Base” option is selected. Click “**Next**” to continue.



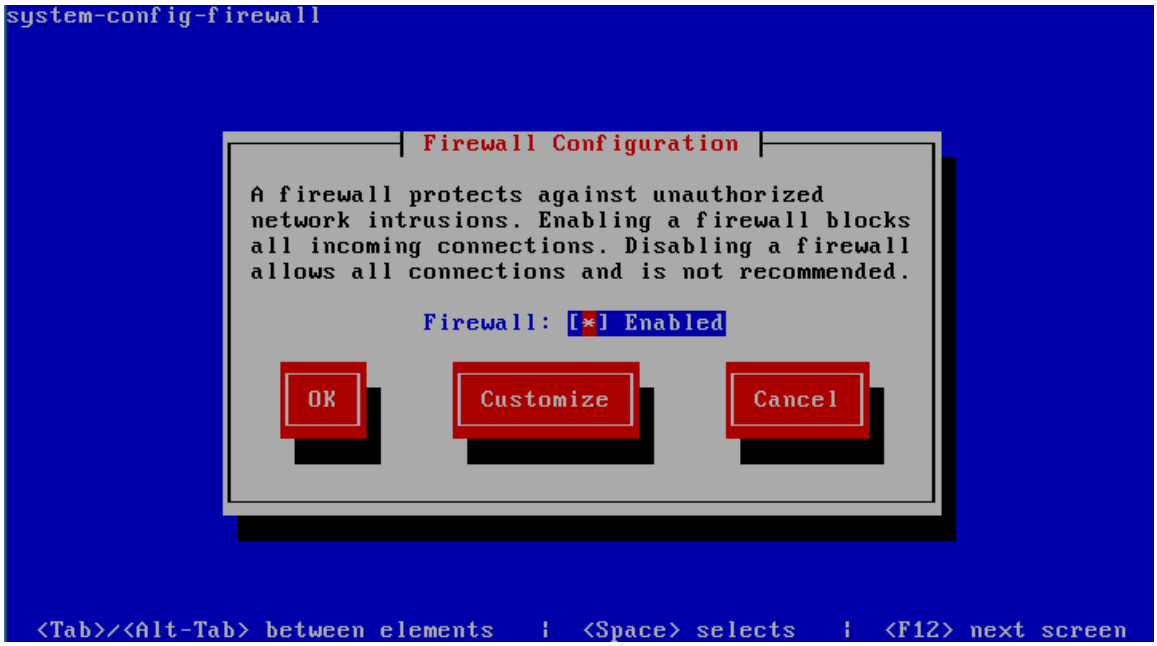
1.14. When the installer has finished checking dependencies, the installation process will begin automatically. The installer will format the disk and install the required packages from the installation media.

1.15. At the successful installation confirmation screen take the media out of the DVD-ROM drive and then click "**Reboot**".

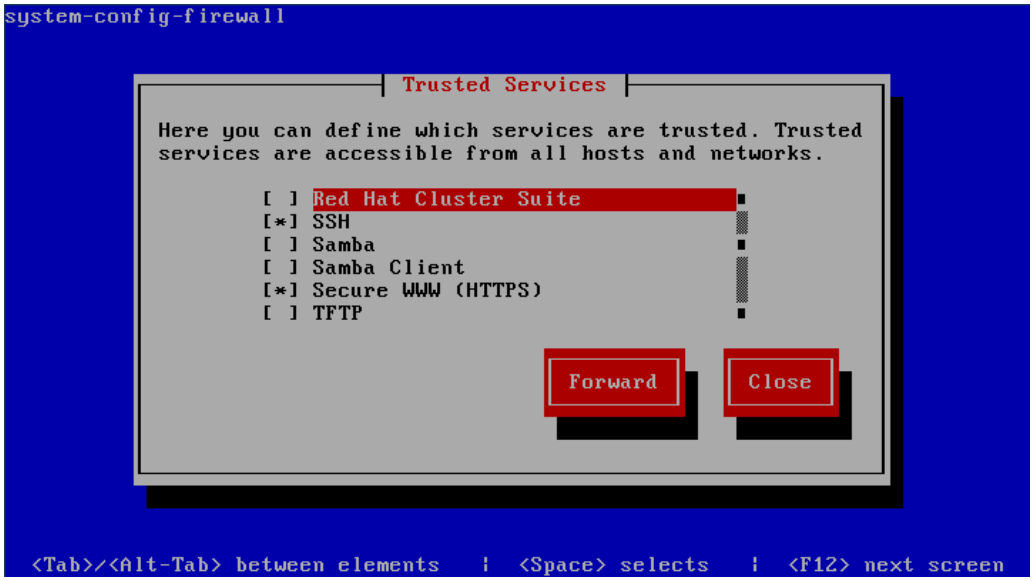


1.16. Do not interfere with the system reboot.

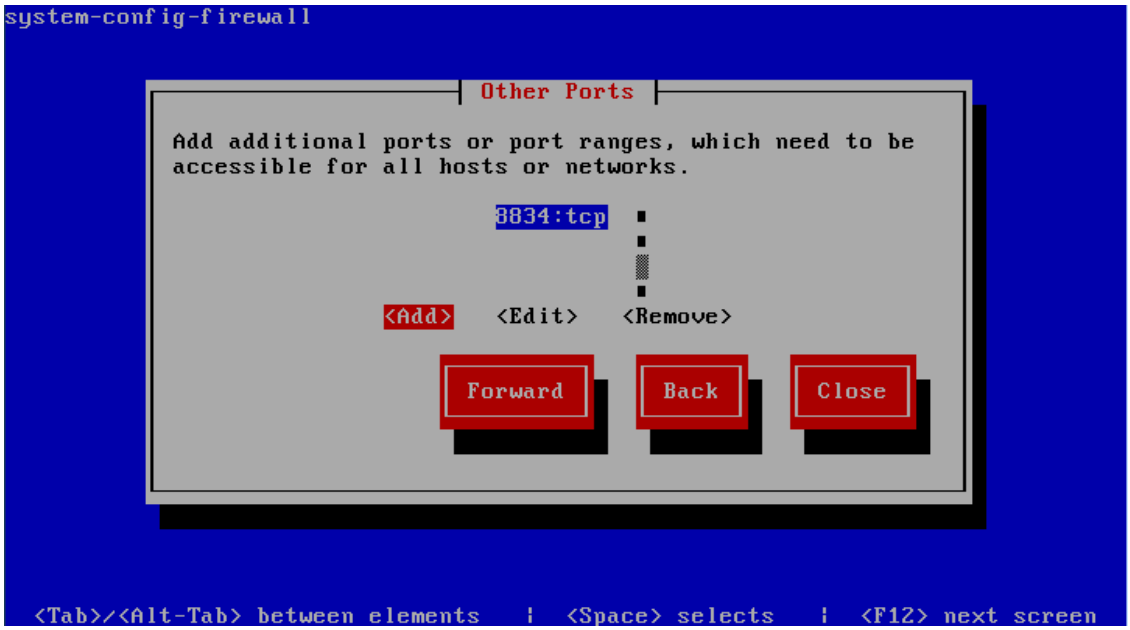
1.17. Run the Firewall configuration tool after logging on as root with the password used in step 1.10 and entering "**`/usr/bin/system-config-firewall-tui`**" or "**`/usr/bin/setup`**" at the command line. It is very important before installing SecurityCenter that SELinux and the firewall are configured correctly.

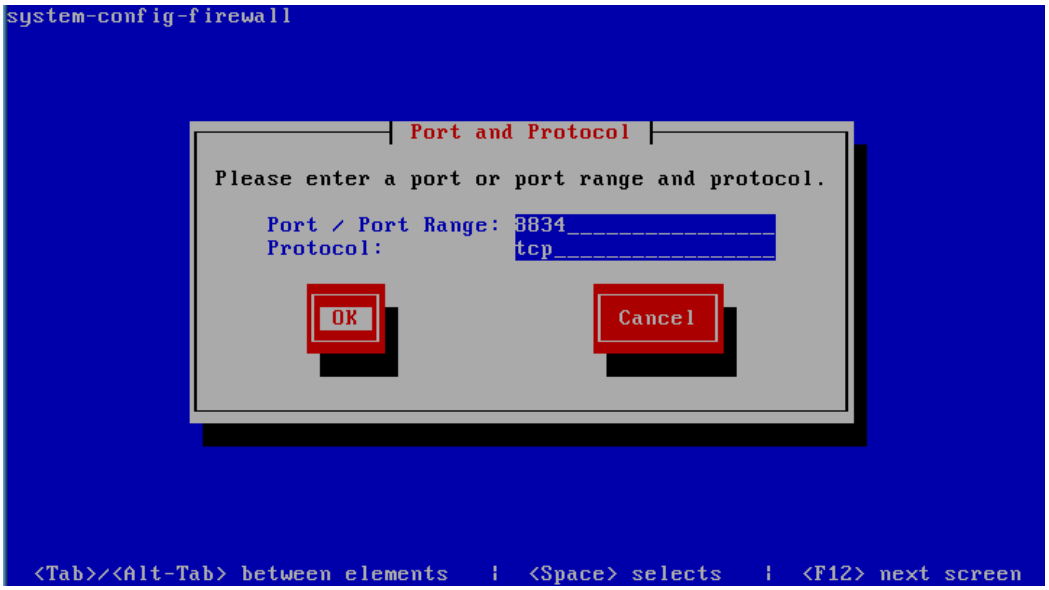


1.18. Select “Customize” from the available options. Define the trusted services from the list. SSH is selected by default and is recommended for remote access. Secure WWW (HTTPS) must be selected. Click “Forward” after the selections have been set.



1.19. If Nessus will be used on the system, select “add” to add a custom port and protocol to the Trusted Services. Set 8834 as the port and tcp as the protocol. Click Forward to continue.



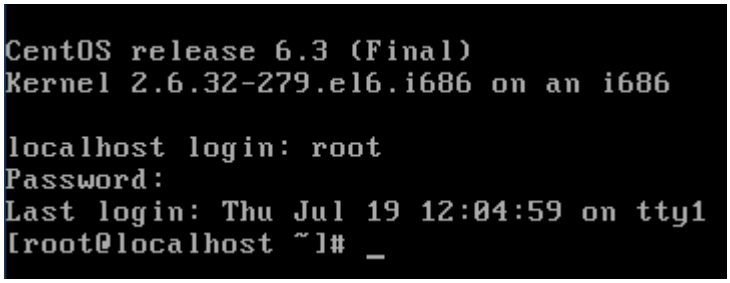


1.20. If needed in your environment, select a trusted interface, masqueraded interface, port forwarding entries, ICMP filters, and Custom Rules to allow settings other than the defaults for your environment. Select Close then OK at the end of the configuration process.

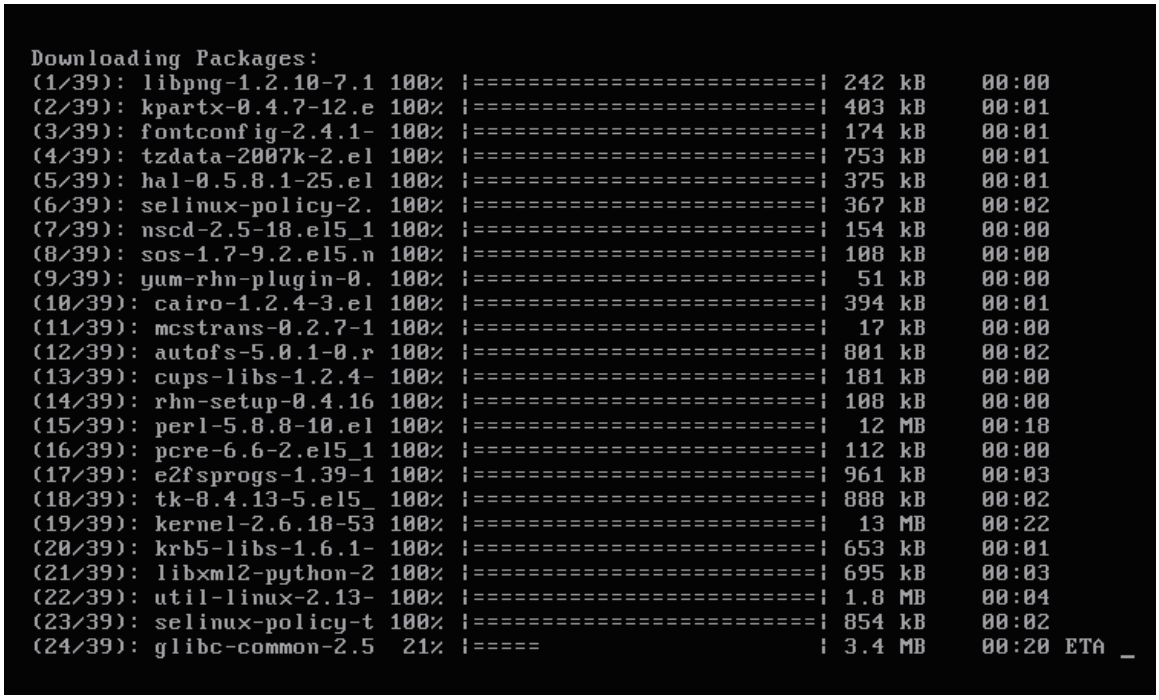
1.21. Switch SELinux to “Permissive” from “Enforcing” by editing the file **`/etc/selinux/config`** and changing the SELINUX=enforcing line to SELINUX=permissive and reboot the system for the new setting to take effect.

Optionally, disable SELinux altogether where the evaluation system will be in a protected environment and intrusion logging is not required.

1.22. The reboot will complete. Sign on to the CentOS 6 host as root using the password you set during the installation in step 1.10.



1.23. Run "**`yum -y update`**" to ensure all the installation packages are up to date on your CentOS 6 host.



1.24. Run "**`yum`**" to install the following packages:

- Java Development Kit package or JRE (java-1.6.0-openjdk.i386)
- LibXSLT (libxslt.i386)
- Libtool-ltdl

Install the packages using the following syntax: "**`yum install -y java libxslt libtool-ltdl`**". The command will install the required packages and their dependencies without prompting for confirmation. Omit the "-y" from the command to review the packages that will be installed.

1.25. If your CentOS 6 host is not connected to the Internet, then you will need to download these packages and their dependencies from a CentOS mirror site. If you require assistance, please contact your Tenable Sales Engineer.

Please ensure that NTP is configured properly and that the time is synchronized between this SecurityCenter and any hosts that it will be communicating with.

2. Install Nessus

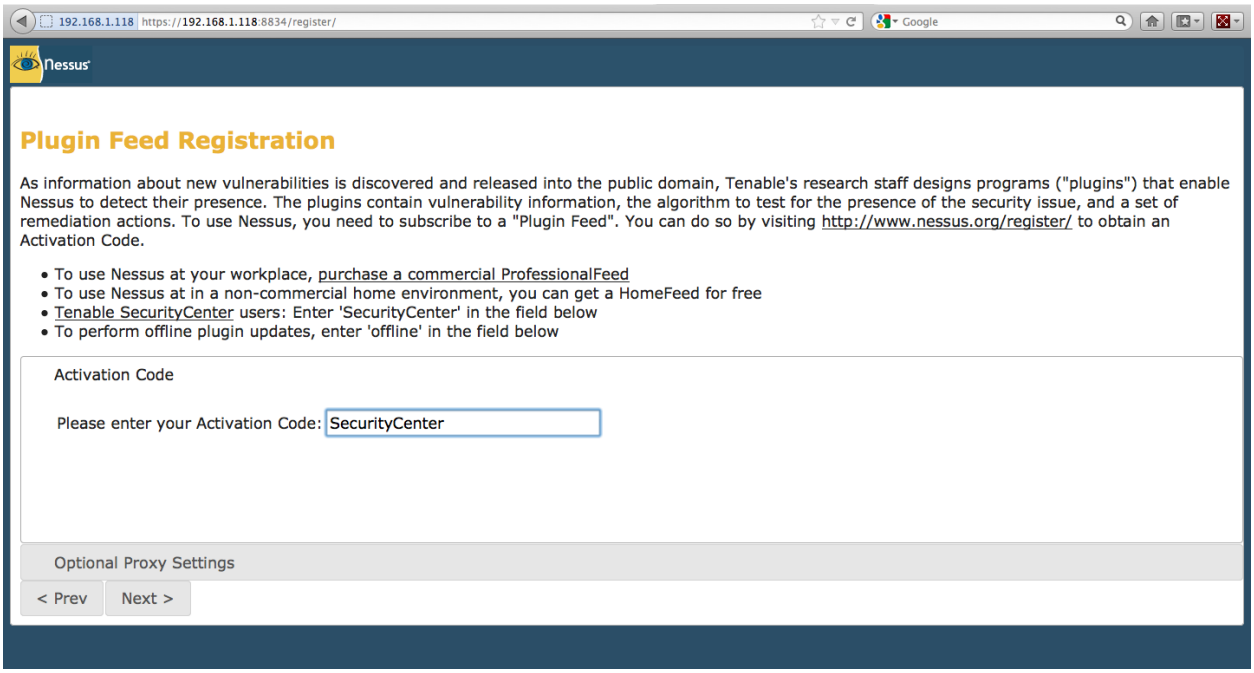
Obtain a copy of the current Nessus RPM for your platform and transfer the Nessus RPM file to the target server.

2.1. SSH to the server, log in as root, change directory to where the Nessus RPM file is located, and then enter the following command (change the command based on the version you have downloaded):

```
# rpm -ivh Nessus-5.X.X-es6.i686.rpm
```

2.2. Start the **nessusd** service with the command "**service nessusd start**" at the command prompt.

2.3. Using a Web browser, navigate to https://<ipaddress>:8834 and complete the installation. When asked for the Plugin Feed Registration, enter SecurityCenter for the Activation Code.



3. Install SecurityCenter

Obtain a copy of the current SecurityCenter RPM package for your platform and transfer the SecurityCenter RPM file to the target server.

SSH to the server, log in as root, change directory to where the SecurityCenter RPM file is located, and then enter the following command (change the command based on the version you have downloaded):

```
# rpm -ivh SecurityCenter-X.X.X-es6.i386.rpm
```

After completion, access the SecurityCenter user interface via a secure browser session:

https://<ipaddress>

Please contact your Sales Engineer for license keys and provide the fully qualified hostname of your newly installed CentOS server as obtained by using the output of the "**hostname**" command.

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CSIS, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com