ThreatQuotient

A Securonix Company

ThreatQ Version 6 RHEL v9 Hardening Guide

Version 2.0.0

October 20, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

About Security Hardening

ThreatQuotient provides steps to assist customers in setting up a hardened Red Hat Enterprise Linux (RHEL) 9.4 and 9.6 environments according to one of the supported CIS or DISA hardening standards below prior to installing ThreatQ v6:

RHEL VERSION	HARDENING STANDARD	SEE...
9.4	• CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 and v2.0.0 - Level 1 and Level 2 Server • DISA STIG for Red Hat Enterprise Linux 9 V1R2	CIS and DISA Hardening for RHEL 9.4
9.6	DISA STIG for Red Hat Enterprise Linux 9 V2R3	DISA Hardening for RHEL 9.6

It is very important that all steps in the guide are followed and all provided commands are executed. Once the deployment is complete, the VM will be running on a RHEL 9.4 OR 9.6 OS hardened according to the selected standard. There is no need to run any additional scripts to further harden the VM. Please consult with ThreatQ Support if you have any questions about the process.

ThreatQ continually updates this guide to provide you with the best possible information.

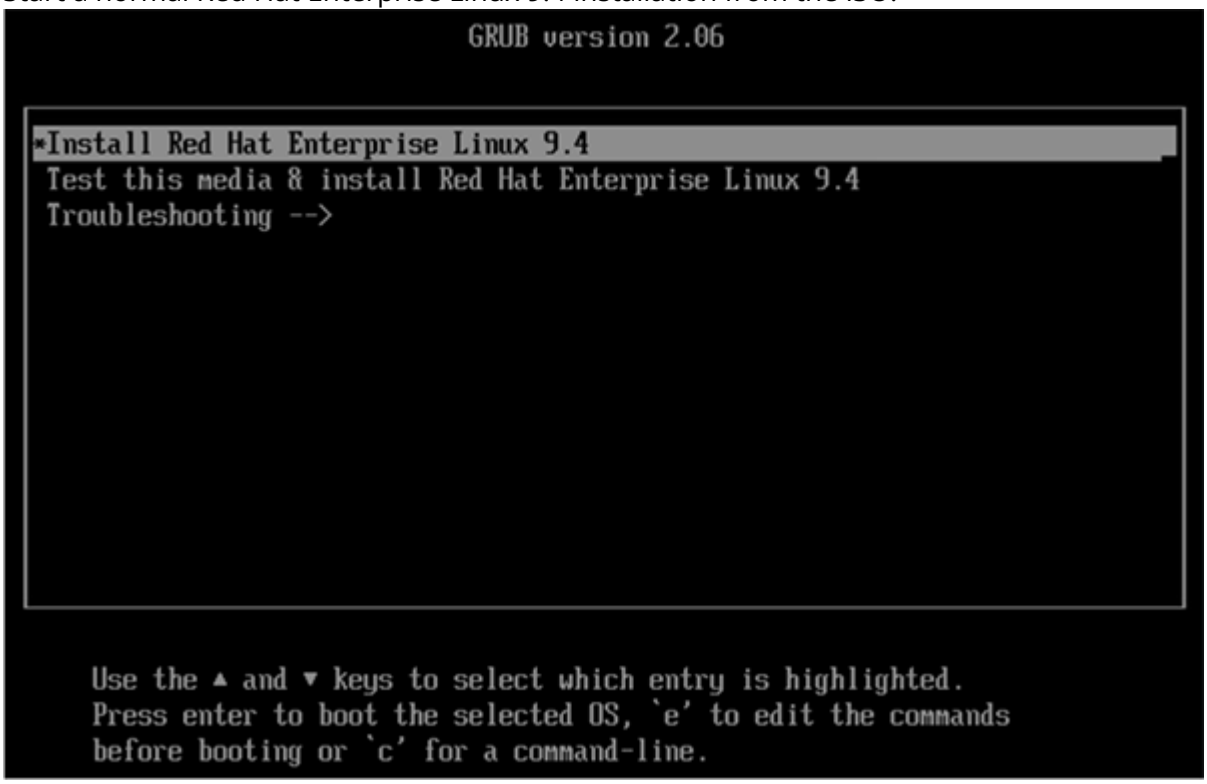
See Red Hat's online documentation for more information on Red Hat Enterprise Linux 9 security hardening options.

CIS and DISA Hardening for RHEL 9.4

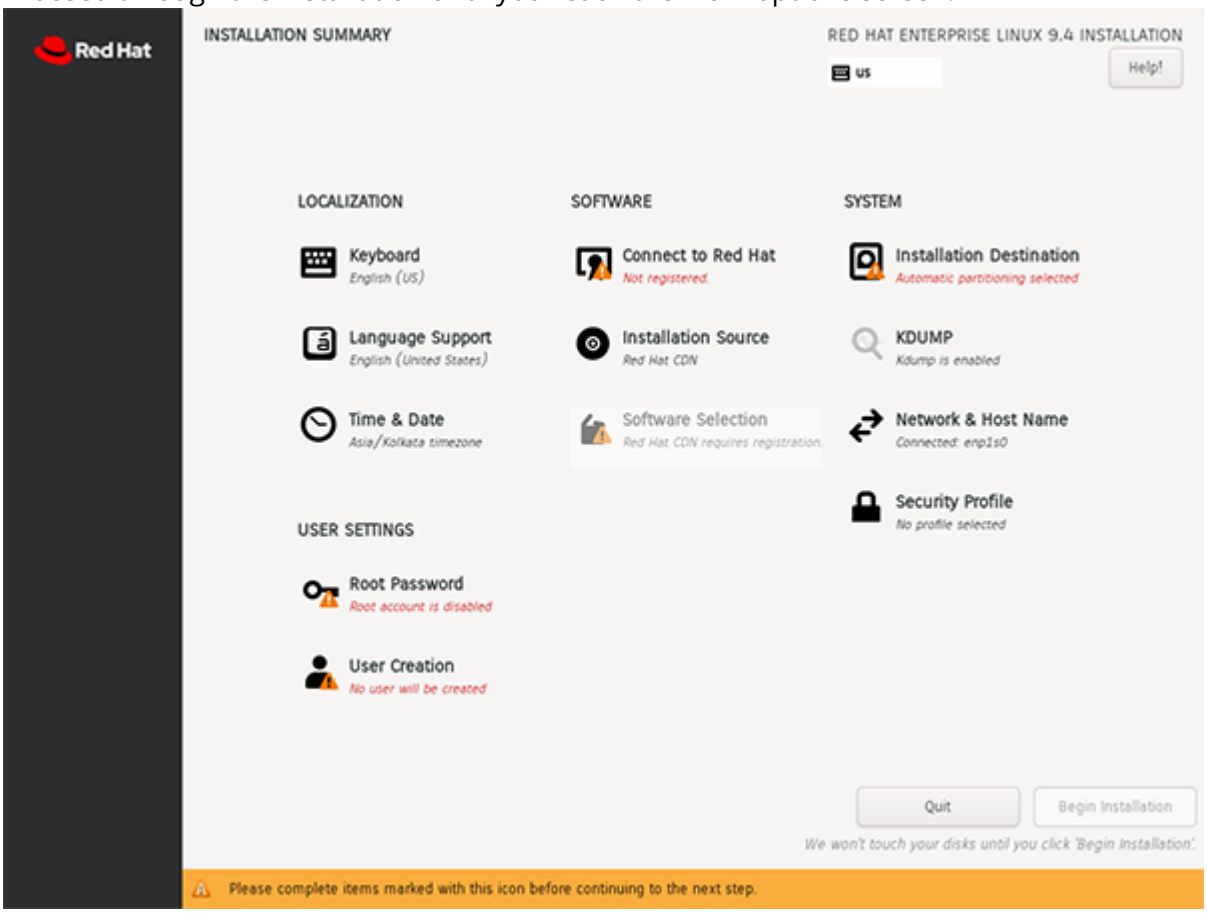
Complete the following steps to set up a hardened Red Hat Enterprise Linux (RHEL) 9 environment according to one of the supported hardening standards below prior to installing ThreatQ v6:

RHEL VERSION	HARDENING STANDARDS
9.4	• CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 and v2.0.0 - Level 1 and Level 2 Server • DISA STIG for Red Hat Enterprise Linux 9 V1R2

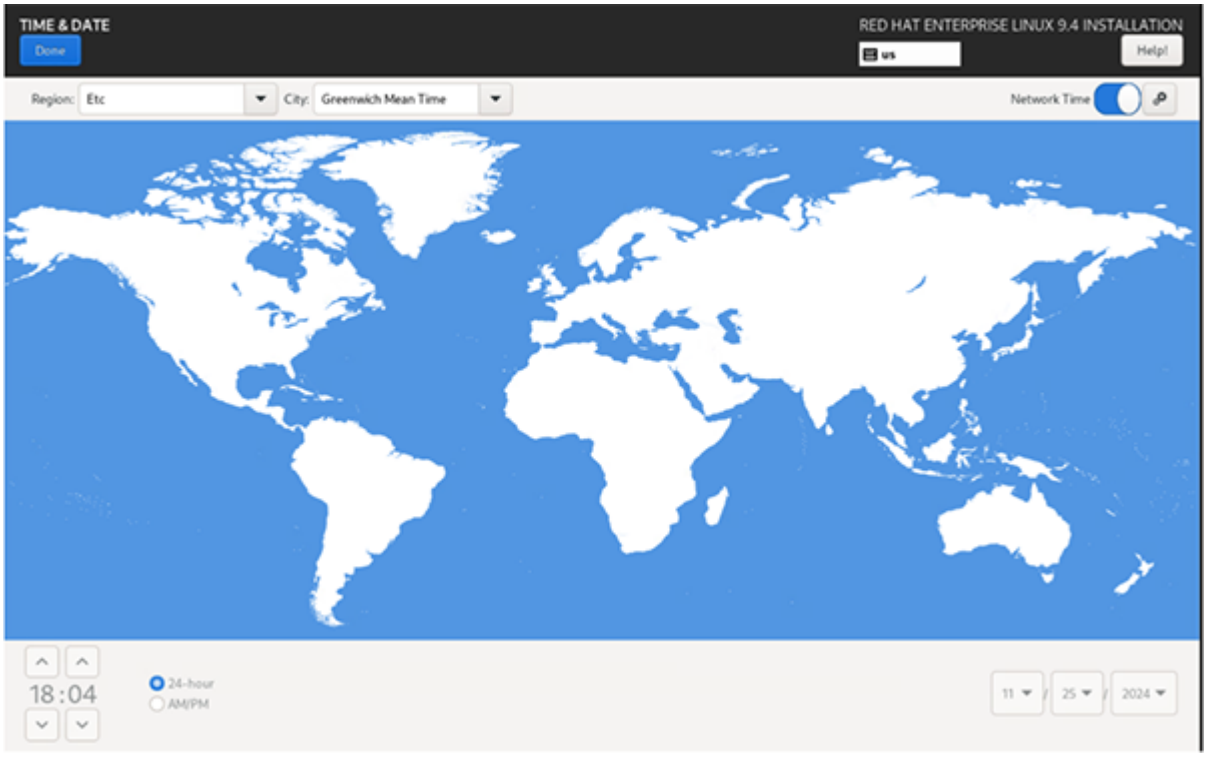
1. Start a normal Red Hat Enterprise Linux 9.4 installation from the ISO.



2. Proceed through the installation until you reach the main options screen.

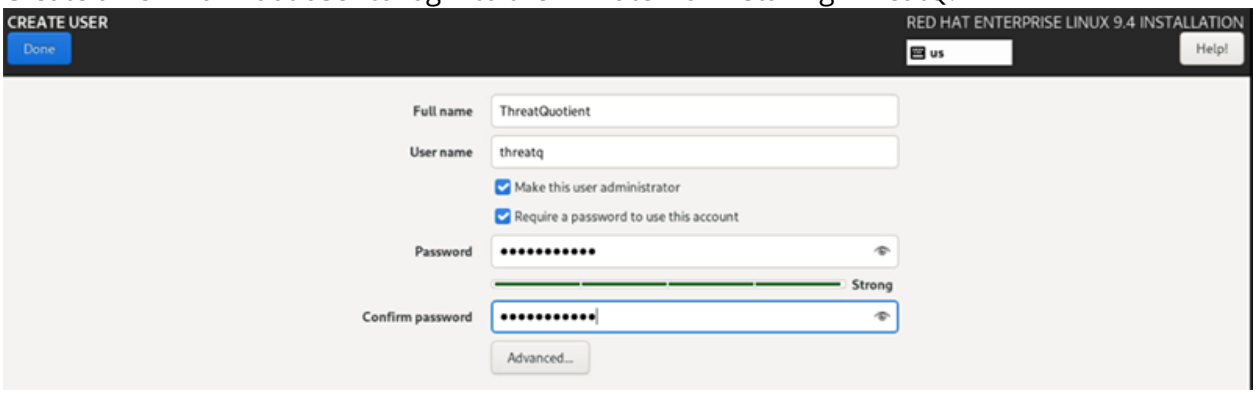


3. Click **Time & Date** and select the **Etc/Greenwich Mean Time** timezone.

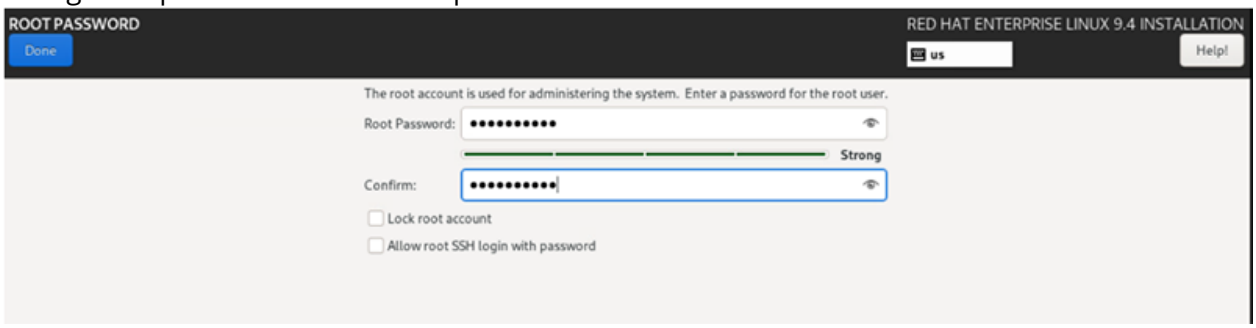


4. To create a non-root user, click the **User Creation** option.

5. Create a new non-root user to login to the VM later for installing ThreatQ.

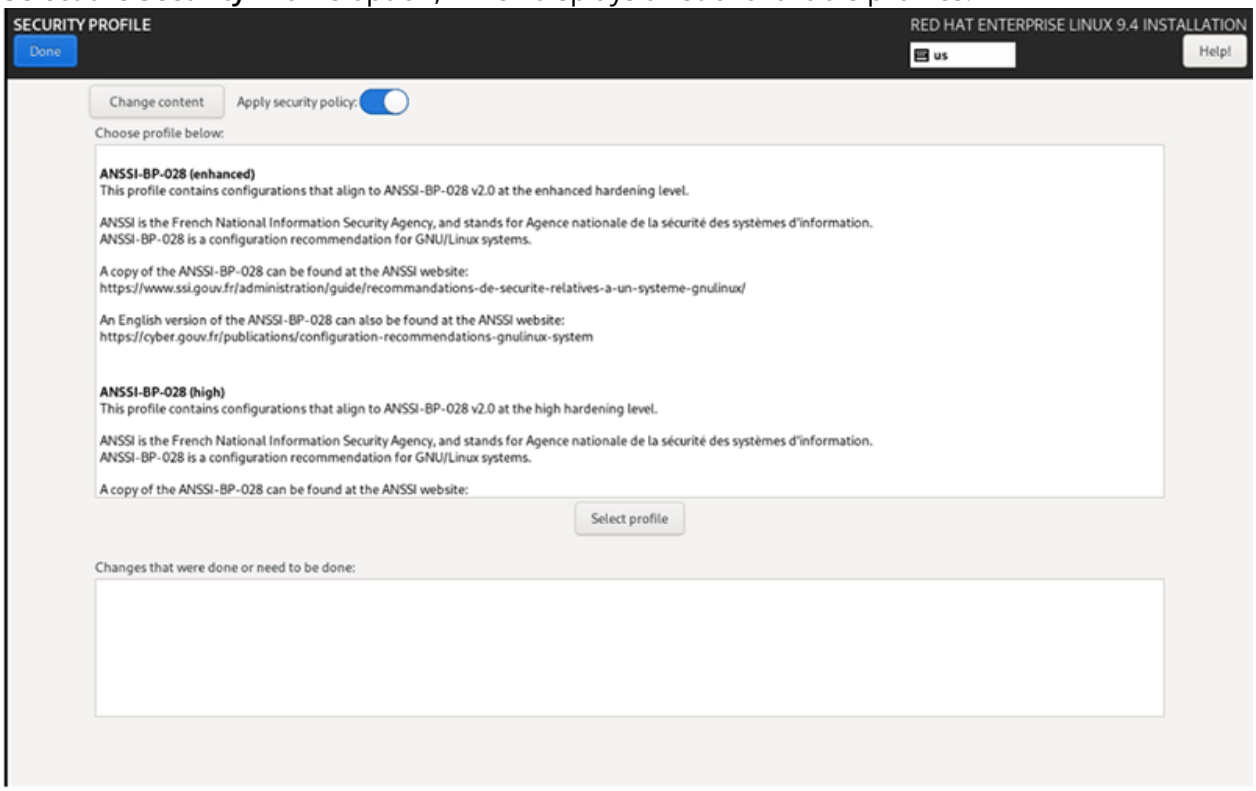


6. Enter a username and an initial password. You will be required to change this password on the first login.
7. Make sure the **Make this user administrator** and **Require a password to use this account** boxes are checked.
8. Click **Done** to save the settings and return to the main menu.
9. Click the **Root Password** option to add an initial password for root. You will be required to change this password in a later step.



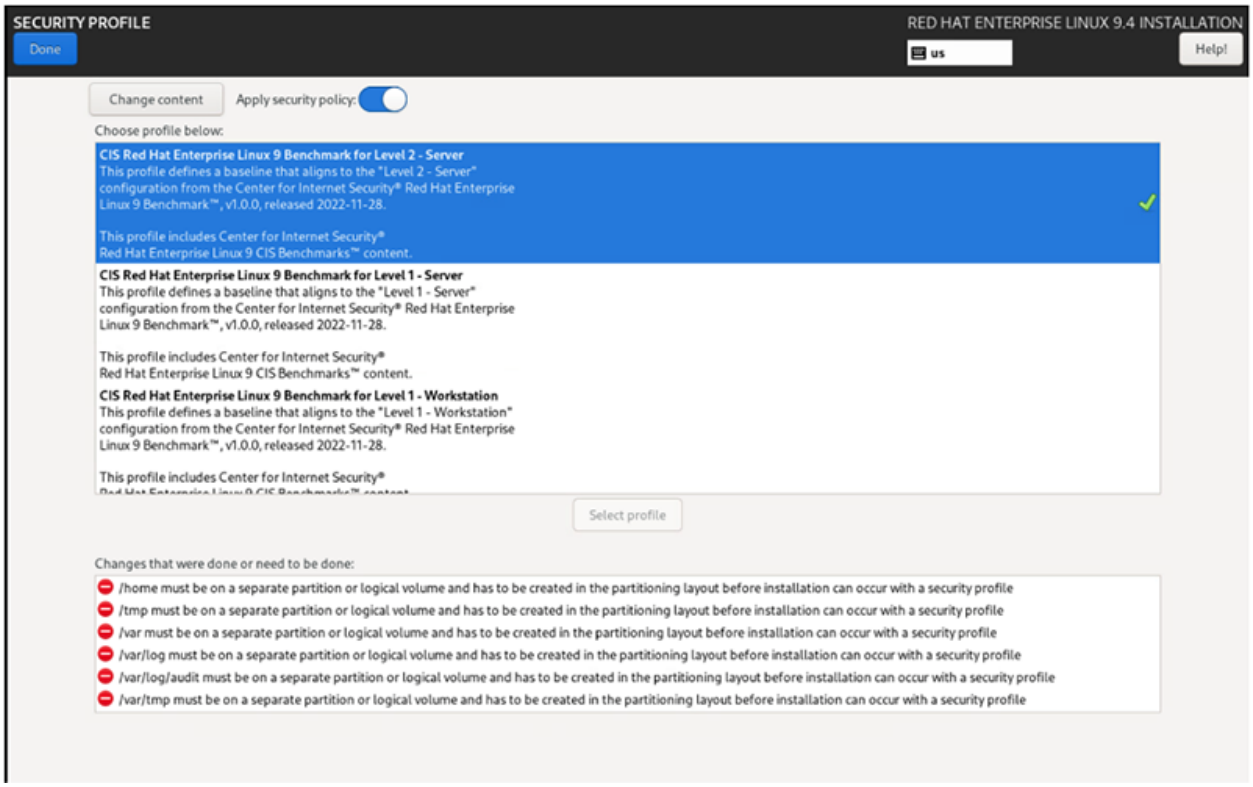
10. Click **Done** to save the settings and return to the main menu.
11. Click the **Connect to Red Hat** option, and register your installation with Red Hat.
12. Click **Done** to save the settings and return to the main menu.

13. Select the **Security Profile** option, which displays a list of available profiles.

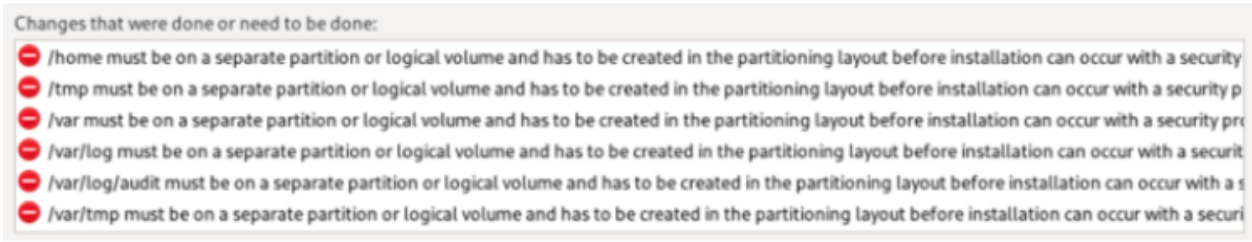


14. Scroll down and select the hardening standard desired. Refer to the list of ThreatQuotient supported standards at the beginning of this document, as many of the standards supported by Red Hat Enterprise Linux 9.4 **ARE NOT** supported for ThreatQuotient installation. Click the **Select profile** button.

> ⚠ Unless you have already configured custom partitioning, this may initially result in a number of partitioning layout errors. CIS Benchmarks and STIG have partitioning requirements that are not satisfied by the automatic partitioning scheme in Red Hat Enterprise Linux 9. These will be addressed in a later step.



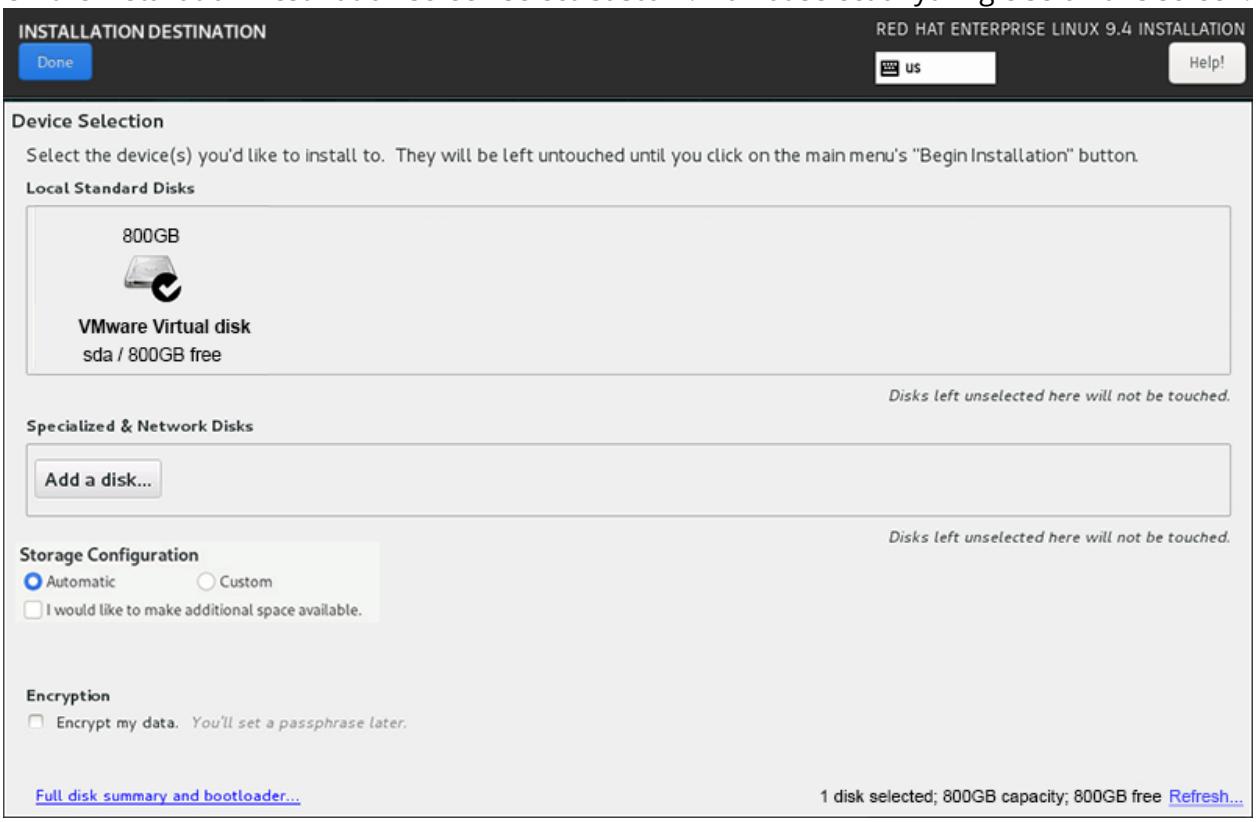
15. Select **Done** and return to the main menu.
16. From the main menu, select the **Installation Destination** option.
    You will need to create a Custom partitioning scheme that satisfies the CIS Benchmark and the ThreatQ requirements. The required partitions are listed under the Security Profile screen.



17. To create the required partitions, click the **Installation Destination** option from the main menu.
18. Use the menu to partition the drive according to the required partitioning in the **ThreatQ v6 Installation Guide**.

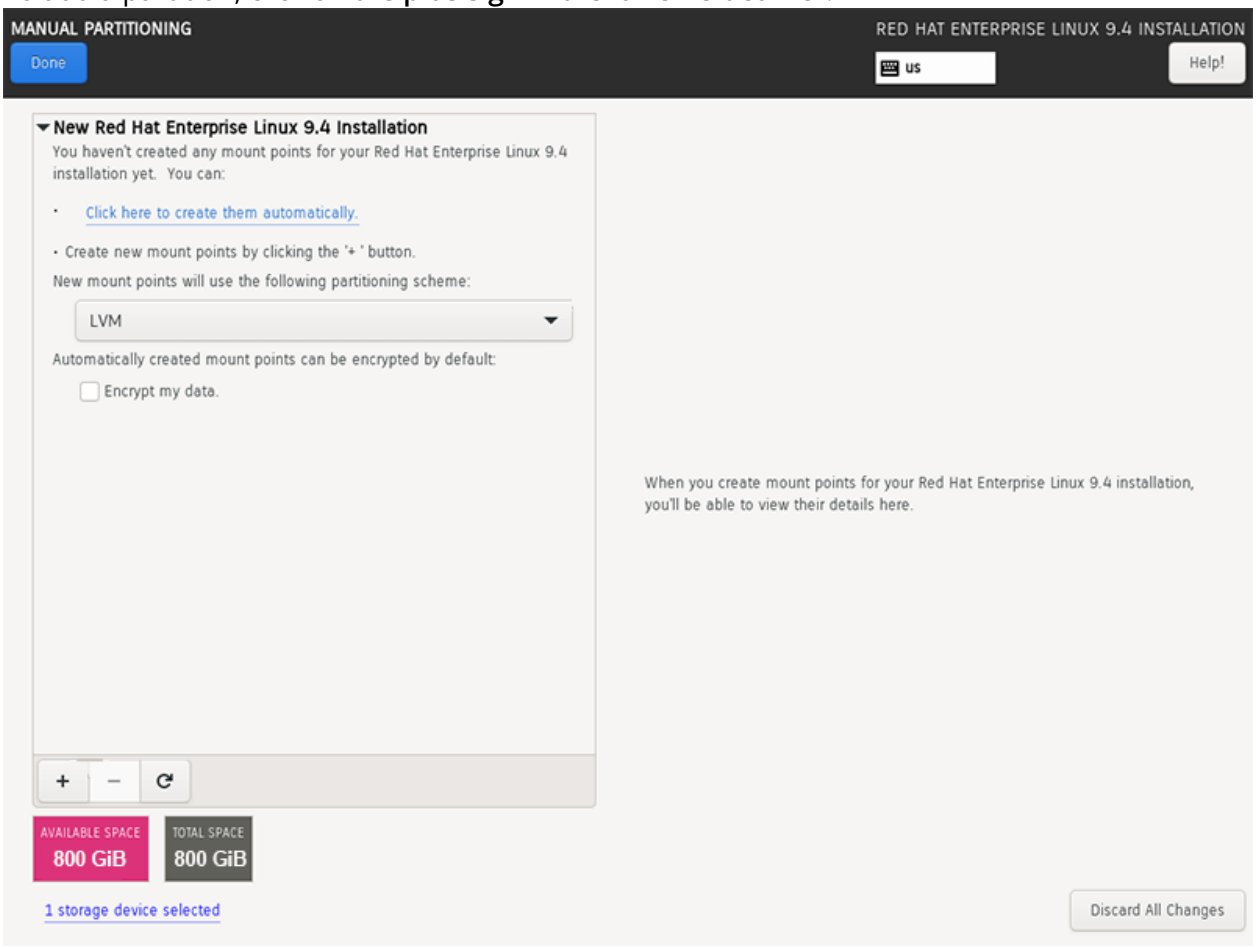
> In addition to the partitions in the ThreatQ Installation Guide, you will need to create a separate **/var** partition which is a requirement for the CIS Benchmarks and STIG.

19. On the Installation Destination screen select **Custom**. Do not select anything else on this screen.



20. Select **Done** to continue with the partitioning.

21. To add a partition, click on the **plus sign** in the lower left corner.

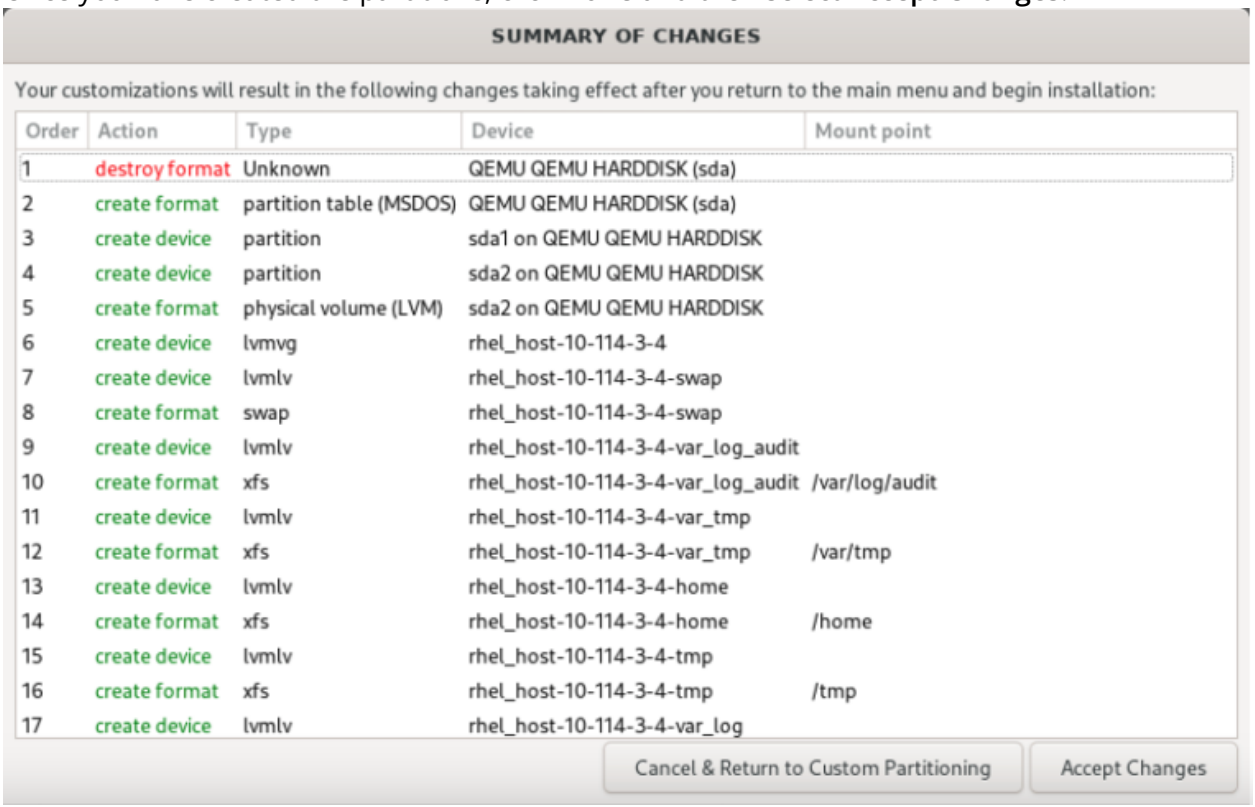


22. Enter the partition path and the size.
23. Click the **Add mount point** option.
24. Continue until you create all required partitions.

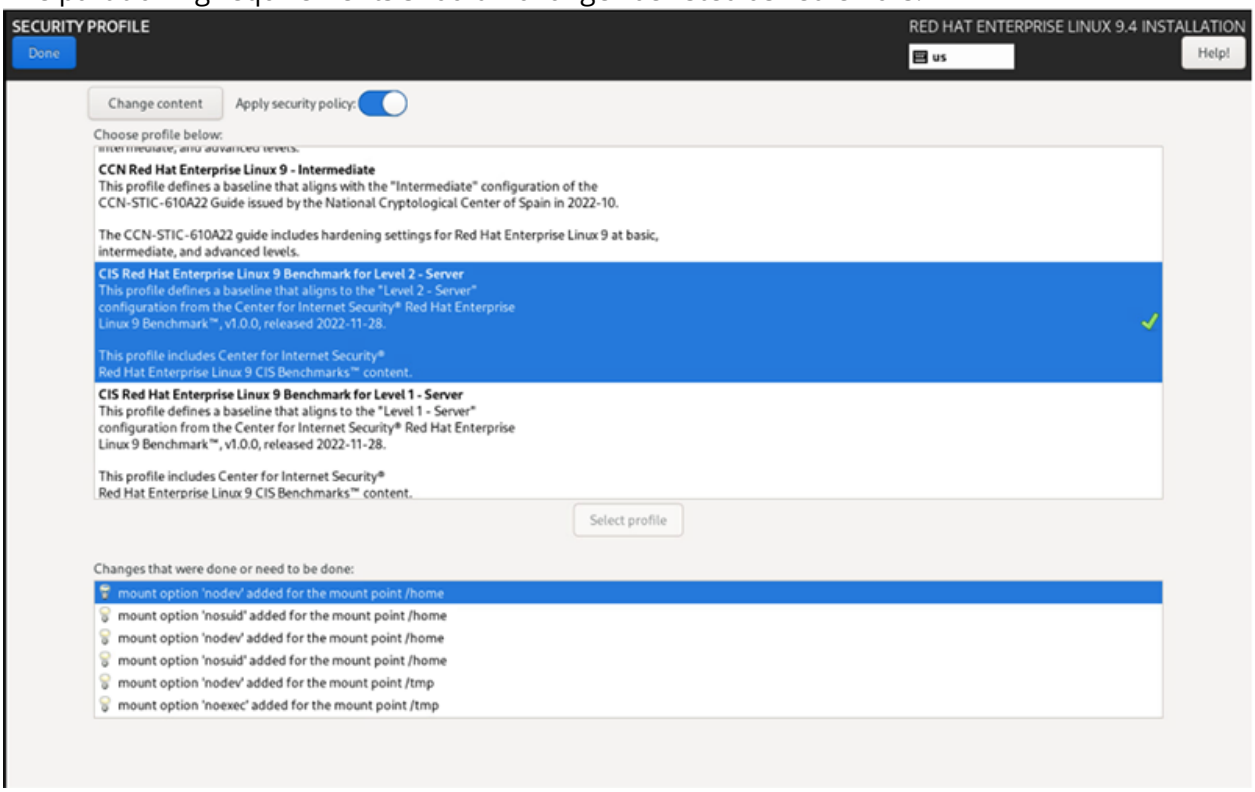
> The partitioning scheme and sizes needed may depend on both the hardening standard selected and the version of the ThreatQuotient software being used. Refer to the hardening standard documentation for any required partitions, and the ThreatQ Installation Guide for partition size guidelines.

25. Click **Done** to save the settings and return to the main menu.

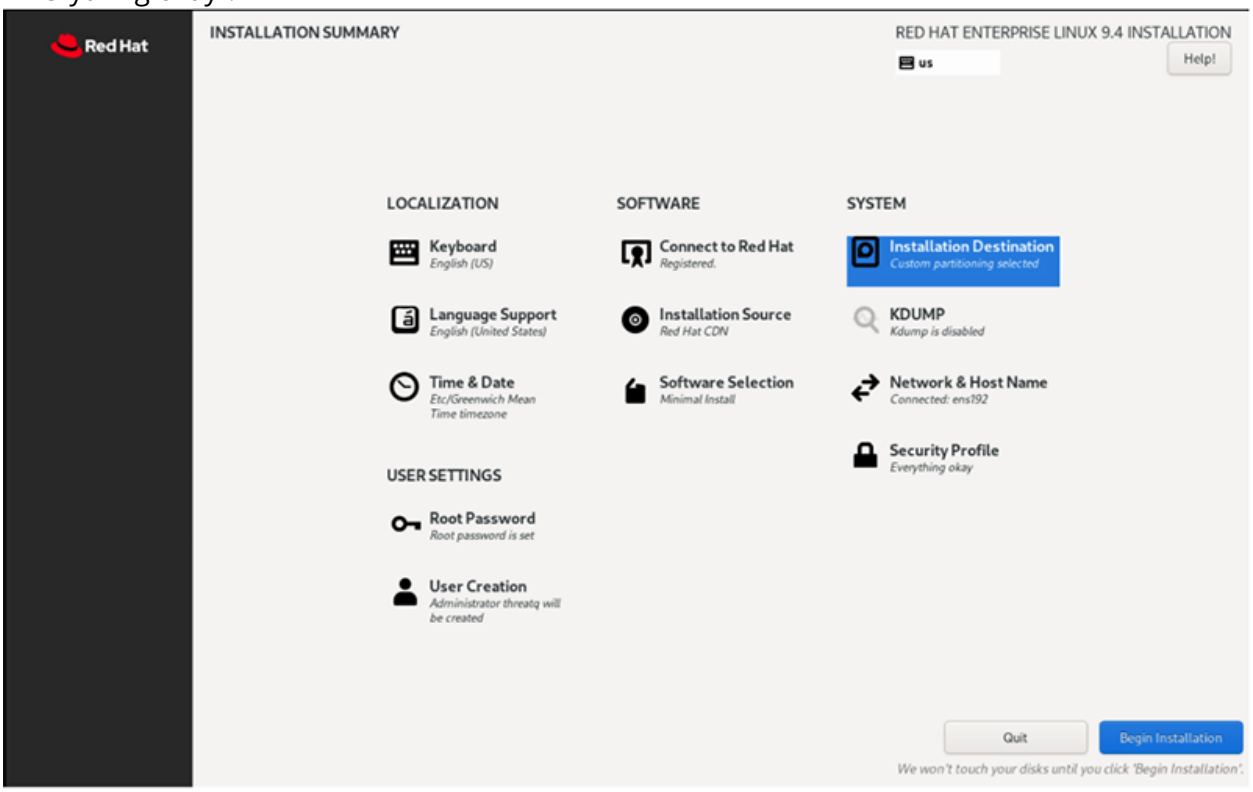
26. Once you have created the partitions, click **Done** and then select **Accept Changes**.



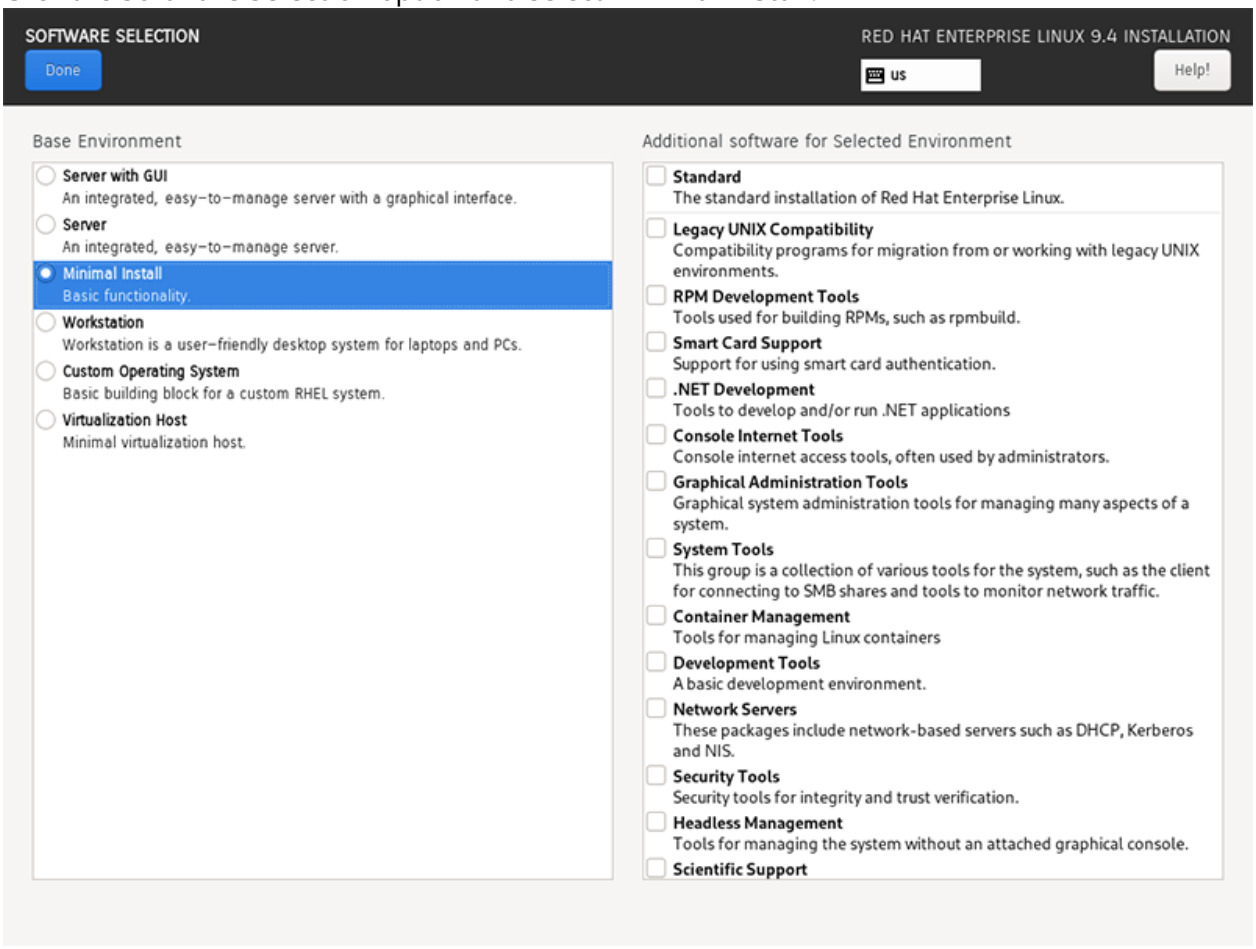
27. Click **Done** to exit back to the main menu.
28. After partitioning, select the **Security Profile** option from the main menu again. The partitioning requirements should no longer be listed as red errors.



29. Select other options as needed for your environment. The **Security Profile** should display "Everything okay".



30. Click the **Software Selection** option and select **Minimal Install**.



31. Click **Done** to save your settings and return to the main menu.
32. When ready, select **Begin Installation**.
    When the installation finishes, the VM will reboot
33. After the reboot, SSH to the VM using the non-root user you created in step 5.
34. After the initial login you will be asked to change the non-root user password. Enter the initial password you set up in step 5 and then enter the new password.

```
valentintodorov@Valentins-MacBook-Pro ~ % ssh tqadmin@10.114.0.72
The authenticity of host '10.114.0.72 (10.114.0.72)' can't be established.
ED25519 key fingerprint is SHA256:YKJt7UeeOC6o6c3HZNLdMctg3FqUuWe7ToCZy/lBw+4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.114.0.72' (ED25519) to the list of known hosts.
Authorized uses only. All activity may be monitored and reported.
tqadmin@10.114.0.72's password:
You are required to change your password immediately (password expired).
You are required to change your password immediately (password expired).
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tqadmin.
Current password:
```

35. After the password is updated, SSH to the VM with the non-root user from step 5 using the new password.
36. Complete the following steps to install your SSH key:

1. Create folder: `mkdir -p ~/.ssh`
2. Create the file **/home/<*non-root user*>/.ssh/authorized_keys** and add your SSH key to it.
3. Change the ownership and permissions of the file:

   ```
   chmod 700 ~/.ssh/
   chmod 600 ~/.ssh/authorized_keys
   ```

37. Update the root password: `sudo passwd -u root`
38. Begin the ThreatQ v6 installation following the provided installation guide.

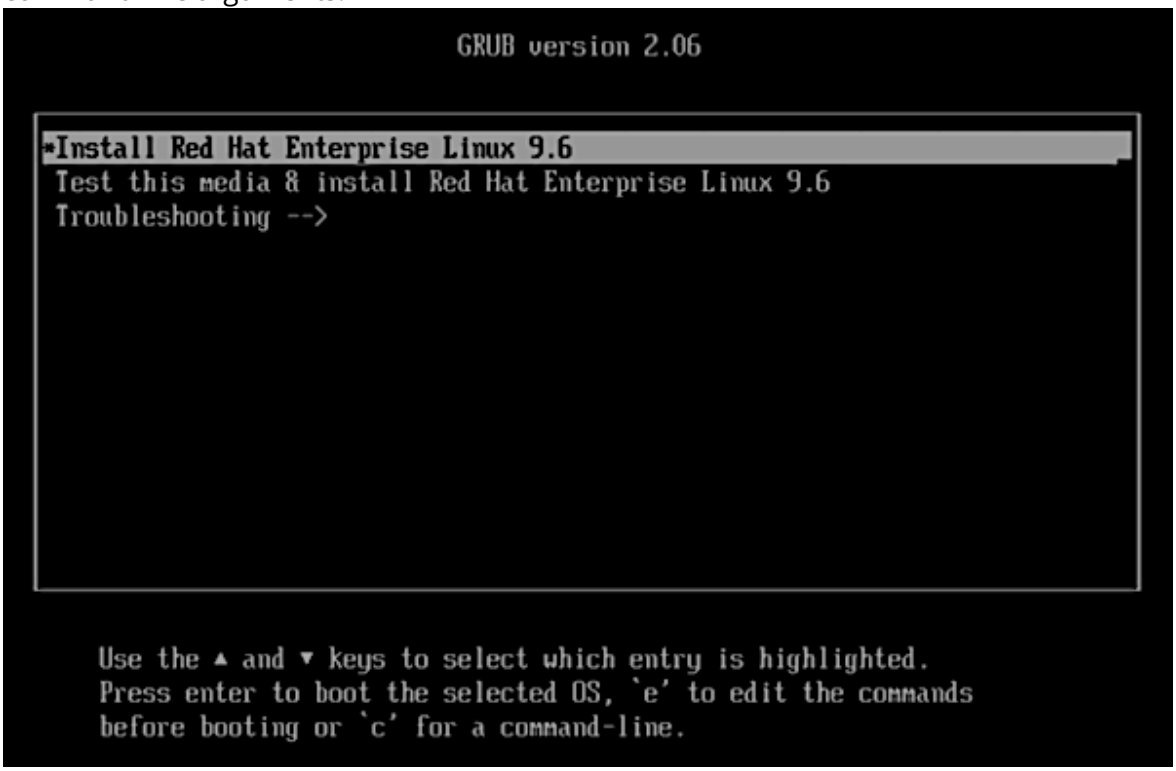
DISA Hardening for RHEL 9.6

Complete the following steps to set up a hardened Red Hat Enterprise Linux (RHEL) 9.6 environment according to the DISA STIG for Red Hat Enterprise Linux 9 V2R3 hardening standard prior to installing ThreatQ v6.

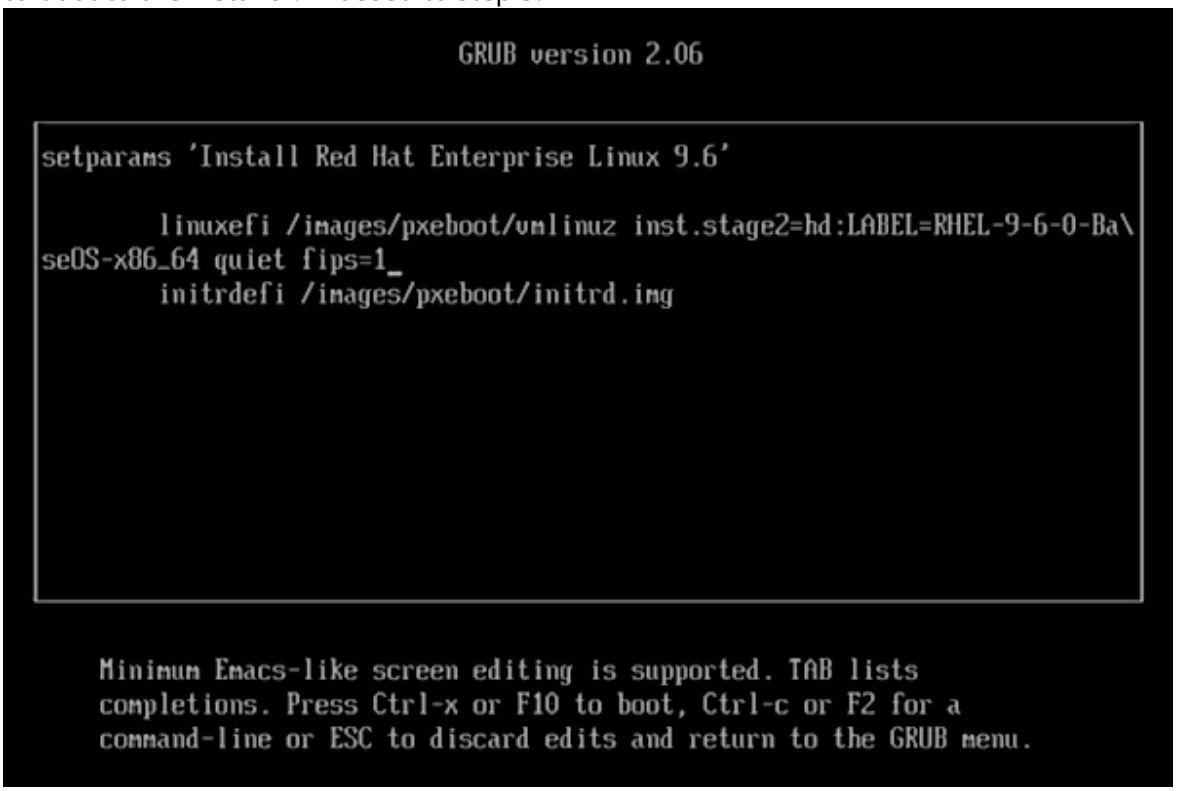
1. Start a normal Red Hat Enterprise Linux 9.6 installation from the ISO.

   > ⚠ Red Hat has changed the install process for RHEL 9.6 in regard to FIPS 140 support. Selecting the STIG Security Profile no longer automatically enables FIPS in the installer and target system. To install a STIG compliant system you MUST follow step 2 below even though it was not required in RHEL 9.4 and prior versions. Failure to do so will result in a system that does not use the correct encryption libraries.

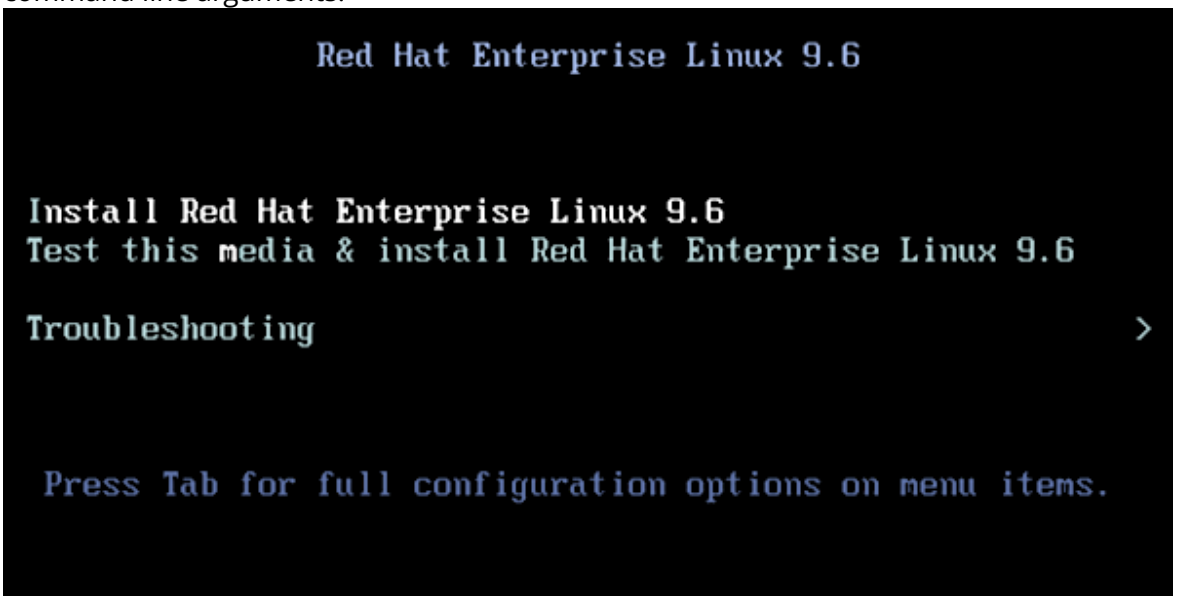
2. This step is ONLY required if you need FIPS 140 support, which is required for DISA STIG. If you do not require FIPS 140 support proceed to step 3. The next step will look slightly different depending on if you are booting via BIOS or EFI:
   - **EFI:** Arrow over to Install Red Hat Enterprise Linux 9.6 and press **e** to edit the kernel command line arguments.



- Select the linuxefi line and add the **fips=1** argument to the end of the list. Press **Control+X** to boot to the installer. Proceed to step 3.

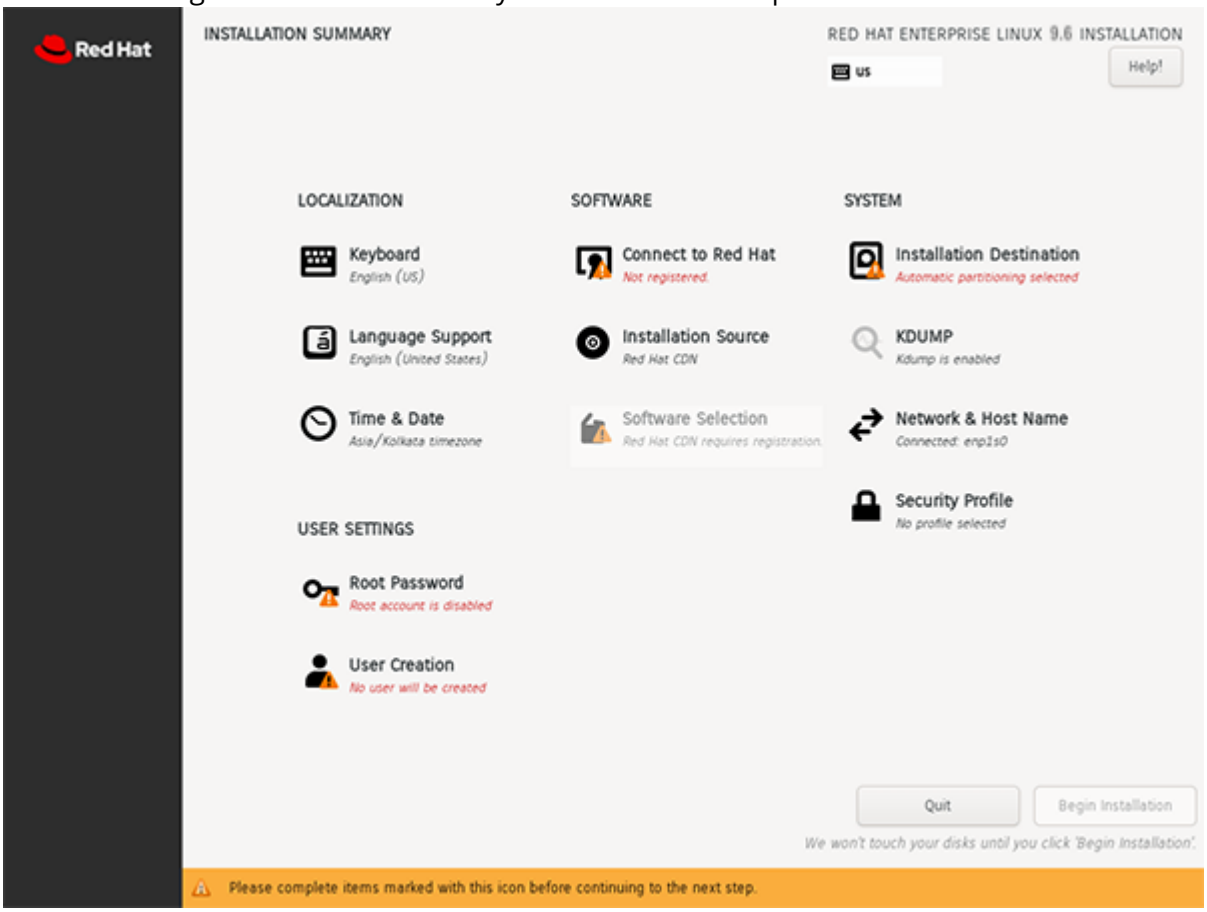


- **BIOS:** Arrow over to Install Red Hat Enterprise Linux 9.6 and press **Tab** to open the kernel command line arguments.

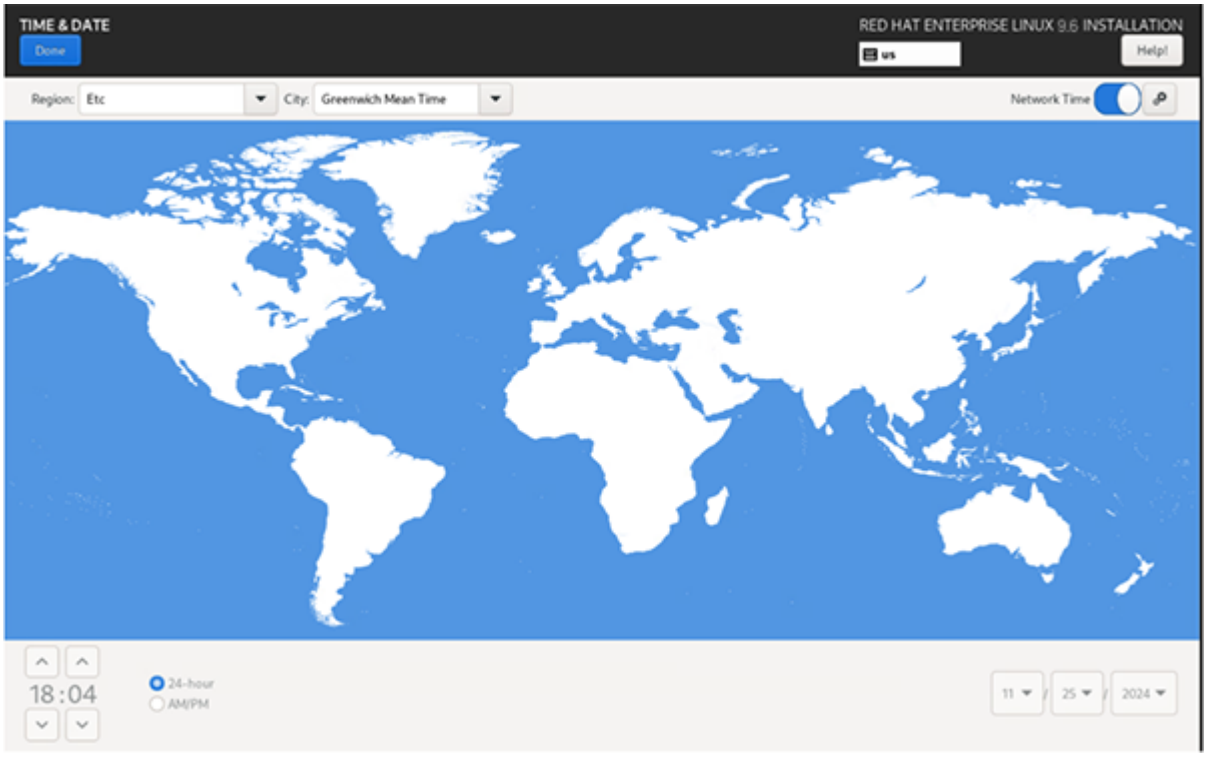


- Add **fips=1** to the end of the argument list and press Enter to boot to the installer. Proceed to step 3.

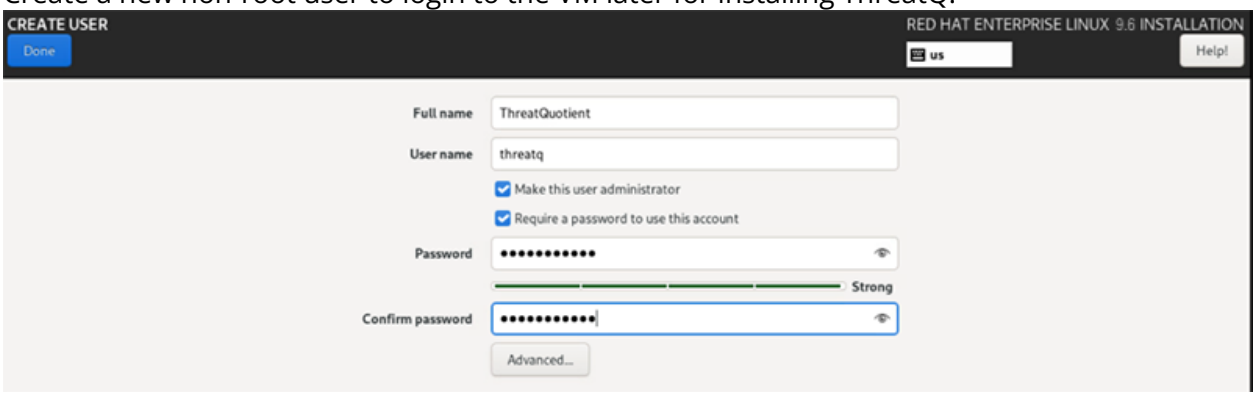
3. Proceed through the installation until you reach the main options screen.



4. Click **Time & Date** and select the **Etc/Greenwich Mean Time** timezone.

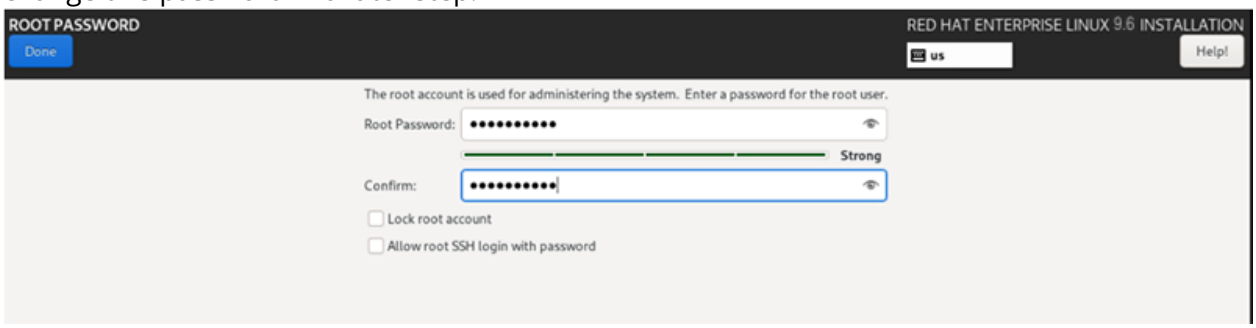


5. To create a non-root user, click the **User Creation** option.
6. Create a new non-root user to login to the VM later for installing ThreatQ.

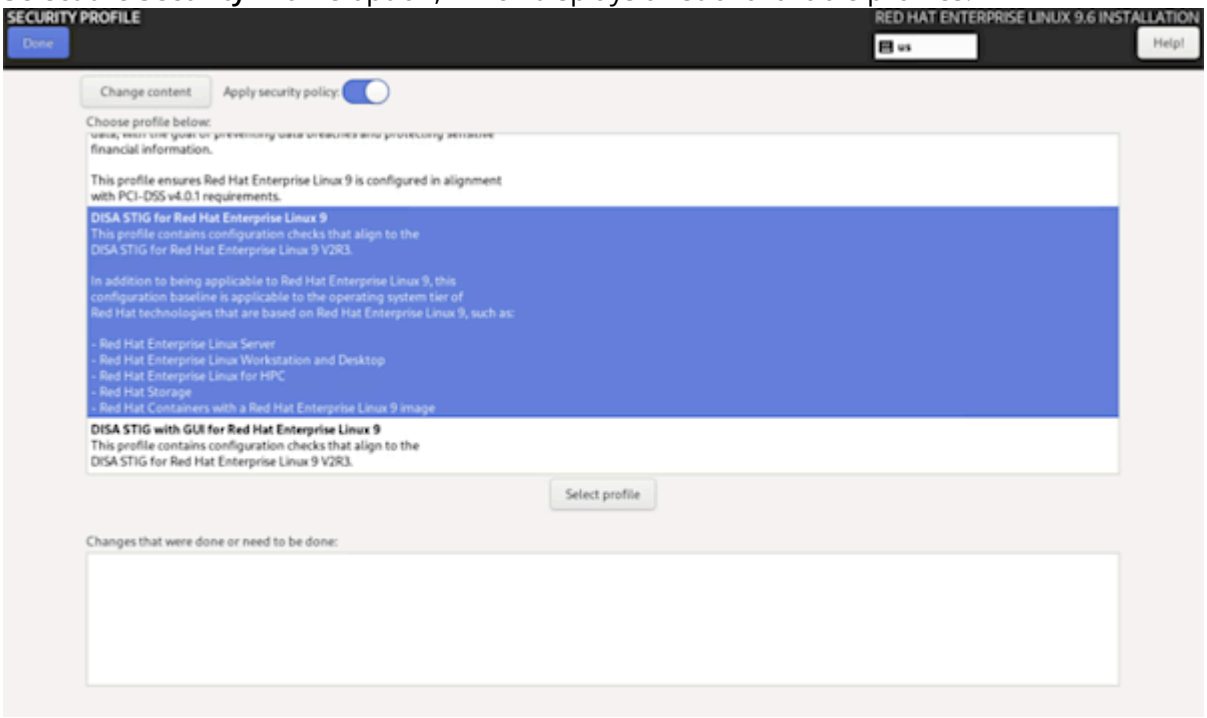


7. Enter a username and an initial password. You will be required to change this password on the first login.
8. Make sure the **Make this user administrator** and **Require a password to use this account** boxes are checked.
9. Click **Done** to save the settings and return to the main menu.

10. Click the **Root Password** option to add an initial password for root. You will be required to change this password in a later step.

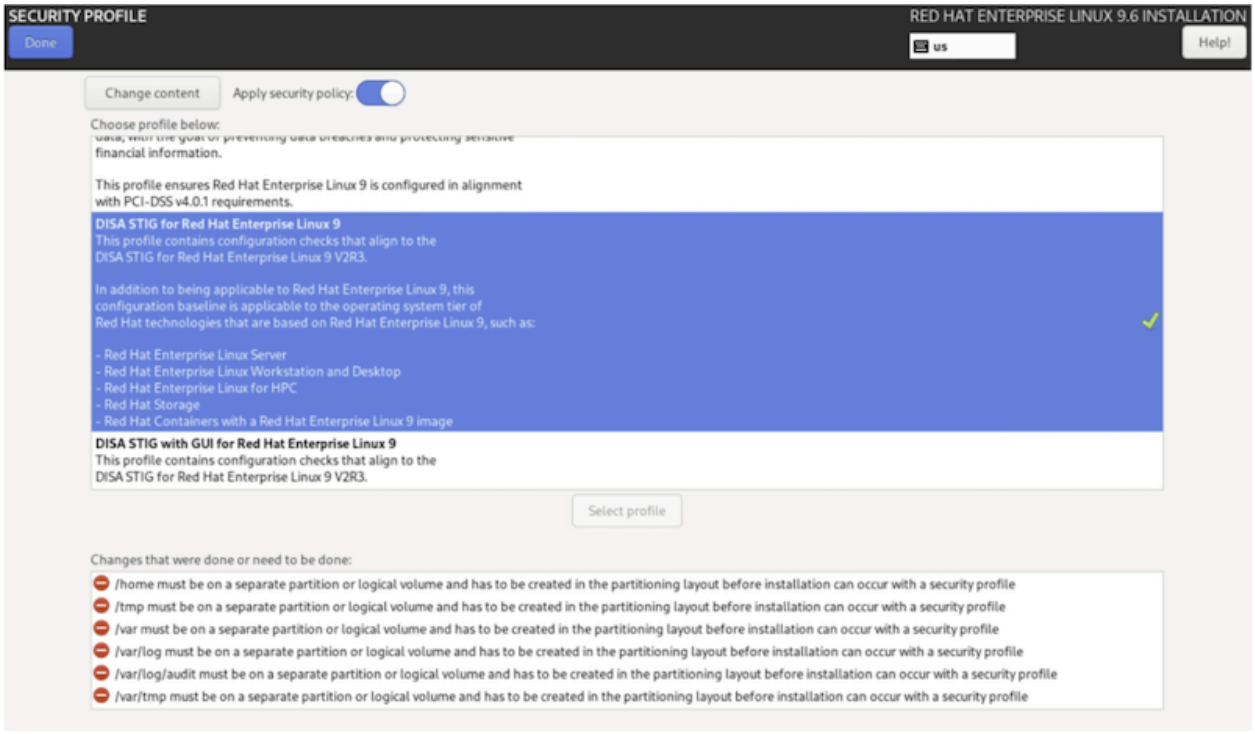


11. Click **Done** to save the settings and return to the main menu.
12. Click the **Connect to Red Hat** option and register your installation with Red Hat.
13. Click **Done** to save the settings and return to the main menu.
14. Select the **Security Profile** option, which displays a list of available profiles.

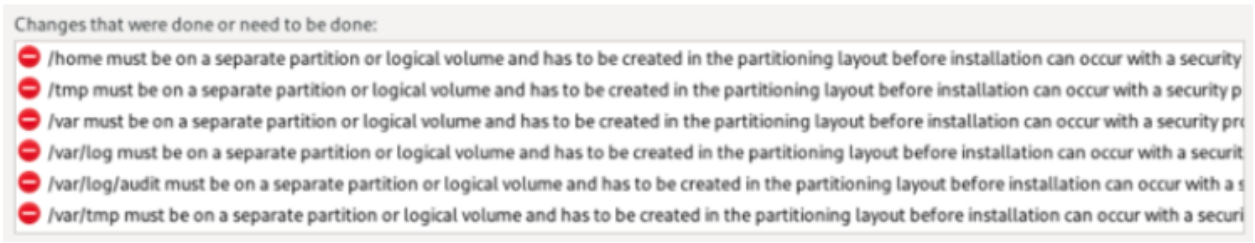


15. Scroll down and select the hardening standard desired. Refer to the list of ThreatQuotient supported standards at the beginning of this document, as many of the standards supported by Red Hat Enterprise Linux 9.6 **ARE NOT** supported for ThreatQuotient installation. Click the **Select profile** button.

> ⚠ Unless you have already configured custom partitioning, this may initially result in a number of partitioning layout errors. CIS Benchmarks and STIG have partitioning requirements that are not satisfied by the automatic partitioning scheme in Red Hat Enterprise Linux 9. These will be addressed in a later step.



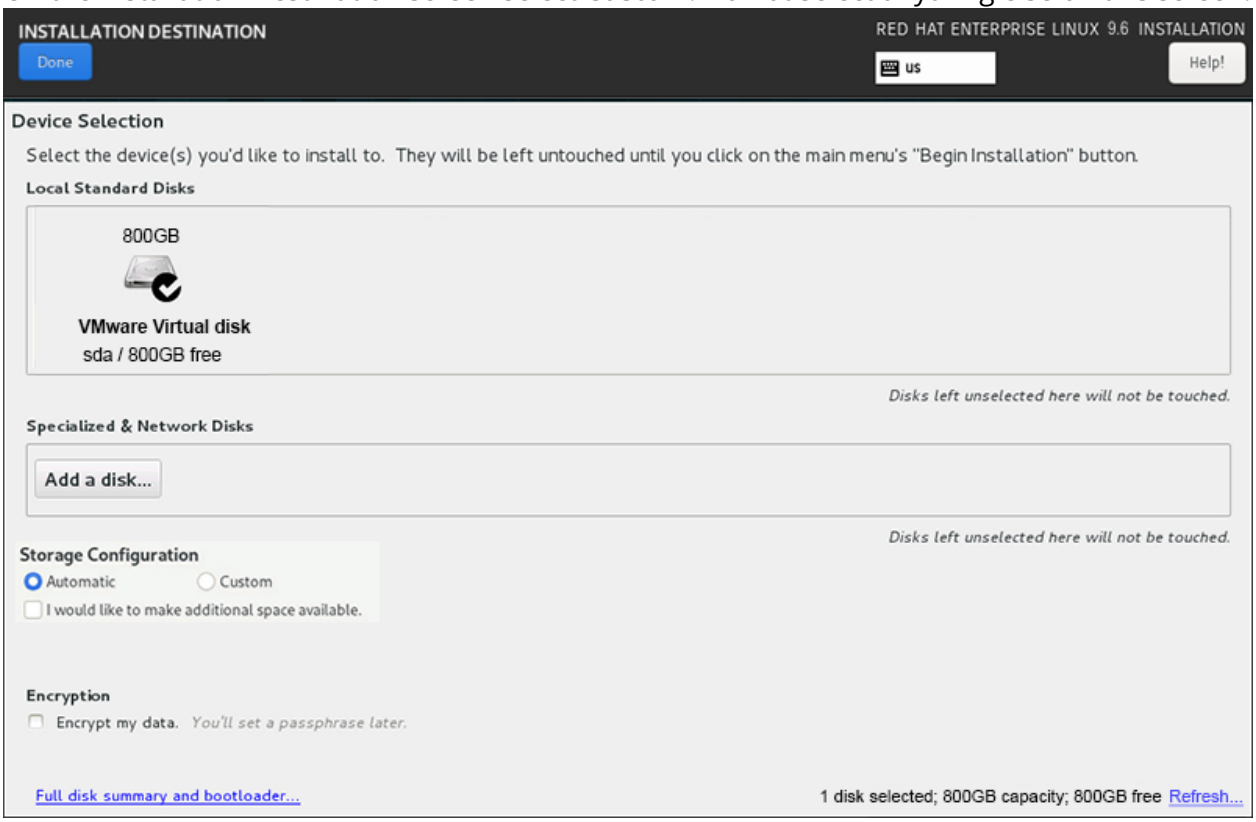
16. Select **Done** and return to the main menu.
17. From the main menu, select the **Installation Destination** option.
    You will need to create a Custom partitioning scheme that satisfies the CIS Benchmark and the ThreatQ requirements. The required partitions are listed under the Security Profile screen.



18. To create the required partitions, click the **Installation Destination** option from the main menu.
19. Use the menu to partition the drive according to the required partitioning in the **ThreatQ v6 Installation Guide**.

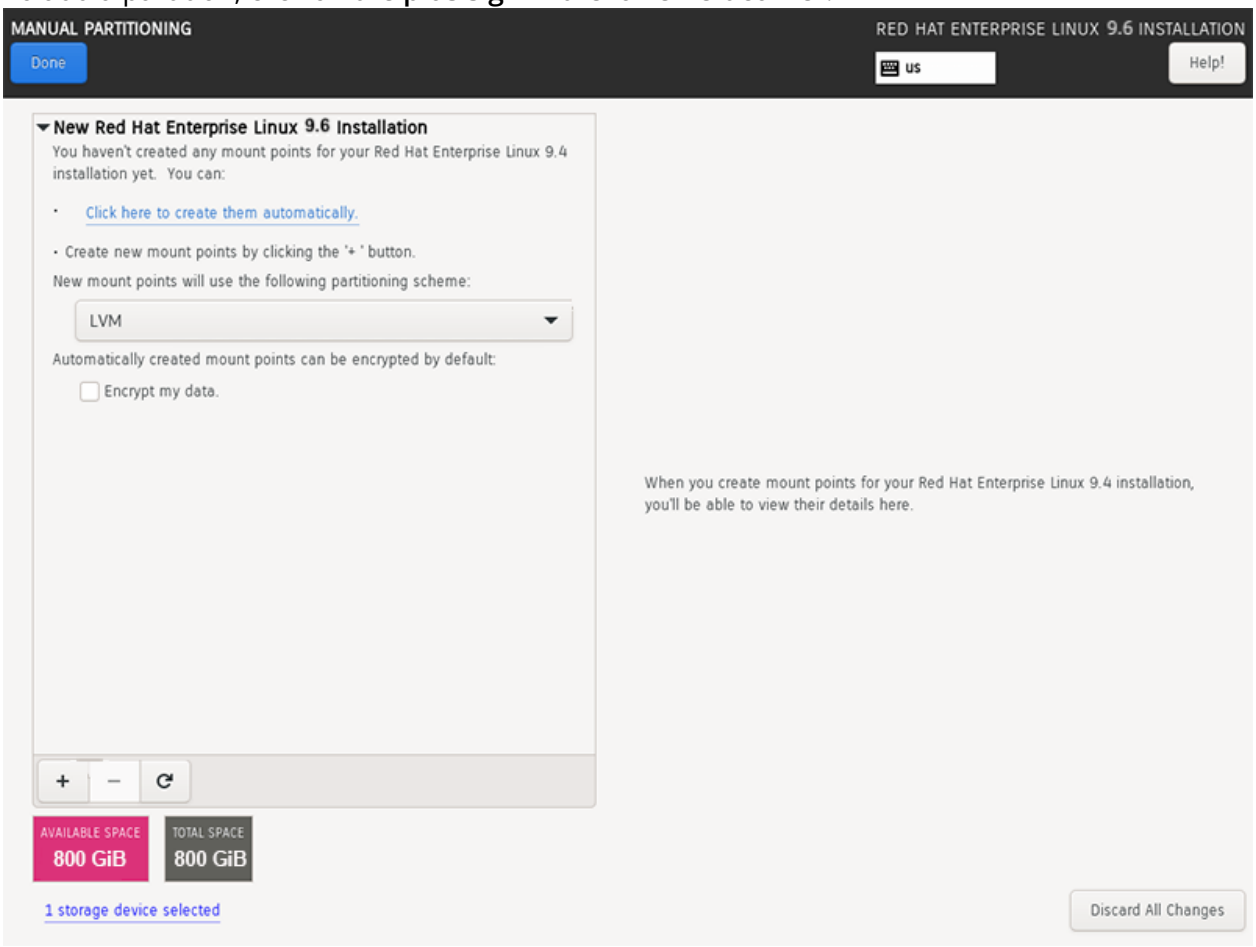
> In addition to the partitions in the ThreatQ Installation Guide, you will need to create a separate **/var** partition which is a requirement for the CIS Benchmarks and STIG.

20. On the Installation Destination screen select **Custom**. Do not select anything else on this screen.



21. Select **Done** to continue with the partitioning.

22. To add a partition, click on the **plus sign** in the lower left corner.

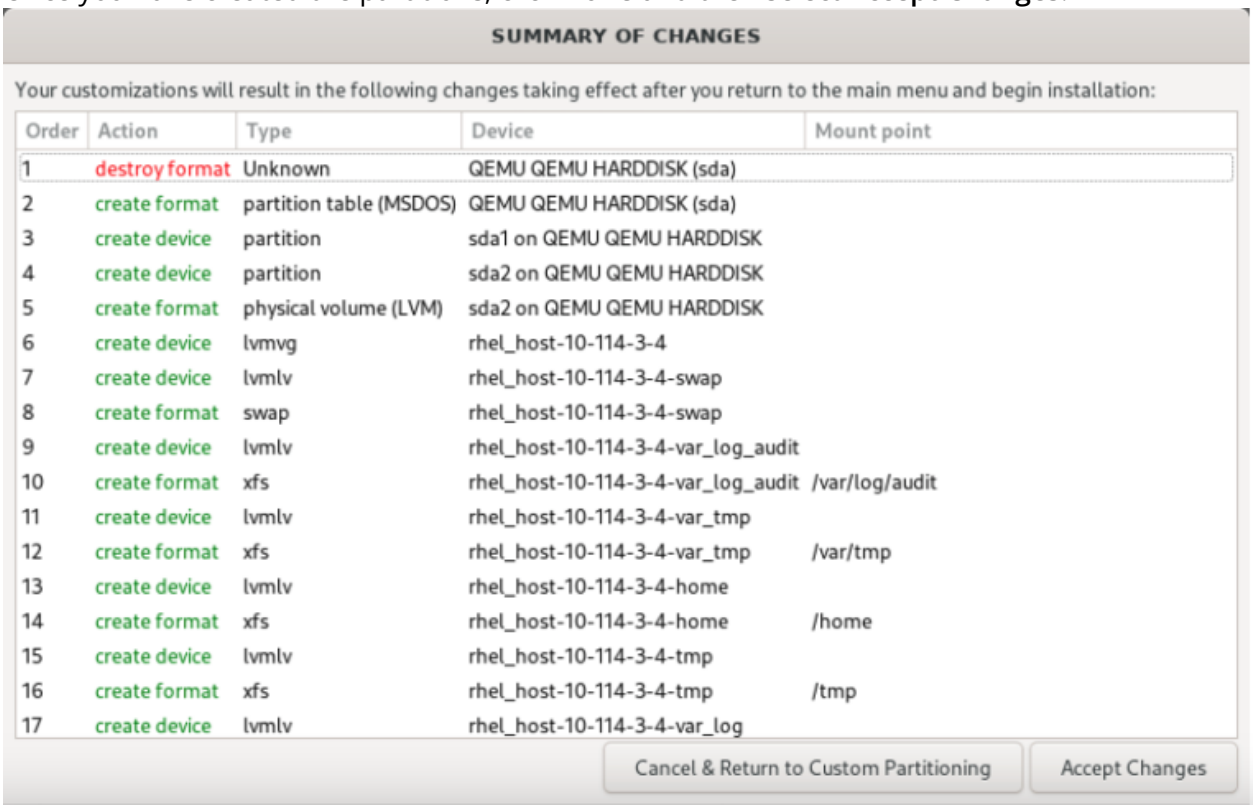


23. Enter the partition path and the size.
24. Click the **Add mount point** option.
25. Continue until you create all required partitions.

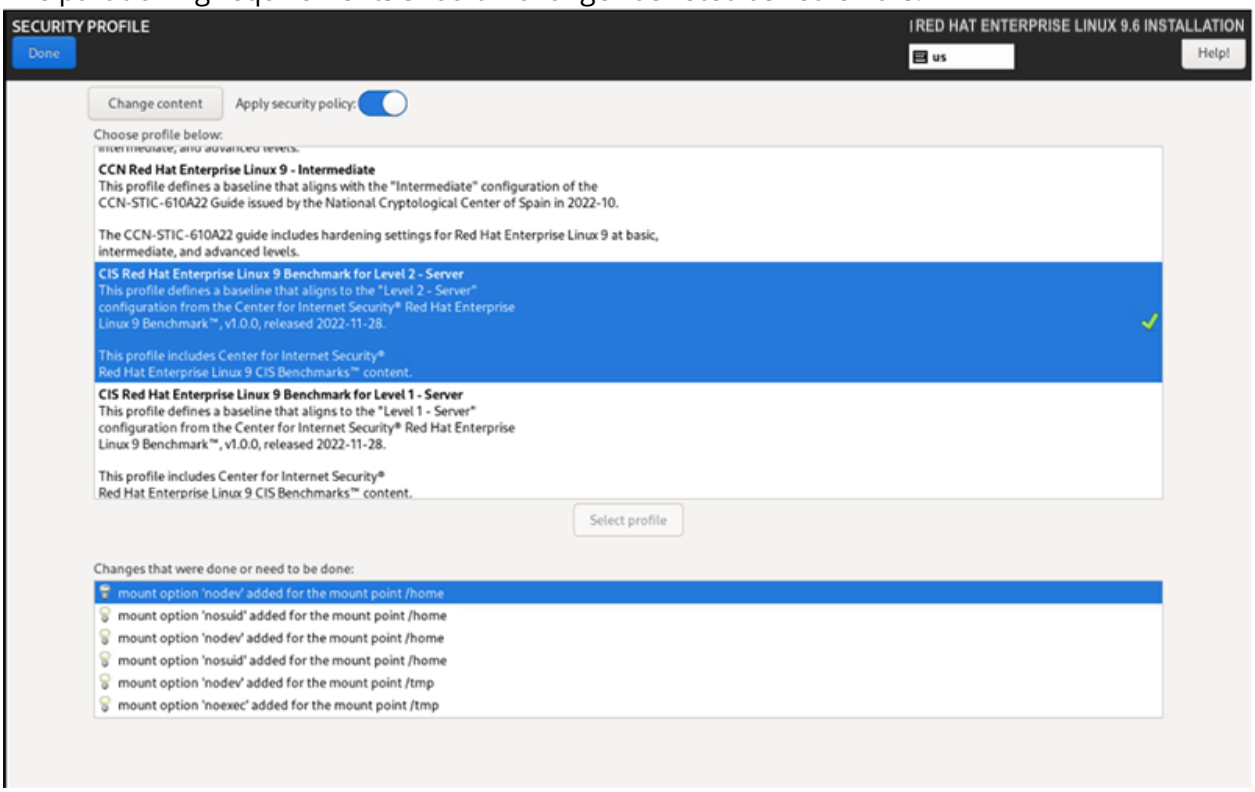
> The partitioning scheme and sizes needed may depend on both the hardening standard selected and the version of the ThreatQuotient software being used. Refer to the hardening standard documentation for any required partitions, and the ThreatQ Installation Guide for partition size guidelines.

26. Click **Done** to save the settings and return to the main menu.

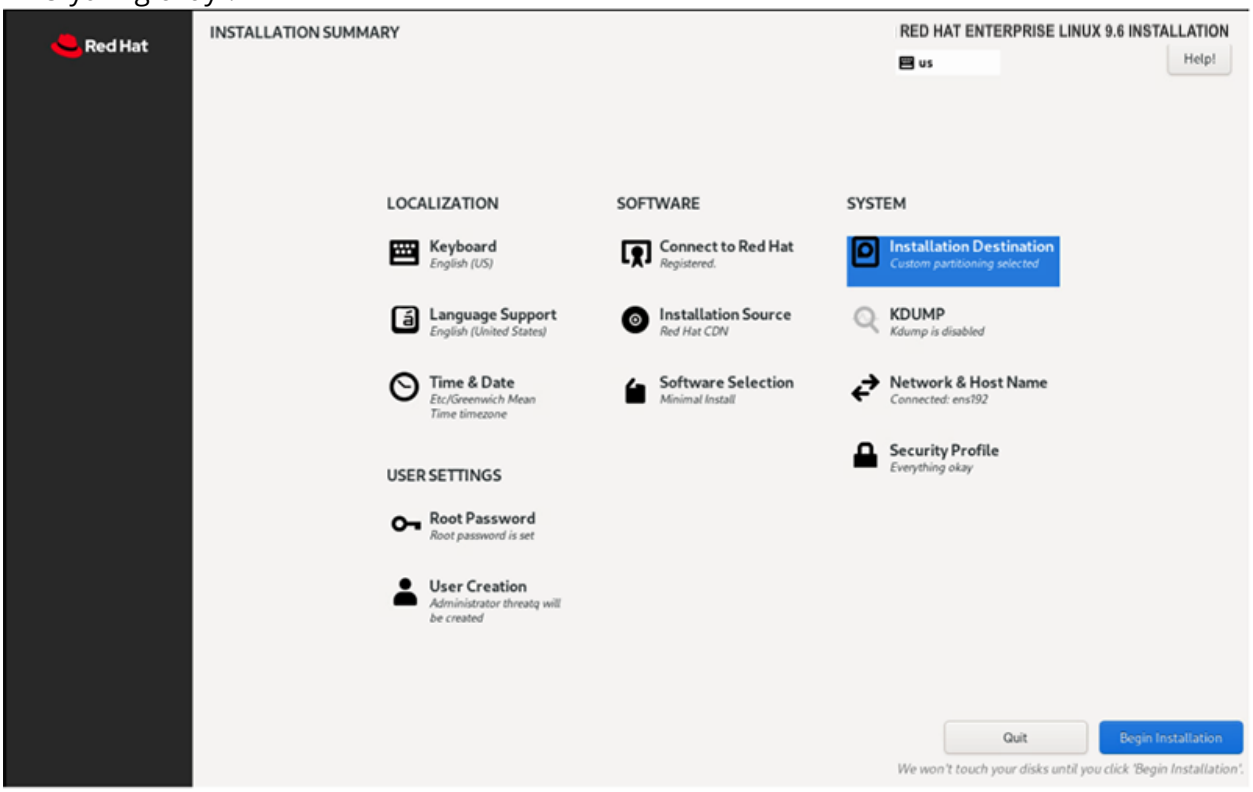
27. Once you have created the partitions, click **Done** and then select **Accept Changes**.



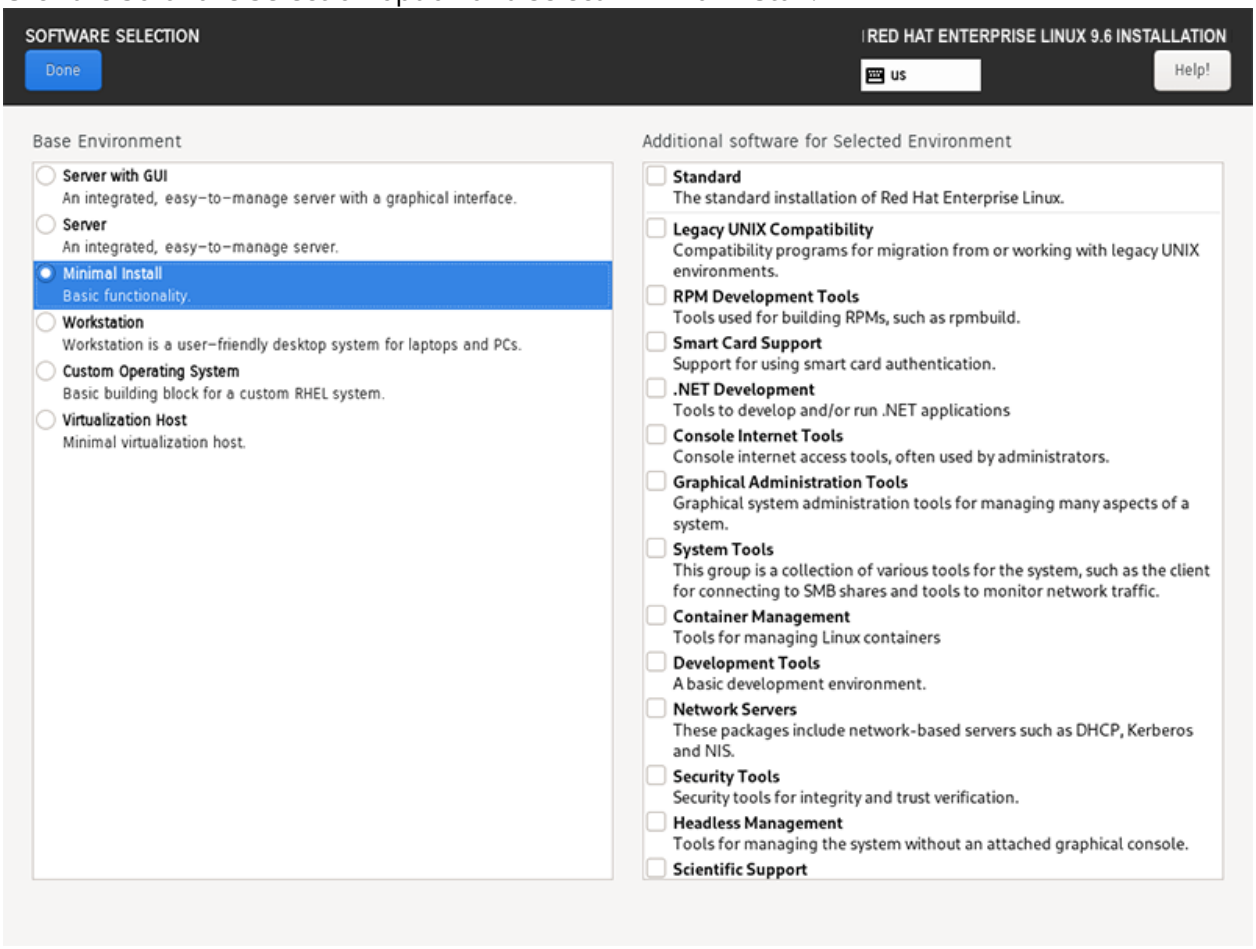
28. Click **Done** to exit back to the main menu.
29. After partitioning, select the **Security Profile** option from the main menu again. The partitioning requirements should no longer be listed as red errors.



30. Select other options as needed for your environment. The **Security Profile** should display "Everything okay".



31. Click the **Software Selection** option and select **Minimal Install**.



32. Click **Done** to save your settings and return to the main menu.
33. When ready, select **Begin Installation**.
    When the installation finishes, the VM will reboot
34. After the reboot, SSH to the VM using the non-root user you created in step 5.
35. After the initial login you will be asked to change the non-root user password. Enter the initial password you set up in step 5 and then enter the new password.

```
valentintodorov@Valentins-MacBook-Pro ~ % ssh tqadmin@10.114.0.72
The authenticity of host '10.114.0.72 (10.114.0.72)' can't be established.
ED25519 key fingerprint is SHA256:YKJt7UeeOC6o6c3HZNLdMctg3FqUuWe7ToCZy/lBw+4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.114.0.72' (ED25519) to the list of known hosts.
Authorized uses only. All activity may be monitored and reported.
tqadmin@10.114.0.72's password:
You are required to change your password immediately (password expired).
You are required to change your password immediately (password expired).
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user tqadmin.
Current password:
```

36. After the password is updated, SSH to the VM with the non-root user from step 5 using the new password.
37. Complete the following steps to install your SSH key:

1. Create folder: `mkdir -p ~/.ssh`
2. Create the file **/home/<*non-root user*>/.ssh/authorized_keys** and add your SSH key to it.
3. Change the ownership and permissions of the file:

   ```
   chmod 700 ~/.ssh/
   chmod 600 ~/.ssh/authorized_keys
   ```

38. Update the root password: `sudo passwd -u root`
39. Begin the ThreatQ v6 installation following the provided installation guide.

Change Log

Version numbers assigned to the change log entries below indicate document versions and not ThreatQ platform versions.

- **Version 2.0.0**
  - Support for RHEL 9.6
- **Version 1.0.1**
  - Image updates
- **Version 1.0.0**
  - Initial Release