

# ThreatQuotient



## ThreatQ Version 6 RHEL v9 Hardening Guide

**Version 1.0.1**

November 28, 2024

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

---

# Contents

Warning and Disclaimer ..... 3

About Security Hardening ..... 4

ThreatQ v6 RHEL v9 Hardening ..... 5

Change Log ..... 16

# 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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# About Security Hardening


This guide outlines recommendations for Security Hardening of ThreatQ v6 instances deployed in Red Hat Enterprise Linux (RHEL) 9.4 or later environments. 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.

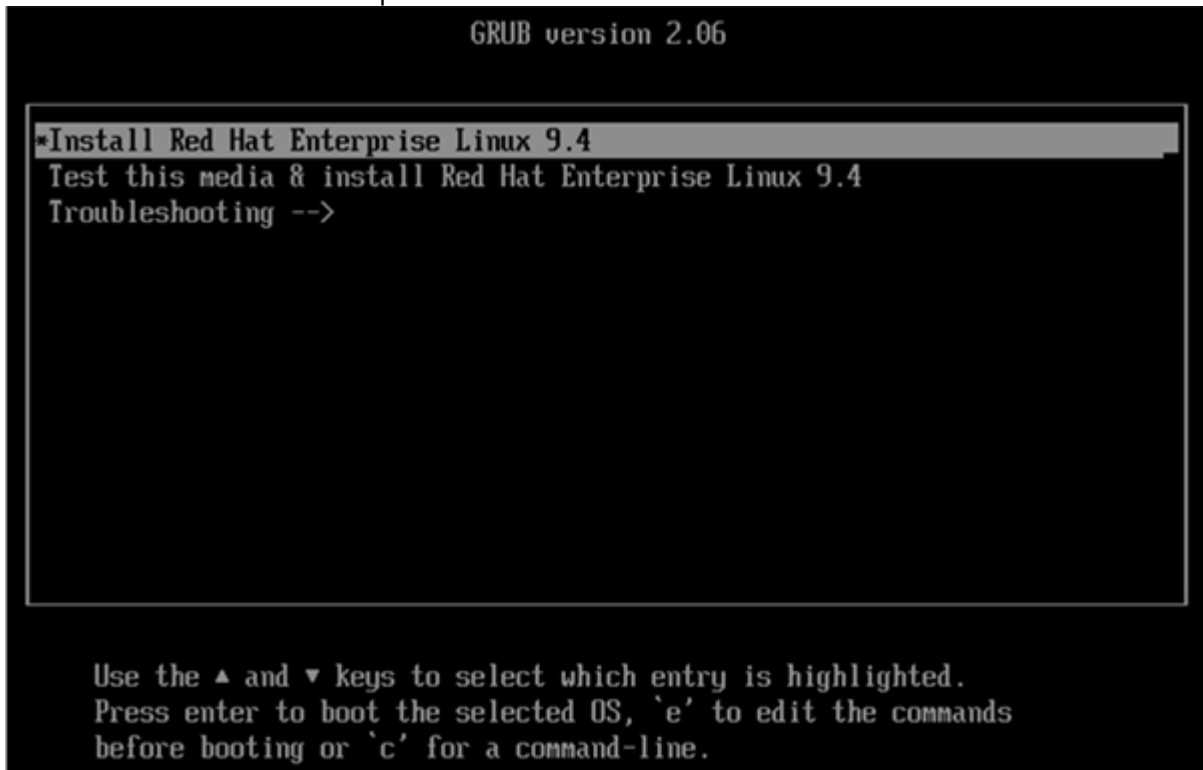
# ThreatQ v6 RHEL v9 Hardening

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

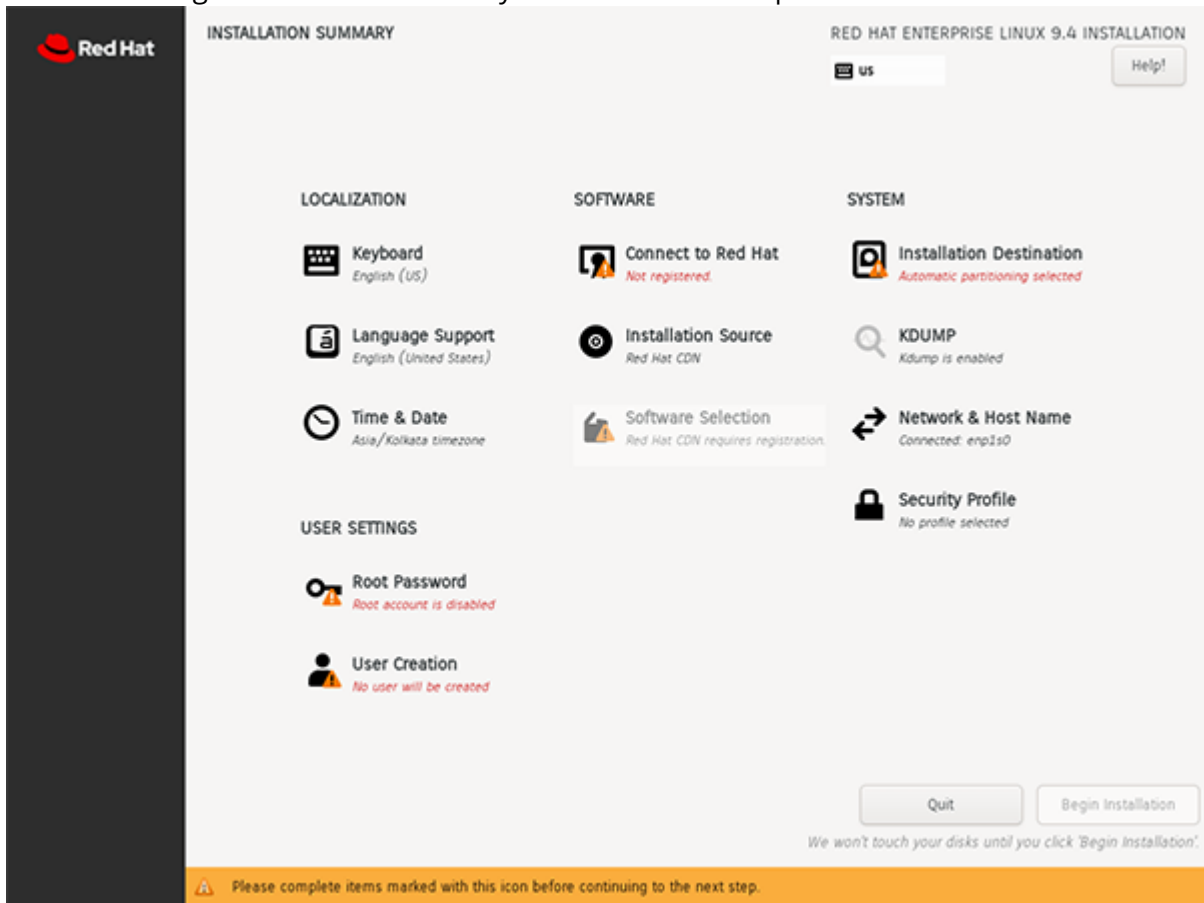
- CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 - Level 1 Server
- CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 - Level 2 Server
- DISA STIG for Red Hat Enterprise Linux 9 V1R2

 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 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.

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



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

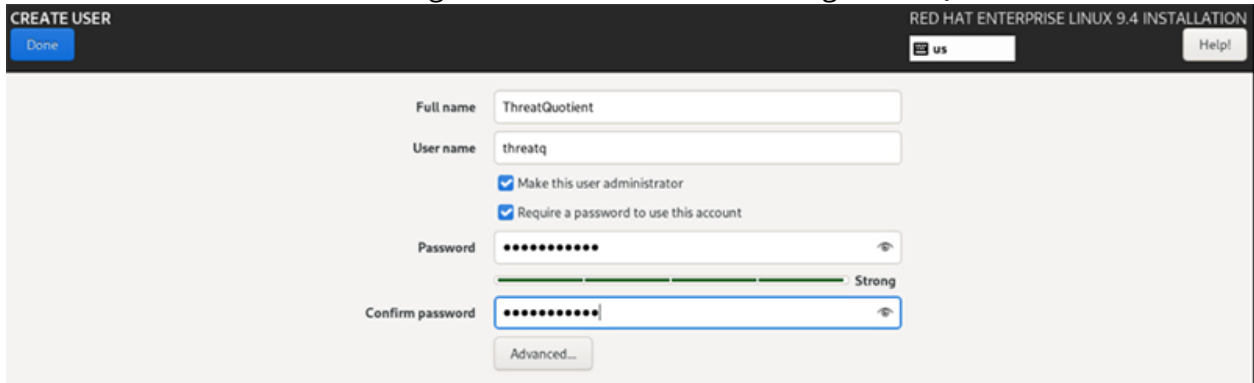


- Click **Time & Date** and select the **Etc/Greenwich Mean Time** timezone.

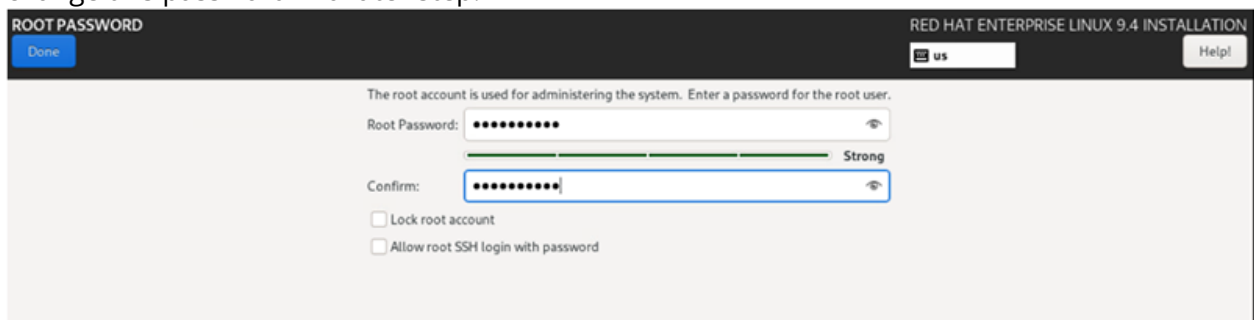


- To create a non-root user, click the **User Creation** option.

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

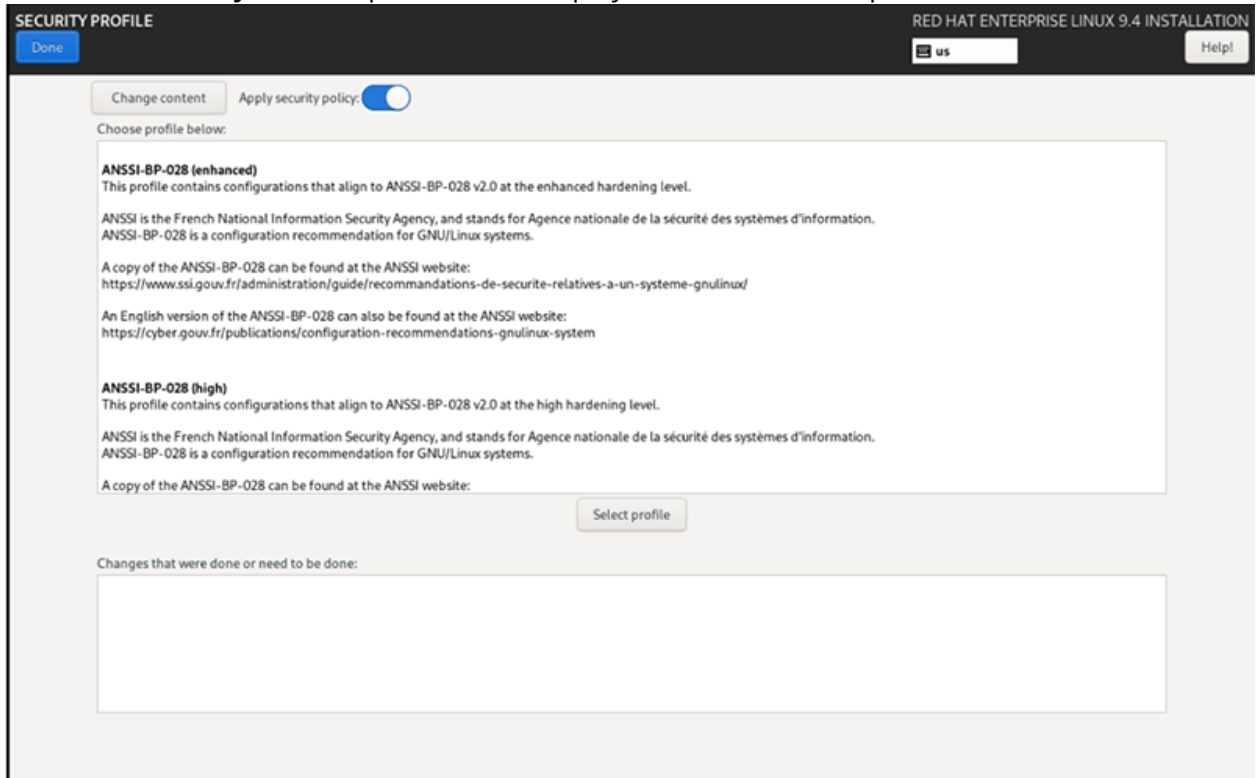


6. Enter a username and an initial password. You will be required to change this password on the first login.
7. Make sure the **Make this user administrator** and **Require a password to use this account** boxes are checked.
8. Click **Done** to save the settings and return to the main menu.
9. Click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



**SECURITY PROFILE** RED HAT ENTERPRISE LINUX 9.4 INSTALLATION

Done us Help

Change content Apply security policy: ☒

Choose profile below:


**ANSSI-BP-028 (enhanced)**  
 This profile contains configurations that align to ANSSI-BP-028 v2.0 at the enhanced hardening level.  
 ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.  
 ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.  
 A copy of the ANSSI-BP-028 can be found at the ANSSI website:  
<https://www.ssi.gov.fr/administration/guide/recommandations-de-securite-relatives-a-un-systeme-gnulinux/>  
 An English version of the ANSSI-BP-028 can also be found at the ANSSI website:  
<https://cyber.gouv.fr/publications/configuration-recommandations-gnulinux-system>

**ANSSI-BP-028 (high)**  
 This profile contains configurations that align to ANSSI-BP-028 v2.0 at the high hardening level.  
 ANSSI is the French National Information Security Agency, and stands for Agence nationale de la sécurité des systèmes d'information.  
 ANSSI-BP-028 is a configuration recommendation for GNU/Linux systems.  
 A copy of the ANSSI-BP-028 can be found at the ANSSI website:

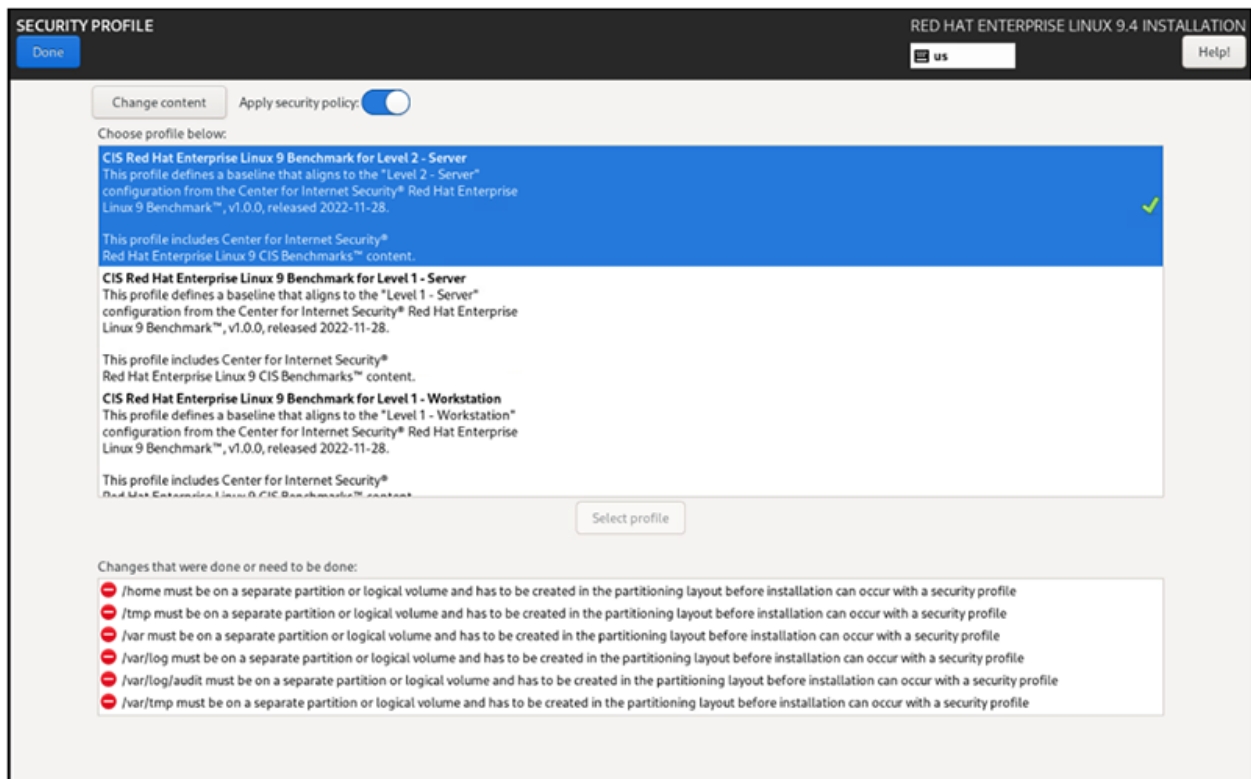
Select profile

Changes that were done or need to be done:

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.

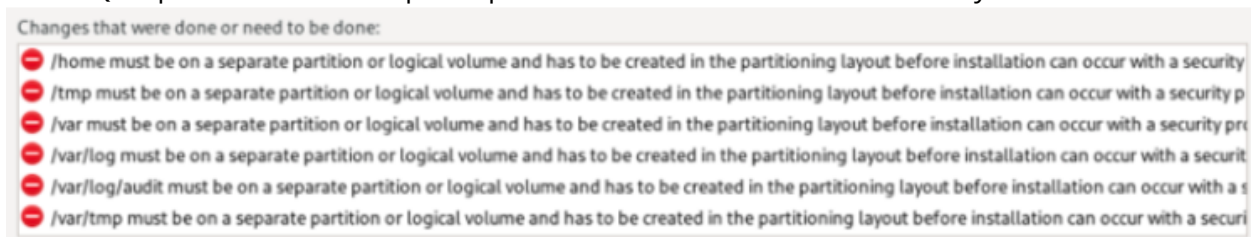




15. Select **Done** and return to the main menu.

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.



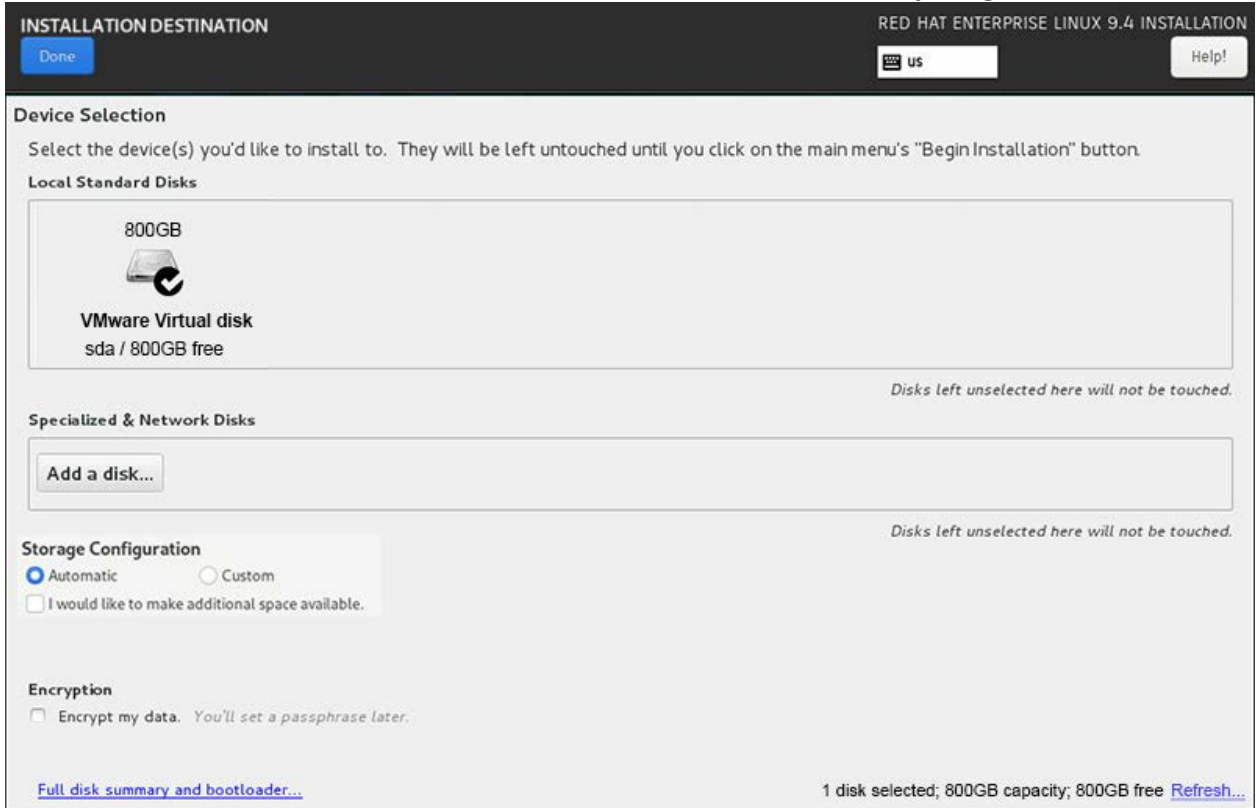
17. To create the required partitions, click the **Installation Destination** option from the main menu.

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.




**INSTALLATION DESTINATION** RED HAT ENTERPRISE LINUX 9.4 INSTALLATION

[Done](#) US [Help!](#)

**Device Selection**  
Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

**Local Standard Disks**

800GB  
  
**VMware Virtual disk**  
sda / 800GB free

*Disks left unselected here will not be touched.*

**Specialized & Network Disks**

[Add a disk...](#)

*Disks left unselected here will not be touched.*

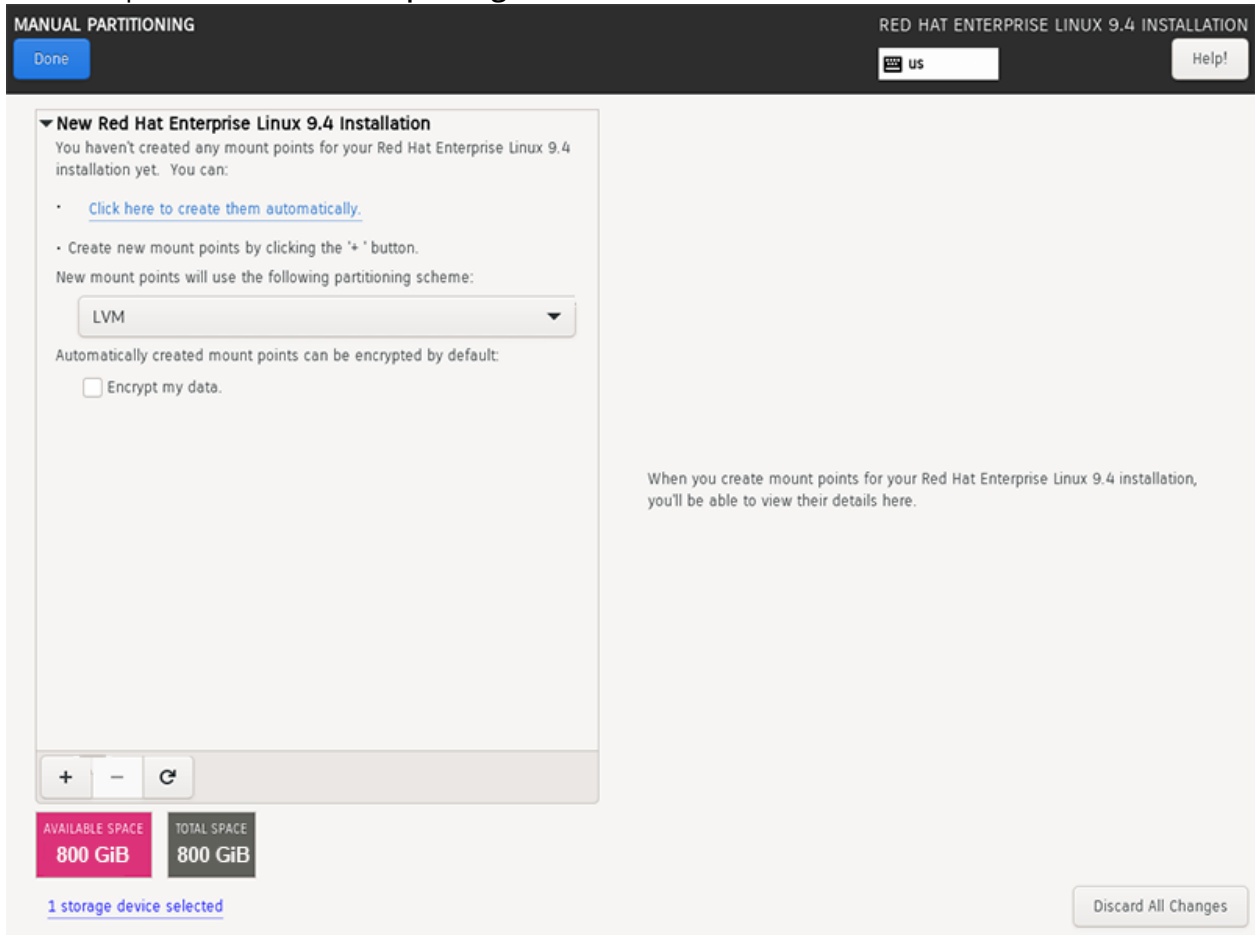
**Storage Configuration**  
☒ Automatic ☐ Custom  
☐ I would like to make additional space available.

**Encryption**  
☐ Encrypt my data. You'll set a passphrase later.


[Full disk summary and bootloader...](#) 1 disk selected; 800GB capacity; 800GB free [Refresh...](#)

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**.

### SUMMARY OF CHANGES

Your customizations will result in the following changes taking effect after you return to the main menu and begin installation:

Order	Action	Type	Device	Mount point
1	destroy format	Unknown	QEMU QEMU HARDDISK (sda)	
2	create format	partition table (MSDOS)	QEMU QEMU HARDDISK (sda)	
3	create device	partition	sda1 on QEMU QEMU HARDDISK	
4	create device	partition	sda2 on QEMU QEMU HARDDISK	
5	create format	physical volume (LVM)	sda2 on QEMU QEMU HARDDISK	
6	create device	lvmvg	rhel_host-10-114-3-4	
7	create device	lvm lv	rhel_host-10-114-3-4-swap	
8	create format	swap	rhel_host-10-114-3-4-swap	
9	create device	lvm lv	rhel_host-10-114-3-4-var_log_audit	
10	create format	xfs	rhel_host-10-114-3-4-var_log_audit	/var/log/audit
11	create device	lvm lv	rhel_host-10-114-3-4-var_tmp	
12	create format	xfs	rhel_host-10-114-3-4-var_tmp	/var/tmp
13	create device	lvm lv	rhel_host-10-114-3-4-home	
14	create format	xfs	rhel_host-10-114-3-4-home	/home
15	create device	lvm lv	rhel_host-10-114-3-4-tmp	
16	create format	xfs	rhel_host-10-114-3-4-tmp	/tmp
17	create device	lvm lv	rhel_host-10-114-3-4-var_log	

Cancel & Return to Custom Partitioning
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.

SECURITY PROFILE
Done
RED HAT ENTERPRISE LINUX 9.4 INSTALLATION
us
Help!

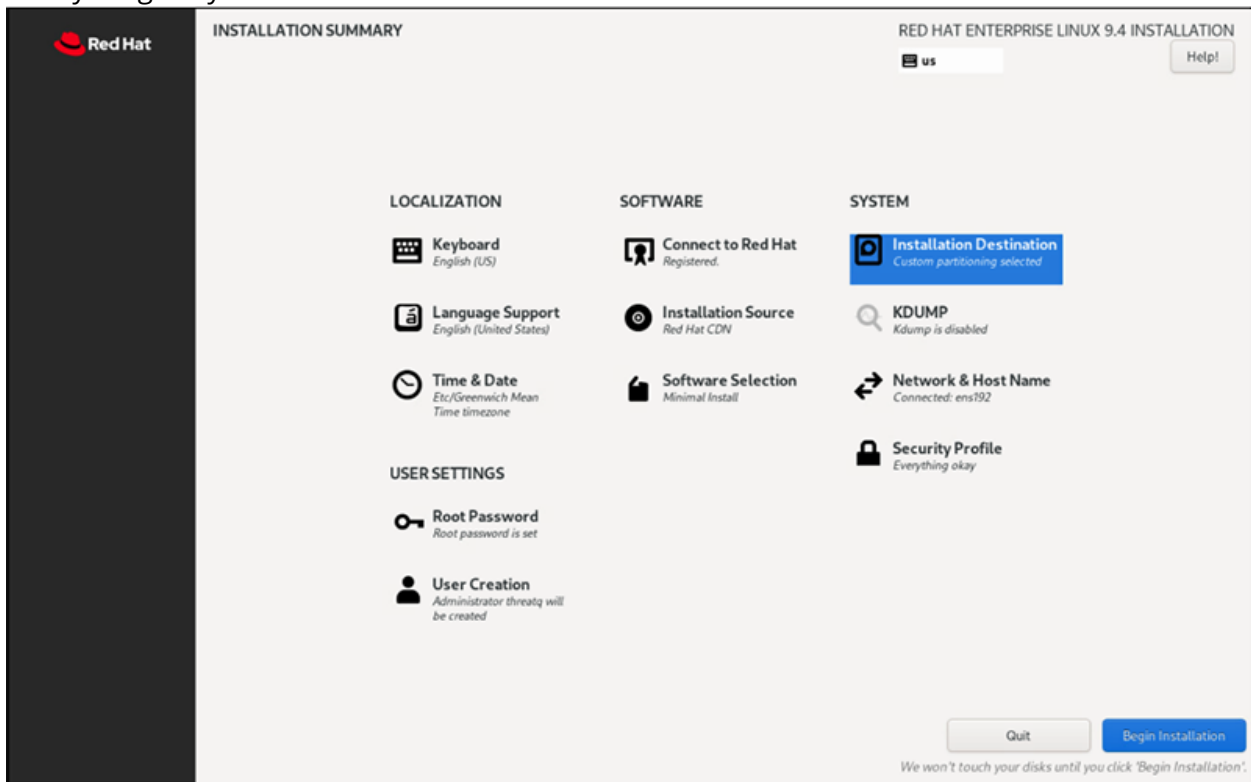
Change content
Apply security policy:

Choose profile below:  
intermediate, and advanced levels.  
**CCN Red Hat Enterprise Linux 9 - Intermediate**  
This profile defines a baseline that aligns with the "Intermediate" configuration of the CCN-STIC-610A22 Guide issued by the National Cryptological Center of Spain in 2022-10.  
The CCN-STIC-610A22 guide includes hardening settings for Red Hat Enterprise Linux 9 at basic, intermediate, and advanced levels.  
**CIS Red Hat Enterprise Linux 9 Benchmark for Level 2 - Server**  
This profile defines a baseline that aligns to the "Level 2 - Server" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.  
This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content. ✓  
**CIS Red Hat Enterprise Linux 9 Benchmark for Level 1 - Server**  
This profile defines a baseline that aligns to the "Level 1 - Server" configuration from the Center for Internet Security® Red Hat Enterprise Linux 9 Benchmark™, v1.0.0, released 2022-11-28.  
This profile includes Center for Internet Security® Red Hat Enterprise Linux 9 CIS Benchmarks™ content.

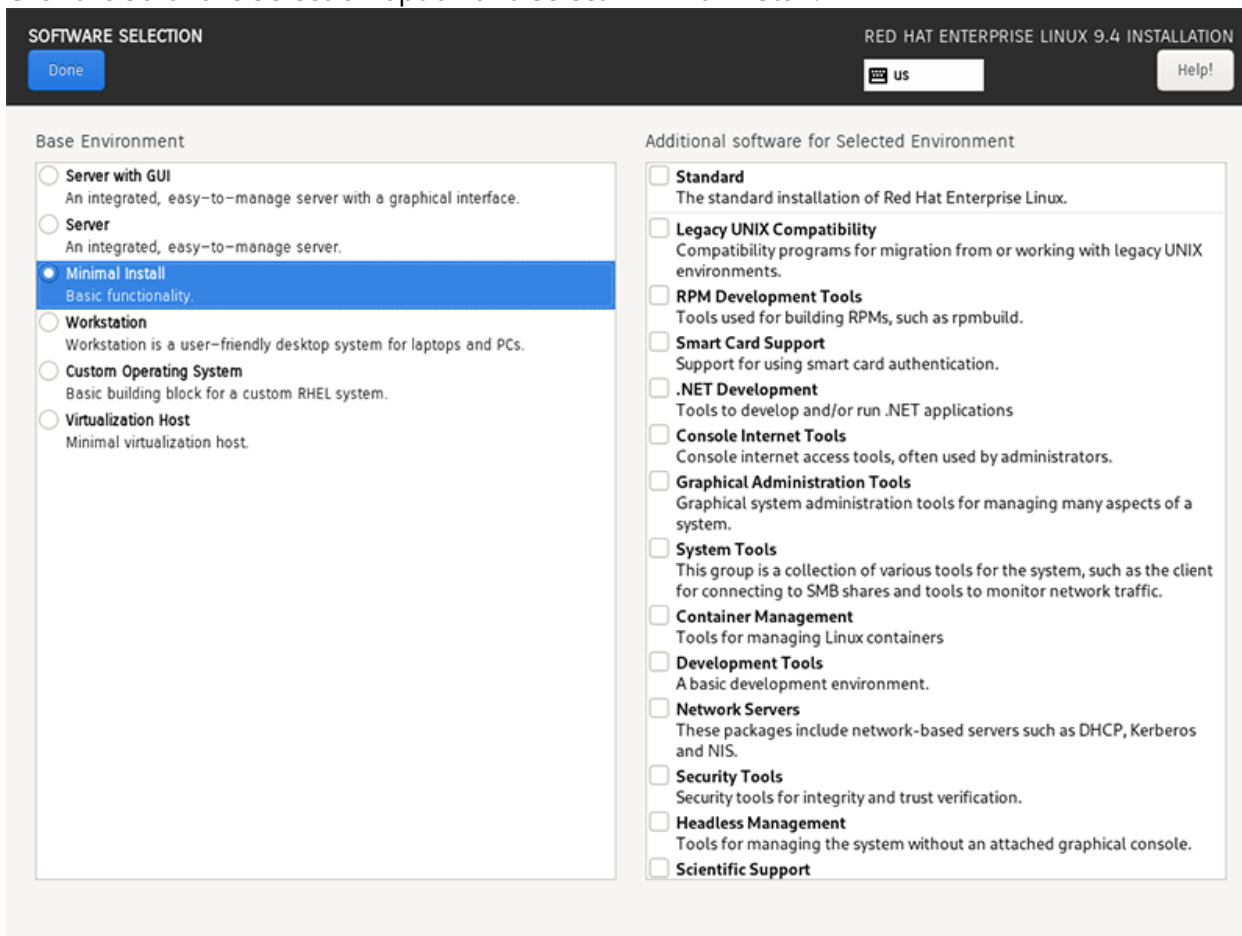
Select profile

Changes that were done or need to be done:  
mount option 'nodev' added for the mount point /home  
mount option 'nosuid' added for the mount point /home  
mount option 'nodev' added for the mount point /home  
mount option 'nosuid' added for the mount point /home  
mount option 'nodev' added for the mount point /tmp  
mount option 'noexec' added for the mount point /tmp

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**.



**SOFTWARE SELECTION** RED HAT ENTERPRISE LINUX 9.4 INSTALLATION

Done us Help!

**Base Environment**

- ☐ **Server with GUI**  
An integrated, easy-to-manage server with a graphical interface.
- ☐ **Server**  
An integrated, easy-to-manage server.
- ☒ **Minimal Install**  
Basic functionality.
- ☐ **Workstation**  
Workstation is a user-friendly desktop system for laptops and PCs.
- ☐ **Custom Operating System**  
Basic building block for a custom RHEL system.
- ☐ **Virtualization Host**  
Minimal virtualization host.

**Additional software for Selected Environment**

- ☐ **Standard**  
The standard installation of Red Hat Enterprise Linux.
- ☐ **Legacy UNIX Compatibility**  
Compatibility programs for migration from or working with legacy UNIX environments.
- ☐ **RPM Development Tools**  
Tools used for building RPMs, such as rpmbuild.
- ☐ **Smart Card Support**  
Support for using smart card authentication.
- ☐ **.NET Development**  
Tools to develop and/or run .NET applications
- ☐ **Console Internet Tools**  
Console internet access tools, often used by administrators.
- ☐ **Graphical Administration Tools**  
Graphical system administration tools for managing many aspects of a system.
- ☐ **System Tools**  
This group is a collection of various tools for the system, such as the client for connecting to SMB shares and tools to monitor network traffic.
- ☐ **Container Management**  
Tools for managing Linux containers
- ☐ **Development Tools**  
A basic development environment.
- ☐ **Network Servers**  
These packages include network-based servers such as DHCP, Kerberos and NIS.
- ☐ **Security Tools**  
Security tools for integrity and trust verification.
- ☐ **Headless Management**  
Tools for managing the system without an attached graphical console.
- ☐ **Scientific Support**

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.

# Change Log



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

- **Version 1.0.1**
  - Image updates
- **Version 1.0.0**
  - Initial Release