National Security Agency | Cybersecurity Report

TENS Virtual Machine Guide

Introduction

The United States Air Force Trusted End Node Security (TENS) solution allows authorized DoD teleworkers to connect to DoD sites and services from an untrusted computer [1]. Some DoD teleworkers may not have Government Furnished Equipment (GFE) for telework use. NSA recommends using TENS to boot into a temporary, trusted operating system to connect to DoD sites and services over using the operating system of an untrusted computer.

Booting TENS from removable media is the recommended method of using TENS. Some users may not be able to use TENS if their computer is not able to boot from removable media or if their computer uses UEFI Secure Boot, which is not currently supported by TENS. Some users may be able to disable Unified Extensible Firmware Interface (UEFI) Secure Boot allowing TENS to boot, but disabling Secure Boot increases the risk of the operating system being successfully compromised by boot malware.

The Air Force is working to get TENS to load when a computer uses UEFI Secure Boot, but until then, this guide provides instructions for configuring a virtual machine to boot TENS. Once TENS supports computers with UEFI Secure Boot enabled, NSA strongly recommends booting TENS using the removable media method instead of a virtual machine. Running TENS in a virtual machine, even as described in this guide, allows an adversary who has compromised the user's computer to observe all activity within the virtual machine using techniques such as screen capture and key logging. Note that the TENS FAQ states that using a virtual machine is considered an unsupported platform [2]:

> *Can I run TENS in a virtual machine?*
>
> *In general, yes, but this is not encouraged since kernel malware on the host can still be a threat. You should be able to take the ISO image and mount it as virtual CD within a virtualized environment and then tell the VM to boot from the image. We use these environments for development and quick testing, but have not formally qualified it as a supported platform. You are welcome to experiment, but keep in mind that this is not as secure as booting directly into TENS. We aren't certain all necessary hardware components (such as CAC readers) will work properly, or that you will see higher video resolutions. We consider virtual machines an unsupported platform.*

Prerequisites

The following requirements need to be met by virtualization software in order to use TENS and authenticate to DoD sites and services:

1. The software must have a no-cost license.
2. The no-cost license of the software must allow government use.
3. The no-cost license of the software must be able to pass through USB smart card reader devices from the host operating system to the guest operating system running TENS so that Common Access Cards (CAC) or Personal Identity Verification (PIV) cards can be used in TENS to connect to DoD sites and services.
4. The licensed software must provide cross-platform support for multiple host operating system vendors.
5. The licensed software must be supported by the vendor.

Oracle®[1] VirtualBox® [3] is one example virtualization software that meets the above requirements. This guide describes how to run TENS 3.0.1 Public Deluxe [4] within VirtualBox 6.1.8. Any compatible virtualization software may be used as long as the prerequisites are met, though at the time of this writing NSA was unable to identify other software which met these inherent prerequisites for home telework use. Before getting started:

1. Download and install the VirtualBox platform package for the host operating system.
2. Download the TENS Public Deluxe ISO file or acquire a TENS CD/DVD from your organization.
3. Obtain a USB smart card reader and a PIV smart card, such as a CAC.

[1] Oracle and VirtualBox are registered trademarks of Oracle and/or its affiliates.

This guide does not cover installation of VirtualBox, but the default installation options for VirtualBox should be correct for most users. Pay attention to any prompts during the installation process. VirtualBox may prompt the user to grant permissions in order to proceed during and after the installation process. The permissions requested by VirtualBox are necessary for VirtualBox to operate correctly.

Note that the license for the VirtualBox Extension Pack, which adds support for USB 2.0 and USB 3.0, does not allow commercial or government use for free. USB smart card readers should be backwards compatible with USB 1.1 which is supported by VirtualBox by default.

Users who install VirtualBox on Linux®[2]-based operating systems need to perform an important configuration change before proceeding with configuring a virtual machine for TENS. The configuration change allows the user to add a USB smart card reader to the virtual machine. Open a terminal and run the following command to add the current user to the vboxusers group:

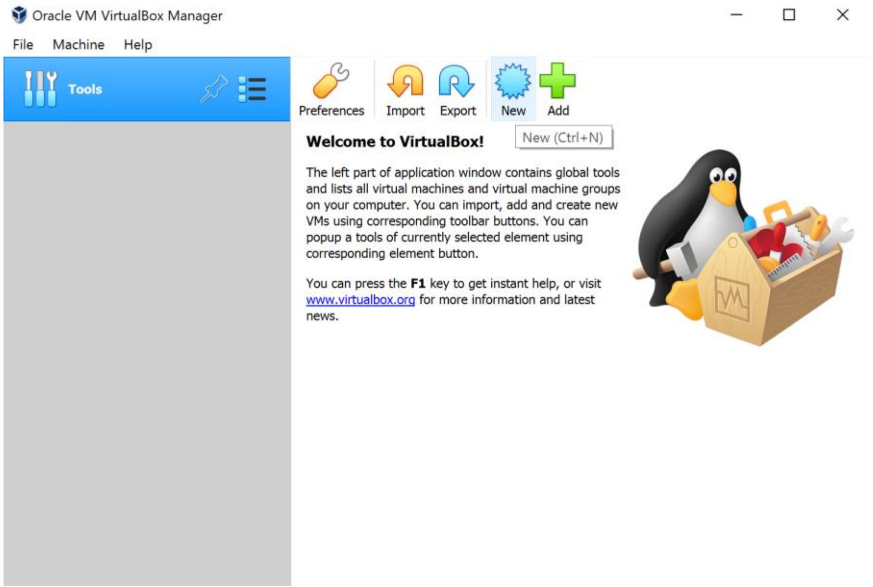
```
        sudo adduser $USERNAME vboxusers
```

Restart the computer after running the command.

Users who install VirtualBox on macOS®[2] may have to grant system extension installation privileges to Oracle Corporation. If granting privileges is required, then a warning box will display during the installation process. The installation process may need to be started again after the privileges are granted.

Configuring a Virtual Machine for TENS

At this point, all prerequisites have been completed for configuring a virtual machine for TENS. Open VirtualBox and click on the blue **New** icon in the **Oracle VM VirtualBox Manager** dialog, displayed in Figure 1, which starts the process for configuring a new virtual machine.



Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

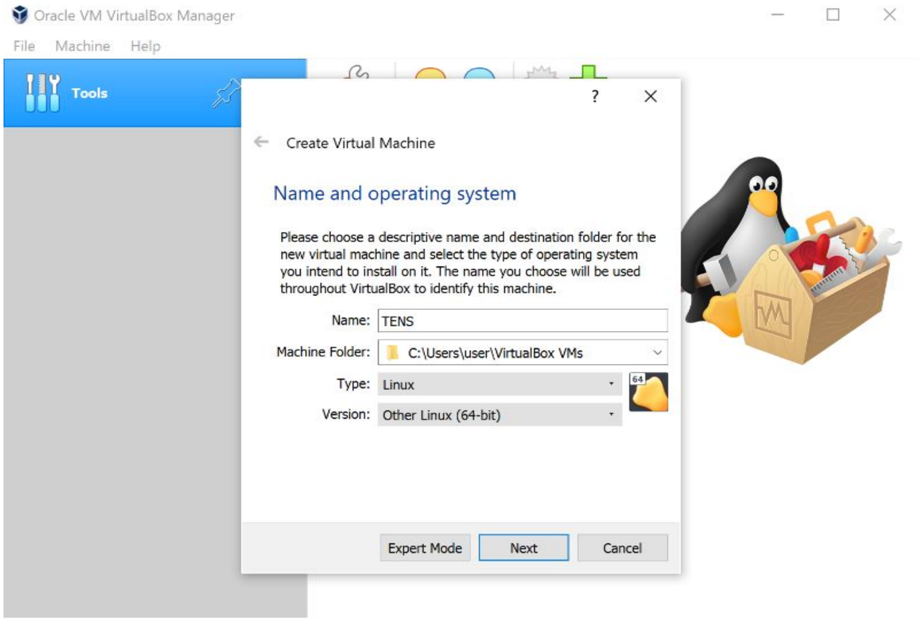
You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

*Figure 1: The **Oracle VM VirtualBox Manager** dialog with the **New** icon that starts the machine creation process.*

Complete the fields in **Name and operating system dialog** as displayed in Figure 2. Enter a name, such as **TENS**, in the **Name** field. Change the **Machine Folder** field value if desired. Select **Linux** from the **Type** drop down menu. Select

[2] Linux is the registered trademark of Linus Torvalds in the U.S. and other counties. macOS is a trademark of Apple Inc., registered in the U.S. and other countries. Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Other Linux (64-bit) from the **Version** drop down menu. Click the **Next** button (Windows®[2] or Linux) or **Continue** button (macOS).



Create Virtual Machine

Name and operating system

Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: TENS

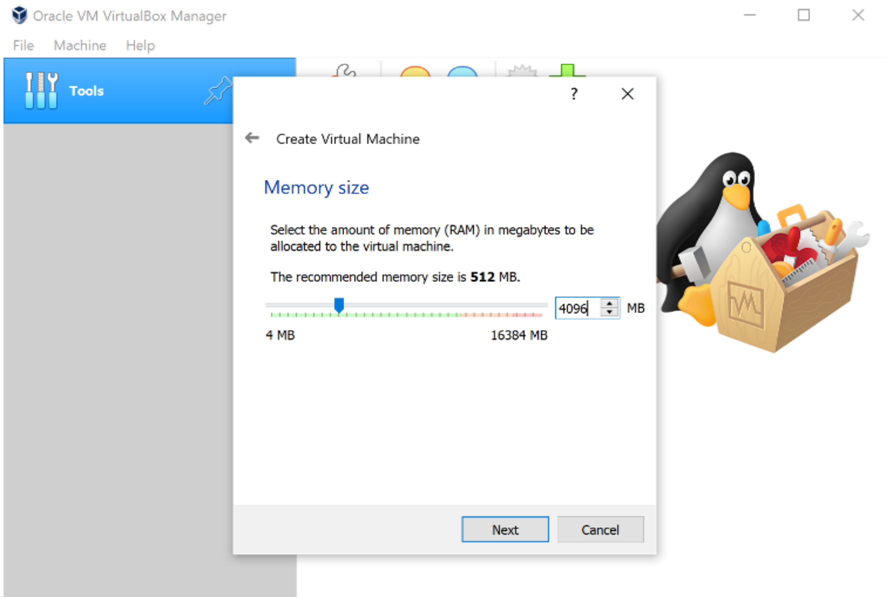
Machine Folder: C:\Users\user\VirtualBox VMs

Type: Linux

Version: Other Linux (64-bit)

*Figure 2: The **Name and operating system** dialog with correct values.*

The default memory size of 512MB is not enough memory for TENS. A minimum of 1.5GB is recommended for TENS Public Deluxe. Allowing more memory to be used by TENS improves the performance of TENS. Entering a value of 4096 into the text field, as displayed in Figure 3, allows the virtual machine to use 4GB of memory. Note that the text field does not allow entering a number greater than the amount of memory available in the host computer. Click the **Next** button or **Continue** button.



Create Virtual Machine

Memory size

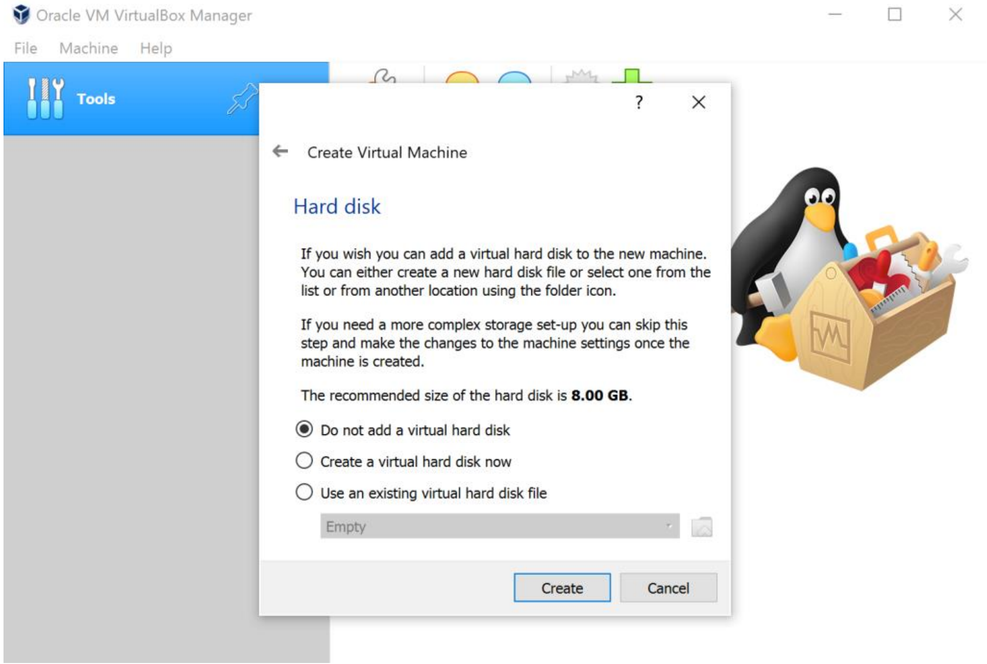
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512** MB.

4096 MB

*Figure 3: The **Memory size** dialog with **4096** (4GB) entered as a value.*

At the **Hard disk** dialog, select the **Do not add a virtual hard disk** radio button, as displayed in Figure 4, and click the **Create** button.



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

● Do not add a virtual hard disk

○ Create a virtual hard disk now

○ Use an existing virtual hard disk file

Empty

*Figure 4: The **Hard disk** dialog with the **Do not add a virtual hard disk** radio button selected.*

After clicking the **Create** button, a warning dialog will display asking if the virtual machine should be created without virtual a hard disk. Since TENS is designed to operate without using a hard disk, click the **Continue** button to proceed. A virtual machine named TENS has been created.

Right click on the **TENS** virtual machine entry in the **Oracle VM VirtualBox** dialog and choose **Settings…** from the menu as displayed in Figure 5.

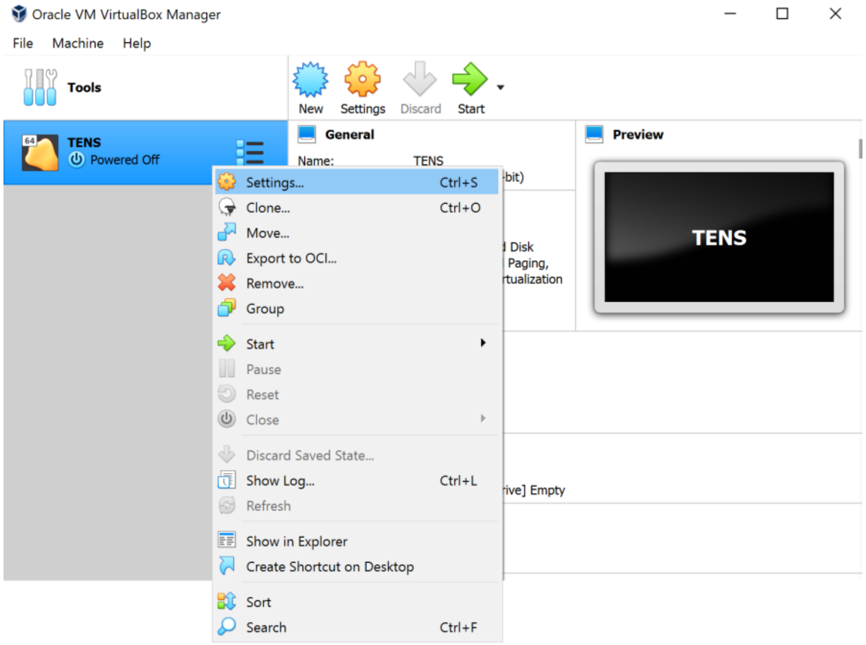
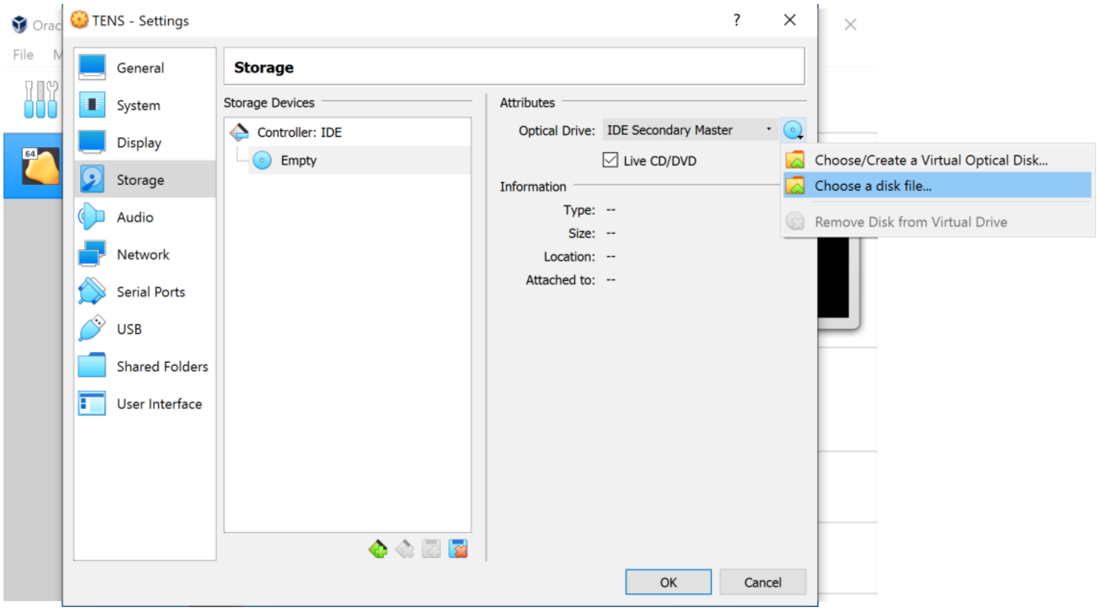


*Figure 5: The **Settings…** option in the TENS virtual machine menu.*

Click the **Storage** icon from the list of configuration options as displayed in Figure 6. Note that the icons for the configuration options may appear as a row (macOS) of icons or as a column (Linux or Windows) of icons depending on the host operating system.

Once the Storage icon has been clicked, the **TENS - Settings** dialog will show a device named **Controller: IDE** under the list of storage devices as displayed in Figure 6. Below the IDE controller entry, there is a CD/DVD icon that will usually be labeled **Empty** unless a CD/DVD is inserted into the computer's CD/DVD drive. Click the CD/DVD icon. Select the **Live CD/DVD** checkbox in the **Attributes** area on the right side of settings dialog.

If using an ISO file, then click the CD icon to the right of the **Optical Drive** label, and select the **Choose a disk file…** option from the menu as displayed in Figure 6. Navigate to the location of the TENS ISO file on the host operating system and click the **Open** button to select the ISO file.



TENS - Settings

Storage

Storage Devices

Controller: IDE

Empty

Attributes

Optical Drive: IDE Secondary Master

☑ Live CD/DVD

Information

Type: --

Size: --

Location: --

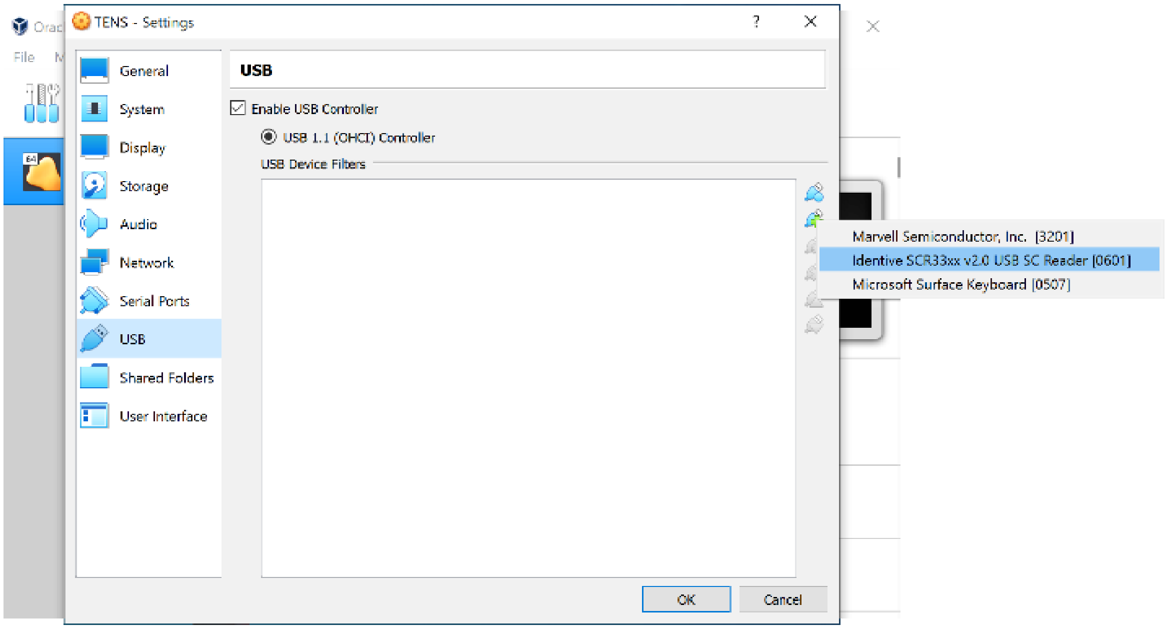
Attached to: --

*Figure 6: The **Choose a disk file** option.*

If using a physical CD/DVD, then click the CD icon to the right of the **Optical Drive** label, and select the **Host Drive 'D:'** option from the menu. Note that the CD/DVD drive letter may be a different letter.

To configure the TENS virtual machine to access the computer's USB smart card reader, choose the **USB** icon from the column (if using Linux or Windows) of icons in the **TENS – Settings** dialog as displayed in Figure 7. macOS users will first need to select the **Ports** icon, and then select the **USB** tab to reach the same settings dialog. The **Enable USB Controller** checkbox should already be selected as displayed in Figure 7. The **USB 1.1 (OHCI) Controller** radio button should be selected by default.

The **USB Device Filters** section of the settings dialog will initially be empty. If the smart card reader is an external device, rather than integrated into the computer (e.g. part of the keyboard or built into a laptop), then plug in the smart card reader into a USB port on the computer. Select the blue USB connector icon that contains a green plus symbol on the right side of the **USB Device Filters** section. A list of all currently connected USB devices will be listed. Select the smart card reader from the list as displayed in Figure 7. The smart card reader may be a generic name or a specific smart card reader model device name. Once the smart card reader has been identified and selected, click the **OK** button to save the configuration.



USB

☑ Enable USB Controller

● USB 1.1 (OHCI) Controller

USB Device Filters

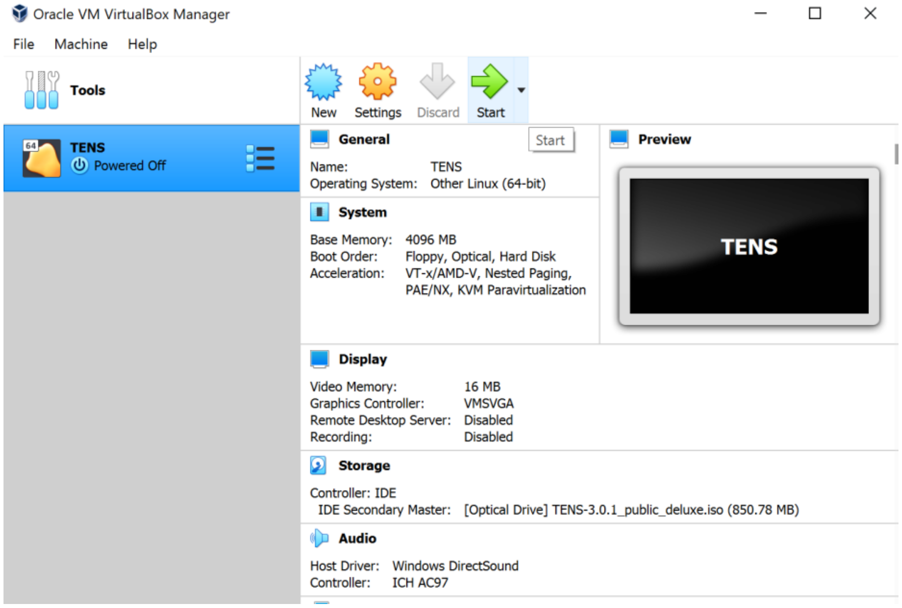
- Marvell Semiconductor, Inc. [3201]
- Identive SCR33xx v2.0 USB SC Reader [0601]
- Microsoft Surface Keyboard [0507]

Figure 7: USB smart card reader device selected in the USB configuration section of the ***TENS – Settings*** *dialog.*

If a smart card reader is not found in the list of devices, then unplug and plug-in the external USB smart card reader and try again. Once the smart card reader device has been found and configured using the steps above, then the TENS virtual machine has been successfully configured for use. If other USB-based devices, such as webcams, are needed for collaboration, then the devices can be added using similar steps.

Using TENS in a Virtual Machine

Do not insert the smart card into smart card reader before starting the TENS virtual machine. If using an external USB smart card reader, then do not plug in the smart card reader into the computer yet. Select the **TENS** virtual machine entry in the **Oracle VM VirtualBox Manager** dialog and click the green **Start** arrow icon, as displayed in Figure 8, to start the virtual machine.



TENS
Powered Off

General

Name: TENS
Operating System: Other Linux (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

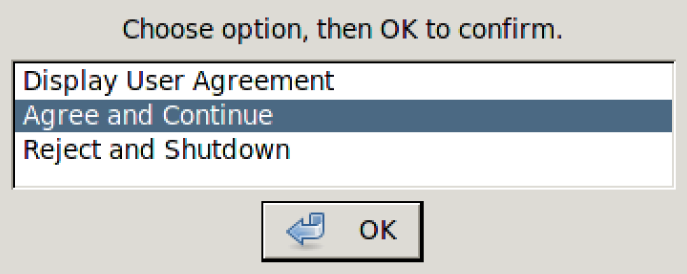
Controller: IDE
IDE Secondary Master: [Optical Drive] TENS-3.0.1_public_deluxe.iso (850.78 MB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Figure 8: The ***Start*** *icon used to start the virtual machine.*

Wait for TENS to boot to the point where the TENS user agreement dialog, as displayed in Figure 9, is presented before plugging in an external smart card reader. Once the user agreement dialog displays in TENS, plug in the external smart card reader, and click the **OK** button to accept the agreement to finish the TENS boot process.



Choose option, then OK to confirm.

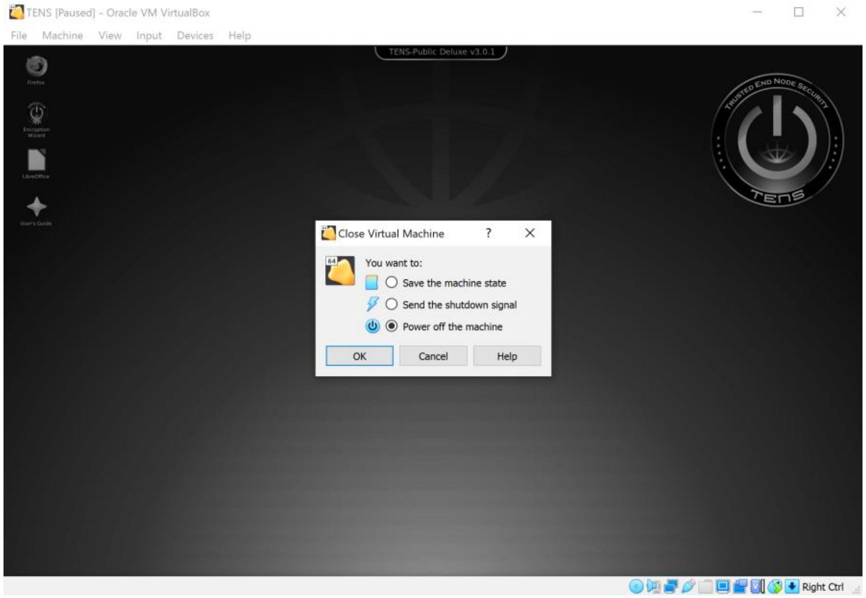
- Display User Agreement
- Agree and Continue
- Reject and Shutdown

Figure 9: TENS user agreement dialog.

Note that a dialog may display on macOS asking to grant VirtualBox permission to monitor keystrokes. Grant the permission. VirtualBox may need to be restarted to use the permission.

Use the TENS virtual machine to perform authorized DoD telework tasks. Insert the smart card into the smart card reader only when needed. Remove the smart card from the smart card reader whenever the smart card is not being actively used (e.g. logging into a protected site or signing an email). Once telework tasks are complete, ensure all work is saved to an authorized location as the data will be lost after TENS is shut down. Before shutting down the TENS virtual machine, ensure the smart card is removed from the reader and unplug the smart card reader from the host if using an external smart card reader.

To shut down the virtual machine, select the shutdown option from within the TENS environment by clicking the **Start** menu and selecting **Shutdown**. Alternatively, close the window of the running TENS virtual machine instance by clicking the X icon in the upper right corner of the TENS instance. When using the X icon to close the running TENS virtual machine instance, choose the **Power off the machine** radio button at the **Close Virtual Machine** dialog, as displayed in Figure 10, and then click the **OK** button. Do not select the **Save the machine state** radio button because saving machine state could leave sensitive data in virtual machine files on the host.



TENS [Paused] - Oracle VM VirtualBox

Close Virtual Machine

You want to:

○ Save the machine state
○ Send the shutdown signal
● Power off the machine

*Figure 10: The **Close Virtual Machine** dialog.*

Remember to leave the smart card reader unplugged from the host computer when the TENS virtual machine is not in use and remove the smart card from the smart reader when the smart card is not being used.

Works Cited

[1] Air Force Research Laboratory (2020). Trusted End Node Security. [Online] Available at: https://tens.af.mil/lipose.htm [Accessed May 20, 2020]

[2] Air Force Research Laboratory (2020). Trusted End Node Security - FAQs. [Online] Available at: https://tens.af.mil/liposeFAQ.htm [Accessed May 20, 2020]

[3] Oracle (2020). Downloads – Oracle VM VirtualBox. [Online] Available at: https://virtualbox.org/downloads [Accessed May 20, 2020]

[4] Air Force Research Laboratory (2020). Trusted End Node Security - Downloads. [Online] Available at: https://tens.af.mil/download.htm [Accessed May 20, 2020]

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov