VMware Health and Security Toolkit

User Guide

Version 1.0.4

August 28, 2026

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

Download Link **5**
Release Notes **5**
Checksum Details **8**
1. Introduction to VMware HST **9**
1.1. Overview 9
1.2. Accessing VMware HST 9
2. Installation and Configuration **10**
2.1. Java Based Installation and Configuration 10
2.1. Prerequisites to Run Security Assessment (SA) on JAR 13
2.2. Virtual Appliance Based Deployment and Configuration 14
2.3. Pre-Scan Configuration and Account Permissions 19
2.4. vCenter Custom Role Privileges (Recommended Best Practice) 19
2.5 Modifying collection.properties: 20
2.6 Port Requirements for HST: 21
2.7 Memory Configuration for HST: 21
3. Using the HST Application **23**
3.1. Login Options 23
3.1.1 Customer Login 24
3.1.2 Broadcom or Partner Login (via SSO) 25
3.1.3 Offline Login 25
3.2. The Project Explorer Page 27
3.2.1. Navigating the Dashboard: 27
3.2.2. Folder Management (Create, Import): 28
3.2.3 Folder Display and Organization **29**
4. Creating a new project 29
4.1 Creating a new TDM or VHA Project 30
4.1.1 Applying Credentials in Bulk 32
4.2 Creating a new Security Assessment (SA) Project 34
4.2.1 Additional Host Details for Security Assessment (SA) Workflows 36
4.4. Monitoring the Host Collection Process 38
5. Monitor Collection Status **38**
6. Status Indicators **40**
7. Analysis and Reporting Tabs **40**
8. Data Management Overview **40**
9. Generating Reports **41**
9.1 Status Indicators 42
10. Health Analyzer Tab **43**
10.1 Best Practices Section 43
10.2 Filtering and Reporting 44

10.3 Health Check Analysis 45
10.4 Bulk Update Include In Report Flag 45
11. Security Assessment Tab Guide 46
11.1 Detailed Control View 47
11.2 Using Filters and Export 48
11.3 Summary View 48
11.4 Steps to Download Executive and Administrative Reports 48
12. Project and Folder Management 51
12.1 Project Explorer Actions 51
12.2 Project-Level Options 52

Download Link

https://www.broadcom.com/support/oem/vmware/health-security-toolkit

Release Notes

Version	Date	Updates
1.0.4 Build 25699684		Updated Release ● Changed the default behavior of SSH to not start with the host ● Increased the default appliance size from 5GB RAM to 8GB RAM, as this provides a better experience for most of the environments. For inventories >30k objects, additional RAM may be needed. ● Implemented new TDM - VMs tab - fields RpHasNamespace and ManagedBy to identify VMs as being managed by WCP / VKS ● Fixed HST application freezing issue when trying to open the Best Practice with a large number of rows. ● Fixed the issue of “Send Data to Broadcom” failing for large projects. ● Fixed an issue where root was not added to the wheel group and could not login over SSH ● Fixed the issue of TDM - Hosts tab - cpuGhz was incorrectly computed. ● Improved logging of failures to identify the Host and iSCSI HBA when iSCSI manager API failure occur ● Fixed issue with health analysis excel report issue for large tables which have more than 1048576 rows ● Fixed issue in TDM excel report where serviceTag coming as N/A, CPU Type was duplicated, and storageCommitted/storageUncommitted were zero when both TDM and VHA were selected for data collection in the project. ● Health Analyzer finding updates: ○ Fixed issue with ESXI-005 triggering false positives for the setting key Misc.SIOControlFlag2. ○ Fixed issue with ST-012 - not generating findings for vSphere 8.0 ○ Fixed issue with VC-017 finding to create the finding correctly considering scalable configuration and providing scalable settings in the Resource Pool Hierarchy Info table ○ Fixed issue with Licensing Summary usage column - LIC-001, LIC-002 ○ Fixed issue with NE-003 where observation text incorrectly included "VMKernel" even when the issue was not related to a

		VMKernel port group ○ Fixed the issue of triggering false positives for the finding ST-013 (NfsIscsiTrafficSeparation) ○ Fixed the issue of triggering false positives for the finding VM-003 (VmVmotionReq) ● Health Analysis word report findings are sorted with priority and then the component, and spelling mistakes are corrected. ● Resolved issue in the Security Assessment module with the NSX Administrator report failing to download. ● Resolved issues in the Security Assessment module with vCenter scans returning a status of “Not Reviewed” for several controls. ● This release contains various security enhancements.
1.0.3 Build 25090906	2025-12-06	Updated Release ● HST now supports bulk selection to include or exclude findings of components and grade from the report. Refer to section 10.4 of this user guide for more information. ● Fixed “unknown error” when saving the observation text in Health Analyzer ● Security improvements for storing local user credentials in the virtual appliance ● Bugfix: Removed automatic inclusion of OK findings from the vHA report ● VMware HST now allows the user to remove vCenter with no inventory. The tool will throw an error “No inventory found for this vCenter”, so that the user can delete the vCenter before exporting the report. ● Performance improvement for large vHA collection by sequentially importing data ● Health Analyzer finding updates: ○ NE-003 - NSX managed portgroups are now excluded from findings ○ SEC-014 - Removed this best practice from vSphere 8.0 and 7.0 catalogs as it is no longer applicable ○ Bugfix, VC-005 was incorrectly counting VMs for this finding, which is has been fixed in this release ○ Bugfix, VM-014 - VMs starting with the name vcls (and in a virtual machine folder named vCLS) are now suppressed from findings ○ VM-016 - guestToolsUnmanaged and guestToolsSupportedNew will not trigger finding ○ vSAN-018 - finding will be triggered when the hostFailuresToTolerate < 1

		○ vSAN-023 - Adjusted grade of this finding to appropriate raise P3 based on the condition ● Security Assessment - both info and INFO will be considered as passed for control NSX 100607 ● Security controls issue fixed for ESXi, VC, VM, and vSAN ● Fixed null pointer exception in the NSX controls ● Fixed the issue with telemetry
1.0.2 Build 24965143	2025-09-20	Updated Release ● HST now supports deleting the running TDM/VHA projects ● When collecting data with HST, selecting the anonymize button will not allow the VHA collection to be selected. ● HST now supports changing existing local user password ● HST collection will not reach the 5480 port instead it will use the sessionId generated for getting the monitoring, health, storage data ● Now users can import the large projects by increasing the memory configuration defined in user guide ● Fixed data issue in TDM report DVS detail, such as vmCount and numHosts when TDM and VHA are selected for collection ● Download time of VHA excel report was improved ● Collection will throw an error if user provided the ESXI host instead of vCenter host ● HST will run the analysis sequentially when multiple vCenters are added in project ● HST will restrict the background analysis for Customer and Guest roles ● Fixed the NSX manager security assessment null pointer issue
1.0.1 Build 24855910	2025-07-17	Updated Release ● HST now supports import projects from legacy TDM and VHA Applications ● Now supports importing projects or folders and downward compatible with previous HST releases ● Fixed password issues with special characters in customer login in OVA. Supports passwords 20 characters long as well starting with $ as first character ● Allow adding Engagement information when merging TDM projects into existing VHA projects ● Enabled Max Heap Size setting for HST Jar in OVA ● Entering host details for data collection, tool tips are added to the import host details screen for clarity so that users should not mistakenly enter Esxi host details.

		● The HST App now ensures that the appropriate vSAN features and services are enabled on relevant clusters, enhancing overall system reliability ● For VHA Word report - the copyright statement now appears on the first page, while subsequent pages feature a simplified footer with appropriate spacing; all host names in the document have been updated to remove “https://” and “/sdk” ● Enabled Max Heap Size setting for HST Jar in OVA ● For SA Module - Automated several previously manual security controls, streamlining the assessment process for controls 100264, 100610, 100611, 100612, 100638, and 100639. ● For SA Module - Automated manual controls for vSAN Controllers, specifically controls 100802 and 100806, improving efficiency and consistency in security analysis ● For SA Module - Status reporting for automated controls is now accurate and reliable.
1.0.0 Build 24821845	2025-06-30	Initial Release ● Supports vSphere 7 and 8 ● Unified TDM and VHA features ● Uses JDK 21 ● Includes Security Assessment for service led engagements ● Role based access control ● VMware HST virtual appliance is built on the Photon OS 5

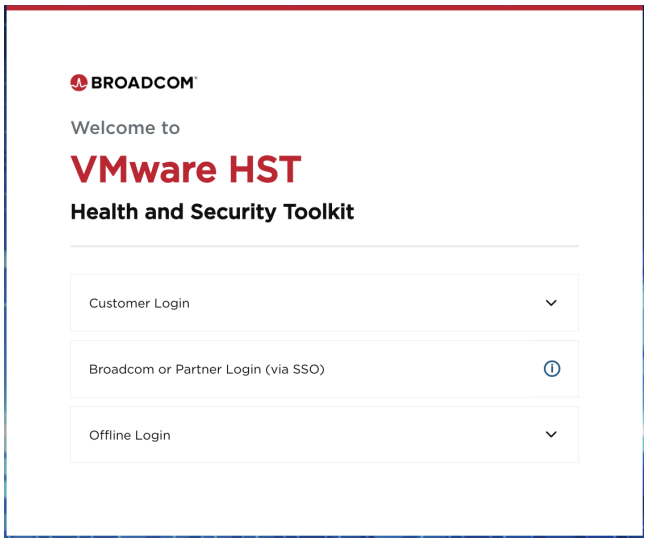
Checksum Details

Virtual Appliance	HST-PRODUCTION-1.0.4-25699684.ova
MD5	0bec318b15c971d5307fe0d11b2a30b6
SHA1	b08eb3322f39f680f74a61d0edccb9218090ad50
SHA256	74ebc9b99c641147c4a8e1e7a4cf61ae8adc33ddc453f6227ef839a616ca5e4b
Java Application	**HST-PRODUCTION-1.0.4-25699684-JAVA.zip**
MD5	647e71c64f9577528ebec01336e0596d
SHA1	5c015819c9b0e3cc9bb49a22254b94fd7d69411a
SHA256	b2055e2a1f45c7f831f5ae32f6e03f0a58fe74dfb46fbb3726fb432c29da9a29

1. Introduction to VMware HST

1.1. Overview

The VMware HST (Health and Security Toolkit), provided by Broadcom, is a comprehensive application designed to assist users in performing thorough health checks, and security assessments of their VMware environments. This guide will help you understand how to access and use the application.



1.2. Accessing VMware HST

1.2.1. JAR-Based Access: This method is suitable for users who want to run the tool locally on their system.

1.2.2. OVA-Based Access: This method involves deploying VMware HST virtual appliance (OVA) on a supported hypervisor, such as, VMware ESXi server, VMware Workstation, or VMware Fusion (supports only Intel processors).

2. Installation and Configuration

2.1. Java Based Installation and Configuration

Prerequisites:

- Google Chrome has been tested and recommended to access the UI
- Ensure JDK 21 is installed on your system.
- Ensure the Java install folder is added to your system's PATH environment variable. If multiple Java applications are in use, it is recommended to update the PATH value for each HST execution, to avoid interrupting other Java applications.

Installation on macOS

1. **Download JDK 21**
    a. Download Adoptium OpenJDK version 21 for macOS using this link or the JDK 21 distribution approved by your organization
2. **Install JDK 21**
    a. Open the downloaded `.pkg` file.
    b. Follow the installation instructions presented by the installer.
3. **Set Environment Variables**
    - Add the following lines to your `~/.bash_profile`, `~/.zshrc`, or `~/.bashrc` file, (To edit these files, you can use a command-line editor like nano or vim in Terminal, e.g., nano ~/.zshrc)
      For Bash (and compatible shells like Zsh if using these files):

```
export JAVA_HOME=$(/usr/libexec/java_home -v 21)
export PATH=$JAVA_HOME/bin:$PATH
```

    - Note: this will modify the default JAVA_HOME and PATH values system wide anytime Terminal is opened. If other Java applications are in use on this system, the above commands can be manually executed each time the shell is opened instead of adding them to the profile.
4. **Verify Installation**
    - After editing your shell configuration file, either close and reopen your Terminal window or run `source ~/.zshrc` (or your respective config file).
    - In Terminal, type the following command to check the installed version:

```
java -version
```

Installation on Windows

1. **Download JDK 21**
    - Download Adoptium OpenJDK version 21 for Windows using this link or the JDK 21distribution approved by your organization
2. **Install JDK 21**
    - Run the downloaded installer file (`.exe` or `.msi`).
    - Follow the installation instructions presented by the wizard.
3. **Verify Installation**
    - Open a new Command Prompt window.
    - Type the following command (adjust the folder name as per your setup) and press Enter:

```
set PATH=C:\Program Files\Eclipse Adoptium\jdk-21.0.<minor>.<version>-hotspot\bin
java -version
```

This should confirm that JDK 21 is available on the system. If you see some other version (ie JDK 11), the HST application may not run as expected.

To Run Application:

- Open Terminal (macOS) or Command Prompt (Windows).
- Navigate to the directory where the HST `.jar` file is located (e.g., `cd /path/to/hst/jar/`).
- For Windows command prompt run `set PATH=C:\Program Files\Eclipse Adoptium\jdk-21.0.<minor>.<version>-hotspot\bin` command described above. A similar setting may be required on macOS if the system wide PATH statement has not been updated, as described in the installation section.
- Execute the following command

```
java -jar HealthAndSecurityToolkit.jar
```

Important Note for JAR Execution:

Always launch the HST JAR file using the command from your Terminal or Command Prompt. Directly double-clicking the `.jar` file is not recommended and may lead to unexpected failures or warnings.

***Note**: If you encounter below mentioned error,*

```
Error: LinkageError occurred while loading main class
org.springframework.boot.loader.launch.JarLauncher
```

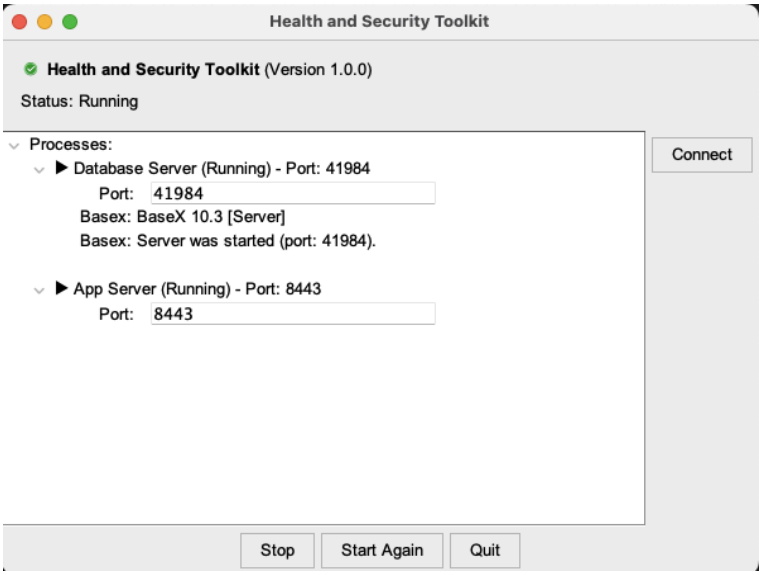
```
java.lang.UnsupportedClassVersionError:
org/springframework/boot/loader/launch/JarLauncher has been compiled by a more
recent version of the Java Runtime (class file version 61.0), this version of
the Java Runtime only recognizes class file versions up to 55.0
```

then check `java -version`

The above mentioned error occurs when the jar is executed with the java version below JDK21.

- **After Successful Execution:**
  - A **Health and Security Toolkit launcher** window will appear on your desktop (see screenshot below)
  - This launcher window displays the status of internal services:
    - **Database Server** status, including the port it's running on (e.g., 41984).
    - **App Server** status, including the port it's running on (default is typically 8443).
  - Click the **Connect** button on the application to launch the default web browser and access the user interface
  - **Additional Options in the Launcher Window:**
    - **Start Again:** If needed, this option restarts the internal database and application services.
    - **Stop:** This option stops the running internal services. The launcher window may remain open.
    - **Quit:** This option stops all services and completely exits the HST launcher application.

      - Note: if for any reasons Database server or App Server do not get Running status use the **Quit** button to close the application and launch again using the steps in the section above.



Skip to section **2.4. vCenter Custom Role Privileges (Recommended Best Practice)**

2.1. Prerequisites to Run Security Assessment (SA) on JAR

Security Assessment requires Services Engagement and is not available for TAMs, as such these steps are not required for TAMs and Customers.

1. Install HomeBrew (macOS only)

- Run the following command in Terminal:
- The terminal might ask to enter password multiple times for different packages (Approx 7-8 times)
- Follow the steps mentioned in the Terminal

```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

2. Install PowerShell (v7.4 or above)

- **PowerShell** (v7.4 or above) should be installed on the system. If it is not installed, follow the instructions windows, mac, linux
    - Steps
        - Run Below command in the Terminal window
            - brew install --cask powershell
- **Internet connectivity** for downloading the PowerShell modules.

Steps *(For Both Windows and Mac)*:

3. Verify PowerShell Installation

Once PowerShell is installed, verify the installed version using the following commands in the terminal:

```
#Opens Powershell

 pwsh

 #Validate Powershell installed version

 $PSVersionTable
```

4. Install the Required Modules

Open a new terminal and execute the following commands to install the necessary modules:

Note: Executing below commands might take few mins

```
# Opens PowerShell
pwsh

# Set PowerShell Gallery as a trusted repository
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

```
# Install PowerCLI from PowerShell Gallery
Install-Module -Name VMware.PowerCLI -Repository PSGallery -RequiredVersion 13.3.0.24145081 -Scope
CurrentUser

# Install SsoAdmin from PowerShell Gallery
Install-Module -Name VMware.vSphere.SsoAdmin -RequiredVersion 1.4.0 -Repository PSGallery -Scope
CurrentUser

# If willing to participate in VMware's customer experience improvement program, set to true.
Set-PowerCLIConfiguration -ParticipateInCEIP $true -Scope User

# If not, set to false.
Set-PowerCLIConfiguration -ParticipateInCEIP $false -Scope User

# Ignore invalid certificate actions
Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Scope User


# To check all powershell modules are installed.

Get-Module VMware* -ListAvailable
```

For more details on PowerCLI Modules installation refer here,

2.2. Virtual Appliance Based Deployment and Configuration

This method involves deploying the HST (OVA) onto a virtual machine.

Prerequisites for OVA Deployment:

1. Users should have access to the vSphere client with necessary permissions to deploy OVA

Deploy a virtual machine from a template	On the destination folder or data center: • **Virtual machine > Edit inventory > Create from existing** • **Virtual machine > Change Configuration > Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine > Provisioning > Deploy template**	Administrator
	On the destination host, cluster or resource pool: • **Resource > Assign virtual machine to resource pool** • **vApp > Import**	Administrator
	On the destination datastore or folder of datastores: **Datastore > Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network > Assign network**	Network Consumer or Administrator

For more information on the permissions, refer [Broadcom Tech Docs | VMware vSphere 8.0 | vSphere Virtual Machine Administration]

2. Users should have downloaded the OVA using the URL in the **Download Link** section above.

Steps to deploy OVA using vSphere client:

1. **Login to vSphere Client:** Access the vSphere Web Client and log in using your vCenter credentials.
2. **Select Target Resource:** Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host.
3. **Initiate Deployment: Choose "**Deploy OVF Template" from the context menu and deploy OVF Template wizard opens.
4. **Select an OVF template:** Select Option Local file and Click Upload files and select the HST OVA file which was downloaded from box and Click Next
5. **Select a name and folder:** Provide a name for the new virtual machine and choose the location within the vCenter inventory where the VM should be located and Click Next.
6. **Select a compute resource:**
    a. Select the destination compute resource ESXi host or cluster where the VM will run,
    b. Make sure the Compatibility checks succeeded,
    c. Enable “Automatically power on deployed VM” for VM to turn on automatically once deployment is complete, If this is not selected, we need to manually turn on VM post deployment is complete, Click Next
7. **Review details:** On the Review details page, verify the OVA template details covering details such as Publisher, Product, Version, Vendor, Description, Download size, Size on disk and click Next.

8. **Select storage**: On Select Storage page, define where and how to store the files for the deployed OVA template, Make sure Compatibility checks succeeded and Click Next
9. **Select networks:** On Select Network page, select the destination network for the Source network and Click next,
10. **Customize template:** On Customize template, Enter the below required details for the HST application

    Application Properties:

    a. Hostname: The hostname for this VM. Leave blank to try to reverse lookup the IP address.
    b. Initial root password: This is the password for the console/ssh. Password must be at least 8 characters long and contain numbers, symbols and letters in the upper and lower case.
    c. Web Application User Name: This is the web application user name which is required to login to the HST application as Customer. This must be between 3-32 ascii characters in length.
    d. Web Application Password: This is a password for the web application user as Customer. The password must be at least 8 characters long and must contain numbers, symbols and letters in the upper and lower case

    Networking Properties:

    a. Host Network IP Address Family: Network IP address family (i.e., 'ipv4' or 'ipv6').
    b. Leave the settings below blank for DHCP or use the steps for Static configuration.
    c. Default Gateway: The default gateway address for this VM.
    d. Domain Name: The domain name of this VM.
    e. Domain Search Path: The domain search path (comma or space separated domain names) for this VM.
    f. Domain Name Servers: The domain name server IP Addresses for this VM (comma or space separated).
    g. Network 1 IP Address: The IP address for this interface.
    h. Network 1 Prefix: The network prefix length (e.g., 24 for 255.255.255.0) for this interface.
    NOTE: Do not confuse the network prefix with the subnet mask.
    If your network uses 255.255.255.0 as the subnet mask, enter 24 in the network prefix field.
    Do not enter 255.255.255.0 or any dotted decimal format in the network prefix field.
11. **Ready to complete:** Review the deployment details and click "Finish" to initiate the deployment.
12. **Checks Recent Tasks:** As a result, a new task for creating the virtual machine appears in the Recent Task pane. After the task is complete, the new virtual machine is created on the selected resource.

NOTE: Depending on the local network connectivity to the vSphere, deployment of OVA could take up to 30 minutes. Make sure there are no network interruptions during the deployment. Do not refresh the tab of vSphere client when deployment tasks are running. Open a new tab and try to access vSphere for other activities.

13. **Open HST Application:** Once VM is deployed and in running state, Look for the IP address on Virtual Machine Details screen and Open browser with the IP address and you can access the deployed HST application now on browser.

Steps to deploy OVA in Workstation:

Prerequisites:

1. Ensure the latest VMware Workstation is installed on your system.
2. Users should have downloaded the OVA file from the HST box location locally.

Steps to deploy OVA on Workstation:

1. **Launching VMware Workstation:** Open VMware Workstation from your desktop or start menu.
2. **Importing the OVA File:** Go to the File menu and select Open, Browse to the location of downloaded OVA file. Select the OVA file and click Open.
3. **Store the Virtual Machine**: Enter the details of Name of the Virtual Machine and Storage path for the Virtual Machine and Click next.
4. **Fill the Properties**:

   Application Properties:

   a. Hostname: The hostname for this VM. Leave blank to try to reverse lookup the IP address.
   b. Initial root password: This is the password for the console/ssh. Password must be at least 8 characters long and contain numbers, symbols and letters in the upper and lower case.
   c. Web Application User Name: This is the web application user name which is required to login to the HST application as Customer. This must be between 3-32 ascii characters in length.
   d. Web Application Password: This is a password for the web application user as Customer. The password must be at least 8 characters long and must contain numbers, symbols and letters in the upper and lower case

   Networking Properties:
   If you are looking for automatic IP allocation based on your DHCP, Skip setting the below properties, if not enter the below details.

   a. Host Network IP Address Family: Network IP address family (i.e., 'ipv4' or 'ipv6').
   b. Default Gateway: The default gateway address for this VM. Leave blank if DHCP is desired.
   c. Domain Name: The domain name of this VM. Leave blank if DHCP is desired.
   d. Domain Search Path: The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired
   e. Domain Name Servers: The domain name server IP Addresses for this VM (comma or space separated). Leave blank if DHCP is desired.

f. Network 1 IP Address: The IP address for this interface. Leave blank if DHCP is desired.
g. Network 1 Prefix: The network prefix length (e.g., 24 for 255.255.255.0) for this interface. Leave blank if DHCP is desired.

NOTE: Do not confuse the network prefix with the subnet mask.
If your network uses 255.255.255.0 as the subnet mask, enter 24 in the network prefix field.
Do not enter 255.255.255.0 or any dotted decimal format in the network prefix field.

5. **Review and Import:** Review the properties set and click on import.
6. **Open HST Application:** Once VM import is completed, you will be prompted to enter the username and password for SSH, Enter root as Username and Enter value you set at Initial root password (5.b) as Password. Once logged in, You will see the message “Health and Security Toolkit is running. access using URL http://IP_ADDRESS:8443”, Open browser with the IP address and you can access the deployed HST application now on browser.

NOTE: If your vCenter is behind a VPN and you want to access that from your workstation, You need to set Network Adapter as NAT and be connected to your VPN. Follow the below instructions to do

1. **Ensure the Virtual Machine is Powered Off**: Shut down the guest operating system of the deployed HST VM, if it is running. Confirm the VM is in a powered-off state (not suspended or running).
2. **Open Virtual Machine Setting**s: In VMware Workstation, select the target virtual machine from the library. Click Edit virtual machine settings (or right-click the VM and select Settings).
3. **Locate the Network Adapter**: In the Hardware tab, find and select Network Adapter from the list.
4. **Change the Network Connection Type**: Under Network connection, select the option labeled NAT,. Ensure Bridged is not selected.
5. **Save and Close Settings**: Click OK to save your changes and close the settings window.
6. **Power On the Virtual Machine**: Start the virtual machine. The VM will now use NAT networking, sharing the host’s IP address for external network access.
7. **Open HST Application:** Once VM is turned on, you will be prompted to enter the username and password for SSH, Enter root as Username and Enter value you set at Initial root password (5.b) as Password. Once logged in, You will see the message “Health and Security Toolkit is running. Access using URL https://IP_ADDRESS:8443”, open the browser with the IP address and you can access the deployed HST application now on the browser.

NOTE: On vCenter deployment When using Launch Web console or On workstation When performing SSH on first time, if you come across message on stating “no authorized SSH keys fingerprints found for user root and see details of SSH Host Keys or Fingerprints”, This behavior is normal and Press enter which will give you the login prompt again and is visible only during first time. Users should perform SSH with the user name as root and password based on the value set for property initial root password which is provided during OVA deployment.

Prerequisites:

1. The HST OVA file must be successfully deployed and the resulting virtual machine powered on.
2. You need to know the IP address assigned to the HST virtual appliance.

- **Steps to Access:**
  1. Open a supported web browser (e.g., Chrome).
  2. In the browser's address bar, navigate to the IP address or hostname of your deployed HST appliance (e.g., `https://<hst-ip-address>:8443`)
  3. The VMware HST login screen will be accessible via this web interface.

2.3. Pre-Scan Configuration and Account Permissions

The following subsections detail the information and permissions required for each component.

Required Information and Credentials:

Before starting, ensure you have the following information for each environment you plan to scan:

vCenter Requirements:

- **vCenter Server** – the FQDN of the vCenter you want to scan.
- **User** – a vCenter account with required Privileges.
- **Password*** – password for above user.

NSX Requirements: (*For Security Assessment only*)

- **NSX Manager** – the FQDN of the NSX Manager you want to scan.
- **User** – a NSX account with Administrative Privileges.
- **Password*** – password for above user.

SDDC-Manager Requirements: (*For Security Assessment only*)

- **SDDC-Manager** – the FQDN of the SDDC-Manager you want to scan.
- **User** – a SDDC account with Administrative Privileges.
- **Password*** – password for above user.

2.4. vCenter Custom Role Privileges (Recommended Best Practice)

To follow the principle, create a custom role in vCenter Server using the privileges outlined in the table below. This ensures full functionality across Health Analyzer (VHA) and data reporting (TDM). The Security Assessment (SA) reporting requires the administrator role.

Privilege ID	Privilege Path (in web client)	Data Reporting (TDM)	Health Analyzer (VHA)
System.Read	Not visible	Required	Required
System.View	Not visible	Required	Required
Global.Licenses	Global > Licenses	Optional1	Optional 1
Host.Config.Storage	Host > Configuration > Storage partition configuration	Not Required	Optional 2
StorageProfile.View	Profile-driven storage > Profile-driven storage view -or- VM storage policies > View VM storage policies	Not Required	Optional 2

Optional 1 = Report will run without this privilege, but no license-related output will be present in TDM reports.
Optional 2 = VHA collection may fail without this privilege. A flag in the `collection.properties` file can bypass checks requiring this privilege.

For details on creating custom roles, refer to the vSphere product documentation: Create a vCenter Server Custom Role

2.5 Modifying collection.properties:

As noted in the vCenter Custom Role Privileges section above, the health assessment has some optional storage related privilege requirements. Collecting data without those privileges may cause collections to fail. If you are unable to access an account with the necessary access, data collection for those storage findings can be disabled by editing the following file:

Appliance path: `/usr/share/vmwarehst/lib/BOOT-INF/classes/collection.properties`
JAR path: `<extracted-folder>/lib/BOOT-INF/classes/collection.properties`

Find the following entries and change their value to `false`:

```
collection.iscsiport.enabled=true
collection.storagepolicies.enabled=true
```

Then restart services (reload the Java applet or use `systemctl restart vmwarehst.service` for the appliance).

2.6 Port Requirements for HST:

The Health and Security Toolkit (HST) requires access to a specific network port to perform data collection across various components.

Source	Destination	Port	Description
Admin Workstation	HST Appliance	22	SSH *
Admin Workstation	HST Appliance	80, 8080, 443	HTTP redirects
Admin Workstation	HST Appliance or JAR	8443	Web Interface SSL
Internal Only	HST Appliance or JAR	41984	Basex Database
HST Appliance or JAR	vCenter Server	443	vCenter Collection
HST Appliance or JAR	VCF 5.2 SDDC Manager	443	Security Assessment SDDC Collection
HST Appliance or JAR	NSX Manager	443	Security Assessment NSX Collection

* Starting with HST 1.0.4, the SSH service is no longer started automatically. You must login to the appliance console and enter `systemctl start sshd` to start the SSH server process. This is a non-persistent change that will be reverted on reboot. If you wish to make this change persist, so that the SSH service starts automatically, you can use `systemctl enable sshd` to change the default behavior.

2.7 Memory Configuration for HST:

HST is a Java based application and depends on Java heap memory for both the application and database processes. The default configuration is typically sufficient for small environments. Additional memory may be required to complete larger projects.

The project export file size can be used to estimate necessary Java heap. In general, 1mb of project file size needs 40mb of memory for the Basex database and application processes.

For example, a 50mb project file would need

50mb (file size) * 40mb (heap memory) = **2000**mb for app & database

The heap settings are applied differently depending on whether the JAVA JAR or Appliance are used. Details can be found below.

JAVA JAR:

To grant additional memory to the Java processes on Windows, the following command can be used.

```
set BASEX_JVM=-Xmx BASEX_MEMORY m
java -Xmx JAVA_MEMORY m -jar HealthAndSecurityToolkit.jar
```

For example:

```
set BASEX_JVM=-Xmx2000m
java -Xmx2000m -jar HealthAndSecurityToolkit.jar
```

For Mac OS, the syntax for creating an environment variable is slightly different (`export` instead of `set`). For example:

```
export BASEX_JVM=-Xmx2000m
java -Xmx2000m -jar HealthAndSecurityToolkit.jar
```

Note: For additional information on launching the java processes from the command line, see the previous section 2.1 on installation.

Appliance:

The HST appliance will dynamically configure Java heap settings at start up based on memory available to the appliance. The logic allocates 1/3 of memory to the Basex (database) and 1/3 of memory to the Java (application) heap. If more heap is needed, the virtual appliance memory allocation can be increased. Using the above example where a project needs ~2GB of heap, the appliance can be configured with 6GB of RAM (calculated heap x 3).

Alternatively, Java heap size can be manually defined for the appliance using the following file:
`/usr/share/vmwarehst/lib/BOOT-INF/classes/memory.properties`

The memory.properties contains the following entries that each need to be adjusted:

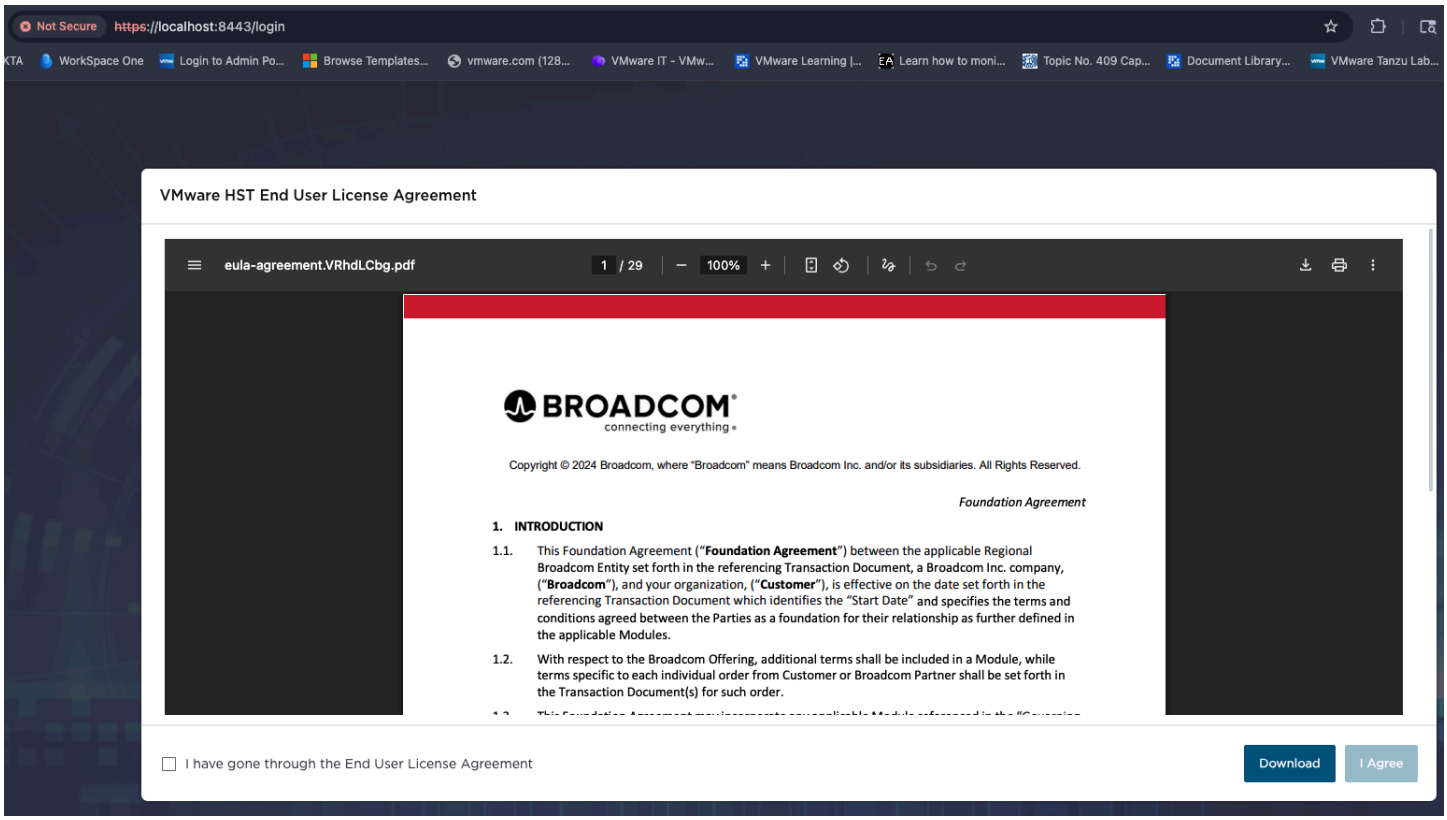
```
memory.enabled=false    <-- Set to true
basex.memory=2048       <-- Adjust to larger size, ie 4096
java.memory=2048        <-- Adjust to larger size, ie 4096
```

Note: Using this file, the configured Java heap can exceed system memory, but OS swapping may occur, resulting in unpredictable performance.

After making changes, restart services (reload the Java applet or use `systemctl restart vmwarehst.service` for the appliance).

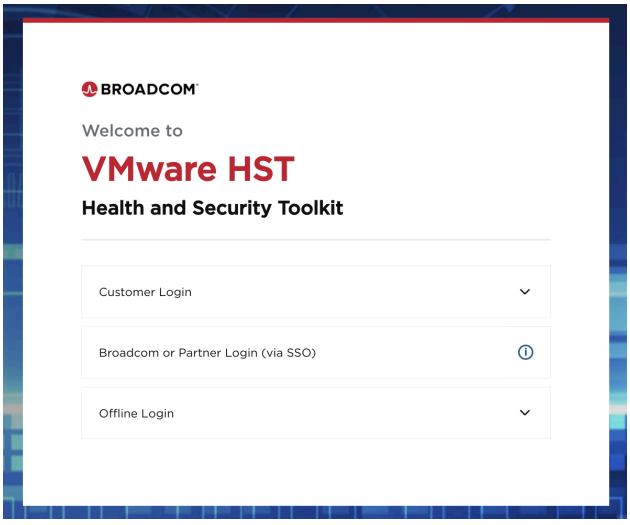
3. Using the HST Application

Users must accept Broadcom's Foundation Agreement presented at the first launch of the application to proceed to the Login page.



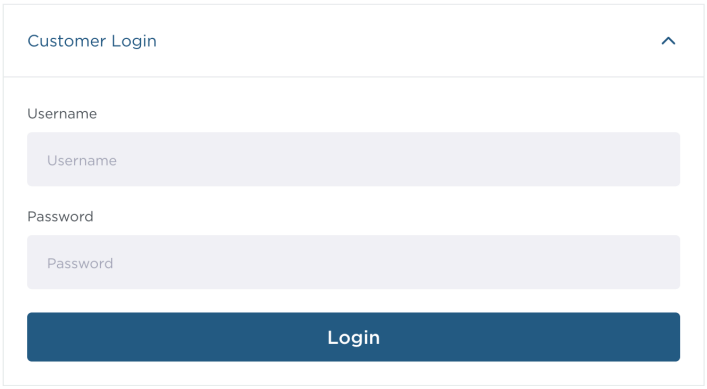
3.1. Login Options

VMware HST provides role based login options for Customers, Broadcom employees and Partners, and also an Offline Login to support running the tool in isolated environments.



3.1.1 Customer Login

Broadcom customers can use this option to access the HST application for running collections or exporting projects.



Login Behavior:

- **For Java:**
  - Click on the **Customer Login** then the **Login** button
    Note: There are no login credentials required for Customer Login when running the Java option of the tool
- **For Virtual Appliance:**
  Note: *Tomcat user name and Tomcat password which were provided during OVA deployment will required to login*
  - Click on the **Customer Login** dropdown.
  - Enter your **Username** in the first field.
  - Enter your **Password** in the second field.
  - Click the **Login** button.

Notes:

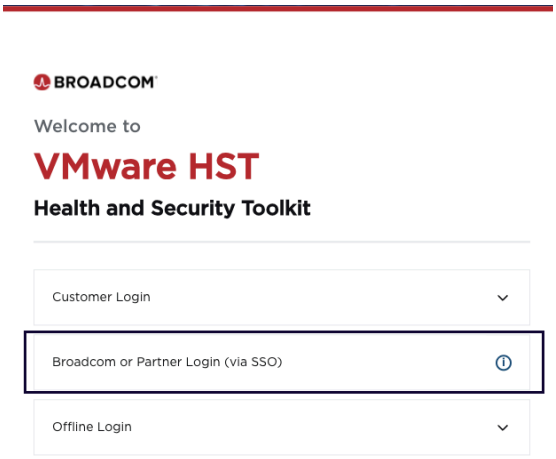
- Ensure your credentials are correct to avoid login errors.
- If you have forgotten your username and password of the appliance, follow these steps to create a new user and regain access:
  SSH into the Machine:
  - Open your terminal or SSH client
  - Connect to the virtual machine using its IP address and your SSH credentials: `ssh root@<vm-ip-address>`
  - Replace `<vm-ip-address>` with your actual VM's IP address.

  Run the User Creation Script

- Once logged in, execute the following script to create a new user:
  `/usr/share/vmwarehst/scripts/create_new_user.sh`
- The script will prompt you to enter a new username and password. Follow the on-screen instructions to complete the process.

3.1.2 Broadcom or Partner Login (via SSO)

Broadcom employees, such as TAMs, Professional Services or Broadcom partners who authenticate using their organization's Single Sign-On system will need to login by clicking on **Broadcom or Partner Login (via SSO)**



Steps:

1. Click on the **Broadcom or Partner Login (via SSO)** dropdown.
2. Click **Login** to be redirected to your organization's SSO login page.
3. Complete your login with the SSO system as prompted.

Notes:

- Make sure you're connected to your organization's secure network if required for SSO.
- Use your corporate credentials to log in.

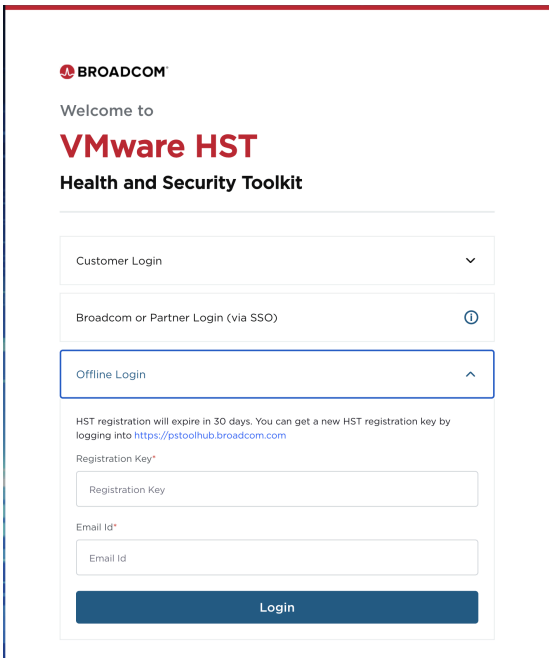
3.1.3 Offline Login

This option is used when you are operating the tool in an environment where internet access may not be available.

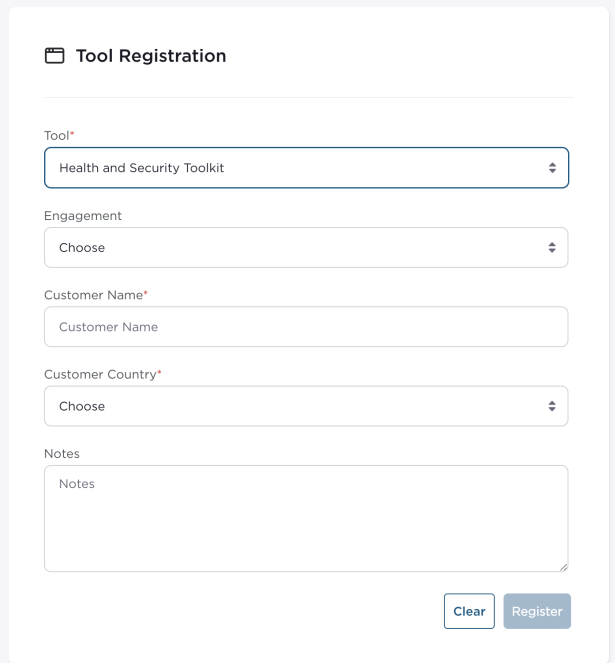
IMPORTANT: You must ensure that you have access to all required modules such as Health Analyzer and/or Security Assessment BEFORE generating an offline login. Validate that you have access to all these modules in Offline mode prior to going to the customer site to avoid delays to the projects.

Offline Login works by requesting a **Registration Key** from the PS Tool Hub.

1. Click **Offline Login** to expand login menu then click the link to go to the PS Too Hub website it should open the link a new tab



2. Fill out the **Tool Registration** form on the PS Tool Hub browser tab



- **Tool:** From the dropdown select **Health and Security Toolkit**
- **Customer Name:** Enter your organization or customer name.
- **Customer Country:** Choose from the dropdown.
- **Notes** (optional): Enter any relevant information.
- Click **Register**.
- The **Registration Key** will be emailed to you on your Broadcom email address

Note: Registration Key is valid for 30 days, you will need to request another key after it expires

3. Using the Offline Login Feature

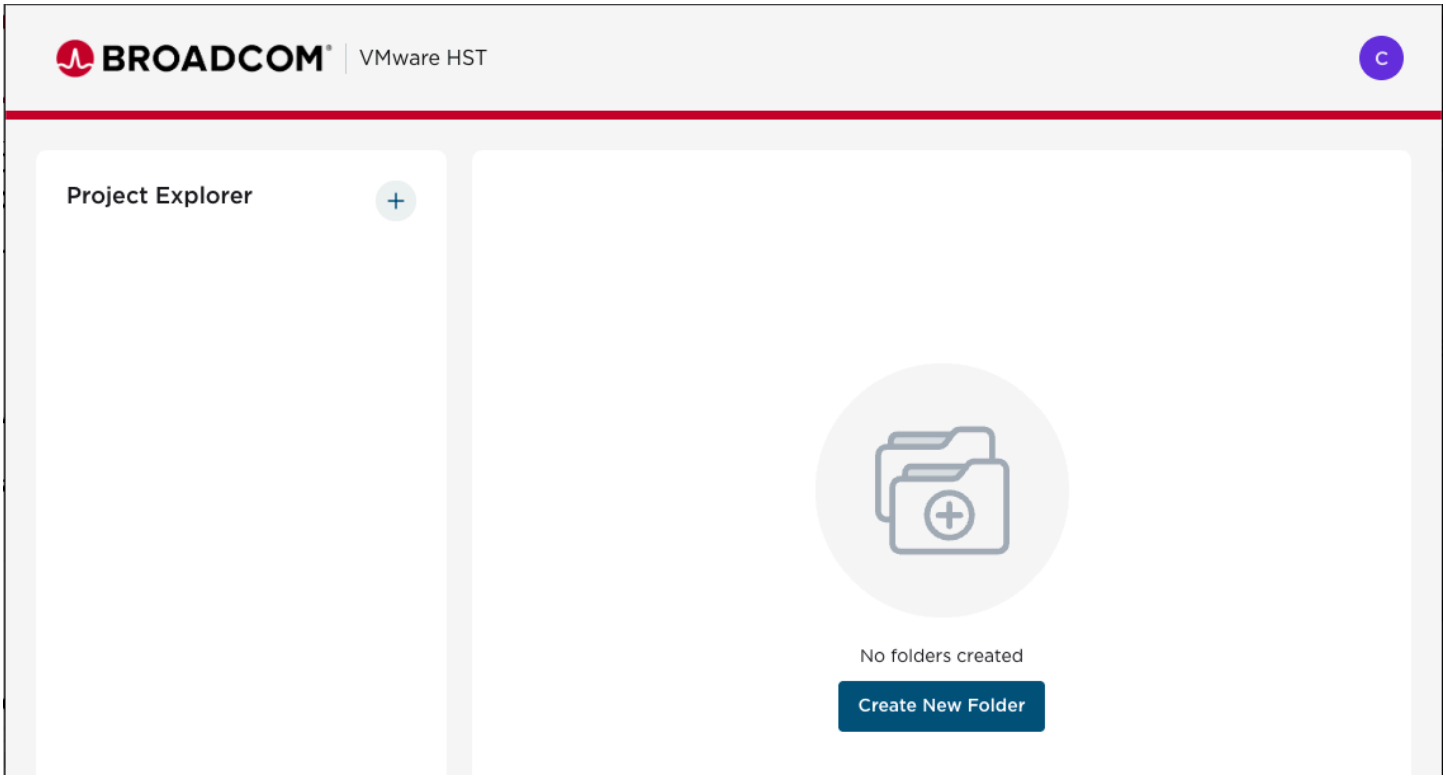
1. Click on the **Offline Login** dropdown in the HST application.
2. Enter the **Registration Key** you obtained.
3. Enter your **Email ID** used during registration process
4. Click the **Login** button.

Notes:

- Ensure you have successfully generated and received a valid **Registration Key** from the PS Tools portal *before* attempting to use the Offline Login.
- The offline mode still requires a valid **Email ID** to associate with your activity and the generated key.

3.2. The Project Explorer Page

After successfully logging into the VMware HST application, you will land on the Project Explorer page.



3.2.1. Navigating the Dashboard:

You will see a clean workspace with the following elements:

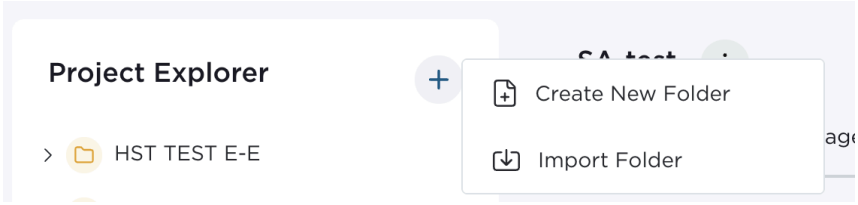
- **Project Explorer Panel (Left):**
  - This section allows you to manage and organize your work.
- **Main Workspace (Center):**
  - Shows folder contents or prompts you to create/import folders

- **Top Right Profile Menu:**
    - Clicking your initials (top right) reveals options like:
        - **User Guide** – Link to documentation.
        - **Download Logs** – For troubleshooting.
        - **Logout** – To securely exit the system.

3.2.2. Folder Management (Create, Import):

To begin working, you need to create or import a folder.

Option A: Create New Folder



1. Click the **"+" icon** next to "Project Explorer" or the **"Create New Folder"** menu option
2. In the Create New Folder popup window enter;
    - **Folder Name** (mandatory)
    - **Description** (optional)
3. Click **Create** to save the folder.

Option B: Import Folder

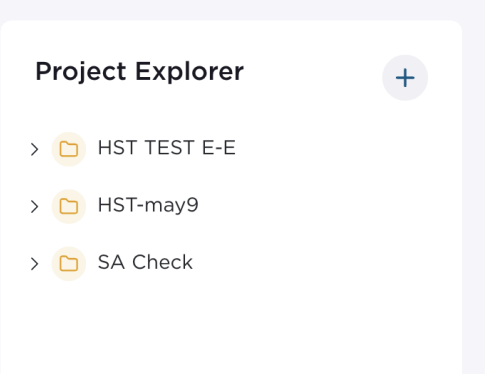
Import Folder helps when upgrading from an older version of VMware HST. Users could simply export folders from the older version then import them into the newly deployed instance of the tool. This provides a safer way to upgrade the tool as well as migration to another instance if needed.

1. Click the **"+" icon** next to "Project Explorer".
2. Select **Import Folder** if you're bringing in an existing folder (e.g., exported from another instance).
3. In **Choose Folder to Import** popup window click **Upload** then select the folder file to import

3.2.3 Folder Display and Organization

Once created or imported, folders appear under **Project Explorer**. You can:

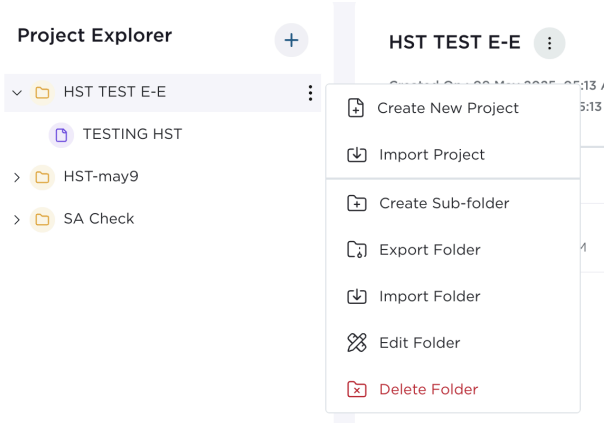
- Click on any folder to open it.
- Add more folders as needed for different projects or environments.

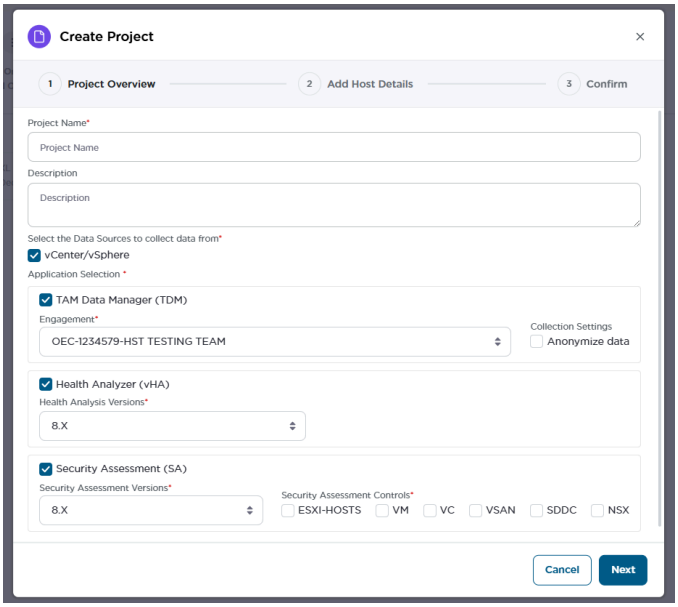


4. Creating a new project

After logging in and creating or importing a folder, users can create projects to begin data collection and analysis.

- Click the vertical ellipsis next to the folder you would like to add the project to
- Select **Create New Project** from the menu





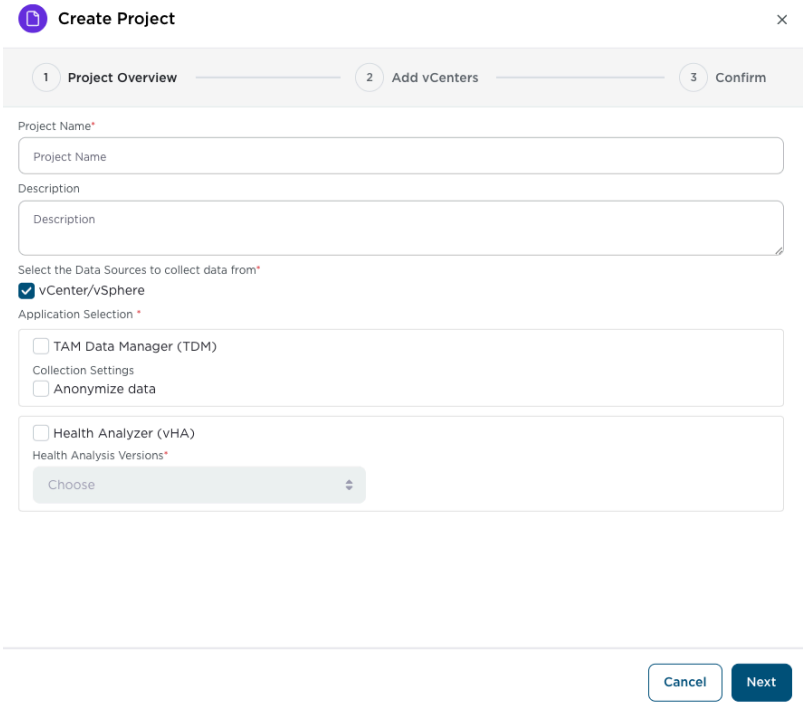
VMware HST provides a dynamic UI which adapts to the input provided by the user as well as the level of access each user has. Users logging in using Customer and TAM roles may only see options to run TAM Data Manager (TDM) and Health Analyzer (vHA) collections. Professional Services and Partners may see Health Analyzer and Security Assessment as their default modules.

For Broadcom employees and partners, if you do not see the modules for your project, you would need to open a support ticket to request access.

The tool supports creating projects by individual modules i.e., TDM, vHA, or SA or a combined project of all three modules together.

For Security Assessment (SA) only projects skip to **4.2 Creating a new Security Assessment (SA) Project**

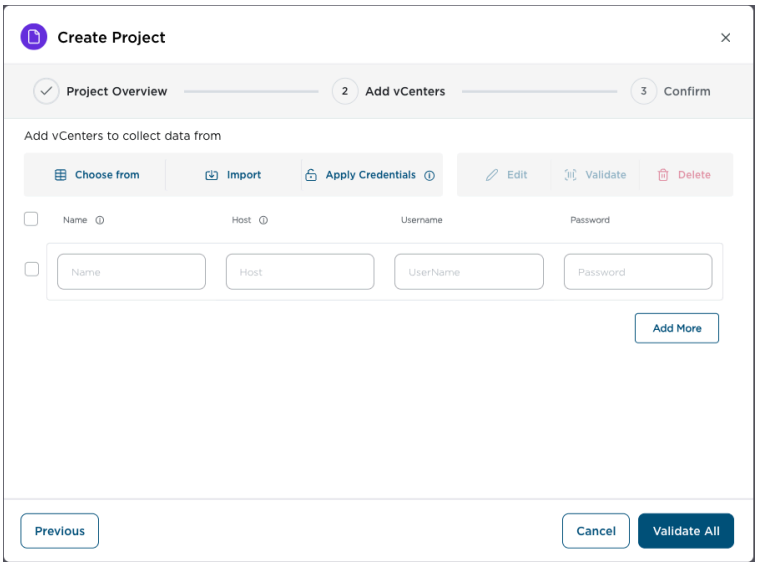
4.1 Creating a new TDM or VHA Project



On **Create Project** wizard enter the following information

- **Project Name:** Enter a unique and meaningful name.
- **Description:** (Optional) Add a brief purpose or reference.
- **Data Sources:** Select from:
  - Ensure **vCenter/vSphere** box is checked
- **Application Selection:** Choose whether you would like to create a TDM, VHA, or a combined TDM and VHA project by selecting appropriate options
- **TAM Data Manager (TDM)**
  - Note: If 'Anonymize data' is selected, object names (like VCs, Clusters, Hosts, etc) are obfuscated with a unique GUID that will change from one collection to another. This is available for TDM collections only. This anonymization is included for data privacy, but makes it difficult to action any recommendations/findings.
- **Health Analyzer (vHA)**
  - Note: Starting with HST 1.0.2, if the TDM 'anonymize data' toggle is selected, it is not possible to collect Health Analyzer data.

- **Engagement ID:** Choose the engagement (e.g., from a dropdown). This is only visible when logged in as Broadcom employee or Partner
- **Health Analysis Version:** Select the vSphere version (e.g., 7.x/8.x).
- Click **Next**.



Continue on **Create Project** wizard to add vCenters servers in scope for this project. Depending on the number of vCenter servers in the environment users can choose to enter the information for each vCenter manually or import the list of servers using a file, or choose servers from a previously run project. Steps for each of these options are listed below;

Option A: Entering vCenter server names manually

Input information in each of the fields listed below

- Name (vCenter name)
- Host (FQDN or IP address of vCenter Server)
- Username*
- Password*

***Note:** If the login credentials are the same across all or multiple vCenter servers then you may choose to apply credentials in bulk. The steps for applying credentials in bulk are provided below skip to **Applying Credentials in Bulk** section.

Option B: Choose from Existing

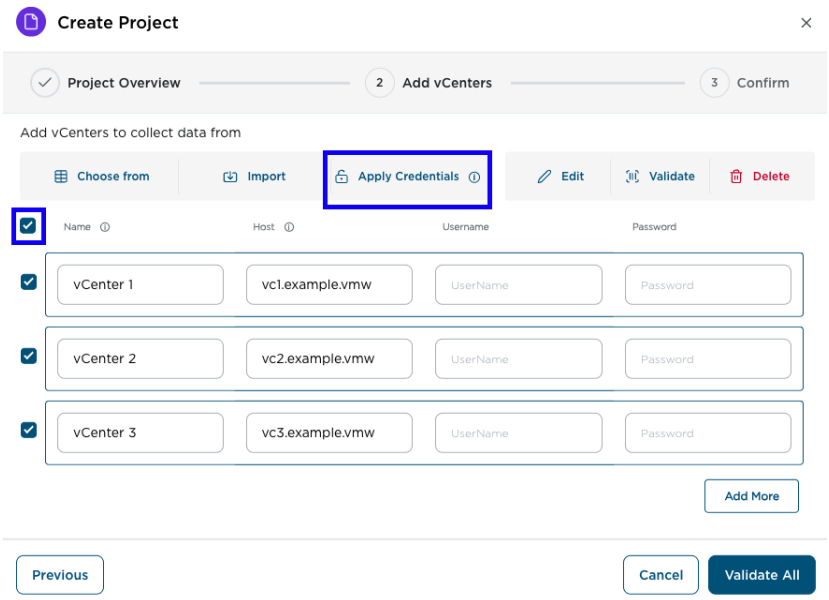
- Click **Choose from**.
- Select vCenter servers from the list
- Click **Add**.

Option C: Import from File

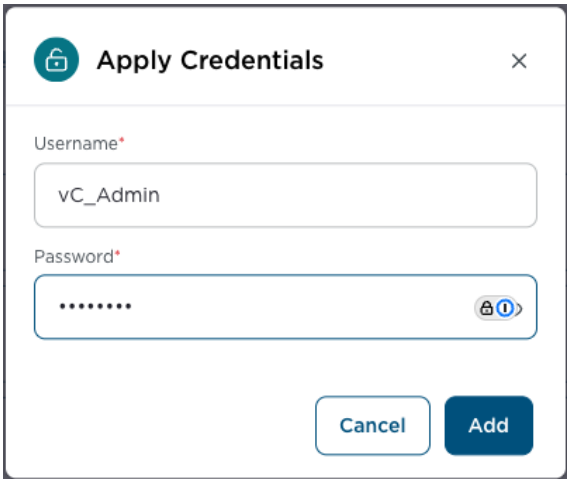
1. Click **Import**.
2. Select the **Upload File** option to upload an `.xlsx` file.
3. If needed, use the **Download Template** option to ensure the correct format is followed before uploading.

4.1.1 Applying Credentials in Bulk

- Select All vCenter servers by checking the box next to **Name.** Alternatively you could only select the servers for which you would like to apply the credentials



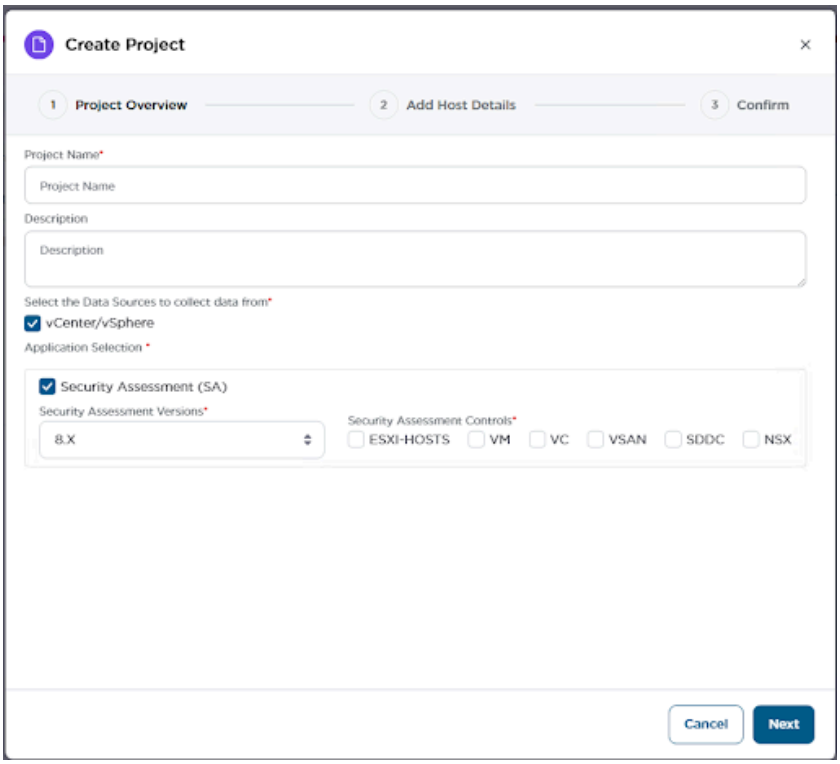
- Click **Apply Credentials** button in the middle of the screen



- Enter Username and Password for the vCenters click **Add** and these credentials will be applied to the selected vCenter servers, repeat these steps if necessary for remaining vCenter servers.
- Click **Validate** to validate the credentials and network connection between VMware HST and the listed vCenter servers

Skip to **Section 4.4 Monitoring Host Collection Process**

4.2 Creating a new Security Assessment (SA) Project



- **Security Assessment (SA)**
  - Note: Selecting SA may present additional environment-specific tabs in the next step(e.g., for NSX, SDDC Manager) depending on the sub-selections made for SA.

I. vCenter Host Details

(This section is for adding vCenter hosts. If your Application Selection also involves Security Assessment for NSX or SDDC Manager, those will be handled in separate tabs as described below.)

- Option A: Manual Entry
  1. Add **vCenter hosts** manually by entering:
     - Name (vCenter host name)
     - Host (FQDN of vCenter Server)
     - Username
     - Password
  2. Optional Fields for vCenter:
     - Mgmt VLAN ID
     - Syslog Server
     - Syslog Servers
     - Ntp Server

        - Ip Fix Collector Address
        - Vc Crypto Admins
        - Vc Crypto Roles
        - Exception Users
        - ESXi Build Number
        - AD Admin Group
        - Backup Third Party
- Option B: Choose from Existing
    1. Click **Choose from**.
    2. Select an existing vCenter from the list.
    3. Click **Add**.

    Option C: Import from File

    4. Click **Import**.
    5. Select the **Upload File** option to upload an `.xlsx` file.
    6. If needed, use the **Download Template** option to ensure the correct format is followed before uploading.

    Important Notes:

    - The downloaded template contains three separate tabs:
        - **vCenter** – For vCenter host details.
        - **NSX** – For NSX VIP connection details.
        - **SDDC** – For SDDC Manager connection details.
    - Ensure you add host details to the correct tab based on the selected environment type.
        - Example:
            - Add vCenter-specific entries only in the **vCenter** tab.
            - Add NSX-related entries in the **NSX** tab.
            - Add SDDC Manager details in the **SDDC** tab.
    - **Do not modify sheet names or the structure of the template.** Incorrect formats may cause upload errors.
- **Adding Multiple vCenter Entries:** You can click **Add More** to input multiple vCenter entries manually.

4.2.1 Additional Host Details for Security Assessment (SA) Workflows

This section appears if you selected "Security Assessment (SA)" in Step 1 and then specified particular environment types for SA. Corresponding tabs will be displayed here.

- A. NSX VIP Flow (for SA)
    - (This tab appears if "NSX " was selected as part of the Security Assessment configuration in Step 1.)
    - A separate **NSX** tab is displayed.
    - The following fields must be filled:
        - **Name**
        - **Host**
        - Username
        - Password
    - Optional Fields for NSX:
        - NTP Servers
        - Syslog Servers
        - NSX Version
        - DHCP Server
        - DHCP Server Addresses
        - T1 Multicast List
        - T0 Multicast List
        - T1 Interface List
        - T0 Interface List
    - Users can:
        - Click **Add More** to add additional NSX managers.
        - Use **Apply Credentials** for bulk credential updates to selected NSX
        - Validate each NSX individually using its **Validate/Validate All** button.
    - Note: This is typically used when NSX infrastructure data collection is required as part of the Security Assessment process.
- B. SDDC Manager Flow (for SA)
    - (This tab appears if "SDDC" was selected as part of the Security Assessment configuration in Step 1.)
    - A separate **SDDC Manager** tab appears.
    - Required fields include:
        - Name
        - **Host**
        - Username
        - Password

    - Optional Fields for SDDC:
        - NTP Servers
        - SFTP Backup Enabled
        - SFTP Servers
        - My VMware Account
        - Current Version
    - Users may:
        - Click **Add More** for additional SDDC entries.
        - Import SDDC details from a file using the **Import** button.
        - Use **Apply Credentials** for bulk credential updates.
        - Validate each SDDC entry using its **Validate/Validate All** button.

III. Apply Credentials and Validate Hosts

- Apply Credentials (for vCenter Hosts):
    - After adding all your vCenter hosts
    - Select the checkbox for the vCenters to which you want to apply common credentials.
        - Click **Apply Credentials**.
        - Enter the common **Username** and **Password**.
        - Click **Add**.
- Validate Hosts:
    - Once all hosts (vCenter, and if applicable, NSX, SDDC Manager) are added and credentials applied:
        - Click **Validate** next to individual host entries to verify access.
        - Alternatively, click **Validate All** to attempt validation for all entered hosts across all relevant tabs.
- Validation Result Indicators:
    - Green – Host validation successful
    - Red – Host validation failed due to incorrect credentials, connectivity issues, or missing details
- After successful validation of required hosts, click **Next**.

Step 3: Confirm

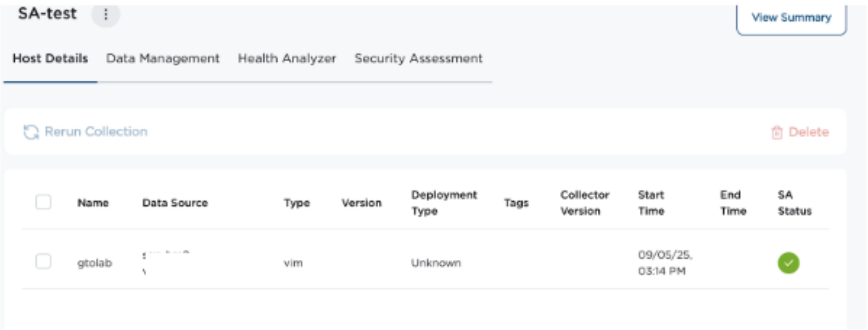
- A summary of the project appears, including:
    - Project Name
    - Data Sources
    - Application Selections
    - Engagement
    - Host details

- Review all details for accuracy.
- Click **Submit** to create the project.

Once submitted, the project will appear under the selected folder in the Project Explorer, and the data collection process begins

4.4. Monitoring the Host Collection Process

Once you submit a project, VMware HST starts collecting data from the defined hosts. You will be redirected to the **Host Details** tab within the project.



5. Monitor Collection Status

In the **Host Details** tab, you will see a list of added hosts with the following information:

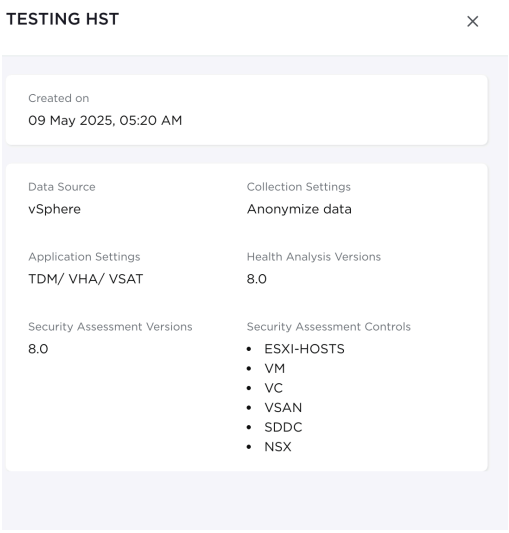
- **Field:** Name
  - **Description:** Host nickname you entered
- **Field:** Data Source
  - **Description:** vCenter or NSX or SDDC
- **Field:** Type / Version
  - **Description:** Host type and version (e.g., vim 8.0.3)
- **Field:** Deployment Type
  - **Description:** Typically “Unknown” if not set
- **Field:** Collector Version
  - **Description:** Collector version running on host
- **Field:** Start/End Time
  - **Description:** When collection began and ended
- **Field:** TDM/VHA Status
  - **Description:** Progress in percentage. Status (green = success, red = failed)
- **Field:** SA Status

- **Description:** Security Assessment result.Progress in percentage. Status (green = success, red = failed)

Actions Available

A. View Summary

- Use the **“View Summary”** button to get an overview of project-level results and health reports (once collection completes).



B. Rerun Collection

- If you want to rerun the collection:
    1. Select the host.
    2. Click **“Rerun Collection”**.
    3. Enter **Username** and **Password**.
    4. Click **Validate All** to re-initiate data collection.

C. Delete Host

- To remove a host:
    1. Select the checkbox next to a host.
    2. Click **Delete**.
    3. Confirm in the pop-up to permanently remove the host.

6. Status Indicators

- **TDM/vHA Status/ or SA Status** shows the real-time progress in percentage (e.g., 4%, 70%).
- **Status** marked as:
    - **Green Tick** – Success
    - **Red Exclamation** – Failure or issue

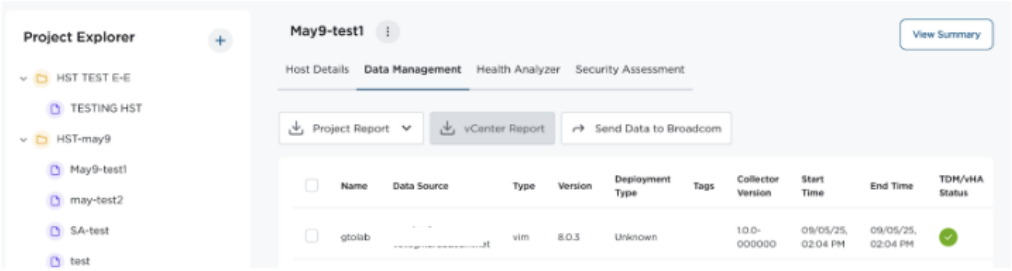
4. Important Tips

- **Collection Duration:** May vary based on host size and network performance.
- **Red Status:** Indicates login failure or collection error — use **“Rerun Collection.”**
- **Green Status:** You can safely view the results from the **“Health Analyzer”** or **“Security Assessment”** tabs.

7. Analysis and Reporting Tabs

Using the Data Management Tab

Once the data collection process completes, users can navigate to the **Data Management** tab to view results and generate reports.



8. Data Management Overview

In this tab, you can:

- View collected data per host
- Generate various reports
- Send collected data to Broadcom (Only for TAMs)

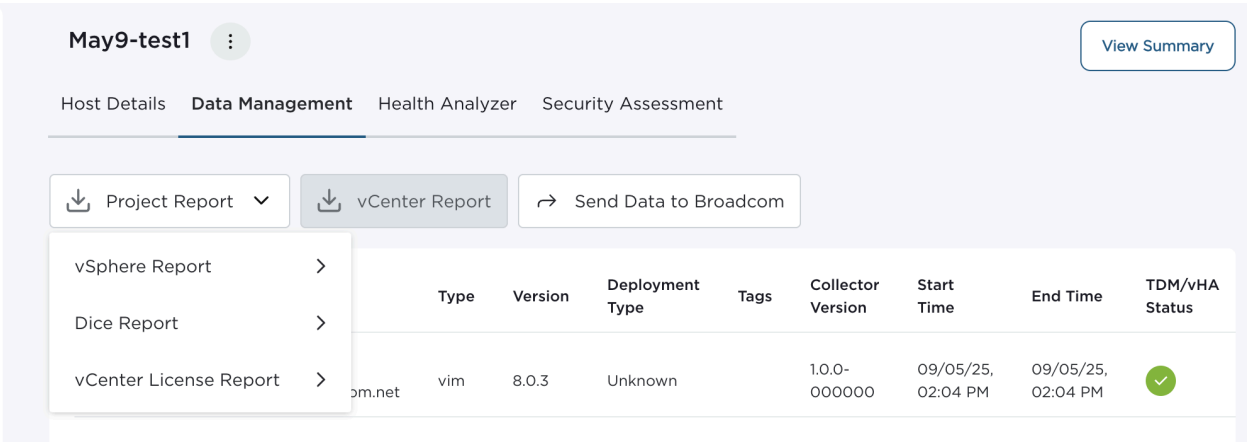
Each host is listed with the following details:

- **Name**
- **Data Source**
- **Type & Version**

- **Collector Version**
- **Start/End Time**
- **TDM/VHA Status**

9. Generating Reports

You will see two main dropdowns:



A. Project Report

Click the **Project Report** dropdown to generate:

- **vSphere Report**
- **Dice Report**
- **vCenter License Report**

Each report can be downloaded in:

- **Excel Report**
- **JSON Report**

Tip: These reports provide high-level and detailed information for health, inventory, and licensing purposes.

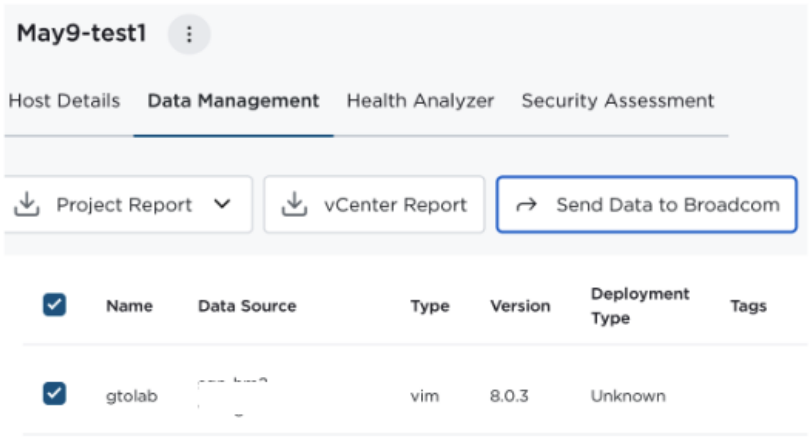
B. vCenter Report

Use this to generate specific host-level reports after selecting a vCenter host from the list.

- Make sure the checkbox beside the host is selected to enable report generation.

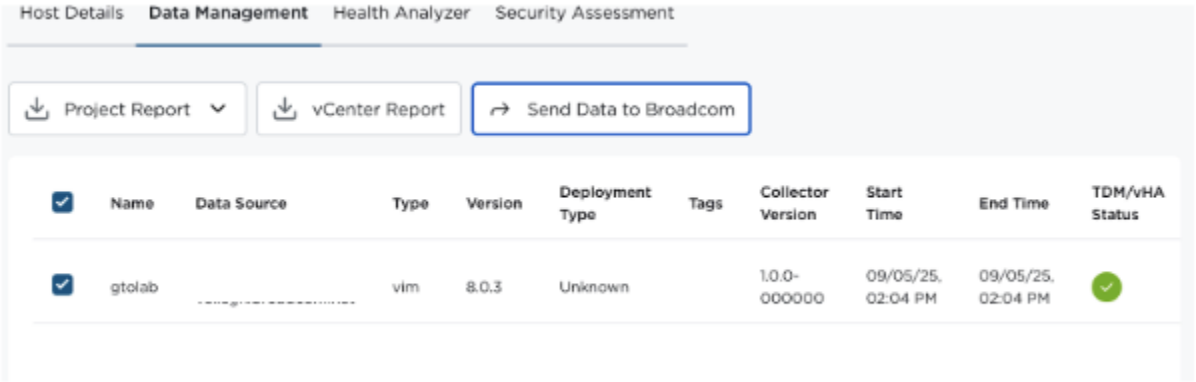
3. Sending Data to Broadcom (Only for TAMs)

Click **Send Data to Broadcom** to upload the collected report data to the Broadcom.



9.1 Status Indicators

- A **green checkmark** under **TDM/VHA Status** indicates the collection was successful.
- If a host is not ready, its data will not be eligible for report generation.

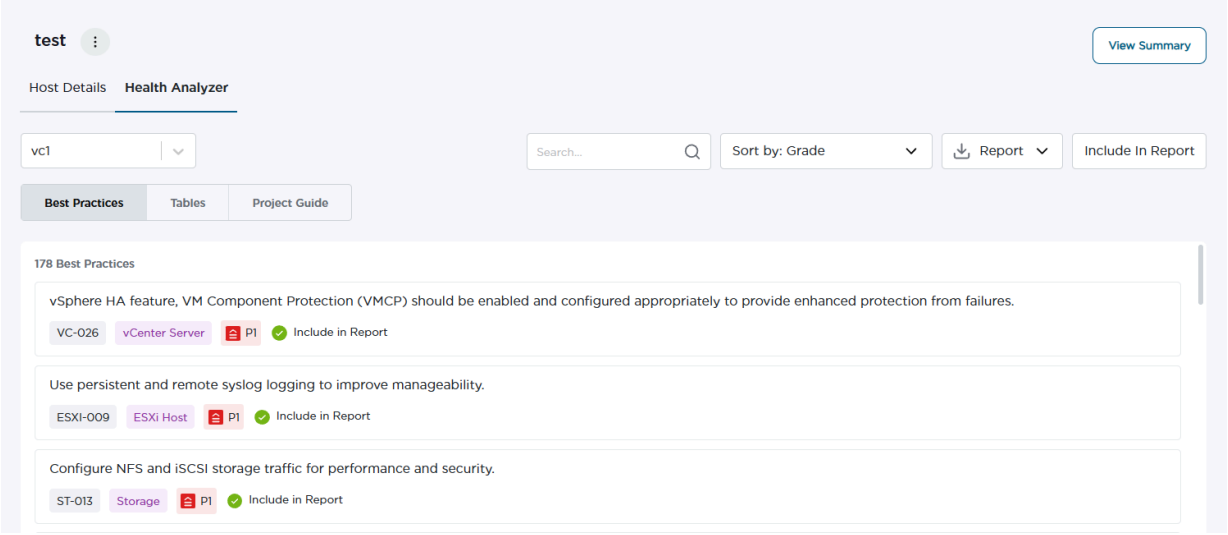


Few Best Practices

- Always validate and review reports before sending them to Broadcom.
- Ensure only completed and green-status hosts are selected when generating reports.
- Use both Excel and JSON formats as needed for compatibility with downstream systems.

10. Health Analyzer Tab

After data collection is completed, the **Health Analyzer** tab provides an in-depth analysis of best practices and recommendations for improving system performance and health.



Navigating Health Analyzer

From your project dashboard:

- Click on the **Health Analyzer** tab.
- Select a host (e.g., XCXCXC) to view detailed results.
- You'll see options like:
    - **Best Practices**
    - **Tables**
    - **Project Guide**

10.1 Best Practices Section

This section displays a list of industry best practices

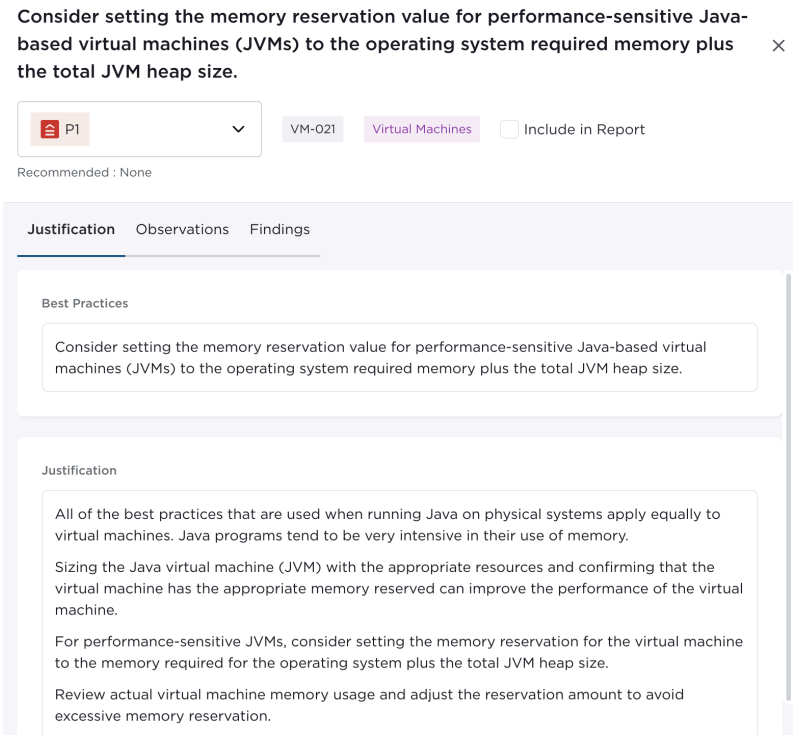
Each row contains:

- Recommendation title
- Category (e.g., Virtual Machines, vCenter Server)
- Status (OK, None, Warning)
- A checkbox to **Include in Report**

Example:
"Consider setting the memory reservation value for performance-sensitive Java-based virtual machines (JVMs)…"

Clicking a Best Practice: Details View

Clicking any best practice opens a detailed view with the following tabs:



A. Justification

- Explains the logic behind the recommendation, often with links to official VMware documentation.

B. Observations

- You can manually add formatted notes or observations using the rich-text editor. These could be site-specific findings or context.

C. Findings

- System-detected issues or deviations related to the best practice. If data is unavailable, it will say “Data not available”.
- Option to **Export** individual recommendation details using the blue **“Export”** button.

10.2 Filtering and Reporting

- Use the **Search** and **Filters** tools at the top to find specific best practices.
- Use the **Report** dropdown to generate health reports including selected recommendations
- Use the **Include In Report** button (introduced in HST 1.0.3) to bulk select/deselect findings by component or grade.

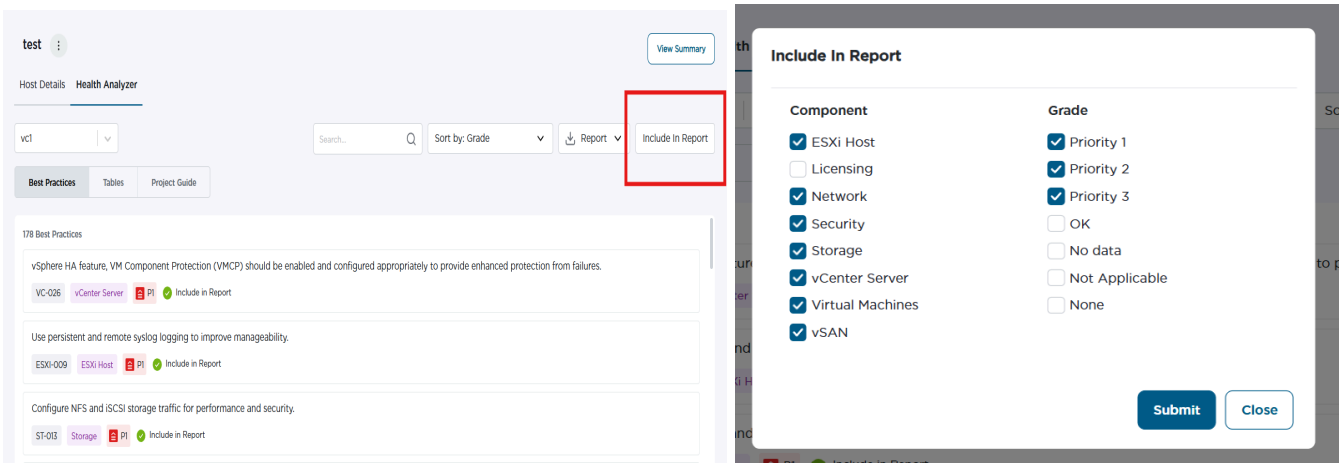
10.3 Health Check Analysis

The Health Analysis process is only performed when a Broadcom Employee or Partner collects or imports an HST project. If a customer completes a collection, then an employee/partner logs in to the same appliance, they may see “Analysis not started.” Today, the project will need to be exported/imported for the analysis to begin.

Note: This behavior changed starting in HST 1.0.2. Prior to this release, analysis began immediately after the data collection. In large collections, this could cause a deadlock where multiple concurrent collections & assessments could cause the application to become non responsive.

10.4 Bulk Update Include In Report Flag

We can do the bulk update to the include in report flag using below option

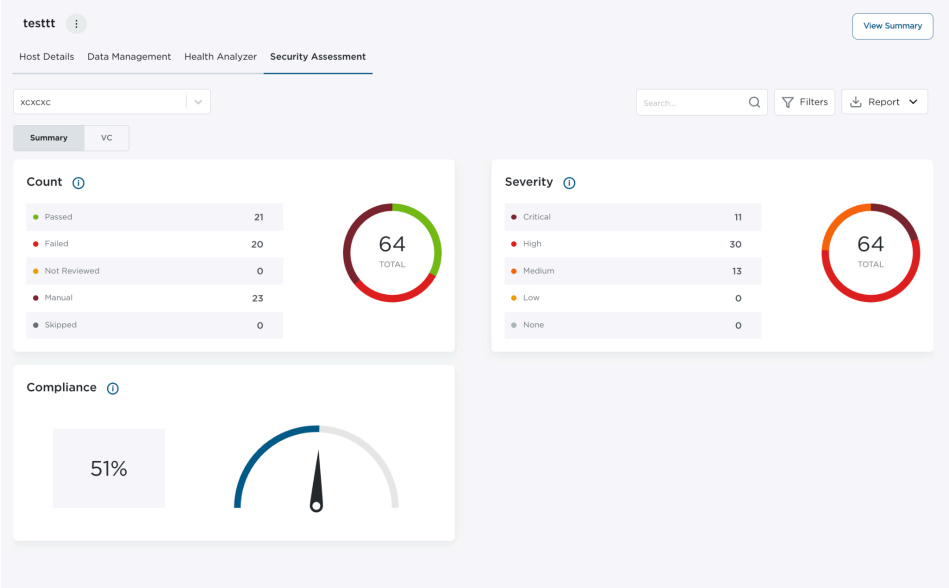


Once you submit this page, the system will update the Include in Report flag for all the Best Practices that match the component types and grades you selected.

This means that only the Best Practices with the chosen component and grade combinations will be included in the report generated.

11. Security Assessment Tab Guide

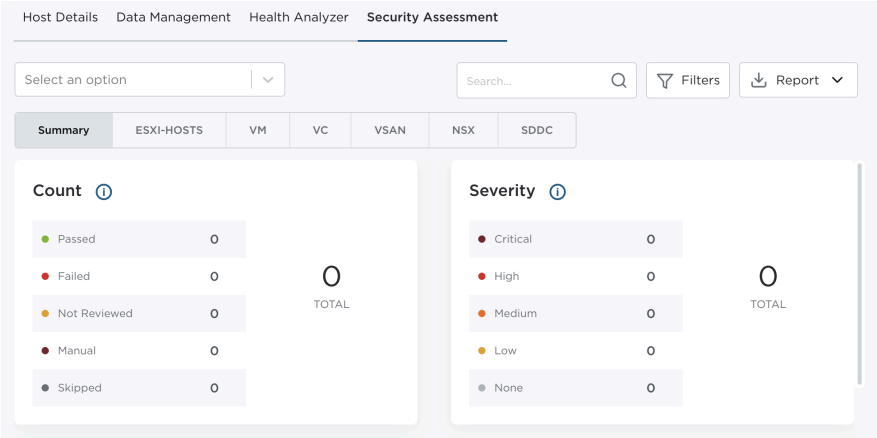
The **Security Assessment** tab helps evaluate compliance of your VMware environment with best-practice security controls. This includes tests for ESXi hosts, VMs, vCenter, vSAN, NSX, and SDDC.



Navigating Security Assessment

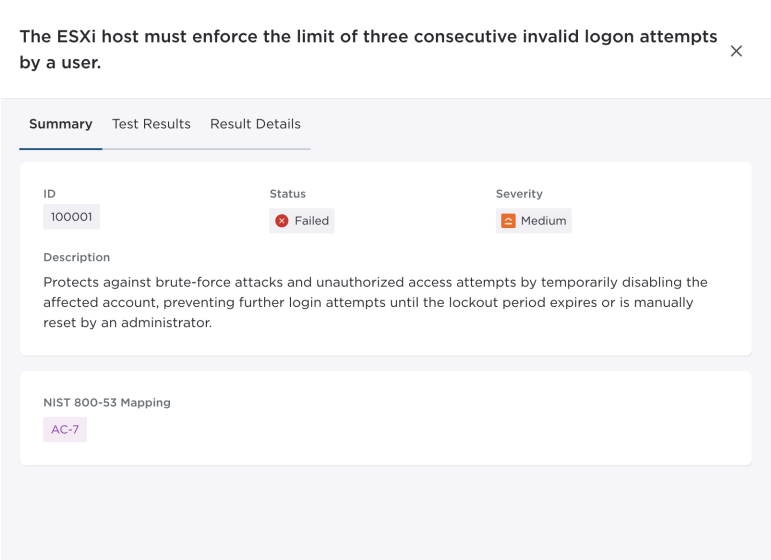
- Go to your project and click the **Security Assessment** tab.
- From the dataset dropdown, select the desired host or data source.
- Tabs available:
    - **Summary**
    - **ESXI-HOSTS**
    - **VM**
    - **VC**
    - **vSAN**
    - **NSX**
    - **SDDC**

Each tab presents results relevant to that component category.



11.1 Detailed Control View

When clicking any of the controls (e.g., “The ESXi host must enforce the limit of three consecutive invalid logon attempts by a user”), you’ll see three tabs:



A. Summary

- Explains the control’s purpose (e.g., protect against brute-force attacks).
- Lists the NIST 800-53 mapping..

B. Test Results

- Displays actual command outputs (e.g., PowerCLI tests).
- Shows expected value vs actual value.
- **Example:** Expected 3, Got 5 = Failed.

C. Result Details

- Provide details on the check and fix tests.

11.2 Using Filters and Export

- Use the **Filters** to sort controls by status or severity.
- Use the **Report** dropdown to export detailed or summary reports.

11.3 Summary View

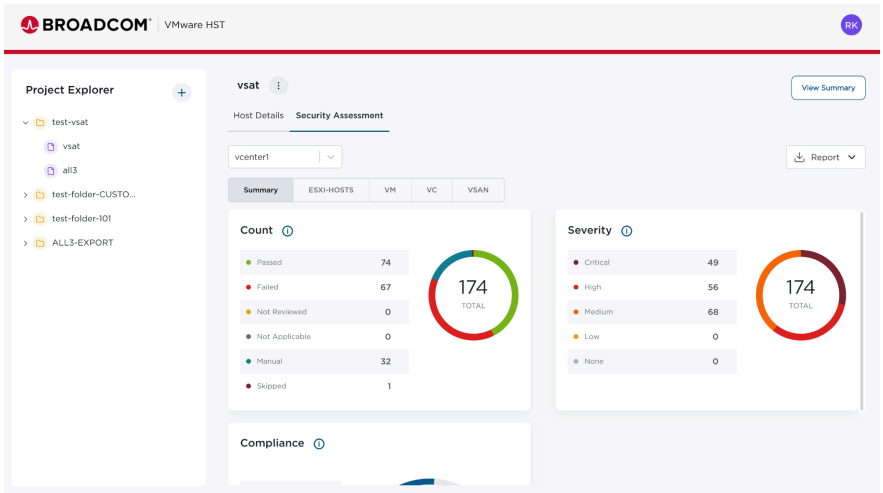
Click the **Summary** tab to see a high-level compliance overview across all components (e.g., number of passed/failed controls in each category).

11.4 Steps to Download Executive and Administrative Reports

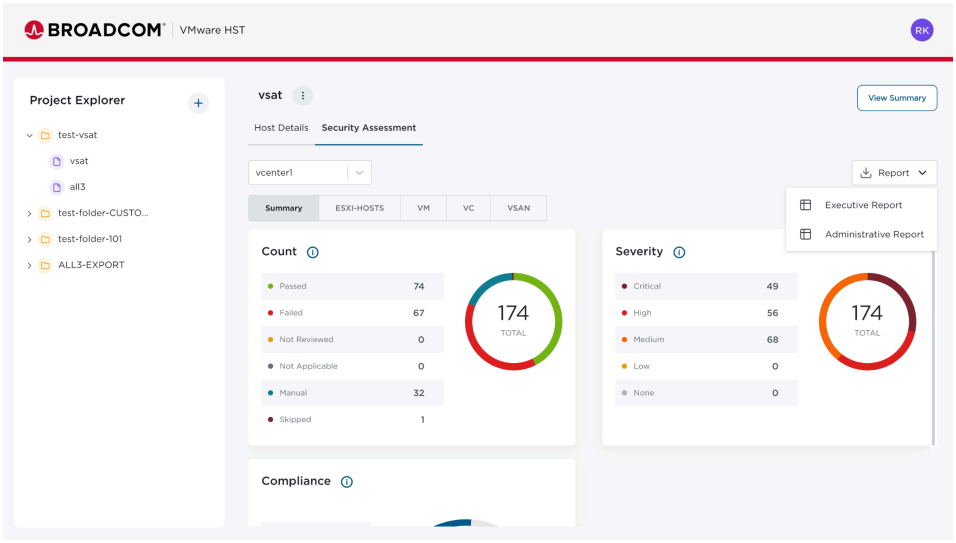
The Security Assessment module allows you to generate executive summaries and detailed administrative reports for your vCenter environments.

To generate a report:

1. **Navigate to the Security Assessment Tab**
    - Click on the **Security Assessment** tab located in the main navigation menu at the top of the screen.



2. **Filter by Entity**
    - Locate the entity filter, which defaults to **All - Summary**.
    - Click the dropdown menu and select **vCenter/NSX/SDDC** from the list. This will scope the report data specifically to your vCenter assets.



Open the Report Menu

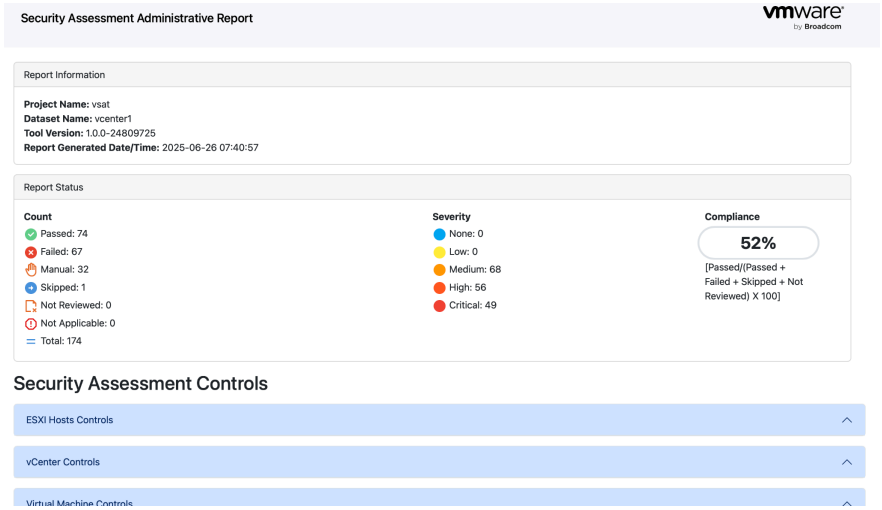
- On the right side of the screen, locate and click the **Report** dropdown button to reveal the available report types.

3. **Select and Download the Report**
   - From the **Report** dropdown menu, click on the report you wish to download:
     - **Executive Report:** Select this for a high-level summary of findings, key risks, and compliance status. This report is ideal for management and stakeholders.
     - **Administrative Report:** Select this for a comprehensive, detailed breakdown of all assessment checks, vulnerabilities, and configuration data. This report is designed for system administrators and technical teams.
4. **Confirm the Download**
   - The selected report will automatically be generated and downloaded by your browser. Check your browser's default "Downloads" folder to access the file.

Sample Executive report:



Administrative Report Sample:

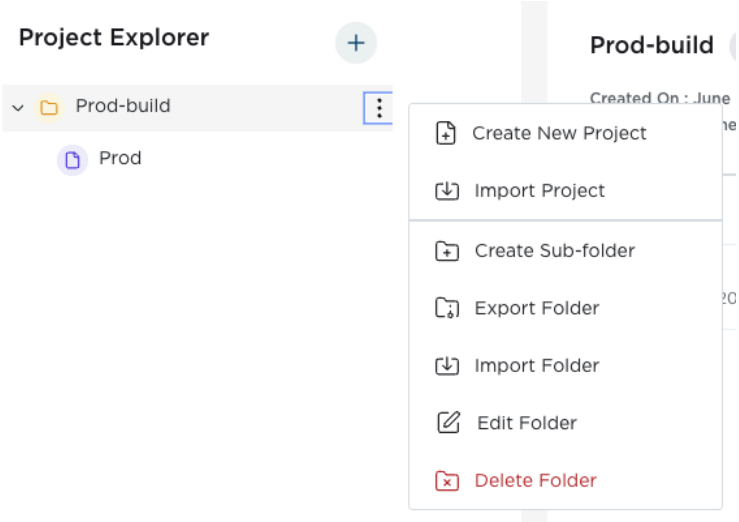


12. Project and Folder Management

Once users are inside the VMware HST dashboard, they can efficiently manage their workspace through folders and project-level operations.

12.1 Project Explorer Actions

Click the **three dots** beside any folder to see a dropdown menu with these options:



a. Create New Project

- Initiates the new project creation wizard.
- You'll walk through steps for adding host data, agreements, and confirming details.

b. Import Project

- Prompts you to upload a project file (csv).
- Restores previously exported project data for review or rerun.

c. Create Sub-Folder

- Adds a nested folder under the selected parent.
- Requires:
  - **Folder name** (mandatory)
  - **Description** (optional)

d. Export Folder

- Saves the folder's contents locally.
- A file like `hst-export-folder-test1232-050820.hst` is downloaded.

e. Import Folder

- Used to restore an exported folder file back into HST.
- Must upload the `.hst` file exported previously.

f. Edit Folder

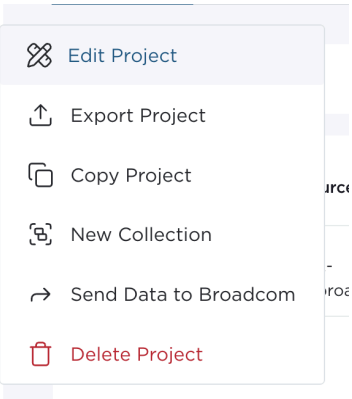
- Allows renaming or updating the folder description.

g. Delete Folder

- Permanently deletes the selected folder and all contents.
- A confirmation prompt appears (e.g., “Are you sure you want to delete ‘Project’?”).

12.2 Project-Level Options

Clicking on a project name (like **test nsx**) and expanding the options shows:



- **Edit Project** – Change basic project metadata.
- **Copy Project** – Duplicate the project (useful for baseline or clone scenarios).
- **New Collection** – Trigger a fresh data collection using the same hosts.
- **Send Data to Broadcom** –
- **Delete Project** – Permanently removes the project and all related data.

Revision History

Version 1.0.4; August 2026

Version 1.0.3; December 2025

Version 1.0.2; September 2025

Version 1.0.1; July 2025

Version 1.0; June, 2025


BROADCOM®