Host Security Scanner

Getting Started Guide

Powered By Retina

 TC:5/15/2019

Table of Contents

BeyondTrust Host Security Scanner Introduction and Overview

This guide shows system administrators how to manually install, configure, and use the BeyondTrust Host Security Scanner.

The BeyondTrust Host Security Scanner is a host-based vulnerability scanner that eliminates the need for connectivity between a traditional network scanner and its target asset. Fast and highly accurate, the Host Security Scanner is a lightweight agent based on BeyondTrust Network Security Scanner's award-winning technology and has over ten years of experience across thousands of enterprise customers.

Unlike network-based scanners, BeyondTrust Host Security Scanner resides on a machine and collects vulnerability, configuration, and asset data locally and sends that information to the BeyondInsight platform for centralized management, reporting, and analysis.

Download the BeyondTrust Host Security Scanner

You can download the Host Security Scanner from our customer portal at www.beyondtrust.com/support.

> ***Note:*** *A username and password are required to log into the portal.*

Host Security Scanner for Windows Prerequisites

BeyondTrust Solutions (Required)	BeyondInsight 6.0 or higher
Operating Systems	Windows 7 SP1 or later (32-bit and 64-bit) Windows 8.1 (32-bit and 64-bit) Windows 10 (32-bit and 64-bit) Windows Server 2008 R2 SP1 or later (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit) Windows Server 2019 (64-bit)
Processor	Intel Dual Core 2.0Ghz (or compatible)
Memory (RAM)	8 GB
Hard Drive	4 GB
Software	Microsoft .Net Framework 4.5.2 or later Microsoft Visual Studio 2008 and 2017 C++ Redistributable (included with the .EXE installer) Universal C Runtime
Network	Ports 443 and 21690 are required for integration with BeyondInsight Network Interface Card (NIC) with TCP/IP enabled

Host Security Scanner for Linux and macOS Prerequisites

BeyondTrust Solutions (Required)	BeyondInsight 12.4.7 or higher
Operating Systems	Debian 8 (x64) Debian 9 (x64) macOS 10.12.x Oracle Enterprise Linux 7.x (x64) Red Hat Enterprise Linux 7.x (x64) Ubuntu 16.x
Processor	Intel Dual Core 2.0Ghz (or compatible)

Memory (RAM)	8 GB
Hard Drive	4 GB
Network	Port 443 is required for integration with BeyondInsight Network Interface Card (NIC) with TCP/IP enabled

Install BeyondTrust Host Security Scanner

You can choose to install the Host Security Scanner manually, or you can automate the installation and configuration process by using the BeyondTrust Deployment Package Wizard. The Deployment Package Wizard allows you to create a standalone installer that includes the settings needed to silently deploy and configure the Host Security Scanner.

> ***Note:*** *The Deployment Package Wizard is limited to BeyondTrust Host Security Scanner for Windows. For deployment options for Linux and macOS, please see the* *Appendix: Linux and macOS Configuration Deployment*.

You can download the Deployment Package Wizard from the customer portal:

www.beyondtrust.com/support

Manually Install Host Security Scanner on Windows

The manual configuration of the Host Security Scanner requires Windows PowerShell 4.0. Only the following Windows operating systems are supported for manual configuration:

- **Windows 8.1:** PowerShell 4.0 installed by default
- **Windows Server 2012 R2:**PowerShell 4.0 installed by default
- **Windows 7 with Service Pack 1:** Requires Windows Management Framework 4.0 to run PowerShell 4.0
- **Windows Server 2008 R2 with Service Pack 1:** Requires Windows Management Framework 4.0 to run PowerShell 4.0

All other supported operating systems require the use of the Deployment Package Wizard.

To manually install the Host Security Scanner, double-click the Host Security Scanner installer, or execute the installer using an elevated command prompt.

Install Host Security Scanner on Linux

The Host Security Scanner for Linux is distributed in standard Linux package formats or as a direct tarball. If the target platform is supported, the package format is preferred.

The Host Security Scanner for Linux comes with different package files that make updating audits easy.

Package Installation

To install the Host Security Scanner for Linux from a Linux package, retrieve the proper package type for the platform, and run the install command specific to that package type.

Debian and Ubuntu Based Systems

For Debian and Ubuntu-based systems, the packages should look similar to the following:

- **host-security-scanner_<version>_amd64.deb**
- **host-security-scanner-common_<version>_all.deb**
- **host-security-scanner-vdb_<version>_all.deb**

> ***Note:*** *If necessary, unpack the tarball by issuing the command* `tar -zxvf BeyondTrust*.tar.gz`.

To test the install, make sure the files are in one location and issue the command:

```
dpkg --dry-run -i *.deb
```

The **--dry-run** parameter skips installing the packages but tests for needed dependencies, such as package integrity.

To run the install, issue the command without the **--dry-run** option:

```
dpkg -i *.deb
```

Red Hat Enterprise Linux

For RHEL, the packages should look similar to the following:

- **host-security-scanner_<version>_amd64.rpm**
- **host-security-scanner-common_<version>.noarch.rpm**
- **host-security-scanner-vdb_<version>.noarch.rpm**

To run the install, issue this command:

```
yum install *.rpm
```

Install Host Security Scanner on macOS

The Host Security Scanner for macOS is distributed as a .zip file. Extract the contents to the location of your choice.

Configure the BeyondTrust Host Security Scanner

Configure Host Security Scanner for Windows

Import the Module

Before the cmdlets will be available, the Host Security Scanner's PowerShell module must be imported into PowerShell. The BeyondTrust PowerShell .dll is located at **<InstallDir>\API\PowerShell**.

Open a PowerShell session, and use the **Import-Module** cmdlet:

```
Import-Module .\Retina.PowerShell.dll
```

If you are not in the **<InstallDir>\API\PowerShell** directory, you need to specify the full path. Place this code into your PowerShell profile to automatically import the module.

Samples

In the **<InstallDir>\API\PowerShell\Samples** directory, there are a number of scripts that use many of the available cmdlets. These scripts are helpful examples of cmdlet usage and can serve as a starting point for your own scripts.

Licensing via PowerShell

1. Launch **PowerShell**.
2. Load the **PowerShell module**.

For more information, please see "Import the Module" on page 8.

3. Execute **License.ps1** in the **<InstallDir>\API\PowerShell\Samples** directory.

```
PS C:\Program Files (x86)\BeyondTrust\Install\Security Scanner\API\PowerShell\Samples\License.ps1
```

4. Enter your serial number.

Activate Central Policy Using PowerShell

1. Launch **PowerShell**.
2. Load the **PowerShell module**.
3. Execute the **ManageCentralPolicy.ps1** script in the **<InstallDir>\API\PowerShell\Samples** directory.

```
& 'C:\Program Files (x86)\BeyondTrust\Security

Scanner\API\PowerShell\Samples\ManageCentralPolicy.ps1
```

4. The script prompts you for the
   - IP Address of your BeyondInsight server
   - Central Policy password

Using this cmdlet, you can retrieve and review the current Central Policy settings.


```
Get-RetinaCentralPolicySettings
```

Using this cmdlet, you can test the current Central Policy settings.

```
Test-RetinaCentralPolicy
```

Set up Events Management

The management console needs to be aware of Host Security Scanner as a supported application. Scanner events are sent to the management console where you can be manage and review scan activities.

> ***Note:** When you initially install the management console, configure the following client settings using the **Events Client Configuration Wizard**: Host and Port information, Workgroup Settings, Certificate Selection, and Agent Applications.*

> For more information on using the wizard, please see the management console's documentation.

To also configure client settings after running the wizard, follow these steps:

1. Start the **Events Client Configuration** tool. The default location is **Start > All Programs > BeyondTrust > Tools**.
2. If it is not already selected, select the **Enabled Applications** tab.
3. Check the **Network Scanner** box.
4. Click **OK**.

Configure Host Security Scanner for Linux

The main configuration for Linux is stored in the **retinaconfig.xml** file. It comes with a simple utility to update common connectivity settings like **config**.

This allows you to configure Central Policy, Events, and Auto-Updates. Central Policy and Event configuration are required in order to centrally manage the Host Security Scanner via BeyondInsight.

When **Auto-Update** is enabled, it checks for updates daily at the time specified by the user.

To run the configuration utility on Linux, follow these steps:

1. Obtain a copy of the **eEyeEMSClient.pfx** from your BeyondInsight server, and copy it into the **/opt/BeyondTrust/host-security-scanner/** directory.
2. Launch **Terminal**.
3. Change the base directory to **/opt/BeyondTrust/host-security-scanner**.
4. Issue the command `./Scanner/config`.

> For more information, please see *Reference Appendix A* of the *BeyondInsight Installation Guide* for steps on generating the **eEyeEMSClient.pfx**.

Get Started Using the BeyondTrust Host Security Scanner

Run a Scan on Windows

The Host Security Scanner can be managed locally via PowerShell or managed centrally via BeyondInsight.

For more information on BeyondInsight central management, please see the *BeyondInsight User Guide*.

You can initiate a localhost scan by calling **StartScan.ps1** found in the **<InstallDir>\API\PowerShell\Samples** directory.

If it is not already loaded, load the PowerShell module. For more information, please see "Import the Module" on page 8.

***Note:** Running the **StartScan.ps1** script starts four scans at the same time. Running this script can take some time.*

```
<InstallDir>\API\PowerShell\Samples\StartScan.ps1
```

This command starts a default **All Audits-Common Ports** scan of the system where the scanner is installed.

For additional scan control via PowerShell, please see the PowerShell Integration Guide.

Run a Report

Reports can be generated by specifying a **Report Type** to run. Currently, you can generate Remediation, Compliance, Dashboard, PCI, Vulnerability Export, and XML Assessment reports.

Reports are generated using the **Get-RetinaScanResults -ReportType** cmdlet

```
Get-RetinaScanResults -ReportType Remediation
```

This generates a report based on your last completed scan. The report is saved in the following location: **<InstallDir>\Reports\Temp**.

***Note:** For consolidated reporting across all your Host Security Scanners, please check out BeyondInsight.*

For advanced reporting options, such as reporting on specific scans, please see the PowerShell Integration Guide.

Run a Scan on Linux

The Central Policy service establishes connections to a BeyondInsight server for configuration and other details, including scan scheduling. It normally runs in the background and invokes the scanner as needed.

1. Change the base directory to **/opt/BeyondTrust/host-security-scanner/**.
2. Issue the command **./Scanner/scanner**.

Run a Report

A simple XML report can be generated from completed scans by running the reporter. By default, the reporter attempts to generate a report for the most recently run scan. Command-line parameters can be passed to specify scans by **JobID**, **GroupID**, or scan file.

> For more information, please see the command-line help.

1. Change the base directory to **/opt/BeyondTrust/host-security-scanner/**.
2. Issue the command **./Scanner/reporter**.

Output

By default, all programs write log files to **<InstallDir>base dir>/WorkFiles/Logs**.

- Scans are stored in files under **<InstallDir> base dir>/WorkFiles/Scans**.
- Reports are stored in files under **<InstallDir> base dir>/WorkFiles/Reports**.

Run a Scan on macOS

The Central Policy service establishes connections to a BeyondInsight server for configuration and other details, including scan scheduling. It normally runs in the background and invokes the scanner as needed.

Run the Central Policy Service

If the Central Policy is not configured to start automatically, it can be manually launched.

1. Change to the base directory **host-security-scanner/Contents/Resources/**.
2. On macOS, issue the command **../MacOS/centralpolicyd**.

Run a Scan

The Central Policy service normally start scans as needed. However, scanning can be invoked manually.

1. Change the base directory to **host-security-scanner/Contents/Resources/**.
2. Issue the command **../MacOS/scanner**.

Run a Report

A simple XML report can be generated from completed scans by running the reporter. By default, the reporter attempts to generate a report for the most recently run scan. Command-line parameters can be passed to specify scans by **JobID**, **GroupID**, or scan file.

> For more information, please see the command-line help.

1. Change the base directory to **host-security-scanner/Contents/Resources/**.
2. Change the base directory to **CCSVM_Host_Agent/Contents/Resources**.
3. Issue the command **../MacOS/reporter**.

Output

By default, all programs write log files to **<InstallDir>base dir>/WorkFiles/Logs**.

- Scans are stored in files under **<InstallDir> base dir>/WorkFiles/Scans**.
- Reports are stored in files under **<InstallDir> base dir>/WorkFiles/Reports**.

Appendix: Linux and macOS Configuration Deployment

Introduction

This guide provides information on deploying configuration settings for the Linux and macOS versions of BeyondTrust Host Security Scanner. Configuration can be performed at one location, and then pushed out to endpoints as needed.

Initial setup

Set up a system by installing the BeyondTrust Host Security Scanner package for the specific platform. This consists of a zip archive for macOS systems, an archive containing a set of **.deb** files for Debian and Ubuntu-based systems, or an archive containing a set of **.rpm** files for RHEL and CentOS-based systems.

Initial configuration

Once installed, open a terminal, and navigate to the base **Host Security Scanner** directory.

For Linux systems:

```
cd /opt/BeyondTrust/host-security-scanner
```

For macOS systems:

```
cd <parent>/host-security-scanner/Contents/Resources
```

This directory contains two configuration files: **retinaconfig.xml** and a hidden **.rdata.xml**. These two files contain the configuration settings that will be collected and pushed out to other systems. To edit these, run the config tool.

For Linux systems:

> ***Note:*** *Make sure to run this config with root privileges.*

```
./Scanner/config
```

For macOS systems:

> ***Note:*** *Make sure to run this config with root privileges.*

```
../MacOS/config
```

The tool runs through a set of options. The general sections are **Event Management**, **Central Policy**, and **Auto-Update**. If one of these is disabled, the settings for that specific section are not shown. The **Event Management** and **Central Policy** settings sections allow you to configure testing servers after configuring one of those sections.

> ***Note:*** *If the configuration tool runs without sufficient privileges, it is unable to write the configuration files at the end of the process. If this occurs, simply re-run after elevating privileges via* ***sudo*** *or* ***su.***

To verify the configuration files were successfully updated, run the following command:

```
ls -lart
```

This command displays a list of all the files in the directory with the newest appearing last. Check that the last two are **retinaconfig.xml** and **.rdata.xml**.

> ***Note:*** *If no settings were changed and the current defaults were kept, the configuration files are not updated and may show earlier in the list.*

Deployment to other systems

To automate deployment, make sure the base product is pushed out and installed on target endpoints. This might be via a deployment script using **scp** and then **unzip/rpm/dpkg** manually. For Linux systems, this can occur by adding the appropriate packages to any in-house, private repositories and triggering a package installation on the target systems. Once the targets have the product installed, the modified configuration can be copied into place.

To propagate the settings to other systems, copy the two configuration files, **retinaconfig.xml** and **.rdata.xml**, along with any specified certificate files used for event management, and push them out to the other endpoints using either a simple command or any normal, in-house automation mechanism.

> ***Note:*** *Be sure not to copy the* ***.sid*** *and* ***.bytrid*** *files because they contain settings to uniquely identify each individual endpoint.*

The two main configuration settings files are compatible across systems, and they can be configured on a single system and pushed out to both Linux and macOS endpoints.

Summary

- Install the product on one system.
- Configure the product on that system.
- Collect the configuration from that system.
  - **retinaconfig.xml**
  - **.rdata.xml**
  - **eEyeEMSClient.pfx** (if event management is enabled)
- Push and install the product on each endpoint.
- Copy the collected configuration files to each endpoint.
- Restart **centralpolicyd**.