Tenable Security Center Scan Tuning Guide

Last Revised: August 07, 2025

Table of Contents

Introduction

This guide describes each aspect of a Tenable Security Center scan configuration, and how you can tune each aspect to make your scan faster or more data-inclusive, depending on your desired outcome.

Considerations

Although your scan configuration plays an important role in your Tenable Security Center scan time and performance, other variables can affect the scan time and performance. The following table describes each variable that you should consider when trying to improve your scan time and performance:

Variable	Impact on Scan Time	Impact Description
Scan configuration	High	Your scan configuration specifies the depth of your scan. In general, increasing the depth of your scan increases the total scan time. Consider the following when planning your scan depth: • What type of port scanning is Tenable Security Center performing? • What ports are Tenable Security Center scanning? • What vulnerabilities are you scanning for? • Are you running credentialed scans? • Are you performing malware checks, filesystem checks, or configuration audits? You can use Tenable-provided templates to perform both targeted and all-encompassing checks. You can create custom policies to customize all possible policy settings.
Scanner resources available	High	The number of IP addresses you can assess simultaneously via a network scan largely depends on two things: • The number of available Nessus scanners to the scan job • The resources available to your internal Nessus scanners

		Increasing one or both of these factors is the fastest way to improve your rate of simultaneous assessment and overall scan time. However, large enterprise networks often have infrastructure or technology limitations that prohibit increasing these resources beyond a certain maximum. Your Nessus scanners should meet the hardware requirements whenever possible, but *exceeding* the minimum requirements lets your scanners assess more targets faster. **Note:** You cannot modify some Tenable Vulnerability Management cloud scanner settings.
Type of assessment	Medium	You have various options available for assessing assets in your environment. While the correct scan configuration can vary depending on your environment, you should build the most efficient scan configuration for your organization's assets or environment. For example: • Use agents for remote systems that are not local to your scanners • Use passive sensors for discovery or sensitive devices
Number of live hosts	Medium	Scanning a dead host takes less time than scanning a live host. A distribution of IP addresses with a low number of associated hosts takes less time to scan than a distribution of IP addresses with a higher number of hosts. You can choose to scan an entire range of IPs, or target specific ones, depending on the use case for that particular scan job. For more information, see Targets.
Target configurations	Medium	Scanning a locked-down system with few exposed network services takes less time than complicated target configurations. For example, a Windows server with a web

		server, database, and host intrusion prevention software takes more time to scan than a Windows 11 workstation.
Scanner proximity to targets	Medium	Tenable recommends placing your scanners close to your targets, connected with minimum latency (for more information, see the following [Tenable blog article](#)). Latency has an additive effect on every packet exchanged between a scanner and its target. The largest impacts tend to be network latency and simultaneous plugin checks. For example: • Scanning through routers, VPNs, load balancers, and firewalls can impact the fidelity of your scan results by blocking ports that should be open or by auto-responding to closed ports. • Scanning numerous hosts behind a single piece of network infrastructure can increase the load on your equipment, given the large number of sessions exchanged between scanner and host.
Time of day and week	Low	In many environments, there are periods of time where infrastructure load is higher. Scheduling assessments outside of these windows can improve scan performance.
Target resources	Low	The resources available to the scan target can impact scan time as well. A public-facing system (a system with load) takes longer to scan than an idle backup system.

Sensor Selection

Tenable Security Center allows you to actively assess targets with up to two sensor types: Tenable Nessus scanners or Tenable Agents.

If you need to scan assets that are external to your network, Tenable recommends using the cloud scanners provided by Tenable. The cloud scanners are managed by Tenable, and do not require any upkeep from your organization. For more information, contact your Tenable Account Team.

To scan assets within your network, you can choose between scanning with Nessus scanners or Tenable Agents. The following table describes the key differences between scanning with Nessus scanners and Nessus Agents:

Nessus scanners	
Pros	**Cons**
• Tenable Nessus scanners can scan entire networks, while Tenable Agents can only scan the asset they are installed on. • Tenable Nessus scanners allow you to perform external and remote security checks. • Unlike Tenable Agents, Nessus scanners provide an "outside view" of your network through features such as port scanning. Nessus scanners can also provide an "inside view" of your network if you configure them with credentials.	• Unlike Tenable Agents, you have to update Nessus scanner credentials manually. This can cause permission and login issues if your organization does not actively update the credentials. • Network scanning with Nessus scanners usually takes longer than scanning individual assets with Tenable Agents.
Tenable Agents	
Pros	**Cons**
• Tenable Agents are installed directly on the target assets, so unlike Tenable Nessus scanners, they do not require managed credentials. • Unlike Nessus scanners, you do not have to	• Tenable Agents are not designed to perform network checks, so certain plugin items cannot be checked if you only run agent scans.

worry about the geographical placement of Tenable Agents. • Generally, scanning individual assets with Tenable Agents is much faster than scanning the entire network. • Tenable Agents can collect and send asset data to their Tenable Nessus Manager. In other words, Tenable Agents enable you to scan assets that cannot communicate with or are not connected to your Tenable Security Center console.	• Tenable Agents cannot perform security checks that require remote connectivity, such as logging into a database server, trying default credentials, or traffic-related enumeration. • Unlike Tenable Nessus scanners, Tenable Agent scans cannot account for any assets that do not have a Tenable Agent installed.

Ultimately, Tenable recommends using whichever sensor best suits your environment and business requirements. In many circumstances, you should use both agents and network assessments for different types of systems and parts of your network. To learn more about the benefits and limitations of agent scanning, see Benefits and Limitations in the *Nessus Agent User Guide*.

Scan Policy Template Selection

Tenable Security Center provides various scanner and Nessus Agent scan templates that meet different business needs. Tenable Security Center provides three categories of scan templates: Common scans, Compliance scans, and Configuration scans. You can view Tenable Security Center's complete offering of scan templates when you add a scan policy template n the user interface.

Click the following scan template categories to view the descriptions. For information about specific scan templates, see Scan Policy Templates.

> **Note:** Depending on the scan template you use, you may not be able to tune some of the settings described. The Advanced Scan and Advanced Agent Scan templates allow you to adjust all the described settings available to each assessment type.

Common / Vulnerability Scans

Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs. Some of Tenable Security Center's most notable vulnerability scan templates are:

- Advanced Agent Scan — The most configurable scan type that Tenable Security Center offers. You can configure this scan template to match any policy search any asset or assets. These policies have the same default settings as the Basic Network/Agent Scan, but they allow for more additional configuration options.

  > **Note:** Advanced scan templates allow Tenable Security Center experts to scan more deeply using custom configuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution.

- Basic Network Scan — Use this template to scan a system or systems with all of Tenable Security Center's current default plugins enabled. This scan provides a quick and easy way to scan systems for vulnerabilities.

- Credentialed Patch Audit (Nessus Scanner only) — Use this template with credentials to give the scanner direct access to the host, scans the target hosts, and enumerates missing patch updates.

- Host Discovery Scan (Nessus Scanner only) — Launch this scan to see what hosts are on your network, and associated information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan.

  Tenable recommends that organizations who do not have a passive network monitor, such as Tenable Network Monitor, run this scan weekly to discover new assets on your network.

  > **Note:** Assets identified by discovery scans do not count toward your license.

Configuration Scans

Tenable recommends using configuration scan templates to check whether host configurations are compliant with various industry standards. Configuration scans are sometimes referred to as *compliance* scans. For more information about the checks that compliance scans can perform, see Audit Files and SCAP scans.

Other / Tactical Scans

Tenable recommends using the tactical scan templates to scan your network for a specific vulnerability or group of vulnerabilities.

Tactical scans are lightweight, timely scan templates that you can use to scan your assets for a particular vulnerability. Tenable frequently updates the library with templates that detect the latest vulnerabilities of public interest.

Scan Policy Settings

Once you select the scan template to use for your scan, there are several configurations that you can use to tune the scan policy configuration's performance. The following sections describe each of the scan policy configuration setting sections (Advanced, Host Discovery, Port Scanning, Service Discovery, Assessment, Brute Force, Malware, SCADA, Web Applications, Windows, Report, Authentication, Compliance, and Plugins) and how you can configure each section to maximize your scan's performance.

> **Note:** Depending on what scan template you choose, you may not see some of the settings and sections described. For example, most scan templates do not allow you to configure plugin families.

Many configuration settings affect the scan's capabilities, accuracy, and performance. Use the settings to configure discovery options, debugging capabilities, assessment methods, performance options, and other scan behavior. Some of the scan policy configuration settings are informational or do not affect scan performance (for example, Name, Description, and Tag settings). This section describes all the settings that can affect scan performance and how to tune them for better scan performance.

Discovery

The Discovery settings determine the scan configuration's discovery-related capabilities: host discovery, port scanning, and service discovery.

Discovery settings are limited for Nessus Agent scan templates because agents cannot perform remote checks or scan the network. You can only set the WMI and SSH settings for agent scans.

Setting	Description	Tuning Tips
Host Discovery		
Ping the remote host	If set to `On`, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options **General Settings** and **Ping Methods** appear. If set to `Off`, the scanner does not ping remote hosts on multiple ports during the scan. **Note:** To scan VMware guest systems, **Ping the remote**	

	host must be set to **Off**.	
Use fast network discovery (available if Ping the remote host is enabled)	When disabled, if a host responds to ping, Tenable Security Center attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is firewalled. When enabled, Tenable Security Center does not perform these checks.	This setting can increase scan speed, but it may not be appropriate in all environments due to target configurations.
Ping Methods (available if Ping the remote host is enabled)	Specifies the sensor's pinging method.	In most environments, Tenable recommends using the default ping methods. Enabling UDP decreases scan speed. For more information, see the Ping Type Order/Hierarchy community article.
Fragile Devices	Determines which fragile devices the scanner or scanners detect. You can enable scanning for network printers, Novell NetWare hosts, and Operational Technology (OT) devices.	Tenable does not recommend scanning fragile devices in a production environment because it may

		cause an operational impact. If you have a need to assess OT devices, consider using OT Security to perform in-depth assessments.
Wake-on-LAN	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan. You can provide a list of hosts that you want to start before scanning by uploading a text file that lists one MAC address per line.	
Port Scanning		
Consider Unscanned Ports as Closed	When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.	
Port Scan Range	Specifies the range of ports to be scanned. The supported ranges are: • `default` — Instructs the scanner to scan approximately 4,790 commonly used ports specified in the `nessus-services` file. You can also combine the `default` keyword with other ports and port ranges. **Note:** You can convert the `nessus-services` file to a custom list of ports by performing four consecutive regular expression (regex)	Scanning more ports will decrease scan speed. If you have insight into local cross-traffic in your network, you can refine this setting to

	replace-all operations in a text editor that supports such operations: - `.*\s+(\d+)\/(tcp|udp)(\r\n|\r|\n) to $1\/$2,` - `(\d+)\/(tcp|udp) to $2:$1` - `tcp to T` - `udp to U` You can find the `nessus-services` file in the following directories, depending on your operating system: - Linux — /opt/nessus/var/nessus/nessus-services - Windows — C:\ProgramData\Tenable\Nessus\nessus\nessus-services - macOS — /Library/Nessus/run/var/nessus/nessus-services - `all` — Instructs the scanner to scan all 65,536 ports, excluding port 0. You cannot combine the `all` keyword with other ranges. - A comma-separated list of ports (for example, **21,23,25,80,110**), port ranges (for example, **1-1024,9000-9200** or **1-65535** to scan all ports but 0 and **T:1-1024,U:300-500** or **1-1024,T:1024-65535,U:1025** to scan separate or overlapping TCP and UDP port ranges), or combinations thereof. If you disable the UDP, SYN, or TCP port scanner settings in the scan policy **Discovery** settings, those ports are not scanned despite what range of ports you specify. The UDP and TCP port scanner settings are	only include the active listening services on your network, but this may cause the scan to miss unknown services. For more information, see Port Scanning Options in the *Tenable Security Center User Guide*.

	disabled by default; the SYN port scanner setting is enabled by default.	
SSH (netstat)	When enabled, the scanner uses the local netstat command to determine open ports while performing an authenticated SSH-based scan.	When the SSH, WMI, or SNMP settings are enabled, the scanner: • ignores any custom range specified in the **Port Scan Range** setting, and • continues to treat unscanned ports as closed if the **Consider unscanned ports as closed** setting is enabled. If any port enumerator (netstat or

		SNMP) is successful, the port range becomes *all*.
WMI (netstat)	When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via a WMI connection to the target.	
SNMP	When enabled, the scanner uses SNMP details to determine open ports while performing an authenticated SNMP-based scan.	
Only run network port scanners if local port enumeration failed	If a local port enumerator runs, all network port scanners will be disabled for that asset. (This is per scan target, and the effect is network port enumeration scan is disabled, not delayed.)	Enabling this setting decreases scan speed.
Verify open TCP ports found by local port enumerators	When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).	Enabling this setting decreases scan speed.
TCP	Use the built-in Tenable Nessus TCP scanner to identify open TCP ports on the targets, using a full TCP three-way handshake. If you enable this option, you can also set the **Override Automatic Firewall Detection** option.	TCP scanning is less efficient than SYN scanning. In most cases, enabling the TCP scanner decreases scan speed.
SYN	Use the built-in Tenable Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK	SYN scanning is more efficient than TCP scanning in

	reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the **Override Automatic Firewall Detection** option.	most circumstances due to less network traffic.
Override automatic firewall detection	When enabled, this setting overrides automatic firewall detection. To use this setting, you must enable the **TCP** or **SYN** option. This setting has three options: • **Ignore closed ports (aggressive)** attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network. • **Do not detect RST rate (soft)** disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device. • **Disabled (softer)** disables the firewall detection feature.	By default, Nessus will not test ports it detects as closed. This setting allows more control over that firewall detection method. Enabling this setting decreases scan speed.
UDP	This option engages the built-in Tenable Nessus UDP scanner and attempts to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports.	Enabling the UDP port scanner may dramatically decreases scan speed and produce unreliable results. Consider using the local port enumeration options instead

		if possible.
Service Discovery		
Probe all ports to find services	When enabled, the scanner attempts to map each open port with the service that is running on that port, as defined by the **Port scan range** option. **Caution:** In some rare cases, probing might disrupt some services and cause unforeseen side effects.	
Search for SSL/TLS/DTLS services	Controls how the scanner tests SSL-based services. **Caution:** Testing for SSL capability on all ports may be disruptive for the tested host.	Enabling CRL checking increases scan speed.

For more information, see Discovery Settings in Vulnerability Management Scans. To learn more about the preconfigured Discovery scan template settings, see Preconfigured Discovery Settings.

Assessment

The Assessment section allows you to configure how the scan identifies vulnerabilities and which vulnerabilities the sensors identify. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

Setting or Settings Group	Description	Tuning Tips
General		
Override normal accuracy	In some cases, Tenable Security Center cannot remotely determine whether a flaw is present or not. If report paranoia is set to **Show potential false alarms**, a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of **Avoid potential false alarms** causes Tenable Security Center to not report any flaw whenever there is a hint of uncertainty about the remote host. As a	

	middle ground between these two settings, disable this setting.	
Perform thorough tests (may disrupt your network or impact scan speed)	Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin analyzes 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.	Enabling this setting decreases scan speed.
Antivirus definition grace period (in days)	Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Tenable to allow for a specific grace time in reporting when antivirus signatures are out of date. By default, Tenable considers signatures out of date regardless of how long ago an update became available (for example, a few hours ago). You can configure this option to allow for up to 7 days before reporting them out of date.	
SMTP	Allows you to enable SMTP testing on the scan configuration.	
Brute Force (Nessus Scanner templates only)		
Only use credentials provided by the user	In some cases, Tenable can test for default accounts and known or default passwords. This can cause a default account or an account with a common name (for example, *admin* or *root*) to lock as a result of consecutive well-known passwords, resulting in invalid attempts that trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Tenable from performing these tests.	Enabling this setting decreases scan speed.

Test default accounts (slow)	Test for known default accounts in Oracle software.	Enabling this setting decreases scan speed.
SCADA (Nessus Scanner templates only) *This is a legacy configuration and should not be altered in most environments. You can use OT Security to assess SCADA systems.*		
Modbus/TCP Coil Access	Modbus uses a function code of 1 to read coils in a Modbus child. Coils represent binary output settings and are mapped to actuators typically. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message.	
ICCP/COTP TSAP Addressing Weakness	The ICCP/COTP TSAP Addressing menu determines a Connection-Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.	
Web Applications (Nessus Scanner templates only)		
Scan web applications	If enabled, Nessus enables web application-level checks. This setting can be useful for scanning network services running web applications. To scan for more generic web application vulnerabilities like Cross Site Scripting or SQL Injection, Tenable recommends using the Tenable Web App Scanning module. For more information, see Tenable Web App Scanning Scanning Overview.	Enabling this setting decreases scan speed.
Windows		
Request information about the SMB	If enabled, domain users are queried instead of local users.	Enabling this setting decreases scan speed.

Domain		
User Enumeration Methods	You can enable as many of the user enumeration methods as appropriate for user discovery.	Enabling this setting decreases scan speed.
Malware		
Malware Scan	Configures the policy to scan for malware on the target hosts. Enable this setting to view the remaining Malware options.	Enabling this setting decreases scan speed.
Disable DNS resolution	Checking this option prevents Tenable from using the cloud to compare scan findings against known malware.	
Provide your own list of known bad MD5 hashes	A text file with one MD5 hash per line that specifies more known bad MD5 hashes. Optionally, you can include a description for a hash by adding a comma after the hash, followed by the description. If the sensor finds any matches when scanning a target, the description appears in the scan results. You can also use hash-delimited comments (for example, fop) in addition to comma-separated comments.	Enabling this setting decreases scan speed.
Provide your own list of known good MD5 hashes	A text file with one MD5 hash per line that specifies more known good MD5 hashes. Optionally, you can include a description for each hash by adding a comma after the hash, followed by the description. If the sensor finds any matches when scanning a target, and you provide a description for the hash, the description appears in the scan results. You can also use hash-delimited comments (for example, #) in addition to comma-separated comments.	

Hosts file allow list	Tenable checks system hosts files for signs of a compromise (for example, Plugin ID 23910 titled Compromised Windows System (hosts File Check)). This option allows you to upload a file containing a list of IPs and hostnames you want Tenable to ignore during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.	
Yara Rules	A .yar file containing the YARA rules to be applied in the scan. You can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io.	Tenable supports all the YARA 3.4 built-in keywords including those defined in the PE and ELF sub-modules, excluding hash functionality. Tenable products do not support Yara imphash checks.
Scan file system	If enabled, Tenable can scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.	Enabling this setting decreases scan speed.
Directories	Enables file system scanning for certain Windows directories and user profiles.	Increasing the number of directories scanned will decrease assessment speed.

Custom Directories (available with Scan file system enabled)	A custom file that lists directories to scan with malware file scanning. List each directory on one line. You cannot list root directories (for example, C://) and you cannot use variables (for example, %Systemroot%).	
Databases (Nessus Scanner templates only)		
Use detected SIDs	When enabled, if at least one host credential and one Oracle database credential are configured, the scanner authenticates to scan targets using the host credentials, and then attempts to detect Oracle System IDs (SIDs) locally. The scanner then attempts to authenticate using the specified Oracle database credentials and the detected SIDs. If the scanner cannot authenticate to scan targets using host credentials or does not detect any SIDs locally, the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials.	

For more information, see the Scan Policy Assessment options.

Report

The Report settings affect the verbosity and formatting of scan reports you can create for the scan configuration. Report settings do not affect scan performance. However, Tenable recommends reviewing and configuring them per your organization's needs. For more information, see Scan Policy Report options.

Advanced

The Advanced section allows you to configure more general settings, performance options, and debugging capabilities.

Setting	Description	Tuning Tips
General Settings (Nessus Scanner templates only)		

Enable safe checks	When enabled, disables all plugins that may have an adverse effect on the remote host.	Tenable does not recommend disabling this setting in production environments; the plugins could crash services or targets. However, disabling the setting may provide more insight for systems likely to be under attack (for example, internet-facing systems).
Stop scanning hosts that become unresponsive during the scan	When enabled, Tenable stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delay the scan.	
Scan IP addresses in a random order	By default, Tenable scans a list of IP addresses in sequential order. When you enable this option, Tenable scans the list of hosts in a random order within an IP address range. This approach is typically useful in helping to distribute the network traffic during large scans.	
Automatically accept detected SSH disclaimer prompts	When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer	

	prompt and continue the scan.	
Scan targets with multiple domain names in parallel	When disabled, to avoid overwhelming a host, Tenable prevents a single scanner from simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.	
Create unique identifier on hosts scanned using credentials	When enabled, the scanner creates a unique identifier for credentialed scans.	
Performance Options (Nessus Scanner templates only)		
Slow down the scan when network congestion is detected	When enabled, Tenable detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable	

	automatically attempts to use the available space within the network pipe again.	
Use Linux kernel congestion detection	When enabled, Tenable uses the Linux kernel to detect when it sends too many packets and the network pipe approaches capacity. If detected, Tenable throttles the scan to accommodate and alleviate the congestion. Once the congestion subsides, Tenable automatically attempts to use the available space within the network pipe again.	
Network timeout (in seconds)	Specifies the time that Tenable waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.	Be cautious when increasing this setting as it impacts every check that relies on a timeout. It can increase scan times by an order of magnitude.
Max simultaneous checks per host	Specifies the maximum number of checks a Tenable scanner will perform against a single host at one time.	Tenable recommends that you monitor scan target performance when adjusting this setting.
Max simultaneous hosts per scan	Specifies the maximum number of hosts that each Nessus scanner scans per scan chunk. The number of scan chunks is determined by the available resources on each Nessus scanner. **Note:** This setting does not apply to Tenable Vulnerability Management cloud scanners.	Increasing this setting's value can decrease scan times, but doing so increases the load on your Nessus scanners. After a certain point, dependent on the available resources on the Nessus scanner and the number of systems being scanned, increasing this

		setting can make scans slower as it tries to make the scanners do more than they are capable of.
Max number of concurrent TCP sessions per host	Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most.	
Max number of concurrent TCP sessions per scan	Specifies the maximum number of established TCP sessions the entire scan, regardless of the number of hosts being scanned. **Note:** The `MAX NUMBER OF CONCURRENT TCP SESSIONS PER SCAN` setting is not enforceable in a Discovery scan. The `global.max_simult_tcp_sessions` Nessus Engine setting (that you set on each scanner) is an absolute cap that applies across all running scans on a scanner. (For example, if you have four scanners and do not want them to generate more than 10000 simultaneous TCP sessions in total at any point in time, you can set that global setting to 2500 for each individual scanner.) For scanners installed on any Windows	

	host, you must set this value to 19 or less to get accurate results.	
Unix find command Options		
Exclude filepath	A plain text file containing a list of filepaths to exclude from all plugins that search using the find command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix find command -path argument. For more information, see the find command man page.	
Exclude filesystem	A plain text file containing a list of filesystems to exclude from all plugins that search using the find command on Unix systems. In the file, enter one filesystem per line, using filesystem types supported by the Unix find command -fstype argument. For more information, see the find command man page.	
Include filepath	A plain text file containing a list of filepaths to include from all plugins that search using the `find` command on Unix systems. In the file, enter one filepath per line, formatted per patterns allowed by the Unix `find` command `-path` argument. For more information, see the `find` command man page.	

	Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible. **Tip:** Avoid having the same filepaths in **Include Filepath** and **Exclude Filepath**. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.	
Stagger scan start (Nessus Agent templates only)		
Maximum delay (minutes)	(Agents 8.2 and later) If set, each agent in the agent group delays starting the scan for a random number of minutes, up to the specified maximum. Staggered starts can reduce the impact of agents that use a shared resource, such as virtual machine CPU. If the maximum delay you set exceeds your scan window, Tenable shortens your maximum delay to ensure that agents begin scanning at least 30 minutes before the scan window closes.	This setting is useful for preventing resource overuse in shared infrastructure (for example, virtual hosts).

For more information, see Scan Policy Advanced options.

For more information about Tenable Security Center scan policy settings, see Scan Policy Options.

Credentials Configuration

Note: You do not need to configure credentials for Tenable Agent scans. Tenable Agents already have the access needed for local security checks because they are installed directly on the asset.

The scan's Credentials configuration determines what credentials the Nessus scanners have for scanning your organization's assets. Giving your Nessus scanners credentials (referred to as *credentialed scanning*) allows you to scan a large network while also scanning for local exposures that require further credentials to access.

In general, giving your scanners more credentials allows them to authenticate more assets, but this ultimately depends on the scan targets and your environment. However, the scan may take longer to complete.

Fully credentialed scans may take longer to complete. However, this depends on other scan configurations and the targets being assessed. In general, fully credentialed scans are preferred, as they create less network overhead and up to ten times more information is returned to help with risk identification and prioritization.

Credentials need to have proper privileges to work (for more information, see Nessus Credentialed Checks in the *Nessus User Guide*). You may also want to provide additional security controls for credential management (for more information, see the How to Protect Scanning Credentials: Overview blog article).

For more information about scan credential settings, see Credentials and Scan Policy Authentication options.

Compliance Configuration

The Compliance section allows you to add audit files (also known as *compliance checks* or *benchmarks*) to your scan configuration. Compliance checks allow the scan to discover how the host is configured and whether it is compliant with various industry standards. You can use Tenable's preconfigured compliance checks, or you can create and upload custom audits.

Similar to credentialed scans, adding compliance checks allows the scan to yield more data, but doing so might also increase the overall scan time.

In general, most authority-based compliance checks (for example, baselines from CIS or DISA) do not impact overall scan times significantly. However, audits that enable File Content checking usually have a significant impact on scan time because they search the target file systems for the noted patterns.

For more information about scan compliance settings, see Configure Compliance Options and Compliance Checks Reference.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

Plugin Configuration

The Plugins section allows you to enable or disable plugin families for the scan configuration. Enabling and disabling plugin families determines what security checks the scan does and does not perform. Your plugin configuration can noticeably affect how much data your scan returns and how long it takes the scan to run. In general, a scan with more plugin families enabled takes longer to complete but yields more scan data, and a scan with fewer plugin families enabled is faster but yields less scan data.

Scanners automatically run the proper plugins and families against each target, and the proper plugins are determined as each system is scanned. In general, Tenable does not recommend disabling plugin families broadly or creating targeted scan policies with different plugin sets for different devices as it is not necessary and can lead to misrepresentations of risk.

For more information about scan plugin settings, see Configure Plugin Options.

Other Tips

Configure your scans for effective assessment based on your network configuration

When exploring the most effective way to perform an assessment, scanning many systems simultaneously isn’t always the best option. You need to consider various network factors to determine your most effective assessment method. For more information, see the Tuning Network Assessments for Performance and Resource Usage blog article.