Nessus Scan Tuning Guide

Last Revised: May 01, 2024

Table of Contents

Introduction

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

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

Table of Contents

Considerations

Although your scan configuration plays an important role in your Nessus 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 Nessus performing? • What ports are Tenable Nessus 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 the resources available to your internal Nessus scanners. Your Nessus scanners should meet the hardware requirements whenever possible, but *exceeding* the minimum requirements lets your scanners assess more targets faster.
Type of	Medium	You have various options available for assessing assets in

assessment		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.
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 General.
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.
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.

Scan Template Selection

Tenable Nessus provides various Scanner templates that meet different business needs. Tenable Nessus provides three template categories: Discovery, Vulnerabilities, and Compliance. You can view the complete offering of Nessus scan templates when you Create a Scan in the user interface.

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

Discovery (Nessus scanner only)

Tenable recommends using discovery scans 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 vulnerability scan.

Vulnerabilities

Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs. Tenable also publishes vulnerability scan templates that allow you to scan your network for a specific vulnerability or group of vulnerabilities. Tenable frequently updates the Nessus scan template library with templates that detect the latest vulnerabilities of public interest.

Some of the most notable vulnerability scan templates are:

- Basic Network Scan — Use this template to scan an asset or assets with all of Nessus's plugins enabled. This scan provides a quick and easy way to scan assets for all vulnerabilities.
- Advanced Network Scan — The most configurable scan type that Nessus offers. You can configure this scan template to match any policy or search any asset or assets. This template has the same default settings as the Basic Network Scan, but they allow for additional configuration options.

  > **Note:** Advanced scan templates allow Nessus 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.

- Advanced Dynamic Scan (Nessus Scanner only) — An advanced network scan that you can configure dynamic plugin filters for instead of manually selecting plugin families or individual plugins. As Tenable releases new plugins, Nessus adds any plugins that match your filters to the scan or policy automatically. This allows you to tailor your scans for specific vulnerabilities while ensuring that the scan stays up to date as new plugins are released.

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

Compliance

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

Settings Configuration

Once you select the scan template to use for your scan, there are several settings that you can use to tune the scan configuration's performance. The following topics describe each of the scan configuration sections—Settings, Credentials, 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.

A scan configuration's settings greatly affect the scan's capabilities, performance, and scan time. Use the settings to configure when and how often Tenable Nessus launches the scan, discovery options, debugging capabilities, assessment methods, performance options, and other scan behavior. Tenable Nessus has into five Settings categories: *Basic*, *Discovery*, *Assessment*, *Report*, and *Advanced*.

Some of the scan configuration settings are informational or do not affect scan performance (for example, Name, Description, and Notification settings). This section describes all the settings that *do* affect scan performance and how to tune them for better scan performance.

Click the following setting categories to learn more about them and how to tune them:

Basic

Use the Basic settings to choose which scanner or agents perform the scan, what targets or assets the sensors scan, and the schedule on which Tenable Nessus launches the scan. All three of these aspects greatly impact the scope and performance of the scan.

Setting	Description	Tuning Tips
General		
Scanner	Specifies the scanner that performs the scan.	
Targets and Upload Targets	(Scanner templates only) The Targets and Upload Targets options are different methods you can use to specify which hosts the scan runs against.	Targeting specific assets provides faster scan results than scans that target IP ranges

		or CIDR notation.
Schedule		
Frequency	Specifies how often Nessus launches the scan. • **Once** — Schedule the scan at a specific time. • **Daily** —Schedule the scan to occur every 1-20 days, at a specific time. • **Weekly** — Schedule the scan to occur every 1-20 weeks, by time and day or days of the week. • **Monthly** — Schedule the scan to occur every 1-20 months, by: ◦ **Day of Month** — The scan repeats monthly on a specific day of the month at the selected time. For example, if you select a start date of October 3, the scan repeats on the 3rd of each subsequent month at the selected time. ◦ **Week of Month** — The scan repeats monthly on a specific day of the week. For example, if you select a start date of the first Monday of the month, the scan runs on the first Monday of each subsequent month at the selected time. **Note:** If you schedule your scan to recur monthly and by time and day of the month, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (for example, the 29th), Nessus cannot run the scan on those days. • **Yearly** — Schedule the scan to occur every 1-20 years, by time and date.	Tenable recommends running full vulnerability scans against most types of assets at least twice a week.

Starts	Specifies the exact date and time when a scan launches. The starting date defaults to the date when you are creating the scan. The starting time is the nearest half-hour interval. For example, if you create your scan on 09/31/2018 at 9:12 AM, Tenable Nessus sets the default starting date and time to *09/31/2018* and *09:30*.	
Time Zone	Specifies the timezone of the value set for **Starts**.	

For more information, see Basic Settings for Scans.

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 (Scanner templates only)		
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 Nessus attempts to avoid false positives, performing additional tests to verify the response	This setting can increase scan speeds, but it may not be appropriate in all environments

	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 Nessus does not perform these checks.	due to target configurations.
Ping Methods	(Available if Ping the remote host is enabled) Specifies the scanner's pinging method.	In most environments, Tenable recommends using the default ping methods. Enabling UDP can greatly increase scan times. 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 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	(Scanner templates only) 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	(Scanner templates only) Specifies the range of ports to be scanned. Supported keyword values are: • `default` instructs the scanner to scan approximately 4,790 commonly used ports. The list of ports can be found in the nessus-services file on the Nessus scanner. • `all` instructs the scanner to scan all 65,536 ports, includingexcluding port 0. Additionally, you can indicate a custom list of ports by using a comma-separated list of ports or port ranges. For example, `21,23,25,80,110` or `1-1024,8080,9000-9200`. If you wanted to scan all ports excluding port 0, you would type `1-65535`. The custom range specified for a port scan is applied to the protocols you have selected in the **Network Port Scanners** group of settings.	If you have insight into local cross-traffic in your network, you can customize this setting to only include the active listening services on your network, but this may cause the scan to unused services.

	If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type `T:1-1024,U:300-500`. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate protocol. For example, `1-1024,T:1024-65535,U:1025`.	
SSH (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 an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials. If any port enumerator (netstat or SNMP) is successful, the port range becomes *all*.	
WMI (netstat)	When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan. In addition, the scanner: • Ignores any custom range specified in the **Port Scan Range** setting. • 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*.	
SNMP	(Scanner templates only)	

	When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits. If any port enumerator (netstat or SNMP) is successful, the port range becomes *all*.	
Only run network port scanners if local port enumeration failed	(Scanner templates only) If a local port enumerator runs, all network port scanners will be disabled for that asset.	
Verify open TCP ports found by local port enumerators	(Scanner templates only) 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).	
TCP	(Scanner templates only) 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.	
SYN	(Scanner templates only) 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 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.	
Override automatic firewall detection	(Scanner templates only) This setting can be enabled if you enable either the **TCP** or **SYN** option. When enabled, this setting overrides automatic firewall detection. This setting has three options: • **Use aggressive detection** 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. • **Use soft detection** disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device. • **Disable detection** disables the firewall detection feature.	
UDP	(Scanner templates only) This option engages the built-in Tenable Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, a port scanner usually cannot tell the difference between open	Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the

	and filtered UDP ports.	netstat or SNMP port enumeration options instead if possible.
Service Discovery (Scanner templates only)		
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 times.

For more information, see Discovery Scan Settings. To learn more about the preconfigured Discovery scan template settings, see Preconfigured Discovery Scan 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 Nessus 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 Nessus 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 increases scan times.
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 Nessus to allow for a specific grace time in reporting when antivirus signatures are out of date. By default, Tenable Nessus 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	(Scanner templates only) Allows you to enable SMTP testing on the scan configuration.	
Brute Force (Scanner templates only)		
Only use credentials provided by the	In some cases, Tenable Nessus can test default accounts and known default passwords. This can cause the account to lock if too many consecutive	

user	invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Tenable Nessus from performing these tests.	
Test default accounts (slow)	Test for known default accounts in Oracle software.	
SCADA (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	The Modbus/TCP Coil Access settings are available for commercial users. This drop-down menu item is generated by the SCADA plugins available with the commercial version of Tenable Nessus. 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 (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.
Windows		
Request information about the SMB Domain	If enabled, domain users are queried instead of local users.	
User Enumeration Methods	You can enable as many of the user enumeration methods as appropriate for user discovery.	
Malware		
Scan for malware	Configures the scan to scan for malware on the target hosts. Enable this setting to view the remaining Malware options.	
Disable DNS resolution	Checking this option prevents Tenable Nessus from using the cloud to compare scan findings against	

	known malware.	
Custom Netstat IP Threat List	A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments. **Note:** Tenable does not detect private IP ranges in the text file.	
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.	
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 Nessus 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 Nessus 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 Nessus 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 increases scan times.
Windows Directories	(Available with Scan file system enabled) Enables file system scanning for certain Windows directories and user profiles.	
Linux Directories	(Available with Scan file system enabled) Enables file system scanning for certain Linux	

	directories.	
MacOS Directories	(Available with Scan file system enabled) Enables file system scanning for certain macOS directories.	
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 (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 Assessment Scan Settings. To learn more about the preconfigured Assessment scan template settings, see Preconfigured Assessment Scan Settings.

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 Report Scan Settings.

Advanced

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

Setting	Description	Tuning Tips
General Settings (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, Nessus 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, Nessus scans a list of IP addresses in sequential order. When you enable this option, Nessus 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 enabled, Nessus 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.	
Trusted CAs	Specifies CA certificates that the scan considers as trusted. This allows you to use self-signed certificates for SSL authentication without triggering plugin 51192 as a vulnerability in Tenable Nessus.	
Performance Options (Scanner templates only)		
Slow down the scan when network	When enabled, Tenable detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is	

congestion is detected	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.	
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.	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 by making 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 for each scan task, regardless of the number of hosts being scanned.Specifies the maximum number of established TCP sessions the entire scan, regardless of the number of hosts being scanned.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.	
Debug Settings		
Note: Tenable does not recommend enabling debug settings in production environments. Debug settings generate a substantial amount of data, and can alter the overall scan time and performance. Tenable only recommends the settings for specific debugging instances, and not for constant use.		
Always report	When enabled, Tenable Nessus generates a report	

SSH commands	of all the commands run over SSH on the host in a machine-readable format. You can view the reported commands under plugin 168017. **Note:** The setting does not function correctly if you disable plugin 168017.	
Enable plugin debugging	Attaches available debug logs from plugins to the vulnerability output of this scan.	
Debug Log Level	Controls the verbosity and content of debug log statements.	Unless Tenable Support instructs your organization otherwise, set Debug Log Level to **Level 3:**.
Enumerate launched plugins	Shows a list of plugins that Tenable Nessus launched during the scan. You can view the list in scan results under plugin 112154. **Note:** The setting does not function correctly if you disable plugin 112154.	
Audit Trail Verbosity	Controls verbosity of the plugin audit trail. Options include: • **No audit trail** — (Default) Nessus does not generate a plugin audit trail. • **All audit trail data** — The audit trail includes the reason why plugins were not included in the scan. • **Only scan errors** — The audit trail includes only errors encountered during the scan.	
Packet Capture Settings (Scanner templates only)		

Packet Capture	When enabled, Tenable Nessus logs the TCP and UDP communications between a scanner and a target host. For more information, see Advanced Debugging - Packet Capture. **Note:** This setting is only available in Tenable Nessus Expert and Tenable Nessus Professional.	
Stagger scan start (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).
Compliance Output Settings		
Maximum compliance output length in KB	Controls the maximum output length for each individual compliance check value that the target returns. If a compliance check value that is greater than this setting's value, Tenable Nessus truncates the result. **Note:** If you notice that your compliance scan processing is slow, Tenable recommends reducing this setting to increase the processing speed.	

For more information, see Advanced Scan Settings. To learn more about the preconfigured Advanced scan template settings, see Preconfigured Advanced Scan Settings.

For more information about Nessus scan settings, see Scan and Policy Settings.

Credentials Configuration

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. You can assign credentials to your scanners at two different levels: individual scans or scan templates.

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). 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 Nessus scan credential settings, see Credentials.

Compliance Configuration

The Compliance section allows you to add compliance checks (also known as *audits*) 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 Compliance.

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 Plugins. For information about configuring dynamic plugins for the Advanced Dynamic Scan template, see Configure Dynamic Plugins.

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.