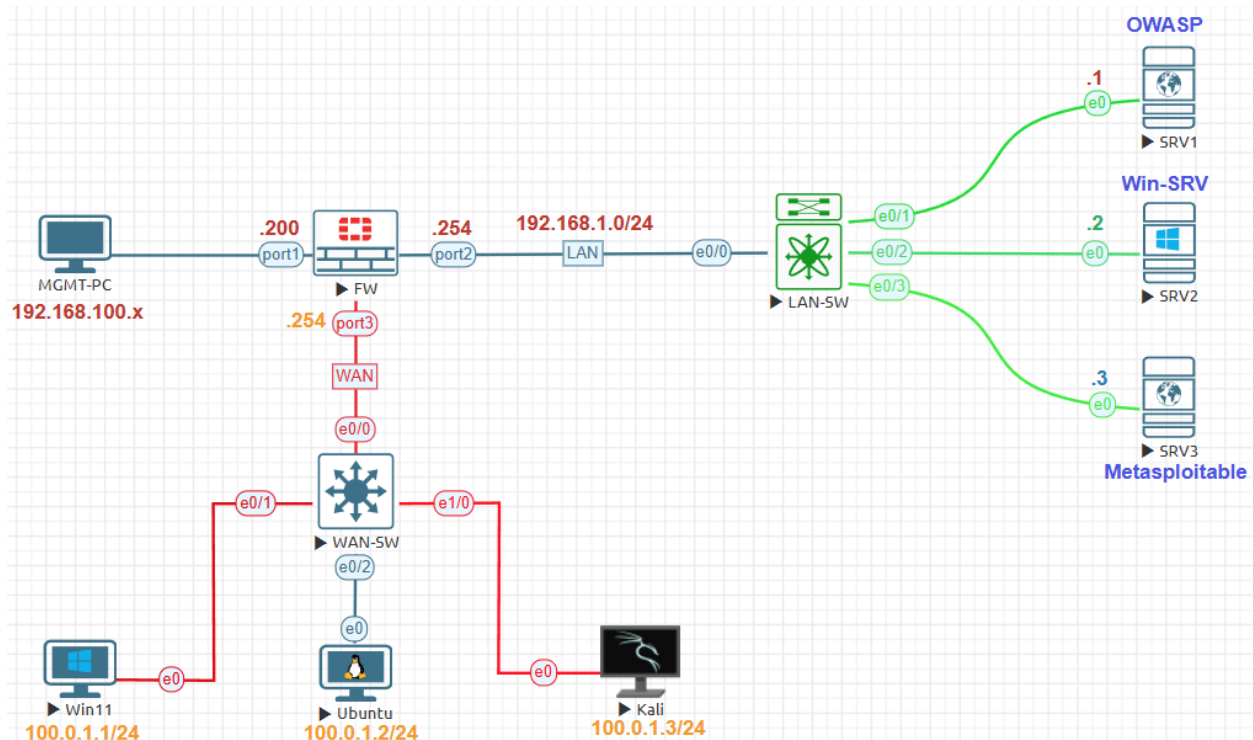


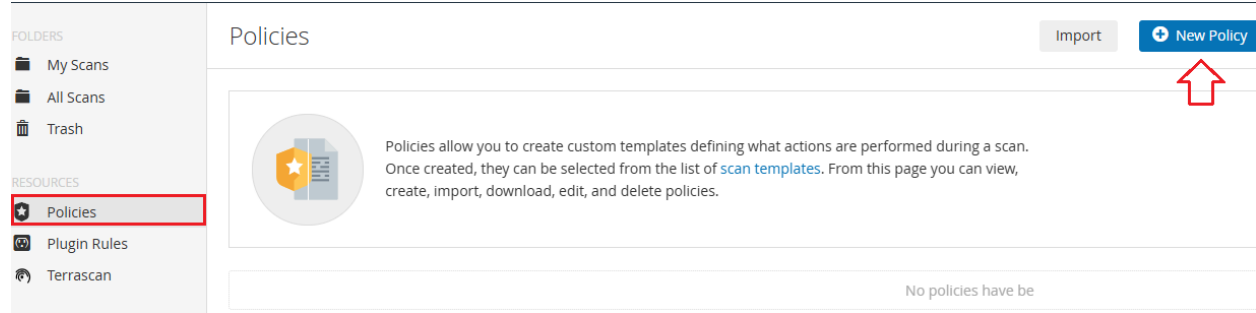
Create Custom Policy Lab:



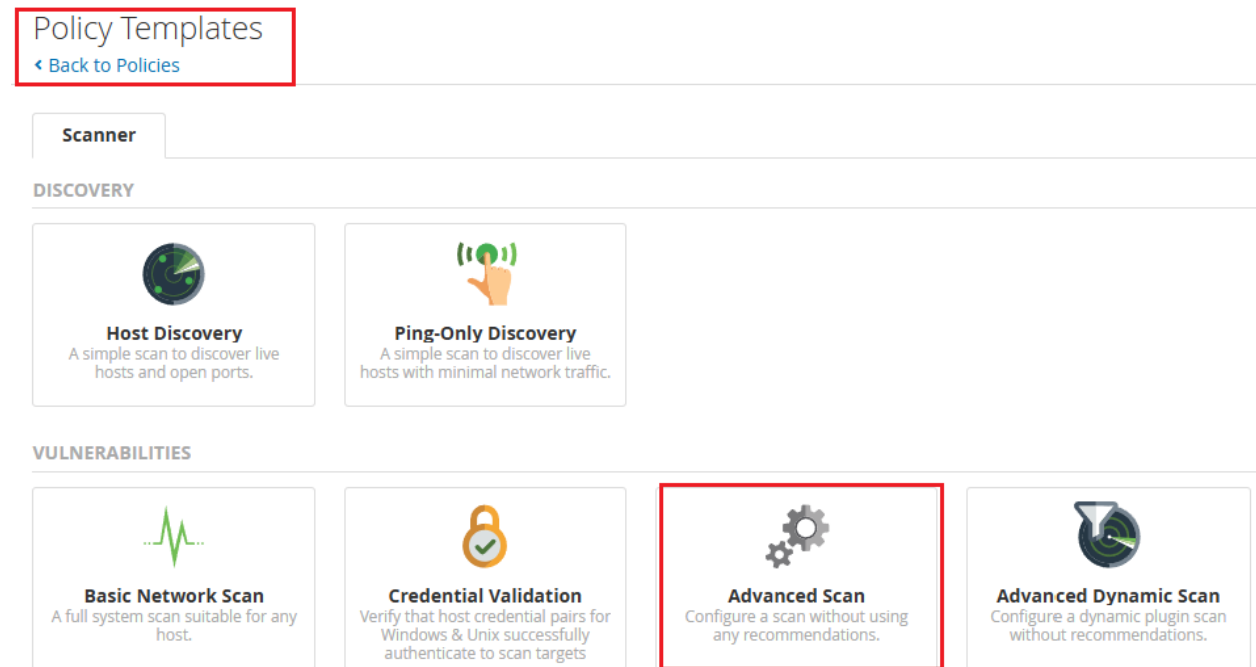
Management Subnet	192.168.100.0/24
FortiGate Management IP	192.168.100.200
Internal Servers Subnet	192.168.1.0/24
FortiGate Firewall External	100.0.1.0/24
FortiGate Firewall Internal IP	192.168.1.254
FortiGate Firewall External IP	100.0.1.254
SRV1 IP Address	192.168.1.1
SRV2 IP Address	192.168.1.2
SRV3 IP Address	192.168.1.3
External Win11 IP Address	100.0.1.1
External Ubuntu IP Address	100.0.1.2
External Kali IP Address	100.0.1.3

Devices	Username	Password
FortiGate 7.0.9	Admin	123
Linux Kali 2025.1c	kali	kali
Linux Ubuntu 22.04 Desktop	user	Test123
Windows 11 x64 SE	user(Administrator)	Test123
Linux Metasploitable 2.0	msfadmin	msfadmin
Linux-OWASP	root	owaspbwa
Windows Server 2012	Administrator	Test123

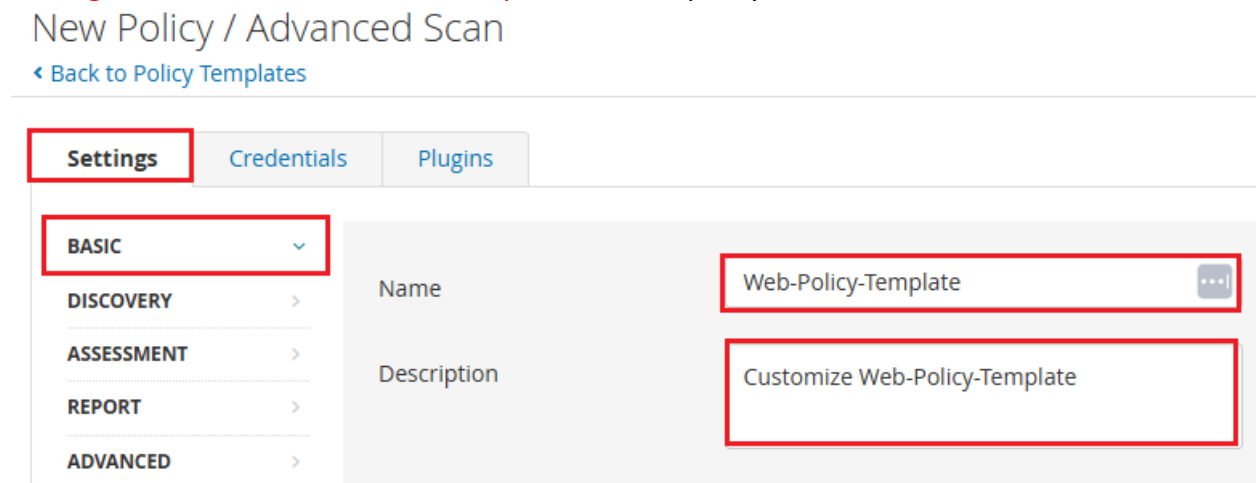
Go to **Scans** on left side click on **Policies**. On Right hand top corner click on **New Policy** to open.



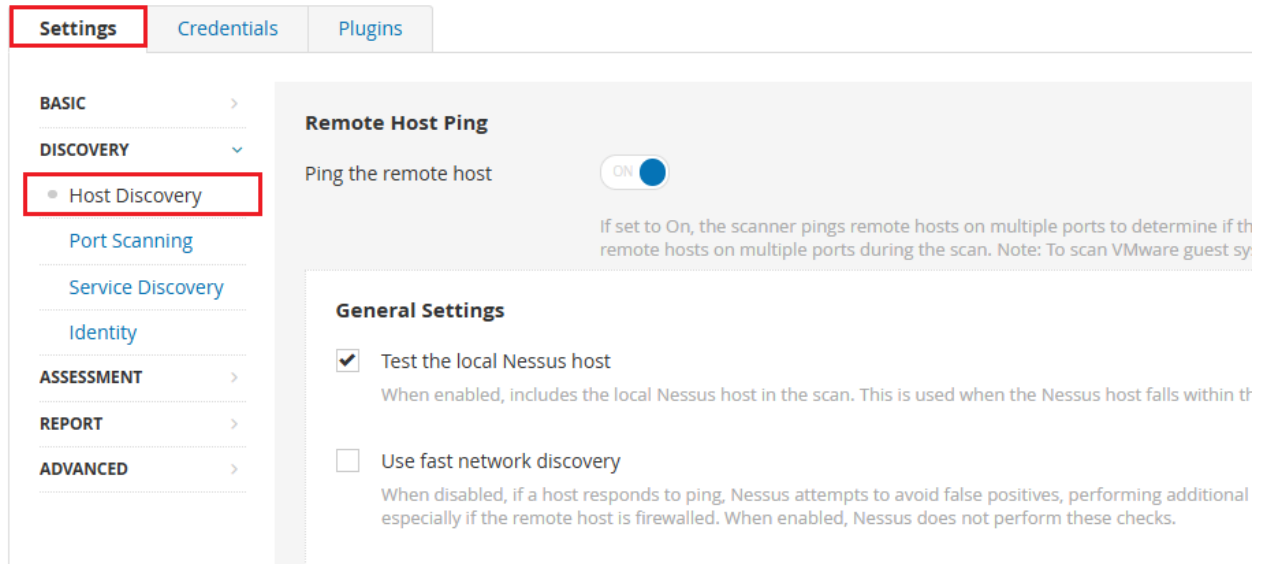
It will open Scanning template choose any to customize.



Settings>**Basic** enter **Name** and **Description** for new policy



Settings>Discovery>Host Discovery customize as per your requirements.



The screenshot shows the Nessus Settings interface. The 'Settings' tab is selected and highlighted with a red box. The left sidebar shows a navigation menu with 'DISCOVERY' expanded, and 'Host Discovery' selected and highlighted with a red box. The main content area is titled 'Remote Host Ping' and features a toggle switch set to 'ON'. Below this, there is a 'General Settings' section with two options: 'Test the local Nessus host' (checked) and 'Use fast network discovery' (unchecked).

Settings Credentials Plugins

BASIC >

DISCOVERY ▾

- **Host Discovery**
- Port Scanning
- Service Discovery
- Identity

ASSESSMENT >

REPORT >

ADVANCED >

Remote Host Ping

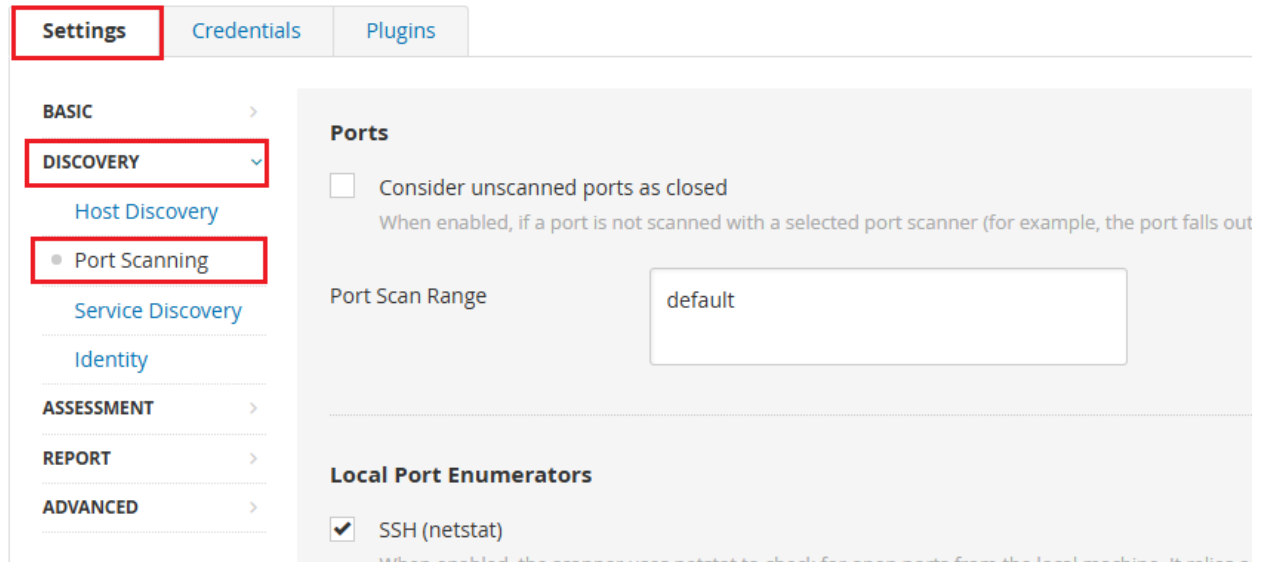
Ping the remote host ON

If set to On, the scanner pings remote hosts on multiple ports to determine if the remote hosts on multiple ports during the scan. Note: To scan VMware guest systems, this option must be disabled.

General Settings

- Test the local Nessus host
When enabled, includes the local Nessus host in the scan. This is used when the Nessus host falls within the scan range.
- Use fast network discovery
When disabled, if a host responds to ping, Nessus attempts to avoid false positives, performing additional checks especially if the remote host is firewalled. When enabled, Nessus does not perform these checks.

Settings>Discovery>Port Scanning customize as per your requirements.



The screenshot shows the Nessus Settings interface. The 'Settings' tab is selected and highlighted with a red box. The left sidebar shows a navigation menu with 'DISCOVERY' expanded, and 'Port Scanning' selected and highlighted with a red box. The main content area is titled 'Ports' and features a checkbox for 'Consider unscanned ports as closed' (unchecked). Below this, there is a 'Port Scan Range' input field with the value 'default'. The 'Local Port Enumerators' section has 'SSH (netstat)' checked.

Settings Credentials Plugins

BASIC >

DISCOVERY ▾

- Host Discovery
- **Port Scanning**
- Service Discovery
- Identity

ASSESSMENT >

REPORT >

ADVANCED >

Ports

- Consider unscanned ports as closed
When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside the scan range).

Port Scan Range

Local Port Enumerators

- SSH (netstat)
When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the local machine's network stack.

Settings>Discovery>Service Discovery customize as per your requirements.

The screenshot shows the 'Settings' page with the 'Discovery' section selected. The 'Service Discovery' sub-section is highlighted. The 'General Settings' area includes a checked checkbox for 'Probe all ports to find services', a toggle for 'Search for SSL/TLS/DTLS services' set to 'ON', and dropdown menus for 'Search for SSL/TLS on' (set to 'All TCP ports') and 'Search for DTLS on' (set to 'None'). A text input field for 'Identify certificates expiring within x days' is set to '60'.

Settings>Discovery>Identity customize as per your requirements.

The screenshot shows the 'Settings' page with the 'Discovery' section selected. The 'Identity' sub-section is highlighted. The 'General Settings' area includes a checkbox for 'Collect Identity Data from Active Directory' which is currently unchecked. A note below states: 'Checking this box will enable collection of identity information from Active Directory using Domain User credentials.'

Settings>Assessment customize as per your requirements.

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT ▾
• General
Brute Force
Web Applications
Windows
Malware
Databases
REPORT >
ADVANCED >

Accuracy

- Override normal accuracy
- Avoid potential false alarms
- Show potential false alarms
- 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 can be more thorough, the scan is more intrusive and is more likely to disrupt the network, while poten

Antivirus

Antivirus definition grace period (in days): 0 ▾

Settings>Assessment>Web Applications customize as per your requirements.

Settings | Credentials | Plugins

BASIC >
DISCOVERY >
ASSESSMENT ▾
General
Brute Force
Web Applications
Windows
Malware
Databases
REPORT >
ADVANCED >

Web Application Settings

Scan web applications

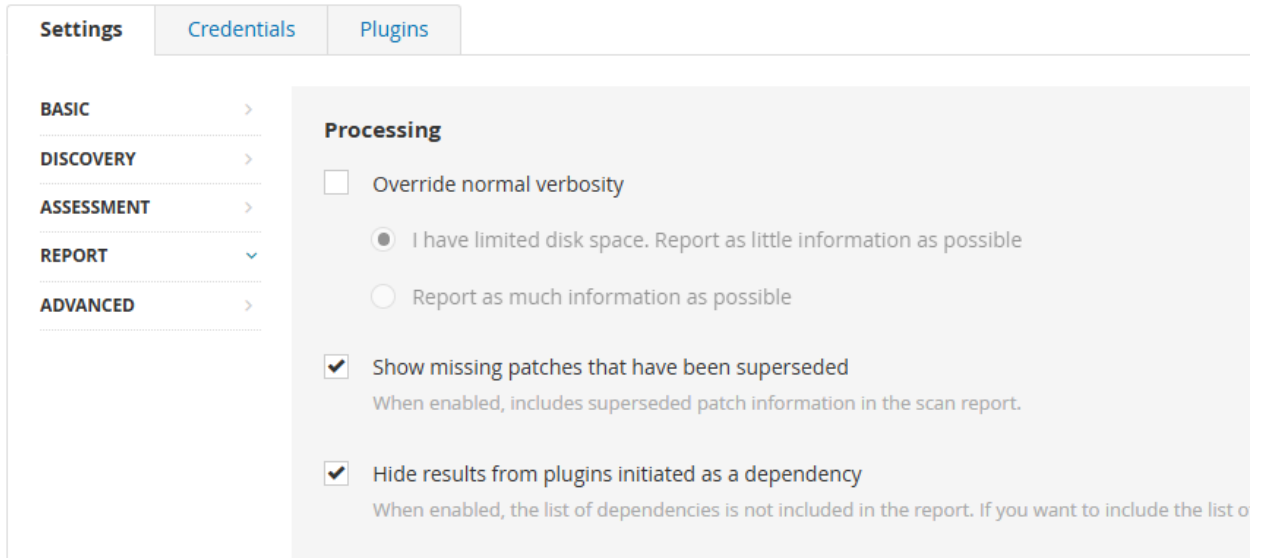
Web Crawler

Start crawling from: /
The URL of the first page that is tested. If multiple pages are

Excluded pages (regex): /server_privileges\.php|logout
Specifies portions of the web site to exclude from being crav

Maximum pages to crawl: 1000
The maximum number of pages to crawl.

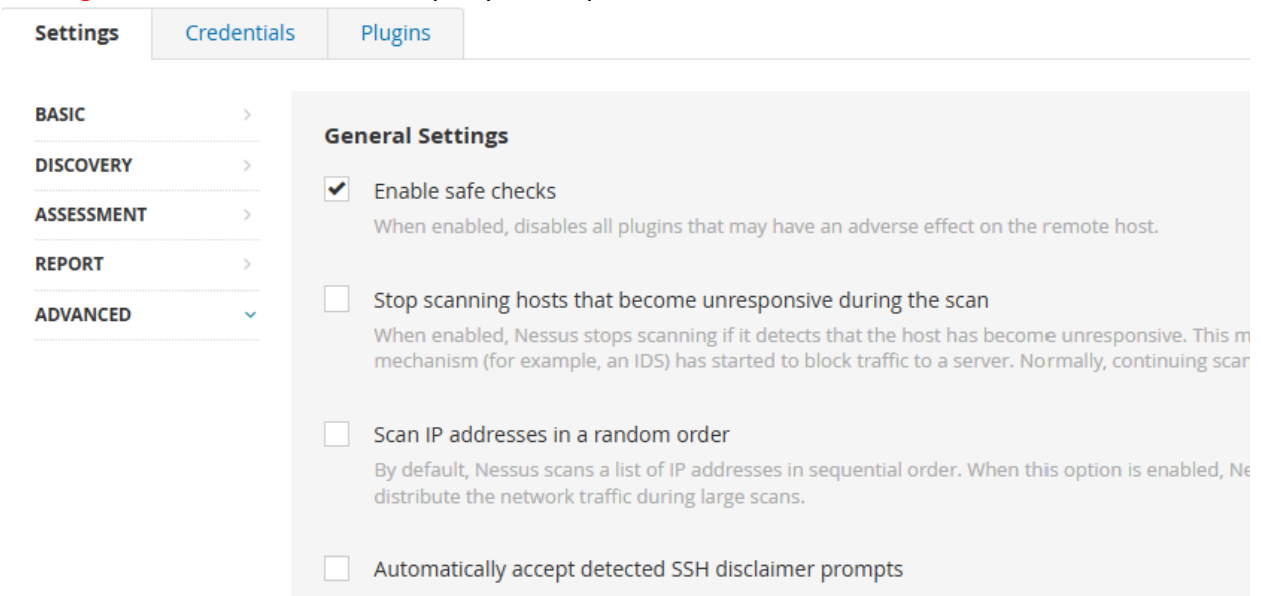
Settings>Reports customize as per your requirements.



The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'REPORT' section is expanded, showing a sidebar with categories: BASIC, DISCOVERY, ASSESSMENT, REPORT (selected), and ADVANCED. The main content area is titled 'Processing' and contains the following options:

- Override normal verbosity
- I have limited disk space. Report as little information as possible
- Report as much information as possible
- Show missing patches that have been superseded
When enabled, includes superseded patch information in the scan report.
- Hide results from plugins initiated as a dependency
When enabled, the list of dependencies is not included in the report. If you want to include the list o

Settings>Advanced customize as per your requirements.



The screenshot shows the 'Settings' interface with tabs for 'Settings', 'Credentials', and 'Plugins'. The 'ADVANCED' section is expanded, showing a sidebar with categories: BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED (selected). The main content area is titled 'General Settings' and contains the following options:

- Enable safe checks
When enabled, disables all plugins that may have an adverse effect on the remote host.
- Stop scanning hosts that become unresponsive during the scan
When enabled, Nessus stops scanning if it detects that the host has become unresponsive. This mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scan
- Scan IP addresses in a random order
By default, Nessus scans a list of IP addresses in sequential order. When this option is enabled, Ne distribute the network traffic during large scans.
- Automatically accept detected SSH disclaimer prompts

Credentials Tab customize as per your requirements.

The screenshot shows the 'Credentials' tab with the following elements:

- Navigation tabs: Settings, Credentials (selected), Plugins
- CATEGORIES: Host (dropdown menu)
- Filter Credentials: Search bar with a magnifying glass icon
- Category list:
 - SNMPv3 (with infinity icon)
 - SSH (with infinity icon)
 - Windows (with infinity icon)

Plugins Tab customize as per your requirements.

STATUS	PLUGIN FAMILY	LOCKED	TOTAL	STATUS
ENABLED	Alibaba Cloud Linux Local Security Checks		804	
ENABLED	Alma Linux Local Security Checks		42	
ENABLED	Amazon Linux Local Security Checks		59	
ENABLED	Artificial Intelligence		3	
ENABLED	Azure Linux Local Security Checks		13	
ENABLED	Backdoors		1	
ENABLED	CentOS Local Security Checks		1	
ENABLED	CGI abuses		753	
ENABLED	CGI abuses : XSS		121	
ENABLED	CISCO		885	
ENABLED	Databases		12	
ENABLED	Debian Local Security Checks		27	

Finally, click **Save**

Web-Policy-Template / Configuration

[← Back to Policies](#)

Settings | Credentials | Plugins

BASIC ▾

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >


Name: Web-Policy-Template

Description: Customize Web-Policy-Template

Save Cancel

In **Policies** now its visible.

Policies

 Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of [scan templates](#). From this page you can view, create, import, download, edit, and delete policies.

Search Policies 2 Policies

<input type="checkbox"/> Name ▾	Template
<input type="checkbox"/> test-Policy	Host Discovery
<input type="checkbox"/> Web-Policy-Template	Advanced Scan

When you click on **New Scan** in **User Defined** Tab you will see the new custom policy to use.

tenable Nessus Essentials | **Scans** | Settings

Scan Templates

[← Back to Scans](#)

Scanner | **User Defined**

Web-Policy-Template
Customize Web-Policy-Template

test-Policy
dsd