Tenable Nessus Command Line Reference Guide

Last Updated: November 18, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to the Tenable Nessus and Tenable Agent Command Line Reference Guide 5

Tenable Nessus Manager, Professional, and Expert 6

Help Commands 7

Backup Commands 10

Create Tenable Nessus Backup 10

Restore Tenable Nessus Backup 11

Fix Commands 12

Reset Registration and Erase Settings 12

Perform a Full Reset 14

View the Current Network Interfaces 16

Manage Advanced Settings 18

Configure Proxy Settings 23

Certificate Commands 24

Create a Nessus Server Digital Certificate 25

Create a Nessus Client-Side Digital Certificate 27

User Management Commands 29

List Users 30

Change a User's Password 31

Add a User 32

Remove a User 35
Update Commands 36
Update Tenable Nessus 36
Force the Plugin and Core Components Update 38
Update the Plugins Only 39
Update a Specific Plugin Archive 41
Network and Port Rules 42
Plugin Rules 43
Fetch Commands 43
Register a Scanner Online 44
Register a Scanner with Tenable Security Center 45
Register a Scanner Offline 46
Confirm Nessus Registration Codes 49
Bug Reporting Commands 51
Tenable Agent 55
Help Agent Commands 56
Fix Agent Settings 58
Local Agents Commands 61
Triggered Agent Scan Commands 64
List Triggered Scan Details 64
Launch a Triggered Scan 66

Link Windows Agents During Installation 67
Local Agent Plugin Commands 69
Retrieve Agent Plugin Info 69
Reset Agent Plugins 71
Update Tenable Agent Plugins 72
Install Tenable Identity Exposure Secure Relay 73
Bug Report Generator Agent Commands 74

Welcome to the Tenable Nessus and Tenable Agent Command Line Reference Guide

This guide describes command line interface commands for Tenable Nessus and Tenable Agent, prerequisites, deployment options, and an installation walk-through. The guide assumes that you have a basic understanding of Unix and vulnerability scanning.

- Tenable Nessus command line reference
- Tenable Agent command line reference

Tenable Nessus Manager, Professional, and Expert

As a user with administrator privileges, you can do certain actions in Tenable Nessus Manager, Tenable Nessus Professional, and Tenable Nessus Expert via the command line. You can manage user accounts, modify advanced settings, manage digital certificates, report bugs, update software and plugins, and view license information.

This command is called **nessuscli** and is available on all supported Tenable Nessus versions.

The majority of the examples show usage for Tenable Nessus Manager and Tenable Nessus Professional. The examples for Tenable Nessus Agents are specified in the Nessus Agents section.

Nessus Command Line Tool

The following table provides instructions for running the Tenable Nessus command line tool **nessuscli** on all supported platforms. The basic usage for all operating systems is listed in the following table:

Operating System	Command
Windows	`"C:\Program Files\Tenable\Nessus\nessuscli.exe" <cmd> <arg1> <arg2>`
macOS	`# /Library/Nessus/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`
FreeBSD	`# /usr/local/nessus/sbin/nessuscli <cmd> <arg1> <arg2>`

Note: If you installed Tenable Nessus in a different location, update your path accordingly.

Command Syntax

- **`# nessuscli`** – This documentation sometimes uses the shorthand `# nessuscli` (instead of the full path to the `nessuscli` tool for the operating system) to represent general usage across different operating systems. However, for your commands to work, you must include the full path for your operating system, as shown above.

  For each command, the documentation contains a quick reference section with the full command for each operating system. You can copy and paste these commands directly into the command line terminal.
- **`<cmd>`** – The command. Do not include the brackets (< >).
- **`<arg 1> <arg 2>`** – The arguments for the command, if applicable. Do not include the brackets (< >).

Help Commands

> **Required User Role:** User with administrator privileges

You can get help to see available commands on the `nessuscli` tool, as well as get help for a specific command.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To get help for the `nessuscli` tool, use the following command:

```
# nessuscli help
```

The help output may vary, depending on your Tenable Nessus license.

The following is example output for Tenable Nessus Manager help:

```
Usage: nessuscli command [options]
Usage: nessuscli command help

Bug Reporting Commands:
- bug-report-generator
- bug-report-generator --quiet [--full] [--scrub]

User Commands:
- rmuser [username]
- chpasswd [username]
- adduser [username]
- lsuser

Manager Commands:
- manager download-core
- manager generate-plugins

Fetch Commands:
- fetch --register <serial>
- fetch --register-offline [<file.rc>]
- fetch --check
- fetch --code-in-use
- fetch --challenge
- fetch --security-center

Fix Commands:
- fix [--secure] --list
- fix [--secure] --set <name=value>
- fix [--secure] --get <name>
- fix [--secure] --delete <name>
- fix --list-interfaces
- fix --reset

Certificate Commands:
- mkcert-client
```

```
- mkcert [-q]

Software Update Commands:
- update
- update --all
- update --plugins-only
- update <plugin archive>
```

Help for a Specific Command

To get help for the usage of a specific command, use the following command:

```
# nessuscli <cmd> help
```

For example, to get help for the usage of the `bug-report-generator` command, type:

```
# nessuscli bug-report-generator help

Usage: nessuscli bug-report-generator
Usage: nessuscli bug-report-generator --quiet [--full] [--scrub]

Generate an archive of system diagnostics.
Running without arguments prompts for values.
--quiet: run the bug report generator without prompting the user for feedback
--scrub: when in quiet mode, bug report generator sanitizes the last two octets of the
IPv4 address
--full: when in quiet mode, bug report generator collects extra data
```

Command Quick Reference

For the full command for your operating system, see the following:

> Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" help
```

macOS

```
/Library/Nessus/run/sbin/nessuscli help
```

Linux

```
/opt/nessus/sbin/nessuscli help
```

Backup Commands

Create Tenable Nessus Backup

Required User Role: User with administrator privileges

To create a .zip backup of your Tenable Nessus instance, use the following command:

```
# nessuscli backup --create <backup_filename>
```

The backup includes your license and setting configurations. The backup does not include scan results.

Optional arguments (Tenable Nessus 10.9.0 and later):

- `--targz` – The backup generates as a tar.gz file.
- `--include-backups` – The backup file includes the `/backups/` directory, which contains all previously generated backups. By default, Tenable Nessus excludes this directory to minimize the backup file size.

For more information, see Back Up Tenable Nessus in the *Tenable Nessus User Guide*.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" backup --create <backup_filename>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli backup --create <backup_filename>
```

Linux

```
/opt/nessus/sbin/nessuscli backup --create <backup_filename>
```

Restore Tenable Nessus Backup

Required User Role: User with administrator privileges

To restore a previously saved backup of Tenable Nessus, use the following command:

```
# nessuscli backup --restore <path/to/backup_filename>
```

For more information, see Back Up Tenable Nessus in the *Tenable Nessus User Guide*.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe backup --restore <path/to/backup_filename>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli backup --restore <path/to/backup_filename>
```

Linux

```
/opt/nessus/sbin/nessuscli backup --restore <path/to/backup_filename>
```

Fix Commands

You can use the `nessuscli fix` command to change Tenable Nessus settings from the command line. This includes managing advanced settings, resetting registration information, and listing network interfaces on the system.

For more information, see the following:

- Reset Registration and Erase Settings
- Perform a Full Reset
- View the Current Network Interfaces
- Manage Advanced Settings
- Configure Proxy Settings

Reset Registration and Erase Settings

Required User Role: User with administrator privileges

You can reset registration information for Tenable Nessus, which erases all settings and unregisters Tenable Nessus.

Note: Performing `nessuscli fix --reset` does not reset the `managed` function.

Note: This command deletes `nessus-fetch.db`, which removes all linking keys (agent, scanner, and child node). You must re-link Tenable Nessus after running this command.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

Before you begin:

Stop the nessusd service, as described in Start or Stop Nessus in the *Tenable Nessus User Guide*.

For example (Linux):

```
# /sbin/service nessusd stop
```

To reset the registration information:

Type the following command:

```
# nessuscli fix --reset
```

You are prompted to confirm the action.

To confirm, enter **y**, as shown in the following example output:

```
# /opt/nessus/sbin/nessuscli fix --reset
```

```
Resetting the Nessus configuration erases all your settings and causes Nessus to become
unregistered.
Do you want to proceed? (y/n) [n]: y
Successfully reset the Nessus configuration.
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --reset
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --reset
```

Linux

```
/opt/nessus/sbin/nessuscli fix --reset
```

Perform a Full Reset

Required User Role: User with administrator privileges

Performing a full reset deletes all scans, scan data, policies, users and user settings, preferences and settings, registration information, and the master password.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

Before you begin:

Stop the nessusd service, as described in Start or Stop Nessus in the *Tenable Nessus User Guide*.

For example (Linux):

```
# /sbin/service nessusd stop
```

Full Reset

Caution: This action cannot be undone. Contact Tenable Support before performing a full reset to ensure your situation warrants a full reset.

Type the following command:

```
# nessuscli fix --reset-all
```

You are prompted to confirm the action.

To confirm, read the warning message, then enter **y**, as shown in the following example output:

```
# /sbin/service nessusd stop
# /opt/nessus/sbin/nessuscli fix --reset-all
WARNING: This option resets Nessus to a fresh state, permanently erasing the following:
* All scans, scan data, and policies
* All users and any user settings
* All preferences and settings
* Registration information (Nessus becomes unregistered)
* Master password for this Nessus installation, if there is one.
Are you sure you want to proceed? (y/n) [n]: y
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --reset-all
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --reset-all
```

Linux

```
/opt/nessus/sbin/nessuscli fix --reset-all
```

View the Current Network Interfaces

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To view current IPv4 and IPv6 interfaces, use the following command:

```
# /opt/nessus/sbin/nessuscli fix --list-interfaces
```

The following is example output:

```
Adapter# 0
      Name............ lo
      Real name ...... lo
      IP address ..... 127.0.0.1
```

```
      Network ........ 127.0.0.0
      Netmask ........ 255.0.0.0
Adapter# 1
      Name............ eth1
      Real name ...... eth1
      IP address ..... 192.0.2.243
      Network ........ 192.0.2.0
      Netmask ........ 255.255.252.0
Adapter# 0
      Name............ lo
      Real name ...... lo
      IPv6 address ... ::1
      IPv6 network ... ::1
      IPv6 netmask ... ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Adapter# 1
      Name............ eth1
      Real name ...... eth1
      IPv6 address ... fe80::250:56ff:fe10:76d
      IPv6 network ... fe80::
      IPv6 netmask ... ffff:ffff:ffff:ffff::
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --list-interfaces
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --list-interfaces
```

Linux

```
/opt/nessus/sbin/nessuscli fix --list-interfaces
```

Manage Advanced Settings

Required User Role: User with administrator privileges

The `nessuscli fix` command has a series of options to manage the advanced settings on your Tenable Nessus scanner.

For information on what advanced settings are configurable in your version of Tenable Nessus, see Advanced Settings in the *Tenable Nessus User Guide*.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To view all advanced settings:

To view all advanced settings, including those you have not set, use the following command:

```
# nessuscli fix --show
```

If you have not set an advanced setting, the default value is listed in the output.

To view a list of currently set advanced settings:

To list all advanced settings that you have set, use the following command:

```
# nessuscli fix --list
```

The following is example output:

```
# nessuscli fix --list
qdb_mem_usage: low
report_crashes: yes
stop_scan_on_disconnect: no
reduce_connections_on_congestion: no
global.max_web_users: 1024
global.max_scans: 0
nasl_log_type: normal
ssl_cipher_list: strong
xmlrpc_idle_session_timeout: 30
xmlrpc_listen_port: 8834
listen_port: 1241
listen_address: 0.0.0.0
slice_network_addresses: no
silent_dependencies: yes
auto_enable_dependencies: yes
safe_checks: yes
plugins_timeout: 320
non_simult_ports: 139, 445, 3389
checks_read_timeout: 5
allow_post_scan_editing: yes
optimize_test: yes
port_range: default
cgi_path: /cgi-bin:/scripts
rules: /Library/Nessus/run/etc/nessus/nessusd.rules
dumpfile: /Library/Nessus/run/var/nessus/logs/nessusd.dump
log_whole_attack: no
www_logfile: /Library/Nessus/run/var/nessus/logs/www_server.log
logfile: /Library/Nessus/run/var/nessus/logs/nessusd.messages
max_checks: 5
global.max_hosts: 2180
max_hosts: 100
auto_update_delay: 24
auto_update: yes
```

To see the current value for an advanced setting:

```
# nessuscli fix --get <setting>
```

For example:

```
# nessuscli fix --get max_hosts
The current value for 'max_hosts' is '100'.
```

To set a specific value for an advanced setting:

```
# /opt/nessus/sbin/nessuscli fix --set <setting>=<value>
```

Example:

```
# /opt/nessus/sbin/nessuscli fix --set max_hosts=200
Successfully set 'max_hosts' to '200'.
```

To delete your value from an advanced setting:

```
# nessuscli fix --delete <setting>
```

Example:

```
# /opt/nessus/sbin/nessuscli fix --delete max_hosts
Successfully deleted 'max_hosts'.
```

Secure Settings

You can use the `--secure` flag to manage encrypted advanced settings, which contain information about registration. Tenable does not recommend changing undocumented `--secure` settings as it may result in an unsupported configuration.

For the following commands, you can use the `--secure` flag:

```
# nessuscli fix --secure --list
```

```
# nessuscli fix --secure --fix --set <setting name=value>

# nessuscli fix --secure --get <setting>

# nessuscli fix --secure --delete <setting>
```

Command Quick Reference

For the full command for your operating system, see the following:

`nessuscli fix --show`

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --show
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --show
```

Linux

```
/opt/nessus/sbin/nessuscli fix --show
```

`nessuscli fix --list`

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --list
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --list
```

Linux

```
/opt/nessus/sbin/nessuscli fix --list
```

nessuscli fix --get <setting>

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --get <setting>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --get <setting>
```

Linux

```
/opt/nessus/sbin/nessuscli fix --get <setting>
```

nessuscli fix --set <setting>=<value>

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" --set <setting>=<value>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --set <setting>=<value>
```

Linux

```
/opt/nessus/sbin/nessuscli fix --set <setting>=<value>
```

`nessuscli fix --delete <setting>`

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fix --delete <setting>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --delete <setting>
```

Linux

```
/opt/nessus/sbin/nessuscli fix --delete <setting>
```

Configure Proxy Settings

Required User Role: User with administrator privileges

You can use the `nessuscli fix` command to use a proxy for plugin updates, as many companies maintain a proxy for security and logging.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To set the proxy settings, use the following command:

```
# nessuscli fix --secure --set <setting>=<value>
```

Replace the setting and value with any of the following:

Do not include the brackets (< >).

- `proxy=<IP address or hostname>`
- `proxy_port=<port>`
- `proxy_userame=<user>`
- `proxy_password=<password>`

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" --set <setting>=<value>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fix --set <setting>=<value>
```

Linux

```
/opt/nessus/sbin/nessuscli fix --set <setting>=<value>
```

Certificate Commands

The `nessuscli mkcert` commands offer the ability to create Tenable Nessus-supported self-signed digital certificates from the command line.

For more information, see the following:

- Create a Nessus Server Digital Certificate
- Create a Nessus Client-Side Digital Certificate

Create a Nessus Server Digital Certificate

> **Required User Role:** User with administrator privileges

You can create a Tenable Nessus-supported self-signed server certificate from the command line.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

> **Note:** When you regenerate or update the [[[Undefined variable Agent.NessusManager]]] CA certificate, existing linked [[[Undefined variable Agent.AgentPlural]]] automatically detect the change and update their local certificate trust. You do not need to unlink and re-link your agents after updating the [[[Undefined variable Agent.NessusManager]]] certificate.

Usage

To create a Tenable Nessus server digital certificate, use the following command:

```
# nessuscli mkcert
```

Read and follow the prompts. Prompt default responses are in brackets. The following is example output:

```
--------------------------------------------------------------------------------
Creation of the Nessus SSL Certificate
--------------------------------------------------------------------------------
```

```
This script asks you for information to create the SSL certificate.
for Nessus. This information is *NOT* sent to anybody
(everything stays local), but anyone with the ability to connect to
your Nessus daemon is able to retrieve this information.

CA certificate life time in days [1460]: 1460
Server certificate life time in days [365]: 365
Your two letter country code [US]: US
Your state or province name [NY]: MD
Your city [New York]: Columbia
Your organization [Nessus Users United]: Tenable Network Security
This hostname [localhost]: nessus-server

--- Confirmation ---
CA certificate life time in days: 1460
Server certificate life time in days: 365
Country: US
State or province: MD
City: Columbia
Organization: Tenable Network Security
This hostname: nessus-server
Is this ok? (y/n) [n]: y

Congratulations. Your server certificate was properly created.

The following files were created:
Certification authority:
Certificate = /opt/nessus/com/nessus/CA/cacert.pem
Private key = /opt/nessus/var/nessus/CA/cakey.pem
Nessus Server:
Certificate = /opt/nessus/com/nessus/CA/servercert.pem
Private key = /opt/nessus/var/nessus/CA/serverkey.pem
```

For more details on configuring Tenable Nessus with custom SSL certificates, see the *Tenable Nessus User Guide*.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" mkcert
```

macOS

```
/Library/Nessus/run/sbin/nessuscli mkcert
```

Linux

```
/opt/nessus/sbin/nessuscli mkcert
```

Create a Nessus Client-Side Digital Certificate

Required User Role: User with administrator privileges

You can create a Tenable Nessus client-side digital certificate from the command line.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

Note: If the user already has credentials, such as a password, this script overwrites any previous credentials. Also, updating the password of the account removes the client certificate for authentication.

To create a Nessus client digital certificate, use the following command:

```
# nessuscli mkcert-client
```

Read and follow the prompts. Prompt default responses are in brackets. The following is example output:

```
--------------------------------------------------------------------------------
Creation of the Nessus SSL Client Certificates
--------------------------------------------------------------------------------

This script asks you for information to create SSL client certificates.

Nessus username for user: admin
admin already exists.  Do you want to overwrite their credentials? (y/n) [n]: y
Client certificate life time in days [365]:
Two letter country code [US]: US
State or province name [NY]: MD
City [New York]: Columbia
Organization [Nessus Users United]: Tenable Network Security
Organizational unit [nessus-users]: nessus-admins
Email [none@none.com]: nessus-admin@example.org

--- Confirmation ---
Username: admin
Client certificate life time in days: 365
Country: US
State or province: MD
City: Columbia
Organization: Tenable Network Security
Organizational unit: nessus-admins
```

```
Email: nessus-admin@example.org
Is this ok? (y/n) [n]: y

Congratulations. Your client certificate was properly created.

The following files were created:
Nessus Client:
Certificate = /Library/Nessus/run/var/nessus/tmp/cert_admin.pem
Private key = /Library/Nessus/run/var/nessus/tmp/key_admin.pem

The certificate was successfully set for admin.

Create another cert? (y/n) [y]: n
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" mkcert-client
```

macOS

```
/Library/Nessus/run/sbin/nessuscli mkcert-client
```

Linux

```
/opt/nessus/sbin/nessuscli mkcert-client
```

User Management Commands

You can manage Tenable Nessus users from the command line.

For more information, see the following:

- List Users
- Change a User's Password
- Add a User
- Remove a User

List Users

> **Required User Role:** User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To list Tenable Nessus users, run the following command:

```
# nessuscli lsuser
```

Command Quick Reference

For the full command for your operating system, see the following:

> Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" lsuser
```

> macOS

```
/Library/Nessus/run/sbin/nessuscli lsuser
```

Linux

```
/opt/nessus/sbin/nessuscli lsuser
```

Change a User's Password

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To change a Tenable Nessus user's password, use the following command:

```
# [path]/nessuscli chpasswd <username>
```

Where *<username>* is the username for which you want to change the password. Do not include the brackets (< >).

Follow and respond to the prompts. In the `Login to change` field, enter the username, and then enter the new password when prompted. The password does not appear on the screen as you type.

The following is example output for Linux:

```
# /opt/nessus/sbin/nessuscli chpasswd auditor
Log in to change: auditor
New password:
New password (again):
Password changed for auditor
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" chpasswd <username>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli chpasswd <username>
```

Linux

```
/opt/nessus/sbin/nessuscli chpasswd <username>
```

Add a User

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To add a new Tenable Nessus user, use the following command:

```
# nessuscli adduser
```

When you add a user, you are prompted for the username, password, administrative rights, and rules. Tenable Nessus rules limit a user's scanning range.

When running `nessuscli adduser` on Tenable Nessus Professional or Tenable Nessus Expert, you are prompted for the user to have Administrator privileges. On Tenable Nessus Manager, you are prompted for the user to have System Administrator privileges. If you wish to set another user type in Tenable Nessus Manager, you must use the user interface.

Note: You cannot have multiple user accounts in Tenable Nessus Professional, Tenable Nessus Expert, Tenable Nessus Essentials, Tenable Nessus Essentials Plus, and managed Tenable Nessus instances. You can have multiple user accounts in Tenable Nessus Manager.

Note: If this is your first time creating a user with this command in your Tenable Nessus Manager instance, Tenable recommends restarting Tenable Nessus to ensure that the user interface properly updates with the new user's information.

Follow the prompts. The following is example output for Linux:

```
# /opt/nessus/sbin/nessuscli adduser
Login: nessususer
Login password:
Login password (again):
Do you want this user to be a Nessus 'system administrator' user (can upload plugins,
etc.)? (y/n) [n]: y
```

When you are adding a new user, Tenable Nessus prompts you for User Rules. Tenable Nessus has a rules system that allows you to restrict the hosts and ports that can be scanned and the plugins that can be used in scans. Administrators can set the rules on a per-user basis.

After you set the username, password, and administrator privileges, you are prompted to set any Tenable Nessus rules:

```
User rules
----------
nessusd has a rules system that allows you to restrict the hosts that nessususer has
the right to test. For instance, you may want to allow the user to scan any system by
default.
```

```
Please see the Nessus Command Line Reference for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done : (the user can
have an empty rules set)

Login    : nessususer
Password : ***********
This user will have 'system administrator' privileges within the Nessus server
Is that ok? (y/n) [n]: y
User added
```

To configure the user with default rules, enter `default`.

To allow the user to test anything by default, enter `default accept`.

> **Note:** A blank rule set also allows the user to test anything.

For more information on rule syntax, see Network and Port Rules and Plugin Rules.

After you enter the desired rules, you are prompted to confirm your new user setup:

```
Login    : nessususer
Password : ***********
This user will have 'system administrator' privileges within the Nessus server
Is that ok? (y/n) [n]: y
User added
```

Command Quick Reference

For the full command for your operating system, see the following:

> Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" adduser
```

macOS

```
/Library/Nessus/run/sbin/nessuscli adduser
```

Linux

```
/opt/nessus/sbin/nessuscli adduser
```

Remove a User

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To remove a Tenable Nessus user, use the following command:

```
# nessuscli rmuser
```

Follow the prompts. The following is example output:

```
Login to remove: auditor
User removed
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" rmuser
```

macOS

```
/Library/Nessus/run/sbin/nessuscli rmuser
```

Linux

```
/opt/nessus/sbin/nessuscli rmuser
```

Update Commands

The `nessuscli` commands offer the ability to update Tenable Nessus and Nessus plugins. By default, the software update options selected through the Tenable Nessus user interface determine the update settings.

For more information, see the following:

- Update Tenable Nessus
- Force the Plugin and Core Components Update
- Update the Plugins Only
- Update a Specific Plugin Archive
- Network and Port Rules
- Plugin Rules

Update Tenable Nessus

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To run update according to the setting in the Tenable Nessus user interface, use the following command:

```
# nessuscli update
```

In the following example, the update options are configured to update both the Tenable Nessus software and the plugins:

```
# /opt/nessus/sbin/nessuscli update

----- Fetching the newest updates from nessus.org -----

Nessus Plugins: Complete

Nessus Core Components: Complete

* Nessus Plugins are now up-to-date and the changes will be automatically processed by
Nessus.
* Nessus Core Components are now up-to-date and the changes will be automatically
processed by Nessus.
```

Note: You cannot use the update command when Tenable Nessus is in offline mode.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" update
```

macOS

```
/Library/Nessus/run/sbin/nessuscli update
```

Linux

```
/opt/nessus/sbin/nessuscli update
```

Force the Plugin and Core Components Update

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

If you want to update all Tenable Nessus core components, you can override your update settings by using `nessuscli update` with the `--all` option.

```
# nessuscli update --all
```

The following is example output for Linux:

```
# /opt/nessus/sbin/nessuscli update --all

----- Fetching the newest updates from nessus.org -----

Nessus Plugins: Complete
```

```
Nessus Core Components: Complete

* Nessus Plugins are now up to date and Nessus processes the changes automatically.
* Nessus Core Components are now up to date and Nessus processes the changes
automatically.
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" update --all
```

macOS

```
/Library/Nessus/run/sbin/nessuscli update --all
```

Linux

```
/opt/nessus/sbin/nessuscli update --all
```

Update the Plugins Only

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

If you want to update Tenable Nessus scanner plugins, you can override your update settings by using `nessuscli update` with the `--plugins-only` option:

```
# nessuscli update --plugins-only
```

The following is example output for Linux:

```
# /opt/nessus/sbin/nessuscli update --plugins-only

----- Fetching the newest updates from nessus.org -----

Nessus Plugins: Complete

* Nessus Plugins are now up to date and Nessus processes the changes automatically.
```

This command applies to Tenable Nessus scanners. To manually update plugins on a Tenable Agent, see Update Tenable Agent Plugins.

Note: This command only works for standalone Tenable Nessus scanners. The command does not work for scanners managed by Tenable One Vulnerability Management or Tenable Security Center.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" update --plugins-only
```

macOS

```
/Library/Nessus/run/sbin/nessuscli update --plugins-only
```

Linux

```
/opt/nessus/sbin/nessuscli update --plugins-only
```

Update a Specific Plugin Archive

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

If you want to supply a plugin archive (for example, for offline updates or supplying custom plugins), add the file name or file path after the update command:

```
# nessuscli update <examplefilename>.tar.gz

* Update successful.  The changes will be automatically processed by Nessus.
```

Note: If the file path has spaces, you must enclose the path in quotation marks.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" update <examplefilename>.tar.gz
```

macOS

```
/Library/Nessus/run/sbin/nessuscli update <examplefilename>.tar.gz
```

Linux

```
/opt/nessus/sbin/nessuscli update <examplefilename>.tar.gz
```

Network and Port Rules

Use the following syntax to configure Nessus network scanning rules:

```
accept|reject address/netmask:ports
```

The address/netmask is in CIDR notation.

For example, based on the following rule, you cannot scan any IP address in the /24 (standard class C) network:

```
reject 10.42.123.0/24
```

Similarly, based on the following rule, you can scan any IP address in the /8 (standard class A) network:

```
accept 10.1.1.0/8
```

Also, you can define ports or a port range to be allowed or denied certain ports. For example, to forbid connecting to port 80 for 10.0.0.1, enter the following rule:

```
reject 10.0.0.1:80
```

To reject multiple non-consecutive ports for the same IP address, define a separate rule for each port. For example, to reject ports 23 and 80 for 10.0.0.1, enter the following rules:

```
reject 10.0.0.1:23
```

```
reject 10.0.0.1:80
```

Similarly to allow connecting to ports 8000 - 10000 for any host in the 192.168.0.0/24 subnet, enter the following rule:

```
accept 192.168.0.0/24:8000-10000
```

Plugin Rules

In addition to setting network scanning limitations, you can also allow or deny the use of certain plugin IDs.

To deny a plugin from being run, use the following syntax:

```
plugin-reject 10335
```

To allow a plugin to run, use the following syntax:

```
plugin-accept 10000-40000
```

Fetch Commands

You can use fetch commands to manage Tenable Nessus registration from the command line.

For online registration the commands include registering the scanner, confirming that Tenable Nessus has a valid registration code, and registering with Tenable Security Center. For offline registration, the commands include registering the scanner and providing the challenge code. The

`nessuscli` commands can also check that Tenable Nessus is properly configured with a valid registration code and can display the current activation code in use.

For more information, see the following:

- Register a Scanner Online
- Register a Scanner with Tenable Security Center
- Register a Scanner Offline
- Confirm Nessus Registration Codes

Register a Scanner Online

> **Required User Role:** User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To register a Tenable Nessus scanner online, use the following command:

```
# nessuscli fetch --register <Activation Code>
```

Use a unique activation code. If the registration code is already in use, the following message appears:

```
Nessus Plugins Error: The provided Activation Code (XXXX-XXXX-XXXX-XXXX) has already
been used.
```

To register Tenable Nessus online but not perform any updates, use the following command:

```
nessuscli fetch --register-only <Activation Code>
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fetch --register
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fetch --register
```

Linux

```
/opt/nessus/sbin/nessuscli fetch --register
```

Register a Scanner with Tenable Security Center

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To register a Nessus scanner with Tenable Security Center, use the following command:

```
# nessuscli fetch --security-center
```

Caution: *Do not use this command if you do not want to switch your Tenable Nessus instance to Tenable Security Center.* This command irreversibly changes the Tenable Nessus scanner or

Manager to a Tenable Security Center-managed scanner, resulting in a number of user interface changes (for example, the site logo changes, and you no longer have access to the **Sensors** page).

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fetch --security-center
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fetch --security-center
```

Linux

```
/opt/nessus/sbin/nessuscli fetch --security-center
```

Register a Scanner Offline

Required User Role: User with administrator privileges

You can register Tenable Nessus offline using the command line interface.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

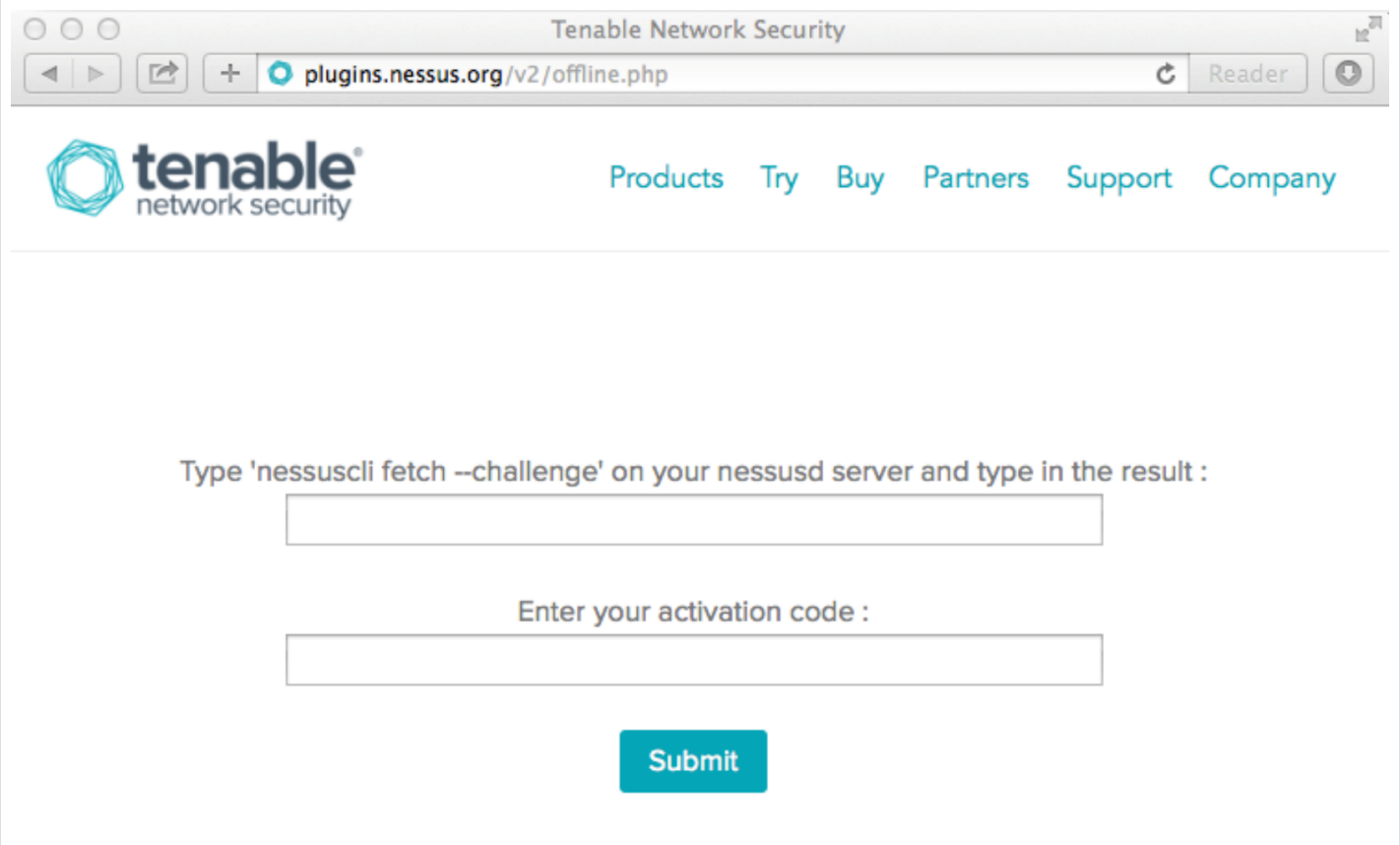
To register Tenable Nessus offline, first obtain the challenge code for Tenable Nessus using the following command:

```
# nessuscli fetch --challenge
```

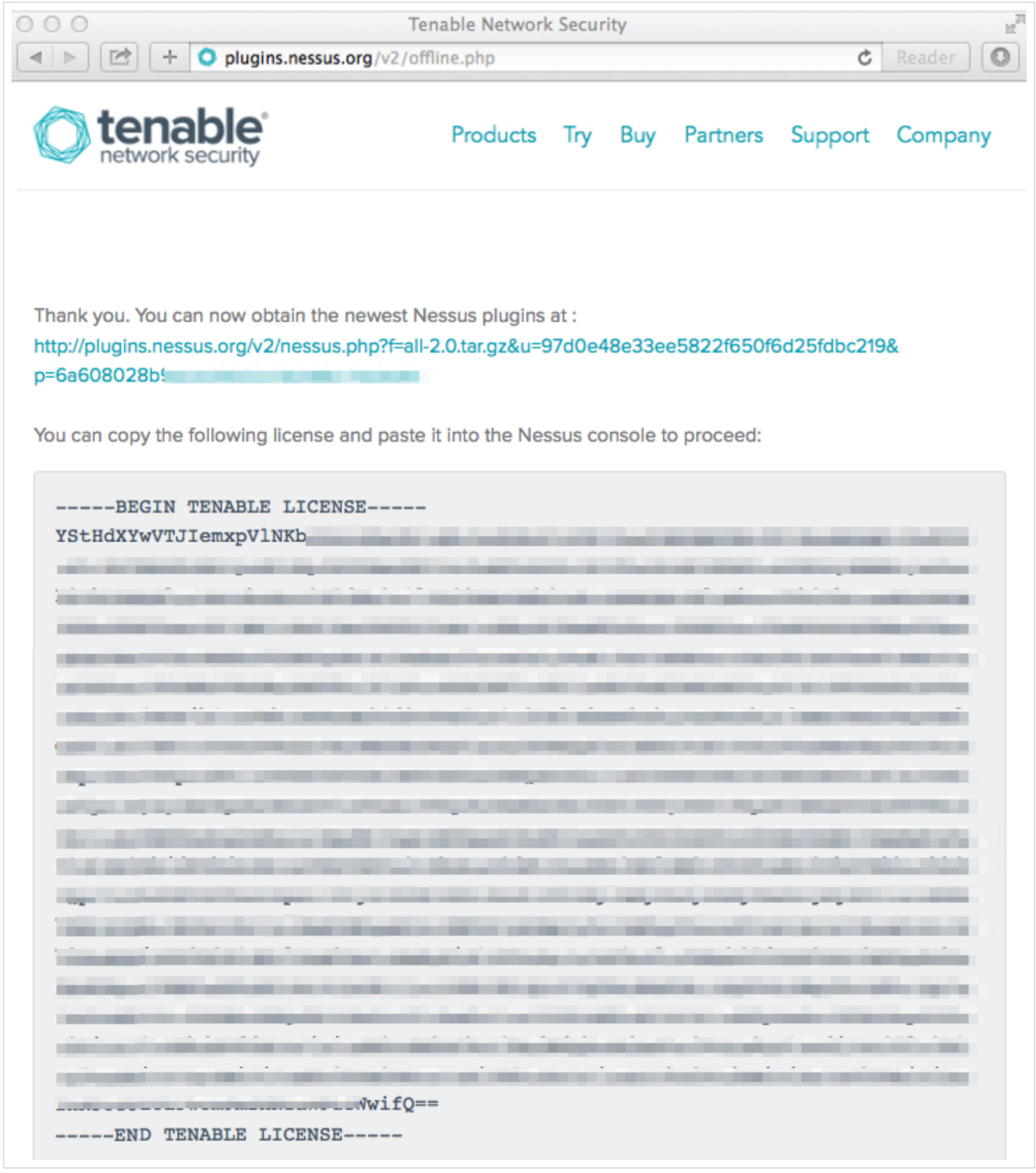
The following is example output in Linux:

```
# /opt/nessus/sbin/nessuscli fetch --challenge
Challenge code: aaaaaa11b2222cc33d44e5f6666a777b8cc99999
You can copy the challenge code above and paste it alongside your
Activation Code at:
https://plugins.nessus.org/v2/offline.php
```

Once you have obtained your challenge code, go to the offline activation website to enter your activation code and the challenge code:



Once registered, you receive the URL to copy and paste the license into your browser, and download the plugins and a link to download the `nessus.license` file. You can also scroll to the bottom of the screen to download the license instead of cutting and pasting it.


Tenable Network Security
plugins.nessus.org/v2/offline.php
Reader
tenable network security
Products Try Buy Partners Support Company
Thank you. You can now obtain the newest Nessus plugins at :
http://plugins.nessus.org/v2/nessus.php?f=all-2.0.tar.gz&u=97d0e48e33ee5822f650f6d25fdbc219&
p=6a608028b
You can copy the following license and paste it into the Nessus console to proceed:
-----BEGIN TENABLE LICENSE-----
YStHdXYwVTJIemxpVlNKb
wifQ==
-----END TENABLE LICENSE-----

After you register your scanner as an offline scanner, register a Tenable Nessus scanner offline using the following command:

```
# nessuscli fetch --register-offline <license.file>
```

The following is example output in Linux:

```
# /opt/nessus/sbin/nessuscli fetch --register-offline nessus.license
Nessus has been registered properly - thank you.
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fetch --register-offline <license.file>
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fetch --register-offline <license.file>
```

Linux

```
/opt/nessus/sbin/nessuscli fetch --register-offline <license.file>
```

Confirm Nessus Registration Codes

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To confirm that the Tenable Nessus scanner is registered properly, use the following command:

```
# nessuscli fetch --check
```

To display that the Tenable Nessus scanner activation code, use the following command:

```
# nessuscli fetch --code-in-use
```

Command Quick Reference

For the full command for your operating system, see the following:

nessuscli fetch --check

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" fetch --check
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fetch --check
```

Linux

```
/opt/nessus/sbin/nessuscli fetch --check
```

nessuscli fetch --code-in-use

Windows

```
C:\Program Files\Tenable\Nessus\nessuscli.exe fetch --code-in-use
```

macOS

```
/Library/Nessus/run/sbin/nessuscli fetch --code-in-use
```

Linux

```
/opt/nessus/sbin/nessuscli fetch --code-in-use
```

Bug Reporting Commands

Required User Role: User with administrator privileges

You can create a .zip bug report that can be sent to Tenable to help diagnose issues.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To create the bug report archive, use the following command:

```
# nessuscli bug-report-generator
```

By default, the script runs in interactive mode.

The following is example output in Linux:

```
# /opt/nessus/sbin/nessuscli bug-report-generator
This script gathers some information about your local system in order to help us
diagnose the problems you are encountering.

This program does not send any data over the network, but simply creates an archive
which contains useful information for the Nessus team to diagnose any problem you may
be encountering.

This script can run in two modes:

If you run in "full" mode, this script gathers information you may deem
to be sensitive (such as IP addresses, the list of running processes and your
system log files). This information allows Tenable to qualify your problem.

If you do not run in "full" mode, this script gathers less information.
Even in normal mode, depending on how you perform scanning some "sensitive" information
may be contained in the resulting archive. Feel free to inspect it before sending it to
Tenable.

Run in "full" mode? (y/n) [n]: n

Would you like to scrub the first two digits of any IPv4 address seen in the log files?
This may take several minutes.

Sanitize IPv4 subnets? (y/n) [n]: y
Bug report file name? [/opt/nessus/var/nessus/logs/nessus-bug-report-archive.zip]:
~/nessus-bug-report-archive.zip

-> Copying /etc/redhat-release...
-> Copying /etc/SuSE-release...
-> Copying /etc/debian_version...
-> Running uname -a...
-> Running /opt/nessus/sbin/nessusd -d...
-> Running ldd /opt/nessus/sbin/nessusd...
-> Running dmesg...
```

```
-> Running tail -n 10000 /opt/nessus/var/nessus/logs/nessusd.messages...
-> Running tail -n 10000 /opt/nessus/var/nessus/logs/nessusd.dump...
-> Copying /opt/nessus/var/nessus/uuid...
-> Running bash -c cd /opt/nessus/var/nessus/logs;ls | grep -v nessusd.messages | grep
-v nessusd.dump | grep -v www_server.log | grep -v nessus-bug-report-archive | xargs
cat...
-> Running killall -USR2 nessusd...
-> Running bash -c cd /opt/nessus/var/nessus/logs;ls | grep -v nessusd.messages | grep
-v nessusd.dump | grep -v www_server.log | grep -v nessus-bug-report-archive | xargs
cat...
-> Running nessuscli fix --list...
-> Running uptime...
-> Running ls -l /opt/nessus/lib/nessus/plugins...
-> Copying /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc...
-> Running bash -c ps auxwwww | grep nessus...
-> Running netstat -i...
-> Running netstat -rn...
-> Running arp -an...
-> Running df -h...
-> Running ls -l /opt/nessus/var/nessus...
-> Running cat /proc/cpuinfo...
-> Running sysctl hw.model...
-> Running free...
-> Running nessuscli fix --list-interfaces...
-> Running bash -c ls -l /opt/nessus/var/nessus/../.....
-> Running du -shk /opt/nessus/var/nessus/../.....
-> Collecting script environment information...

Thank you. Send the file /root/nessus-bug-report-archive.zip to:
- bug-reports@nessus.org (if you are not a direct feed customer)
or
- Tenable Support (if you are a direct feed customer)
```

You can also add the following options:

- `--quiet` – Run the bug report generator without prompting the user for feedback.
- `--scrub` – When in quiet mode, the bug report generator sanitizes the first two octets of the IPv4 address.
- `--full` – When in quiet mode, the bug report generator collects extra data.
- `--targz` (Tenable Nessus 10.9.0 and later) – The bug report generates as a tar.gz file.

Note: Using `--full` or `--scrub` is dependent on using `--quiet` first. If the `--quiet` option is not used, the bug report generator ignores anything else and runs in full mode.

Note: Even in normal mode, the script may pick up sensitive information, depending on how your scans are configured.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" bug-report-generator [--quiet] [--scrub] [--full]
```

macOS

```
/Library/Nessus/run/sbin/nessuscli bug-report-generator [--quiet] [--scrub] [--full]
```

Linux

```
/opt/nessus/sbin/nessuscli bug-report-generator [--quiet] [--scrub] [--full]
```

Tenable Agent

As an administrator user, you can manage certain settings for Tenable Agent via the command line.

Tenable Agent has its own `nessuscli` tool.

Tenable Agent Command Line Tool

For Tenable Nessus Agent, use the following command syntax for your operating system.

Operating System	Command
Windows	`"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" <cmd> <arg1> <arg2>`
macOS	`# /Library/NessusAgent/run/sbin/nessuscli <cmd> <arg1> <arg2>`
Linux	`# /opt/nessus_agent/sbin/nessuscli <cmd> <arg1> <arg2>`

Command Syntax

- **`# nessuscli`** – This documentation sometimes uses the shorthand `# nessuscli` (instead of the full path to the `nessuscli` tool for the operating system) to represent general usage across different operating systems. However, for your commands to work, you must include the full path for your operating system, as shown above.

  For each command, the documentation contains a quick reference section with the full command for each operating system. You can copy and paste these commands directly into the command line terminal.
- **`<cmd>`** – The command. Do not include the brackets (< >).
- **`<arg 1> <arg 2>`** – The arguments for the command, if applicable. Do not include the brackets (< >).

For more information, see the following:

- Help Agent Commands
- Fix Agent Settings
- Local Agents Commands
- Bug Report Generator Agent Commands

Help Agent Commands

> **Required User Role:** User with administrator privileges

You can get help to see available commands on the `nessuscli` tool, as well as get help for a specific command.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To display the command line usage for the Agent `nessuscli` tool, type the following:

```
# nessuscli help
```

The output shows as follows:

```
Usage: nessuscli command [options]
Usage: nessuscli command help

Fix Commands:
- fix [--secure] --list
- fix [--secure] --set <name=value>
```

```
- fix [--secure] --get <name>
- fix [--secure] --delete <name>
- fix --list-interfaces
- fix --reset

Local Agent Commands:
- agent link --key=<key> [--name=<name>] [--groups=<group1,group2,...>] [--ca-path=<ca_
file_name>] [host] [proxy]
- agent unlink
- agent status
- agent update --file=<plugins_set.tgz>

Bug Reporting Commands:
- bug-report-generator
- bug-report-generator --quiet [--full] [--scrub]
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus\nessuscli.exe" help
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli help
```

Linux

```
/opt/nessus_agent/sbin/nessuscli help
```

Fix Agent Settings

The following settings describe `nessuscli fix` commands that relate to Tenable Agent.

Command	Description
`# nessuscli fix --list`	Shows a list of agent settings and their values.
`nessuscli fix --set <setting>=<value>`	Set an agent setting to the specified value. For a list of agent settings, see Advanced Settings in the *Tenable Agent User Guide*.
`# nessuscli fix --set update_hostname="<value>"`	Updates agent hostnames automatically in Tenable One Vulnerability Management or Tenable Nessus Manager. You can set the `update_hostname` parameter to `yes` or `no`. By default, this preference is disabled. **Note:** Restart the agent service for the change to take effect in Tenable Nessus Manager.
`# nessuscli fix --set agent_update_channel=<value>`	(Tenable One Vulnerability Management-linked agents only) Sets the agent update plan to determine what version the agent automatically updates to. Values: • **ga** – Automatically updates to the latest Tenable NessusAgent version when it is made generally available (GA). **Note:** This date is the same day the version is made generally available.This date is usually *one week after* the version is made generally available. For versions that address critical security issues, Tenable may

Command	Description
	make the version available immediately. • **ea** – Automatically updates to the latest Tenable NessusAgent version as soon as it is released for Early Access (EA), typically a few weeks before general availability. • **stable** – Does not automatically update to the latest Tenable NessusTenable Agent version. Remains on an earlier version of Tenable NessusTenable Agent set by Tenable, usually one release older than the current generally available version, but no earlier than 8.10.0.7.7.0. When Tenable NessusTenable Agent releases a new version, your Tenable Nessus instance agent updates software versions, but stays on a version prior to the latest release. **Note:** For agents linked to Tenable One Vulnerability Management, you need to run the `agent_update_channel` command from the agent `nessuscli` utility. For agents linked to Tenable Nessus Manager, you need to run the `agent_update_channel` command from the Tenable Nessus Manager`nessuscli` utility.
`# nessuscli fix --set maximum_scans_per_day=<value>`	(Tenable One Vulnerability Management-linked agents only) Sets the maximum number of scans an agent can run per day. The minimum amount is **1**, the maximum amount is **48**, and the default amount is **10**.
`# nessuscli fix --set max_retries="<value>"`	Sets the maximum number of times an agent should retry in the event of a failure when executing the `agent link`, `agent status`, or `agent unlink` commands. The commands retry, the specified number of times, consecutively, sleeping increasing increments of time set by `retry_sleep_milliseconds` between attempts. The default value for

Command	Description
	`max_retries` is 0. The minimum value is 0, and the maximum value is 10. For example, if you set `max_retries` to 4 and set `retry_sleep_milliseconds` to the default of 1500, then the agent will sleep for 1.5 seconds after the first try, 3 seconds after the second try, and 4.5 seconds after the third try. **Note:** This setting does not affect offline updates or the agent's normal 24 hour check-in after it is linked.
`# nessuscli fix --set retry_sleep_milliseconds="<value>"`	Sets the number of milliseconds that an agent sleeps for between retries in event of a failure when executing the `agent link`, `agent status`, or `agent unlink` commands. The default is 1500 milliseconds (1.5 seconds).
`# nessuscli fix --set niap_mode=enforcing`	Enforces NIAP mode for Tenable Agent. For more information about NIAP mode, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set niap_mode=non-enforcing`	Disables NIAP mode for Nessus Agent. For more information about NIAP mode, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set fips_mode=enforcing`	Enforces the current validated FIPS module for Tenable Agent communication and database encryption. The FIPS module does not affect scanning encryption. **Note:**Tenable Agent also enforces the FIPS module when you enforce

Command	Description
	NIAP mode. For more information, see Configure Tenable Agent for NIAP Compliance.
`# nessuscli fix --set fips_mode=non-enforcing`	Disables the FIPS module for Tenable Agent communication and database encryption. **Note:** Tenable Agent also disables the FIPS module when you disable NIAP mode. For more information, see Configure Tenable Agent for NIAP Compliance.

`# nessuscli fix --set process_priority="<value>"`
 	
`# nessuscli fix --get process_priority`
 	
`# nessuscli fix --delete process_priority`
	Set, get, or delete the `process_priority` setting.
	
	You can control the priority of the Tenable Agent relative to the priority of other tasks running on the system by using the `process_priority` preference.
	
	For valid values and more information on how the setting works, see Agent CPU Resource Control.

Local Agents Commands

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

You can link agents, unlink agents, and get a report on the status of the agent.

Link the Nessus Agent

The `nessuscli agent link` command links the agent to Tenable Nessus Manager or Tenable One Vulnerability Management, using the manager linking key.

```
# nessuscli agent link --
key=00b5a8fec9f3a21fa1cff66ce99c6324adf324226948c6f1516eb9f9433b964744
```

Required arguments:

- `--key=<key>`
- `--host=<host>`
- `--port=<port>`

Optional arguments:

- `--name=<name>`
- `--groups=<group1,group2,...>`
- `--ca-path=<ca_file_name>`
- `--offline-install`
- `--proxy-host=<host>`
- `--proxy-port=<port>`
- `--proxy-username=<username>`
- `--proxy-password=<password>`
- `--proxy-agent=<agent>`

Command Quick Reference

For the full command for your operating system, see the following:

> Windows

```
C:\Program Files\Tenable\Nessus Agent\nessuscli.exe agent link
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli agent link
```

Linux

```
/opt/nessus_agent/sbin/nessuscli agent link
```

Success or Failure Messages

Once the agent is successfully linked, the following output appears:

```
# nessuscli agent link --
key=00b5a8fec9f3a21fa1cff66ce99c6324adf324226948c6f1516eb9f9433b964744 --groups=
Workstation --host=ndev3 --port=8834
Agent successfully linked
```

If there were issues connecting the agent to the manager, a **Failed to link the agent** message appears.

```
# nessuscli agent link --
key=00abd4c487c472edb77cea8a14bb8c603a88203a2e6bf1f6df46159b5ad5ef18df --
name=Workstation --groups=Accounting --host=192.0.2.252 --port=8834
Failed to link the agent:
```

Check the Nessus Agent Status

The agent status shows you if an agent is linked, and how many jobs are pending if it is linked.

```
# nessuscli agent status
Agent linked
0 jobs pending
```

If the agent is not linked, the status shows that it is not linked to any servers.

```
# nessuscli agent status
Agent not linked to a server
```

If the agent is linked, the status shows the IP address of the connected server and port:

```
# nessuscli agent status
Agent is linked to 192.0.2.184:8834
0 jobs pending
```

Unlink the Nessus Agent

The `nessuscli agent unlink` command unlinks the agent from Tenable Nessus Manager or Tenable One Vulnerability Management.

```
# nessuscli agent unlink
```

Triggered Agent Scan Commands

List Triggered Scan Details

> **Required User Role:** User with administrator privileges

List details about the agent's triggered scan rules by running the following command:

```
# nessuscli scan-triggers --list
```

The output includes the following information:

- Scan name
- Status (for example, **uploaded**)
- Time of last activity (shown next to the status)
- Scan description
- Time of last policy modification
- Time of last run
- Scan triggers
- Scan configuration template
- Command to launch the scan (`nessuscli scan-triggers --start --UUID=<scan-uuid>`)

Note: Triggered scanning is only available for agents linked to Tenable One Vulnerability Management. For more information, see Triggered Agent Scans in the *Tenable One Vulnerability Management User Guide*.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" scan-triggers --list
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli scan-triggers ---list
```

Linux

```
/opt/nessus_agent/sbin/nessuscli scan-triggers --list
```

Launch a Triggered Scan

Required User Role: User with administrator privileges

Launch an existing triggered scan manually by running the following command:

```
# nessuscli scan-triggers --start --UUID=<scan-uuid>
```

Note: Triggered scanning is only available for agents linked to Tenable One Vulnerability Management. For more information, see Triggered Agent Scans in the *Tenable One Vulnerability Management User Guide*.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" scan-triggers --start --UUID=<scan-uuid>
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli scan-triggers --start --UUID=<scan-uuid>
```

Linux

```
/opt/nessus_agent/sbin/nessuscli scan-triggers --start --UUID=<scan-uuid>
```

Link Windows Agents During Installation

Required User Role: User with administrator privileges

Usage

You can deploy and link Tenable Agents on Windows with the `msiexec` command. For example:

```
# msiexec /i NessusAgent-versionnumber.msi NESSUS_GROUPS="Remote Agent Group 1"NESSUS_
SERVER="192.0.2..34:8834" NESSUS_
KEY=00a0927cb3df64d466ccd7ccbcc2d63fea1ea91f5ea5ebe22390a4d69caa6c6acf /qn
```

The following are available linking parameters:

Parameter	Description
`NESSUS_OFFLINE_INSTALL`	You can install the Tenable Agent on a system even if it is offline. Add the command line option `NESSUS_OFFLINE_INSTALL="yes"` to the command line input. The Tenable Agent will periodically attempt to link itself to either Tenable One Vulnerability Management or Tenable Nessus Manager. If the agent cannot connect to the controller then it retries every hour, and if the agent can connect to the controller but the link fails then it retries every 24 hours.
`ADDLOCAL=ALL`	Install the Tenable Agent system tray application, as described in step 8 of Install a Tenable Nessus Agent on Windows in the *Tenable Agent User Guide*.
`ADDLOCAL=ALL`	Install the Tenable Agent system tray application, as described in step 8 of Install a Tenable Nessus

	Agent on Windows in the *Tenable Agent User Guide*.
`NESSUS_PLUGINS_ FILEPATH="C:\path\to\plugins_ set.tgz"`	Install a full plugins set before linking to reduce the bandwidth impact during a mass installation. Add the command line option `NESSUS_PLUGINS_ FILEPATH="C:\path\to\plugins_set.tgz"` where *plugins_set.tgz* is a recent plugins set tarball less than five days old. A stale plugins set older than five days will force a full plugins download to occur. You can download a recent plugins set from the Tenable downloads page.
`NESSUS_GROUPS`	Specify existing agent group or groups where you want to add the agent. If you do not specify an agent group during the install process, you can add your linked agent to an agent group later in Tenable Nessus Manager or Tenable One Vulnerability Management. **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`). **Note:** Quotation marks (") are necessary when listing multiple groups, or one group with spaces in its name. For example: • GroupName • "Group Name" • "Group, Another Group"
`NESSUS_PROCESS_PRIORITY`	Determine the priority of the agent relative to the priority of other tasks running on the system. For

	valid values and more information on how the setting works, see Agent CPU Resource Control *Tenable Agent Deployment and User Guide*.
NESSUS_NAME	Specify the name for your agent. If you do not specify a name for your agent, the name defaults to the name of the computer where you are installing the agent.
NESSUS_CA_PATH	Specify a custom CA certificate to use to validate the manager's server certificate.
NESSUS_PROXY_SERVER	Specify the hostname or IP address of your proxy server.
NESSUS_PROXY_USERNAME	Specify the name of a user account that has permissions to access and use the proxy server.
NESSUS_PROXY_PASSWORD	Specify the password of the user account that you specified as the username.
NESSUS_PROXY_AGENT	Specify the user agent name, if your proxy requires a preset user agent.

For more information on installing Tenable Agents on Windows, see Install a Nessus Agent on Windows in the *Tenable Nessus User Guide*.

Local Agent Plugin Commands

Retrieve Agent Plugin Info

Required User Role: User with administrator privileges

To list details about the agent's current plugins, use the following command:

```
# nessuscli plugins --info
```

The output shows the following information about the agent's `full` and `inventory` plugin sets:

- `Installed version`
- `Last downloaded`
- `Last needed`
- `Expires in` – The plugin set's expiration time and date (that is, when the plugin set is no longer needed).
- `Plugins` – The total number of plugins in the plugin set.
- `Uncompressed source size`

The output also lists general details and statistics about the agent's plugins, such as:

- `Last plugin update time`
- `Last plugin update check time`
- `Total compressed plugins source size`
- `Total compiled plugins size`
- `Total plugins attributes data`
- `Total plugin size on disk`

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" plugins --info
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli plugins --info
```

Linux

```
/opt/nessus_agent/sbin/nessuscli plugins --info
```

Reset Agent Plugins

Required User Role: User with administrator privileges

To delete all plugins and plugin-related data off the disk, use the following command:

```
# nessuscli plugins --reset
```

The agent is able to download new plugins immediately after the deletion completes.

Note: This command only triggers if the agent has plugin data on its disk.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" plugins --reset
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli plugins --reset
```

Linux

```
/opt/nessus_agent/sbin/nessuscli plugins --reset
```

Update Tenable Agent Plugins

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

If you want to manually install a plugin set on a Tenable Agent (for example, for offline updates or manual plugin updates), use the following command:

```
# nessuscli agent update --file=<plugins_set.tgz>
```

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" agent update --file=<plugins_set.tgz>
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli agent update --file=<plugins_set.tgz>
```

Linux

```
/opt/nessus_agent/sbin/nessuscli agent update --file=<plugins_set.tgz>
```

Install Tenable Identity Exposure Secure Relay

Required User Role: User with administrator privileges

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To install a Tenable One Identity Exposure Secure Relay on the agent, use the following command:

```
# nessuscli install-relay --linking-key=<Tenable One Identity Exposure relay linking key>
```

To retrieve the Tenable One Identity Exposure relay linking key, see Secure Relay in the *Tenable One Identity Exposure Guide*.

`install-relay` supports the following optional parameters:

- `proxy_address` – The proxy IP or DNS to use if you require a proxy to reach Tenable domains. If you enter a `proxy_address`, you need to enter a `proxy_port`.
- `proxy_port` – The proxy port to use if you require a proxy to reach Tenable domains. If you enter a `proxy_port`, you need to enter a `proxy_address`.
- `proxy_basic_login` – The proxy login username. If you enter a `proxy_basic_login`, you need to enter a `proxy-basic-password`.

- `proxy-basic-password` – The proxy login password. If you enter a `proxy-basic-password`, you need to enter a `proxy_basic_login`.

If you do not want to specify a proxy, do not enter any proxy parameters. To specify an unauthorized proxy, enter a `proxy_address` and a `proxy_port`. To specify an authorized proxy, enter a `proxy_address`, a `proxy_port`, a `proxy_basic_login`, and a `proxy-basic-password`.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" install-relay --linking-key=<relay linking key>
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli install-relay --linking-key=<relay linking key>
```

Linux

```
/opt/nessus_agent/sbin/nessuscli install-relay --linking-key=<relay linking key>
```

Bug Report Generator Agent Commands

Required User Role: User with administrator privileges

You can create a .zip bug report that can be sent to Tenable to help diagnose issues.

To see and copy the full command for your specific operating system, see the Command Quick Reference.

Usage

To create the bug report archive, use the following command:

```
# nessuscli bug-report-generator
```

If you run this command without arguments, the utility prompts you for values.

Optional arguments:

- `--quiet` – Run the bug report generator without prompting user for feedback.
- `--scrub` – The bug report generator sanitizes the last two octets of the IPv4 address.
- `--full` – The bug report generator collects extra data.
- `--targz` (Tenable Nessus 10.9.0 and later) – The bug report generates as a tar.gz file.

Command Quick Reference

For the full command for your operating system, see the following:

Windows

```
"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" bug-report-generator
```

macOS

```
/Library/NessusAgent/run/sbin/nessuscli bug-report-generator
```

Linux

```
/opt/nessus_agent/sbin/nessuscli bug-report-generator
```