# Enable Secure Mode

*For supported software information, click here.*

Note: Contact Versa Networks Customer Support before deploying secure mode.

To protect user information and the history of user activity and to harden Linux core OS components, you can run Versa Operating System$^{TM}$ (VOS$^{TM}$) and Director devices in secure mode. You can also configure secure mode to protect the menu for GRUB, which is Ubuntu boot loader, and to protect the VOS console UI.

## Enable Secure Mode on Director and VOS Devices

To enable secure mode, issue the following CLI command from the Director node or the VOS device:

```
request system secure-mode enable [grub-password password] [disable-nodejs]
```

To protect the GRUB menu, include the **grub-password** option. The password can be any password string. Each time you enter the GRUB menu from the console, you are prompted to enter this password. The GRUB menu username is root, and this user is different from the system root user. Specifying this option does not affect any VOS reboots, because you issue those reboot commands from the CLI, using the **request system reboot** command.

To secure the VOS console UI, include the **disable-nodejs** option to disable the node. After you disable node.js, you must restart the VOS device by issuing the **vsh restart** command.

The following table describes the system components that you can protect when you enable secure mode.

| Component | Protection |
|---|---|
| SSH options (for Releases 16.1R2S7 and earlier, and for Releases 20.1 and later) | To protect SSH options, you can do the following:<br>• Set LoginGraceTime to 60 so that the server disconnects a user if they have not successfully logged in after 60 seconds.<br>• Set MaxSessions to 5, to limit the number of multiplexed SSH sessions that can be present on a single SSH session. Session multiplexing allows you to set up a single master connection that all other |

| Component | Protection |
|---|---|
|  | connections to the same host can use or reuse. Limiting the maximum number of multiplexed SSH sessions has no effect on port forwarding, on the SOCKS proxy, or on your ability to connect again to the same host through a new network connection. Use a PrivilegeSeparation sandbox, which is specific to connection multiplexing, to help prevent privilege escalation by containing an attacker within the unprivileged process.<br>• Set MaxAuthTries to 2, to limit the maximum number of authentication attempts permitted per connection. The default is 6.<br>• Set Compression to No to disable compression.<br>• Set TCPKeepAlive to No to ensure that messages are sent on an encrypted channel.<br>• Set X11Forwarding to No to disable remote display forwarding.<br>• Set AllowTcpForwarding to No to prevent all TCP forwarding.<br>After you make these modifications, the SSH service restarts, and all other users are disconnected from the SSH shell. |
| Passwords for shell users | Secure mode enforces the following rules to harden the password scheme for shell users:<br>• Dictionary passwords are not allowed.<br>• When a user changes passwords, the last 10 passwords are not allowed.<br>• Passwords generated by non-admin users expire every 30 days.<br>• After a user resets a password, they cannot reset it for 24 hours.<br>• All system accounts cannot log in using SSH.<br>• Password length must be 8 characters, and the password must contain at least one uppercase letter, one special character, and one number.<br>• A new password cannot match the old password. |
| USB storage | Restart the VOS device to blacklist the USB storage. |

| Component | Protection |
|---|---|
| Accounting | Use the AcctOn option to enable process accounting. |
| System performance monitoring | Issue the **sysstat** command to enable system performance monitoring. |
| Binary files | Non-admin users cannot execute binary files. Admin users can execute the following executables only through sudo access: nmap, netcar, nc. curl, ftp, gcc, perl, telnet, netcat, python, and wget. |
| Banner file | Permission to edit this file is restricted. |
| Job scheduling | Job scheduling is disabled. |
| Shadow group | Users are removed from the shadow group. |
| Root login | Logging in as the user "root" is disabled. |

## View Secure-Mode Logs

Secure-mode logs are placed in the following files:

- On a Director node—/var/log/vnms/upstart/versa-appstart.log
- On a VOS device—/var/log/versa/versa-appstart.log

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

Firewall Requirements
Perform Manual Hardening for Versa Analytics
Perform Manual Hardening for Versa Branches, Controllers, and Hubs
Perform Manual Hardening for Versa Director