Linux Server - Install RedHat 9 SSH configuration

> Last verified: October 2026 against Red Hat's RHEL 9 system-wide cryptographic policies guide and the sshd_config manual.

On Red Hat Enterprise Linux 9 (RHEL 9 / Rocky Linux 9 / AlmaLinux 9 etc.), SSH configuration is primarily managed through system-wide crypto policies. Direct settings in /etc/ssh/sshd_config for KexAlgorithms, Ciphers, etc., are often ignored unless you properly override the policy.

1. Recommended: Add Curve25519 (preferred) and Diffie-Hellman group exchange

Curve25519-sha256 (and its @libssh.org variant) is already enabled by default in RHEL 9 and is the modern, secure choice.

diffie-hellman-group-exchange-sha256 is also generally available and reasonably secure.

Create a drop-in config. Red Hat's guidance is to use a two-digit prefix smaller than 50 so the file is read before `50-redhat.conf` (which pulls in the crypto policy). sshd uses the **first** value it reads for each keyword:

```
sudo mkdir -p /etc/ssh/sshd_config.d
sudo tee /etc/ssh/sshd_config.d/49-custom-kex.conf << EOF
# Only offer these KEX algorithms (the client chooses the order)
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512
EOF
```

2. Test the config

```
sudo sshd -t
```

If no errors, reload SSH:

```
sudo systemctl reload sshd
```

3. Temporarily allow legacy algorithms (if needed for old clients/servers)

Legacy algorithms (e.g., SHA-1 based ones like diffie-hellman-group1-sha1 or older group-exchange) are disabled for security.

Best temporary option (least impact):

```
# Append legacy KEX to OpenSSH's built-in default list
sudo tee /etc/ssh/sshd_config.d/48-legacy-kex.conf << EOF
KexAlgorithms +diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
EOF
```

Because 48-legacy-kex.conf is read first, its KexAlgorithms line is used instead of the one in 49-custom-kex.conf while it exists. Test with `sudo sshd -t`, reload sshd, and delete the file when the old clients are gone.

Or use the broader (but riskier) **LEGACY** crypto policy:

```
sudo update-crypto-policies --set LEGACY
sudo reboot
```

Warning: LEGACY weakens many other things system-wide (not just SSH). Revert with `sudo update-crypto-policies --set DEFAULT` and reboot when done. Red Hat recommends a reboot after changing the policy so every service picks it up.

Verification commands

```
# Available KEX algorithms
ssh -Q kex

# Effective configuration used by sshd
sudo sshd -T | grep -E '^(kexalgorithms|ciphers|macs)'
```

```
# Test connection
ssh -v user@yourserver
```

Notes for your homelab / self-hosted setup

- Prefer **drop-in files** under /etc/ssh/sshd_config.d/ (numbered < 50, for example 49-*.conf, so they are read before Red Hat's 50-redhat.conf; the first value read wins).
- After any change: sshd -t → systemctl reload sshd.
- If you have specific old clients (e.g., very old Windows, network devices, or RHEL 6-era), the + syntax to append is safest.

Sources

- https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/security_hardening/using-the-system-wide-cryptographic-policies_security-hardening
- https://man.openbsd.org/sshd_config

Revision #1
Created 21 July 2026 11:32:29 by Admin
Updated 24 October 2026 14:10:46 by Admin