

Linux Server - Install RedHat 9 SSH configuration

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 (best practice — it takes precedence correctly):

Bash

```
sudo mkdir -p /etc/ssh/sshd_config.d
sudo tee /etc/ssh/sshd_config.d/50-custom-kex.conf << EOF
# Prioritize strong modern KEX (append to defaults with + if needed)
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

Bash

```
sudo sshd -t
```

If no errors, reload SSH:

Bash

```
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):

Bash

```
# Append legacy KEX to the defaults
sudo tee /etc/ssh/sshd_config.d/49-legacy-kex.conf << EOF
KexAlgorithms +diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
EOF
```

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

Bash

```
sudo update-crypto-policies --set LEGACY
sudo systemctl restart sshd
```

Warning: LEGACY weakens many other things system-wide (not just SSH). Revert with DEFAULT when done.

Verification commands

Bash

```
# 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` to override Red Hat's `50-redhat.conf`).
- 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.

Revision #1

Created 21 July 2026 11:32:29 by Steve Ling

Updated 21 July 2026 11:35:38 by Steve Ling