DUXNET

Best Practice Guide to Firmware & Configuration

Taming the firmware jungle with best practice basics.

Config Chaos? Not on Our Watch!



WHY FIRMWARE AND CONFIGURATION UPDATES MATTER

Correct firmware management and configuration practices are essential to long-term network performance, especially in environments where uptime, stability, and remote access are critical. Poor planning or neglecting firmware routines can result in avoidable downtime, device failure, or inconsistent behaviour across sites.

This guide outlines the key best practices for ensuring smooth firmware updates and consistent, secure configuration management on your DuxNet devices and other network hardware.

COMMON MISTAKES TO AVOID

Installers and integrators often overlook these small details with potentially disastrous consequences:

- **Forgetting to back up config before firmware upgrades:** One wrong click and you're rebuilding from scratch.
- **Using outdated firmware "because it still works.":** Older versions often contain known vulnerabilities and performance bugs.
- **Deploying without testing:** Don't assume a config file that worked last year will work post-upgrade.
- **Leaving remote admin enabled on public IPs:** This opens the door to attacks. Always secure your interfaces.
- **Copy-pasting from forums or customer sites:** Every network has unique requirements. Generic configs are risky.

BEST PRACTICE CHECKLIST

- **Always update to the latest stable firmware before deployment:** Outdated firmware can contain known bugs or vulnerabilities. Apply updates in a controlled test environment first.
- **Download firmware only from official, verified sources:** Avoid using firmware from third-party or unofficial sites, even for older devices.
- **Use long-term support (LTS) firmware where possible:** LTS firmware versions prioritise stability and support for enterprise and ISP environments.
- **Create full configuration backups after setup and before any firmware change:** Store with clear filenames, dates, and device info for quick rollback if needed.
- **Standardise your configuration templates:** Using consistent base configs across sites reduces troubleshooting time and human error.
- **Never copy/paste old config files without verifying compatibility:** New firmware may deprecate features or change syntax, always double-check.
- **Test critical changes in a lab environment first:** Especially for VLANs, QoS, routing, or complex bridging.
- **Secure your configuration and firmware interfaces:** Disable remote admin where unnecessary, avoid default ports, and enforce strong passwords.
- **Document any customisation clearly:** Where supported, use comments in config files and maintain internal change logs.
- **Plan and document your rollback procedure:** If a firmware update fails or causes issues, a rollback path with prior config is essential.

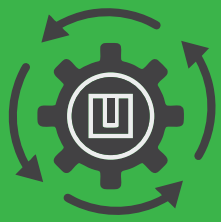
FIRMWARE GOLDEN RULES

- **Test before you trust:** Always trial firmware and config changes in a lab environment first.
- **Backup everything:** Save current config files, firmware versions, and restore points before making any changes.
- **Use only official sources:** Never download firmware from third-party or “mirrored” sites.
- **Standardise where possible:** Use known-good templates to reduce risk and support calls.
- **Document as you go:** Good notes today = faster fixes tomorrow.

DUXNET

Installer Firmware and Configuration Checklist

Best Practices for Firmware and Configuration Updates



BEFORE YOU BEGIN

- [ ] Confirm latest stable or long-term support (LTS) firmware is available for the device
- [ ] Download firmware only from the official vendor site
- [ ] Check compatibility with existing configuration files
- [ ] Label and safely store the current configuration backup (with date/version/device name)
- [ ] Review changelog or release notes for known issues or major changes
- [ ] If this is a remote site: confirm stable electricity and data connection

LAB/TEST PREP

- [ ] Test firmware upgrade in a lab or demo unit before field install
- [ ] Load the planned configuration and confirm no errors or warnings
- [ ] Validate that services (e.g., routing, VLANs, VPN) start up correctly
- [ ] Test failover, reboot, and recovery scenarios if relevant
- [ ] Document working settings for future rollout/reference

DURING DEPLOYMENT

- [ ] Upgrade firmware only when site conditions are stable (no load shedding or line cuts expected)
- [ ] Apply configuration from verified template or tested backup
- [ ] Check system logs for warnings, errors, or rejected settings
- [ ] Disable unused services and interfaces
- [ ] Change all default passwords and disable remote admin access unless secured
- [ ] Set up NTP (time sync) for accurate log and certificate management

POST-INSTALL AND SUPPORT

- [ ] Reboot device and confirm persistent config and full service availability
- [ ] Export current config and firmware version to support folder
- [ ] Label file: SITE_DEVICE_DATE.cfg and store with version number
- [ ] Record all changes in customer or internal handover documentation
- [ ] If using multiple devices, update asset register with new firmware and config status

OPTIONAL (BUT RECOMMENDED)

- [ ] Create a rollback plan: store previous firmware and config locally or in cloud
- [ ] Snapshot key screenshots (interfaces, firewall, VLANs) for quick support reference
- [ ] Submit config template to team repo if custom-built or site-specific