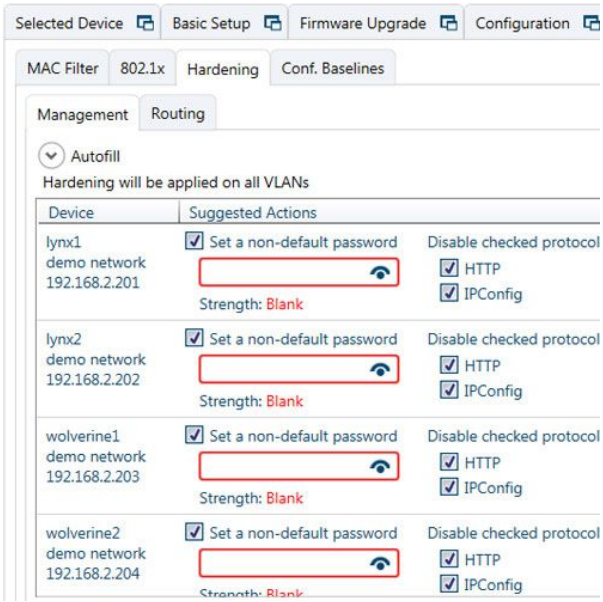
Cybersecurity configurations made easy using WeConfig

For a long time, infrastructural and industrial applications have been relatively unaffected by cyber-attacks but that is changing. Cyber threats are increasing globally and many attacks have been specifically directed towards industrial applications. Westermo will always recommend that proper network security is applied in any infrastructure and industrial data communication network. WeConfig has been developed to make it easy to achieve a good protection against cyber-attacks. WeConfig can perform a security analysis and suggest changes and system wide security configuration can be applied quick and simple.
Features:

- Deploy MAC filters system wide
- Change passwords system wide and password strength analyser
- Analyse switch attach surface (Switch Hardening)
- System wide 802.1x configuration
- Threat detection (compare configuration file with baseline)
- CPU bandwidth limits
- Per port bandwidth limits
- Disable unused ports
- Password protection of project files
- Deploy MD5 signature to dynamic router protocol
- Set port up/down traps

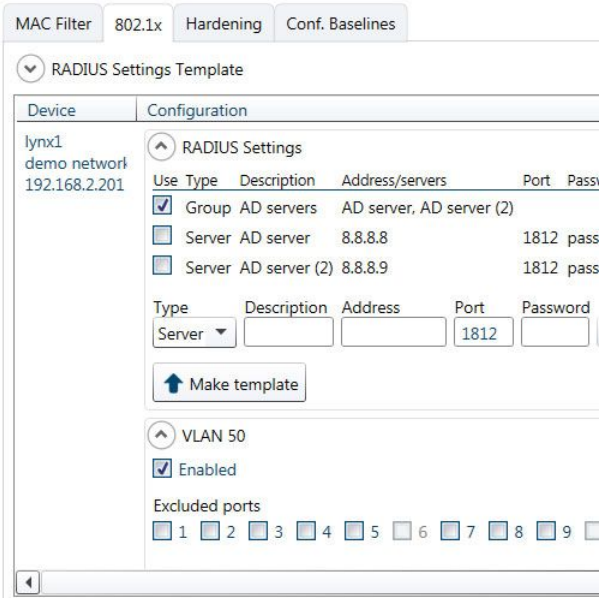
One-click network scan



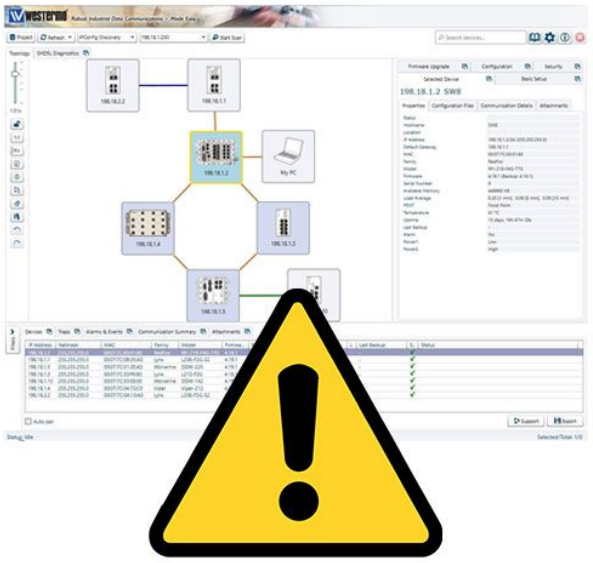
WeConfig can reach out to all switches in a network and scan for and find vulnerabilities. Simple things such as not changing the switch default password or using unsafe protocols can be a risk. WeConfig security scan will highlight vulnerabilities and suggest a solution. You can automatically deploy system wide security configuration quick and easy.

WeConfig will guide you to a secure system

Lack of time and knowledge are common reasons for ignoring unsecure network configuration and potential risks. However, WeConfig can make system wide configuration for increased security quick and easy. No WeConfig user have to refrain from secure configuration because of time or knowledge restrictions.



Automatically see if configuration has changed



WeConfig offers a configuration baseline feature which creates alerts if changes have been made to network settings. Detecting the changes is the first step in intrusion detection and preventing a full assault on the network. The changes can be small, such as a change in a firewall rule, an added port to a VLAN or an opened insecure configuration protocol. No unauthorized change will escape WeConfig.