

Cyber NAC

Network Access Control



Centrally manage network security policies:

Your top security experts can set, monitor and enforce access policies.

Cross-platform:

NAC Compliance Director handles the transition to each device, making it ideal for networks using multiple makes of routers; operators do not need to learn intricate and widely varying device architectures for every make of router in use.

Set network policies quickly and easily:

Even with hundreds or thousands of network devices, each with its own security policy, you can minimize security vulnerability and manage risks through efficient, centralized ACL management.

Revision control:

History and rollback features let you quickly return to a functional configuration in case a mistake is made.

Fine-tune your network access policies:

NAC Compliance Director enables you to set specific, granular policies for which networks and people have access to network resources for optimal network security.

Easy to use:

The intuitive interface is designed to minimize mistakes, resulting in less downtime and less time spent on troubleshooting.

Find network problems quickly:

Troubleshooting features help operators identify problems quickly, fewer technician hours used and less overall downtime.

Supported Devices

- Cisco (IOS) Routers
- Juniper Routers
- Cisco Catalyst Switches
- Cisco PIX
- Cisco ASA
- Netscreen Firewalls
- Force 10 Routers
- Aruba Mobility Controllers
- iptables and ip6tables

