

Shavlik NetChk Configure is a configuration management solution that audits and enforces security settings on your network.

Shavlik NetChk Configure simplifies and automates the critical to perform tasks of managing configuration settings and compliance auditing. It enables you to keep up with changes brought by dynamic networks, meet your compliance objectives, lower your costs, and reduce your risk of exposure.



Fastest Time to Value:

"We no longer have to pull operational resources to gather data for upcoming audits. Shavlik's solution has provided us with push-button audit preparation."

Director of Information Security, Global E-Commerce Solutions Provider

Simplify and Automate Configuration Management and Compliance Auditing

When you implement NetChk Configure, in hours, not days or weeks, your IT organization will BE READY...

For your next audit, in hours, not days or weeks

- ▶ Reduce Spend - time, money and IT staff while improving the level of security and conformance with internal policies and external regulations
- ▶ Increase visibility and control over configuration changes providing measurable proof of effectiveness
- ▶ Centralized management frees up critical IT staff

To better leverage existing systems management platforms

- ▶ Easily access those hard to manage systems through agentless technology and close their security gaps
- ▶ Validate that policy settings, distributed through GPO or other, were actually implemented
- ▶ Clear and direct mapping of configuration settings to internal policy or regulatory frameworks

To regain control of your configurations

- ▶ Establishes a configuration baseline and then proactively enforces that policy through continuous assessment of security and configuration controls
- ▶ Simplifies and automates security and IT operations to improve speed, accuracy, and productivity, lower costs, and support higher scale
- ▶ Develops a sustainable configuration management program through the streamlining of management, audit, and reporting processes

Shavlik Security Suite



Shavlik NetChk Configure is a vital component of the Shavlik Security Suite.

Shavlik NetChk Configure

Easy to configure and manage:

- ▶ Get up and running in 30 minutes or less
- ▶ Industry standard interface – takes the complexity out of managing configuration settings
- ▶ Fastest direct route to policy conformance and regulatory compliance
- ▶ Operationalize security/free up IT staff

Accurate and reliable scanning technology that enforces corporate security policies:

- ▶ Automated policy baseline development and enforcement
- ▶ Complements and supports GPO, validating network wide that settings were truly enforced
- ▶ Security auditing based on ISO 27702 and NIST 800-53 security controls
- ▶ One of only a few SCAP-validated products that simplifies and automates both assessment and remediation
- ▶ Straightforward and direct mapping of configuration settings to mandates and industry initiatives such as FDCC or PCI

Highly Flexible Architecture:

- ▶ Fully automate scanning and remediation for hands - off operation
- ▶ Agentless technology ensures seamless integration/ deployment and network-wide discovery
- ▶ Fine grained control over remediation including Change Management

Audit Ready Reporting:

- ▶ Reports are available daily, weekly, and monthly on the latest threats and vulnerabilities
- ▶ Reports directly indicate the degree of compliance with standards and policies
- ▶ Through on-going, real-time management, reports are generated to provide auditors proof of compliance

“Clear Return on Investment due to ease of administration, right out of the box! With other products we would have required at least one additional full time Systems Administrator.”

Desktop Manager, Global Hotel Group

The screenshot shows the 'Procedure' tab in the software. It displays a table of required password policy elements:

Policy	Required Setting
1. Enforce password history	6 passwords remembered
2. Maximum password age	60 days
3. Minimum password age	2 days
4. Minimum password length	7 characters
5. Passwords must meet complexity requirements	Enabled
6. Store password using reversible encryption for all users in the domain	Disabled

Apply and enforce configuration policies.

The screenshot shows the 'Scan Executive Summary' report. It includes a pie chart for 'Scan Summary Compliance' and a table for 'Top Ten Non Compliant Security Settings'.

Scan Summary Compliance:

Compliant/Non Compliant	Ratio	Percentage
Compliant Settings	678 of 1031	65.76%
NonCompliant Settings	353 of 1031	34.24%

Top Ten Non Compliant Security Settings:

Security Setting	Count
Domain Member: Require Strong (Windows 2000 or Later) Session Key	10
Devices: Unsigned Driver Installation Behavior	9
Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always)	9
Domain Member: Disable Machine Account Password Changes	8
Microsoft Network Client: Digitally Sign Communications (Always)	8
Network Security: LAN Manager Authentication Level	8
Interactive Logon: Smart Card Removal Behavior	7
Recovery Console: Allow Automatic Administrative Logon	7
Interactive Logon: Message Text for Users Attempting to Log On	7
Network Security: LAN Manager Authentication Level	7

Executive reporting allows immediate understanding of real-time compliance status.