

SECURITY CONFIGURATION MANAGER

IT-Service Walter

Jörn Walter
www.it-service-walter.com
31.10.2025

SECURITY CONFIGURATION MANAGER

ÜBERBLICK

DER **SECURITY CONFIGURATION MANAGER V6.5** IST EIN PROFESSIONELLES WERKZEUG ZUR AUTOMATISIERTEN PRÜFUNG UND OPTIMIERUNG VON WINDOWS-SICHERHEITSEINSTELLUNGEN NACH INTERNATIONAL ANERKANNTEN STANDARDS:

- **BSI GRUNDSCHUTZ** (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK)
- **NIST CYBERSECURITY FRAMEWORK** (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY)

Security Configuration Manager v6.5

Benutzerhandbuch & Dokumentation

Inhaltsverzeichnis

1. Überblick
2. Installation & Systemanforderungen
3. Hauptfunktionen
4. Vorteile der toolbasierten Sicherheitsverwaltung
5. Bedienungsanleitung
6. Best Practices
7. Technische Details
8. Fehlerbehebung
9. FAQ

Kernziele

Compliance-Prüfung: Automatisierte Überprüfung von hunderten Sicherheitseinstellungen innerhalb und außerhalb einer Domäne.

[Speziell für gemietete Online-Server, Terminal-Server oder Umgebungen ohne administrative Erfahrungen.](#)

Hardening: Sichere Konfiguration nach Best Practices

Dokumentation: Detaillierte Reports und Audit-Trails

Effizienz: Stunden manuelle Arbeit in Minuten erledigen

Remote-Verwaltung: Zentrale Verwaltung mehrerer Server

Installation & Systemanforderungen

Systemanforderungen

Minimum:

- Windows 10/11 oder Windows Server 2016+
- .NET Framework 4.8 oder höher
- 50 MB freier Festplattenspeicher
- Administrator-Rechte

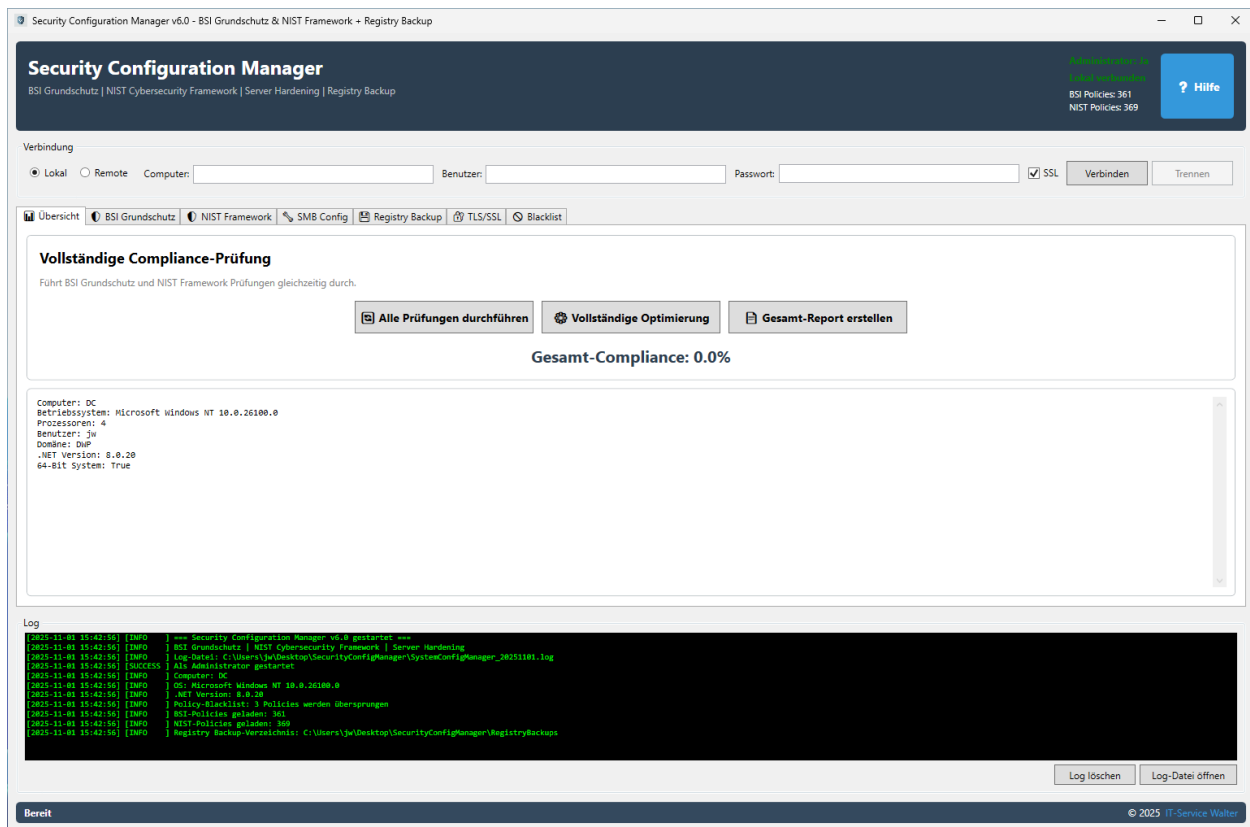
Empfohlen:

- Windows 11 oder Windows Server 2022
- .NET 8.0 oder höher
- 4 GB RAM

Installation

1. **Entpacken** Sie das Archiv in ein Verzeichnis Ihrer Wahl
2. **Starten** Sie SystemConfigManager.exe
3. **Bestätigen** Sie die UAC-Abfrage (Administrator erforderlich)
4. Das Tool erstellt automatisch:
 - Log-Dateien im Unterordner Logs\
 - Registry-Backups im Unterordner RegistryBackups\
 - Policy-Blacklist als PolicyBlacklist.json

Hauptfunktionen



1. BSI Grundschatz Compliance

Was wird geprüft?

Der BSI-Grundschatz ist der deutsche Standard für IT-Sicherheit. Das Tool prüft **über 360 Sicherheitseinstellungen** in folgenden Kategorien:

Netzwerksicherheit

- Router Discovery Deaktivierung
- TCP/IP Stack Härtung
- NetBIOS-Sicherheit
- LMHOSTS-Konfiguration
- Multicast-DNS Einstellungen

Anti-Malware & Defender

- Potentially Unwanted Applications (PUA) Schutz
- Controlled Folder Access
- Real-Time Protection
- Cloud-Based Protection
- Automatische Sample-Übermittlung
- Script-Scanning

Firewall & Logging

- Windows Defender Firewall
- Protokollierung von verworfenen Paketen
- Syslog-Integration
- Event-Log-Größen

Authentifizierung

- Credential Guard
- LSA Protection
- Token Leak Detection
- NTLM-Einschränkungen
- Kerberos-Härtung

Dienste & Features

- Windows Sandbox
- Plattform-Virtualisierung
- SMB-Verschlüsselung
- Remote Desktop Security

Und viele weitere...

Wie funktioniert die Prüfung?

1. Klick auf "BSI Prüfen"
2. Tool liest alle relevanten Registry-Werte
3. Vergleich mit BSI-Empfehlungen
4. Anzeige der Ergebnisse in übersichtlicher Tabelle
5. Farbcodierung:  Grün = Konform,  Rot = Nicht konform

Security Configuration Manager v6.0 - BSI Grundschutz & NIST Framework - Registry Backup

Security Configuration Manager
BSI Grundschutz | NIST Cybersecurity Framework | Server Hardening | Registry Backup

BSI Policies: 361
NIST Policies: 369

Hilfe

Verbindung
☐ Lokal ☒ Remote Computer: ms1.windowsscp.de Benutzer: Passwort: ☐ SSL Verbinden Trennen

Übersicht BSI Grundschutz NIST Framework SMB Config Registry Backup TLS/SSL Blacklist

BSI Grundschutz Compliance
BSI: 10.2% Konform

Prüfen Optimieren Report

Status	Severity	Kategorie	Policy	Aktuell	Empfohlen
OK	CRITICAL	Attack Surface Reduction	ASR: Block Win32 API calls from Office macros	NULL	1
	CRITICAL	Benutzerkontrolle	UAC aktiviert	1	1
	CRITICAL	Authentifizierung	Klartext-Passwörter verhindern	NULL	0
	CRITICAL	CPU Security	Spectre/Meltdown Mitigations	NULL	72
	CRITICAL	CPU Security	Spectre/Meltdown Mask	NULL	3
	CRITICAL	Services	SMB1 Protocol Disabled	NULL	4
	CRITICAL	Exploit Protection	Kernel Mitigation Options	NULL	0xffffffffffffff
	CRITICAL	Boot Security	Secure Boot Status	NULL	1
	CRITICAL	Data Encryption	BitLocker Verschlüsselung erzwingen	NULL	1
	CRITICAL	Authentifizierung	Minimale Passwort-Länge	NULL	14
	CRITICAL	Credential Protection	Credential Guard Konfiguration	NULL	1

Gesamt: 361
Konform: 37
Nicht konform: 324

Log

```
[2025-11-01 10:01:00] [INFO] Reading remote registry value: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CloudContent\DisableWindowsConsumerFeatures
[2025-11-01 10:01:00] [INFO] + Current: NULL | Expected: 1
[2025-11-01 10:01:00] [INFO] [360/361] Checking: Disable Cloud Optimized Content
[2025-11-01 10:01:00] [INFO] Reading remote registry value: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CloudContent\DisableCloudOptimizedContent
[2025-11-01 10:01:00] [INFO] + Current: NULL | Expected: 1
[2025-11-01 10:01:00] [INFO] [361/361] Checking: Disable Soft Landing
[2025-11-01 10:01:00] [INFO] Reading remote registry value: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CloudContent\DisableSoftLanding
[2025-11-01 10:01:00] [INFO] + Current: NULL | Expected: 1
[2025-11-01 10:01:00] [INFO] BSI Compliance check completed: 37/361 compliant
[2025-11-01 10:01:00] [INFO] BSI-Prüfung abgeschlossen: 10 Policies
[2025-11-01 10:01:00] [INFO] ✓ Automatisch nach Kategorie sortiert
[2025-11-01 10:01:00] [SUCCESS] BSI-Prüfung abgeschlossen: 10.2% konform
```

Log löschen Log-Datei öffnen

BSI-Prüfung abgeschlossen © 2025 IT-Service Walter

Optimierung durchführen

1. Klick auf "BSI Optimieren"
2. Tool wendet empfohlene Einstellungen an
3. Batch-Verarbeitung (10 Policies pro Batch, 500ms Pause)
4. Detailliertes Logging aller Änderungen
5. Erfolgsstatistik am Ende

Severity-Level:

- **CRITICAL:** Muss unbedingt umgesetzt werden
- **HIGH:** Sehr wichtig für Sicherheit
- **MEDIUM:** Empfohlen (optional inkludierbar)

Security Configuration Manager v6.0 - BSI Grundschatz & NIST Framework - Registry Backup

Security Configuration Manager
BSI Grundschatz | NIST Cybersecurity Framework | Server Hardening | Registry Backup

Verbindung
☐ Lokal ☒ Remote Computer: ms1.windowspapst.de Benutzer: Passwort: ☒ SSL

Übersicht | **BSI Grundschatz** | NIST Framework | SMB Config | Registry Backup | TLS/SSL | Blacklist

BSI Grundschatz Compliance
BSI: 90.0% Konform

Status	Severity	Kategorie	Policy	Aktuell	Empfohlen
OK	CRITICAL	Attack Surface Reduction	ASR: Block Office from creating child processes	1	1
OK	HIGH	Attack Surface Reduction	ASR: Block executable content from email	1	1
OK	CRITICAL	Audit	NTLM Traffic Audit	2	2
OK	HIGH	Audit	Security Log Maximum Size	1073741824	1073741824
OK	MEDIUM	Audit	Process Creation mit Command Line	1	1
OK	HIGH	Audit	Audit Object Access	1	1
OK	MEDIUM	Audit	System Log Maximum Size	536870912	536870912
OK	HIGH	Audit	Audit Policy Change	1	1
OK	MEDIUM	Audit	Application Log Maximum Size	536870912	536870912
OK	HIGH	Audit	Security Log Retention	0	0
OK	HIGH	Audit	Audit System Events	1	1

Gesamt: 361
Konform: 325
Nicht konform: 36

Log

```
[2025-11-05 16:06:22] [INFO] Reading remote registry value: HKLM:\SOFTWARE\Policies\Microsoft\Windows\CloudContent\DisableWindowsConsumerFeatures
[2025-11-05 16:06:22] [INFO] + Current: 1 | Expected: 1
[2025-11-05 16:06:22] [INFO] [360/361] Checking: Disable Cloud Optimized Content
[2025-11-05 16:06:22] [INFO] Reading remote registry value: HKLM:\SOFTWARE\Policies\Microsoft\Windows\CloudContent\DisableCloudOptimizedContent
[2025-11-05 16:06:22] [INFO] + Current: 1 | Expected: 1
[2025-11-05 16:06:22] [INFO] [361/361] Checking: Disable Soft Landing
[2025-11-05 16:06:22] [INFO] Reading remote registry value: HKLM:\SOFTWARE\Policies\Microsoft\Windows\CloudContent\DisableSoftLanding
[2025-11-05 16:06:22] [INFO] + Current: NULL | Expected: 1
[2025-11-05 16:06:22] [INFO] BSI Compliance check completed: 325/361 compliant
[2025-11-05 16:06:22] [INFO] BSI-Prüfung abgeschlossen: 361 Policies
[2025-11-05 16:06:22] [INFO] ✓ Automatisch nach Policy-Gründung sortiert
[2025-11-05 16:06:23] [SUCCESS] BSI-Prüfung abgeschlossen: 90,0% konform
```

BSI-Prüfung abgeschlossen © 2025 IT-Service Walker

2. NIST Cybersecurity Framework

Was wird geprüft?

Das NIST Framework ist der US-amerikanische Standard für Cybersecurity. Das Tool prüft **über 360 Controls** in Kategorien:

The screenshot displays the Security Configuration Manager v6.0 interface. The main window shows the NIST Cybersecurity Framework assessment results. The top bar indicates the current status: "NIST Cybersecurity Framework" with a progress bar showing 7.9% compliance. Below this, a table lists the controls and their status. The table has columns for Status, Severity, Framework, Control, Aktuell, and Empfohlen. The controls are grouped by severity: MEDIUM, HIGH, and OK. The bottom section shows the log of the assessment process, including the completion of the NIST Framework assessment.

Status	Severity	Framework	Control	Aktuell	Empfohlen
	MEDIUM	Audit and Accountability	Geschützte Ereignisprotokollierung	NULL	1
	MEDIUM	Audit and Accountability	Firewall Logging Public	NULL	1
	HIGH	Audit Content	Anmeldeereignisse protokollieren	NULL	3
	MEDIUM	Audit Content	Objektzugriff protokollieren	NULL	3
	MEDIUM	Audit Content	Prozessverfolgung protokollieren	NULL	3
OK	MEDIUM	Audit Failure Response	Security Log Aufbewahrung	0	0
OK	LOW	Audit Failure Response	Bei Audit-Fehler System anhalten	0	0
	HIGH	Audit Generation	Richtlinienänderungen protokollieren	NULL	3
	HIGH	Audit Generation	Kontenverwaltung protokollieren	NULL	3
	MEDIUM	Audit Generation	Verwendung von Berechtigungen protokollieren	NULL	3
	HIGH	Audit Generation	Systemereignisse protokollieren	NULL	3

Gesamt: 369
Konforme: 29
Nicht konform: 340

Log

```
[2025-11-03 10:00:00] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows\System\SmartScreenEnabled
[2025-11-03 10:00:00] [INFO] - Current: NULL, Expected: 1
[2025-11-03 10:00:00] [INFO] [369/369] Checking: SmartScreen Integration
[2025-11-03 10:00:00] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen\EnableSmartScreenInShell
[2025-11-03 10:00:00] [INFO] - Current: NULL, Expected: 1
[2025-11-03 10:00:00] [INFO] [369/369] Checking: Windows Defender SmartScreen
[2025-11-03 10:00:00] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen\ConfigureWindowsDefenderSmartScreen
[2025-11-03 10:00:00] [INFO] - Current: NULL, Expected: 1
[2025-11-03 10:00:00] [INFO] NIST Compliance Check Completed: 29/369 compliant
[2025-11-03 10:00:00] [INFO] NIST-Prüfung abgeschlossen: 369 Policies
[2025-11-03 10:00:00] [INFO] ✓ Automatisch nach Kategorie sortiert
[2025-11-03 10:00:00] [SUCCESS] NIST-Prüfung abgeschlossen: 7,9% konform
```

Log löschen Log-Datei öffnen

NIST-Prüfung abgeschlossen © 2025 IT-Service Walter

Privacy & Datenschutz

- Sample-Übermittlung an Microsoft
- Telemetrie-Einstellungen
- Fehlerberichterstattung
- Diagnosedaten

Update Management

- Windows Update Konfiguration
- Feature Update Deferrals
- Quality Update Deferrals
- Branch Readiness Level

USB & Wechselmedien

- Removable Storage Security
- USB-Gerätezugriff
- AutoRun/AutoPlay

SMB Security

- SMB1 Protokoll Deaktivierung
- SMB Signing
- SMB Verschlüsselung

DNS Security

- DNS over HTTPS (DoH)
- DNS Client Konfiguration

Data Protection

- BitLocker-Einstellungen
- EFS-Konfiguration

Attack Surface Reduction

- ASR Rules
- Exploit Protection
- Network Protection

Optimierung durchführen

Analog zur BSI-Optimierung, mit NIST-spezifischen Controls.

Security Configuration Manager v6.0 - BSI Grundsatz & NIST Framework - Registry Backup

Security Configuration Manager

BSI Grundsatz | NIST Cybersecurity Framework | Server Hardening | Registry Backup

Administration - IT
Benutzername: Administrator (NT AUTHORITY\SYSTEM)
BSI Policies: 361
NIST Policies: 369

Hilfe

Verbindung

☐ Lokal

☒ Remote

Computer: ms1.windowsapst.de

Benutzer: jw

Passwort: *****

☒ SSL

Verbinden

Trennen

Übersicht | BSI Grundsatz | NIST Framework | SMB Config | Registry Backup | TLS/SSL | Blacklist

NIST Cybersecurity Framework

NIST: 91.1% Konform

Prüfen

Optimieren

Report

Status	Severity	Framework	Control	Aktuell	Empfohlen
OK	MEDIUM	Audit and Accountability	Geschützte Ereignisprotokollierung	1	1
OK	MEDIUM	Audit and Accountability	Firewall Logging Public	1	1
OK	HIGH	Audit Content	Anmeldeereignisse protokollieren	3	3
OK	MEDIUM	Audit Content	Objektzugriff protokollieren	3	3
OK	MEDIUM	Audit Content	Prozessverfolgung protokollieren	3	3
OK	MEDIUM	Audit Failure Response	Security Log Aufbewahrung	0	0
OK	LOW	Audit Failure Response	Bei Audit-Fehler System anhalten	0	0
OK	HIGH	Audit Generation	Richtlinienänderungen protokollieren	3	3
OK	HIGH	Audit Generation	Kontenveränderungen protokollieren	3	3
OK	MEDIUM	Audit Generation	Verwendung von Berechtigungen protokollieren	3	3
OK	HIGH	Audit Generation	Systemereignisse protokollieren	3	3

Gesamt: 369

Konform: 336

Nicht konform: 33

Log

[2025-11-01 16:15:41] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows\System\SmartScreen\Enabled

[2025-11-01 16:15:41] [INFO] => Current: 1 | Expected: 1

[2025-11-01 16:15:41] [INFO] [369/369] Checking: SmartScreen Integration

[2025-11-01 16:15:41] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen\EnabledSmartScreenInShell

[2025-11-01 16:15:41] [INFO] => Current: 1 | Expected: 1

[2025-11-01 16:15:41] [INFO] [369/369] Checking: Windows Defender SmartScreen

[2025-11-01 16:15:41] [INFO] Reading remote registry value: HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen\ConfigureWindowsDefenderSmartScreen

[2025-11-01 16:15:41] [INFO] => Current: 1 | Expected: 1

[2025-11-01 16:15:41] [INFO] NIST Compliance Check completed: 336/369 compliant

[2025-11-01 16:15:41] [INFO] NIST-Prüfung abgeschlossen: 369 Policies

[2025-11-01 16:15:41] [INFO] ✓ Automatisch nach Kategorie sortiert

[2025-11-01 16:15:41] [SUCCESS] NIST-Prüfung abgeschlossen: 91.1% konform

Log löschen

Log-Datei öffnen

NIST-Prüfung abgeschlossen

© 2025 IT-Service Walter

3. SMB (Server Message Block) Konfiguration

Was ist SMB?

SMB ist das Protokoll für Windows-Dateifreigaben und Netzwerkkommunikation.

SMB Server Konfiguration
SMB1/2/3 Protokoll, Verschlüsselung, Signing und Dateisystem

LadenAnwendenOptimieren

SMB Protokoll-Einstellungen

☐ SMB1 Protokoll aktivieren (UNSICHER - nicht empfohlen!)
⚠ SMB1 ist veraltet und unsicher. Sollte deaktiviert bleiben!

SMB Verschlüsselung

☐ SMB3 Datenverschlüsselung erzwingen
✅ Empfohlen: Verschlüsselt alle SMB3-Verbindungen

☐ Unverschlüsselte Zugriffe ablehnen
✅ Empfohlen: Blockiert alle unverschlüsselten SMB-Verbindungen

SMB Signing (Message Signing)

☐ SMB Signing erzwingen (Required)
✅ Empfohlen: Verhindert Man-in-the-Middle Angriffe

☐ SMB Signing aktivieren (Enabled)
✅ Empfohlen: Aktiviert SMB Signing-Unterstützung

Dateisystem-Einstellungen

☐ Lange Pfade aktivieren (über 260 Zeichen)
✅ Empfohlen: Ermöglicht Dateipfade > 260 Zeichen (Windows 10+)

(i) Empfohlene Sicherheits-Konfiguration:

- SMB1: Deaktiviert (unsicheres Protokoll)
- SMB3 Verschlüsselung: Aktiviert
- Unverschlüsselte Zugriffe: Blockiert
- SMB Signing: Erzwingen (Required + Enabled)
- Lange Pfade: Aktiviert

⚠ WICHTIG: Nach Änderungen ist ein Neustart des SMB-Dienstes oder des Servers erforderlich!

Konfigurierbare Einstellungen

Einstellung	Beschreibung	Empfehlung
SMB1 Protokoll	Veraltetes, unsicheres Protokoll	❌ Deaktiviert
SMB3 Verschlüsselung	Ende-zu-Ende-Verschlüsselung	✅ Aktiviert
SMB Signing	Digitale Signaturen	✅ Erzwingen
Unverschlüsselte Zugriffe blockieren	Nur verschlüsselte Verbindungen	✅ Aktiviert
Long Paths	Pfade >260 Zeichen	✅ Aktiviert

Bedienung

Tab "SMB-Konfiguration"

→ "Aktualisieren" = Aktuelle Einstellungen lesen

→ Checkboxen anpassen

→ "Anwenden" = Einstellungen speichern

→ "Optimieren" = Sichere Standardkonfiguration

The screenshot shows the "SMB Server Konfiguration" web interface. At the top, there's a green header bar with the title "SMB Server Konfiguration" and the subtitle "SMB1/2/3 Protokoll, Verschlüsselung, Signing und Dateisystem". To the right of the header are three buttons: "Laden", "Anwenden", and "Optimieren".

The main content area is divided into several sections:

- SMB Protokoll-Einstellungen:** Contains a checkbox for "SMB1 Protokoll aktivieren (UNSICHER - nicht empfohlen!)" which is currently unchecked. Below it is a red warning icon and text: "SMB1 ist veraltet und unsicher. Sollte deaktiviert bleiben!".
- SMB Verschlüsselung:** Contains two checked checkboxes: "SMB3 Datenverschlüsselung erzwingen" and "Unverschlüsselte Zugriffe ablehnen". Below each checkbox is a green checkmark and text indicating the recommended action: "Empfohlen: Verschlüsselt alle SMB3-Verbindungen" and "Empfohlen: Blockiert alle unverschlüsselten SMB-Verbindungen".
- SMB Signing (Message Signing):** Contains two checked checkboxes: "SMB Signing erzwingen (Required)" and "SMB Signing aktivieren (Enabled)". Below each checkbox is a green checkmark and text indicating the recommended action: "Empfohlen: Verhindert Man-in-the-Middle Angriffe" and "Empfohlen: Aktiviert SMB Signing-Unterstützung".
- Dateisystem-Einstellungen:** Contains one checked checkbox: "Lange Pfade aktivieren (über 260 Zeichen)". Below it is a green checkmark and text indicating the recommended action: "Empfohlen: Ermöglicht Dateipfade > 260 Zeichen (Windows 10+)".

At the bottom, there's a grey box titled "Empfohlene Sicherheits-Konfiguration:" which lists the following settings:

- SMB1: Deaktiviert (unsicheres Protokoll)
- SMB3 Verschlüsselung: Aktiviert
- Unverschlüsselte Zugriffe: Blockiert
- SMB Signings: Erzwingen (Required = Enabled)
- Lange Pfade: Aktiviert

Below this list is a red warning icon and text: "WICHTIG: Nach Änderungen ist ein Neustart des SMB-Dienstes oder des Servers erforderlich!".

4. TLS/SSL Konfiguration

Warum ist TLS/SSL wichtig?

TLS/SSL verschlüsselt die Netzwirkommunikation. Veraltete Protokolle und Cipher haben Sicherheitslücken.

The screenshot shows the 'TLS/SSL & SCHANNEL Konfiguration' window. The title bar is purple with buttons for 'Auslesen', 'Optimieren', and 'Report'. Below the title bar, a status message reads: 'Status: ⚠ Unsicher - Optimierung dringend empfohlen!'. The main content area is titled 'SSL/TLS Protokoll-Status' and lists several protocols with their status and client/server settings.

Protokoll	Status	Client	Server
SSL 2.0	⚠ UNSICHER - Muss deaktiviert sein	Deaktiviert	Deaktiviert
SSL 3.0	⚠ UNSICHER - Muss deaktiviert sein	Deaktiviert	Deaktiviert
TLS 1.0	⚠ VERALTET - Sollte deaktiviert sein	Deaktiviert	Deaktiviert
TLS 1.1	⚠ VERALTET - Sollte deaktiviert sein	Deaktiviert	Deaktiviert
TLS 1.2	✅ SICHER - Sollte aktiviert sein	Deaktiviert	Deaktiviert
TLS 1.3	✅ MODERNSTER STANDARD - Empfohlen!	Deaktiviert	Deaktiviert

Below the table, a section titled 'Empfohlene Protokoll-Konfiguration:' lists the recommended settings:

- SSL 2.0/3.0: DEAKTIVIERT (unsicher)
- TLS 1.0/1.1: DEAKTIVIERT (veraltet)
- TLS 1.2: AKTIVIERT (Standard)
- TLS 1.3: AKTIVIERT (modernster Standard)

Was wird konfiguriert?

Protokolle:

- ❌ SSL 2.0 (unsicher, deaktivieren)
- ❌ SSL 3.0 (unsicher, deaktivieren)
- ❌ TLS 1.0 (veraltet, deaktivieren)
- ❌ TLS 1.1 (veraltet, deaktivieren)
- ✅ TLS 1.2 (aktivieren)
- ✅ TLS 1.3 (aktivieren)

Cipher Suites:

- ☒ AES-128/256 (aktivieren)
- ☐ DES/3DES (deaktivieren)
- ☐ RC4 (deaktivieren)
- ☐ NULL (deaktivieren)

Hash-Algorithmen:

- ☐ MD5 (deaktivieren)
- ☐ SHA-1 (deaktivieren)
- ☒ SHA-256/384/512 (aktivieren)

Cipher Suite Order: Moderne, sichere Cipher Suite Reihenfolge mit Präferenz für:

- ECDHE (Perfect Forward Secrecy)
- AES-GCM (Authenticated Encryption)
- ChaCha20-Poly1305

ECC Curves:

- Curve25519
- NIST P-256/384/521
- Brainpool Curves

Bedienung

Tab "TLS/SSL"

- "Status laden" = Aktuelle Konfiguration anzeigen
- Detaillierter Report mit Sicherheitsbewertung
- "Optimieren" = Sichere TLS 1.3 Konfiguration
- "Report exportieren" = HTML/TXT Report speichern

TLS/SSL & SCHANNEL Konfiguration

Sichere Protokolle, Cipher-Suites und Kryptographie-Einstellungen

Status: ✓ Sicher konfiguriert

Auslesen

Optimieren

Report

Protokolle

Verschlüsselung

Details

SSL/TLS Protokoll-Status

SSL 2.0	⚠ UNSICHER - Muss deaktiviert sein	Client: ☐ Deaktiviert	Server: ☐ Deaktiviert
SSL 3.0	⚠ UNSICHER - Muss deaktiviert sein	Client: ☐ Deaktiviert	Server: ☐ Deaktiviert
TLS 1.0	⚠ VERALTET - Sollte deaktiviert sein	Client: ☐ Deaktiviert	Server: ☐ Deaktiviert
TLS 1.1	⚠ VERALTET - Sollte deaktiviert sein	Client: ☐ Deaktiviert	Server: ☐ Deaktiviert
TLS 1.2	☑ SICHER - Sollte aktiviert sein	Client: ✓ Aktiviert	Server: ✓ Aktiviert
TLS 1.3	☑ MODERNSTER STANDARD - Empfohlen!	Client: ✓ Aktiviert	Server: ✓ Aktiviert

📋 Empfohlene Protokoll-Konfiguration:

- SSL 2.0/3.0: DEAKTIVIERT (unsicher)
- TLS 1.0/1.1: DEAKTIVIERT (veraltet)
- TLS 1.2: AKTIVIERT (Standard)
- TLS 1.3: AKTIVIERT (modernster Standard)

⚠ **WICHTIG:** Nach TLS-Optimierung ist ein **Neustart erforderlich!**

5. Registry Backup & Recovery

Warum Backups?

Registry-Änderungen können System-Funktionalität beeinträchtigen. Backups ermöglichen Wiederherstellung.

Backup erstellen

Beschreibung (optional):

vor der TLS Optimierung

Backup erstellen

[i] Backup-Informationen:

- Sichert alle wichtigen Registry-Bereiche
- Sicherheits-Einstellungen (LSA, SCHANNEL)
- Netzwerk-Konfiguration (SMB, WinRM)
- Windows Update & Defender
- Firewall & Event Log
- Remote Desktop & UAC

Format: JSON (leicht lesbar)

Gespeicherte Backups

Backups gefunden: 0

Erfolg



Registry-Backup erfolgreich erstellt:
C:\Users\JörnWalter\source\repos\SystemConfigManager\SystemConfigManager\bin\Release\net8.0-windows\RegistryBackups\RegistryBackup_20251101_163103.json

OK

Funktionen

Backup erstellen:

Tab "Registry Backup"

→ Beschreibung eingeben (optional)

→ "Backup erstellen"

→ JSON-Datei wird gespeichert

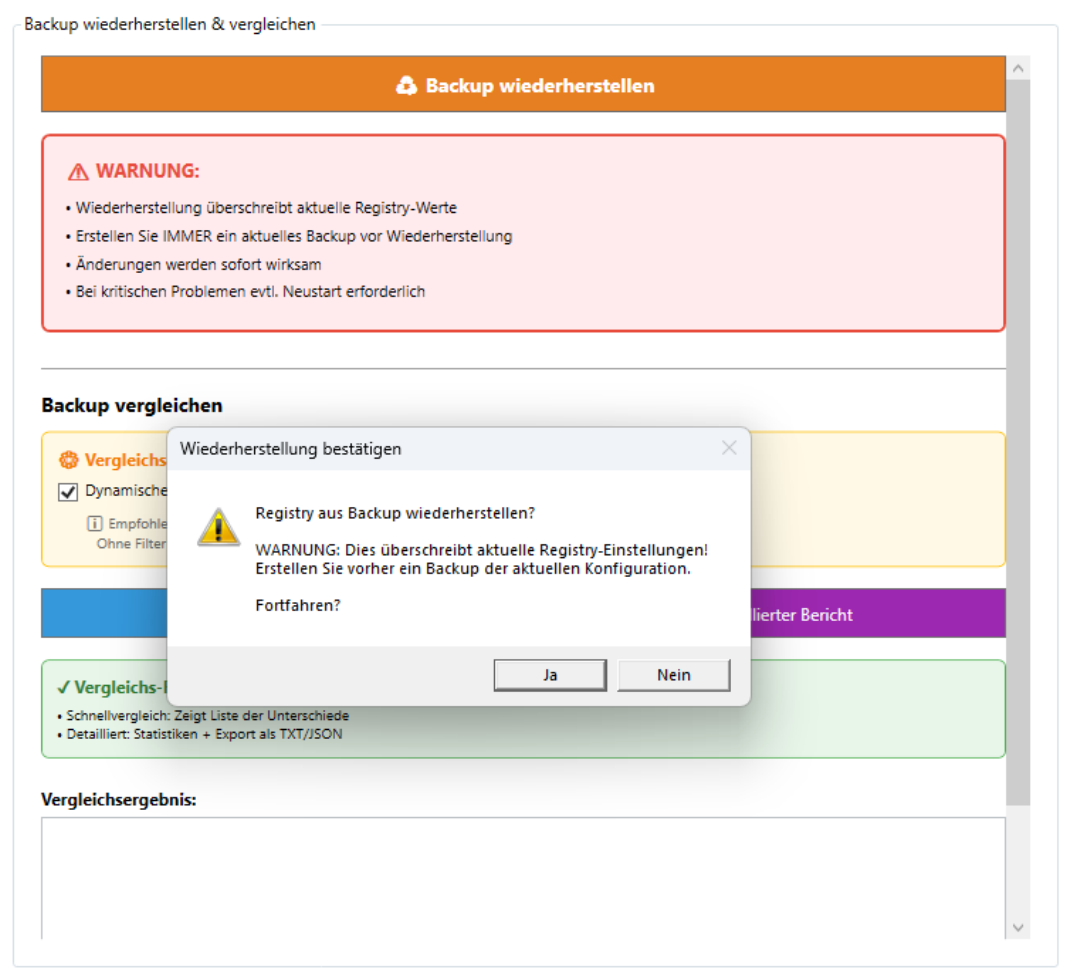
Backup wiederherstellen:

→ "Wiederherstellen" klicken

→ Backup-Datei auswählen

→ Bestätigung

→ Registry wird wiederhergestellt



Backup vergleichen:

- "Vergleichen" klicken
- Backup-Datei auswählen
- Zeigt Unterschiede zwischen aktuellem System und Backup
- Option: Dynamische Werte ignorieren (empfohlen)

 Schnellvergleich

 Detaillierter Bericht

✓ **Vergleichs-Funktion:**

- Schnellvergleich: Zeigt Liste der Unterschiede
- Detailliert: Statistiken + Export als TXT/JSON

Vergleichsergebnis:

```
[DWord] HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Scan\AllowFullScanRemovableDriveScanning:
Backup: (nicht vorhanden)
Aktuell: 1

[DWord] HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\SubmitSamplesConsent:
Backup: (nicht vorhanden)
Aktuell: 1

[DWord] HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet\SpynetReporting:
Backup: (nicht vorhanden)
Aktuell: 2
```

Detaillierter Vergleich:

- "Detaillierter Bericht" klicken
- Statistik mit genauen Zahlen
- Auflistung aller Unterschiede
- Fehlerprotokoll
- Export als TXT oder JSON möglich

 Schnellvergleich

 Detaillierter Bericht

STATISTIK

Backup: 01.11.2025 16:09:38
Vergleich: 01.11.2025 16:17:56
Computer: ms1.windowspapst.de

✓ Übereinstimmend: 80
X Unterschiede: 559
Ø Ignoriert: 15 (dynamisch)

✓ Vergleichs-Funktion:

- Schnellvergleich: Zeigt Liste der Unterschiede
- Detailliert: Statistiken + Export als TXT/JSON

Dynamische Werte

Einige Registry-Werte ändern sich ständig (z.B. LsaPid, Timestamps, Session-IDs).
Diese werden beim Vergleich standardmäßig ignoriert.

6. Policy Blacklist Management

Was ist die Blacklist?

Manche Policies passen nicht zu jeder Umgebung. Mit der Blacklist können Sie Policies von der automatischen Optimierung ausschließen.

Policy Blacklist Verwaltung
Policies von der automatischen Optimierung ausschließen
Blacklist: 3 Policies

Laden Alle löschen Export

Verfügbare Policies (BSI + NIST)

Hinweis:
Wählen Sie Policies aus, die NICHT automatisch optimiert werden sollen.

Suchen...

Policy	Kategorie	Severity
Virtualization Based Security	Credential Protection	CRITICAL
Credential Guard Konfiguration	Credential Protection	CRITICAL
Platform Security Features	Platform Security	HIGH
AppLocker Aktivierung	Application Control	HIGH
Software Restriction Default Level	Application Control	HIGH
Kernel Mitigation Options	Exploit Protection	CRITICAL
Structured Exception Handler Overwrite Protection	Exploit Protection	HIGH
LDAP Server Signing	LDAP Security	HIGH
LDAP Client Signing	LDAP Security	HIGH
LDAP Channel Binding	LDAP Security	HIGH
DNSSEC Validierung	DNS Security	HIGH
DNS over HTTPS	DNS Security	MEDIUM
Potentially Unwanted Application Protection	Malware Protection	MEDIUM
Controlled Folder Access	Ransomware Protection	HIGH
Network Protection	Network Protection	HIGH
Attack Surface Reduction Rules	Attack Surface Reduction	HIGH

Zur Blacklist hinzufügen

Auf Blacklist (werden übersprungen)

Diese Policies werden übersprungen:

- Bei BSI/NIST Optimierung
- Bei Vollständige Optimierung

[MEDIUM] Remote Access → WinRM Auto Config
[MEDIUM] Login Notification → Letzte Anmeldeinformationen anzeigen
[HIGH] Remote-Zugriff → Remote Desktop deaktivieren

Von Blacklist entfernen

Verwendung

Policies zur Blacklist hinzufügen:

Tab "Blacklist-Verwaltung"

→ "Daten laden" = Zeigt alle verfügbaren Policies

→ Suchfunktion nutzen

→ Policy auswählen

→ "Zur Blacklist hinzufügen"

Von Blacklist entfernen:

→ Policy in Blacklist-Liste auswählen

→ "Von Blacklist entfernen"

Blacklist exportieren:

→ "Exportieren" = Erstellt TXT-Datei mit allen Blacklist-Einträgen

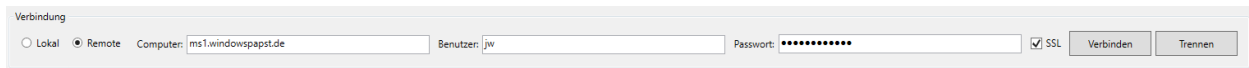
Persistenz

Die Blacklist wird in PolicyBlacklist.json gespeichert und bleibt über Neustarts erhalten.

7. Remote-Verwaltung

PowerShell Remoting

Das Tool kann Windows-Server remote verwalten über **WinRM** (Windows Remote Management).



Voraussetzungen

Auf dem Ziel-Server:

PowerShell Remoting aktivieren

Enable-PSRemoting -Force

Firewall-Regel prüfen (Port 5985 HTTP oder 5986 HTTPS)

Get-NetFirewallRule -Name "WINRM-HTTP-In-TCP"

Optional: TrustedHosts konfigurieren (bei Workgroup)

Set-Item WSMan:\localhost\Client\TrustedHosts -Value "SERVER-NAME"

Verbindung herstellen

Hauptfenster → Connection-Bereich

→ "Remote" auswählen

→ Computer-Name eingeben

→ Benutzername/Passwort (optional bei Domäne)

→ "SSL verwenden" = Port 5986 (empfohlen)

→ "Verbinden" klicken

SSL vs. Unverschlüsselt:

-  **SSL (Port 5986):** Verschlüsselt, sicherer, benötigt Zertifikat
-  **HTTP (Port 5985):** Unverschlüsselt, nur im vertrauenswürdigen Netzwerk

Features bei Remote-Verbindung

- Alle Compliance-Checks funktionieren remote
- Registry-Änderungen werden auf Remote-System angewendet
- Computer-Info zeigt Remote-System-Details
- Logging zeigt Remote-Computer-Namen

8. Kombinierte Reports

Gesamt-Compliance-Report

Erstellt einen HTML-Report mit:

- BSI Compliance-Ergebnissen
- NIST Compliance-Ergebnissen
- Unsichere Services
- Fehlende Patches
- Administrator-Accounts

Verwendung

Tab "Zusammenfassung"

→ "Alle prüfen" = Führt alle Checks durch

→ "Gesamtreport" = Erstellt HTML-Report

→ Report wird im Browser geöffnet

Report-Inhalt

- Executive Summary mit Compliance-Prozentzahlen
- Detaillierte Policy-Auflistung
- Farb-codierte Risikobewertung
- Empfehlungen für Verbesserungen
- Zeitstempel und Computer-Info

Vor einer Optimierung:

BSI Grundschutz Security Compliance Report
Erstellt am: 01.11.2025 16:52:05
Computer: msl.windowspapst.de (Remote)
Betriebssystem: Microsoft Windows NT 10.0.26100.0
Bericht erstellt auf: DC

BSI Grundschutz Compliance

89.5%	323	38	361
Gesamt-Compliance	Konform	Nicht Konform	Gesamt

Access Control

Control	Beschreibung	Aktuell	Empfohlen	Severity	Status
Anonymen Zugriff einschränken	2 = Ohne explizite anonyme Berechtigungen kein Zugriff	2	2	CRITICAL	OK
User Account Control aktivieren	Erzwingt UAC für alle Benutzer	1	1	HIGH	OK
UAC-Verhalten für Administratoren	2 = Immer nach Bestätigung fragen	2	2	HIGH	OK
Anonyme SID-Übersetzung verhindern	0 = Anonymous ist nicht in Everyone-Gruppe	0	0	HIGH	OK
Null Session Named Pipes	Leere Liste = Keine Anonymous Pipes erlaubt			CRITICAL	OK
Remote SAM Enumeration einschränken	O:BAG:BAD(A;;RC;;;BA) = Nur Admins dürfen SAM remote abfragen	O:BAG:BAD(A;;RC;;;BA)	O:BAG:BAD(A;;RC;;;BA)	CRITICAL	OK
Null Session Shares	Leere Liste = Keine anonymen Shares erlaubt			HIGH	OK
Restrict Anonymous SAM	1 = Anonymer Zugriff auf SAM-Konten verweigern	1	1	HIGH	OK
Restrict Anonymous	1 = Anonyme Enumeration von SAM-Konten verhindern	2	1	HIGH	Erwartet: 1
Everyone Includes Anonymous	0 = Anonymous ist nicht in Everyone-Gruppe	0	0	HIGH	OK
Disable Registry Editing Tools	0 = Regedit für Benutzer verfügbar (Admin-Zugriff erforderlich)	Nicht gesetzt	0	LOW	

Nach einer Optimierung:

BSI Grundsutz Compliance Report

Erstellt am: 01.11.2025 16:42:38

Computer: msl.windowspapst.de (Remote)

Betriebssystem: Microsoft Windows NT 10.0.26100.0

Bericht erstellt auf: DC

BSI Grundsutz Compliance

10.0%

Gesamt-Compliance

36

Konform

325

Nicht Konform

361

Gesamt

Access Control

Control	Beschreibung	Aktuell	Empfohlen	Severity	Status
Anonymen Zugriff einschränken	2 = Ohne explizite anonyme Berechtigungen kein Zugriff	0	2	CRITICAL	Erwartet: 2
User Account Control aktivieren	Erzwingt UAC für alle Benutzer	1	1	HIGH	OK
UAC-Verhalten für Administratoren	2 = Immer nach Bestätigung fragen	5	2	HIGH	Erwartet: 2
Anonyme SID-Übersetzung verhindern	0 = Anonymous ist nicht in Everyone-Gruppe	0	0	HIGH	OK
Null Session Named Pipes	Leere Liste = Keine Anonymous Pipes erlaubt			CRITICAL	OK
Remote SAM Enumeration einschränken	O:BAG:BAD(A;RC;BA) = Nur Admins dürfen SAM remote abfragen	Nicht gesetzt	O:BAG:BAD(A;RC;BA)	CRITICAL	
Null Session Shares	Leere Liste = Keine anonymen Shares erlaubt	Nicht gesetzt		HIGH	
Restrict Anonymous SAM	1 = Anonymer Zugriff auf SAM-Konten verweigern	1	1	HIGH	OK
Restrict Anonymous	1 = Anonyme Enumeration von SAM-Konten verhindern	0	1	HIGH	Erwartet: 1
Everyone Includes Anonymous	0 = Anonymous ist nicht in Everyone-Gruppe	0	0	HIGH	OK
Disable Registry Editing Tools	0 = Regedit für Benutzer verfügbar (Admin-Zugriff erforderlich)	Nicht gesetzt	0	LOW	

Vorteile der toolbasierten Sicherheitsverwaltung

1. Zeitersparnis

Manuelle Prüfung:

- 30+ Registry-Keys einzeln öffnen und prüfen
- Pro Einstellung ca. 2-3 Minuten
- **Gesamt: 5-8 Stunden für vollständige Prüfung**

Mit Tool:

- Alle Einstellungen auf einmal prüfen
- Automatisierte Auswertung
- **Gesamt: 2-3 Minuten**

Zeitersparnis: > 95%

2. Fehlerreduktion

Manuelle Konfiguration:

- **✗** Tippfehler bei Registry-Pfaden
- **✗** Falsche Datentypen (DWORD vs. String)
- **✗** Vergessene Einstellungen
- **✗** Inkonsistente Konfiguration
- **✗** Keine Dokumentation

Mit Tool:

- **✓** Vordefinierte, getestete Policies
- **✓** Automatische Typ-Konvertierung
- **✓** Vollständige Abdeckung
- **✓** Konsistente Anwendung
- **✓** Automatisches Logging

Fehlerquote: Nahezu 0%

3. Compliance & Audit

Manuelle Dokumentation:

- Aufwändige Erfassung
- Fehleranfällig
- Zeitintensiv
- Schwer nachvollziehbar

Mit Tool:

- ☒ Automatische HTML-Reports
- ☒ Detaillierte Logs mit Timestamps
- ☒ Nachvollziehbare Änderungen
- ☒ Audit-Trail für Compliance-Nachweise
- ☒ Exportierbare Ergebnisse

Perfekt für ISO 27001, BSI IT-Grundschutz, DSGVO-Audits

4. Reproduzierbarkeit

Problem bei manueller Konfiguration:

- Unterschiedliche Konfigurationen auf verschiedenen Servern
- "Tribal Knowledge" (nur eine Person kennt die Einstellungen)
- Schwierig, identische Setups zu erstellen

Mit Tool:

- ☒ Einheitliche Konfiguration auf allen Systemen
- ☒ Wiederholbare Prozesse
- ☒ Identische Sicherheitsstandards
- ☒ Einfaches Onboarding neuer Server

5. Zentrale Verwaltung

Remote-Verwaltung Vorteile:

- ☒ Keine RDP-Sitzungen erforderlich
- ☒ Mehrere Server von einer Station aus verwalten
- ☒ Batch-Operationen möglich
- ☒ Zentrale Übersicht
- ☒ Reduzierte Reisezeiten

6. Aktualität

Herausforderung bei manueller Pflege:

- BSI/NIST Standards ändern sich
- Neue Bedrohungen erfordern neue Controls
- Manuelle Updates der Dokumentation

Mit Tool:

- ☒ Zentral gepflegte Policy-Definitionen
- ☒ Updates durch neue Tool-Version
- ☒ Automatische Berücksichtigung neuer Standards

7. Risikominimierung

Vorteile:

- ☒ Backup & Restore vor Änderungen
- ☒ Blacklist für kritische Systeme
- ☒ Batch-Verarbeitung verhindert System-Überlastung
- ☒ Detaillierte Logs für Troubleshooting
- ☒ Vergleichsfunktion zeigt Abweichungen

8. Best-Practice Implementierung

Problem:

- BSI/NIST Dokumente sind hunderte Seiten lang
- Interpretation erforderlich
- Umsetzung unklar

Mit Tool:

- ☒ Fertig umgesetzte Best Practices
- ☒ Deutsche + US-Standards kombiniert
- ☒ Von Security-Experten geprüft
- ☒ Produktionsreif

9. Wissensdatenbank

Das Tool als Lernressource:

- Zeigt konkrete Registry-Pfade und Werte
- Erklärt Zweck jeder Einstellung (Description)
- Reference zu BSI/NIST Controls
- Severity-Einstufung hilft bei Priorisierung

Wissenstransfer im Team wird einfacher

Bedienungsanleitung

Grundlegender Workflow

1. Tool als Administrator starten
2. [Optional] Remote-Verbindung aufbauen
3. [Empfohlen] Registry-Backup erstellen
4. Compliance-Checks durchführen:
 - BSI Grundschatz prüfen
 - NIST Framework prüfen
 - SMB-Konfiguration prüfen
 - TLS/SSL-Status laden
5. Ergebnisse analysieren
6. [Optional] Policies zur Blacklist hinzufügen
7. Optimierung durchführen
8. Report exportieren
9. [Bei TLS-Änderungen] System neu starten

Benutzeroberfläche

Hauptfenster

Oberer Bereich:

- Connection-Einstellungen (Lokal/Remote)
- Admin-Status
- Computer-Info

Tab "BSI Compliance":

- DataGrid mit allen BSI-Policies
- Buttons: Prüfen, Optimieren, Exportieren
- Fortschrittsanzeige und Details

Tab "NIST Compliance":

- DataGrid mit allen NIST-Controls
- Buttons: Prüfen, Optimieren, Exportieren
- Fortschrittsanzeige und Details

Tab "SMB-Konfiguration":

- Checkboxen für SMB-Einstellungen
- Buttons: Aktualisieren, Anwenden, Optimieren

Tab "TLS/SSL":

- Protocol Status (SSL 2.0 - TLS 1.3)
- Cipher Status
- Hash Status
- Detaillierter Bericht
- Buttons: Status laden, Optimieren, Report exportieren

Tab "Zusammenfassung":

- Gesamt-Compliance-Anzeige
- Buttons: Alle prüfen, Alle optimieren, Gesamtreport

Tab "Registry Backup":

- Backup-Liste
- Buttons: Erstellen, Wiederherstellen, Vergleichen
- Backup-Verwaltung

Tab "Blacklist-Verwaltung":

- Policy-Liste (alle verfügbaren Policies)
- Blacklist-Anzeige
- Suchfunktion
- Buttons: Laden, Hinzufügen, Entfernen, Exportieren

Tab "Log":

- Echtzeit-Logging aller Operationen
- Buttons: Log löschen, Log-Datei öffnen

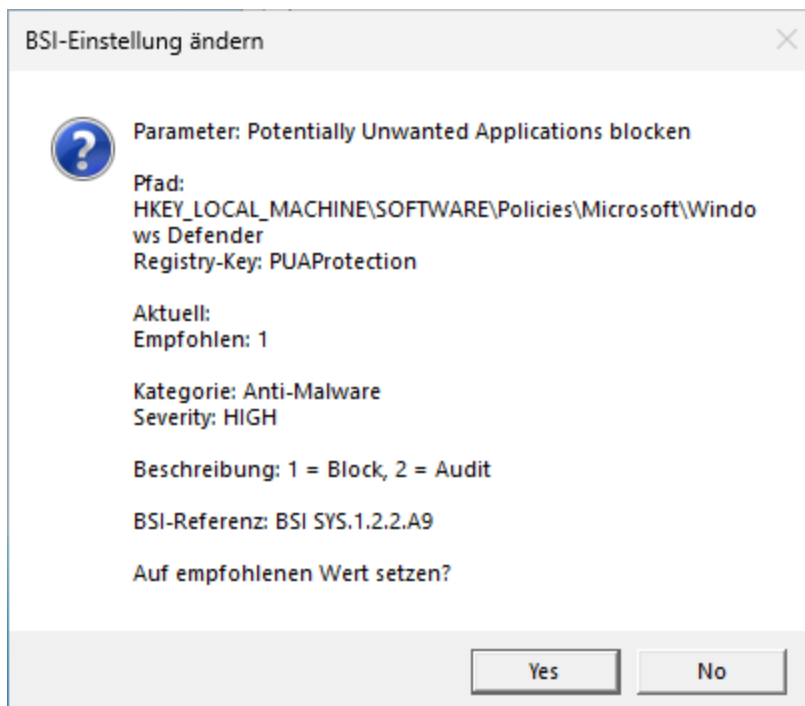
Unterer Bereich:

- Statuszeile
- Copyright-Link zur Website

Doppelklick-Funktionen

In BSI/NIST Grids:

- Doppelklick auf eine Policy zeigt Details
- Dialog mit vollständigen Informationen
- Option: "Auf empfohlenen Wert setzen"
- Sofortige Anwendung einzelner Policies möglich



Sortierung und Filterung

DataGrids:

- Klick auf Spaltenüberschrift sortiert
- Standard-Sortierung nach Kategorie (automatisch)
- Manuelle Sortierung nach:
 - Severity (CRITICAL, HIGH, MEDIUM)
 - Compliance-Status (✓ / ✗)
 - Kategorie
 - DisplayName

Best Practices

1. Vor Produktions-Einsatz

✓ Test-System verwenden:

- Testen Sie alle Änderungen zuerst auf einem Test-Server
- Prüfen Sie, ob Anwendungen noch funktionieren
- Dokumentieren Sie Probleme

✓ Backup erstellen:

- **IMMER** vor Optimierung ein Registry-Backup erstellen
- Zusätzlich System-Snapshot/Backup empfohlen
- Backups an sicheren Ort speichern

✓ Dokumentation lesen:

- Verstehen Sie, was jede Policy bewirkt
- Lesen Sie BSI/NIST-Referenzen
- Bei Unklarheit: Research oder Blacklist

2. Schrittweise Optimierung

✗ NICHT empfohlen:

"Alle optimieren" auf Produktions-Server ohne Test

✓ Empfohlen:

1. Nur CRITICAL Policies (ohne MEDIUM)
2. Test der Funktionalität
3. Dann HIGH Policies
4. Test der Funktionalität
5. Bei Bedarf MEDIUM Policies
6. Kontinuierliche Überwachung

3. Blacklist nutzen

Szenarien für Blacklist:

✦ Anwendungsinkompatibilität:

Beispiel: Legacy-Anwendung benötigt TLS 1.0

→ TLS 1.0 Deaktivierung auf Blacklist setzen

✦ Spezielle Anforderungen:

Beispiel: Druckerserver benötigt SMB1 für alte Drucker

→ SMB1-Deaktivierung auf Blacklist setzen

✦ Compliance-Ausnahmen:

Beispiel: Bestimmte Policy widerspricht firmeninterner Policy

→ Policy auf Blacklist setzen

4. Monitoring nach Änderungen

In den ersten 24h nach Optimierung:

- Event-Log überwachen (System, Application, Security)
- Anwendungs-Funktionalität testen
- Netzwerk-Konnektivität prüfen
- Benutzer-Feedback sammeln
- Performance-Metriken beobachten

5. Regelmäßige Compliance-Checks

Empfohlener Rhythmus:

- **Wöchentlich:** Schneller Check auf kritischen Systemen
- **Monatlich:** Vollständiger Compliance-Check
- **Quartalsweise:** Vollständiger Report für Management
- **Jährlich:** Audit-Report für Zertifizierungen

6. Remote-Verwaltung absichern

Sicherheits-Checkliste:

- ☒ SSL-Verbindung verwenden (Port 5986)
- ☒ Starke Passwörter/Zertifikate
- ☒ Zugriff auf Admin-Gruppe beschränken
- ☒ Firewall-Regeln auf notwendige IPs beschränken
- ☒ WinRM-Logging aktivieren
- ☒ Regelmäßig Audit-Logs prüfen

7. Versionskontrolle für Backups

Naming Convention:

RegistryBackup_YYYYMMDD_HHMMSS_[Beschreibung].json

Beispiele:

RegistryBackup_20250131_143000_VorBSIOptimierung.json

RegistryBackup_20250131_150000_NachBSIOptimierung.json

RegistryBackup_20250205_100000_Produktiv_Baseline.json

Aufbewahrung:

- Mindestens 3 Backups vor Änderungen
- Baseline-Backup nach erfolgreicher Optimierung
- Regelmäßige Backups (z.B. monatlich)
- Alte Backups archivieren (nicht löschen)

8. Change Management Integration

In größeren Umgebungen:

1. Compliance-Check durchführen
2. Report erstellen
3. Change Request erstellen mit:
 - Ist-Zustand (Report)
 - Soll-Zustand (nach Optimierung)
 - Risikobewertung
 - Rollback-Plan (Backup)
4. Change Request genehmigen lassen
5. Wartungsfenster planen
6. Optimierung durchführen
7. Validierung dokumentieren
8. Change Request schließen

Technische Details

Registry-Zugriff

Lokaler Zugriff:

- Verwendet .NET Microsoft.Win32.Registry API
- 64-Bit Registry View (Registry64)
- Timeout-Schutz (5 Sekunden)

Remote-Zugriff:

- PowerShell Remoting über System.Management.Automation
- WsMan-ConnectionInfo (WinRM)
- Unterstützt SSL/TLS-verschlüsselte Verbindungen
- Credential-Management für Domäne und Workgroup

Datentyp-Handling

DWORD-Konvertierung:

- Registry API verwendet Int32 intern
- Tool konvertiert zwischen Int32 ↔ UInt32
- Bit-Pattern-Preservation für Werte $> 2^{31}$
- Unterstützt Hex-Notation (0xFFFFFFFF)

Unterstützte Registry-Typen:

- DWord (REG_DWORD)
- QWord (REG_QWORD)
- String (REG_SZ)
- ExpandString (REG_EXPAND_SZ)
- MultiString (REG_MULTI_SZ)
- Binary (REG_BINARY)

Batch-Verarbeitung

Performance-Optimierung:

Batch-Größe: 10 Policies

Delay zwischen Batches: 500ms

Delay zwischen Keys: 100ms

Zweck:

- Vermeidung von System-Überlastung
- Bessere Fehler-Isolierung
- Fortschrittsanzeige für Benutzer

Policy-Definitionen

Struktur:

```
class PolicyDefinition {  
    string Name          // Eindeutiger Identifier  
    string DisplayName    // Anzeigename  
    string Path           // Registry-Pfad  
    string ValueType      // DWORD, String, etc.  
    object RecommendedValue  
    string Severity       // CRITICAL, HIGH, MEDIUM  
    string Category       // Gruppierung  
    string Description     // Was macht die Policy?  
    string Reference       // BSI/NIST Reference  
}
```

Logging

Log-Levels:

- INFO: Allgemeine Informationen
- SUCCESS: Erfolgreiche Operationen
- WARNING: Warnungen (keine Fehler)
- ERROR: Fehler

Log-Speicherort:

%PROGRAMDIR%\Logs\SecurityConfig_YYYYMMDD.log

Features:

- Automatische Datei-Rotation (täglich)
- UTF-8 Encoding
- Thread-Safe
- Echtzeit-Anzeige im UI

Fehlerbehebung

Problem: "Keine Administrator-Rechte"

Symptom:

- Tool zeigt "Administrator: Nein" an
- Registry-Änderungen schlagen fehl

Lösung:

1. Tool schließen
2. Rechtsklick auf SystemConfigManager.exe
3. "Als Administrator ausführen"
4. UAC-Abfrage bestätigen

Problem: Remote-Verbindung schlägt fehl

Symptom:

"Verbindung fehlgeschlagen: Zugriff verweigert"

Diagnose & Lösung:

1. WinRM-Status prüfen (auf Ziel-Server):

Service-Status

Get-Service WinRM

Sollte "Running" sein, sonst:

Start-Service WinRM

WinRM-Konfiguration

winrm quickconfig

2. Firewall-Regel prüfen:

HTTP (Port 5985)

Get-NetFirewallRule -Name "WINRM-HTTP-In-TCP"

HTTPS (Port 5986)

Get-NetFirewallRule -Name "WINRM-HTTPS-In-TCP"

Falls nicht vorhanden:

Enable-PSRemoting -Force

3. Authentication:

Bei Workgroup: TrustedHosts konfigurieren (auf Client)

Set-Item WSMan:\localhost\Client\TrustedHosts -Value "SERVER-NAME" -Force

Bei Domäne: Domänen-Credentials verwenden

4. SSL-Zertifikat (für Port 5986):

Zertifikat prüfen

Get-ChildItem WSMan:\localhost\Listener

Selbstsigniertes Zertifikat erstellen (Test):

```
New-SelfSignedCertificate -DnsName "SERVER-NAME" -CertStoreLocation  
Cert:\LocalMachine\My
```

WinRM HTTPS-Listener erstellen

```
New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -  
CertificateThumbPrint THUMBPRINT
```

Problem: Policies werden nicht angewendet

Symptom:

- Optimierung zeigt "Erfolgreich"
- Aber Policies bleiben X Nicht konform

Mögliche Ursachen:

1. Group Policy Override:

- Domänen-GPOs haben Vorrang
- Lösung: GPO-Einstellungen prüfen (gpresult /h report.html)

2. Registry-Pfad existiert nicht:

- Tool erstellt Pfade automatisch
- Bei Remote: Pfad-Erstellung schlägt fehl
- Lösung: Pfad manuell erstellen oder lokal anwenden

3. Berechtigungen:

- Bestimmte Keys haben spezielle ACLs
- Lösung: Als SYSTEM ausführen (psexec) oder ACLs anpassen

Problem: TLS-Optimierung funktioniert nicht

Symptom:

- Nach TLS-Optimierung + Neustart: Keine Änderung

Überprüfung:

Registry-Keys prüfen

Get-ItemProperty -Path

"HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client"

Sollte zeigen:

Enabled: 1

DisabledByDefault: 0

Mögliche Probleme:

1. .NET Framework Cache:

- .NET cached alte TLS-Einstellungen
- Lösung: Auch .NET Framework Settings anpassen (wird vom Tool gemacht)

2. Application Override:

- Manche Apps erzwingen eigene TLS-Einstellungen
- Lösung: App-spezifische Konfiguration prüfen

Problem: System instabil nach Optimierung

Sofortmaßnahmen:

1. Registry wiederherstellen:

Tool starten → Registry Backup Tab

→ Letztes Backup vor Optimierung auswählen

→ "Wiederherstellen" klicken

→ System neu starten

2. Problematische Policy identifizieren:

1. Backup wiederherstellen
2. Policies einzeln anwenden (Doppelklick)
3. Nach jeder Policy: Funktionalität testen
4. Problematische Policy auf Blacklist setzen

Problem: Log-Datei wird zu groß

Lösung:

- Tool erstellt täglich neue Log-Dateien
- Alte Logs manuell archivieren/löschen
- Empfohlen: Logs älter als 90 Tage archivieren

Automatisierung (PowerShell):

```
$logPath = "C:\Path\To\Tool\Logs"
```

```
$archivePath = "C:\Path\To\Archive"
```

```
$cutoffDate = (Get-Date).AddDays(-90)
```

```
Get-ChildItem $logPath -Filter "*.log" |
```

```
Where-Object { $_.LastWriteTime -lt $cutoffDate } |
```

```
Move-Item -Destination $archivePath
```

FAQ

Allgemein

F: Ist das Tool für alle Windows-Versionen geeignet?

A: Das Tool ist optimiert für:

-  Windows 10 (1809+)
-  Windows 11
-  Windows Server 2016/2019/2022/2025
-  Windows Server 2012 R2: Eingeschränkt (manche Policies nicht verfügbar)
-  Windows 7/8: Nicht unterstützt

F: Kann ich das Tool auf Domain Controllern verwenden?

A: Ja, aber mit Vorsicht:

-  Erstellen Sie **definitiv** ein Backup
-  Testen Sie zuerst auf Member-Server
-  Manche AD-spezifische Einstellungen könnten betroffen sein
-  Nutzen Sie die Blacklist für DC-spezifische Ausnahmen

Empfehlung: Für DCs besser GPOs verwenden als lokale Registry-Änderungen.

F: Werden meine Änderungen rückgängig gemacht, wenn Windows-Updates installiert werden?

A: In der Regel **NEIN**. Registry-Änderungen bleiben bestehen. Ausnahmen:

-  Große Feature-Updates (z.B. 22H2 → 23H2) könnten Einstellungen zurücksetzen
-  Normale Qualitätsupdates ändern Einstellungen nicht

Empfehlung: Nach großen Updates Compliance-Check wiederholen.

Sicherheit

F: Ist das Tool selbst sicher?

A: Ja:

- ☒ Keine Netzwerk-Kommunikation (außer Remote-Verwaltung)
 - ☒ Keine Telemetrie oder "Phone Home"
 - ☒ Alle Daten bleiben lokal
 - ☒ Open-Source-Code (überprüfbar)
 - ☒ Detailliertes Logging aller Aktionen
 - ☒ Kein Code-Obfuscation
-

F: Warum blockieren manche Antivirus-Programme das Tool?

A: **False-Positive-Problem:**

- Tool modifiziert Registry → Verhaltensweisen ähnlich wie Malware
- Tool benötigt Admin-Rechte → Verdächtig für AV
- PowerShell Remoting → Wird manchmal blockiert

Lösung:

1. Tool bei VirusTotal hochladen (Prüfung durch 60+ Engines)
2. Bei False-Positive: Ausnahme in AV konfigurieren
3. Tool-Verzeichnis zur AV-Whitelist hinzufügen

Beruhigung: Tool ist legitimes Admin-Werkzeug, kein Virus.

F: Kann das Tool Malware entfernen?

A: **Nein.** Das Tool:

- ☒ Härt das System gegen zukünftige Angriffe
- ☒ Reduziert Angriffsfläche
- ☒ Aktiviert Schutzmechanismen

- ❌ Entfernt **keine** vorhandene Malware

Bei Malware-Befall:

1. Zuerst: Malware entfernen (mit Anti-Malware-Tools)
2. Dann: System härten mit diesem Tool
3. Prüfen: Kompromittierung ausschließen

Performance

F: Beeinflusst die Optimierung die System-Performance?

A: **Minimal bis gar nicht:**

Positiv:

- ✅ Deaktivierung unnötiger Protokolle → Weniger Overhead
- ✅ Bessere Netzwerk-Sicherheit → Weniger Angriffe → Stabileres System

Potenziell negativ:

- ⚠️ Manche Security-Features haben minimalen Overhead (< 1%)
- ⚠️ Erweiterte Logging-Einstellungen → Mehr Disk I/O

Fazit: Performance-Impact ist vernachlässigbar auf modernen Systemen.

F: Wie lange dauert eine vollständige Optimierung?

A:

- **BSI Optimierung:** 30-60 Sekunden (360+ Policies)
- **NIST Optimierung:** 30-60 Sekunden (360+ Policies)
- **TLS Optimierung:** 10-20 Sekunden
- **Gesamt:** 1-2 Minuten für komplette Härtung

Compliance & Auditing

F: Ist die Optimierung ausreichend für ISO 27001 Zertifizierung?

A: **Teilweise:**

-  Tool implementiert wichtige technische Controls
-  Reports helfen bei Audits
-  ISO 27001 erfordert auch:
 - Organisatorische Maßnahmen
 - Policies und Prozesse
 - Risikoanalyse
 - Dokumentation
 - Awareness-Training
 - Incident Response

Fazit: Tool ist ein wichtiger **Baustein**, aber nicht ausreichend allein.

F: Werden BSI/NIST Standards regelmäßig aktualisiert?

A: Ja:

- BSI Grundschatz: Updates mehrmals pro Jahr
- NIST CSF: Updates alle 2-3 Jahre

Tool-Updates:

- Neue Versionen enthalten aktualisierte Policy-Definitionen
- Check auf GitHub/Website für Updates
- Empfehlung: Update alle 6-12 Monate

Troubleshooting

F: Policy wird nicht auf Blacklist gesetzt.

A: Prüfen Sie:

1. **"Daten laden"** Button geklickt? (Policy-Liste muss geladen sein)
 2. Richtige Policy ausgewählt?
 3. Log-Fenster für Fehlermeldungen checken
 4. PolicyBlacklist.json Schreibrechte vorhanden?
-

F: Remote-Computer-Info zeigt nur "Unbekannt".

A: Bekanntes Problem bei manchen PowerShell-Versionen:

- **Workaround:** Funktionalität ist **nicht** eingeschränkt
 - Registry-Zugriffe funktionieren trotzdem
 - Alternative: Verbindung trennen und neu verbinden
-

F: Backup-Wiederherstellung schlägt teilweise fehl.

A: Normal bei:

- System-Keys mit speziellen Berechtigungen
- Temporäre Werte (z.B. Session-IDs)
- Nur-Lese-Keys

Lösung:

- Log-Datei prüfen, welche Keys fehlschlagen
 - Kritische Keys manuell prüfen/setzen
 - Bei Bedarf: Als SYSTEM ausführen (PSEXec)
-

Support & Weiterführende Informationen

Offizielle Ressourcen

BSI Grundschutz:

-  <https://www.bsi.bund.de/grundschutz>
-  BSI IT-Grundschutz-Kompendium (PDF)

NIST Cybersecurity Framework:

-  <https://www.nist.gov/cyberframework>
-  NIST CSF 2.0 Documentation

Microsoft Security Baselines:

-  <https://learn.microsoft.com/en-us/windows/security/>

PowerShell Remoting:

-  <https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/>

Tool-Informationen

Website: <https://www.it-service-walter.com>

Version: 6.5

Lizenz: Kommerziell

Support: support@it-service-walter.com

Installation & Systemanforderungen

Systemanforderungen

Minimum:

- Windows 10/11 oder Windows Server 2016+
- .NET Framework 4.8 oder höher
- 50 MB freier Festplattenspeicher
- Administrator-Rechte

Empfohlen:

- Windows 11 oder Windows Server 2022
- .NET 8.0 oder höher
- 4 GB RAM

Rechtliche Hinweise

Haftungsausschluss

Dieses Tool wird "wie besehen" ohne jegliche Gewährleistung bereitgestellt. Der Autor übernimmt keine Haftung für:

- Datenverlust
- System-Instabilität
- Funktionsstörungen
- Compliance-Probleme

Empfehlung: Immer zuerst in Test-Umgebung testen!

Lizenz

Kommerziell

Zusammenfassung

Der **Security Configuration Manager v6.5** ist ein unverzichtbares Tool für IT-Administratoren, die:

- ✓ Windows-Systeme nach BSI/NIST Standards härten wollen
- ✓ Compliance automatisiert prüfen müssen
- ✓ Zeit und Kosten bei Security-Audits sparen wollen
- ✓ Konsistente Konfigurationen über mehrere Server verwalten
- ✓ Professionelle, audit-sichere Dokumentation benötigen

Zeit- und Kostenersparnis von über 90% bei gleichzeitig **höherer Qualität und Fehlerfreiheit** macht das Tool zur ersten Wahl für professionelle IT-Sicherheit.

© 2025 IT-Service Walter | Alle Rechte vorbehalten

Eine unverzichtbare Lösung für professionelles Windows-Sicherheitsmanagement und Compliance-Erfüllung.

Verkauf

Das Tool kostet einmalig ab 299,00 € inkl. 19% MwSt.