SECURITY CONFIGURATION MANAGER

IT-Service Walter

Jörn Walter
www.it-service-walter.com
04.11.2025

SECURITY CONFIGURATION MANAGER ÜBERBLICK

DER **SECURITY CONFIGURATION MANAGER V6.0** 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)

Inhalt

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

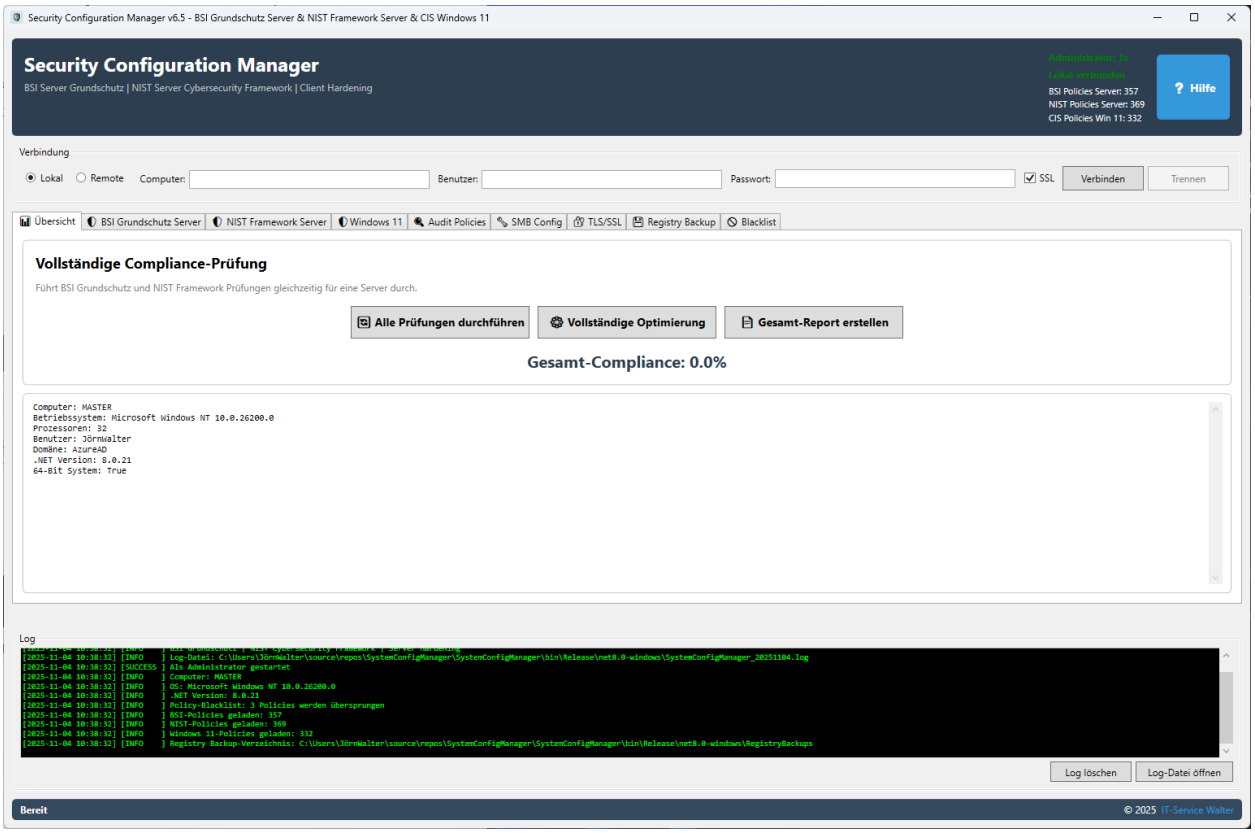
Empfohlen:

- Windows 11 oder Windows Server 2022
- .NET 6.0 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



BSI Grundschutz Compliance

Was wird geprüft?

Der BSI-Grundschutz ist der deutsche Standard für IT-Sicherheit. Das Tool prüft **über 350 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

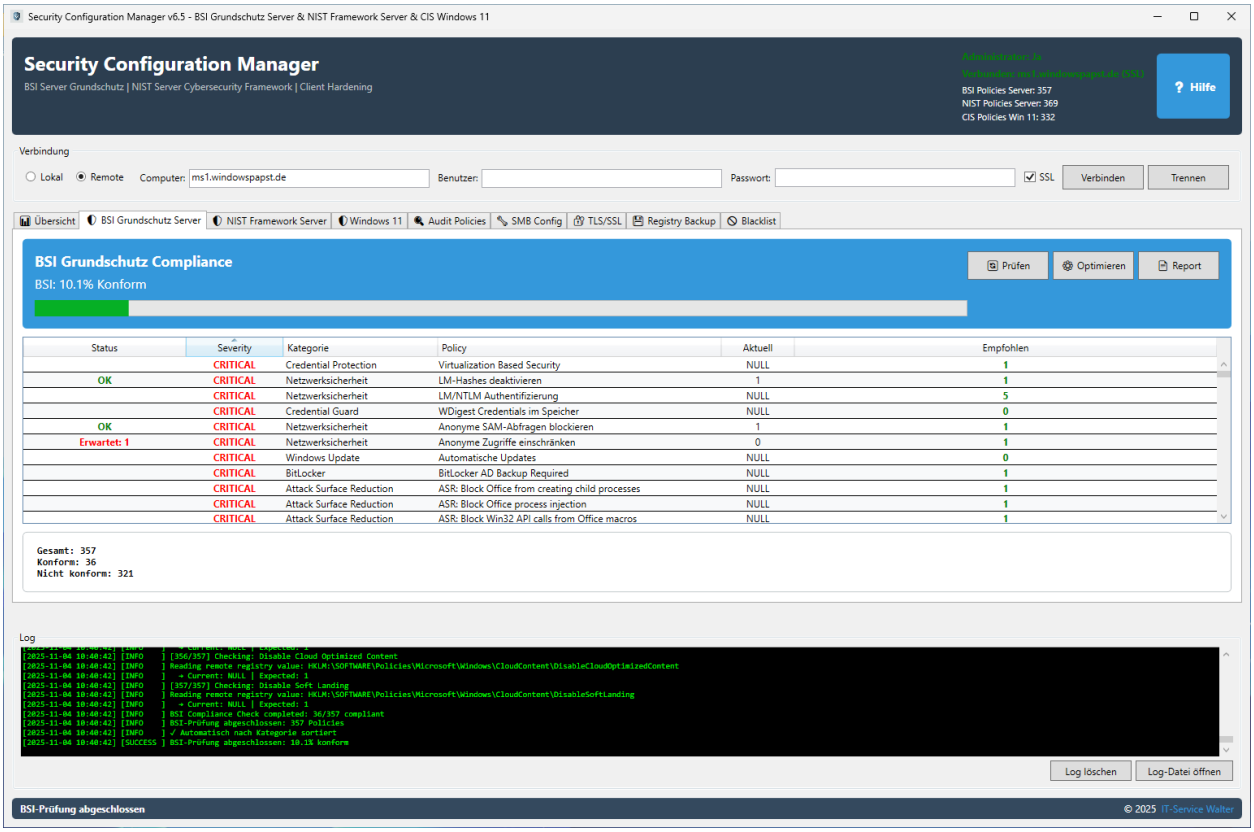
Dienste & Features

- 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

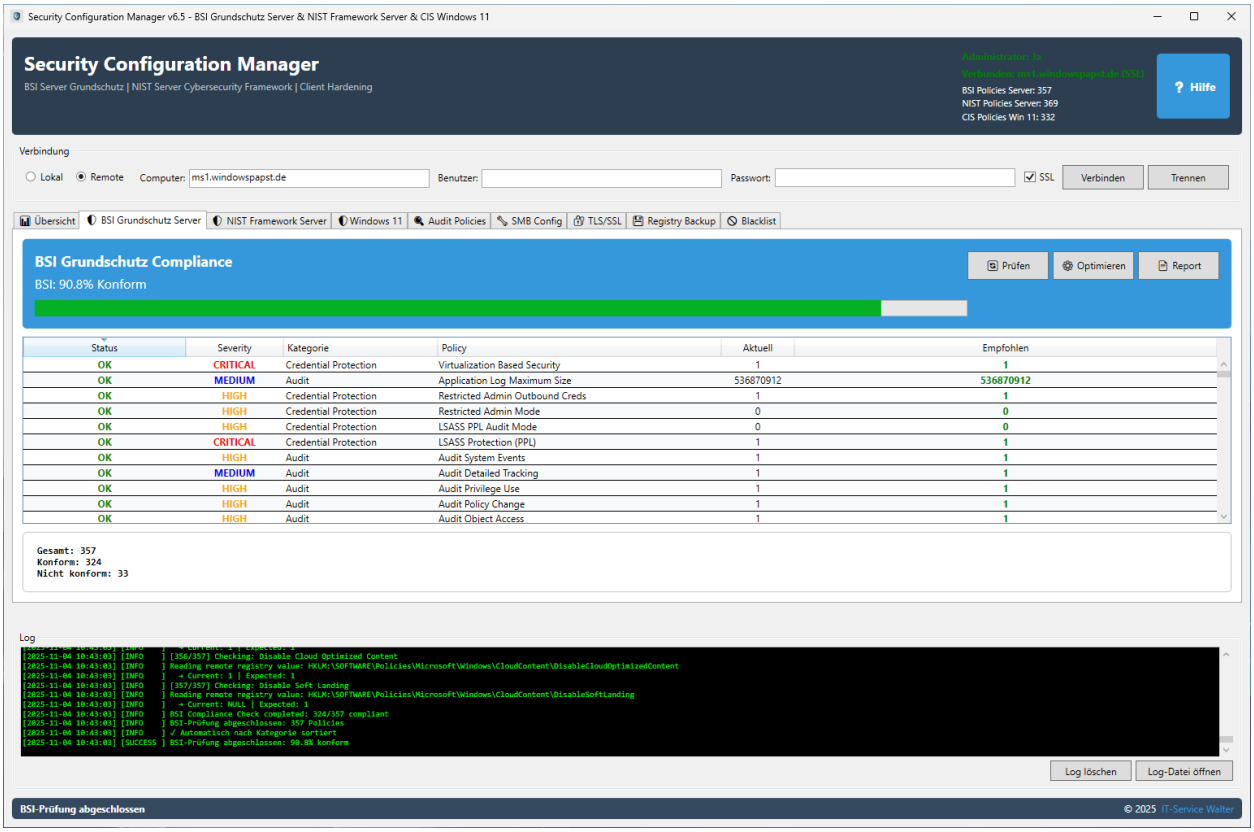


Optimierung durchführen

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:

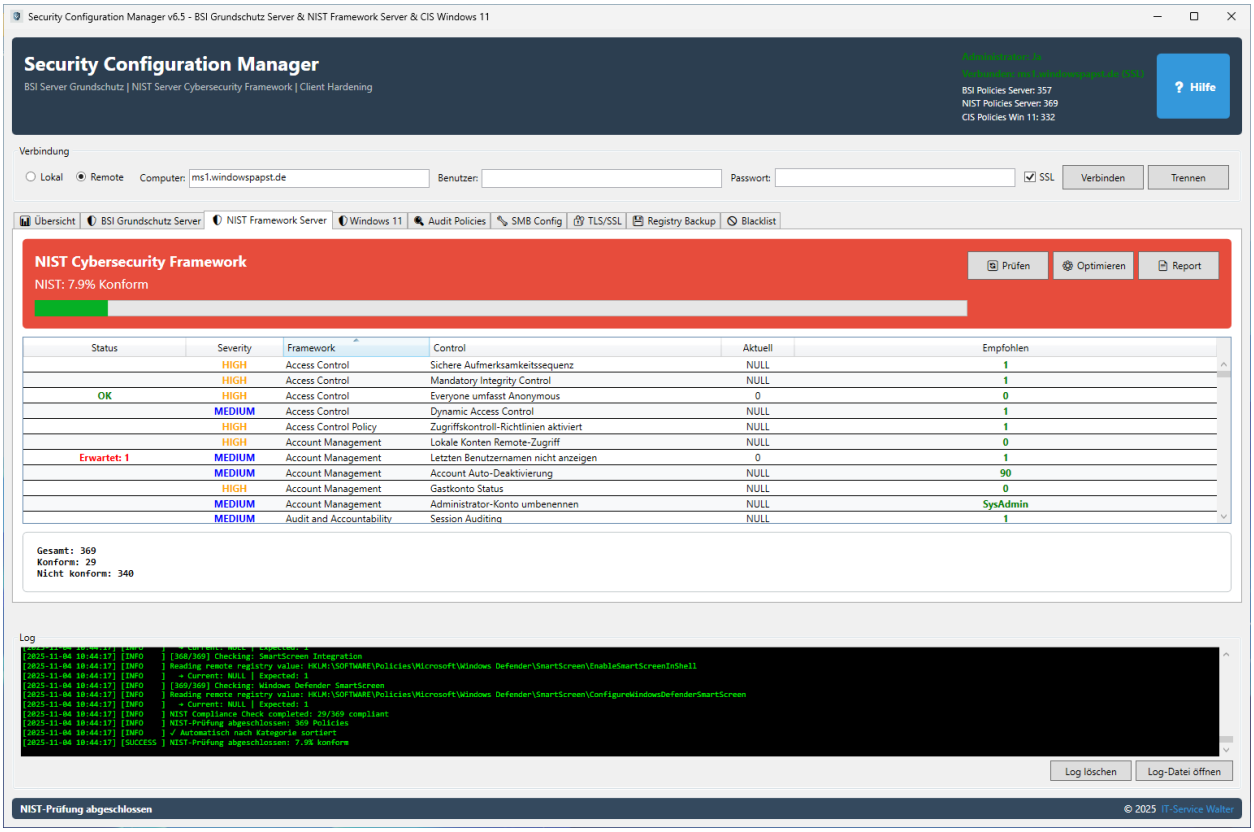
- 🔴 **CRITICAL**: Muss unbedingt umgesetzt werden
- 🟠 **HIGH**: Sehr wichtig für Sicherheit
- 🟡 **MEDIUM**: Empfohlen (optional inkludierbar)



NIST Cybersecurity Framework

Was wird geprüft?

Das NIST Framework ist der US-amerikanische Standard für Cybersecurity. Das Tool prüft **über 350 Controls** in Kategorien:



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

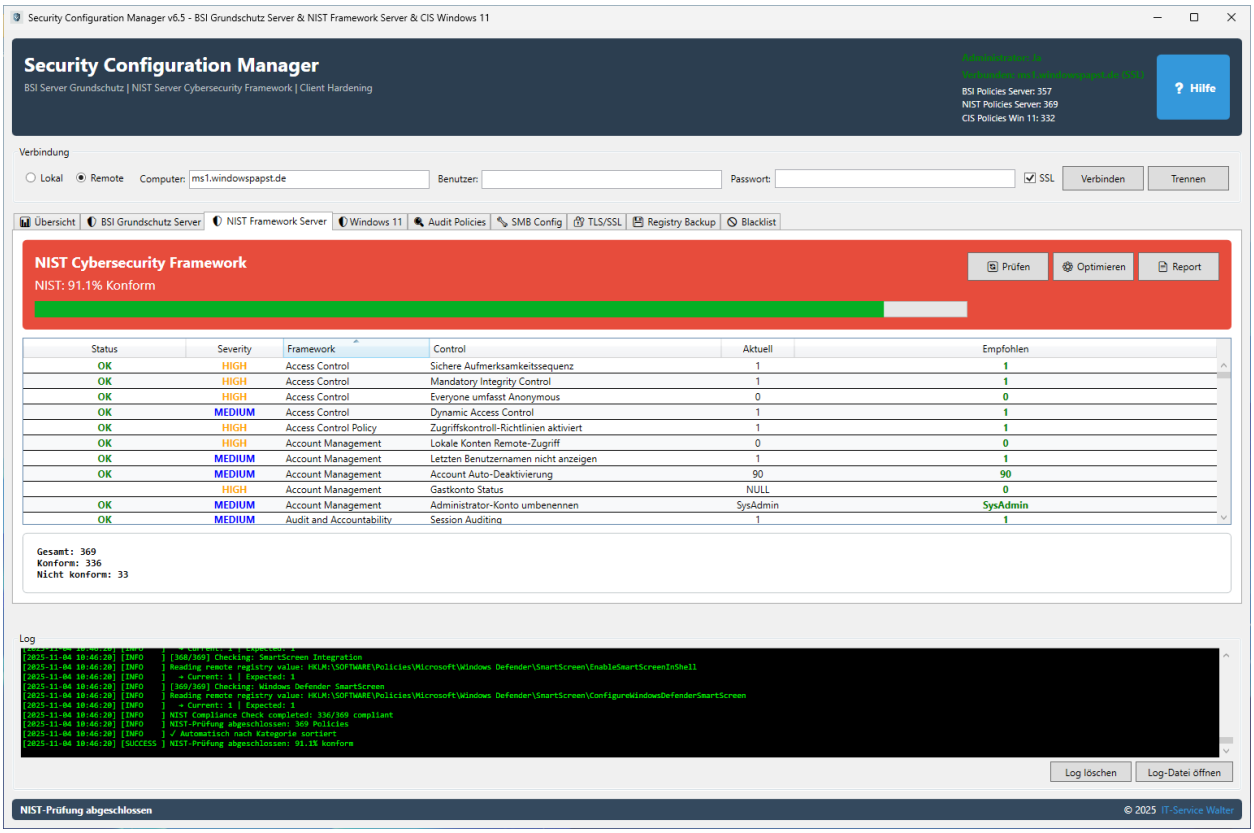
- BitLocker-Einstellungen
- EFS-Konfiguration

Attack Surface Reduction

- ASR Rules
- Exploit Protection
- Network Protection

Optimierung durchführen

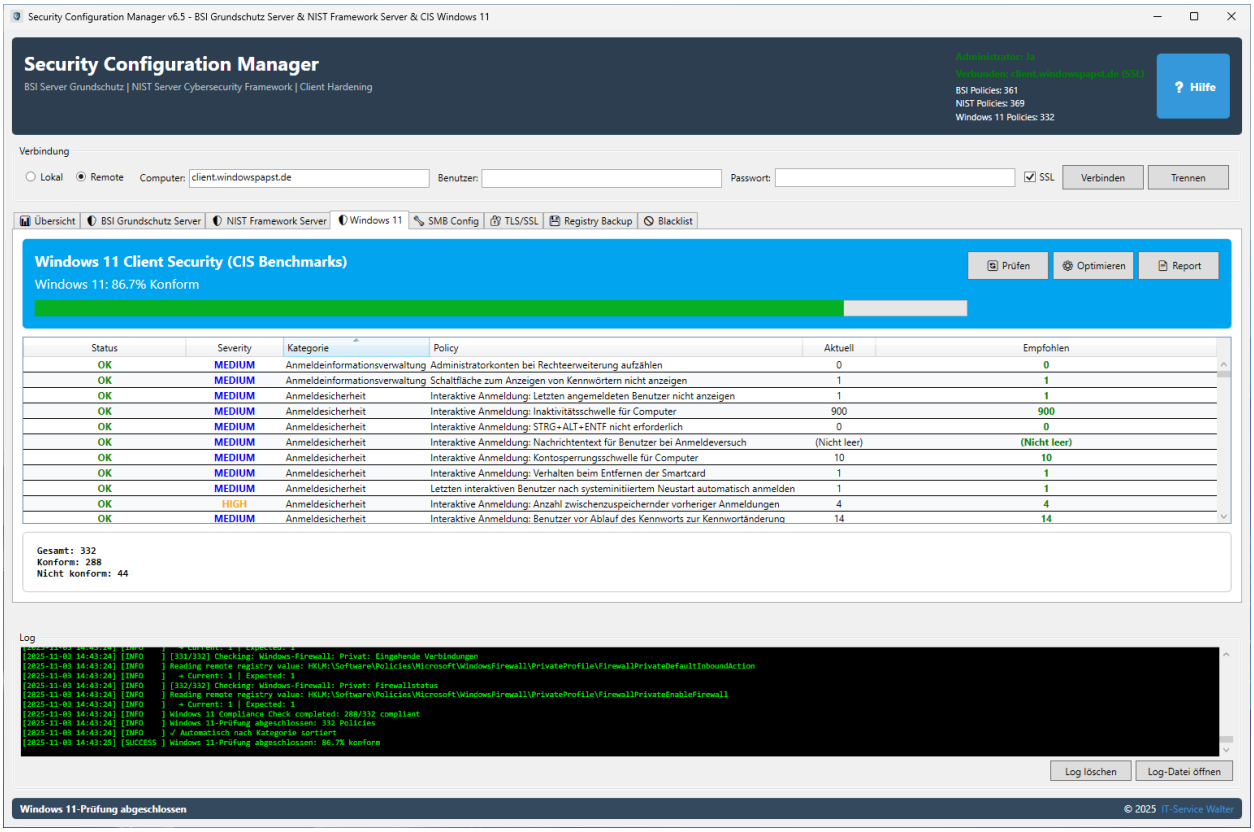
Analog zur BSI-Optimierung, mit NIST-spezifischen Controls.



Windows 11 CIS Benchmarks (Client Security)

Was sind CIS-Benchmarks?

Das Center for Internet Security (CIS) entwickelt weltweit anerkannte Sicherheitsstandards. Das Tool implementiert die CIS Microsoft Windows 11 Enterprise Benchmarks speziell für Client-Systeme.



Was wird konfiguriert?

Benutzerkontensteuerung (UAC)

- UAC-Verhalten für Administratoren
- UAC-Verhalten für Standardbenutzer
- Elevation-Prompts konfigurieren
- Secure Desktop für UAC-Prompts

Windows Defender & Firewall

- Defender Antivirus Konfiguration
- Windows Firewall Profile-Einstellungen
- SmartScreen-Konfiguration
- Exploit Guard Einstellungen

Anmeldesicherheit & Kennwörter

- Interaktive Anmelde-Richtlinien
- Kennwort-Komplexitätsanforderungen
- Kontosperrung-Richtlinien
- Cached Credentials Limits

Netzwerksicherheit

- SMB Client-Konfiguration
- LAN Manager Authentication Level
- Network Security Settings
- NTLM Security Settings

Windows Update & Apps

- Automatische Updates-Konfiguration
- Microsoft Store App-Richtlinien
- Windows Features On/Off
- Delivery Optimization

Remote Desktop & Administrative Tools

- Remote Desktop Services Konfiguration
- Terminal Services Einstellungen
- Windows Remote Management (WinRM)
- PowerShell Execution Policy

Optimierung durchführen

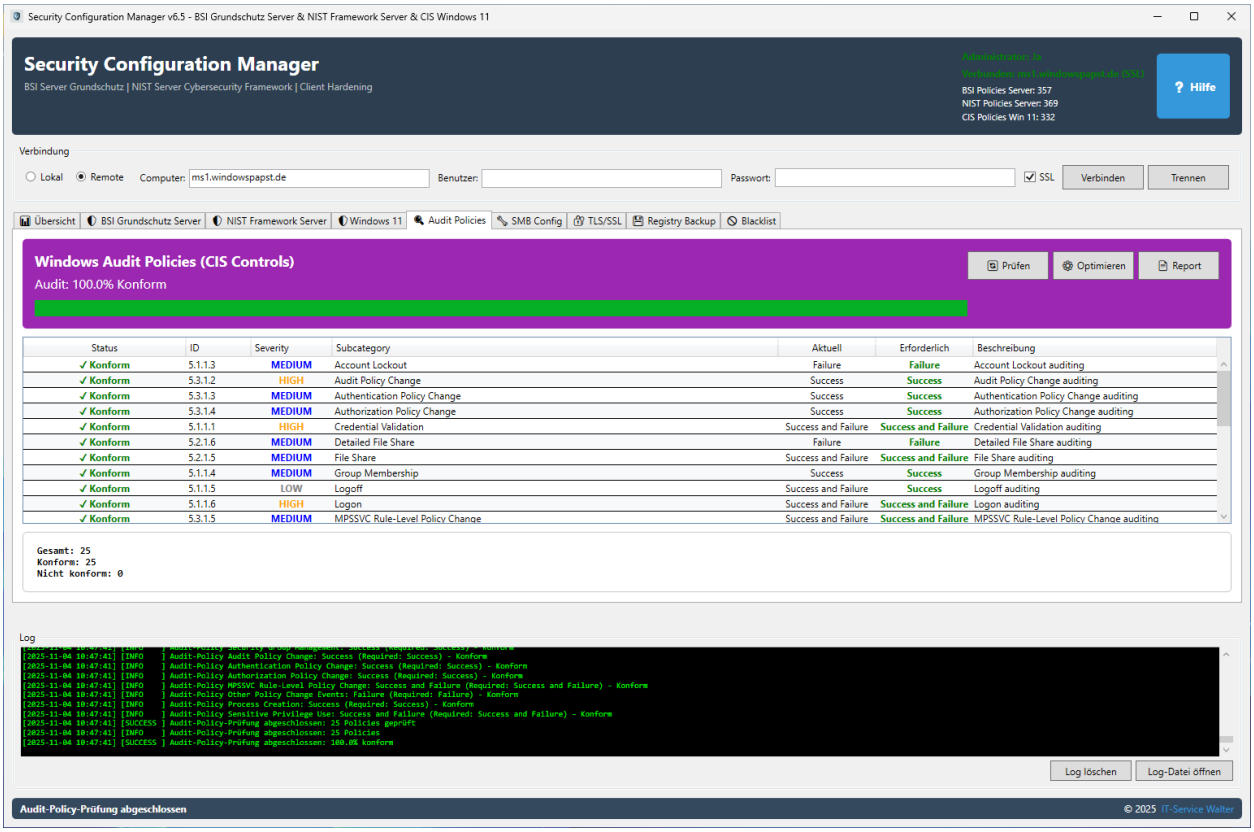
Die Windows 11 CIS-Optimierung wendet alle **CRITICAL, HIGH und MEDIUM** CIS-Benchmark-Einstellungen an. Diese sind speziell auf Client-Systeme ausgelegt und berücksichtigen die Benutzerfreundlichkeit.

1. Klick auf "Windows 11 Optimieren"
2. Bestätigung der Sicherheitsabfrage
3. Automatische Anwendung aller CIS-Benchmark-Einstellungen
4. Detailliertes Logging und Erfolgsstatistik

Audit Policies Management (Logging & Monitoring)

Was sind Audit Policies?

Windows Audit Policies steuern, welche Sicherheitsereignisse in den Event Logs protokolliert werden. Das Tool implementiert die CIS-Benchmark-Empfehlungen für Audit Policies, um eine umfassende Sicherheitsüberwachung zu gewährleisten.



Warum sind Audit Policies wichtig?

- **Compliance-Anforderungen:** ISO 27001, SOX, HIPAA, DSGVO
- **Incident Response:** Forensische Analyse nach Sicherheitsvorfällen
- **Threat Detection:** Früherkennung von Angriffsversuchen
- **Administrative Überwachung:** Monitoring privilegierter Aktivitäten

Überwachte Audit-Kategorien

Account Logon Events

- Credential Validation (Success/Failure)
- Kerberos Authentication Service
- Kerberos Service Ticket Operations
- Other Account Logon Events

Account Management

- User Account Management (Success/Failure)
- Computer Account Management
- Security Group Management
- Distribution Group Management
- Application Group Management

Logon/Logoff Events

- Logon (Success/Failure)
- Logoff (Success)
- Account Lockout (Failure)
- Special Logon (Success)

Object Access

- File System Access (Success/Failure)
- Registry Access (Success/Failure)
- Handle Manipulation
- Central Policy Staging
- Removable Storage

Policy Change

- Audit Policy Change (Success)
- Authentication Policy Change (Success)
- Authorization Policy Change (Success)
- MPSSVC Rule-Level Policy Change

Privilege Use

- Sensitive Privilege Use (Success/Failure)
- Non Sensitive Privilege Use
- Other Privilege Use Events

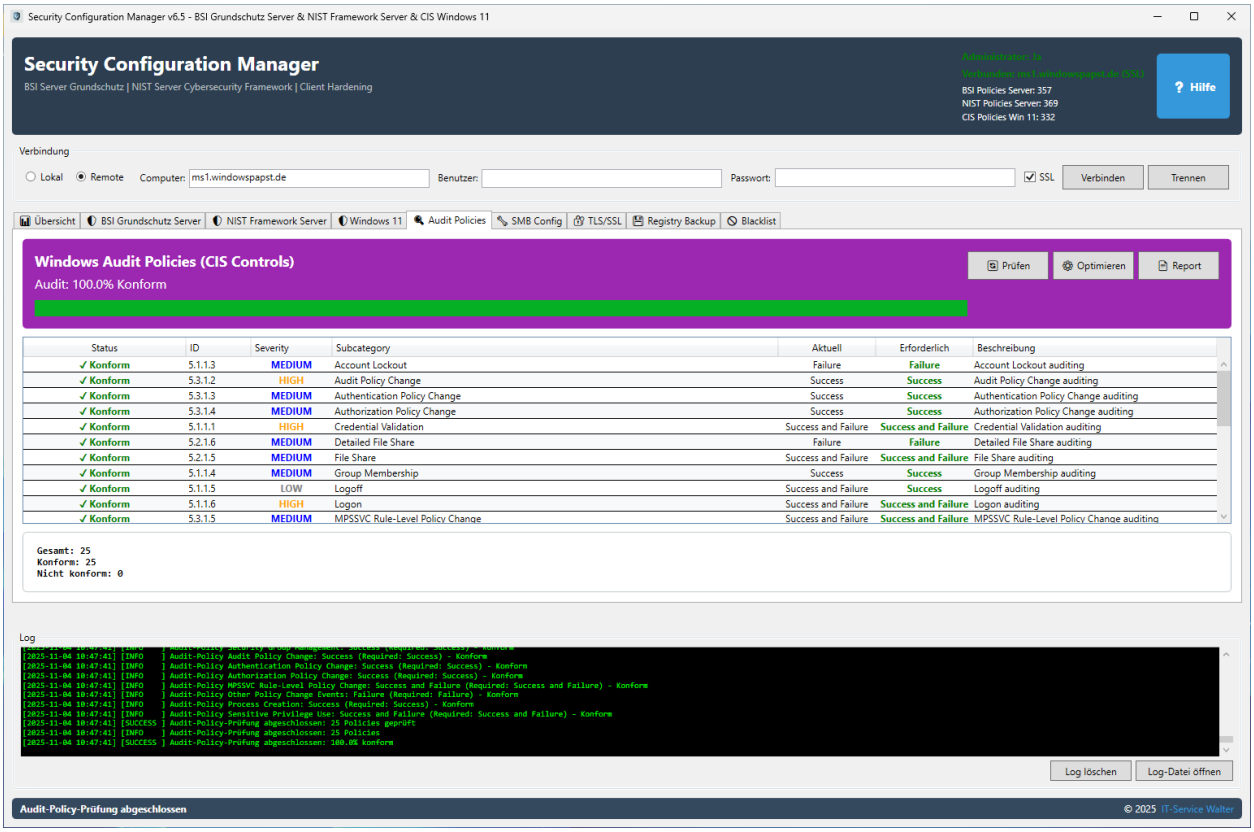
System Events

- Security State Change (Success)
- Security System Extension (Success)
- System Integrity (Success/Failure)
- IPSec Driver (Success/Failure)

Audit-Optimierung durchführen

Die Audit-Policy-Optimierung konfiguriert alle Audit-Einstellungen nach CIS-Benchmark-Empfehlungen. Dies stellt sicher, dass alle sicherheitsrelevanten Ereignisse ordnungsgemäß protokolliert werden.

1. Klick auf "Audit Policies Prüfen"
2. Überprüfung aller Audit-Kategorien
3. Klick auf "Audit Policies Optimieren"
4. Automatische Konfiguration nach CIS-Standards
5. Erfolgsbestätigung und Detailstatistik



Performance-Überlegungen

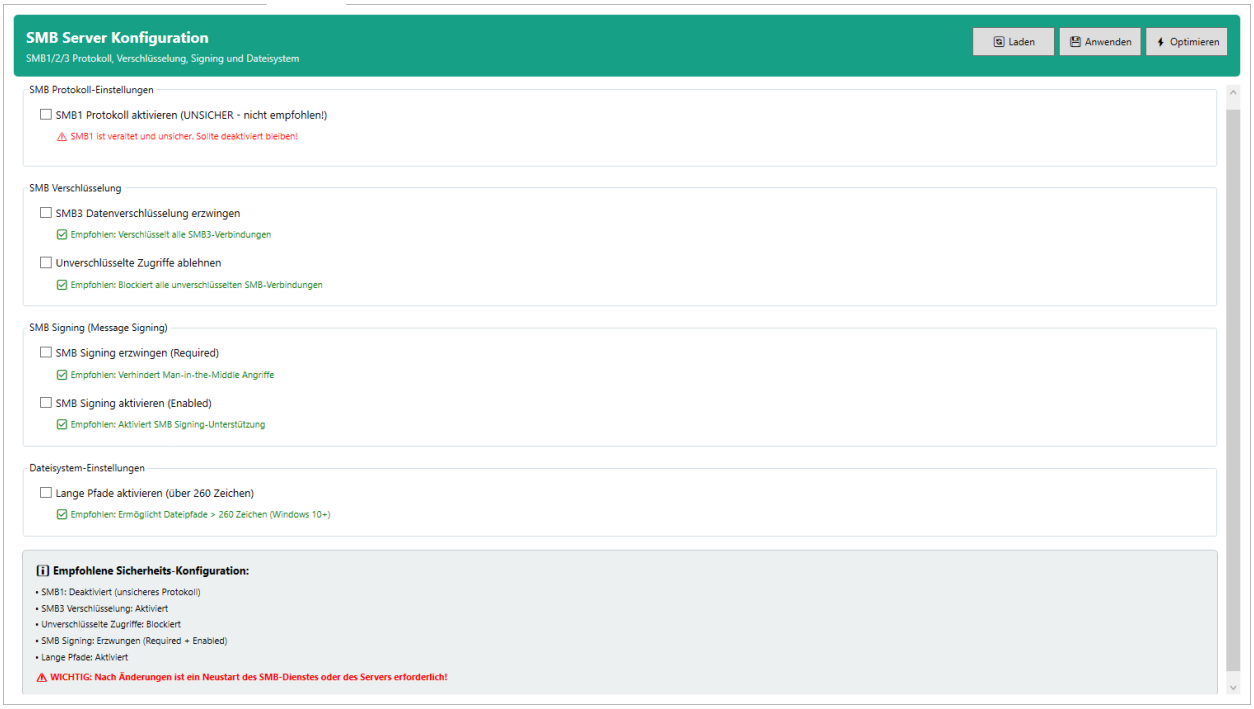
Wichtig: Audit Policies erzeugen Event-Log-Einträge und können bei sehr hoher Last das System minimal belasten. Die CIS-Empfehlungen sind jedoch auf ein ausgewogenes Verhältnis zwischen Sicherheit und Performance ausgelegt.

- Minimaler Performance-Impact auf modernen Systemen
- Automatische Log-Rotation verhindert Speicherprobleme
- Fokus auf sicherheitskritische Events

SMB (Server Message Block) Konfiguration

Was ist SMB?

SMB ist das Protokoll für Windows-Dateifreigaben und Netzwerkkommunikation.



Konfigurierbare Einstellungen

Einstellung	Beschreibung	Empfehlung
SMB1 Protokoll	Veraltetes, unsicheres Protokoll	❌ Deaktiviert
SMB3 Verschlüsselung	Ende-zu-Ende-Verschlüsselung	✅ Aktiviert

Einstellung	Beschreibung	Empfehlung
SMB Signing	Digitale Signaturen	✅ Erzwungen
Unverschlüsselte Zugriffe blockieren	Nur verschlüsselte Verbindungen	✅ Aktiviert
Long Paths	Pfade >260 Zeichen	✅ Aktiviert

Bedienung

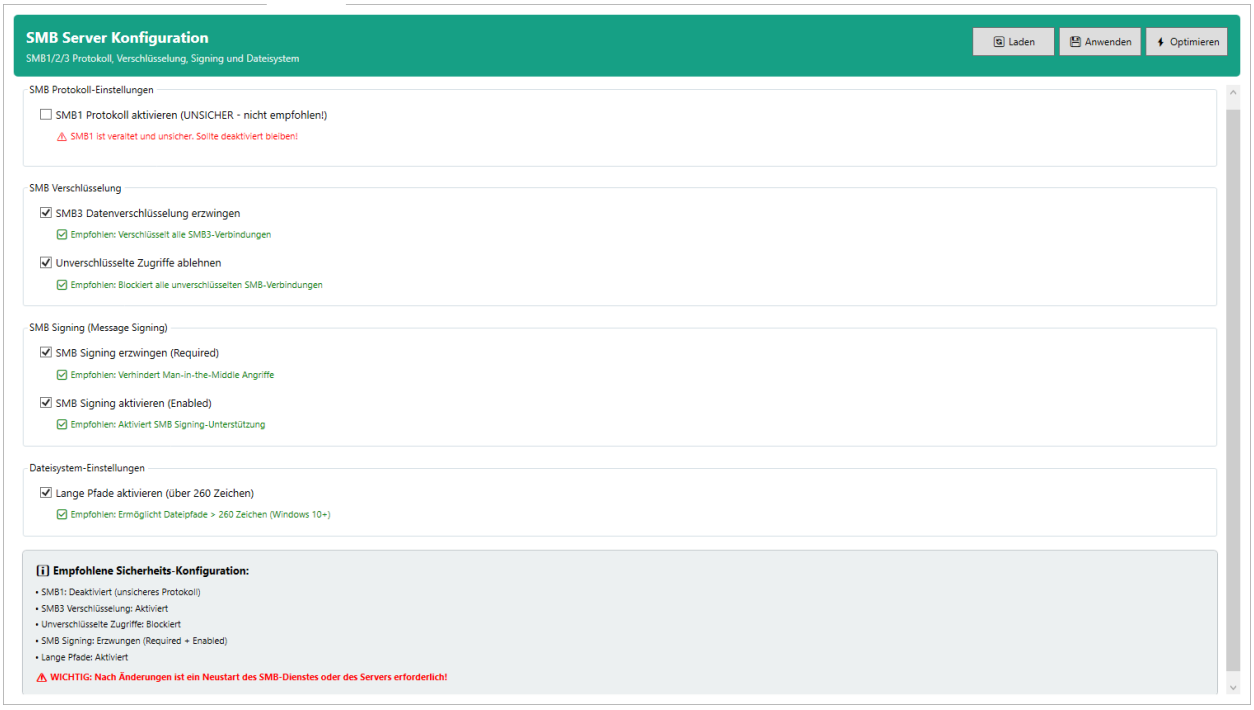
Tab "SMB-Konfiguration"

→ "Aktualisieren" = Aktuelle Einstellungen lesen

→ Checkboxen anpassen

→ "Anwenden" = Einstellungen speichern

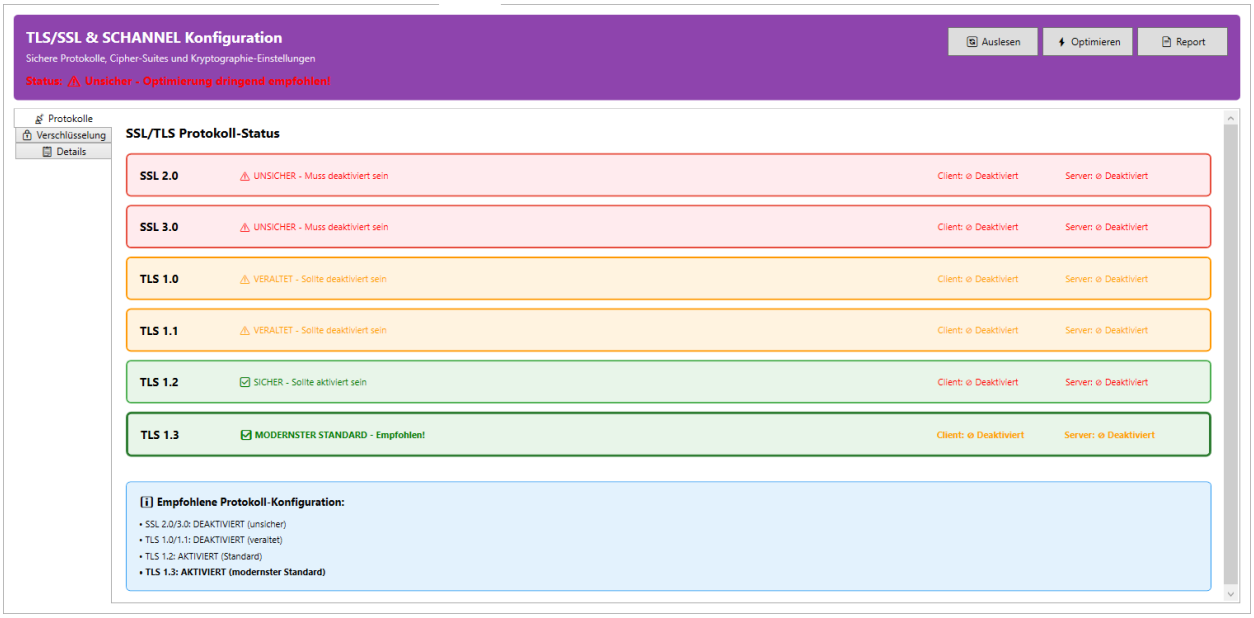
→ "Optimieren" = Sichere Standardkonfiguration



TLS/SSL Konfiguration

Warum ist TLS/SSL wichtig?

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



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

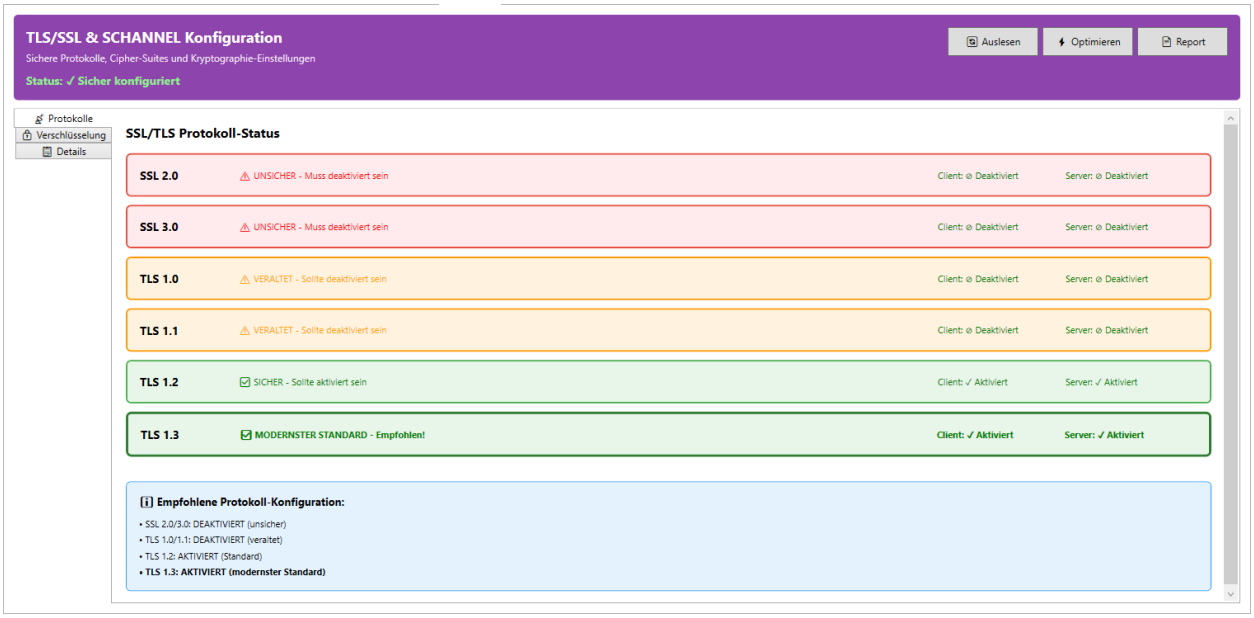
Tab "TLS/SSL"

→ "Status laden" = Aktuelle Konfiguration anzeigen

→ Detaillierter Report mit Sicherheitsbewertung

→ "Optimieren" = Sichere TLS 1.3 Konfiguration

→ "Report exportieren" = HTML/TXT Report speichern

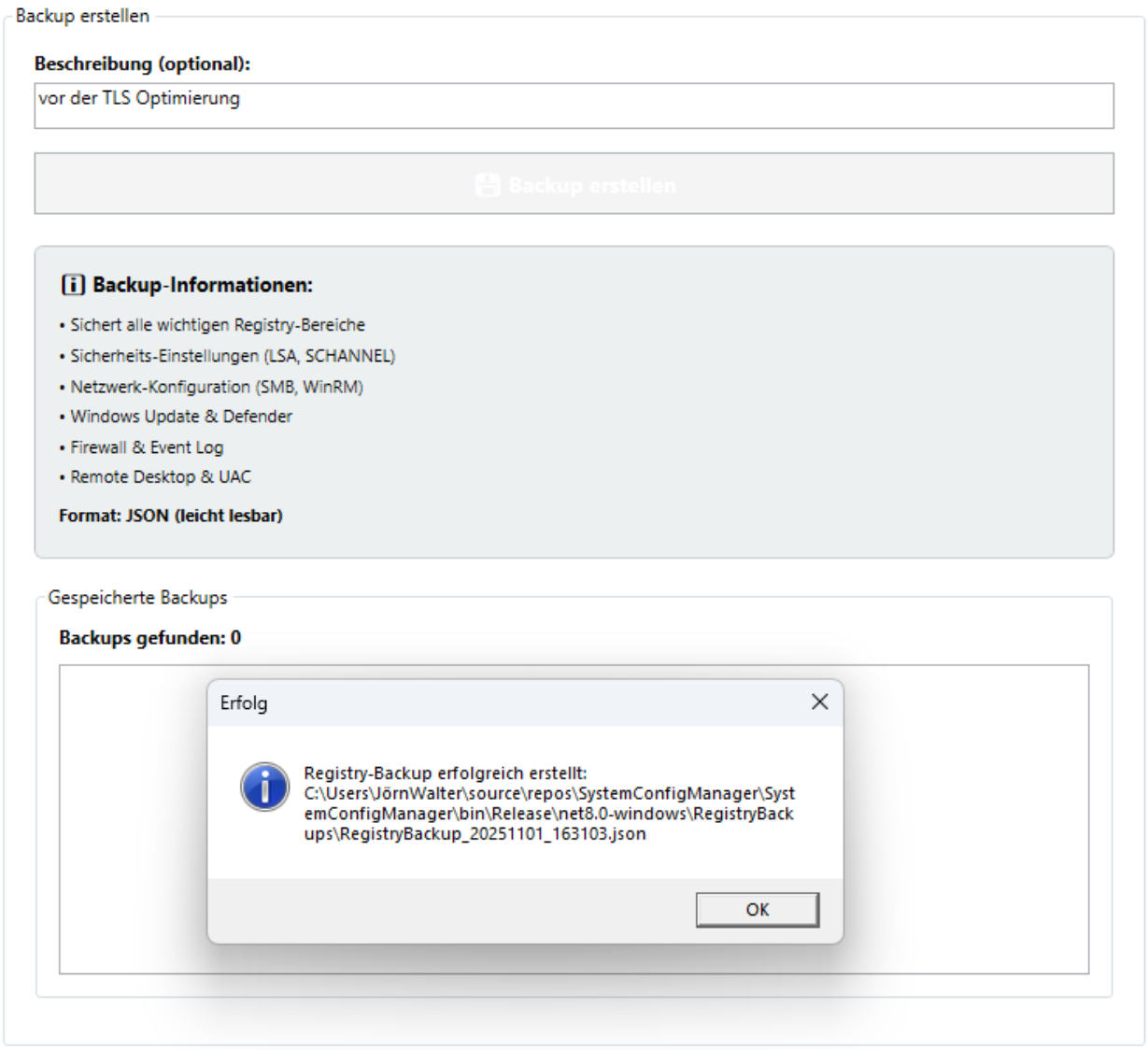


⚠️ **WICHTIG**: Nach TLS-Optimierung ist ein **Neustart erforderlich**!

Registry Backup & Recovery

Warum Backups?

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



Funktionen

Backup erstellen:

Tab "Registry Backup"

→ Beschreibung eingeben (optional)

→ "Backup erstellen"

→ JSON-Datei wird gespeichert

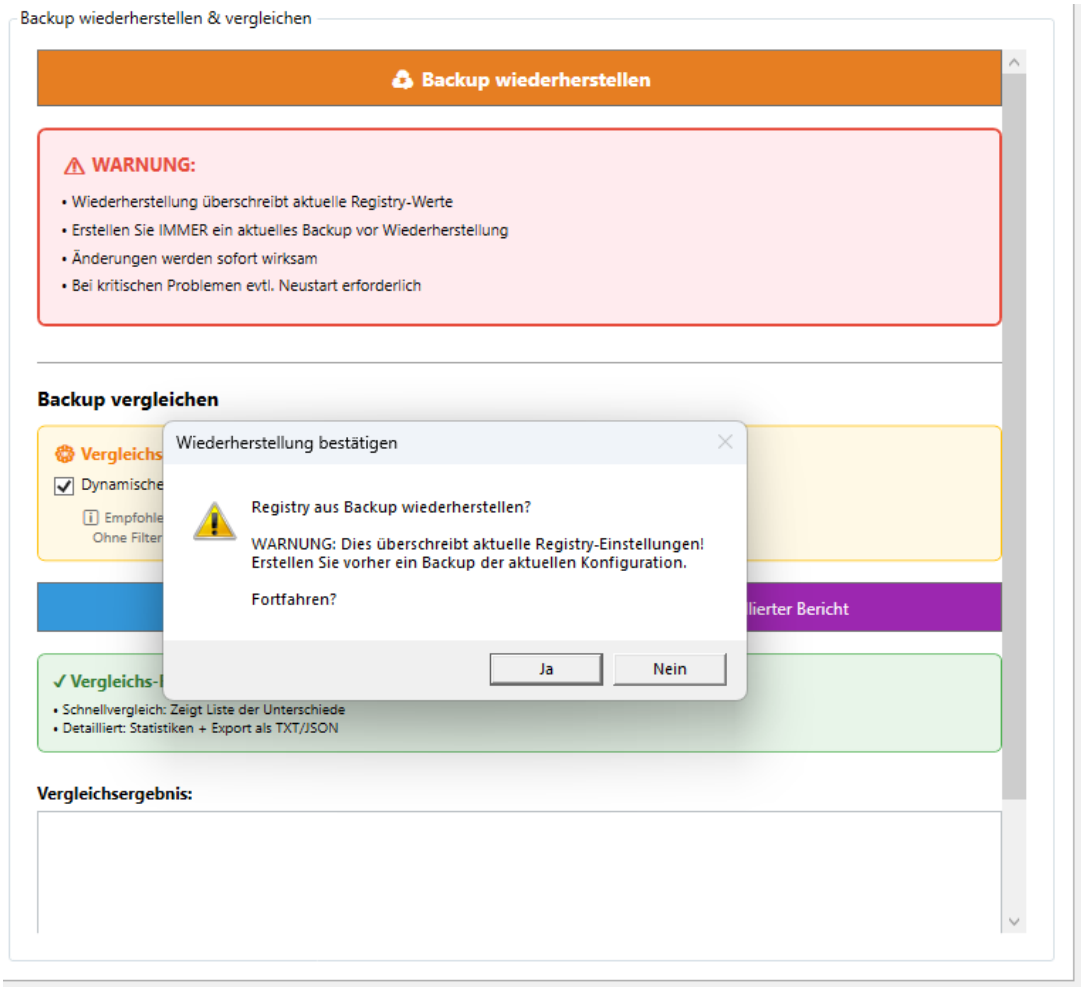
Backup wiederherstellen:

→ "Wiederherstellen" klicken

→ Backup-Datei auswählen

→ Bestätigung

→ Registry wird wiederhergestellt



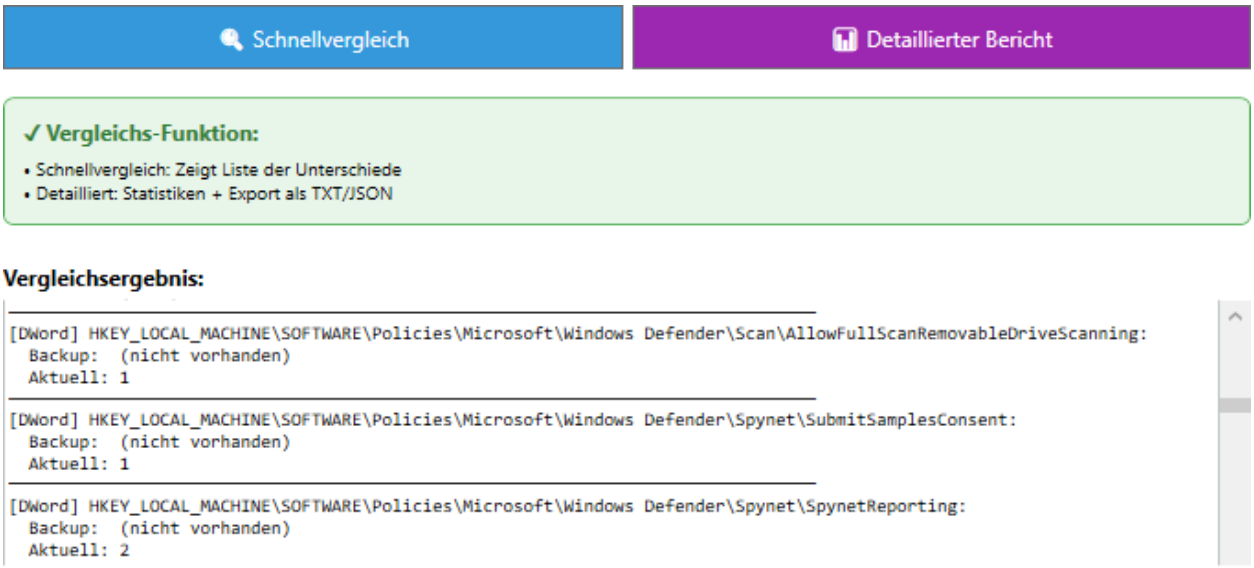
Backup vergleichen:

→ "Vergleichen" klicken

→ Backup-Datei auswählen

→ Zeigt Unterschiede zwischen aktuellem System und Backup

→ Option: Dynamische Werte ignorieren (empfohlen)



Detaillierter Vergleich:

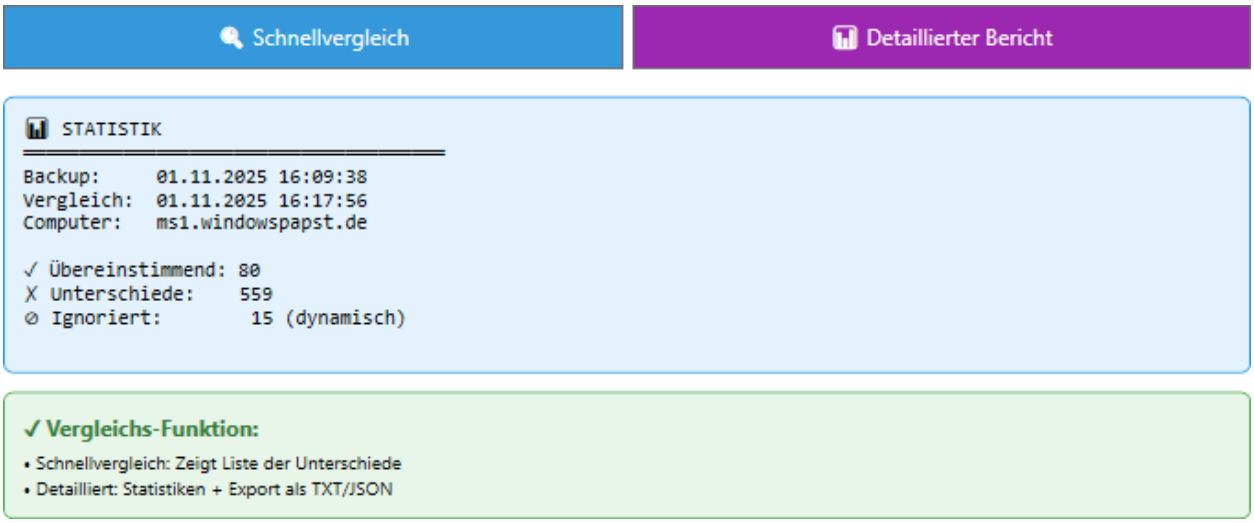
→ "Detaillierter Bericht" klicken

→ Statistik mit genauen Zahlen

→ Auflistung aller Unterschiede

→ Fehlerprotokoll

→ Export als TXT oder JSON möglich



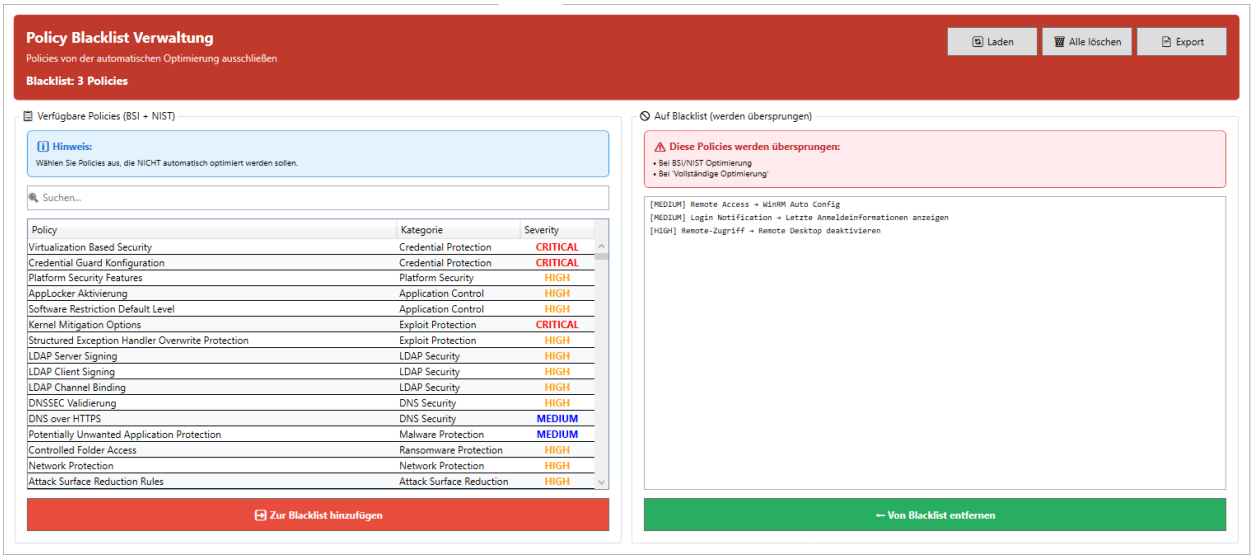
Dynamische Werte

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

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.



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

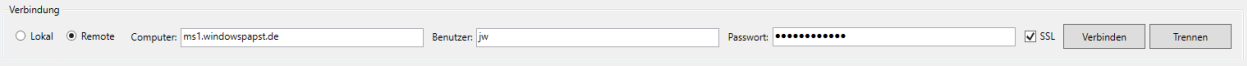
Persistenz

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

9. 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

10. 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

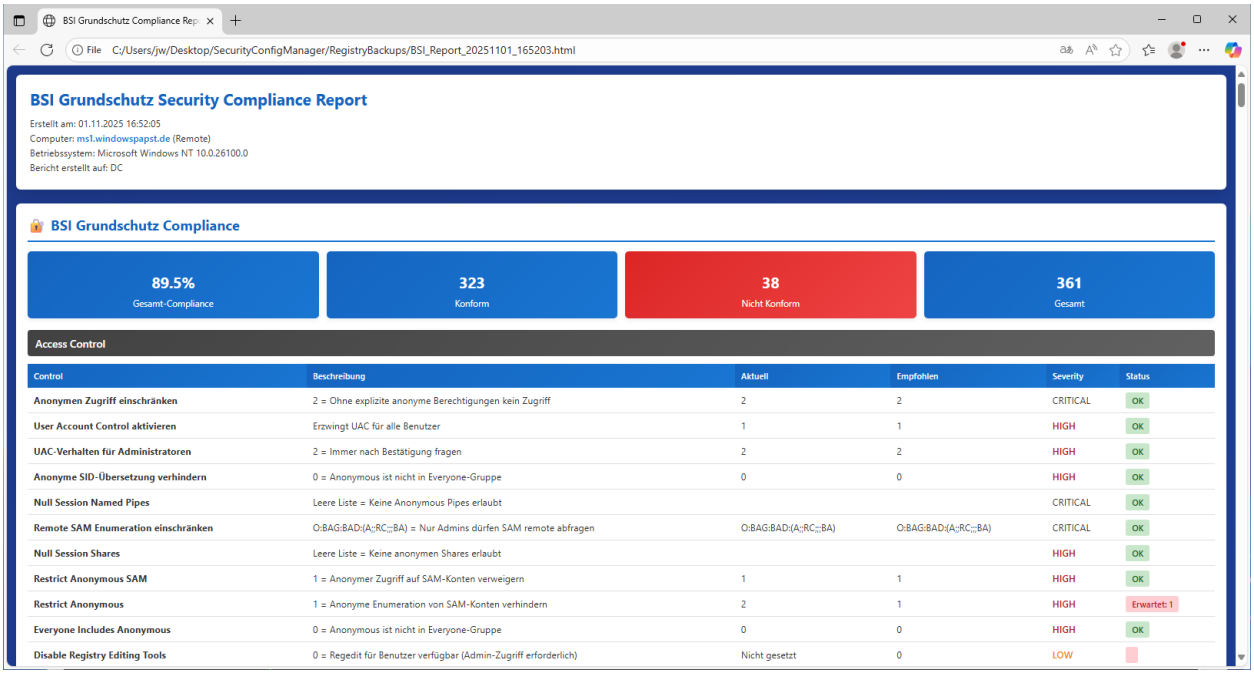
→ "Gesamtreport" = Erstellt HTML-Report

→ Report wird im Browser geöffnet

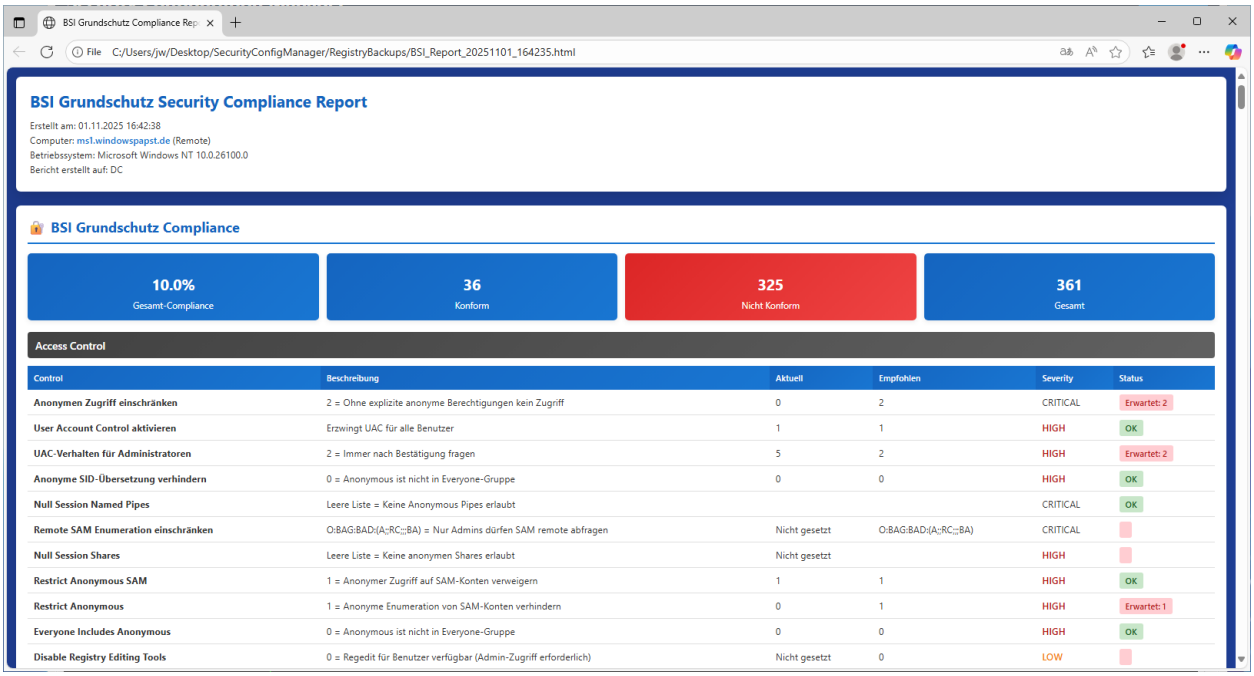
Report-Inhalt

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

Vor einer Optimierung:



Nach einer Optimierung:



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 Grundschutz 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

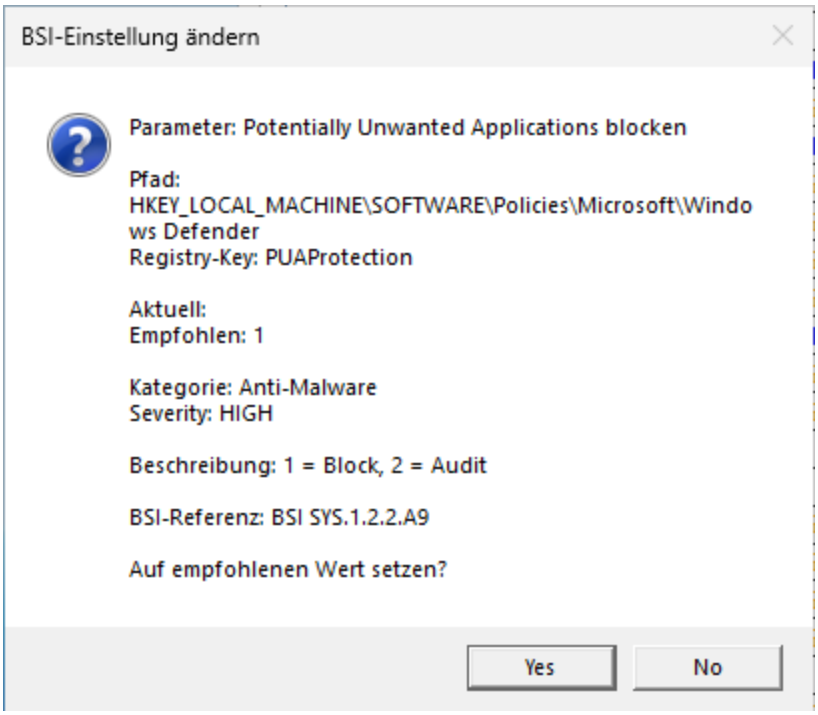
Unterer Bereich:

- 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 ✗ 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 Grundschutz: 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 fehlschlugen
- 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: 6.0
Lizenz: Kommerziell
Support: support@it-service-walter.com

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.

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

Verkauf

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