WINRM MANAGEMENT TOOL

IT-Service Walter

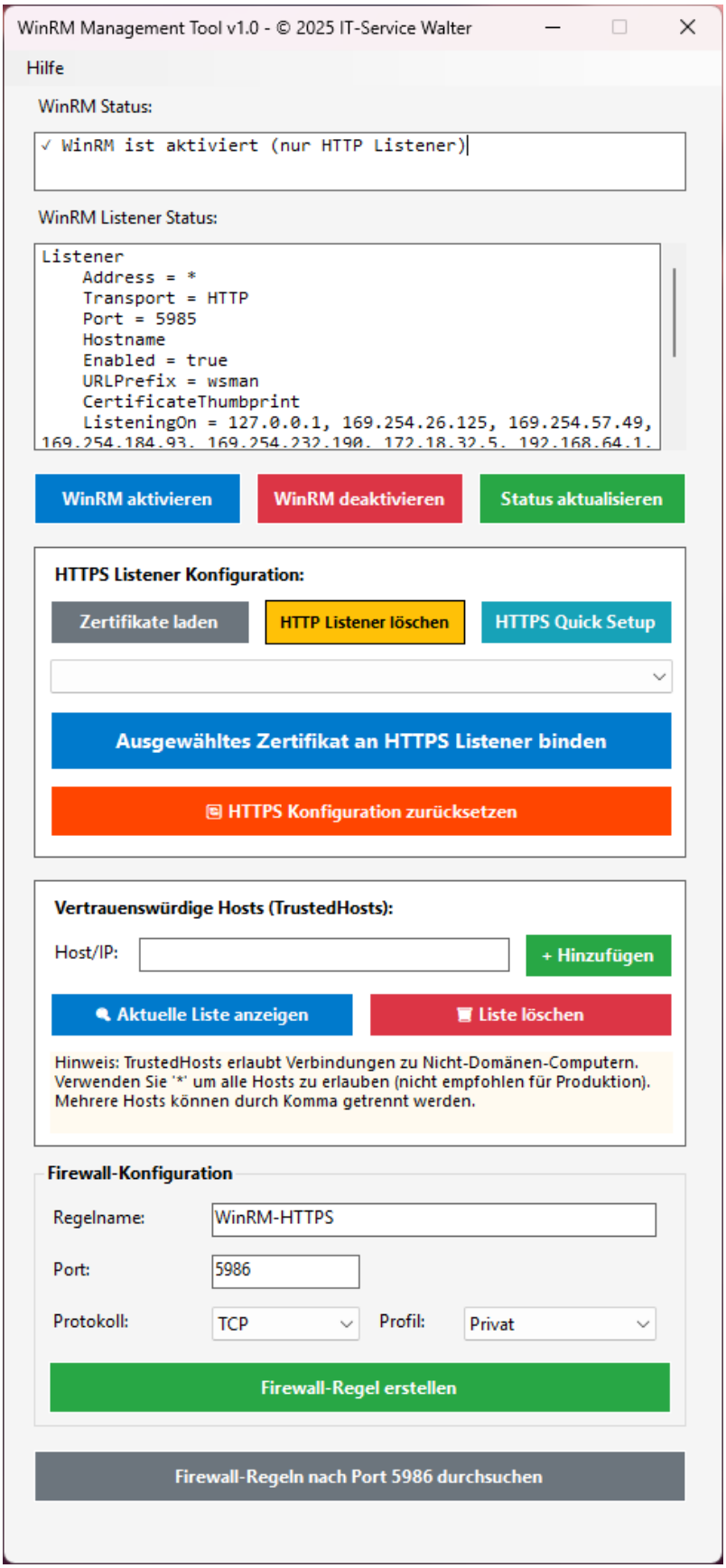
Jörn Walter
www.it-service-walter.com
06.10.2025

WINRM MANAGEMENT TOOL V1.0 ÜBERBLICK

DAS WINRM MANAGEMENT TOOL IST EINE GRAFISCHE BENUTZEROBERFLÄCHE ZUR VERWALTUNG DER WINDOWS REMOTE MANAGEMENT (WINRM) KONFIGURATION. ES ERMÖGLICHT DIE EINFACHE EINRICHTUNG UND VERWALTUNG VON WINRM-DIENSTEN, HTTPS-LISTENERN, ZERTIFIKATBINDUNGEN UND FIREWALL-REGELN OHNE DIE VERWENDUNG VON KOMMANDOZEILEN-BEFEHLEN.

WinRM Management Tool v1.0 - Benutzerhandbuch

Inhaltsverzeichnis


WinRM Management Tool v1.0 - © 2025 IT-Service Walter
Hilfe
WinRM Status:
✓ WinRM ist aktiviert (nur HTTP Listener)
WinRM Listener Status:
Listener
Address = *
Transport = HTTP
Port = 5985
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 169.254.26.125, 169.254.57.49,
169.254.184.93, 169.254.232.190, 172.18.32.5, 192.168.64.1,
WinRM aktivieren
WinRM deaktivieren
Status aktualisieren
HTTPS Listener Konfiguration:
Zertifikate laden
HTTP Listener löschen
HTTPS Quick Setup
Ausgewähltes Zertifikat an HTTPS Listener binden
HTTPS Konfiguration zurücksetzen
Vertrauenswürdige Hosts (TrustedHosts):
Host/IP:
+ Hinzufügen
Aktuelle Liste anzeigen
Liste löschen
Hinweis: TrustedHosts erlaubt Verbindungen zu Nicht-Domänen-Computern.
Verwenden Sie '*' um alle Hosts zu erlauben (nicht empfohlen für Produktion).
Mehrere Hosts können durch Komma getrennt werden.
Firewall-Konfiguration
Regelname:
WinRM-HTTPS
Port:
5986
Protokoll:
TCP
Profil:
Privat
Firewall-Regel erstellen
Firewall-Regeln nach Port 5986 durchsuchen

1. Einführung

Das WinRM Management Tool ist eine grafische Benutzeroberfläche zur Verwaltung der Windows Remote Management (WinRM) Konfiguration. Es ermöglicht die einfache Einrichtung und Verwaltung von WinRM-Diensten, HTTPS-Listenern, Zertifikatbindungen und Firewall-Regeln ohne die Verwendung von Kommandozeilen-Befehlen.

Hauptmerkmale

- WinRM-Dienstverwaltung mit einem Klick
- HTTPS-Listener-Konfiguration mit Zertifikatbindung
- TrustedHosts-Verwaltung für Nicht-Domänen-Computer
- Automatische Firewall-Regelkonfiguration
- Übersichtliche Status-Anzeige aller WinRM-Komponenten

2. Systemanforderungen

- **Betriebssystem**: Windows 10/11 oder Windows Server 2016/2019/2022
- **Berechtigungen**: Administratorrechte (zwingend erforderlich)
- **.NET Framework**: Version 4.7 oder höher
- **PowerShell**: Version 5.0 oder höher
- **WinRM**: Muss auf dem System installiert sein (standardmäßig vorhanden)

3. Installation und Start

Installation

Das Tool benötigt keine Installation. Es handelt sich um eine portable Anwendung.

Programmstart

1. **Als Administrator ausführen** (Rechtsklick → "Als Administrator ausführen")
2. Bei UAC-Abfrage mit "Ja" bestätigen
3. Das Hauptfenster öffnet sich mit automatischer Statusprüfung

Wichtig: Ohne Administratorrechte können keine Änderungen vorgenommen werden!

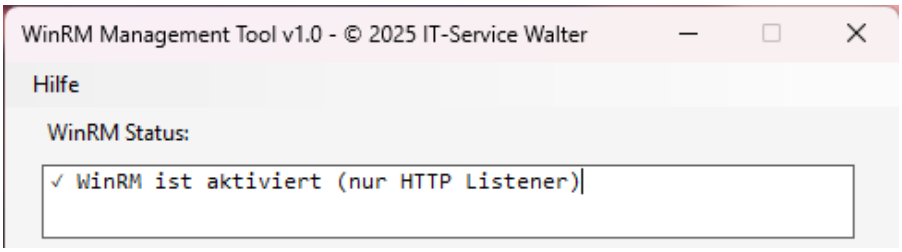
4. Hauptfunktionen

4.1 WinRM Status-Bereich

Statusanzeige

Der obere Bereich zeigt den aktuellen WinRM-Status:

- ✓ **WinRM ist aktiviert**: Dienst läuft
- ✗ **WinRM ist deaktiviert**: Dienst ist gestoppt
- Zusätzliche Informationen über konfigurierte Listener (HTTP/HTTPS)

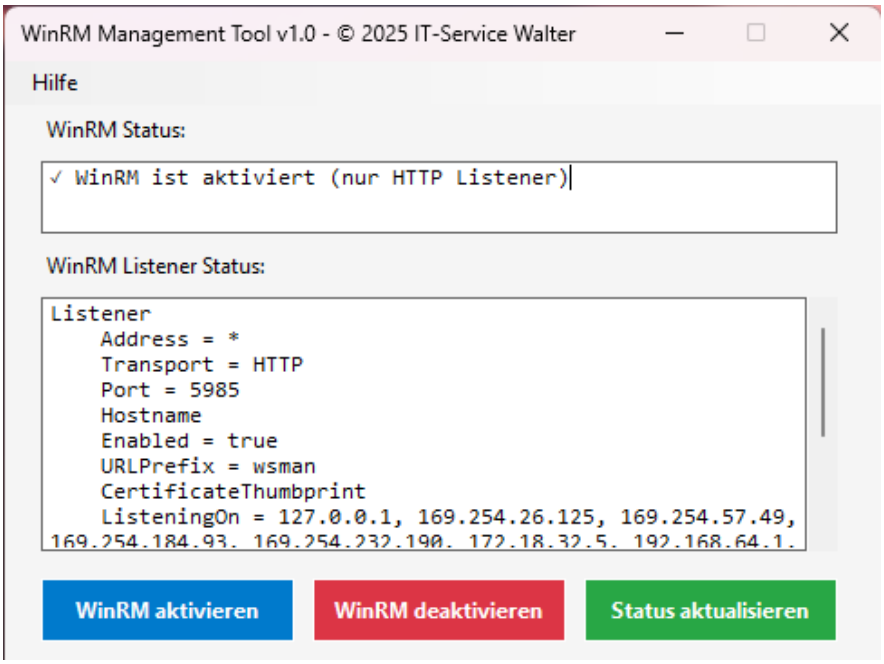


WinRM aktivieren

- **Funktion**: Startet den WinRM-Dienst
- **Verwendung**: Klick auf "WinRM aktivieren"
- **Resultat**: WinRM-Dienst wird gestartet und auf "Automatisch" gesetzt

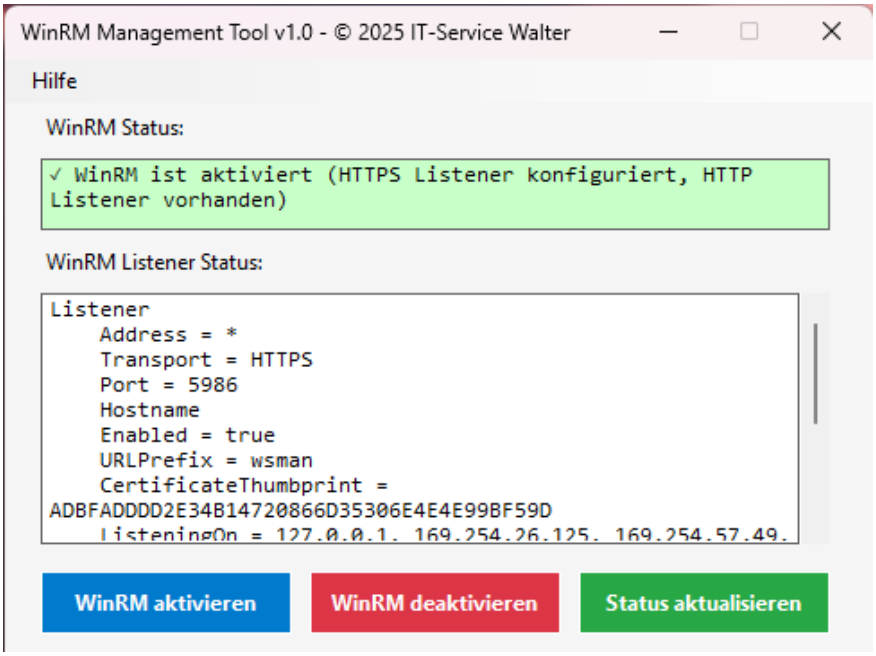
WinRM deaktivieren

- **Funktion**: Stoppt den WinRM-Dienst
- **Verwendung**: Klick auf "WinRM deaktivieren"
- **Resultat**: WinRM-Dienst wird beendet



Status aktualisieren

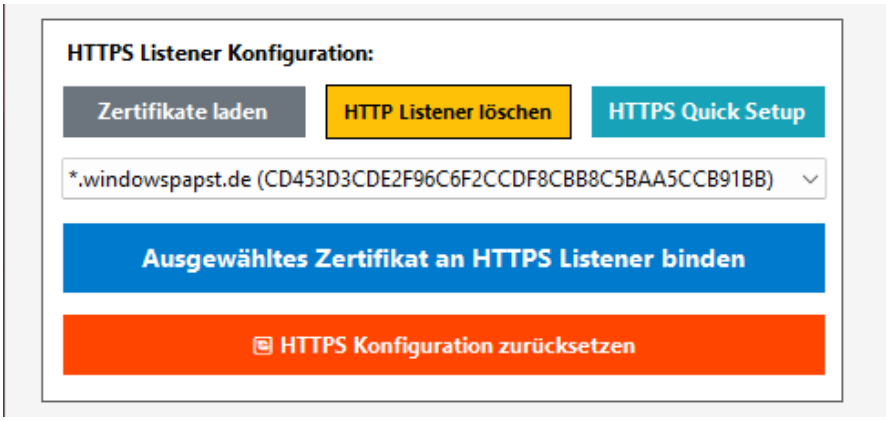
- **Funktion**: Aktualisiert die Anzeige aller WinRM-Listener
- **Verwendung**: Klick auf "Status aktualisieren"
- **Resultat**: Zeigt aktuelle Listener-Konfiguration im Textfeld



4.2 HTTPS Listener Konfiguration

Zertifikate laden

- **Funktion**: Lädt alle verfügbaren Server-Authentifizierungs-Zertifikate
- **Voraussetzung**: Zertifikate müssen im lokalen Maschinenspeicher vorhanden sein
- **Filterung**: Nur Zertifikate mit EKU "Server Authentication" werden angezeigt

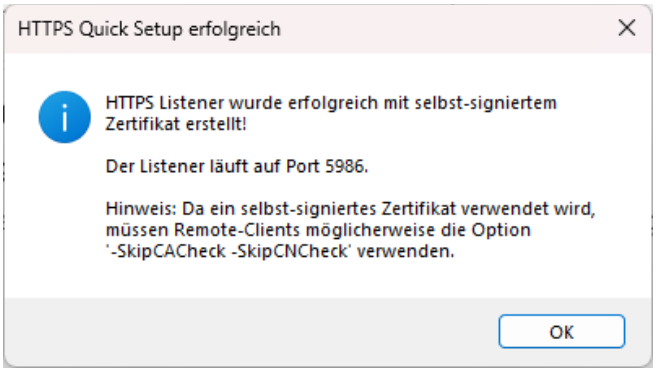


HTTP Listener löschen

- **Funktion**: Entfernt den unsicheren HTTP-Listener (Port 5985)
- **Verwendung**: Für reine HTTPS-Umgebungen
- **Warnung**: Nach dem Löschen ist nur noch HTTPS-Verbindung möglich

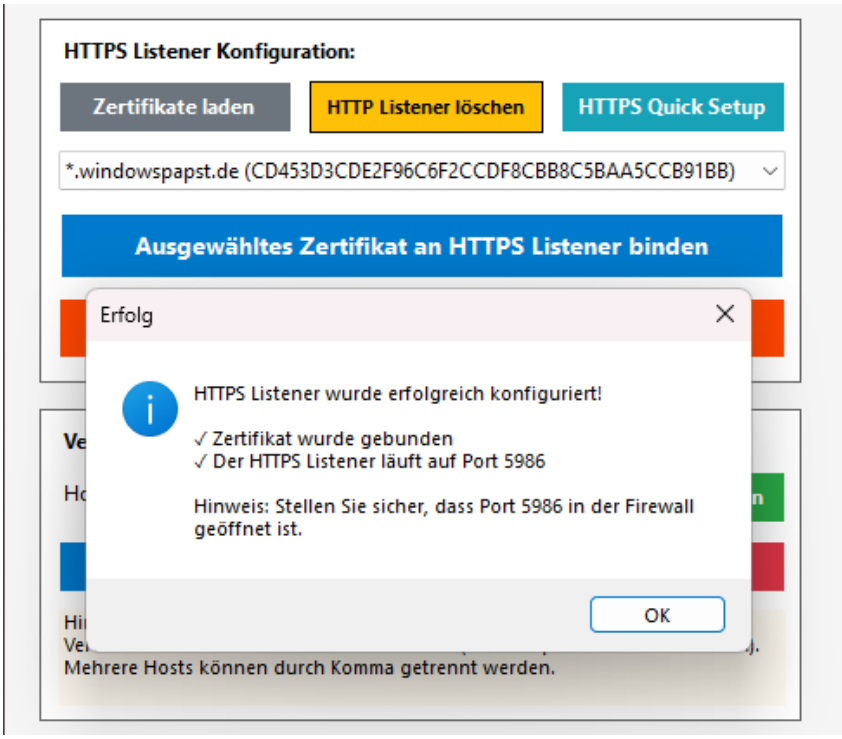
HTTPS Quick Setup

- **Funktion**: Automatische HTTPS-Konfiguration mit selbst-signiertem Zertifikat
- **Ablauf**:
    1. Erstellt selbst-signiertes Zertifikat (5 Jahre gültig)
    2. Bindet Zertifikat an HTTPS-Listener
    3. Konfiguriert Port 5986
- **Ideal für**: Testumgebungen oder schnelle Einrichtung



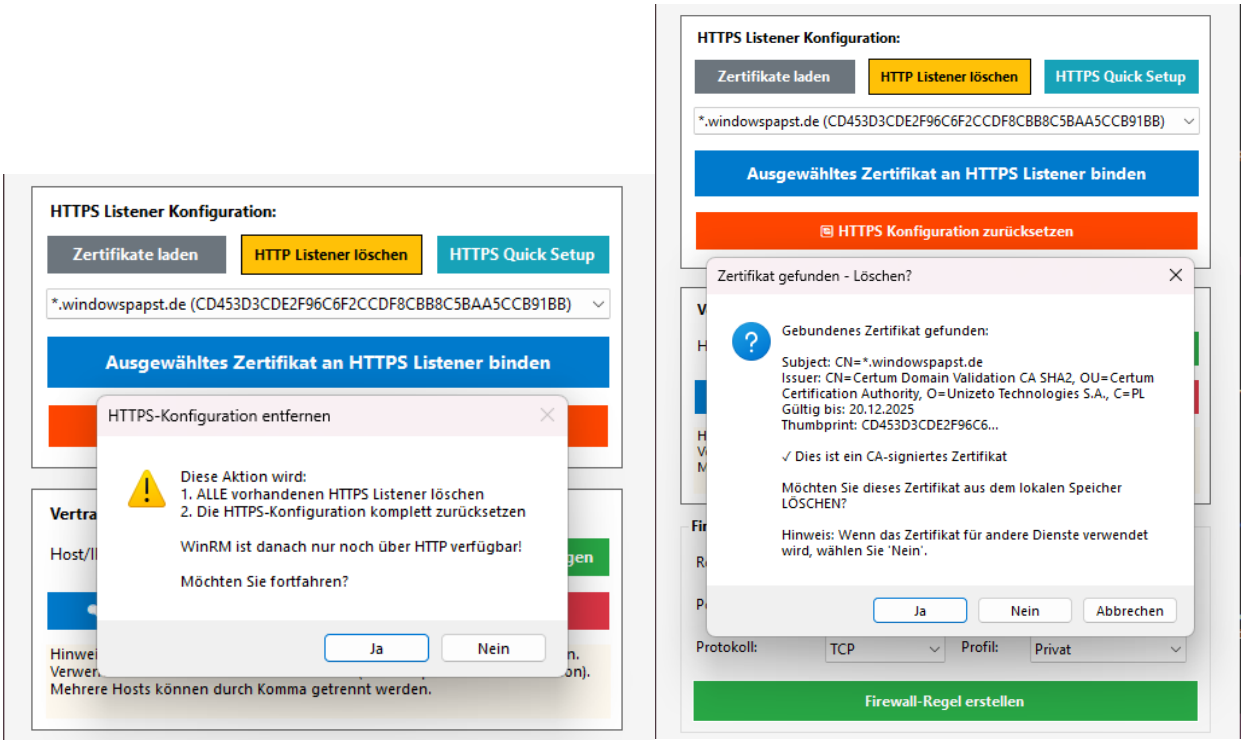
Zertifikat an HTTPS Listener binden

- **Funktion**: Bindet ausgewähltes Zertifikat an HTTPS-Listener
- **Ablauf**:
    1. "Zertifikate laden" klicken
    2. Zertifikat aus Dropdown auswählen
    3. "Ausgewähltes Zertifikat an HTTPS Listener binden" klicken
- **Resultat**: HTTPS-Listener mit gewähltem Zertifikat auf Port 5986



HTTPS Konfiguration zurücksetzen

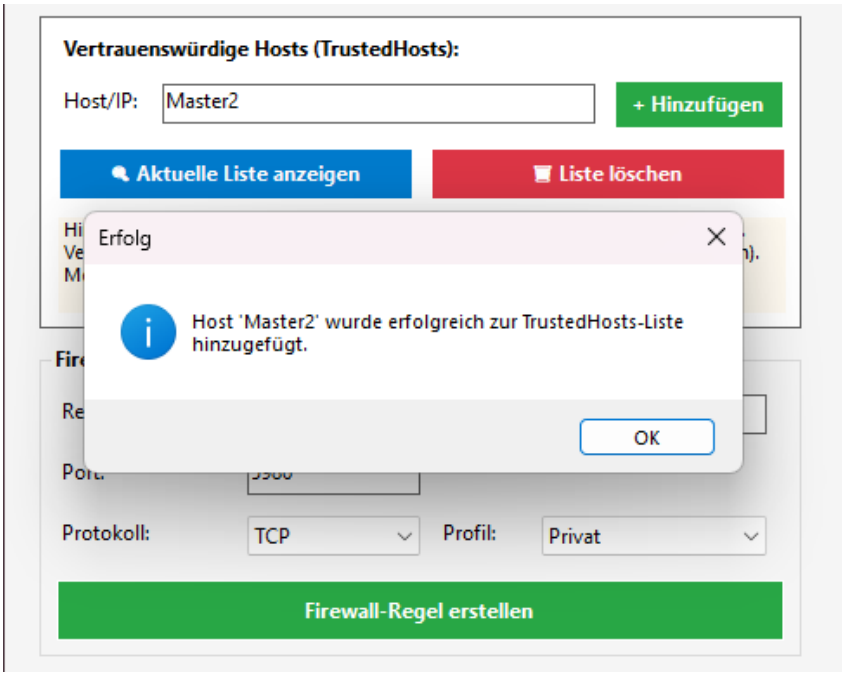
- **Funktion**: Entfernt alle HTTPS-Listener und optional das gebundene Zertifikat
- **Ablauf**:
    1. Bestätigung erforderlich
    2. Option zum Löschen/Behalten des Zertifikats
    3. HTTP-Listener wird bei Bedarf erstellt
- **Verwendung**: Bei fehlerhafter Konfiguration oder Neustart



4.3 Vertrauenswürdige Hosts (TrustedHosts)

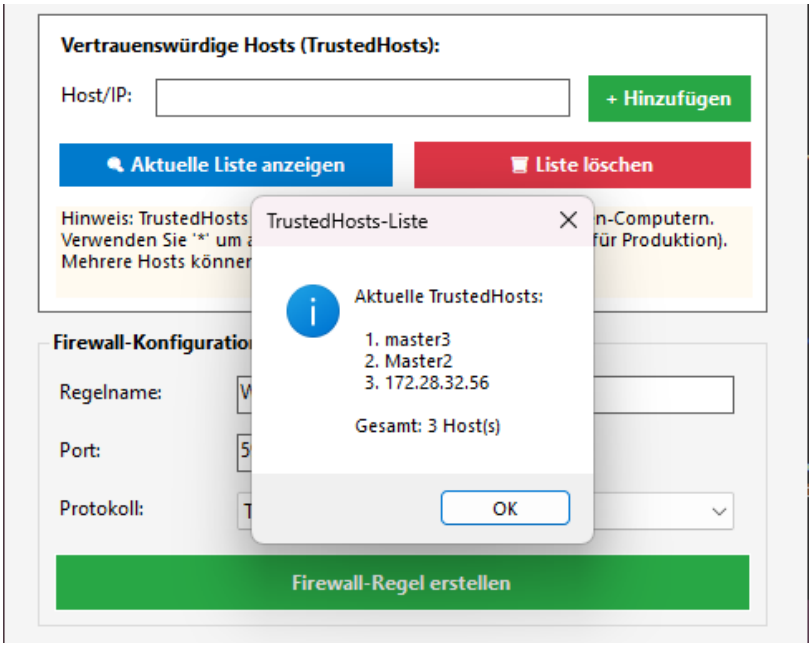
Host hinzufügen

- **Funktion**: Fügt Computer zur TrustedHosts-Liste hinzu
- **Eingabeformate**:
  - Hostname: SERVER01
  - IP-Adresse: 192.168.1.100
  - Wildcard: *.domain.local oder * (alle Hosts)
- **Sicherheit**: Warnung bei Wildcard-Verwendung



Aktuelle Liste anzeigen

- **Funktion**: Zeigt alle konfigurierten TrustedHosts
- **Anzeige**: Nummerierte Liste aller Einträge
- **Warnung**: Bei Wildcard (*) wird Sicherheitsrisiko angezeigt



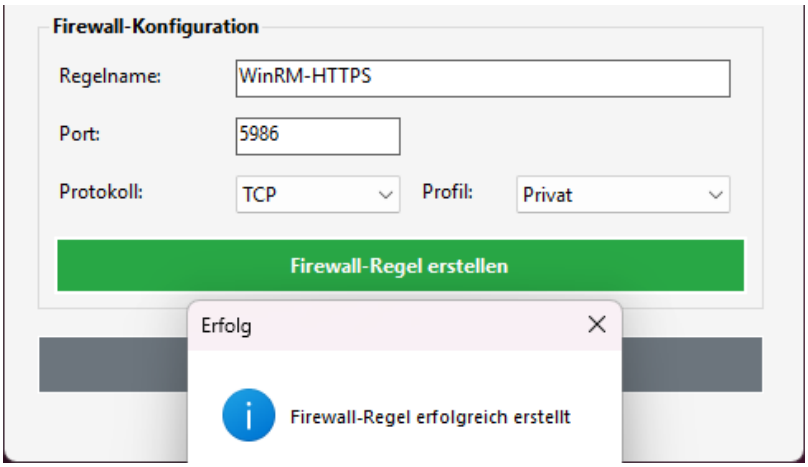
Liste löschen

- **Funktion**: Entfernt alle TrustedHosts-Einträge
- **Warnung**: Bestätigung erforderlich
- **Resultat**: Keine Nicht-Domänen-Verbindungen mehr möglich

4.4 Firewall-Konfiguration

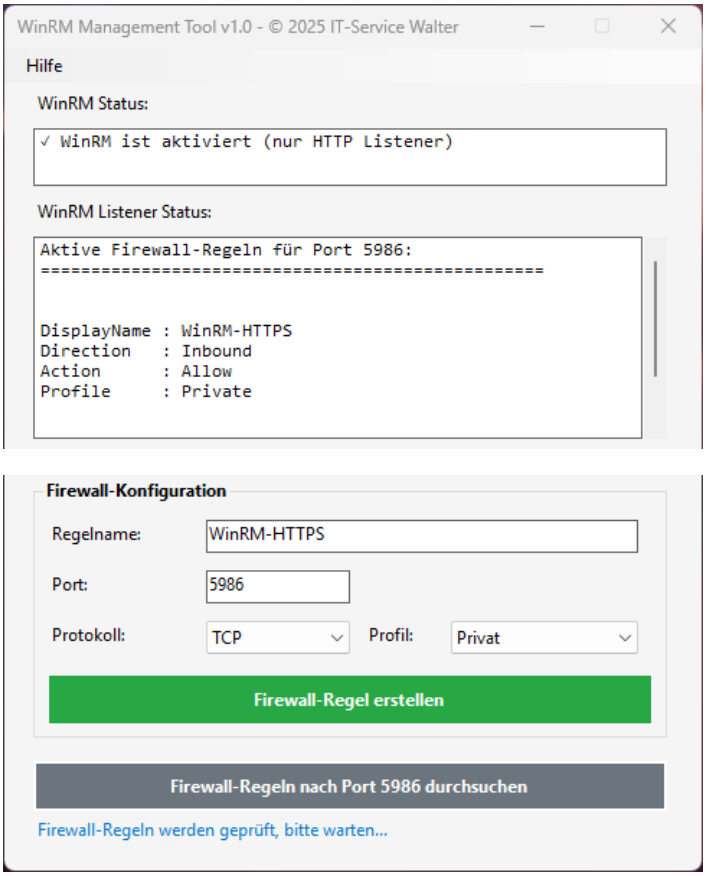
Firewall-Regel erstellen

- **Parameter**:
    - **Regelname**: Eindeutige Bezeichnung (Standard: "WinRM-HTTPS")
    - **Port**: Zu öffnender Port (Standard: 5986 für HTTPS)
    - **Protokoll**: TCP oder UDP (Standard: TCP)
    - **Profil**: Privat, Domäne, Öffentlich oder Alle
- **Empfehlung**: Port 5986 für HTTPS, Port 5985 für http



Firewall-Regeln nach Port 5986 durchsuchen

- **Funktion**: Prüft vorhandene Firewall-Regeln für WinRM-HTTPS
- **Anzeige**: Liste aller aktiven Regeln für Port 5986
- **Verwendung**: Zur Überprüfung der Firewall-Konfiguration



5. Erweiterte Konfiguration

5.1 Zertifikatsanforderungen für WinRM

Für die HTTPS-Bindung muss ein Zertifikat folgende Eigenschaften haben:

- **Enhanced Key Usage (EKU)**: Server Authentication (1.3.6.1.5.5.7.3.1)
- **Subject CN**: Sollte dem Computernamen entsprechen
- **Gültigkeit**: Zertifikat darf nicht abgelaufen sein
- **Speicherort**: LocalMachine\My (Lokaler Computer → Eigene Zertifikate)

5.2 Empfohlene Konfigurationsschritte

Für Produktionsumgebungen:

1. WinRM aktivieren
2. CA-signiertes Zertifikat installieren
3. Zertifikate laden und CA-Zertifikat auswählen
4. Zertifikat an HTTPS Listener binden
5. HTTP Listener löschen (optional für erhöhte Sicherheit)
6. Firewall-Regel für Port 5986 erstellen
7. TrustedHosts nur bei Bedarf konfigurieren

Für Testumgebungen:

1. WinRM aktivieren
2. HTTPS Quick Setup ausführen
3. Firewall-Regel für Port 5986 erstellen
4. TrustedHosts nach Bedarf konfigurieren

5.3 PowerShell-Verbindungstest

Nach der Konfiguration können Sie die Verbindung testen:

```
# HTTPS-Verbindung (mit selbst-signiertem Zertifikat)

Enter-PSSession -ComputerName SERVERNAME -UseSSL -Credential (Get-Credential) -
SessionOption (New-PSSessionOption -SkipCACheck -SkipCNCheck)

# HTTP-Verbindung (nur in vertrauenswürdigen Netzwerken)

Enter-PSSession -ComputerName SERVERNAME -Credential (Get-Credential)
```

6. Fehlerbehebung

Problem: "Zugriff verweigert" Meldungen

Lösung: Tool als Administrator neu starten

Problem: "WinRM-Dienst kann nicht gestartet werden"

Lösungen:

1. In PowerShell als Admin: Enable-PSRemoting -Force
2. Dienst "Windows-Remoteverwaltung" in services.msc prüfen
3. Windows-Updates installieren

Problem: "Keine Listener konfiguriert" nach WinRM-Aktivierung

Lösungen:

1. "HTTPS Quick Setup" verwenden
2. Oder in CMD als Admin: winrm quickconfig

Problem: HTTPS-Listener kann nicht erstellt werden

Prüfpunkte:

- Zertifikat hat Server Authentication EKU
- Zertifikat ist gültig (nicht abgelaufen)
- CN des Zertifikats entspricht dem Hostnamen
- WinRM-Dienst läuft

Problem: Firewall blockiert Verbindungen

Lösungen:

1. Firewall-Regel über das Tool erstellen
2. "Firewall-Regeln nach Port 5986 durchsuchen" zur Überprüfung
3. Windows Defender Firewall temporär deaktivieren (nur zum Testen)

Problem: TrustedHosts können nicht gesetzt werden

Lösungen:

1. WinRM muss aktiviert sein
2. In PowerShell als Admin: winrm quickconfig
3. Manuell: Set-Item WSMan:\localhost\Client\TrustedHosts -Value "HOSTNAME" -Force

7. Sicherheitshinweise

Wichtige Sicherheitsempfehlungen

HTTPS vs. HTTP

- **Verwenden Sie immer HTTPS in Produktionsumgebungen**
- HTTP überträgt Daten unverschlüsselt
- HTTPS verschlüsselt die gesamte Kommunikation

TrustedHosts-Konfiguration

- **Vermeiden Sie Wildcard (*)**
- Fügen Sie nur bekannte und vertrauenswürdige Hosts hinzu
- Regelmäßig überprüfen und nicht benötigte Einträge entfernen

Zertifikatsverwaltung

- Verwenden Sie CA-signierte Zertifikate in Produktion
- Selbst-signierte Zertifikate nur für Testumgebungen
- Zertifikate vor Ablauf erneuern

Firewall-Regeln

- Beschränken Sie Regeln auf notwendige Netzwerkprofile

- Verwenden Sie spezifische Quell-IP-Bereiche wenn möglich
- Dokumentieren Sie alle erstellten Regeln

Zugriffskontrolle

- WinRM-Zugriff nur für autorisierte Administratoren
- Verwenden Sie starke Passwörter
- Implementieren Sie Zwei-Faktor-Authentifizierung wo möglich

Compliance und Best Practices

- Protokollieren Sie alle WinRM-Konfigurationsänderungen
- Testen Sie Änderungen zuerst in einer Testumgebung
- Halten Sie Dokumentation der konfigurierten Systeme aktuell
- Führen Sie regelmäßige Sicherheitsüberprüfungen durch

Support und Kontakt

IT-Service Walter

- Webseite: https://www.it-service-walter.com
- Tool-Version: 1.0.0
-

Für weitere Unterstützung besuchen Sie bitte unsere Webseite über das Hilfe-Menü im Tool.

Verkauf

Das Tool kostet für den Einzelplatz 19,00 € inkl. 19% MwSt. Als Firmenlizenz einmalig 109,00 € inkl. 19% MwSt.