GMSA & MSA MANAGEMENT

IT-Service Walter

Jörn Walter
www.it-service-walter.com
16.09.2025

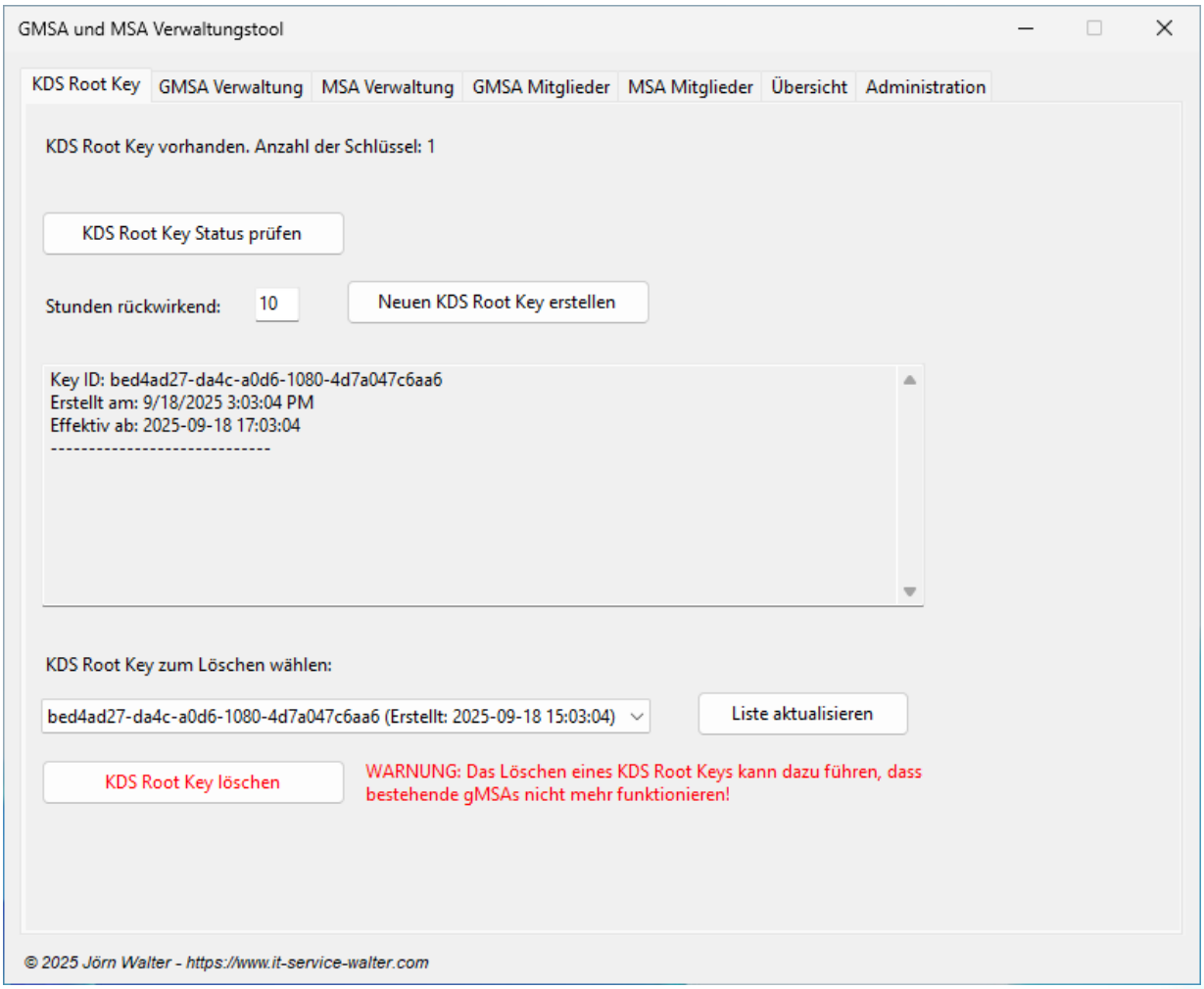
DAS GMSA & MSA MANAGEMENT TOOL ÜBERBLICK

DAS GMSA UND MSA VERWALTUNGSTOOL IST EINE UMFASSENDE WINDOWS FORMS-ANWENDUNG ZUR ZENTRALEN VERWALTUNG VON MANAGED SERVICE ACCOUNTS IN ACTIVE DIRECTORY-UMGEBUNGEN. DAS TOOL BIETET EINE INTUITIVE GRAFISCHE OBERFLÄCHE FÜR AUFGABEN, DIE NORMALERWEISE KOMPLEXE POWERSHELL-BEFEHLE ERFORDERN WÜRDEN.

GMSA und MSA Verwaltungstool – Funktionsbeschreibung

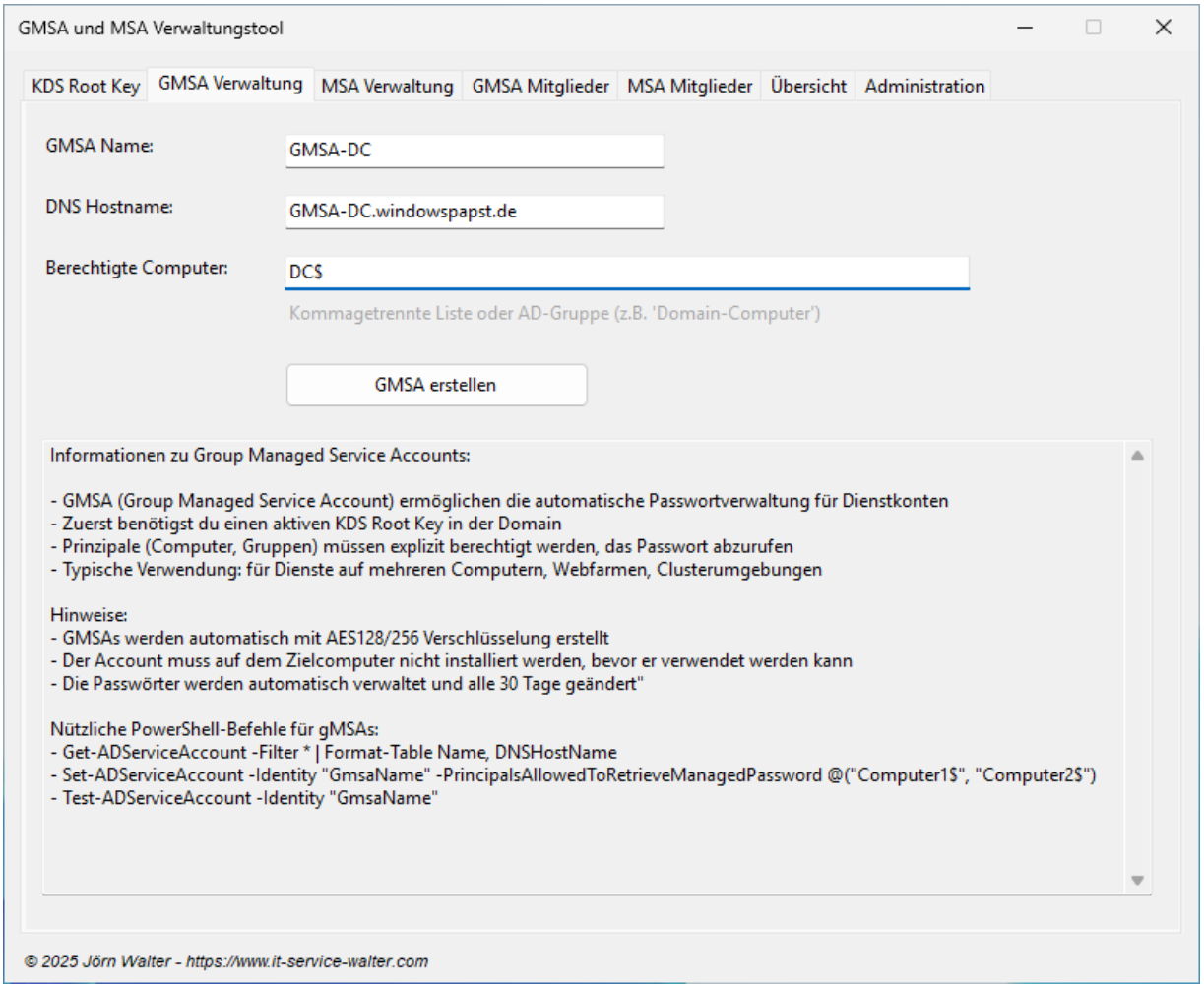
KDS Root Key Verwaltung - Das Fundament für Group Managed Service Accounts

Die KDS Root Key Verwaltung bildet das technische Fundament für den Betrieb von Group Managed Service Accounts in Active Directory. Das Tool ermöglicht Administratoren eine vollständige Kontrolle über diese kritische Komponente. Bei der Statusprüfung analysiert das System die vorhandenen KDS Root Keys in der Domain und präsentiert diese in einer übersichtlichen Darstellung mit allen relevanten Details wie Key-ID, Erstellungszeitpunkt und Effektivzeit. Die Erstellung neuer Keys erfolgt über einen intuitiven Dialog, bei dem die Effektivzeit flexibel eingestellt werden kann. Für Produktionsumgebungen empfiehlt sich die standardmäßige Vorlaufzeit von 10 Stunden, während in Testumgebungen eine sofortige Aktivierung durch rückwirkende Zeitangabe möglich ist. Das Tool warnt explizit vor dem Löschen von Keys, da dies erhebliche Auswirkungen auf bestehende GMSAs haben kann. Die integrierte Aktualisierungsfunktion stellt sicher, dass Administratoren stets mit aktuellen Informationen arbeiten.



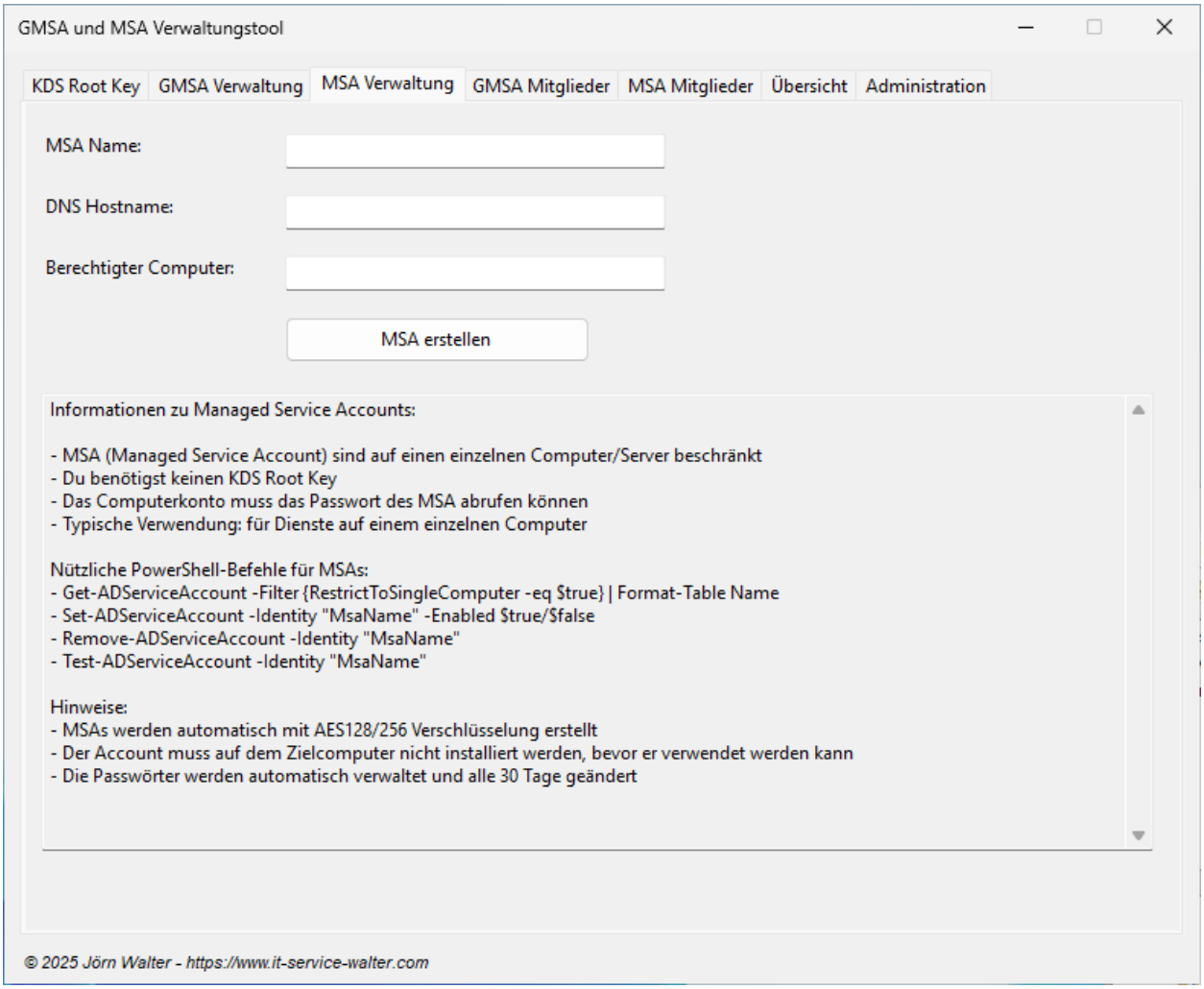
GMSA-Erstellung und Verwaltung - Automatisierte Sicherheit für Dienste

Die Verwaltung von Group Managed Service Accounts stellt den Kernbereich des Tools dar. Bei der Erstellung eines neuen GMSAs führt das Tool den Administrator durch einen strukturierten Prozess, der mit der Eingabe des Account-Namens und des DNS-Hostnamens beginnt. Die Zuweisung der berechtigten Computer erfolgt über ein flexibles Eingabefeld, das sowohl einzelne Computernamen als auch kommagetrennte Listen und AD-Gruppen akzeptiert. Das System konfiguriert automatisch die moderne AES-Verschlüsselung und stellt sicher, dass alle notwendigen Attribute korrekt gesetzt werden. Eine optionale Checkbox ermöglicht das automatische Löschen der Eingabefelder nach erfolgreicher Erstellung, was besonders bei der Anlage mehrerer Accounts die Effizienz steigert. Der manuelle Lösch-Button bietet zusätzliche Flexibilität für Administratoren, die ihre Arbeitsweise individuell gestalten möchten.



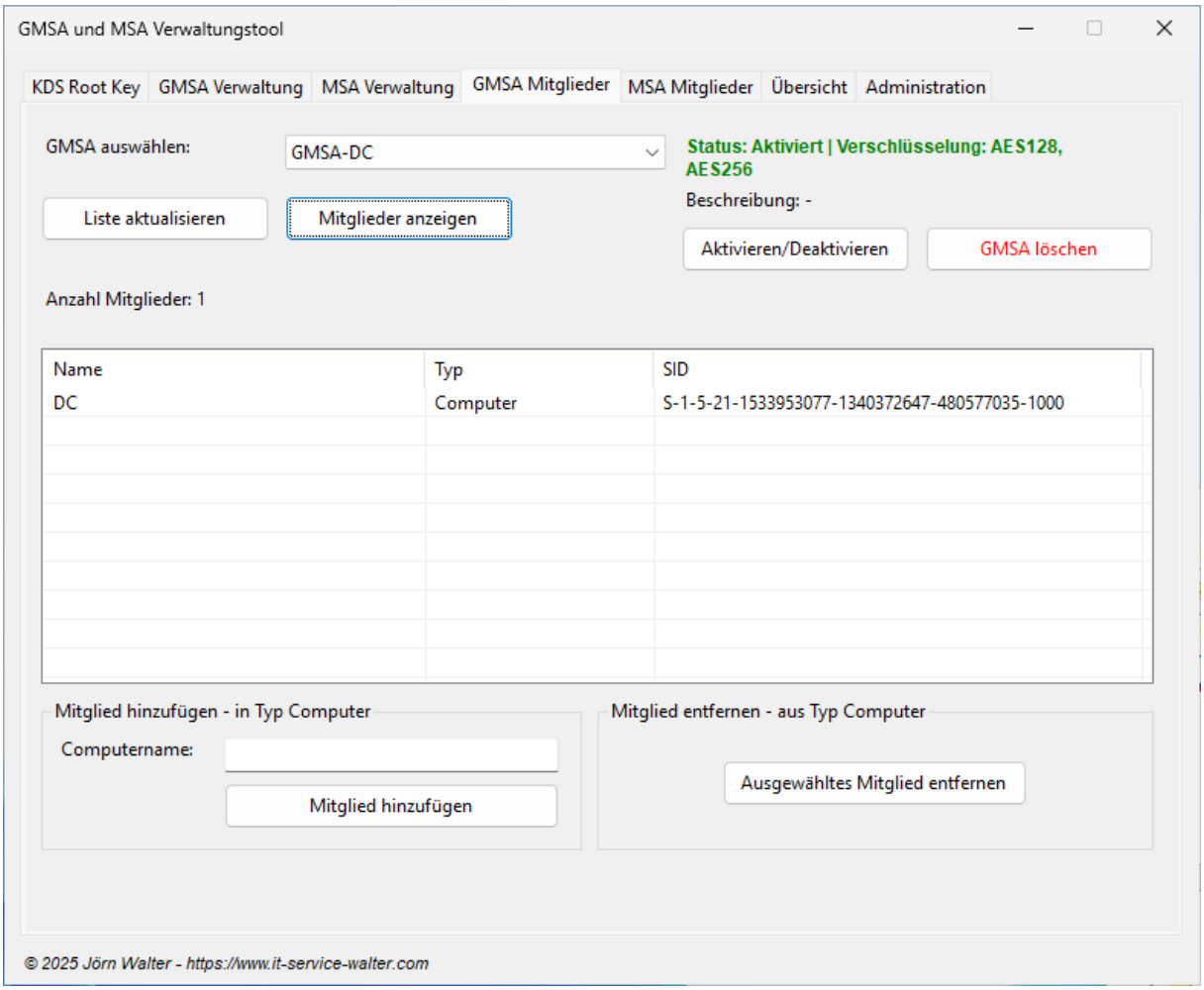
MSA-Verwaltung - Service Accounts für einzelne Computer

Die Verwaltung klassischer Managed Service Accounts folgt einem ähnlichen Muster wie bei GMSAs, berücksichtigt aber die spezifischen Einschränkungen dieser Account-Art. MSAs sind auf einen einzelnen Computer beschränkt und benötigen keinen KDS Root Key, was ihre Einrichtung in manchen Szenarien vereinfacht. Das Tool führt durch den Erstellungsprozess mit Feldern für Account-Name, DNS-Hostname und den berechtigten Computer. Auch hier steht die Option zur Verfügung, die Eingabefelder nach erfolgreicher Erstellung automatisch zu löschen.



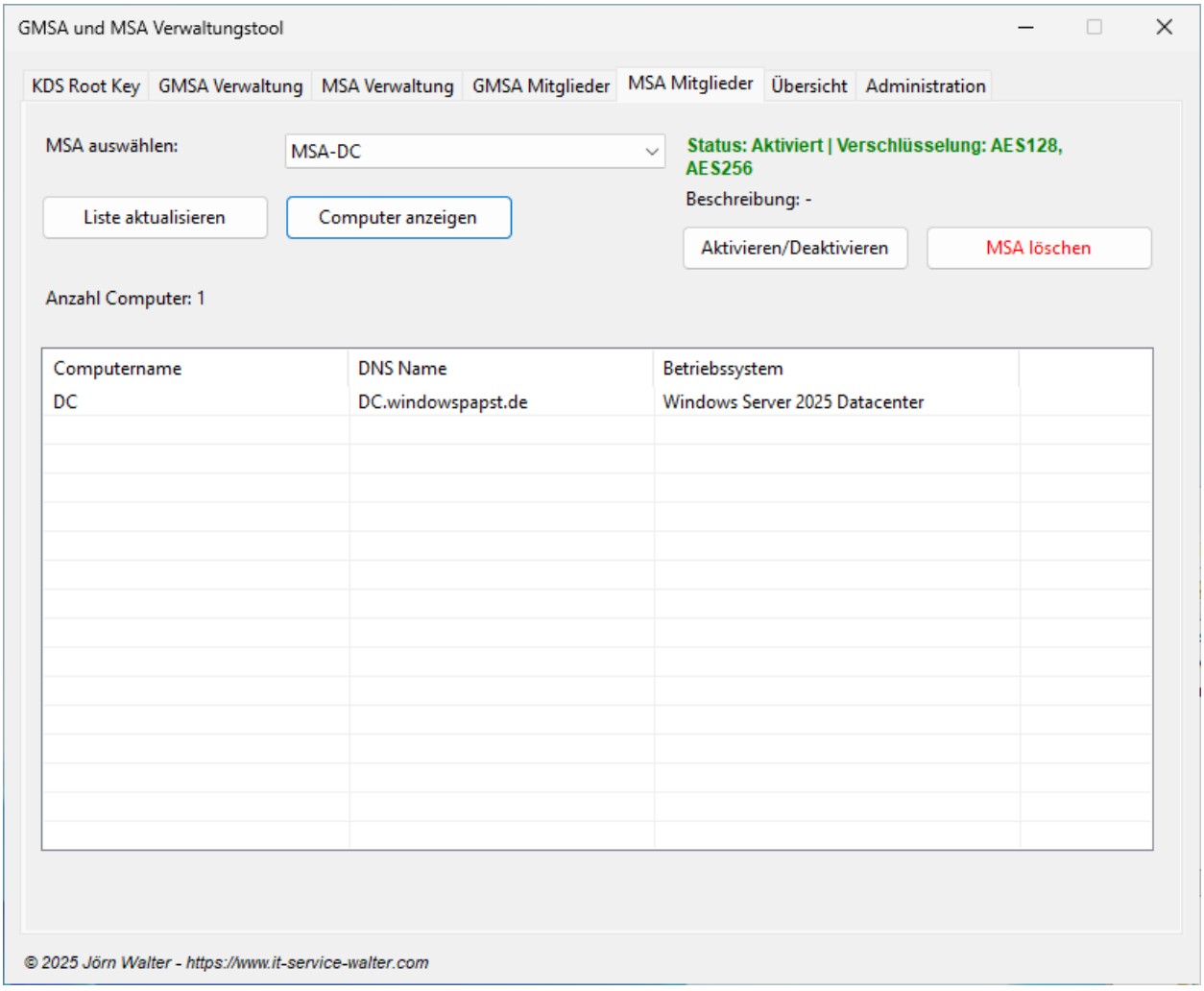
Mitgliederverwaltung für GMSAs - Dynamische Berechtigungskontrolle

Die GMSA-Mitgliederverwaltung ermöglicht eine granulare Kontrolle über die Zugriffsberechtigungen. Nach Auswahl eines GMSAs aus der Dropdown-Liste zeigt das Tool den aktuellen Status, die Beschreibung und eine vollständige Liste aller berechtigten Computer und Gruppen an. Jedes Mitglied wird mit Name, Typ und Security Identifier dargestellt, was eine eindeutige Identifikation ermöglicht. Neue Mitglieder können über ein einfaches Eingabefeld hinzugefügt werden, wobei das System automatisch die korrekten AD-Objekte auflöst. Das Entfernen von Berechtigungen erfolgt durch Auswahl aus der Liste und Bestätigung der Sicherheitsabfrage. Zusätzlich bietet dieser Bereich die Möglichkeit, GMSAs zu aktivieren, deaktivieren oder vollständig zu löschen, wobei alle Aktionen mit entsprechenden Warnhinweisen versehen sind.



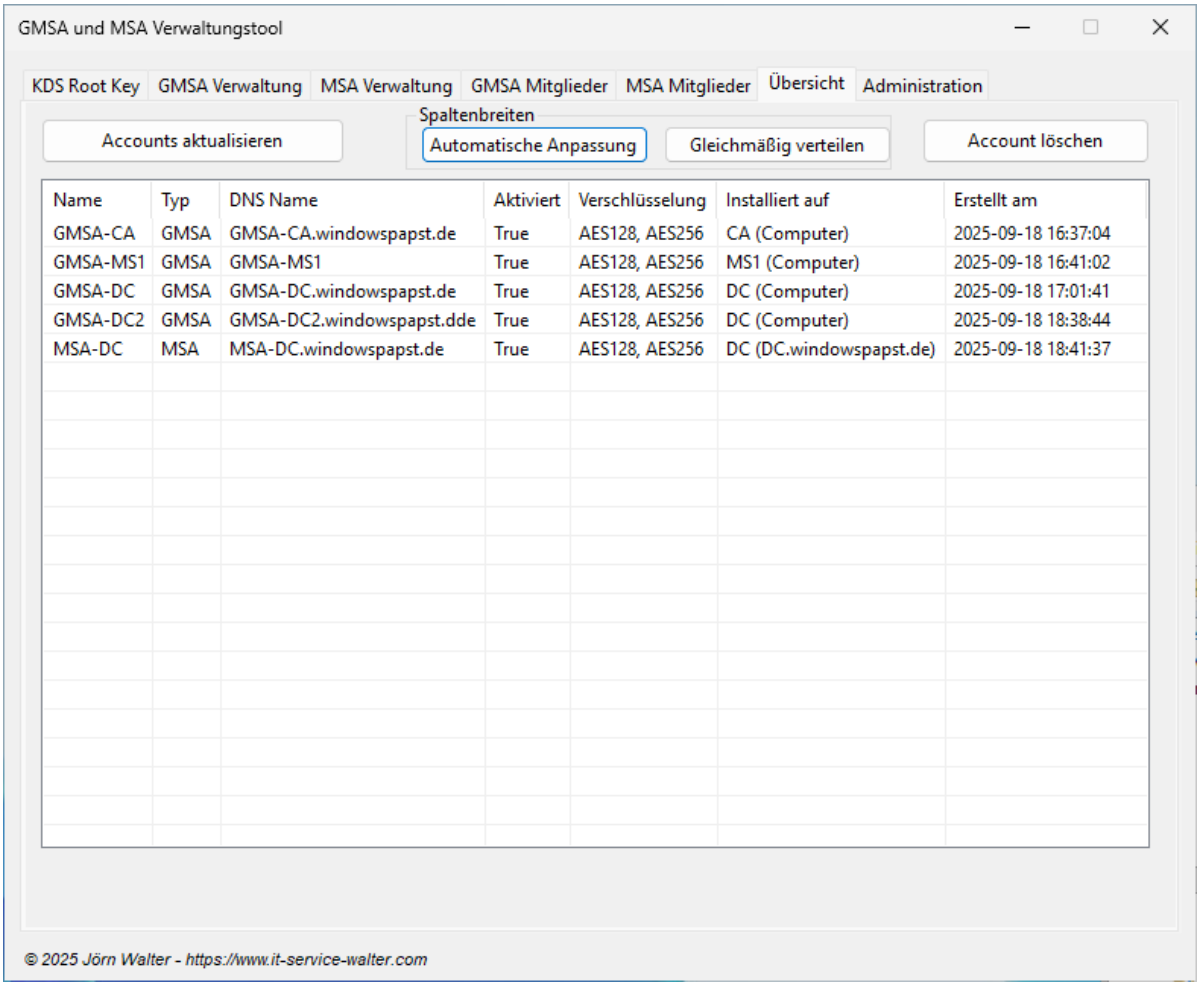
MSA-Mitgliederverwaltung - Fokussierte Einzelcomputer-Zuordnung

Die MSA-Mitgliederverwaltung konzentriert sich auf die Verwaltung der Einzelcomputer-Zuordnung. Da MSAs konstruktionsbedingt nur einem Computer zugewiesen werden können, zeigt dieser Bereich den aktuell zugewiesenen Computer mit erweiterten Informationen wie DNS-Name und Betriebssystem an. Die Statusverwaltung ermöglicht das schnelle Aktivieren oder Deaktivieren von MSAs, was besonders bei Wartungsarbeiten oder Fehlersuche nützlich ist. Wie bei GMSAs können auch MSAs vollständig gelöscht werden, wobei das Tool vor den Konsequenzen dieser Aktion warnt, und eine Bestätigung erfordert.



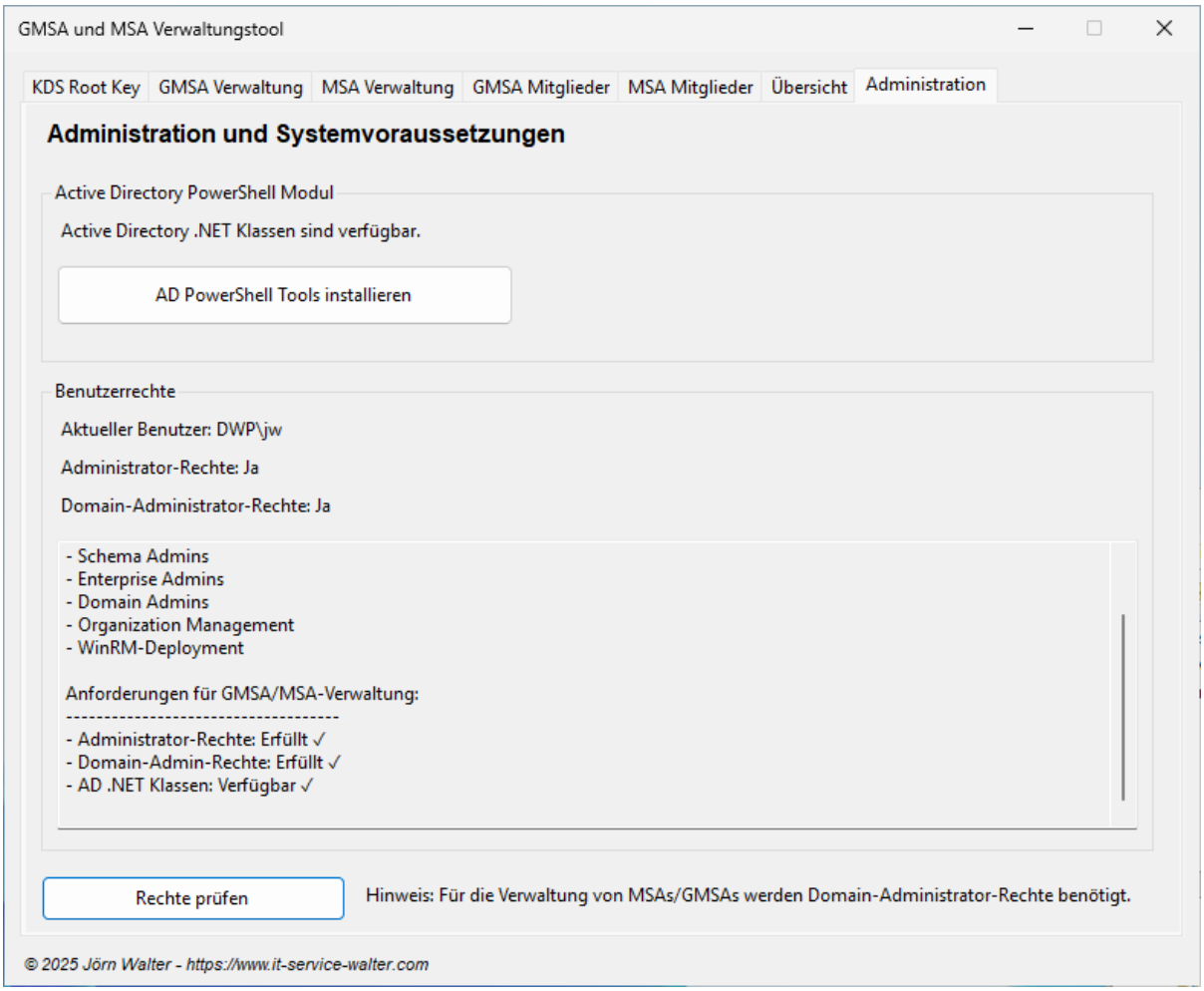
Zentrale Übersicht - Dashboard für alle Service Accounts

Die Übersichtsseite bietet einen konsolidierten Blick auf alle Service Accounts in der Domain. Die tabellarische Darstellung zeigt auf einen Blick Account-Name, Typ (GMSA oder MSA), DNS-Hostname, Aktivierungsstatus, konfigurierte Verschlüsselungstypen, Installationsorte und Erstellungsdatum. Die Spaltenbreiten können entweder automatisch an den Inhalt angepasst oder gleichmäßig über die verfügbare Breite verteilt werden. Diese Flexibilität ermöglicht es Administratoren, die Ansicht nach ihren Bedürfnissen zu optimieren. Ein Kontextmenü bietet Schnellzugriff auf häufig benötigte Funktionen wie das Löschen von Accounts. Die Übersicht eignet sich besonders für Audit-Zwecke, da alle relevanten Informationen auf einen Blick erfasst werden können. Bei Accounts mit mehreren berechtigten Computern zeigt das Tool eine kompakte Zusammenfassung mit der Option, weitere Details abzurufen.



Administration und Diagnose - Systemkontrolle und Fehleranalyse

Der Administrationsbereich vereint wichtige Systemfunktionen und Diagnosewerkzeuge. Das Tool überprüft beim Start automatisch, ob es mit administrativen Rechten ausgeführt wird, und verweigert den Start ohne diese Berechtigung, um Fehlfunktionen zu vermeiden. Im Admin-Tab werden der aktuelle Benutzer, dessen Administrator-Status und Domain-Administrator-Rechte sowie alle Gruppenmitgliedschaften angezeigt. Diese Informationen sind essentiell für die Fehlersuche bei Berechtigungsproblemen. Die integrierte Installationsfunktion für die Active Directory PowerShell-Tools ermöglicht es, fehlende Komponenten direkt nachzuinstallieren. Die Diagnosefunktion öffnet ein separates Fenster mit detaillierten Informationen über die AD-Verbindung, alle gefundenen Service Accounts und deren Konfiguration. Diese technischen Details sind besonders wertvoll bei der Zusammenarbeit mit dem Support oder bei der Dokumentation von Problemen.



Benutzerführung und Hilfefunktionen - Intuitive Bedienung für alle Erfahrungsstufen

Das Tool wurde mit besonderem Augenmerk auf eine intuitive Benutzerführung entwickelt. Visuelle Elemente wie Trennlinien gliedern die verschiedenen Funktionsbereiche und schaffen eine klare Struktur. Farbcodierte Statusanzeigen in Grün und Rot ermöglichen eine sofortige visuelle Erfassung des Systemzustands. In jedem Tab sind kontextbezogene Hilfetexte integriert, die nicht nur die Funktionsweise erklären, sondern auch die entsprechenden PowerShell-Befehle für manuelle Operationen anzeigen. Dies macht das Tool zu einem wertvollen Lernwerkzeug für Administratoren, die ihre PowerShell-Kenntnisse vertiefen möchten. Bei kritischen Operationen wie dem Löschen von Accounts oder KDS Root Keys werden mehrstufige Sicherheitsabfragen eingeblendet, die detailliert über die möglichen Konsequenzen informieren. Die durchgängige Verwendung deutscher Bezeichnungen bei gleichzeitiger Anzeige der englischen PowerShell-Befehle erleichtert die Arbeit in gemischten Umgebungen.

GMSA und MSA-Verwaltungstool – Funktionsübersicht in Kurzform

1. KDS Root Key Verwaltung

Status-Prüfung

- Überprüft vorhandene KDS Root Keys in der Active Directory Domain
- Zeigt Anzahl, Key-IDs, Erstellungsdatum und Effektivzeit an
- Listet alle Keys mit detaillierten Informationen auf

Key-Erstellung

- Erstellt neue KDS Root Keys mit konfigurierbarer Effektivzeit
- Rückwirkende Aktivierung in Stunden einstellbar (Standard: 10 Stunden)
- Sofortige Aktivierung für Testumgebungen möglich

Key-Verwaltung

- Aktualisierung der Key-Liste per Knopfdruck
- Löschung nicht mehr benötigter KDS Root Keys
- Sicherheitswarnungen vor kritischen Operationen

2. GMSA Erstellung und Verwaltung

Account-Erstellung

- Anlegen neuer Group Managed Service Accounts
- DNS-Hostname-Konfiguration
- Zuweisung berechtigter Computer oder AD-Gruppen
- Kommagetrennte Listen für mehrere Berechtigungen
- Automatische AES128/256-Verschlüsselung

Test-Funktionen

- Lokaler Test auf aktuellem System
- Remote-Test auf beliebigen Domänen-Computern
- SSL/TLS-Unterstützung für sichere Verbindungen (Port 5986)
- Automatische Credential-Abfrage bei Bedarf
- Detaillierte Fehlerdiagnose mit Lösungsvorschlägen

Verkauf

Das Tool kostet für den Einzelplatz 29,00 € inkl. 19% MwSt. Als Firmenlizenz einmalig 149,00 € inkl. 19% MwSt.