Konfigurations- und Sicherheitseinstellungen unter Windows XP

In diesem Dokument sind die für den Baustein 3.209 Client unter Windows XP relevanten Konfigurations-und Sicherheitseinstellungen aufgeführt.
Sie umfassen folgende Schwerpunkte:

- Sichere Installation von Windows XP (siehe auch Maßnahme M 4.248)
- Sicherheit beim Fernzugriff unter Windows XP (siehe auch Maßnahme M 2.327)
- Basiseinstellungen für Windows XP GPOs (siehe auch Maßnahme M 4.245)
- Konfiguration der Systemdienste unter Windows XP (siehe auch Maßnahme M 4.246)
- Restriktive Berechtigungsvergabe unter Windows XP (siehe auch Maßnahme M 4.247)

Sichere Installation von Windows XP (siehe M 4.248)

Systemkomponenten

Im Folgenden werden Komponenten aufgezählt, die für eine Basis-Installation von Windows XP verwendet werden sollten (Status: *Aktiviert*). Je nach existierenden geschäftlichen Anforderungen können weitere Komponenten installiert werden, die in der nachfolgenden Tabelle als *Optional* markiert werden. Von der Installation der Windows-Komponenten, die mit *Deaktiviert* markiert sind, ist aus Sicherheitssicht abzuraten.

Komponenten	Status (Aktiviert/Deaktiviert/ Optional)
Aktualisierung von Stammzertifikaten	Optional
Faxdienste	Optional
Indexdienst	Optional
Internet Explorer	Aktiviert
Internet-Informationsdienste (IIS)	Deaktiviert
Message Queuing	Deaktiviert
MSN Explorer	Deaktiviert
Netzwerkdienste	
Einfache TCP/IP-Deinste	Deaktiviert
Internet Gateway Gerätesuche und -Steuerungsclient	Optional
Peer-to-Peer	Deaktiviert
RIP-Überwachung	Deaktiviert
UpnP-Benutzerschnittstelle	Deaktiviert
Outlook Express	Deaktiviert
Verwaltungs- und Überwachungsprogramme	
SNMP	Optional
WMI SNMP provider	Optional
Weitere Datei- und Druckdienste für das Netzwerk	
Druckdienste für Unix	Deaktiviert
Windows Media Player	Optional
Windows Messenger	Optional
Zubehör und Dienstprogramme	Optional

Sicherheit beim Fernzugriff unter Windows XP (siehe M 2.327)

Basiseinstellungen für GPOs

Die nachfolgenden Einstellungen gelten nur für den Einsatz von Remotedesktop und/oder Remoteunterstützung. Soll einer der beiden oder gar beide Fernsteuerungsmechanismen nicht verwendet werden, so ist dieser zu deaktivieren. Hierfür ist die Modifikation der unten angegebenen Richtlinieneinstellungen notwendig.
Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Computer auf, die für die Benutzung von Remotedesktop und Remoteunterstützung konfiguriert werden sollten.

Richtlinie	Status	Einstellung
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Verschlüsselung und Sicherheit | Verschlüsselungsstufe der Clientverbindung festlegen	Aktiviert	Höchste Stufe
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Verschlüsselung und Sicherheit | RPC-Sicherheitsrichtlinie | Sicherer Server (Sicherheit erforderlich)	Aktiviert	
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Verschlüsselung und Sicherheit | Clients bei der Verbindungsherstellung immer zur Kennworteingabe auffordern	Aktiviert	
Computerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Client/Server-Datenumleitung | *	Aktiviert/ Deaktiviert	
Computerkonfiguration | Administrative Vorlagen | System | Remote Unterstützung |Remoteunterstützung anbieten	Deaktiviert	
Computerkonfiguration | Administrative Vorlagen | System | Remote Unterstützung | Angeforderte Remoteunterstützung	Aktiviert	Helfer dürfen den Computer remote steuern,
Maximale Gültigkeitsdauer: 8 Stunden		

Die nachfolgende Tabelle listet Gruppenrichtlinieneinstellungen für Benutzer auf, die für die Benutzung von Remotedesktop und Remoteunterstützung konfiguriert werden sollten.

Richtlinie	Status	Einstellung
Benutzerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste | Regeln für Remoteüberwachung von Terminaldienste-Benutzersitzungen festlegen	Aktiviert	Vollzugriff mit Erlaubnis des Benutzers
Benutzerkonfiguration | Windows-Einstellungen | Administrative Vorlagen | Terminaldienste |Client | Speichern von Kennwörtern nicht zulassen	Aktiviert	

Basiseinstellungen für Windows XP GPOs (siehe M 4.245)
Im Folgenden werden Vorgaben für die Sicherheitseinstellungen aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen innerhalb einer Gruppenrichtlinie dienen können.
Die angegebenen Werte müssen auf jeden Fall an die lokalen Bedingungen angepasst werden. Im Rahmen des Gruppenrichtlinienkonzeptes sind die einzelnen Werte zudem auf unterschiedliche Gruppenrichtlinienobjekte zu verteilen und jeweils an den Verwendungszweck anzupassen. Dadurch können für einzelne Einträge auch jeweils unterschiedliche Werte zustande kommen.

Kontorichtlinien | Kennwortrichtlinien	
Richtlinie	Computereinstellung
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen	6 Gespeicherte Kennwörter
Kennwörtern für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern	Deaktiviert
Maximales Kennwortalter	90 Tage
Minimale Kennwortlänge	8 Zeichen
Minimales Kennwortalter	1 Tag

Kontorichtlinien | Kontosperrungsrichtlinien	
Richtlinie	Computereinstellung
Kontensperrungsschwelle	3 Ungültige Anmeldeversuche
Kontosperrdauer	0 (Hinweis: Konto ist gesperrt, bis Administrator Sperrung aufhebt)
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

Kontorichtlinien | Kerberos-Richtlinie	
Richtlinie	Computereinstellung
Benutzeranmeldeeinschränkungen erzwingen	Aktiviert
Max. Gültigkeitsdauer des Benutzertickets	8 Stunden
Max. Gültigkeitsdauer des Diensttickets	60 Minuten
Max. Toleranz für die Synchronisation des Computertakts	5 Minuten
Max. Zeitraum, in dem ein Benutzerticket erneuert werden kann	1 Tag

Lokale Richtlinien | Überwachungsrichtlinie	
Richtlinie	Computereinstellung
Active Directory-Zugriff überwachen	Nicht definiert
Anmeldeereignisse überwachen	Erfolgreich, Fehlgeschlagen
Anmeldeversuche überwachen	Erfolgreich, Fehlgeschlagen
Kontenverwaltung überwachen	Erfolgreich, Fehlgeschlagen
Objektzugriffsversuche überwachen	Fehlgeschlagen
Prozessverfolgung überwachen	Nicht definiert (kann bei Fehlersuche lokal aktiviert werden)
Rechteverwendung überwachen	Fehlgeschlagen
Richtlinienänderungen überwachen	Erfolgreich, Fehlgeschlagen
Systemereignisse überwachen	Erfolgreich, Fehlgeschlagen

Sicherheitsoptionen	
Richtlinie	Computereinstellung

DCOM: Computerstarteinschränkungen in Security Descriptor Definition Language (SDDL)-Syntax	Nicht definiert
DCOM: Computerzugriffseinschränkungen in Security Descriptor Definition Language (SDDL)-Syntax	Nicht definiert
Domänencontroller: Änderungen von Computerkontenkennwörtern verweigern	Nicht definiert
Domänencontroller: Serveroperatoren das Einrichten von geplanten Tasks erlauben	Nicht definiert
Domänencontroller: Signaturanforderungen für LDAP-Server	Nicht definiert
Domänenmitglied: Änderungen von Computerkontenkennwörtern deaktivieren	Deaktiviert
Domänenmitglied: Daten des sicheren Kanals digital signieren (wenn möglich)	Aktiviert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Aktiviert
Domänenmitglied: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Aktiviert
Domänenmitglied: Maximalalter von Computerkontenkennwörtern	30 Tage
Domänenmitglied: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Aktiviert
Geräte: Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Geräte: Entfernen ohne vorherige Anmeldung erlauben	Deaktiviert
Geräte: Formatieren und Auswerfen von Wechselmedien zulassen	Administratoren und interaktive Benutzer
Geräte: Verhalten bei der Installation von nichtsignierten Treibern	Warnen, aber Installation erlauben
Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Herunterfahren: Auslagerungsdatei des virtuellen Arbeitspeichers löschen	Aktiviert
Herunterfahren: Herunterfahren des Systems ohne Anmeldung zulassen	Deaktiviert
Interaktive Anmeldung: Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern	14 Tage
Interaktive Anmeldung: Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)	0 Anmeldungen
Interaktive Anmeldung: Domänencontrollerauthentifizierung zum Aufheben der Sperrung der Arbeitsstation erforderlich	Aktiviert
Interaktive Anmeldung: Kein STRG+ALT+ENTF erforderlich	Deaktiviert
Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen	Aktiviert
Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen	Dieses System ist auf autorisierte Benutzer beschränkt. Der Versuch, nicht autorisierten Zugriff zu erlangen, wird strafrechtlich verfolgt.
Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen	SIE MACHEN SICH STRAFBAR, WENN SIE OHNE ERFORDERLICHE AUTORISIERUNG FORTFAHREN
Interaktive Anmeldung: Smartcard erforderlich	Nicht definiert
Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards	Arbeitsstation sperren
Konten: Administrator umbenennen	<Neuer Kontoname>
Konten: Administratorkontostatus	Deaktiviert
Konten: Gastkontenstatus	Deaktiviert
Konten: Gastkonto umbenennen	<Neuer Kontoname>
Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken	Aktiviert
Microsoft-Netzwerk (Client): Kommunikation digital signieren (immer)	Aktiviert

Sicherheitsoptionen	
Microsoft-Netzwerk (Client): Kommunikation digital signieren (wenn Server zustimmt)	Aktiviert
Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an SMB-Server von Drittanbietern senden	Deaktiviert
Microsoft-Netzwerk (Server): Clientverbindungen aufheben, wenn die Anmeldezeit überschritten wird	Aktiviert
Microsoft-Netzwerk (Server): Kommunikation digital signieren (immer)	Aktiviert
Microsoft-Netzwerk (Server): Kommunikation digital signieren (wenn Client zustimmt)	Aktiviert
Microsoft-Netzwerk (Server): Leerlaufzeitspanne bis zum Anhalten der Sitzung	15 Minuten
Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen	Aktiviert
Netzwerksicherheit: Keine LAN Manager-Hashwerte für nächste Kennwortänderung speichern	Aktiviert
Netzwerksicherheit: LAN Manager-Authentifizierungsebene	Nur NTLMv2-Antworten senden\LM & NTLM verweigern
Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Clients (einschließlich sicherer RPC-Clients)	Nachrichtenintegrität erfordern, Nachrichtenvertraulichkeit erfordern, NTLMv2-Sitzungssicherheit erfordern, 128-Bit-Verschlüsselung erfordern
Netzwerksicherheit: Minimale Sitzungssicherheit für NTLM-SSP-basierte Server (einschließlich sicherer RPC-Server)	Nachrichtenintegrität erfordern, Nachrichtenvertraulichkeit erfordern, NTLMv2-Sitzungssicherheit erfordern, 128-Bit-Verschlüsselung erfordern
Netzwerksicherheit: Signaturanforderungen für LDAP-Clients	Signatur aushandeln
Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten nicht erlauben	Aktiviert
Netzwerkzugriff: Anonyme Aufzählung von SAM-Konten und Freigaben nicht erlauben	Aktiviert
Netzwerkzugriff: Anonyme SID-/Namensübersetzung zulassen	Deaktiviert
Netzwerkzugriff: Die Verwendung von 'Jeder'-Berechtigungen für anonyme Benutzer ermöglichen	Deaktiviert
Netzwerkzugriff: Freigaben, auf die anonym zugegriffen werden kann	
Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten	Klassisch - lokale Benutzer authentifizieren sich als sie selbst
Netzwerkzugriff: Named Pipes, auf die anonym zugegriffen werden kann	
Netzwerkzugriff: Registrierungspfade, auf die von anderen Computern aus zugegriffen werden kann	
Netzwerkzugriff: Speicherung von Anmeldeinformationen oder .NET-Passports für die Netzwerkauthentifikation nicht erlauben	Aktiviert
Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden	Deaktiviert
Systemobjekte: Groß-/Kleinschreibung für Nicht-Windows-Subsysteme ignorieren	Aktiviert
Systemobjekte: Standardberechtigungen interner Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken	Aktiviert
Systemobjekte: Standardbesitzer für Objekte, die von Mitgliedern der Administratorengruppe erstellt werden	Objektersteller
Überwachung: Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen	Deaktiviert
Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können	Deaktiviert
Überwachung: Zugriff auf globale Systemobjekte prüfen	Deaktiviert

Sicherheitsoptionen	
Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen	Deaktiviert
Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen	Deaktiviert

Ereignisprotokoll	
Richtlinie	Computereinstellung
Anwendungsprotokoll aufbewahren für	Nicht definiert
Aufbewahrungsmethode des Anwendungsprotokolls	Ereignisse bei Bedarf überschreiben
Aufbewahrungsmethode des Sicherheitsprotokolls	Ereignisse bei Bedarf überschreiben Hinweis: Im Hochsicherheitsbereich ist folgende Einstellung zu wählen: Ereignisse nicht überschreiben (Protokoll manuell aufräumen)
Aufbewahrungsmethode des Systemprotokolls	Ereignisse bei Bedarf überschreiben
Lokalen Gastkontozugriff auf Anwendungsprotokoll verhindern	Aktiviert
Lokalen Gastkontozugriff auf Sicherheitsprotokoll verhindern	Aktiviert
Lokalen Gastkontozugriff auf Systemprotokoll verhindern	Aktiviert
Maximale Größe des Anwendungsprotokolls	30080 Kilobytes
Maximale Größe des Sicherheitsprotokolls	100992 Kilobytes
Maximale Größe des Systemprotokolls	30080 Kilobytes
Sicherheitsprotokoll aufbewahren für	Nicht definiert
Systemprotokoll aufbewahren für	Nicht definiert

Konfiguration der Systemdienste unter Windows XP (siehe M 4.246)

Im Folgenden werden Vorgaben für die Konfiguration der Systemdienste aufgezeigt, die als Ausgangsbasis für die Sicherheitseinstellungen dienen können. Es sei darauf hingewiesen, dass die Konfiguration einzelner Systemdienste immer von lokalen Gegebenheiten oder Anforderungen abhängt und daher immer im spezifischen Kontext zu sehen ist. Im Einzelfall muss sogar aufgrund lokaler Gegebenheiten auf weniger sichere Konfigurationen ausgewichen werden. Dann sollten aber zusätzliche Schutzmaßnahmen eingeleitet werden, die die fehlende Sicherheit in der Dienstkonfiguration ausgleichen. Beispiele hierfür sind der Einsatz einer zusätzlichen Firewall oder auch organisatorische Maßnahmen.

Dienstbezeichnung	Starttyp
Ablagemappe	Deaktiviert
Anmeldedienst	Automatisch
Anwendungsverwaltung	Deaktiviert
Arbeitsstationsdienst	Automatisch
ASP.NET-Statusdienst	Manuell
Automatische Updates	Automatisch
COM+ Eriegnissystem	Manuell
COM+ Systemanwendung	Manuell
Computerbrowser	Deaktiviert
Designs	Deaktiviert
DHCP-Client	Automatisch

Dienst für Seriennummern der tragbaren Medien	Deaktiviert
Dienstbezeichnung	Starttyp
Distributed Transaction Coordinator	Deaktiviert
DNS-Client	Automatisch
Druckwarteschlange	Automatisch
Eingabegerätezugang	Deaktiviert
Ereignisprotokoll	Automatisch
Fax Service	Deaktiviert
Fehlerberichterstattungsdienst	Deaktiviert
FTP-Publishing-Dienst	Deaktiviert
Gatewaydienst auf Anwendungsebene	Deaktiviert
Geschützter Speicher	Automatisch
Hilfe and Support	Automatisch
HTTP-SSL	Deaktiviert
IIS-Verwaltungsdienst	Deaktiviert
IMAPI-CD-Brenn-COM-Dienste	Deaktiviert
Indexdienst	Deaktiviert
Infrarotüberwachung	Deaktiviert
Intelligenter Hintergrundübertragungsdienst	Manuell
IPSec-Dienste	Deaktiviert
Kompatibilität für schnelle Benutzerumschaltung	Deaktiviert
Konfigurationsfreie drahtlose Verbindung	Deaktiviert
Kryptografiedienste	Automatisch
Leistungsdatenprotokolle und Warnungen	Manuell
MS Software Shadow Copy Provider	Deaktiviert
Nachrichtendienst	Deaktiviert
NetMeeting-Remotedesktop-Freigabe	Deaktiviert
Netzwerk-DDE-Dienst	Deaktiviert
Netzwerk-DDE-Serverdienst	Deaktiviert
Netzwerkverbindungen	Manuell
NLA (Network Location Awareness)	Manuell
NT-LM-Sicherheitsdienst	Manuell
Plug & Play	Automatisch
QoS-RSVP	Manuell
RAS-Verbindungsverwaltung	Deaktiviert
Remoteprozeduraufruf (RPC)	Automatisch
Remote-Registrierung	Automatisch
Routing and RAS	Deaktiviert
RPC-Locator	Manuell
Sekundäre Anmeldung	Automatisch
Server	Automatisch
Sicherheitskontenverwaltung	Automatisch
Sitzungs-Manager für Remotedesktop	Deaktiviert
Smartcard	Manuell
SSDP-Suchdienst	Manuell
Systemereignisbenachrichtigung	Automatisch
Systemwiederherstellungsdienst	Deaktiviert

Dienstbezeichnung	Starttyp
Taskplaner	Manuell
TCP/IP-NetBIOS-Hilfsprogramm	Automatisch
Telefonie	Manuell
Telnet	Deaktiviert
Terminaldienste	Manuell
Treibererweiterungen für Windows-Verwaltungsinstrumentation	Manuell
Überwachung verteilter Verknüpfungen (Client)	Deaktiviert
Universeller Plug & Play-Gerätehost	Deaktiviert
Unterbrechungsfreie Stromversorgung	Manuell
Upload-Manager	Automatisch
Verwaltung für automatische RAS-Verbindung	Deaktiviert
Verwaltung logischer Datenträger	Manuell
Verwaltungsdienst für die Verwaltung logischer Datenträger	Manuell
Volumenschattenkopie	Deaktiviert
Warndienst	Deaktiviert
WebClient	Deaktiviert
Wechselmedien	Deaktiviert
Windows Audio	Automatisch
Windows Bilderfassung (WIA)	Manuell
Windows Installer	Manuell
Windows-Firewall/Gemeinsame Nutzung der Internetverbindung	Deaktiviert
Windows-Verwaltungsadministration	Automatisch
Windows-Zeitgeber	Automatisch
WMI-Leistungsadapter	Manuell
WWW-Publishing-Dienst	Deaktiviert

Restriktive Berechtigungsvergabe unter Windows XP (siehe M 4.247)

Basiseinstellungen Benutzerrechte/Systemberechtigungen

Die nachfolgenden Vorgaben zeigen Sicherheitseinstellungen auf, die als Ausgangsbasis für die Sicherheitseinstellungen in der Windows XP Umgebung eines Unternehmens bzw. einer Behörde dienen können. Diese sollten vor dem Einsatz gegebenenfalls angepasst werden.

Lokale Richtlinien | Zuweisen von Benutzerrechten	
Richtlinie	Computereinstellung
Als Dienst anmelden	Definiert, aber leer
Ändern der Systemzeit	Administratoren
Anheben der Zeitplanungspriorität	Administratoren
Anmelden als Stapelverarbeitungsauftrag	Definiert, aber leer
Anmeldung als Batchauftrag verweigern	Nicht definiert
Anmeldung als Dienst verweigern	Nicht definiert
Anmeldung über Terminaldienste verweigern	Nicht definiert
Anmeldung über Terminaldienste zulassen	Nicht definiert
Annehmen der Clientidentität nach Authentifizierung	Nicht definiert

Lokale Richtlinien | Zuweisen von Benutzerrechten	
Anpassen von Speicherkontingenten für einen Prozess	
Auf diesen Computer vom Netzwerk aus zugreifen	Administratoren, Authentifizierte Benutzer
Auslassen der durchsuchenden Überprüfung	Jeder
Debuggen von Programmen	Nicht definiert
Durchführen von Volumenwartungsaufgaben	Administratoren
Einsetzen als Teil des Betriebssystems	Definiert, aber leer
Entfernen des Computers von der Dockingstation	Administratoren
Ermöglichen, dass Computer- und Benutzerkonten für Delegierungszwecke vertraut wird	Administratoren
Ersetzen eines Tokens auf Prozessebene	Definiert, aber leer
Erstellen einer Auslagerungsdatei	Administratoren
Erstellen eines Profils der Systemleistung	Administratoren
Erstellen eines Profils für einen Einzelprozess	Administratoren
Erstellen eines Tokenobjekts	Definiert, aber leer
Erstellen globaler Objekten	Administratoren
Erstellen von dauerhaft freigegebenen Objekten	Definiert, aber leer
Erzwingen des Herunterfahrens von einem Remotesystem aus	Administratoren
Generieren von Sicherheitsüberwachungen	Definiert, aber leer
Herunterfahren des Systems	Administratoren
Hinzufügen von Arbeitsstationen zur Domäne	Definiert, aber leer
Laden und Entfernen von Gerätetreibern	Administratoren
Lokal anmelden	Administratoren, Benutzer
Lokale Anmeldung verweigern	Gäste
Sichern von Dateien und Verzeichnissen	Sicherungs-Operatoren
Sperren von Seiten im Speicher	Definiert aber leer
Synchronisieren von Verzeichnisdienstdaten	Definiert, aber leer
Übernehmen des Besitzes von Dateien und Objekten	Administratoren
Verändern der Firmwareumgebungsvariablen	Administratoren
Verwalten von Überwachungs- und Sicherheitsprotokollen	Administratoren
Wiederherstellen von Dateien und Verzeichnissen	Administratoren
Zugriff vom Netzwerk auf diesen Computer verweigern	Nicht definiert

Zugriffsrechte für Systemverzeichnisse und -dateien

In der nachfolgenden Tabelle werden folgende Methoden verwendet:

- Propagieren: Die Zugriffsrechte werden zusätzlich zu existierenden vererbt, sofern anwendbar.
- Ersetzen: Die Zugriffsrechte werden ersetzt, sofern anwendbar.
- Ignorieren: Die bestehenden Zugriffsrechte sollen nicht ersetzt werden.

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%AllUserProfile%	Administratoren	Vollzugriff	Propagieren
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	

%AllUserProfile%\Anwendungsdaten	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer Benutzer	Vollzugriff Vollzugriff (Nur Unterordner und Dateien) Vollzugriff Lesen, Ausführen Schreiben (Diesen Ordner, Unterordner)	Propagieren

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%AllUserProfile%\Anwendungsdaten\ Microsoft	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Lesen, Ausführen	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\Crypto\DSS\MachineKeys	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Ordner auflisten, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen, Ordner erstellen, Attribute schreiben, Erweiterte Attribute schreiben, Berechtigungen lesen (Nur diesen Ordner)	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\Crypto\RSA\MachineKeys	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Ordner auflisten, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen, Ordner erstellen, Attribute schreiben, Erweiterte Attribute schreiebn, Berechtigungen lesen (Nur diesen Ordner)	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\Dr Watson	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer Benutzer	Vollzugriff Vollzugriff (Nur Unterordner und Dateien) Vollzugriff Lesen, Ausführen Ordner durchsuchen, Dateien erstellen, Ordner erstellen (Nur Unterordner und Dateien)	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\Dr Watson\drwtsn32.log	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterordner und Dateien) Vollzugriff Ändern	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\HTML Help	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff	Ersetzen
%AllUserProfile%\Anwendungsdaten\ Microsoft\Media Index	Administratoren SYSTEM Benutzer Benutzer Benutzer	Vollzugriff Vollzugriff Lesen, Ausführen Dateien erstellen, Ordner erstellen, Attribute schreiben, Erweiterte Attribute schreiben, Berechtigungen lesen (Nur diesen Ordner) Write (Nur Unterordner und Dateien)	Ersetzen

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%AllUserProfile%\Dokumente	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff	
		(Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
	Benutzer	Schreiben	
		(Diesen Ordner, Unterordner)	
%AllUserProfile%\Dokumente\desktop.ini	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%AllUsersProfile%\DRM			Ignorieren
%ProgramFiles%	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%	Administratoren	Vollzugriff	Propagieren
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\autoexec.bat %SystemDrive%\config.sys	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\boot.ini	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemDrive%\Dokumente und Einstellungen	Administratoren	Vollzugriff	Propagieren
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\Dokumente und Einstellungen\Administrator	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemDrive%\Dokumente und Einstellungen\Default User	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\io.sys	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\msdos.sys	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemDrive%\My Download Files	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Read, Write, Execute	
%SystemDrive%\ntbootdd.sys	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%SystemDrive%\ntdetect.com	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemDrive%\ntldr	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemDrive%\System Volume Information			Ignorieren
%SystemDrive%\Temp	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Ordner durchsuchen, Dateien erstellen, Ordner erstellen	
		(Diesen Ordner, Unterordner)	
%SystemRoot%	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemRoot%\$NtServicePackUninstall$	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemRoot%\$NtUninstall*	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemRoot%\CSC	Administratoren	Vollzugriff	Ersetzen
%SystemRoot%\debug	Administratoren	Vollzugriff	Propagieren
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemRoot%\debug\UserMode	Administratoren	Vollzugriff	Propagieren
	SYSTEM	Vollzugriff	
	Benutzer	Ordner durchsuchen, Ordner auflisten, Dateien erstellen	
		(Nur diesen Ordner)	
	Benutzer	Dateien erstellen, Ordner erstellen (Nur Dateien)	
%SystemRoot%\Debug\UserMode\userenv.log	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Daten schreiben, Daten anhängen	
%SystemRoot%\Installer	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemRoot%\Offline Web Pages			Ignorieren
%SystemRoot%\Prefetch	Administratoren	Vollzugriff (Nur diesen Ordner)	Ersetzen
	Administratoren	Lesen, Ausführen (Nur Dateien)	
	SYSTEM	Vollzugriff (Nur Dateien)	
%SystemRoot%\regedit.exe	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%SystemRoot%\Registration	Administratoren	Vollzugriff (Diesen Ordner, Dateien)	Ersetzen
	SYSTEM	Vollzugriff (Diesen Ordner, Dateien)	
	Benutzer	Read (Diesen Ordner, Dateien)	
%SystemRoot%\Registration\CRMLog	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Ordner durchsuchen, Ordner auflisten, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen, Berechtigungen lesen (Nur diesen Ordner)	
	Benutzer	Daten lesen, Attribute lesen, Erweiterte Attribute lesen, Write data, Daten anhängen, Attribute schreiben, Erweiterte Attribute schreiben, Delete, Berechtigungen lesen (Nur Dateien)	
%SystemRoot%\repair	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemRoot%\security	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
%SystemRoot%\system32	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemRoot%\system32\appmgmt	Administratoren	Vollzugriff	Propagieren
	SYSTEM	Vollzugriff	
	Benutzer	Lesen, Ausführen	
%SystemRoot%\system32\config	Administratoren	Vollzugriff	Ersetzen
	SYSTEM	Vollzugriff	
%SystemRoot%\system32\dllcache	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff (Nur Unterordner und Dateien)	
	SYSTEM	Vollzugriff	
%SystemRoot%\system32\Group Policy	Administratoren	Vollzugriff	Propagieren
	Authentifizierte Benutzer	Lesen, Ausführen	
	SYSTEM	Vollzugriff	
%SystemRoot%\system32\ias	Administratoren	Vollzugriff	Ersetzen
	ERSTELLER-BESITZER	Vollzugriff	
	SYSTEM	Vollzugriff	
%SystemRoot%\system32\MSDTC	Administratoren	Vollzugriff	Propagieren
	NETZWERKDIENST	Lesen, Schreiben, Ausführen	
	SYSTEM	Vollzugriff	

Verzeichnis/Datei	Benutzer/Gruppe	Zugriffsrecht	Methode
%SystemRoot%\system32\ arp.exe, at.exe, ciadv.msc, com\comexp.msc, compmgmt.msc, devmgmt.msc, dfrg.msc, diskmgmt.msc, eventvwr.msc, fsmgmt.msc, gpedit.msc, lusrmgr.msc, nbtstat.exe, netsh.exe, netstat.exe, nslookup.exe, Ntbackup.exe, ntmsmgr.msc, ntmsoprq.msc, perfmon.msc, rcp.exe, reg.exe, regedt32.exe, regini.exe, rexec.exe, route.exe, rsh.exe, RSoP.msc, secedit.exe, secpol.msc, services.msc, systeminfo.exe, tftp.exe, wmimgmt.msc	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
%SystemRoot%\system32\NTMSData	Administratoren SYSTEM	Vollzugriff Vollzugriff	Propagieren
%SystemRoot%\system32\Setup	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Lesen, Ausführen	Propagieren
%SystemRoot%\system32\spool\Printers	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterordner und Dateien) Vollzugriff Ordner durchsuchen, Attribute lesen, Erweiterte Attribute lesen, Dateien erstellen, Ordner erstellen (Diesen Ordner, Unterordner)	Ersetzen
%SystemRoot%\Tasks			Ignorieren
%SystemRoot%\Temp	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterordner und Dateien) Vollzugriff Ordner durchsuchen, Dateien erstellen, Ordner erstellen (Diesen Ordner, Unterordner)	Ersetzen

Zugriffsrechte Registrierung

HKCR\	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Ersetzen
\HKLM\SOFTWARE	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Ersetzen

\HKLM\SOFTWARE\Microsoft\Cryptography\Calais	Administratoren ERSTELLER-BESITZER LOKALER DIENST SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Wert abfragen, Wert festlegen, Unterschlüssel erstellen, Unterschlüssel auflisten, Benachrichtigen, Löschen, Lesekontrolle Vollzugriff Lesen	Ersetzen
\HKLM\SOFTWARE\Microsoft\MSDTC	Administratoren NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Wert abfragen, Wert festlegen, Unterschlüssel erstellen, Unterschlüssel auflisten, Benachrichtigen, Lesekontrolle Vollzugriff Lesen	Propagieren
\HKLM\SOFTWARE\Microsoft\MSDTC\Security\XAKey	Administratoren NETZWERKDIENST SYSTEM	Vollzugriff Wert abfragen, Wert festlegen, Unterschlüssel erstellen, Unterschlüssel auflisten, Benachrichtigen, Lesekontrolle Vollzugriff	Ersetzen
\HKLM\SOFTWARE\Microsoft\NetDDE	Administratoren ERSTELLER-BESITZER SYSTEM	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff	Ersetzen
\HKLM\SOFTWARE\Microsoft\UPnP Device Host	Administratoren ERSTELLER-BESITZER LOKALER DIENST SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Vollzugriff Lesen	Ersetzen
\HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AsrCommands	Administratoren Backup Operators ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Query, Wert festlegen, Unterschlüssel erstellen, Enumerate Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Ersetzen
\HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	Administratoren ERSTELLER-BESITZER INTERACTIVE NETZWERKDIENST SYSTEM	Vollzugriff Vollzugriff (Nur Unterschlüssel) Lesen Lesen Vollzugriff	Ersetzen
Windows NT\CurrentVersion\SeCEdit	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy	Administratoren Authentisierte Benutzer SYSTEM	Vollzugriff Lesen Vollzugriff	Propagieren
\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Lesen	Propagieren
\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	Administratoren Authentisierte Benutzer SYSTEM	Vollzugriff Lesen Vollzugriff	Propagieren

\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings	Administratoren Benutzer	Vollzugriff Lesen	Ersetzen
\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony	Administratoren ERSTELLER-BESITZER LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Vollzugriff Vollzugriff Lesen	Ersetzen
\HKLM\SYSTEM	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Ersetzen
\HKLM\SYSTEM\clone			Ignorieren
\HKLM\SYSTEM\controlset0*	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Control\Class	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Control\Network	Administratoren LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff Vollzugriff Lesen	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg	Administratoren Backup Operators LOKALER DIENST	Vollzugriff Lesen (Nur diesen Schlüssel) Lesen	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Control\Wmi\Security	Administratoren Administratoren ERSTELLER-BESITZER SYSTEM	Lesen Vollzugriff (Nur diesen Schlüssel) Vollzugriff (Nur diesen Schlüssel) Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Enum			Ignorieren
\HKLM\SYSTEM\CurrentControlSet\Hardware Profiles	Administratoren ERSTELLER-BESITZER SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\ClipSrv\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\CryptSvc\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen

\HKLM\SYSTEM\CurrentControlSet\Services\DNSCache	Administratoren LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Services\Ersvc\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\IRENUM\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Netbt	Administratoren LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Services\Netdde\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Netddedsdm\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\RemoteAccess	Administratoren LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Services\Rpcss\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Samss\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Scarddrv\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Scardsvr\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\ SNMP\Parameters\ValidCommunities	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Stisvc\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\SysmonLog\Log Queries	Administratoren ERSTELLER-BESITZER NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff Vollzugriff Lesen	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Tapisrv\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen

\HKLM\SYSTEM\CurrentControlSet\Services\Tcpip	Administratoren LOKALER DIENST NETZWERKDIENST SYSTEM Benutzer	Vollzugriff Vollzugriff Vollzugriff Vollzugriff Lesen	Propagieren
\HKLM\SYSTEM\CurrentControlSet\Services\W32time\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
\HKLM\SYSTEM\CurrentControlSet\Services\Wmi\Security	Administratoren SYSTEM	Vollzugriff Vollzugriff	Ersetzen
HKU\.DEFAULT	Administratoren Benutzer ERSTELLER-BESITZER SYSTEM	Vollzugriff Lesen Vollzugriff (Nur Unterschlüssel) Vollzugriff	Ersetzen
HKU\.DEFAULT\Software\Microsoft\NetDDE	Administratoren ERSTELLER-BESITZER SYSTEM	Vollzugriff Vollzugriff (Nur Unterschlüssel) Vollzugriff	Ersetzen
HKU\.DEFAULT\Software\Microsoft\SystemCertificates\Root\ProtectedRoots	Administratoren SYSTEM Benutzer	Vollzugriff Vollzugriff Lesen	Ersetzen