

User Account Control (UAC) - Benutzerkontensteuerung

Mitglieder der Gruppe **Administratoren** erhalten Split-Token.

a) Standard Token

whoami /groups

GRUPPENINFORMATIONEN

Gruppenname	Typ	SID	Attribute
Jeder	Bekannte Gruppe	S-1-1-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
W7\HomeUsers	Alias	S-1-5-21-3518013323-732246516-3825431306-1000	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
VORDEFINIERT\Administratoren	Alias	S-1-5-32-544	Gruppen, die nur zum Ablehnen verwendet wird
VORDEFINIERT\Benutzer	Alias	S-1-5-32-545	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\INTERAKTIV	Bekannte Gruppe	S-1-5-4	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
KONSOLEANMELDUNG	Bekannte Gruppe	S-1-2-1	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Authentifizierte Benutzer	Bekannte Gruppe	S-1-5-11	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Diese Organisation	Bekannte Gruppe	S-1-5-15	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
LOKAL	Bekannte Gruppe	S-1-2-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\NTLM-Authentifizierung	Bekannte Gruppe	S-1-5-64-10	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
Verbindliche Beschriftung\Mittlere Verbindlichkeitsstufe	Bezeichnung	S-1-16-8192	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

whoami /priv

BERECHTIGUNGSINFORMATIONEN

Berechtigungsname	Beschreibung	Status
SeShutdownPrivilege	Herunterfahren des Systems	Deaktiviert
SeChangeNotifyPrivilege	Auslassen der durchsuchenden Überprüfung	Aktiviert
SeUndockPrivilege	Entfernen des Computers von der Dockingstation	Deaktiviert
SeIncreaseWorkingSetPrivilege	Arbeitssatz eines Prozesses vergrößern	Deaktiviert
SeTimeZonePrivilege	Ändern der Zeitzone	Deaktiviert

b) elevated Token**whoami /groups**

GRUPPENINFORMATIONEN

Gruppenname	Typ	SID	Attribute
Jeder	Bekannte Gruppe	S-1-1-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
W7\HomeUsers	Alias	S-1-5-21-3518013323-732246516-3825431306-1000	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
VORDEFINIERT\Administratoren	Alias	S-1-5-32-544	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe, Gruppenbesitzer
VORDEFINIERT\Benutzer	Alias	S-1-5-32-545	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\INTERAKTIV	Bekannte Gruppe	S-1-5-4	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
KONSOLENANMELDUNG	Bekannte Gruppe	S-1-2-1	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Authentifizierte Benutzer	Bekannte Gruppe	S-1-5-11	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\Diese Organisation	Bekannte Gruppe	S-1-5-15	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
LOKAL	Bekannte Gruppe	S-1-2-0	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
NT-AUTORITÄT\NTLM-Authentifizierung	Bekannte Gruppe	S-1-5-64-10	Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe
Verbindliche Beschriftung\Hohe Verbindlichkeitsstufe Bezeichnung	S-1-16-12288		Verbindliche Gruppe, Standardmäßig aktiviert, Aktivierte Gruppe

whoami /priv

BERECHTIGUNGSINFORMATIONEN

Berechtigungsname	Beschreibung	Status
SeIncreaseQuotaPrivilege	Anpassen von Speicherkontingenten für einen Prozess	Deaktiviert
SeSecurityPrivilege	Verwalten von Überwachungs- und Sicherheitsprotokollen	Deaktiviert
SeTakeOwnershipPrivilege	Übernehmen des Besitzes von Dateien und Objekten	Deaktiviert
SeLoadDriverPrivilege	Laden und Entfernen von Gerätetreibern	Deaktiviert
SeSystemProfilePrivilege	Erstellen eines Profils der Systemleistung	Deaktiviert
SeSystemtimePrivilege	Ändern der Systemzeit	Deaktiviert
SeProfileSingleProcessPrivilege	Erstellen eines Profils für einen Einzelprozess	Deaktiviert
SeIncreaseBasePriorityPrivilege	Anheben der Zeitplanungspriorität	Deaktiviert
SeCreatePagefilePrivilege	Erstellen einer Auslagerungsdatei	Deaktiviert
SeBackupPrivilege	Sichern von Dateien und Verzeichnissen	Deaktiviert
SeRestorePrivilege	Wiederherstellen von Dateien und Verzeichnissen	Deaktiviert
SeShutdownPrivilege	Herunterfahren des Systems	Deaktiviert
SeDebugPrivilege	Debuggen von Programmen	Deaktiviert
SeSystemEnvironmentPrivilege	Verändern der Firmwareumgebungsvariablen	Deaktiviert
SeChangeNotifyPrivilege	Auslassen der durchsuchenden Überprüfung	Aktiviert
SeRemoteShutdownPrivilege	Erzwingen des Herunterfahrens von einem Remotesystem aus	Deaktiviert
SeUndockPrivilege	Entfernen des Computers von der Dockingstation	Deaktiviert
SeManageVolumePrivilege	Durchführen von Volumewartungsaufgaben	Deaktiviert
SeImpersonatePrivilege	Annehmen der Clientidentität nach Authentifizierung	Aktiviert
SeCreateGlobalPrivilege	Erstellen globaler Objekte	Aktiviert
SeIncreaseWorkingSetPrivilege	Arbeitssatz eines Prozesses vergrößern	Deaktiviert
SeTimeZonePrivilege	Ändern der Zeitzone	Deaktiviert
SeCreateSymbolicLinkPrivilege	Erstellen symbolischer Verknüpfungen	Deaktiviert