SID S-I-D Sicherheits ID

Windows verwendet zur Identifizierung von Objekten sogenannte SIDs (Security Identifier). SIDs bestehen aus einer folge alphanumerischer Werte. Jedes Objekt wie z.B. Benutzer, Computerkonten, Gruppen und Betriebssysteme erhalten eine eindeutige Windows-Sicherheitskennung (SID).

Eine SID besteht aus 4 Komponenten.

S-**1**-**5**-**32**-**544**

S = SID
1 = Revisionstand
5 = Bezeichner-Berechtigungswert
32 = Domänenkennung oder lokales System
544 = Benutzernummer (RID) - relative Kennung (Administrator)

SIDs für integrierte Konten und Gruppen haben immer die gleiche Domänenkennung „32", da sie auf jedem System vorhanden sind. Der Geltungsbereich für Konten und Gruppen beschränkt sich immer auf das lokale System, daher gibt es keine Unterschiede zu anderen Systemen.

Vordefinierte Konten und Gruppen müssen im Rahmen der vordefinierten Domäne voneinander unterschieden werden. Daher weist die SID für jedes Konto und jede Gruppe eine eindeutige relative Kennung auf. Ein relativer Bezeichnerwert von 544 ist unique und steht für die integrierte Administratorgruppe. Kein anderes Benutzerkonto oder Gruppe in der vordefinierten Domäne hat eine SID mit dem Wert 544.

Ein Beispiel:

Das ist eine SID der lokalen Gruppe Domänenadministratoren. Jede Domäne hat eine Gruppe Domänen-Admins mit unterschiedlicher SID wobei die relative Kennung 512 immer gleich ist.

S-1-5-21-1004336348-1177238915-682003330-512

Weitere SIDs:

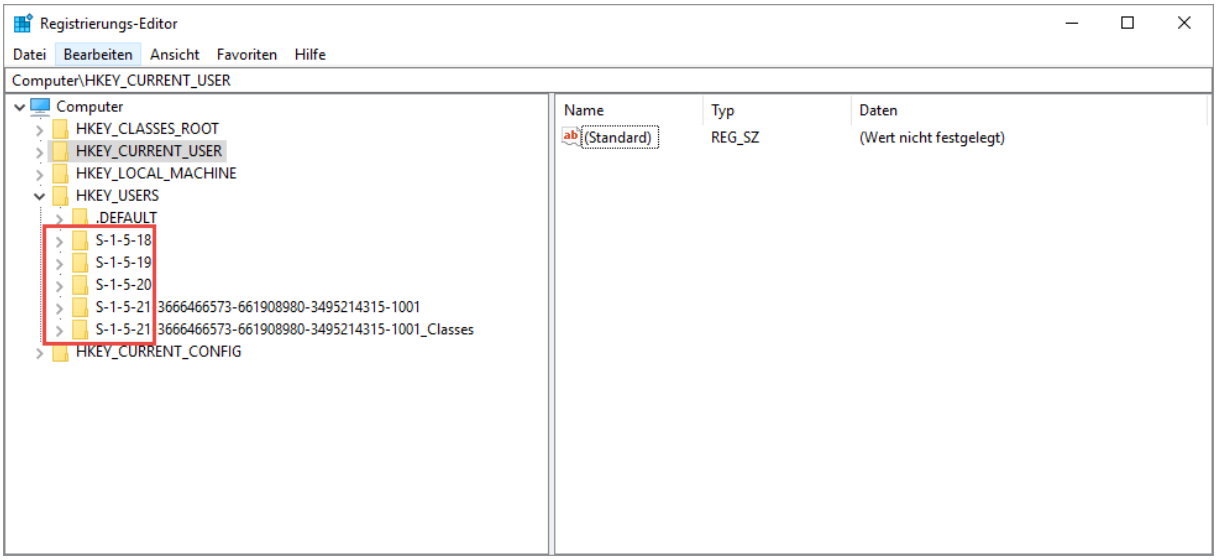
S-1-1-0	Everyone
S-1-5-14	Remote Interactive Logon
S-1-5-18	Local System, Service Account
S-1-5-19	NT Authority, Local Service
S-1-5-20	NT Authority, Network Service
S-1-5-29	Network Service

S-1-5-x-500	System Administrator
S-1-5-x-501	Guest User
S-1-5-x-512	Domain Admins
S-1-5-x-513	Domain Users
S-1-5-x-514	Domain Guest
S-1-6	Site Server Authority
S-1-7	Interner Site Authority
S-1-8	Exchange Authority
S-1-9	Ressource Manager Authority

x = Domain

Erstellt von Jörn Walter **01.01.2020**

SID S-I-D Sicherheits ID



Eine Liste bekannter und gängiger SIDs:

- SID: S-1-0
  Name: Null-Autorität
  Beschreibung: Bezeichnerautorität.

- SID: S-1-0-0
  Name: Niemand
  Beschreibung: Kein Sicherheitsprinzipal.

- SID: S-1-1
  Name: Globale Autorität
  Beschreibung: Bezeichnerautorität.

- SID: S-1-1-0
  Name: Jeder
  Beschreibung: Gruppe, die alle Benutzer einschließlich der anonymen Benutzer und Gäste enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

  Hinweis Auf Computern mit Windows XP Service Pack 2 (SP2) sind anonyme Benutzer standardmäßig nicht mehr Mitglied der Gruppe „Jeder".

- SID: S-1-2
  Name: Lokale Autorität
  Beschreibung: Bezeichnerautorität.

- SID: S-1-2-0

  Name: Lokal

  Beschreibung: Gruppe, die alle Benutzer enthält, die sich lokal angemeldet haben.

- SID: S-1-2-1

  Name: Konsolenanmeldung

  Beschreibung: Gruppe, die alle Benutzer enthält, die sich an der physischen Konsole angemeldet haben.

Hinweis Hinzugefügt in Windows 7 und Windows Server 2008 R2

- SID: S-1-3
  Name: Erstellerautorität
  Beschreibung: Bezeichnerautorität.
- SID: S-1-3-0
  Name: Ersteller-Besitzer
  Beschreibung: Platzhalter in einem vererbbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Objekterstellers.
- SID: S-1-3-1
  Name: Erstellergruppe
  Beschreibung: Platzhalter in einem vererbbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID für die primäre Gruppe des Objekterstellers. Die primäre Gruppe wird nur vom POSIX-Subsystem verwendet.
- SID: S-1-3-2
  Name: Ersteller-Besitzer-Server
  Beschreibung: Dieser SID wird in Windows 2000 nicht verwendet.
- SID: S-1-3-3
  Name: Ersteller-Gruppen-Server
  Beschreibung: Dieser SID wird in Windows 2000 nicht verwendet.
- SID: S-1-3-4 Name: Besitzerrechte

  Beschreibung: Gruppe, die den aktuellen Besitzer eines Objekts angibt. Wird ein ACE mit diesem SID auf ein Objekt angewendet, ignoriert das System die impliziten READ_CONTROL- und WRITE_DAC-Berechtigungen für den Objektbesitzer.
- SID: S-1-5-80-0
  Name: Alle Dienste
  Beschreibung: Gruppe, die alle auf dem System konfigurierten Dienstprozesse enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008
- SID: S-1-4
  Name: Nicht eindeutige Autorität
  Beschreibung: Bezeichnerautorität.
- SID: S-1-5
  Name: NT-Autorität
  Beschreibung: Bezeichnerautorität.
- SID: S-1-5-1
  Name: DFÜ
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich über eine DFÜ-Verbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

SID S-I-D Sicherheits ID

- SID: S-1-5-2
  Name: Netzwerk
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich über eine Netzwerkverbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-3
  Name: Batch
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich über eine Batch-Warteschlangeneinrichtung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-4
  Name: Interaktiv
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich interaktiv angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-5-X-Y
  Name: Anmeldesitzung
  Beschreibung: Eine Anmeldesitzung. Die X- und Y-Werte für diese SIDs unterscheiden sich von Sitzung zu Sitzung.
- SID: S-1-5-6
  Name: Dienst
  Beschreibung: Gruppe, die alle Sicherheitsprinzipale enthält, die sich als Dienst angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-7
  Name: Anonym
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich anonym angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-8
  Name: Proxy
  Beschreibung: Dieser SID wird in Windows 2000 nicht verwendet.
- SID: S-1-5-9
  Name: Domänencontroller der Organisation
  Beschreibung: Gruppe, die alle Domänencontroller in einer Gesamtstruktur enthält, die einen Verzeichnisdienst des Active Directory verwenden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-10
  Name: Selbstprinzipal
  Beschreibung: Platzhalter in einem vererbbaren ACE-Eintrag für ein Konto- oder Gruppenobjekt im Active Directory. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Sicherheitsprinzipals, dem das Konto gehört.
- SID: S-1-5-11
  Name: Authentifizierte Benutzer
  Beschreibung: Gruppe, die alle Benutzer enthält, deren Identitäten bei der Anmeldung authentifiziert wurden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

SID S-I-D Sicherheits ID

- SID: S-1-5-12
  Name: Eingeschränkter Code
  Beschreibung: Dieser SID ist für eine mögliche zukünftige Verwendung reserviert.
- SID: S-1-5-13
  Name: Terminalserverbenutzer
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich bei einem Terminaldiensteserver angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
- SID: S-1-5-14
  Name: Interaktive Remoteanmeldung
  Beschreibung: Gruppe, die alle Benutzer enthält, die sich über eine Terminaldiensteanmeldung angemeldet haben.
- SID: S-1-5-15
  Name: Diese Organisation
  Beschreibung: Gruppe, die alle Benutzer derselben Organisation enthält. Nur bei AD-Konten und Domänencontrollern ab Windows Server 2003 oder höheren Versionen.
- SID: S-1-5-17
  Name: Diese Organisation
  Beschreibung: Konto, das vom Standardbenutzer von Internetinformationsdienste (Internet Information Services, IIS) verwendet wird.
- SID: S-1-5-18
  Name: Lokales System
  Beschreibung: Dienstkonto, das vom Betriebssystem genutzt wird.
- SID: S-1-5-19
  Name: NT-Autorität
  Beschreibung: Lokaler Dienst
- SID: S-1-5-20
  Name: NT-Autorität
  Beschreibung: Netzwerkdienst
- SID: S-1-5-21**Domäne**-500
  Name: Administrator
  Beschreibung: Benutzerkonto für den Systemadministrator. Es handelt sich um das einzige Benutzerkonto, das standardmäßig uneingeschränkten Zugriff auf das System hat.
- SID: S-1-5-21**Domäne**-501
  Name: Gast
  Beschreibung: Benutzerkonto für Personen, die kein Einzelkonto haben. Für dieses Benutzerkonto ist kein Kennwort erforderlich. Standardmäßig ist das Gastkonto deaktiviert.
- SID: S-1-5-21**Domäne**-502
  Name: KRBTGT
  Beschreibung: Dienstkonto, das vom KDC-Dienst verwendet wird (KDC = Key Distribution Center = Schlüsselverteilungscenter).
- SID: S-1-5-21**Domäne**-512
  Name: Domänen-Admins

Beschreibung: Globale Gruppe, deren Mitglieder zur Verwaltung der Domäne berechtigt sind. Standardmäßig ist die Gruppe "Domänen-Admins" Mitglied der Administratorengruppe auf allen Computern, die der Domäne beigetreten sind, einschließlich der Domänencontroller. Die Gruppe "Domänen-Admins" ist der Standardbesitzer aller Objekte, die von einem Mitglied der Gruppe erstellt werden.

- SID: S-1-5-21**Domäne**-513
  Name: Domänenbenutzer
  Beschreibung: Globale Gruppe, die standardmäßig alle Benutzerkonten einer Domäne enthält. Wenn Sie in einer Domäne ein Benutzerkonto erstellen, wird es dieser Gruppe standardmäßig hinzugefügt.

- SID: S-1-5-21**Domäne**-514
  Name: Domänengäste
  Beschreibung: Globale Gruppe, die standardmäßig nur ein Mitglied hat (das in der Domäne vordefinierte Gastkonto).

- SID: S-1-5-21**Domäne**-515
  Name: Domänencomputer
  Beschreibung: Globale Gruppe, die alle Clients und Server enthält, die der Domäne beigetreten sind.

- SID: S-1-5-21**Domäne**-516
  Name: Domänencontroller
  Beschreibung: Globale Gruppe, die alle Domänencontroller einer Domäne enthält. Neue Domänencontroller werden dieser Gruppe standardmäßig hinzugefügt.

- SID: S-1-5-21**Domäne**-517
  Name: Zertifikatherausgeber
  Beschreibung: Globale Gruppe, die alle Computer enthält, auf denen Organisationszertifizierungsstellen betrieben werden. Zertifikatherausgeber sind berechtigt, Zertifikate für Benutzerobjekte im Active Directory zu veröffentlichen.

- SID: S-1-5-21**Stammdomäne**-518
  Name: Schema-Admins
  Beschreibung: Universelle Gruppe in einer Domäne mit einheitlichem Modus; globale Gruppe in einer Domäne mit gemischtem Modus. Die Gruppe ist berechtigt, Schemaänderungen im Active Directory vorzunehmen. Standardmäßig ist das Administratorkonto für die Gesamtstrukturdomäne einziges Mitglied dieser Gruppe.

- SID: S-1-5-21**Stammdomäne**-519
  Name: Organisations-Admins
  Beschreibung: Universelle Gruppe in einer Domäne mit einheitlichem Modus; globale Gruppe in einer Domäne mit gemischtem Modus. Die Gruppe ist berechtigt, Änderungen vorzunehmen, die die Gesamtstruktur des Active Directory betreffen wie z. B. das Hinzufügen von untergeordneten Domänen. Standardmäßig ist das Administratorkonto für die Gesamtstrukturdomäne einziges Mitglied dieser Gruppe.

- SID: S-1-5-21**Domäne**-520
  Name: Richtlinien-Ersteller-Besitzer
  Beschreibung: Globale Gruppe, die berechtigt ist, neue Gruppenrichtlinienobjekte im Active Directory zu erstellen. Standardmäßig ist der Administrator einziges Mitglied dieser Gruppe.

SID S-I-D Sicherheits ID

- SID: S-1-5-21**Domäne**-526
  Name: Schlüsseladministratoren
  Beschreibung: Eine Sicherheitsgruppe. Diese Gruppe verfügt über delegierten Schreibzugriff nur auf das Attribut „msdsKeyCredentialLink". Diese Gruppe eignet sich für Szenarien, in denen vertrauenswürdige externe Entitäten (z. B. Active Directory-Verbunddienste) für Änderungen an diesem Attribut verantwortlich sind. Nur vertrauenswürdige Administratoren sollten Mitglieder dieser Gruppe sein.

- SID: S-1-5-21**Domäne**-527
  Name: Unternehmensschlüsseladministratoren
  Beschreibung: Eine Sicherheitsgruppe. Diese Gruppe verfügt über delegierten Schreibzugriff nur auf das Attribut „msdsKeyCredentialLink". Diese Gruppe eignet sich für Szenarien, in denen vertrauenswürdige externe Entitäten (z. B. Active Directory-Verbunddienste) für Änderungen an diesem Attribut verantwortlich sind. Nur vertrauenswürdige Administratoren sollten Mitglieder dieser Gruppe sein.

- SID: S-1-5-21**Domäne**-553
  Name: RAS- und IAS-Server
  Beschreibung: Lokale Gruppe einer Domäne. Standardmäßig hat diese Gruppe keine Mitglieder. Server in dieser Gruppe haben Lesezugriff auf Kontenbeschränkungen und Anmeldeinformationen für Benutzerobjekte in der lokalen Domänengruppe des Active Directory.

- SID: S-1-5-32-544
  Name: Administratoren
  Beschreibung: Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist das Administratorkonto einziges Mitglied der Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe "Domänen-Admins" der Administratorengruppe hinzugefügt. Wenn ein Server zum Domänencontroller wird, wird die Gruppe "Organisations-Admins" ebenfalls zur Administratorengruppe hinzugefügt.

- SID: S-1-5-32-545
  Name: Benutzer
  Beschreibung: Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist die Gruppe der authentifizierten Benutzer einziges Mitglied dieser Gruppe. Wenn ein Computer einer Domäne beitritt, wird die Gruppe der Domänenbenutzer zur Benutzergruppe auf dem Computer hinzugefügt.

- SID: S-1-5-32-546
  Name: Gäste
  Beschreibung: Vordefinierte Gruppe. Standardmäßig ist das Gastkonto einziges Mitglied dieser Gruppe. Die Gästegruppe ermöglicht es Gelegenheitsbenutzern oder einmaligen Benutzern, sich mit eingeschränkten Berechtigungen über das vordefinierte Gastkonto auf einem Computer anzumelden.

- SID: S-1-5-32-547
  Name: Hauptbenutzer
  Beschreibung: Vordefinierte Gruppe. Standardmäßig hat diese Gruppe keine Mitglieder. Hauptbenutzer können lokale Benutzer und Gruppen erstellen, von ihnen selbst erstellte Konten ändern und löschen und Benutzer aus den Hauptbenutzer-, Benutzer- und Gästegruppen löschen. Hauptbesucher können

außerdem Programme installieren, lokale Drucker erstellen, verwalten und löschen sowie Dateifreigaben erstellen und löschen.

- SID: S-1-5-32-548
  Name: Konten-Operatoren
  Beschreibung: Vordefinierte Gruppe, die nur auf Domänencontrollern existiert. Standardmäßig hat diese Gruppe keine Mitglieder. Kontenoperatoren sind standardmäßig berechtigt, Konten für Benutzer, Gruppen und Computer in allen Containern und Organisationseinheiten des Active Directory zu erstellen, zu ändern und zu löschen; ausgenommen hiervon sind der vordefinierte Container und die Organisationseinheit der Domänencontroller. Kontenoperatoren sind nicht berechtigt, die Gruppen "Administratoren" und "Domain-Admins" zu ändern. Auch dürfen sie die Konten von Mitgliedern dieser Gruppen nicht ändern.

- SID: S-1-5-32-549
  Name: Server-Operatoren
  Beschreibung: Vordefinierte Gruppe, die nur auf Domänencontrollern existiert. Standardmäßig hat diese Gruppe keine Mitglieder. Serveroperatoren können sich interaktiv an einem Server anmelden, Netzwerkfreigaben erstellen und löschen, Dienste starten und stoppen, Dateien sichern und wiederherstellen, die Festplatte des Computers neu formatieren und den Computer herunterfahren.

- SID: S-1-5-32-550
  Name: Druck-Operatoren
  Beschreibung: Vordefinierte Gruppe, die nur auf Domänencontrollern existiert. Standardmäßig ist die Gruppe "Domänenbenutzer" einziges Mitglied dieser Gruppe. Druck-Operatoren können Drucker und Druckerwarteschlangen verwalten.

- SID: S-1-5-32-551
  Name: Sicherungs-Operatoren
  Beschreibung: Vordefinierte Gruppe. Standardmäßig hat diese Gruppe keine Mitglieder. Sicherungsoperatoren können alle Dateien auf einem Computer sichern und wiederherstellen, unabhängig von den Berechtigungen, durch die diese Dateien geschützt sind. Sicherungsoperatoren können sich außerdem bei dem Computer anmelden und ihn herunterfahren.

- SID: S-1-5-32-552
  Name: Replikatoren
  Beschreibung: Vordefinierte Gruppe, die vom Dateireplikationsdienst auf Domänencontrollern verwendet wird. Standardmäßig hat diese Gruppe keine Mitglieder. Fügen Sie dieser Gruppe keine Benutzer hinzu.

- SID: S-1-5-64-10
  Name: NTLM-Authentifizierung
  Beschreibung: Ein SID, der verwendet wird, wenn ein NTLM-Autentifizierungspaket den Client authentifiziert hat.

- SID: S-1-5-64-14
  Name: SChannel-Authentifizierung
  Beschreibung: Ein SID, der verwendet wird, wenn ein SChannel-Autentifizierungspaket den Client authentifiziert hat.

- SID: S-1-5-64-21
  Name: Digestauthentifizierung

SID S-I-D Sicherheits ID

Beschreibung: Ein SID, der verwendet wird, wenn ein Digestautentifizierungspaket den Client authentifiziert hat.

- SID: S-1-5-80
  Name: NT-Dienst
  Beschreibung: Ein NT-Dienstkontopräfix

- SID: S-1-5-80-0
  SID S-1-5-80-0 = NT SERVICES\ALL SERVICES
  Name: Alle Dienste
  Beschreibung: Gruppe, die alle auf dem System konfigurierten Dienstprozesse enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

  Hinweis Hinzugefügt in Windows Server 2008 R2

- SID: S-1-5-83-0
  Name: NT VIRTUAL MACHINE\Virtual Machines
  Beschreibung: Vordefinierte Gruppe. Diese Gruppe wird bei der Installation der Hyper-V-Rolle erstellt. Die Mitgliedschaft in der Gruppe wird durch den Hyper-V-Verwaltungsdienst (VMMS) verwaltet. Diese Gruppe benötigt die Berechtigungen „Erstellen symbolischer Verknüpfungen" (SeCreateSymbolicLinkPrivilege) und „Anmelden als Dienst" (SeServiceLogonRight).

  Hinweis Hinzugefügt in Windows 8 und Windows Server 2012

- SID: S-1-16-0
  Name: Nicht vertrauenswürdige Verbindlichkeitsstufe
  Beschreibung: Eine nicht vertrauenswürdige Integritätsebene Hinweis: Hinzugefügt in Windows Vista und Windows Server 2008

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-4096
  Name: Niedrige Verbindlichkeitsstufe
  Beschreibung: Eine niedrige Integritätsebene

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-8192
  Name: Mittlere Verbindlichkeitsstufe
  Beschreibung: Eine mittlere Integritätsebene

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-8448
  Name: Mittlere gehobene Verbindlichkeitsstufe
  Beschreibung: Eine mittlere gehobene Integritätsebene

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-12288
  Name: Hohe Verbindlichkeitsstufe
  Beschreibung: Eine hohe Integritätsebene

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

SID S-I-D Sicherheits ID

- SID: S-1-16-16384
  Name: Systemverbindlichkeitsstufe
  Beschreibung: Eine Systemintegritätsebene

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-20480
  Name: Verbindlichkeitsstufe für geschützte Prozesse
  Beschreibung: Eine Integritätsebene für geschützte Prozesse

  Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

- SID: S-1-16-28672
  Name: Verbindlichkeitsstufe für sichere Prozesse
  Beschreibung: Eine Integritätsebene für sichere Prozesse

Hinweis Hinzugefügt in Windows Vista und Windows Server 2008

Die folgenden Gruppen werden als SIDs angezeigt, bis ein Windows Server 2003-Domänencontroller zum Inhaber der Rolle „Betriebsmaster" des primären Domänencontrollers (PDC) gemacht wird. Der „Betriebsmaster" wird auch als FSMO (Flexible Single Master Operations) bezeichnet. Die folgenden zusätzlichen integrierten Gruppen werden erstellt, wenn ein Windows Server 2003-Domänencontroller zur Domäne hinzugefügt wird:

- SID: S-1-5-32-554
  Name: BUILTIN\Prä-Windows 2000 kompatibler Zugriff
  Beschreibung: Ein von Windows 2000 hinzugefügter Aliasname. Eine Abwärtskompatibilitätsgruppe, die den Lesezugriff auf alle Benutzer und Gruppen in der Domäne ermöglicht.

- SID: S-1-5-32-555
  Name: BUILTIN\Remotedesktopbenutzer
  Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe sind berechtigt, sich remote anzumelden.

- SID: S-1-5-32-556
  Name: BUILTIN\Netzwerkkonfigurations-Operatoren
  Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe können über bestimmte administrative Berechtigungen verfügen, um die Konfiguration von Netzwerkfeatures zu verwalten.

- SID: S-1-5-32-557
  Name: BUILTIN\Erstellungen eingehender Gesamtstrukturvertrauensstellung
  Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe können eingehende Einwegvertrauensstellungen für diese Gesamtstruktur erstellen.

- SID: S-1-5-32-558
  Name: BUILTIN\Systemmonitorbenutzer
  Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe haben zwecks Überwachung Remotezugriff auf diesen Computer.

- SID: S-1-5-32-559
  Name: BUILTIN\Leistungsprotokollbenutzer

Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe haben Remotezugriff, um eine Protokollierung der Leistungsindikatoren auf diesem Computer einzuplanen.

- SID: S-1-5-32-560
  Name: BUILTIN\Windows-Authentifizierungszugriffsgruppe
  Beschreibung: Ein Aliasname. Mitglieder dieser Gruppe haben Zugriff auf das berechnete Attribut "tokenGroupsGlobalAndUniversal" von Benutzerobjekten.
- SID: S-1-5-32-561
  Name: BUILTIN\Lizenzserver für Terminalserver
  Beschreibung: Ein Aliasname. Gruppe für Terminalserver-Lizenzserver. Bei der Installation von Windows Server 2003 Service Pack 1 wird eine neue lokale Gruppe erstellt.
- SID: S-1-5-32-562
  Name: BUILTIN\Distributed COM-Benutzer
  Beschreibung: Ein Aliasname. Eine Gruppe für COM, die computerweite Zugriffssteuerungen bereitstellt, mit denen der Zugriff auf alle Aufruf-, Aktivierungs- und Startanforderungen auf dem Computer verwaltet werden kann.

Die folgenden Gruppen werden als SIDs angezeigt, bis ein Windows Server 2008- oder Windows Server 2008 R2-Domänencontroller zum Inhaber der Rolle „Betriebsmaster" des primären Domänencontrollers (PDC) gemacht wird. Der „Betriebsmaster" wird auch als FSMO (Flexible Single Master Operations) bezeichnet. Die folgenden zusätzlichen integrierten Gruppen werden erstellt, wenn ein Windows Server 2008- oder Windows Server 2008 R2-Domänencontroller zur Domäne hinzugefügt wird:

- SID: S-1-5- 21*Domäne*-498
  Name: Domänencontroller der Organisation ohne Schreibzugriff
  Beschreibung: Eine universelle Gruppe. Mitglieder dieser Gruppe sind schreibgeschützte Domänencontroller in der Organisation
- SID: S-1-5- 21*Domäne* -521
  Name: Domänencontroller ohne Schreibzugriff
  Beschreibung: Eine globale Gruppe. Mitglieder dieser Gruppe sind schreibgeschützte Domänencontroller in der Domäne.
- SID: S-1-5-32-569
  Name: BUILTIN\Kryptografie-Operatoren
  Beschreibung: Eine vordefinierte lokale Gruppe. Mitglieder sind autorisiert, kryptografische Vorgänge durchzuführen.
- SID: S-1-5-21 *Domäne* -571
  Name: Zulässige RODC-Kennwortreplikationsgruppe
  Beschreibung: Lokale Gruppe einer Domäne. Mitglieder dieser Gruppe können ihr Kennwort auf alle schreibgeschützten Domänencontroller in der Domäne replizieren.
- SID: S-1-5- 21 *Domäne* -572
  Name: Abgelehnte RODC-Kennwortreplikationsgruppe
  Beschreibung: Lokale Gruppe einer Domäne. Mitglieder dieser Gruppe können ihr Kennwort nicht auf schreibgeschützte Domänencontroller in der Domäne replizieren.
- SID: S-1-5-32-573
  Name: BUILTIN\Ereignisprotokollleser

Beschreibung: Eine vordefinierte lokale Gruppe. Mitglieder dieser Gruppe können Ereignisprotokolle auf dem lokalen Computer lesen.

- SID: S-1-5-32-574
  Name: BUILTIN\Zertifikatdienst-DCOM-Zugriff
  Beschreibung: Eine vordefinierte lokale Gruppe. Mitglieder dieser Gruppe sind berechtigt, eine Verbindung zu Zertifizierungsstellen in der Organisation herzustellen.

Die folgenden Gruppen werden als SIDs angezeigt, bis ein Windows Server 2012-Domänencontroller zum Inhaber der Rolle „Betriebsmaster" des primären Domänencontrollers (PDC) gemacht wird. Der „Betriebsmaster" wird auch als FSMO (Flexible Single Master Operations) bezeichnet. Die folgenden zusätzlichen integrierten Gruppen werden erstellt, wenn ein Windows Server 2012-Domänencontroller zur Domäne hinzugefügt wird:

- SID: S-1-5-21-*Domäne*-522
  Name: Klonbare Domänencontroller
  Beschreibung: Eine globale Gruppe. Mitglieder dieser Gruppe, bei denen es sich um Domänencontroller handelt, können geklont werden.

- SID: S-1-5-32-575
  Name: BUILTIN\RDS Remote Access Servers
  Beschreibung: Eine vordefinierte lokale Gruppe. Die Server in dieser Gruppe ermöglichen den Benutzern von RemoteApp-Programmen und persönlichen virtuellen Desktops Zugriff auf diese Ressourcen. In Bereitstellungen mit Internetzugriff werden diese Server normalerweise in einem Umkreisnetzwerk bereitgestellt. Diese Gruppe muss auf Servern aufgefüllt werden, auf denen der RD-Verbindungsbroker läuft. Die in der Bereitstellung verwendeten RD-Gatewayserver und Server mit Web Access für Remotedesktop müssen in dieser Gruppe enthalten sein.

- SID: S-1-5-32-576
  Name: BUILTIN\RDS Endpoint Servers
  Beschreibung: Eine vordefinierte lokale Gruppe. Die Server in dieser Gruppe führen virtuelle Computer und Hostsitzungen aus, in denen RemoteApp-Programme und persönliche virtuelle Desktops laufen. Diese Gruppe muss auf Servern aufgefüllt werden, auf denen der RD-Verbindungsbroker läuft. Die in der Bereitstellung verwendeten RD-Sitzungshostserver und RD-Virtualisierungshosts müssen in dieser Gruppe enthalten sein.

- SID: S-1-5-32-577
  Name: BUILTIN\RDS Management Servers
  Beschreibung: Eine vordefinierte lokale Gruppe. Auf den Servern dieser Gruppe werden administrative Routineaktionen für Server ausgeführt, auf denen die Remotedesktopdienste installiert sind. Die Gruppe muss auf allen Servern aufgefüllt werden, die Teil der RDS-Bereitstellung sind Server, auf denen der zentrale RDS-Verwaltungsdienst ausgeführt wird, müssen dieser Gruppe angehören

- SID: S-1-5-32-578
  Name: BUILTIN\Hyper-V Administrators
  Beschreibung: Eine vordefinierte lokale Gruppe. Die Mitglieder dieser Gruppe erhalten uneingeschränkten Zugriff auf sämtliche Features von Hyper-V.

SID S-I-D Sicherheits ID

- SID: S-1-5-32-579
  Name: BUILTIN\Access Control Assistance Operators
  Beschreibung: Eine vordefinierte lokale Gruppe. Mitglieder dieser Gruppe können Autorisierungsattribute und Berechtigungen für Ressourcen auf dem Computer remote abfragen.
- SID: S-1-5-32-580
  Name: BUILTIN\Remote Management Users
  Beschreibung: Eine vordefinierte lokale Gruppe. Mitglieder dieser Gruppe können über Verwaltungsprotokolle auf WMI-Ressourcen zugreifen (z. B. WS-Verwaltung über den Windows-Remoteverwaltungsdienst). Dies gilt nur für WMI-Namespaces, die dem Benutzer Zugriff gewähren.

UNIVERSAL WELL-KNWON SID

S-1-0-0 Null SID A group with no members. This is often used when a SID value is not known.

S-1-1-0 World A group that includes all users.

S-1-2-0 Local Users who log on to terminals that are locally (physically) connected to the system.

S-1-2-1 Console Logon A group that includes users who are logged on to the physical console.

S-1-3-0 Creator Owner ID A security identifier to be replaced by the security identifier of the user who created a new object. This SID is used in inheritable ACEs.

S-1-3-1 Creator Group ID A security identifier to be replaced by the primary-group SID of the user who created a new object. Use this SID in inheritable ACEs.

S-1-3-2 Creator Owner Server

S-1-3-3 Creator Group Server

S-1-3-4 Owner Rights A group that represents the current owner of the object. When an ACE that carries this SID is applied to an object, the system ignores the implicit READ_CONTROL and WRITE_DAC permissions for the object owner.

S-1-4 Non-unique Authority A SID that represents an identifier authority.

S-1-5 NT Authority A SID that represents an identifier authority.

S-1-5-80-0

SECURITY_NT_AUTHORITY

S-1-5-1 Dialup A group that includes all users who are logged on to the system by means of a dial-up connection.

S-1-5-113 Local account You can use this SID when restricting network logon to local accounts instead of "administrator" or equivalent. This SID can be effective in blocking network logon for local users and groups by account type regardless of what they are actually named.

SID S-I-D Sicherheits ID

S-1-5-114 Local account and member of Administrators group You can use this SID when restricting network logon to local accounts instead of "administrator" or equivalent. This SID can be effective in blocking network logon for local users and groups by account type regardless of what they are actually named.

S-1-5-2 Network A group that includes all users who are logged on by means of a network connection. Access tokens for interactive users do not contain the Network SID.

S-1-5-3 Batch A group that includes all users who have logged on by means of a batch queue facility, such as task scheduler jobs.

S-1-5-4 Interactive A group that includes all users who log on interactively. A user can start an interactive logon session by logging on directly at the keyboard, by opening a Remote Desktop Services connection from a remote computer, or by using a remote shell such as Telnet. In each case, the user's access token contains the Interactive SID. If the user signs in by using a Remote Desktop Services connection, the user's access token also contains the Remote Interactive Logon SID.

S-1-5-5- *X *- *Y * Logon Session The *X * and *Y * values for these SIDs uniquely identify a particular logon session.

S-1-5-6 Service A group that includes all security principals that have signed in as a service.

S-1-5-7 Anonymous Logon A user who has connected to the computer without supplying a user name and password.

The Anonymous Logon identity is different from the identity that is used by Internet Information Services (IIS) for anonymous web access. IIS uses an actual account—by default, IUSR_ *ComputerName *, for anonymous access to resources on a website. Strictly speaking, such access is not anonymous because the security principal is known even though unidentified people are using the account. IUSR_ *ComputerName * (or whatever you name the account) has a password, and IIS logs on the account when the service starts. As a result, the IIS "anonymous" user is a member of Authenticated Users but Anonymous Logon is not.

S-1-5-8 Proxy Does not currently apply: this SID is not used.

S-1-5-9 Enterprise Domain Controllers A group that includes all domain controllers in a forest of domains.

S-1-5-10 Self A placeholder in an ACE for a user, group, or computer object in Active Directory. When you grant permissions to Self, you grant them to the security principal that is represented by the object. During an access check, the operating system replaces the SID for Self with the SID for the security principal that is represented by the object.

S-1-5-11 Authenticated Users A group that includes all users and computers with identities that have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password.

This group includes authenticated security principals from any trusted domain, not only the current domain.

SID S-I-D Sicherheits ID

S-1-5-12 Restricted Code An identity that is used by a process that is running in a restricted security context. In Windows and Windows Server operating systems, a software restriction policy can assign one of three security levels to code: unrestricted, restricted, or disallowed. When code runs at the restricted security level, the Restricted SID is added to the user's access token.

S-1-5-13 Terminal Server User A group that includes all users who sign in to a server with Remote Desktop Services enabled.

S-1-5-14 Remote Interactive Logon A group that includes all users who log on to the computer by using a remote desktop connection. This group is a subset of the Interactive group. Access tokens that contain the Remote Interactive Logon SID also contain the Interactive SID.

S-1-5-15 This Organization A group that includes all users from the same organization. Only included with Active Directory accounts and only added by a domain controller.

S-1-5-17 IIS_USRS An account that is used by the default Internet Information Services (IIS) user.

S-1-5-18 System (or LocalSystem) An identity that is used locally by the operating system and by services that are configured to sign in as LocalSystem.

System is a hidden member of Administrators. That is, any process running as System has the SID for the built-in Administrators group in its access token.

When a process that is running locally as System accesses network resources, it does so by using the computer's domain identity. Its access token on the remote computer includes the SID for the local computer's domain account plus SIDs for security groups that the computer is a member of, such as Domain Computers and Authenticated Users.

S-1-5-19 NT Authority (LocalService) An identity that is used by services that are local to the computer, have no need for extensive local access, and do not need authenticated network access. Services that run as LocalService access local resources as ordinary users, and they access network resources as anonymous users. As a result, a service that runs as LocalService has significantly less authority than a service that runs as LocalSystem locally and on the network.

S-1-5-20 Network Service An identity that is used by services that have no need for extensive local access but do need authenticated network access. Services running as NetworkService access local resources as ordinary users and access network resources by using the computer's identity. As a result, a service that runs as NetworkService has the same network access as a service that runs as LocalSystem, but it has significantly reduced local access.

S-1-5-domain-500 Administrator A user account for the system administrator. Every computer has a local Administrator account and every domain has a domain Administrator account.

The Administrator account is the first account created during operating system installation. The account cannot be deleted, disabled, or locked out, but it can be renamed.

By default, the Administrator account is a member of the Administrators group, and it cannot be removed from that group.

S-1-5-domain-501 Guest A user account for people who do not have individual accounts. Every computer has a local Guest account, and every domain has a domain Guest account.

By default, Guest is a member of the Everyone and the Guests groups. The domain Guest account is also a member of the Domain Guests and Domain Users groups.

Unlike Anonymous Logon, Guest is a real account, and it can be used to log on interactively. The Guest account does not require a password, but it can have one.

S-1-5-domain-502 krbtgt A user account that is used by the Key Distribution Center (KDC) service. The account exists only on domain controllers.

S-1-5-domain-512 Domain Admins A global group with members that are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined the domain, including domain controllers.

Domain Admins is the default owner of any object that is created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

S-1-5-domain-513 Domain Users A global group that includes all users in a domain. When you create a new User object in Active Directory, the user is automatically added to this group.

S-1-5-domain-514 Domain Guests A global group, which by default, has only one member: the domain's built-in Guest account.

S-1-5-domain-515 Domain Computers A global group that includes all computers that have joined the domain, excluding domain controllers.

S-1-5-domain-516 Domain Controllers A global group that includes all domain controllers in the domain. New domain controllers are added to this group automatically.

S-1-5-domain-517 Cert Publishers A global group that includes all computers that host an enterprise certification authority.

Cert Publishers are authorized to publish certificates for User objects in Active Directory.

S-1-5-root domain-518 Schema Admins A group that exists only in the forest root domain. It is a universal group if the domain is in native mode, and it is a global group if the domain is in mixed mode. The Schema Admins group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain.

S-1-5-root domain-519 Enterprise Admins A group that exists only in the forest root domain. It is a universal group if the domain is in native mode, and it is a global group if the domain is in mixed mode.

SID S-I-D Sicherheits ID

The Enterprise Admins group is authorized to make changes to the forest infrastructure, such as adding child domains, configuring sites, authorizing DHCP servers, and installing enterprise certification authorities.

By default, the only member of Enterprise Admins is the Administrator account for the forest root domain. The group is a default member of every Domain Admins group in the forest.

S-1-5-domain-520 Group Policy Creator Owners A global group that is authorized to create new Group Policy Objects in Active Directory. By default, the only member of the group is Administrator.

Objects that are created by members of Group Policy Creator Owners are owned by the individual user who creates them. In this way, the Group Policy Creator Owners group is unlike other administrative groups (such as Administrators and Domain Admins). Objects that are created by members of these groups are owned by the group rather than by the individual.

S-1-5-domain-553 RAS and IAS Servers A local domain group. By default, this group has no members. Computers that are running the Routing and Remote Access service are added to the group automatically.

Members of this group have access to certain properties of User objects, such as Read Account Restrictions, Read Logon Information, and Read Remote Access Information.

S-1-5-32-544 Administrators A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group.

S-1-5-32-545 Users A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group.