

Contents

Identitäts- und Zugriffsmanagement

Richtlinie für den technischen Support für verlorene oder vergessene Kennwörter

Übersicht über die Zugriffssteuerung

Übersicht über die dynamische Zugriffssteuerung

Sicherheitsbezeichner

Sicherheitsprinzipale

Lokale Konten

Active Directory-Konten

Microsoft-Konten

Dienstkonten

Active Directory-Sicherheitsgruppen

Besondere Identitäten

Benutzerkontensteuerung

Funktionsweise der Benutzerkontensteuerung

Sicherheitsrichtlinieneinstellungen für die Benutzerkontensteuerung

Gruppenrichtlinien und Einstellungen für Registrierungsschlüssel zur Benutzerkontensteuerung

Windows Hello for Business

Schützen abgeleiteter Domänenanmeldeinformationen mit Credential Guard

Funktionsweise von Credential Guard

Anforderungen von Credential Guard

Verwalten von Credential Guard

Von Credential Guard nicht abgedeckte Schutzszenarien

Überlegungen zur Verwendung von Credential Guard

Credential Guard: Weitere Risikominderungen

Credential Guard: Bekannte Probleme

Schützen von Remotedesktop-Anmeldeinformationen mit Remote Credential Guard

Smartcards

Funktionsweise der Smartcardanmeldung in Windows

Smartcardarchitektur

Zertifikatanforderungen und Enumeration

Smartcard und Remotedesktopdienste

Smartcards für den Windows-Dienst

Zertifikatverteilungsdienst

Dienst „Richtlinie zum Entfernen der Smartcard“

Tools und Einstellungen für Smartcards

Smartcards-Debuginformationen

Gruppenrichtlinien- und Registrierungseinstellungen für Smartcards

Smartcardereignisse

Virtuelle Smartcards

Grundlagen und Evaluierung virtueller Smartcards

Erste Schritte mit virtuellen Smartcards: Handbuch mit exemplarischer Vorgehensweise

Verwenden virtueller Smartcards

Bereitstellen virtueller Smartcards

Bewerten der Sicherheit virtueller Smartcards

Tpmvscmgr

Anheften von Enterprise-Zertifikaten

Installieren digitaler Zertifikate unter Windows 10 Mobile

Kurzanleitung zum Verhindern des Diebstahls von Windows10-Anmeldeinformationen

Konfigurieren von S/MIME für Windows 10 und Windows 10 Mobile

Technische VPN-Anleitung

VPN-Verbindungstypen

VPN-Routingentscheidungen

VPN-Authentifizierungsoptionen

VPN und bedingter Zugriff

VPN-Namensauflösung

Automatisch ausgelöste VPN-Profiloptionen

VPN-Sicherheitsfeatures

VPN-Profiloptionen

So konfigurieren Sie ein Diffie-Hellman-Protokoll über IKEv2-VPN-Verbindungen

Verwenden von Single Sign-On (SSO) über VPN- und WLAN-Verbindungen

Identitäts- und management

03.12.2019 • 2 minutes to read

Weitere Informationen zu Identitäts- und Zugriffsverwaltungstechnologien in Windows10 und Windows10 Mobile.

ABSCHNITT	BESCHREIBUNG
Richtlinien für den technischen Support für verlorene oder vergessene Kennwörter	Erläutert, wie Microsoft Ihnen beim Zurücksetzen eines verlorenen oder vergessenen Kennworts helfen kann, und enthält Links zu den entsprechenden Anweisungen.
Zugriffssteuerung	Beschreibt die Zugriffssteuerung in Windows, die das Verfahren zum Autorisieren von Benutzern, Gruppen und Computern für den Zugriff auf Objekte im Netzwerk oder Computer ist. Schlüsselkonzepte, die die Zugriffssteuerung ausmachen, sind Berechtigungen, Besitz von Objekten, Vererbung von Berechtigungen, Benutzerrechte und Objektüberwachung.
Konfigurieren von S/MIME für Windows 10 und Windows 10 Mobile	In Windows10 können Benutzer ausgehende Nachrichten und Anlagen von S/MIME verschlüsseln, sodass nur beabsichtigte Empfänger, die über eine digitale Identifikation (ID) verfügen, die auch als Zertifikat bezeichnet wird, diese lesen können. Benutzer können eine Nachricht digital signieren. So haben Empfänger eine Möglichkeit, die Identität des Absenders zu überprüfen und sicherzustellen, dass die Nachricht nicht manipuliert wurde.
Installieren digitaler Zertifikate unter Windows10 Mobile	Mit digitalen Zertifikaten wird die Identität eines Benutzers oder Computers an ein Schlüsselpaar gebunden, das zum Verschlüsseln und Signieren von digitalen Informationen verwendet werden kann. Zertifikate werden von einer Zertifizierungsstelle (ZS) ausgestellt, von der die Identität des Zertifikatinhabers bestätigt wird. Außerdem ermöglichen sie die sichere Clientkommunikation mit Websites und Diensten.
Schützen abgeleiteter Domänenanmeldeinformationen mit Credential Guard	Der in Windows10 Enterprise eingeführte Anmelde Informationsschutz verwendet auf Virtualisierung basierende Sicherheit, um Geheimnisse zu isolieren, damit nur privilegierte System Software darauf zugreifen kann. Ein nicht autorisierter Zugriff auf diese geheimen Schlüssel kann zu Angriffen mit dem Ziel des Diebstahls von Anmeldeinformationen, z.B. Pass-the-Hash oder Pass-The-Ticket, führen. Credential Guard verhindert diese Angriffe durch den Schutz von NTLM-Kennworthashes und Kerberos-TGTs.
Schützen von Remotedesktop-Anmeldeinformationen mit Remote Credential Guard	Mit Remote Credential Guard können Sie Ihre Anmeldeinformationen über eine Remotedesktopverbindung schützen, indem Kerberos-Anforderungen an das Gerät zurückgeleitet werden, das die Verbindung anfordert.

ABSCHNITT	BESCHREIBUNG
Benutzerkontensteuerung	Enthält Informationen zur Benutzerkontensteuerung (User Account Control, UAC), mit der verhindert wird, dass Malware einen PC schädigt, und Organisationen dabei helfen, einen besser verwalteten Desktop bereitzustellen. UAC kann helfen, die automatische Installation von nicht autorisierten apps zu blockieren und unbeabsichtigte Änderungen an den Systemeinstellungen zu verhindern.
Virtuelle Smartcards	Enthält Informationen zum Bereitstellen und Verwalten virtueller Smartcards, die mit physikalischen Smartcards vergleichbar sind und in Windows als immer eingefügte Smartcards angezeigt werden. Virtuelle Smartcards verwenden den TPM-Chip (Trusted Platform Module), der auf Computern in vielen Organisationen zur Verfügung steht, anstatt eine separate physische Smartcard und einen separaten Reader zu verwenden.
Technische VPN-Anleitung	Virtuelle private Netzwerke (VPN) bieten Ihren Benutzern sicheren Remotezugriff auf das Unternehmensnetzwerk. Windows10 fügt nützliche neue VPN-Profiloptionen hinzu, mit denen Sie die Verbindung zwischen Benutzern verwalten können.
Smartcards	Enthält eine Sammlung von Referenzthemen zu Smartcards, bei denen es sich um manipulationssichere tragbare Speichergeräte handelt, mit denen die Sicherheit von Aufgaben wie Authentifizierung von Clients, Signieren von Code, Sichern von e-Mails und Anmelden mit einem Windows-Domänenkonto verbessert werden kann.
Windows Hello for Business	In Windows10 ersetzt Windows Hello Kennwörter durch eine starke zweistufige Authentifizierung auf PCs und mobilen Geräten. Diese Authentifizierung besteht aus einer neuen Art von Benutzeranmeldeinformationen, die an ein Gerät und ein biometrisches Merkmal oder eine PIN gebunden sind.
Windows 10-Leitfaden für die Diebstahl Minderung von Anmeldeinformationen	Weitere Informationen finden Sie unter Eindämmung des Identitätsdiebstahls in Windows 10.

Richtlinien für den technischen Support für verlorene oder vergessene Kennwörter

03.12.2019 • 2 minutes to read

Microsoft nimmt die Sicherheit ernst. Dies dient zu Ihrem Schutz. Zu Microsoft-Konten, dem Windows-Betriebssystem und anderen Microsoft-Produkten gehören Kennwörter, die Ihnen helfen, Ihre Informationen zu schützen. Dieser Artikel enthält einige Optionen, mit denen Sie Ihr Kennwort zurücksetzen oder wiederherstellen können, wenn Sie es vergessen. Beachten Sie, dass Microsoft-Supporttechniker Ihnen beim Abrufen oder umgehen eines verloren gegangenen oder vergessenen Kennworts nicht helfen können, wenn diese Optionen nicht funktionieren.

Wenn Sie ein Kennwort verloren oder vergessen haben, können Sie die Links in diesem Artikel verwenden, um veröffentlichte Supportinformationen zu finden, die Ihnen beim Zurücksetzen des Kennworts helfen.

Zurücksetzen eines Kennworts für ein Domänenkonto

Wenn Sie das Kennwort für ein Domänenkonto verlieren oder vergessen, wenden Sie sich an Ihren IT-Administrator oder den Helpdesk. Weitere Informationen finden Sie unter [ändern oder Zurücksetzen Ihres Windows-Kennworts](#).

Zurücksetzen eines Kennworts für ein Microsoft-Konto

Wenn Sie das Kennwort für Ihr Microsoft-Konto verloren gehen oder vergessen haben, verwenden Sie den Assistenten zum [Wiederherstellen Ihres Kontos](#).

Dieser Assistent fordert ihre Sicherheitsbeweise an. Wenn Sie Ihre Sicherheitsbeweise vergessen haben oder keinen Zugriff mehr darauf haben, wählen Sie **Ich habe diesen nicht mehr**. Nachdem Sie diese Option ausgewählt haben, füllen Sie ein Formular für das Microsoft-Konto Team aus. Geben Sie so viele Informationen wie möglich in diesem Formular ein. Das Microsoft-Konto Team überprüft die von Ihnen bereitgestellten Informationen, um festzustellen, ob Sie der Kontoinhaber sind. Diese Entscheidung ist endgültig. Microsoft hat keinen Einfluss auf die Wahlmöglichkeiten des Teams.

Zurücksetzen eines Kennworts für ein lokales Konto auf einem Windows-Gerät

Lokale Konten auf einem Gerät umfassen das Administrator Konto des Geräts.

Windows 10

Wenn Sie das Kennwort für ein lokales Konto auf einem Gerät, auf dem Windows 10 ausgeführt wird, verlieren oder vergessen, lesen Sie [Zurücksetzen des Kennworts für Ihr lokales Windows 10-Konto](#).

Windows 8,1 oder Windows 7

Wenn Sie das Kennwort für ein lokales Konto auf einem Gerät, auf dem Windows 8,1 oder Windows 7 ausgeführt wird, verlieren oder vergessen, lesen Sie [ändern oder Zurücksetzen Ihres Windows-Kennworts](#). In diesem Artikel können Sie die Version des Betriebssystems im Menü **Produktversion auswählen** auswählen.

Zurücksetzen eines Hardware-BIOS-Kennworts

Wenn Sie das Kennwort für das Hardware-BIOS eines Geräts verloren gehen oder vergessen, wenden Sie sich an

den Gerätehersteller, um Hilfe und Support zu erhalten. Wenn Sie sich online mit dem Hersteller in Verbindung setzen, stellen Sie sicher, dass Sie die Website des Herstellers besuchen und nicht die Website von Drittanbietern.

Zurücksetzen eines Kennworts für eine einzelne Datei

In einigen Anwendungen können Sie einzelne Dateien mit einem Kennwort schützen. Wenn Sie ein solches Kennwort verloren oder vergessen haben, können Sie sich darauf verlassen, dass diese Anwendung Sie nur zurücksetzt oder wiederherstellen kann. Microsoft-Supporttechniker können Ihnen beim Zurücksetzen, Abrufen oder umgehen solcher Kennwörter nicht helfen.

Verwenden von Kennwort-Tools von Drittanbietern

Einige Drittanbieter behaupten, Kennwörter umgehen zu können, die auf Dateien und Funktionen angewendet wurden, die von Microsoft-Programmen verwendet werden. Aus rechtlichen Gründen können wir keines dieser Unternehmen empfehlen oder bestätigen. Wenn Sie Hilfe beim umgehen oder Zurücksetzen eines Kennworts benötigen, können Sie eine Drittpartei für diese Hilfe suchen und kontaktieren. Sie verwenden diese Produkte und Dienstleistungen von Drittanbietern jedoch auf Ihr eigenes Risiko.

Übersicht über die Zugriffssteuerung

12.09.2019 • 5 minutes to read

Betrifft

- Windows10
- Windows Server 2016

In diesem Thema für den IT-Experten wird die Zugriffssteuerung in Windows beschrieben, bei der Benutzer, Gruppen und Computer für den Zugriff auf Objekte im Netzwerk oder Computer autorisiert werden. Schlüsselkonzepte, die die Zugriffssteuerung ausmachen, sind Berechtigungen, Besitz von Objekten, Vererbung von Berechtigungen, Benutzerrechte und Objektüberwachung.

Featurebeschreibung

Auf Computern, auf denen eine unterstützte Version von Windows ausgeführt wird, kann die Verwendung von System- und Netzwerkressourcen über die miteinander verknüpften Authentifizierungs- und Autorisierungsmechanismen gesteuert werden. Nachdem ein Benutzer authentifiziert wurde, verwendet das Windows-Betriebssystem integrierte Autorisierungs- und Zugriffssteuerungstechnologien, um die zweite Phase des Schutzes von Ressourcen zu implementieren: ermitteln, ob ein authentifizierter Benutzer über die richtigen Berechtigungen für den Zugriff auf eine Ressource verfügt.

Freigegebene Ressourcen stehen Benutzern und Gruppen außer dem Besitzer der Ressource zur Verfügung und müssen vor unbefugter Verwendung geschützt werden. Im Modell für die Zugriffssteuerung werden Benutzer und Gruppen (auch als "Sicherheitsprinzipale" bezeichnet) durch eindeutige Sicherheits-IDs (SIDs) dargestellt. Ihnen werden Rechte und Berechtigungen zugewiesen, die das Betriebssystem informieren, was die einzelnen Benutzer und Gruppen tun können. Jede Ressource verfügt über einen Besitzer, der Sicherheitsprinzipalen Berechtigungen gewährt. Während der Zugriffs Kontroll Überprüfung werden diese Berechtigungen überprüft, um zu ermitteln, welche Sicherheitsprinzipale auf die Ressource zugreifen können und wie Sie darauf zugreifen können.

Sicherheitsprinzipale führen Aktionen (einschließlich lesen, schreiben, ändern oder Vollzugriff) für Objekte aus. Objekte umfassen Dateien, Ordner, Drucker, Registrierungsschlüssel und Active Directory-Domänendienste (AD DS)-Objekte. Freigegebene Ressourcen verwenden Zugriffssteuerungslisten (ACLs), um Berechtigungen zuzuweisen. Auf diese Weise können Ressourcenmanager die Zugriffssteuerung wie folgt erzwingen:

- Verweigern des Zugriffs auf nicht autorisierte Benutzer und Gruppen
- Festlegen von klar definierten Grenzwerten für den Zugriff, der für autorisierte Benutzer und Gruppen bereitgestellt wird

Objektbesitzer erteilen im allgemeinen Berechtigungen für Sicherheitsgruppen und nicht für einzelne Benutzer. Benutzer und Computer, die vorhandenen Gruppen hinzugefügt werden, übernehmen die Berechtigungen dieser Gruppe. Wenn ein Objekt (beispielsweise ein Ordner) andere Objekte (wie Unterordner und Dateien) enthalten kann, wird es als Container bezeichnet. In einer Hierarchie von Objekten wird die Beziehung zwischen einem Container und dessen Inhalt durch Verweisen auf den Container als übergeordnetes Element ausgedrückt. Ein Objekt im Container wird als untergeordnetes Element bezeichnet, und das untergeordnete Element erbt die Zugriffssteuerungseinstellungen des übergeordneten Elements. Objektbesitzer definieren häufig Berechtigungen für Containerobjekte anstelle einzelner untergeordneter Objekte, um die Verwaltung von Zugriffssteuerungen zu vereinfachen.

Dieser Inhaltssatz enthält:

- [Übersicht über die dynamische Zugriffssteuerung](#)
- [Sicherheitsbezeichner](#)
- [Sicherheitsprinzipale](#)
 - [Lokale Konten](#)
 - [Active Directory-Konten](#)
 - [Microsoft-Konten](#)
 - [Dienstkonten](#)
 - [Active Directory-Sicherheitsgruppen](#)

Praktische Anwendungsfälle

Administratoren, die die unterstützte Version von Windows verwenden, können die Anwendung und Verwaltung der Zugriffssteuerung auf Objekte und Themen einschränken, um die folgende Sicherheit zu gewährleisten:

- Schützen Sie eine größere Anzahl und Vielfalt von Netzwerkressourcen vor Missbrauch.
- Bereitstellen von Benutzern für den Zugriff auf Ressourcen auf eine Weise, die mit den Organisationsrichtlinien und den Anforderungen ihrer Aufgaben in Einklang steht.
- Ermöglichen Sie Benutzern den Zugriff auf Ressourcen von einer Vielzahl von Geräten an verschiedenen Standorten.
- Aktualisieren Sie die Benutzer Fähigkeit, regelmäßig auf Ressourcen zuzugreifen, wenn sich die Richtlinien einer Organisation ändern oder sich die Aufgaben der Benutzer ändern.
- Berücksichtigen Sie eine wachsende Zahl von Nutzungsszenarien (wie Zugriff von Remotestandorten oder von einer schnell wachsenden Vielzahl von Geräten wie Tablet-Computern und Mobiltelefonen).
- Identifizieren und Beheben von Zugriffsproblemen, wenn legitime Benutzer nicht auf Ressourcen zugreifen können, die Sie zum Ausführen ihrer Aufgaben benötigen.

Berechtigungen

Berechtigungen definieren den Typ des Zugriffs, der einem Benutzer oder einer Gruppe für ein Objekt oder eine Objekteigenschaft gewährt wird. Beispielsweise kann der Gruppe "Finanzen" Lese- und Schreibberechtigungen für eine Datei mit dem Namen Payroll. dat gewährt werden.

Mithilfe der Benutzeroberfläche für die Zugriffssteuerung können Sie NTFS-Berechtigungen für Objekte wie Dateien, Active Directory-Objekte, Registrierungsobjekte oder Systemobjekte wie Prozesse festlegen. Berechtigungen können Benutzern, Gruppen oder Computern gewährt werden. Es empfiehlt sich, Gruppen Berechtigungen zuzuweisen, da dadurch die Systemleistung verbessert wird, wenn der Zugriff auf ein Objekt überprüft wird.

Für jedes Objekt können Sie folgende Berechtigungen erteilen:

- Gruppen, Benutzer und andere Objekte mit Sicherheitskennungen in der Domäne.
- Gruppen und Benutzer in dieser Domäne und alle vertrauenswürdigen Domänen.
- Lokale Gruppen und Benutzer auf dem Computer, auf dem sich das Objekt befindet.

Die an ein Objekt angefügten Berechtigungen hängen vom Typ des Objekts ab. Beispielsweise unterscheiden sich die Berechtigungen, die an eine Datei angefügt werden können, von denen, die an einen Registrierungsschlüssel angefügt werden können. Einige Berechtigungen sind jedoch für die meisten Objekttypen üblich. Diese

allgemeinen Berechtigungen lauten wie folgt:

- Lesen
- Ändern
- Besitzer ändern
- Delete

Wenn Sie Berechtigungen festlegen, geben Sie die Zugriffsebene für Gruppen und Benutzer an. So können Sie beispielsweise zulassen, dass ein Benutzer den Inhalt einer Datei liest, dass ein anderer Benutzer Änderungen an der Datei vorzunehmen und alle anderen Benutzer daran hindern, auf die Datei zuzugreifen. Sie können ähnliche Berechtigungen für Drucker festlegen, damit bestimmte Benutzer den Drucker konfigurieren können und andere Benutzer nur drucken können.

Wenn Sie die Berechtigungen für eine Datei ändern müssen, können Sie Windows-Explorer ausführen, mit der rechten Maustaste auf den Dateinamen klicken und dann auf **Eigenschaften** klicken. Auf der Registerkarte **Sicherheit** können Sie die Berechtigungen für die Datei ändern. Weitere Informationen finden Sie unter [Verwalten von Berechtigungen](#).

Hinweis eine andere Art von Berechtigungen, so genannte Freigabeberechtigungen, wird auf der Registerkarte Freigabe der **Eigenschaften** Seite eines Ordners oder mithilfe des Assistenten für freigegebene Ordner festgesetzt. Weitere Informationen finden Sie unter [Freigabe- und NTFS-Berechtigungen auf einem Datei Server](#).

Besitz von Objekten

Ein Besitzer wird einem Objekt zugewiesen, wenn dieses Objekt erstellt wird. Standardmäßig ist der Besitzer der Ersteller des Objekts. Unabhängig davon, welche Berechtigungen für ein Objekt eingestellt werden, kann der Besitzer des Objekts immer die Berechtigungen ändern. Weitere Informationen finden Sie unter [Verwalten des Objektbesitzes](#).

Vererbung von Berechtigungen

Durch Vererbung können Administratoren Berechtigungen einfach zuweisen und verwalten. Dieses Feature bewirkt automatisch, dass Objekte in einem Container alle vererbten Berechtigungen dieses Containers erben. Beispielsweise erben die Dateien in einem Ordner die Berechtigungen des Ordners. Nur Berechtigungen, die als geerbt markiert sind, werden geerbt.

Benutzerrechte

Benutzerrechte gewähren Benutzern und Gruppen in Ihrer Computerumgebung bestimmte Berechtigungen und Anmelderechte. Administratoren können bestimmte Rechte für Gruppenkonten oder einzelne Benutzerkonten zuweisen. Diese Rechte autorisieren Benutzern, bestimmte Aktionen auszuführen, wie beispielsweise die interaktive Anmeldung bei einem System oder das Sichern von Dateien und Verzeichnissen.

Benutzerrechte unterscheiden sich von den Berechtigungen, da Benutzerrechte für Benutzerkonten gelten und den Objekten Berechtigungen zugeordnet sind. Obwohl Benutzerrechte auf einzelne Benutzerkonten zutreffen können, werden Benutzerrechte am besten auf der Basis eines Gruppenkontos verwaltet. Die Benutzeroberfläche der Zugriffssteuerung bietet keine Unterstützung, um Benutzerrechte zu gewähren. Die Zuweisung von Benutzerrechten kann jedoch über **Lokale Sicherheitseinstellungen** verwaltet werden.

Weitere Informationen zu Benutzerrechten finden Sie unter [Zuweisen von Benutzerrechten](#).

Objektüberwachung

Mit den Berechtigungen des Administrators können Sie den erfolgreichen oder fehlgeschlagenen Zugriff von Benutzern auf Objekte überwachen. Sie können mithilfe der Benutzeroberfläche für die Zugriffssteuerung auswählen, welcher Objektzugriff überwacht werden soll, doch müssen Sie zuerst die Überwachungsrichtlinie

aktivieren, indem Sie unter **lokale Richtlinien** in den **lokalen Sicherheitseinstellungen** die Option **Überwachungsobjektzugriff** auswählen. Sie können diese sicherheitsrelevanten Ereignisse dann im Sicherheitsprotokoll in der Ereignisanzeige anzeigen.

Weitere Informationen zur Überwachung finden Sie unter [Übersicht über die Sicherheitsüberwachung](#).

Weitere Informationen:

- Weitere Informationen zur Zugriffssteuerung und Autorisierung finden Sie unter [Zugriffssteuerung und Autorisierung \(Übersicht\)](#).

Übersicht über die dynamische Zugriffssteuerung

12.09.2019 • 8 minutes to read

Betrifft

- Windows Server 2016

Dieses Übersichtsthema für den IT-Experten beschreibt die dynamische Zugriffssteuerung und die zugehörigen Elemente, die in Windows Server 2012 und Windows 8 eingeführt wurden.

Mithilfe der domänenbasierten dynamischen Zugriffssteuerung können Administratoren Zugriffssteuerungsberechtigungen und -Einschränkungen auf Grundlage klar definierter Regeln anwenden, die die Vertraulichkeit der Ressourcen, des Auftrags oder der Rolle des Benutzers sowie die Konfiguration des Geräts berücksichtigen können, das wird für den Zugriff auf diese Ressourcen verwendet.

Beispielsweise kann ein Benutzer unterschiedliche Berechtigungen besitzen, wenn er auf eine Ressource von seinem Office-Computer aus zugreift, und zwar im Vergleich mit einem tragbaren Computer über ein virtuelles privates Netzwerk. Oder der Zugriff ist nur möglich, wenn ein Gerät die Sicherheitsanforderungen erfüllt, die von den Netzwerkadministratoren definiert werden. Bei Verwendung der dynamischen Zugriffssteuerung ändern sich die Berechtigungen eines Benutzers dynamisch ohne zusätzlichen Administratoreingriff, wenn sich die Position oder Rolle des Benutzers ändert (was zu Änderungen an den Kontoattributen des Benutzers in AD DS führt). Ausführlichere Beispiele für die Verwendung der dynamischen Zugriffssteuerung finden Sie in den in der [dynamischen Zugriffssteuerung beschriebenen Szenarien: Szenario \(Übersicht\)](#).

Die dynamische Zugriffssteuerung wird unter Windows-Betriebssystemen vor Windows Server 2012 und Windows 8 nicht unterstützt. Wenn die dynamische Zugriffssteuerung in Umgebungen mit unterstützten und nicht unterstützten Versionen von Windows konfiguriert ist, werden die Änderungen nur von den unterstützten Versionen implementiert.

Zu den Features und Konzepten, die mit der dynamischen Zugriffssteuerung verbunden sind, gehören:

- [Zentrale Zugriffsregeln](#)
- [Richtlinien für den zentralen Zugriff](#)
- [Ansprüche](#)
- [Ausdrücke](#)
- [Vorgeschlagene Berechtigungen](#)

Zentrale Zugriffsregeln

Eine zentrale Zugriffsregel ist ein Ausdruck von Autorisierungsregeln, die eine oder mehrere Bedingungen einbeziehen können, die Benutzergruppen, benutzeransprüche, Geräteansprüche und Ressourceneigenschaften umfassen. Mehrere zentrale Zugriffsregeln können zu einer zentralen Zugriffsrichtlinie kombiniert werden.

Wenn eine oder mehrere zentrale Zugriffsregeln für eine Domäne definiert wurden, können Dateifreigabe Administratoren bestimmte Regeln mit bestimmten Ressourcen und geschäftlichen Anforderungen abgleichen.

Richtlinien für den zentralen Zugriff

Zentrale Zugriffsrichtlinien sind Autorisierungsrichtlinien, die bedingte Ausdrücke enthalten. Angenommen, eine Organisation hat eine geschäftliche Anforderung, den Zugriff auf personenbezogene Informationen (PII) in Dateien nur auf den Dateibesitzer und die Mitglieder der Personalabteilung (HR) zu beschränken, die personenbezogene Informationen anzeigen dürfen. Dies stellt eine organisationsweite Richtlinie dar, die für PII-

Dateien gilt, unabhängig davon, wo Sie sich auf Dateiservern in der gesamten Organisation befinden. Um diese Richtlinie zu implementieren, muss eine Organisation in der Lage sein, Folgendes zu tun:

- Identifizieren und markieren Sie die Dateien, in denen die PII enthalten sind.
- Identifizieren Sie die Gruppe von Personalmitgliedern, die berechtigt sind, die PII-Informationen anzuzeigen.
- Fügen Sie die zentrale Zugriffsrichtlinie einer zentralen Zugriffsregel hinzu, und wenden Sie die zentrale Zugriffsregel auf alle Dateien an, die die PII enthalten, unabhängig davon, wo Sie sich auf den Dateiservern in der gesamten Organisation befinden.

Zentrale Zugriffsrichtlinien fungieren als Sicherheitsschirme, die von einer Organisation auf Ihren Servern angewendet werden. Diese Richtlinien sind zusätzlich zu den lokalen Zugriffsrichtlinien oder DACLs (Discretionary Access Control Lists), die auf Dateien und Ordner angewendet werden (aber nicht ersetzen).

Ansprüche

Bei einem Anspruch handelt es sich um eine eindeutige Information zu einem Benutzer, Gerät oder einer Ressource, die von einem Domänencontroller veröffentlicht wurde. Der Titel des Benutzers, die Abteilungs Klassifizierung einer Datei oder der Integritätsstatus eines Computers sind gültige Beispiele für einen Anspruch. Eine Entität kann mehr als einen Anspruch umfassen, und eine beliebige Kombination von Ansprüchen kann verwendet werden, um den Zugriff auf Ressourcen zu autorisieren. Die folgenden Arten von Ansprüchen sind in den unterstützten Versionen von Windows verfügbar:

- **Benutzeransprüche** Active Directory-Attribute, die einem bestimmten Benutzer zugeordnet sind.
- **Geräteansprüche** Active Directory-Attribute, die einem bestimmten Computerobjekt zugeordnet sind.
- **Ressourcenattribute** Globale Ressourceneigenschaften, die für die Verwendung in Autorisierungsentscheidungen markiert und in Active Directory veröffentlicht werden.

Mit Ansprüchen können Administratoren präzise Organisations-oder unternehmensweite Aussagen zu Benutzern, Geräten und Ressourcen vornehmen, die in Ausdrücke, Regeln und Richtlinien integriert werden können.

Ausdrücke

Bedingte Ausdrücke stellen eine Erweiterung der Zugriffssteuerungsverwaltung dar, die den Zugriff auf Ressourcen nur unter bestimmten Bedingungen ermöglicht oder verweigert, beispielsweise Gruppenmitgliedschaft, Standort oder Sicherheitsstatus des Geräts. Ausdrücke werden über das Dialogfeld Erweiterte Sicherheitseinstellungen des ACL-Editors oder des zentralen Zugriffsregel-Editors im Active Directory-Verwaltungs Center (ADAC) verwaltet.

Mithilfe von Ausdrücken können Administratoren den Zugriff auf sensible Ressourcen mit flexiblen Bedingungen in zunehmend komplexen Unternehmensumgebungen verwalten.

Vorgeschlagene Berechtigungen

Vorgeschlagene Berechtigungen ermöglichen einem Administrator, die Auswirkungen potenzieller Änderungen auf die Zugriffssteuerungseinstellungen genauer zu modellieren, ohne Sie tatsächlich zu ändern.

Wenn Sie den effektiven Zugriff auf eine Ressource vorhersagen, können Sie die Berechtigungen für diese Ressourcen planen und konfigurieren, bevor Sie diese Änderungen implementieren.

Weitere Änderungen

Weitere Verbesserungen in den unterstützten Windows-Versionen, die die dynamische Zugriffssteuerung unterstützen, sind:

Unterstützung des Kerberos-Authentifizierungsprotokolls zur zuverlässigen Bereitstellung von benutzeransprüchen, geräteansprüchen und Gerätegruppen.

Standardmäßig können Geräte, auf denen eine der unterstützten Windows-Versionen ausgeführt wird, dynamische Zugriffs Steuerungs bezogene Kerberos-Tickets verarbeiten, die Daten umfassen, die für die Verbundauthentifizierung erforderlich sind. Domänencontroller können Kerberos-Tickets mit zusammengesetzten Authentifizierungsinformationen ausgeben und darauf antworten. Wenn eine Domäne für die Erkennung der dynamischen Zugriffssteuerung konfiguriert ist, erhalten Geräte während der erst Authentifizierung Ansprüche von Domänencontrollern, und Sie erhalten Verbund Authentifizierungstickets, wenn Sie Service Ticket-Anforderungen übermitteln. Die Verbundauthentifizierung führt zu einem Zugriffstoken, das die Identität des Benutzers und des Geräts für die Ressourcen enthält, die die dynamische Zugriffssteuerung erkennen.

Unterstützung für die Verwendung der Schlüssel Verteilungs Center-Gruppenrichtlinieneinstellung, um die dynamische Zugriffssteuerung für eine Domäne zu aktivieren.

Jeder Domänencontroller muss dieselbe Richtlinieneinstellung für administrative Vorlagen aufweisen, die sich auf der **Computer Configuration\Policies\Administrative Templates\System\KDC\Support Dynamic Access Control und Kerberos armoring** befindet.

Unterstützung in Active Directory zum Speichern von Benutzer-und geräteansprüchen, Ressourceneigenschaften und zentralen Zugriffsrichtlinien Objekten.

Unterstützung für die Verwendung von Gruppenrichtlinien zum Bereitstellen von zentralen Access-Richtlinienobjekten.

Mit der folgenden Gruppenrichtlinieneinstellung können Sie zentrale Zugriffsrichtlinien Objekte auf Dateiservern in Ihrer Organisation bereitstellen: **Computer Configuration\Policies\ Windows Settings\Security Settings\File System\Central Access-Richtlinie.**

Unterstützung der anspruchsbasierten Dateiautorisierung und-Überwachung für Dateisysteme mithilfe von Gruppenrichtlinien und globaler Objektzugriffsüberwachung

Sie müssen die Überprüfung der bereitgestellten zentralen Zugriffsrichtlinien aktivieren, um den effektiven Zugriff auf die zentrale Zugriffsrichtlinie mithilfe der vorgeschlagenen Berechtigungen zu überwachen. Sie können diese Einstellung für den Computer unter **Erweiterte Überwachungsrichtlinienkonfiguration** in den **Sicherheitseinstellungen** eines Gruppenrichtlinienobjekts (GPO) konfigurieren. Nachdem Sie die Sicherheitseinstellung im Gruppenrichtlinienobjekt konfiguriert haben, können Sie das Gruppenrichtlinienobjekt auf Computern in Ihrem Netzwerk bereitstellen.

Unterstützung für das Transformieren oder Filtern von Anspruchs Richtlinienobjekten, die Active Directory-Gesamtstrukturvertrauensstellungen durchlaufen

Sie können eingehende und ausgehende Ansprüche filtern oder transformieren, die eine Gesamtstrukturvertrauensstellung durchlaufen. Es gibt drei grundlegende Szenarien für das Filtern und Transformieren von Ansprüchen:

- **Wertbasierte Filter**Filter können auf dem Wert eines Anspruchs basieren. Dadurch kann die vertrauenswürdige Gesamtstruktur verhindern, dass Ansprüche mit bestimmten Werten an die vertrauenswürdige Gesamtstruktur gesendet werden. Domänencontroller in vertrauenden Gesamtstrukturen können mithilfe von Wert basierter Filterung gegen Angriffe mit erhöhten Rechten geschützt werden, indem die eingehenden Ansprüche mit bestimmten Werten aus der vertrauenswürdigen Gesamtstruktur gefiltert werden.
- **Anspruchstypen basierte Filter**Filter basieren auf dem Typ des Anspruchs und nicht auf dem Wert des Anspruchs. Sie geben den Anspruchstyp mit dem Namen des Anspruchs an. Sie verwenden Anspruchstyp basierte Filterung in der vertrauenswürdigen Gesamtstruktur und verhindern, dass Windows Ansprüche sendet, die Informationen an die vertrauenswürdige Gesamtstruktur weiter geben.
- **Die Anspruchstyp basierte Transformation**bearbeitet einen Anspruch, bevor er an das beabsichtigte Ziel gesendet wird. Sie verwenden Anspruchstypen basierte Transformation in der vertrauenswürdigen Gesamtstruktur, um einen bekannten Anspruch zu verallgemeinern, der bestimmte Informationen enthält. Sie können Transformationen verwenden, um den Claim-Typ, den Claim-Wert oder beides zu verallgemeinern.

Softwareanforderungen

Da Ansprüche und Verbundauthentifizierung für die dynamische Zugriffssteuerung Kerberos-Authentifizierungserweiterungen erfordern, müssen alle Domänen, die eine dynamische Zugriffssteuerung unterstützen, über genügend Domänencontroller verfügen, auf denen die unterstützten Versionen von Windows unterstützt werden. Authentifizierung von Kerberos-Clients mit dynamischer Zugriffssteuerung Standardmäßig müssen Geräte Domänencontroller auf anderen Websites verwenden. Wenn keine solchen Domänencontroller verfügbar sind, schlägt die Authentifizierung fehl. Daher müssen Sie eine der folgenden Bedingungen unterstützen:

- Jede Domäne, die die dynamische Zugriffssteuerung unterstützt, muss über genügend Domänencontroller verfügen, auf denen die unterstützten Versionen von Windows Server zur Unterstützung der Authentifizierung von allen Geräten mit den unterstützten Versionen von Windows oder Windows Server ausgeführt werden.
- Geräte, auf denen die unterstützten Windows-Versionen ausgeführt werden oder die Ressourcen nicht mithilfe von Ansprüchen oder zusammengesetzten Identitäten schützen, sollten die Kerberos-Protokollunterstützung für die dynamische Zugriffssteuerung deaktivieren.

Bei Domänen, die benutzeransprüche unterstützen, muss jeder Domänencontroller, auf dem die unterstützten Versionen von Windows Server ausgeführt werden, mit der entsprechenden Einstellung für die Unterstützung von Ansprüchen und der zusammengesetzten Authentifizierung sowie zum Bereitstellen von Kerberos-Rüstung konfiguriert sein. Konfigurieren Sie die Einstellungen in der Richtlinie für die KDC-administrative Vorlage wie folgt:

- **Immer Bereitstellen von Ansprüchen** verwenden Sie diese Einstellung, wenn auf allen Domänencontrollern die unterstützten Versionen von Windows Server ausgeführt werden. Darüber hinaus können Sie die Domänenfunktionsebene auf Windows Server 2012 oder höher einstellen.
- **Unterstützt** Wenn Sie diese Einstellung verwenden, überwachen Sie die Domänencontroller, um sicherzustellen, dass die Anzahl der Domänencontroller, auf denen die unterstützten Versionen von Windows Server ausgeführt werden, ausreichend für die Anzahl der Clientcomputer ist, die auf Ressourcen zugreifen müssen. durch dynamische Zugriffssteuerung geschützt.

Wenn sich die Benutzerdomäne und die Dateiserver Domäne in unterschiedlichen Gesamtstrukturen befinden, müssen alle Domänencontroller im Gesamtstrukturstamm des Dateiservers auf der Funktionsebene Windows Server 2012 oder höher eingestellt sein.

Wenn Clients die dynamische Zugriffssteuerung nicht erkennen, muss eine bidirektionale Vertrauensstellung zwischen den beiden Gesamtstrukturen vorhanden sein.

Wenn Ansprüche transformiert werden, wenn Sie eine Gesamtstruktur belassen, müssen alle Domänencontroller im Gesamtstrukturstamm des Benutzers auf der Funktionsebene Windows Server 2012 oder höher eingestellt sein.

Ein Dateiserver mit einem Server Betriebssystem, das die Dynamic-Zugriffssteuerung unterstützt, muss über eine Gruppenrichtlinieneinstellung verfügen, die angibt, ob benutzeransprüche für Benutzertoken abgerufen werden sollen, die keine Ansprüche tragen. Diese Einstellung ist standardmäßig auf **Automatic** festgelegt, was dazu führt, dass diese Gruppenrichtlinieneinstellung aktiviert ist, **wenn eine** zentrale Richtlinie vorhanden ist, die Benutzer- oder Geräteansprüche für diesen Dateiserver enthält. Wenn der Dateiserver freigegebene ACLs enthält, die benutzeransprüche enthalten, müssen Sie diese Gruppenrichtlinie auf **ein** festlegen, damit der Server im Namen von Benutzern Ansprüche anfordern kann, die beim Zugriff auf den Server keine Ansprüche stellen.

Weitere Informationen:

- [Übersicht über die Zugriffssteuerung](#)

Sicherheitsbezeichner

14.01.2020 • 27 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Thema für IT-Experten werden Sicherheitskennungen und deren Funktionsweise in Bezug auf Konten und Gruppen im Windows-Betriebssystem beschrieben.

Was sind Sicherheitskennungen?

Eine Sicherheits-ID (Security Identifier, SID) wird verwendet, um einen Sicherheitsprinzipal oder eine Sicherheitsgruppe eindeutig zu identifizieren. Sicherheitsprinzipale können alle Entitäten darstellen, die vom Betriebssystem authentifiziert werden können, beispielsweise ein Benutzerkonto, ein Computerkonto oder ein Thread oder Prozess, der im Sicherheitskontext eines Benutzer- oder Computerkontos ausgeführt wird.

Jedes Konto oder jede Gruppe oder jeder Prozess, der im Sicherheitskontext des Kontos ausgeführt wird, weist eine eindeutige SID auf, die von einer Zertifizierungsstelle, beispielsweise einem Windows-Domänencontroller, ausgestellt wurde. Sie wird in einer Sicherheitsdatenbank gespeichert. Das System generiert die SID, die zum Zeitpunkt der Erstellung des Kontos oder der Gruppe ein bestimmtes Konto oder eine bestimmte Gruppe identifiziert. Wenn eine SID als eindeutiger Bezeichner für einen Benutzer oder eine Gruppe verwendet wurde, kann Sie nicht mehr verwendet werden, um einen anderen Benutzer oder eine andere Gruppe zu identifizieren.

Jedes Mal, wenn sich ein Benutzer anmeldet, erstellt das System ein Zugriffstoken für diesen Benutzer. Das Zugriffstoken enthält die SID des Benutzers, die Benutzerrechte und die SIDs für alle Gruppen, zu denen der Benutzer gehört. Dieses Token stellt den Sicherheitskontext für alle Aktionen bereit, die der Benutzer auf diesem Computer ausführt.

Zusätzlich zu den eindeutig erstellten domänenspezifischen SIDs, die bestimmten Benutzern und Gruppen zugewiesen sind, gibt es bekannte SIDs, die generische Gruppen und generische Benutzer identifizieren. Beispielsweise identifizieren die SIDs everyone und World eine Gruppe, die alle Benutzer umfasst. Bekannte SIDs weisen Werte auf, die für alle Betriebssysteme konstant bleiben.

SIDs sind ein grundlegender Baustein des Windows-Sicherheitsmodells. Sie arbeiten mit bestimmten Komponenten der Autorisierungs- und Zugriffssteuerungstechnologien in der Sicherheitsinfrastruktur der Windows Server-Betriebssysteme. Dies trägt zum Schutz des Zugriffs auf Netzwerkressourcen bei und bietet eine sicherere Computerumgebung.

Der Inhalt in diesem Thema bezieht sich auf Computer, auf denen die unterstützten Versionen des Windows-Betriebssystems ausgeführt werden, wie in der Liste **betrifft zu** Beginn dieses Themas angegeben.

Funktionsweise von Sicherheitskennungen

Benutzer verweisen auf Konten mit dem Kontonamen, das Betriebssystem bezieht sich jedoch intern auf Konten und Prozesse, die im Sicherheitskontext des Kontos ausgeführt werden, indem Sie deren Sicherheits-IDs (SIDs) verwenden. Bei Domänenkonten wird die SID eines Sicherheitsprinzipals erstellt, indem die SID der Domäne mit einem relativen Bezeichner (RID) für das Konto verkettet wird. SIDs sind innerhalb ihres Bereichs (Domäne oder lokal) eindeutig und werden nie wieder verwendet.

Das Betriebssystem generiert eine SID, die zum Zeitpunkt der Erstellung des Kontos oder der Gruppe ein

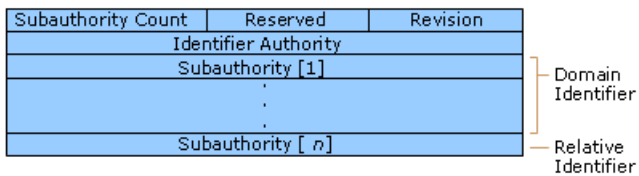
bestimmtes Konto oder eine bestimmte Gruppe identifiziert. Die sid für ein lokales Konto oder eine lokale Gruppe wird von der lokalen Sicherheitsautorität (Local Security Authority, LSA) auf dem Computer generiert und mit anderen Kontoinformationen in einem sicheren Bereich der Registrierung gespeichert. Die sid für ein Domänenkonto oder eine Gruppe wird von der Domänen Sicherheitsautorität generiert und als Attribut des Benutzer-oder Gruppenobjekts in den Active Directory-Domänendiensten gespeichert.

Für jedes lokale Konto und jede Gruppe ist die SID eindeutig für den Computer, auf dem Sie erstellt wurde. Keine zwei Konten oder Gruppen auf dem Computer haben jemals dieselbe SID. Ebenso ist die sid für jedes Domänenkonto und jede Gruppe innerhalb eines Unternehmens eindeutig. Dies bedeutet, dass die sid für ein Konto oder eine Gruppe, die in einer Domäne erstellt wird, nie mit der sid für ein Konto oder eine Gruppe übereinstimmt, das in einer anderen Domäne des Unternehmens erstellt wurde.

SIDs bleiben immer eindeutig. Sicherheitsbehörden geben nie dieselbe SID zweimal aus, und Sie verwenden nie SIDs für gelöschte Konten wieder. Wenn beispielsweise ein Benutzer mit einem Benutzerkonto in einer Windows-Domäne seinen Job verlässt, löscht ein Administrator sein Active Directory-Konto, einschließlich der SID, die das Konto identifiziert. Wenn Sie später zu einem anderen Auftrag im gleichen Unternehmen zurückkehrt, erstellt ein Administrator ein neues Konto, und das Windows Server-Betriebssystem generiert eine neue SID. Die neue SID entspricht nicht dem alten; Daher wird der Zugriff des Benutzers auf Ihr altes Konto nicht auf das neue Konto übertragen. Ihre zwei Konten stellen zwei völlig unterschiedliche Sicherheitsprinzipale dar.

Sicherheits-ID-Architektur

Eine Sicherheits-ID ist eine Datenstruktur im Binärformat, die eine Variable Anzahl von Werten enthält. Die ersten Werte in der Struktur enthalten Informationen zur SID-Struktur. Die verbleibenden Werte sind in einer Hierarchie angeordnet (ähnlich einer Telefonnummer), und Sie identifizieren die SID-ausstellende Autorität (beispielsweise "NT Authority"), die SID-ausstellende Domäne und einen bestimmten Sicherheitsprinzipal oder eine bestimmte Gruppe. Die folgende Abbildung zeigt die Struktur einer SID.



Die einzelnen Werte einer sid werden in der folgenden Tabelle beschrieben.

KOMMENTAR	BESCHREIBUNG
Revision	Gibt die Version der SID-Struktur an, die in einer bestimmten sid verwendet wird.
Identifier Authority	Identifiziert die höchste Autoritätsebene, die SIDs für einen bestimmten Typ von Sicherheitsprinzipal ausgeben kann. Der Wert der Identifier Authority in der sid für die Gruppe "jeder" lautet beispielsweise 1 (Welt-Authority). Der Wert der Identifier Authority in der sid für ein bestimmtes Windows Server-Konto oder eine bestimmte Gruppe ist 5 (NT Authority).

KOMMENTAR	BESCHREIBUNG
Autoren	> enthält die wichtigsten Informationen in einer SID, die in einer Reihe von einem oder mehreren unter Autoren Werten enthalten ist. Alle Werte bis zum, aber nicht einschließlich des letzten Werts in der Reihe identifizieren eine Domäne in einem Unternehmen gemeinsam. Dieser Teil der Serie wird als Domänenbezeichner bezeichnet. Der letzte Wert in der Reihe, der als relativer Bezeichner (RID) bezeichnet wird, gibt ein bestimmtes Konto oder eine bestimmte Gruppe relativ zu einer Domäne an.

Die Komponenten einer SID können einfacher visualisiert werden, wenn SIDs aus einer Binärdatei in ein Zeichenfolgenformat konvertiert werden, indem die Standard Notation verwendet wird:

S-R-X-Y1-Y2-Yn-1-Yn

In dieser Notation werden die Komponenten einer SID wie in der folgenden Tabelle dargestellt dargestellt.

KOMMENTAR	BESCHREIBUNG
S	Gibt an, dass die Zeichenfolge eine SID ist.
R	Gibt die Änderungs Ebene an.
X	Gibt den Wert der Identifier Authority an
Y	Stellt eine Reihe von unter Autoren Werten dar, wobei n die Anzahl der Werte ist

Die wichtigsten Informationen zur sid sind in der Reihe der unter Autoren Werte enthalten. Der erste Teil der Serie (-Y1-Y2-Yn-1) ist der Domänenbezeichner. Dieses Element der SID wird in einem Unternehmen mit mehreren Domänen erheblich, da der Domänenbezeichner SIDs unterscheidet, die von einer Domäne von SIDs ausgestellt werden, die von allen anderen Domänen des Unternehmens ausgestellt werden. Keine zwei Domänen in einem Unternehmen verwenden denselben Domänenbezeichner.

Das letzte Element in der Reihe der unter Autoren Werte (-Yn) ist der relative Bezeichner. Sie unterscheidet ein Konto oder eine Gruppe von allen anderen Konten und Gruppen in der Domäne. Keine zwei Konten oder Gruppen in einer Domäne verwenden denselben relativen Bezeichner.

Beispielsweise wird die sid für die integrierte Administratorengruppe in der standardisierten sid-Notation als die folgende Zeichenfolge dargestellt:

S-1-5-32-544

Diese SID besteht aus vier Komponenten:

- Eine Überarbeitungs Ebene (1)
- Ein Identifier Authority-Wert (5, NT Authority)
- Eine Domänen-ID (32, Builtin)
- Ein relativer Bezeichner (544, Administratoren)

SIDs für integrierte Konten und Gruppen weisen immer denselben Domänen Bezeichnerwert auf: 32. Dieser Wert

gibt die Domäne **BuiltIn**, die auf jedem Computer vorhanden ist, auf dem eine Version des Betriebssystems Windows Server ausgeführt wird. Es ist nie notwendig, die integrierten Konten und Gruppen eines Computers von den integrierten Konten und Gruppen eines anderen Computers zu unterscheiden, da Sie im Bereich lokal sind. Sie sind lokal auf einem einzelnen Computer oder im Fall von Domänencontrollern für eine Netzwerkdomäne lokal auf mehreren Computern, die als eins fungieren.

Integrierte Konten und Gruppen müssen im Bereich der **integrierten** Domäne voneinander unterschieden werden. Daher verfügt die sid für jedes Konto und jede Gruppe über einen eindeutigen relativen Bezeichner. Der relative Identifier-Wert von 544 ist für die integrierte Gruppe Administratoren eindeutig. Kein anderes Konto oder keine andere Gruppe in der **integrierten** Domäne hat eine SID mit dem endgültigen Wert von 544.

In einem anderen Beispiel sollten Sie die sid für die globale Gruppe, Domänenadministratoren, in Frage stellen. Jede Domäne in einem Unternehmen verfügt über eine Gruppe der Domänenadministratoren, und die sid für jede Gruppe ist anders. Im folgenden Beispiel wird die sid für die Gruppe der Domänenadministratoren in der Domäne contoso, Ltd. (Contoso\Domain-Administratoren) dargestellt:

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

Die sid für Contoso\Domain-Administratoren hat Folgendes:

- Eine Überarbeitungs Ebene (1)
- Eine Identifier Authority (5, NT Authority)
- Eine Domänen-ID (21-1004336348-1177238915-682003330, Contoso)
- Ein relativer Bezeichner (512, Domänenadministratoren)

Die sid für Contoso\Domain-Administratoren unterscheidet sich von den SIDs für andere Domänenadministratoren Gruppen in demselben Unternehmen durch ihren Domänenbezeichner: 21-1004336348-1177238915-682003330. In keiner anderen Domäne des Unternehmens wird dieser Wert als Domänenbezeichner verwendet. Die sid für Contoso\Domain-Administratoren unterscheidet sich von den SIDs für andere Konten und Gruppen, die in der Domäne contoso mithilfe ihres relativen Bezeichners 512 erstellt werden. Kein anderes Konto oder keine andere Gruppe in der Domäne hat eine SID mit einem endgültigen Wert von 512.

Zuordnung relativer Bezeichner

Wenn Konten und Gruppen in einer Kontodatenbank gespeichert werden, die von einem lokalen Security Accounts Manager (Sam) verwaltet wird, ist es für das System relativ einfach, einen eindeutigen relativen Bezeichner für jedes Konto und in einer Gruppe zu generieren, die auf einem eigenständigen Computer erstellt wird. Der Sam auf einem eigenständigen Computer kann die relativen Bezeichnerwerte nachvollziehen, die er zuvor verwendet hat, und sicherstellen, dass er diese nie wieder verwendet.

In einer Netzwerkdomäne ist das Generieren eindeutiger relativer Bezeichner jedoch ein komplexerer Prozess. Windows Server-Netzwerkdomänen können mehrere Domänencontroller aufweisen. Jeder Domänencontroller speichert Informationen zu Active Directory-Konten. Das bedeutet, dass es in einer Netzwerkdomäne so viele Kopien der Kontodatenbank gibt, wie Domänencontroller vorhanden sind. Darüber hinaus ist jede Kopie der Kontodatenbank eine Masterkopie. Neue Konten und Gruppen können auf jedem Domänencontroller erstellt werden. Änderungen, die an Active Directory auf einem Domänencontroller vorgenommen werden, werden auf alle anderen Domänencontroller in der Domäne repliziert. Der Vorgang des replizierens von Änderungen in einer Masterkopie der Kontodatenbank auf alle anderen Masterkopien wird als Multimaster-Vorgang bezeichnet.

Der Prozess der Generierung eindeutiger relativer Bezeichner ist ein Einzelmaster Vorgang. Einem Domänencontroller wird die Rolle des RID-Masters (relative Identifier) zugewiesen, und er ordnet jedem Domänencontroller in der Domäne eine Sequenz von relativen Bezeichnern zu. Wenn ein neues Domänenkonto

oder eine neue Gruppe in einem Domänencontroller Replikat von Active Directory erstellt wird, wird ihm eine SID zugewiesen. Der relative Bezeichner für die neue SID wird von der Zuweisung relativer IDs des Domänencontrollers übernommen. Wenn die Bereitstellung relativer Bezeichner langsam abläuft, fordert der Domänencontroller einen weiteren Block vom RID-Master an.

Jeder Domänencontroller verwendet jeden Wert in einem Block mit relativen Bezeichnern nur einmal. Der RID-Master ordnet jeden Block relativer Bezeichnerwerte nur einmal zu. Durch diesen Vorgang wird sichergestellt, dass jedes in der Domäne erstellte Konto und jede Gruppe einen eindeutigen relativen Bezeichner aufweist.

Sicherheits-IDs und global eindeutige IDs

Beim Erstellen eines neuen Domänenbenutzer-oder Gruppenkontos speichert Active Directory die SID des Kontos in der Eigenschaft "**Objekte**" eines Benutzer-oder Gruppenobjekts. Außerdem wird dem neuen Objekt eine GUID (Globally Unique Identifier) zugewiesen, bei der es sich um einen 128-Bit-Wert handelt, der nicht nur im Unternehmen, sondern auch in der ganzen Welt eindeutig ist. GUIDs werden jedem Objekt zugewiesen, das von Active Directory erstellt wird, nicht nur von Benutzer-und Gruppenobjekten. Die GUID jedes Objekts wird in der **objectGUID** -Eigenschaft gespeichert.

Active Directory verwendet GUIDs intern, um Objekte zu identifizieren. Beispielsweise ist die GUID eine der Eigenschaften eines Objekts, die im globalen Katalog veröffentlicht wird. Beim Durchsuchen des globalen Katalogs nach einer Benutzerobjekt-GUID werden Ergebnisse erzielt, wenn der Benutzer ein Konto im Unternehmen hat. In der Tat ist die Suche nach Objekten nach **objectGUID** möglicherweise die zuverlässigste Methode, um das Objekt zu finden, das Sie suchen möchten. Die Werte anderer Objekteigenschaften können sich ändern, aber die **objectGUID** -Eigenschaft ändert sich nie. Wenn einem Objekt eine GUID zugewiesen wird, bleibt dieser Wert für das Leben erhalten.

Wenn ein Benutzer von einer Domäne zu einer anderen wechselt, erhält der Benutzer eine neue SID. Die sid für ein Gruppenobjekt ändert sich nicht, da Gruppen in der Domäne verbleiben, in der Sie erstellt wurden. Wenn sich die Benutzer jedoch bewegen, können Ihre Konten mit Ihnen verschoben werden. Wenn ein Mitarbeiter von Nordamerika nach Europa wechselt, aber im selben Unternehmen bleibt, kann ein Administrator des Unternehmens das Benutzerobjekt des Mitarbeiters aus, beispielsweise Contoso\NoAm, in Contoso\Europe verschieben. Wenn der Administrator dies tut, benötigt das Benutzerobjekt für das Konto eine neue SID. Der Domänen Kennungs Teil einer SID, der in Noam ausgestellt wird, ist für Noam eindeutig; die sid für das Konto des Benutzers in Europa weist also eine andere Domänenkennung auf. Der relative Identifier-Teil einer SID ist relativ zur Domäne eindeutig; Wenn sich die Domäne ändert, ändert sich auch der relative Bezeichner.

Wenn ein Benutzerobjekt von einer Domäne zu einer anderen wechselt, muss für das Benutzerkonto eine neue SID generiert und in der Eigenschaft **Objekte** gespeichert werden. Bevor der neue Wert in die Eigenschaft geschrieben wird, wird der vorherige Wert in eine andere Eigenschaft eines Benutzerobjekts, **sid**, kopiert. Diese Eigenschaft kann mehrere Werte enthalten. Jedes Mal, wenn ein Benutzerobjekt zu einer anderen Domäne wechselt, wird eine neue SID generiert und in der Eigenschaft **Objekt** -ID gespeichert, und der Liste der alten SIDs in **sid** wird ein anderer Wert hinzugefügt. Wenn sich ein Benutzer anmeldet und erfolgreich authentifiziert wird, fragt der Domänen Authentifizierungsdienst Active Directory nach allen SIDs ab, die dem Benutzer zugeordnet sind, einschließlich der aktuellen SID des Benutzers, den alten SIDs des Benutzers und den SIDs für die Gruppen des Benutzers. Alle diese SIDs werden an den Authentifizierungs Client zurückgegeben, und Sie sind im Zugriffstoken des Benutzers enthalten. Wenn der Benutzer versucht, auf eine Ressource zuzugreifen, kann eine der SIDs im Zugriffstoken (einschließlich einer der SIDs in **sid**) den Benutzer Zugriff zulassen oder verweigern.

Wenn Sie den Benutzern den Zugriff auf eine Ressource basierend auf Ihren Aufträgen erlauben oder verweigern, sollten Sie den Zugriff auf eine Gruppe und nicht auf eine einzelne Person zulassen oder verweigern. Auf diese Weise können Sie, wenn Benutzeraufträge ändern oder zu anderen Abteilungen wechseln, Ihren Zugriff einfach anpassen, indem Sie Sie aus bestimmten Gruppen entfernen und anderen Personen hinzufügen.

Wenn Sie jedoch den Zugriff einzelner Benutzer auf Ressourcen zulassen oder verweigern, möchten Sie wahrscheinlich, dass der Zugriff des Benutzers identisch bleibt, unabhängig davon, wie oft sich die Kontodomäne

des Benutzers ändert. Die Eigenschaft " **sid** " macht dies möglich. Wenn ein Benutzerdomänen ändert, ist es nicht erforderlich, die Zugriffssteuerungsliste (ACL) für eine Ressource zu ändern. Wenn eine ACL die alte SID des Benutzers, aber nicht das neue, enthält, befindet sich die alte SID weiterhin im Zugriffstoken des Benutzers. Sie wird unter den SIDs für die Gruppen des Benutzers aufgelistet, und dem Benutzer wird basierend auf der alten SID der Zugriff gewährt oder verweigert.

Bekannte SIDs

Die Werte bestimmter SIDs sind in allen Systemen konstant. Sie werden erstellt, wenn das Betriebssystem oder die Domäne installiert ist. Sie werden als bekannte SIDs bezeichnet, da Sie generische Benutzer oder generische Gruppen identifizieren.

Es gibt universelle Bekannte SIDs, die auf allen sicheren Systemen, die dieses Sicherheitsmodell verwenden, sinnvoll sind, einschließlich anderer Betriebssysteme als Windows. Darüber hinaus gibt es bekannte SIDs, die nur unter Windows-Betriebssystemen sinnvoll sind.

In der folgenden Tabelle sind die universellen bekannten SIDs aufgelistet.

WERT	UNIVERSELLE BEKANNTE SID	IDENTIFIZIERT
S-1-0-0	NULL-sid	Eine Gruppe ohne Mitglieder. Dies wird häufig verwendet, wenn ein SID-Wert unbekannt ist.
S-1-1-0	World	Eine Gruppe, die alle Benutzer umfasst.
S-1-2-0	Lokal	Benutzer, die sich an Terminals anmelden, die lokal (physisch) mit dem System verbunden sind.
S-1-2-1	Konsolenanmeldung	Eine Gruppe mit Benutzern, die bei der physikalischen Konsole angemeldet sind.
S-1-3-0	Besitzer-ID des Erstellers	Eine Sicherheits-ID, die durch die Sicherheits-ID des Benutzers ersetzt werden soll, der ein neues Objekt erstellt hat. Diese SID wird in vererbaren ACEs verwendet.
S-1-3-1	Creator-Gruppen-ID	Eine Sicherheits-ID, die durch die primäre Gruppen-SID des Benutzers ersetzt werden soll, der ein neues Objekt erstellt hat. Verwenden Sie diese SID in vererbaren ACEs.
S-1-3-2	Creator-Besitzer Server	
S-1-3-3	Creator-Gruppen Server	
S-1-3-4	Besitzerrechte	Eine Gruppe, die den aktuellen Besitzer des Objekts darstellt. Wenn ein ACE, der diese SID trägt, auf ein Objekt angewendet wird, ignoriert das System die impliziten READ_CONTROL- und WRITE_DAC Berechtigungen für den Objektbesitzer.

WERT	UNIVERSELLE BEKANNTE SID	IDENTIFIZIERT
S-1-4	Nicht eindeutige Autorität	Eine SID, die eine Identifier Authority darstellt.
S-1-5	NT-Zertifizierungsstelle	Eine SID, die eine Identifier Authority darstellt.
S-1-5-80-0	Alle Dienste	Eine Gruppe, die alle auf dem System konfigurierten Dienstprozesse umfasst. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

In der folgenden Tabelle sind die vordefinierten Bezeichner Authority-Konstanten aufgeführt. Die ersten vier Werte werden mit universellen bekannten SIDs verwendet, und der letzte Wert wird mit bekannten SIDs in Windows-Betriebssystemen verwendet, die in der Liste **gilt für** angegeben sind.

IDENTIFIER AUTHORITY	WERT	SID-ZEICHENFOLGEN PRÄFIX
SECURITY_NULL_SID_AUTHORITY	0	S-1-0
SECURITY_WORLD_SID_AUTHORITY	1	S-1-1
SECURITY_LOCAL_SID_AUTHORITY	2	S-1-2
SECURITY_CREATOR_SID_AUTHORITY	3	S-1-3

Die folgenden Rid-Werte werden mit universellen bekannten SIDs verwendet. Die Spalte "Identifier Authority" zeigt das Präfix der Autoritäts-ID, mit der Sie Rid kombinieren können, um eine universelle bekannte SID zu erstellen.

RELATIVE IDENTIFIER AUTHORITY	WERT	IDENTIFIER AUTHORITY
SECURITY_NULL_RID	0	S-1-0
SECURITY_WORLD_RID	0	S-1-1
SECURITY_LOCAL_RID	0	S-1-2
SECURITY_CREATOR_OWNER_RID	0	S-1-3
SECURITY_CREATOR_GROUP_RID	1	S-1-3

Die vordefinierte ID-Berechtigung _NT_AUTHORITY (S-1-5) erzeugt SIDs, die nicht universell sind und nur in Installationen der Windows-Betriebssysteme sinnvoll sind, die in der Liste "**gilt für**" am Anfang dieses Themas angegeben sind. In der folgenden Tabelle sind die bekannten SIDs aufgelistet.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-1	Einwahl	Eine Gruppe, die alle Benutzer umfasst, die über eine DFÜ-Verbindung am System angemeldet sind.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-113	Lokales Konto	Sie können diese SID verwenden, wenn Sie die Netzwerkanmeldung auf lokale Konten anstatt auf "Administrator" oder gleichwertig einschränken. Diese SID kann die Netzwerkanmeldung für lokale Benutzer und Gruppen nach Kontotyp unabhängig davon, was Sie tatsächlich benannt sind, effektiv blockieren.
S-1-5-114	Lokales Konto und Mitglied der Gruppe "Administratoren"	Sie können diese SID verwenden, wenn Sie die Netzwerkanmeldung auf lokale Konten anstatt auf "Administrator" oder gleichwertig einschränken. Diese SID kann die Netzwerkanmeldung für lokale Benutzer und Gruppen nach Kontotyp unabhängig davon, was Sie tatsächlich benannt sind, effektiv blockieren.
S-1-5-2	Netzwerk	Eine Gruppe, die alle Benutzer umfasst, die über eine Netzwerkverbindung angemeldet sind. Zugriffstoken für interaktive Benutzer enthalten keine Netzwerk-sid.
S-1-5-3	Batch	Eine Gruppe, die alle Benutzer umfasst, die sich mit einer Batchwarteschlange angemeldet haben, beispielsweise Aufgaben Planungs Aufträge.
S-1-5-4	Interaktive	Eine Gruppe, die alle Benutzer umfasst, die sich interaktiv anmelden. Benutzer können eine interaktive Anmeldesitzung starten, indem Sie sich direkt an der Tastatur anmelden, indem Sie eine Remote Desktop Dienste-Verbindung von einem Remotecomputer aus öffnen oder eine Remote-Shell wie Telnet verwenden. In jedem Fall enthält das Zugriffstoken des Benutzers die interaktive sid. Wenn sich der Benutzer mithilfe einer Remote Desktop Dienste-Verbindung anmeldet, enthält das Zugriffstoken des Benutzers auch die sid für die interaktive Remoteanmeldung.
S-1-5-5- X-Y	Anmeldesitzung	Die X -und Y -Werte für diese SIDs identifizieren eine bestimmte Anmeldesitzung eindeutig.
S-1-5-6	Dienst	Eine Gruppe, die alle Sicherheitsprinzipale enthält, die sich als Dienst angemeldet haben.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-7	Anonyme Anmeldung	<p>Ein Benutzer, der mit dem Computer verbunden ist, ohne einen Benutzernamen und ein Kennwort anzugeben.</p> <p>Die Identität der anonymen Anmeldung unterscheidet sich von der Identität, die von Internet Informationsdienste (IIS) für anonymen Web Access verwendet wird. IIS verwendet ein echtes Konto – standardmäßig IUSR_ <i>Computernam</i>e für den anonymen Zugriff auf Ressourcen auf einer Website. Genau genommen ist dieser Zugriff nicht anonym, da der Sicherheitsprinzipal bekannt ist, auch wenn unbekannte Personen das Konto verwenden. IUSR_ <i>Computer Name</i> (oder was auch immer Sie dem Konto nennen) verfügt über ein Kennwort, und IIS meldet sich beim Starten des Diensts beim Konto an. Infolgedessen ist der IIS-Benutzer "Anonym" ein Mitglied von authentifizierten Benutzern, aber anonyme Anmeldung nicht.</p>
S-1-5-8	Proxy	Gilt derzeit nicht: diese SID wird nicht verwendet.
S-1-5-9	Unternehmensdomänencontroller	Eine Gruppe, die alle Domänencontroller in einer Gesamtstruktur von Domänen umfasst.
S-1-5-10	Self	<p>Ein Platzhalter in einem ACE für ein Benutzer-, Gruppen- oder Computerobjekt in Active Directory. Wenn Sie selbst Berechtigungen erteilen, erteilen Sie diese dem Sicherheitsprinzipal, der durch das Objekt dargestellt wird. Während einer Zugriffsüberprüfung ersetzt das Betriebssystem die sid für Self durch die SID des Sicherheitsprinzipals, der durch das Objekt dargestellt wird.</p>
S-1-5-11	Authentifizierte Benutzer	<p>Eine Gruppe, die alle Benutzer und Computer mit authentifizierten Identitäten enthält. Authentifizierte Benutzer schließen keinen Gast ein, auch wenn das Gastkonto über ein Kennwort verfügt.</p> <p>Diese Gruppe umfasst authentifizierte Sicherheitsprinzipale aus einer vertrauenswürdigen Domäne, nicht nur der aktuellen Domäne.</p>

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-12	Eingeschränkter Code	Eine Identität, die von einem Prozess verwendet wird, der in einem eingeschränkten Sicherheitskontext ausgeführt wird. In Windows- und Windows Server-Betriebssystemen kann eine Richtlinie für Softwareeinschränkungen eine von drei Sicherheitsstufen dem Code zuweisen: uneingeschränkt, eingeschränkt oder nicht zulässig. Wenn Code auf der eingeschränkten Sicherheitsstufe ausgeführt wird, wird die eingeschränkte SID dem Zugriffstoken des Benutzers hinzugefügt.
S-1-5-13	Terminal Server-Benutzer	Eine Gruppe, die alle Benutzer umfasst, die sich bei einem Server anmelden und die Remote Desktop Dienste aktiviert sind.
S-1-5-14	Interaktive Remote Anmeldung	Eine Gruppe, die alle Benutzer umfasst, die sich mit einer Remotedesktopverbindung am Computer anmelden. Diese Gruppe ist eine Teilmenge der interaktiven Gruppe. Zugriffstoken, die die SID der interaktiven Remote Anmeldung enthalten, enthalten auch die interaktive sid.
S-1-5-15	Diese Organisation	Eine Gruppe, die alle Benutzer aus der gleichen Organisation umfasst. Nur in Active Directory-Konten enthalten und nur von einem Domänencontroller hinzugefügt.
S-1-5-17	IIS_USRS	Ein Konto, das vom Standardbenutzer für Internet Informationsdienste (IIS) verwendet wird.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-18	System (oder LocalSystem)	<p>Eine Identität, die lokal vom Betriebssystem und von Diensten verwendet wird, die für die Anmeldung als LocalSystem konfiguriert sind. System ist ein verborgenes Mitglied von Administratoren. Das heißt, dass jeder Prozess, der als System ausgeführt wird, die sid für die integrierte Administratorengruppe in seinem Zugriffstoken aufweist. Wenn ein lokal als System ausgeführter Prozess auf Netzwerkressourcen zugreift, erfolgt dies unter Verwendung der Domänenidentität des Computers. Das Zugriffstoken auf dem Remotecomputer enthält die SID des Domänenkontos des lokalen Computers sowie SIDs für Sicherheitsgruppen, in denen der Computer Mitglied ist, wie etwa Domänencomputer und authentifizierte Benutzer.</p>
S-1-5-19	NT-Zertifizierungsstelle (LocalService)	<p>Eine Identität, die von Diensten verwendet wird, die sich lokal auf dem Computer befinden, benötigen keinen umfangreichen lokalen Zugriff und benötigen keinen authentifizierten Netzwerkzugriff. Dienste, die als LocalService ausgeführt werden, greifen auf lokale Ressourcen als normale Benutzer zu, und Sie greifen als anonyme Benutzer auf Netzwerkressourcen zu. Infolgedessen hat ein Dienst, der als LocalService ausgeführt wird, erheblich weniger Autorität als ein Dienst, der lokal und im Netzwerk als lokales System ausgeführt wird.</p>
S-1-5-20	Netzwerkdienst	<p>Eine Identität, die von Diensten verwendet wird, die keinen umfangreichen lokalen Zugriff benötigen, aber authentifizierten Netzwerkzugriff benötigen. Dienste, die als Network Service ausgeführt werden, greifen auf lokale Ressourcen als normale Benutzer zu und greifen mithilfe der Identität des Computers auf Netzwerkressourcen zu. Infolgedessen verfügt ein Dienst, der als Network Service ausgeführt wird, über denselben Netzwerkzugriff wie ein Dienst, der als "LocalSystem" ausgeführt wird, aber einen deutlich reduzierten lokalen Zugriff hat.</p>

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-Domäne-500	Administrator	<p>Ein Benutzerkonto für den System Administrator. Jeder Computer verfügt über ein lokales Administratorkonto, und jede Domäne verfügt über ein Domänenadministratorkonto.</p> <p>Das Administrator Konto ist das erste Konto, das bei der Installation des Betriebssystems erstellt wurde. Das Konto kann nicht gelöscht, deaktiviert oder gesperrt werden, aber es kann umbenannt werden.</p> <p>Standardmäßig ist das Administrator Konto ein Mitglied der Gruppe Administratoren und kann nicht aus dieser Gruppe entfernt werden.</p>
S-1-5-Domäne-501	Gast	<p>Ein Benutzerkonto für Personen, die nicht über einzelne Konten verfügen. Jeder Computer verfügt über ein lokales Gastkonto, und jede Domäne verfügt über ein Domänen Gastkonto.</p> <p>Standardmäßig ist Guest ein Mitglied der Gruppen jeder und Gast. Das Domänen Gastkonto ist auch ein Mitglied der Gruppe "Domänengäste" und "Domänenbenutzer".</p> <p>Im Gegensatz zur anonymen Anmeldung ist Guest ein echtes Konto und kann für die interaktive Anmeldung verwendet werden. Für das Gastkonto ist kein Kennwort erforderlich, es kann jedoch über ein Kennwort verfügen.</p>
S-1-5-Domäne-502	krbtgt	<p>Ein Benutzerkonto, das vom KDC-Dienst (Key Distribution Center) verwendet wird. Das Konto ist nur auf Domänencontrollern vorhanden.</p>
S-1-5-Domäne-512	Domänenadministratoren	<p>Eine globale Gruppe mit Mitgliedern, die zum Verwalten der Domäne autorisiert sind. Standardmäßig ist die Gruppe Domänen-Admins ein Mitglied der Gruppe Administratoren auf allen Computern, die der Domäne beigetreten sind, einschließlich Domänencontrollern.</p> <p>Domänenadministratoren ist der Standardbesitzer eines beliebigen Objekts, das von einem Mitglied der Gruppe im Active Directory der Domäne erstellt wird. Wenn Mitglieder der Gruppe andere Objekte wie Dateien erstellen, ist der Standardbesitzer die Gruppe Administratoren.</p>

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-Domäne-513	Domänenbenutzer	Eine globale Gruppe, die alle Benutzer in einer Domäne umfasst. Wenn Sie ein neues Benutzerobjekt in Active Directory erstellen, wird der Benutzer automatisch zu dieser Gruppe hinzugefügt.
S-1-5-Domäne-514	Domänengäste	Eine globale Gruppe, die standardmäßig nur ein Mitglied hat: das integrierte Gastkonto der Domäne.
S-1-5-Domäne-515	Domänencomputer	Eine globale Gruppe, die alle Computer enthält, die der Domäne beigetreten sind, ohne Domänencontroller.
S-1-5-Domäne-516	Domänencontroller	Eine globale Gruppe, die alle Domänencontroller in der Domäne umfasst. Neue Domänencontroller werden dieser Gruppe automatisch hinzugefügt.
S-1-5-Domäne-517	CERT-Herausgeber	Eine globale Gruppe, die alle Computer umfasst, die eine Unternehmenszertifizierungsstelle hosten. CERT-Herausgeber sind berechtigt, Zertifikate für Benutzerobjekte in Active Directory zu veröffentlichen.
S-1-5-Root-Domäne-518	Schema Administratoren	Eine Gruppe, die nur in der Gesamtstruktur-Stammdomäne vorhanden ist. Es handelt sich um eine universelle Gruppe, wenn sich die Domäne im einheitlichen Modus befindet und es sich um eine globale Gruppe handelt, wenn sich die Domäne im gemischten Modus befindet. Die Gruppe "Schemaadministratoren" ist berechtigt, Schemaänderungen in Active Directory vorzunehmen. Standardmäßig ist das einzige Mitglied der Gruppe das Administrator Konto für die Stammdomäne der Gesamtstruktur.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-Root-Domäne-519	Unternehmensadministratoren	<p>Eine Gruppe, die nur in der Gesamtstruktur-Stammdomäne vorhanden ist. Es handelt sich um eine universelle Gruppe, wenn sich die Domäne im einheitlichen Modus befindet und es sich um eine globale Gruppe handelt, wenn sich die Domäne im gemischten Modus befindet.</p> <p>Die Gruppe "Unternehmensadministratoren" ist berechtigt, Änderungen an der Gesamtstruktur Infrastruktur vorzunehmen, wie beispielsweise das Hinzufügen von untergeordneten Domänen, das Konfigurieren von Websites, das Autorisieren von DHCP-Servern und das Installieren von Unternehmenszertifizierungsstellen. Standardmäßig ist das einzige Mitglied von Unternehmensadministratoren das Administrator Konto für die Stammdomäne der Gesamtstruktur. Die Gruppe ist ein Standardmitglied jeder Gruppe der Domänenadministratoren in der Gesamtstruktur.</p>
S-1-5-Domäne-520	Besitzer von Gruppenrichtlinien Erstellern	<p>Eine globale Gruppe, die zum Erstellen neuer Gruppenrichtlinienobjekte in Active Directory autorisiert ist. Standardmäßig ist das einzige Mitglied der Gruppe Administrator.</p> <p>Objekte, die von Mitgliedern der Besitzer von Gruppenrichtlinien Erstellern erstellt werden, sind Eigentum des einzelnen Benutzers, der Sie erstellt. Auf diese Weise ist die Gruppe Richtlinien-Ersteller-Besitzer anders als andere administrative Gruppen (wie Administratoren und Domänenadministratoren). Objekte, die von Mitgliedern dieser Gruppen erstellt werden, sind Eigentum der Gruppe und nicht der einzelnen Personen.</p>
S-1-5-Domäne-553	RAS-und IAS-Server	<p>Eine lokale Domänengruppe. Standardmäßig hat diese Gruppe keine Mitglieder. Computer, auf denen der Routing-und RAS-Dienst ausgeführt wird, werden der Gruppe automatisch hinzugefügt.</p> <p>Mitglieder dieser Gruppe können auf bestimmte Eigenschaften von Benutzerobjekten zugreifen, beispielsweise Lesen von Kontoeinschränkungen, Lesen von Anmeldeinformationen und Lesen von Remote Zugriffsinformationen.</p>

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-32-544	Administratoren	Eine integrierte Gruppe. Nach der erstmaligen Installation des Betriebssystems ist das einzige Mitglied der Gruppe das Administrator Konto. Wenn ein Computer einer Domäne Beitritt, wird die Gruppe "Domänen-Admins" der Gruppe "Administratoren" hinzugefügt. Wenn ein Server zu einem Domänencontroller wird, wird auch die Gruppe "Unternehmensadministratoren" der Gruppe "Administratoren" hinzugefügt.
S-1-5-32-545	Users	Eine integrierte Gruppe. Nach der erstmaligen Installation des Betriebssystems ist das einzige Mitglied die Gruppe "authentifizierte Benutzer".
S-1-5-32-546	Gäste	Eine integrierte Gruppe. Standardmäßig ist das einzige Mitglied das Gastkonto. Die Gruppe "Gäste" ermöglicht gelegentlichen oder einmaligen Benutzern die Anmeldung mit Einschränkungen für das integrierte Gastkonto eines Computers.
S-1-5-32-547	Power User	Eine integrierte Gruppe. Standardmäßig hat die Gruppe keine Mitglieder. Power User können lokale Benutzer und Gruppen erstellen; ändern und Löschen von Konten, die Sie erstellt haben; und entfernen Sie Benutzer aus den Gruppen "Hauptbenutzer", "Benutzer" und "Gäste". Power-User können auch Programme installieren; Erstellen, verwalten und Löschen lokaler Drucker und Dateifreigaben erstellen und löschen.
S-1-5-32-548	Kontooperatoren	Eine integrierte Gruppe, die nur auf Domänencontrollern vorhanden ist. Standardmäßig hat die Gruppe keine Mitglieder. Standardmäßig verfügen Konto-Operatoren über die Berechtigung zum Erstellen, ändern und Löschen von Konten für Benutzer, Gruppen und Computer in allen Containern und Organisationseinheiten von Active Directory mit Ausnahme des integrierten Containers und der Domänencontroller-OU. Kontooperatoren verfügen nicht über die Berechtigung zum Ändern der Gruppen Administratoren und Domänenadministratoren sowie über die Berechtigung zum Ändern der Konten für Mitglieder dieser Gruppen.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-32-549	Server Operatoren	Beschreibung: eine integrierte Gruppe, die nur auf Domänencontrollern vorhanden ist. Standardmäßig hat die Gruppe keine Mitglieder. Serveroperatoren können sich interaktiv bei einem Server anmelden; Erstellen und Löschen von Netzwerkfreigaben Starten und Beenden von Diensten Sichern und Wiederherstellen von Dateien Formatieren Sie die Festplatte des Computers. und fahren Sie den Computer herunter.
S-1-5-32-550	Druckoperatoren	Eine integrierte Gruppe, die nur auf Domänencontrollern vorhanden ist. Standardmäßig ist das einzige Mitglied die Gruppe "Domänenbenutzer". Druckoperatoren können Drucker und Dokumentwarteschlangen verwalten.
S-1-5-32-551	Sicherungs-Operatoren	Eine integrierte Gruppe. Standardmäßig hat die Gruppe keine Mitglieder. Sicherungs-Operatoren können alle Dateien auf einem Computer sichern und wiederherstellen, und zwar unabhängig von den Berechtigungen, mit denen diese Dateien geschützt werden. Backup-Operatoren können sich auch am Computer anmelden und ihn Herunterfahren.
S-1-5-32-552	Replikatoren	Eine integrierte Gruppe, die vom Dateireplikationsdienst auf Domänencontrollern verwendet wird. Standardmäßig hat die Gruppe keine Mitglieder. Fügen Sie dieser Gruppe keine Benutzer hinzu.
S-1-5-64-10	NTLM-Authentifizierung	Eine SID, die verwendet wird, wenn das NTLM-Authentifizierungspaket den Client authentifiziert hat
S-1-5-64-14	SChannel-Authentifizierung	Eine SID, die verwendet wird, wenn das SChannel-Authentifizierungspaket den Client authentifiziert hat.
S-1-5-64-21	Digest-Authentifizierung	Eine SID, die verwendet wird, wenn der Client vom Digestauthentifizierung-Authentifizierungspaket authentifiziert wurde.
S-1-5-80	NT-Dienst	Eine SID, die als Präfix für das NT-Dienstkonto verwendet wird.

SID	ANZEIGENAME	BESCHREIBUNG
S-1-5-80-0	Alle Dienste	Eine Gruppe, die alle auf dem System konfigurierten Dienstprozesse umfasst. Die Mitgliedschaft wird vom Betriebssystem gesteuert. SID S-1-5-80-0 entspricht den NT-SERVICES\ALL-Diensten. Diese SID wurde in Windows Server 2008 R2 eingeführt.
S-1-5-83-0	Virtuelle NT-MACHINE\Virtual-Maschinen	Eine integrierte Gruppe. Die Gruppe wird erstellt, wenn die Hyper-V-Rolle installiert ist. Die Mitgliedschaft in der Gruppe wird vom Hyper-V-Verwaltungsdienst (VMMS) verwaltet. Für diese Gruppe ist die Berechtigung " symbolische Links erstellen " (SeCreateSymbolicLinkPrivilege) und auch das Recht " Anmelden als Dienst " (SeServiceLogonRight) erforderlich.
S-1-16-0	Nicht vertrauenswürdige obligatorische Ebene	Eine SID, die eine nicht vertrauenswürdige Integritätsstufe darstellt.
S-1-16-4096	Niedrige Pflicht Stufe	Eine SID, die eine niedrige Integritätsstufe darstellt.
S-1-16-8192	Obligatorische Mittelstufe	Diese SID stellt eine mittlere Integritätsstufe dar.
S-1-16-8448	Mittel plus obligatorische Ebene	Eine SID, die eine mittlere Plus Integritätsstufe darstellt.
S-1-16-12288	Hohes Pflicht Niveau	Eine SID, die eine hohe Integritätsstufe darstellt.
S-1-16-16384	System Pflicht Stufe	Eine SID, die eine System Integritätsstufe darstellt.
S-1-16-20480	Obligatorische Stufe des geschützten Prozesses	Eine SID, die eine Integritätsstufe des geschützten Prozesses darstellt.
S-1-16-28672	Obligatorische Sicherheitsstufe des Prozesses	Eine SID, die eine sichere Prozess Integritätsstufe darstellt.

Die folgenden Rid sind relativ zu jeder Domäne.

LOSZUWERDEN	IDENTIFIZIERT
DOMAIN_USER_RID_ADMIN	Das administrative Benutzerkonto in einer Domäne.
DOMAIN_USER_RID_GUEST	Das Gastbenutzerkonto in einer Domäne Benutzer, die nicht über ein Konto verfügen, können sich automatisch bei diesem Konto anmelden.

LOSZUWERDEN	IDENTIFIZIERT
DOMAIN_GROUP_RID_USERS	Eine Gruppe, die alle Benutzerkonten in einer Domäne enthält. Alle Benutzer werden dieser Gruppe automatisch hinzugefügt.
DOMAIN_GROUP_RID_GUESTS	Das Gruppen Gastkonto in einer Domäne.
DOMAIN_GROUP_RID_COMPUTERS	Die Gruppe "Domänen Computer". Alle Computer in der Domäne sind Mitglieder dieser Gruppe.
DOMAIN_GROUP_RID_CONTROLLERS	Die Gruppe des Domänencontrollers. Alle Domänencontroller in der Domäne sind Mitglieder dieser Gruppe.
DOMAIN_GROUP_RID_CERT_ADMINS	Die Gruppe der Zertifikatherausgeber. Computer mit Active Directory-Zertifikatdiensten sind Mitglieder dieser Gruppe.
DOMAIN_GROUP_RID_SCHEMA_ADMINS	Die Gruppe "Schemaadministratoren". Mitglieder dieser Gruppe können das Active Directory-Schema ändern.
DOMAIN_GROUP_RID_ENTERPRISE_ADMINS	Die Gruppe der Unternehmensadministratoren. Mitglieder dieser Gruppe haben uneingeschränkten Zugriff auf alle Domänen in der Active Directory-Gesamtstruktur. Unternehmensadministratoren sind für Vorgänge auf Gesamtstrukturebene wie das Hinzufügen oder Entfernen neuer Domänen verantwortlich.
DOMAIN_GROUP_RID_POLICY_ADMINS	Die Gruppe "Richtlinienadministratoren".

Die folgende Tabelle enthält Beispiele für Domänen relative RID, die für die Bildung bekannter SIDs für lokale Gruppen verwendet werden.

LOSZUWERDEN	IDENTIFIZIERT
DOMAIN_ALIAS_RID_ADMINS	Administratoren der Domäne.
DOMAIN_ALIAS_RID_USERS	Alle Benutzer in der Domäne.
DOMAIN_ALIAS_RID_GUESTS	Gäste der Domäne.
DOMAIN_ALIAS_RID_POWER_USERS	Ein Benutzer oder eine Gruppe von Benutzern, die ein System so behandeln möchten, als ob es sich um einen eigenen Computer und nicht um eine Workstation für mehrere Benutzer handelt.
DOMAIN_ALIAS_RID_BACKUP_OPS	Eine lokale Gruppe, die verwendet wird, um die Zuweisung der Benutzerrechte für die Dateisicherung und-Wiederherstellung zu steuern.
DOMAIN_ALIAS_RID_REPLICATOR	Eine lokale Gruppe, die für das Kopieren von Sicherheitsdatenbanken vom primären Domänencontroller zu den Sicherungsdomänencontrollern verantwortlich ist. Diese Konten werden nur vom System verwendet.

LOSZUWERDEN	IDENTIFIZIERT
DOMAIN_ALIAS_RID_RAS_SERVERS	Eine lokale Gruppe, die den Remotezugriff und Server mit dem Internet Authentifizierungsdienst (IAS) darstellt. Diese Gruppe ermöglicht den Zugriff auf verschiedene Attribute von Benutzerobjekten.

Änderungen der Funktionalität der Sicherheits-ID

In der folgenden Tabelle werden die Änderungen der SID-Implementierung in den Windows-Betriebssystemen beschrieben, die in der Liste angegeben sind.

ÄNDERN	BETRIEBSSYSTEMVERSION	BESCHREIBUNG UND RESSOURCEN
Die meisten Betriebssystemdateien gehören der TrustedInstaller-Sicherheits-ID (Security Identifier, SID).	Windows Server 2008, Windows Vista	Mit dieser Änderung soll verhindert werden, dass ein Prozess, der als Administrator oder unter dem LocalSystem-Konto ausgeführt wird, die Betriebssystemdateien automatisch ersetzt.
Eingeschränkte SID-Prüfungen sind implementiert	Windows Server 2008, Windows Vista	Wenn Einschränkende SIDs vorhanden sind, führt Windows zwei Zugriffsüberprüfungen durch. Die erste ist die normale Zugriffsüberprüfung, und die zweite ist die gleiche Zugriffsüberprüfung mit den einschränkenden SIDs im Token. Beide Zugriffsüberprüfungen müssen übergeben werden, damit der Prozess auf das Objekt zugreifen kann.

Funktions-SIDs

Funktionen-Sicherheits-IDs (Security Identifiers, SIDs) werden zur eindeutigen und unveränderlich Identifizierung von Funktionen verwendet. Funktionen stellen ein nicht zu fälschende Autoritäts Zeichen dar, das Zugriff auf Ressourcen (Beispiele: Dokumente, Kamera, Speicherorte usw.) für universelle Windows-Anwendungen gewährt. Eine APP, die über eine Funktion verfügt, erhält Zugriff auf die Ressource, mit der die Funktion verknüpft ist, und eine Funktion, die keine Funktion besitzt, verweigert den Zugriff auf die Ressource.

Alle Funktions-SIDs, die das Betriebssystem kennt, werden in der Windows-Registrierung im Pfad "HKEY_LOCAL_MACHINE \software\microsoft\securitymanager\capabilityclasses\allcachedcapabilities" gespeichert. Jeder Funktions-sid, die Windows von First-oder Drittanbieter-Anwendungen hinzugefügt wird, wird diesem Speicherort hinzugefügt.

Beispiele für Registrierungsschlüssel von Windows 10, Version 1909, 64-Bit Enterprise Edition

Unter AllCachedCapabilities werden möglicherweise die folgenden Registrierungsschlüssel angezeigt:

```
HKEY_LOCAL_MACHINE \software\microsoft\securitymanager\capabilityclasses\allcachedcapabilities\
capabilityClass_DevUnlock HKEY_LOCAL_MACHINE
\software\microsoft\securitymanager\capabilityclasses\allcachedcapabilities\ capabilityClass_DevUnlock_Internal
HKEY_LOCAL_MACHINE \software\microsoft\securitymanager\capabilityclasses\allcachedcapabilities\
capabilityClass_Enterprise HKEY_LOCAL_MACHINE \software\microsoft\securitymanager\capabilityclasses
\Allcachedcapabilities\ capabilityClass_General HKEY_LOCAL_MACHINE
```

\software\microsoft\securitymanager\capabilityclasses\allcachedcapabilities\ capabilityClass_Restricted
HKEY_LOCAL_MACHINE \software\microsoft\securitymanager\ Capabilityclasses\allcachedcapabilities\
capabilityClass_Windows

Alle Funktions-SIDs werden mit dem Präfix S-1-15-3

Weitere Informationen

- [Übersicht über die Zugriffssteuerung](#)

Sicherheitsprinzipale

12.09.2019 • 10 minutes to read

Betrifft

- Windows10
- Windows Server 2016

Dieses Referenzthema für den IT-Experten beschreibt Sicherheitsprinzipale in Bezug auf Windows-Konten und Sicherheitsgruppen zusätzlich zu Sicherheitstechnologien, die sich auf Sicherheitsprinzipale beziehen.

Was sind Sicherheitsprinzipale?

Sicherheitsprinzipale sind alle Entitäten, die vom Betriebssystem authentifiziert werden können, beispielsweise ein Benutzerkonto, ein Computerkonto oder ein Thread oder Prozess, der im Sicherheitskontext eines Benutzer-oder Computerkontos ausgeführt wird, oder die Sicherheitsgruppen für diese Konten. Sicherheitsprinzipale sind seit langem eine Grundlage für das Steuern des Zugriffs auf sicherungsfähige Ressourcen auf Windows-Computern. Jeder Sicherheitsprinzipal wird im Betriebssystem durch eine eindeutige Sicherheits-ID (Security Identifier, SID) dargestellt.

Der folgende Inhalt bezieht sich auf die Windows-Versionen, die in der Liste "**gilt für**" am Anfang dieses Themas angegeben sind.

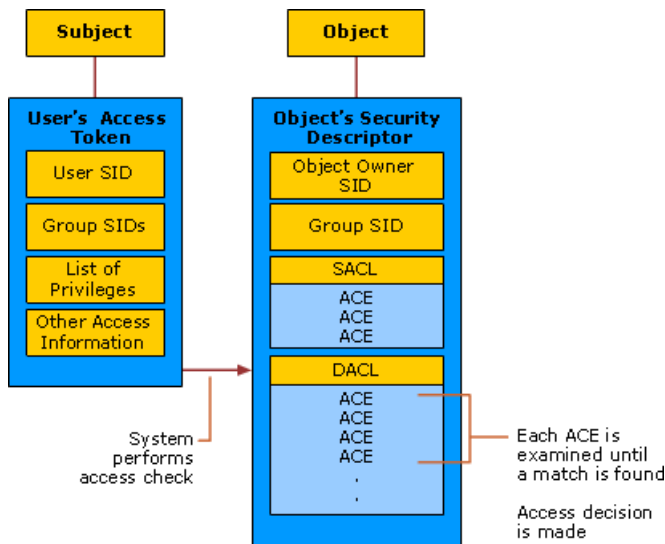
Funktionsweise von Sicherheitsprinzipalen

Sicherheitsprinzipale, die in einer ActiveDirectory-Domäne erstellt werden, sind Active Directory-Objekte, die zum Verwalten des Zugriffs auf Domänenressourcen verwendet werden können. Jedem Sicherheitsprinzipal wird ein eindeutiger Bezeichner zugewiesen, den er während seiner gesamten Lebensdauer behält. Lokale Benutzerkonten und Sicherheitsgruppen werden auf einem lokalen Computer erstellt, und Sie können verwendet werden, um den Zugriff auf Ressourcen auf diesem Computer zu verwalten. Lokale Benutzerkonten und Sicherheitsgruppen werden vom Sam (Security Accounts Manager) auf dem lokalen Computer verwaltet.

Autorisierungs-und Zugriffssteuerungskomponenten

Das folgende Diagramm veranschaulicht den Windowsauthorization und den Zugriffssteuerungsprozess. In diesem Diagramm versucht der Betreff (ein von einem Benutzer initiiertes Prozess), auf ein Objekt zuzugreifen, beispielsweise einen freigegebenen Ordner. Die Informationen im Zugriffstoken des Benutzers werden mit den Zugriffssteuerungseinträgen (ACEs) in der Sicherheitsbeschreibung des Objekts verglichen, und die Zugriffsentscheidung wird getroffen. Die SIDs von Sicherheitsprinzipalen werden im Zugriffstoken des Benutzers und in den ACEs in der Sicherheitsbeschreibung des Objekts verwendet.

Autorisierungs-und Zugriffssteuerungsprozess



Sicherheitsprinzipale stehen in engem Zusammenhang mit den folgenden Komponenten und Technologien:

- [Sicherheitsbezeichner](#)
- [Zugriffstoken](#)
- [Sicherheitsbeschreibungen und Zugriffssteuerungslisten](#)
- [Berechtigungen](#)

Sicherheitsbezeichner

Sicherheits-IDs (SIDs) stellen einen grundlegenden Baustein des Windows-Sicherheitsmodells dar. Sie arbeiten mit bestimmten Komponenten der Autorisierungs- und Zugriffssteuerungstechnologien in der Sicherheitsinfrastruktur der Windows Server-Betriebssysteme. Dies trägt zum Schutz des Zugriffs auf Netzwerkressourcen bei und bietet eine sicherere Computerumgebung.

Eine SID ist ein Wert mit variabler Länge, der verwendet wird, um einen Sicherheitsprinzipal eindeutig zu identifizieren, der alle Entitäten darstellt, die vom System authentifiziert werden können. Zu diesen Entitäten gehören ein Benutzerkonto, ein Computerkonto oder ein Thread oder Prozess, der im Sicherheitskontext eines Benutzer- oder Computerkontos ausgeführt wird. Jedem Sicherheitsprinzipal wird beim Erstellen automatisch eine SID zugewiesen. Die SID wird in einer Sicherheitsdatenbank gespeichert. Wenn eine SID als eindeutiger Bezeichner für einen Benutzer oder eine Gruppe verwendet wird, kann Sie niemals dazu verwendet werden, einen anderen Benutzer oder eine andere Gruppe zu identifizieren.

Jedes Mal, wenn sich ein Benutzer anmeldet, erstellt das System ein Zugriffstoken für diesen Benutzer. Das Zugriffstoken enthält die SID des Benutzers, die Benutzerrechte und die SIDs für Gruppen, zu denen der Benutzer gehört. Dieses Token stellt den Sicherheitskontext für alle Aktionen bereit, die der Benutzer auf diesem Computer ausführt.

Zusätzlich zu den eindeutig erstellten domänenspezifischen SIDs, die bestimmten Benutzern und Gruppen zugewiesen sind, gibt es bekannte SIDs, die generische Gruppen und generische Benutzer identifizieren. Beispielsweise identifizieren die SIDs jeder und die Welt Gruppen, die alle Benutzer umfassen. Bekannte SIDs weisen Werte auf, die für alle Betriebssysteme konstant bleiben.

Zugriffstoken

Ein Zugriffstoken ist ein geschütztes Objekt, das Informationen über die Identität und die Benutzerrechte enthält, die einem Benutzerkonto zugeordnet sind.

Wenn sich ein Benutzer interaktiv anmeldet oder versucht, eine Netzwerkverbindung mit einem Computer unter Windows herzustellen, werden die Anmeldeinformationen des Benutzers vom Anmeldeprozess authentifiziert. Wenn die Authentifizierung erfolgreich ist, gibt der Prozess eine sid für den Benutzer und eine Liste der SIDs für die Sicherheitsgruppen des Benutzers zurück. Die Local Security Authority (LSA) auf dem Computer verwendet

diese Informationen, um ein Zugriffstoken zu erstellen (in diesem Fall das primäre Zugriffstoken). Dazu gehören die vom Anmeldevorgang zurückgegebenen SIDs sowie eine Liste der Benutzerrechte, die dem Benutzer und den Sicherheitsgruppen des Benutzers durch die lokale Sicherheitsrichtlinie zugewiesen werden.

Nachdem die LSA das primäre Zugriffstoken erstellt hat, wird eine Kopie des Zugriffstokens an alle Threads und Prozesse angefügt, die im Namen des Benutzers ausgeführt werden. Wenn ein Thread oder Prozess mit einem sicherungsfähigen Objekt interagiert oder versucht, eine Systemaufgabe auszuführen, die Benutzerrechte erfordert, überprüft das Betriebssystem das Zugriffstoken, das dem Thread zugeordnet ist, um die Autorisierungsstufe zu ermitteln.

Es gibt zwei Arten von Zugriffstoken: Primär- und Identitätswechsel. Jeder Prozess verfügt über ein primäres Token, das den Sicherheitskontext des Benutzerkontos beschreibt, das dem Prozess zugeordnet ist. Ein primäres Zugriffstoken wird normalerweise einem Prozess zugewiesen, um die Standard Sicherheitsinformationen für diesen Prozess darzustellen. Identitätswechselforen werden dagegen in der Regel für Client- und Server Szenarien verwendet. Identitätswechselforen ermöglichen die Ausführung eines Threads in einem Sicherheitskontext, der vom Sicherheitskontext des Prozesses abweicht, der den Thread besitzt.

Sicherheitsbeschreibungen und Zugriffssteuerungslisten

Eine Sicherheitsbeschreibung ist eine Datenstruktur, die jedem sicherungsfähigen Objekt zugeordnet ist. Alle Objekte in Active Directory und alle sicherungsfähigen Objekte auf einem lokalen Computer oder im Netzwerk verfügen über Sicherheitsbeschreibungen, die Ihnen helfen, den Zugriff auf die Objekte zu kontrollieren. Sicherheitsbeschreibungen umfassen Informationen darüber, wer Besitzer eines Objekts ist, wer darauf zugreifen kann und auf welche Weise und welche Zugriffsarten überwacht werden. Sicherheitsbeschreibungen enthalten die Zugriffssteuerungsliste (ACL) eines Objekts, die alle Sicherheitsberechtigungen enthält, die für dieses Objekt gelten. Die Sicherheitsbeschreibung eines Objekts kann zwei Arten von ACLs enthalten:

- Eine freigegebene Zugriffssteuerungsliste (Discretionary Access Control List, DACL), die die Benutzer und Gruppen identifiziert, denen der Zugriff gewährt oder verweigert wird
- Eine SACL (System Access Control List), die steuert, wie Access überwacht wird

Sie können dieses Zugriffssteuerungsmodell verwenden, um Objekte und Attribute wie Dateien und Ordner, Active Directory-Objekte, Registrierungsschlüssel, Drucker, Geräte, Ports, Dienste, Prozesse und Threads einzeln zu sichern. Aufgrund dieses einzelnen Steuerelements können Sie die Sicherheit von Objekten anpassen, um die Anforderungen Ihrer Organisation zu erfüllen, die Autorität über Objekte oder Attribute zu delegieren und benutzerdefinierte Objekte oder Attribute zu erstellen, für die ein eindeutiger Sicherheitsschutz erforderlich ist.

Berechtigungen

Berechtigungen ermöglichen dem Besitzer jedes sicherungsfähigen Objekts, beispielsweise einer Datei, eines ActiveDirectory-Objekts oder eines Registrierungsschlüssels, zu steuern, wer einen Vorgang oder eine Gruppe von Vorgängen für die Objekt- oder Objekteigenschaft ausführen kann. Berechtigungen werden in der Sicherheitsarchitektur als Zugriffssteuerungseinträge (ACEs) ausgedrückt. Da der Zugriff auf ein Objekt im Ermessen des Besitzers des Objekts liegt, wird der Typ der in Windows verwendeten Zugriffssteuerung als diskretionäre Zugriffssteuerung bezeichnet.

Berechtigungen unterscheiden sich von den Benutzerrechten darin, dass Berechtigungen an Objekte angefügt sind und Benutzerrechte für Benutzerkonten gelten. Administratoren können Benutzerrechte für Gruppen oder Benutzer zuweisen. Diese Rechte autorisieren Benutzern, bestimmte Aktionen auszuführen, wie beispielsweise die interaktive Anmeldung bei einem System oder das Sichern von Dateien und Verzeichnissen.

Auf Computern können Administratoren durch Benutzerrechte steuern, wer über die Berechtigung zum Ausführen von Vorgängen verfügt, die sich auf einen ganzen Computer und nicht auf ein bestimmtes Objekt auswirken. Administratoren weisen einzelnen Benutzern oder Gruppen Benutzerrechte als Teil der Sicherheitseinstellungen für den Computer zu. Obwohl Benutzerrechte zentral über GroupPolicy verwaltet werden können, werden Sie lokal angewendet. Benutzer können (und in der Regel) unterschiedliche

Benutzerrechte auf unterschiedlichen Computern besitzen.

Informationen dazu, welche Benutzerrechte verfügbar sind und wie Sie implementiert werden können, finden Sie unter [Zuweisen von Benutzerrechten](#).

Sicherheitskontext in der Authentifizierung

Ein Benutzerkonto ermöglicht es einem Benutzer, sich bei Computern, Netzwerken und Domänen mit einer Identität anzumelden, die vom Computer, dem Netzwerk oder der Domäne authentifiziert werden kann.

In Windows ist jeder Benutzer, jeder Dienst, jede Gruppe oder jeder Computer, der eine Aktion initiieren kann, ein Sicherheitsprinzipal. Sicherheitsprinzipale verfügen über Konten, die lokal auf einem Computer oder Domänen basiert sein können. So können beispielsweise Domänen verbundene Windows-Clientcomputer an einer Netzwerkdomäne teilnehmen, indem Sie mit einem Domänencontroller kommunizieren, auch wenn kein Benutzer angemeldet ist.

Um die Kommunikation zu initiieren, muss der Computer über ein aktives Konto in der Domäne verfügen. Bevor die Kommunikation vom Computer akzeptiert wird, authentifiziert die lokale Sicherheitsautorität auf dem Domänencontroller die Identität des Computers und definiert dann den Sicherheitskontext des Computers genauso wie für den Sicherheitsprinzipal eines Benutzers.

Dieser Sicherheitskontext definiert die Identität und die Funktionen eines Benutzers oder Diensts auf einem bestimmten Computer oder eines Benutzers, Diensts, einer Gruppe oder eines Computers in einem Netzwerk. So werden beispielsweise die Ressourcen (wie eine Dateifreigabe oder ein Drucker), auf die zugegriffen werden kann, und die Aktionen (wie lesen, schreiben oder ändern) definiert, die von einem Benutzer, Dienst oder Computer für diese Ressource ausgeführt werden können.

Der Sicherheitskontext eines Benutzers oder Computers kann von einem Computer zu einem anderen variieren, beispielsweise wenn sich ein Benutzer bei einem Server oder einer anderen Workstation als der primären Workstation des Benutzers authentifiziert. Sie kann auch von einer Sitzung zu einer anderen variieren, beispielsweise, wenn ein Administrator die Rechte und Berechtigungen des Benutzers ändert. Darüber hinaus ist der Sicherheitskontext in der Regel anders, wenn ein Benutzer oder Computer auf eigenständiger Basis, in einer gemischten Netzwerkdomäne oder als Teil einer Active Directory-Domäne betrieben wird.

Konten und Sicherheitsgruppen

Konten und Sicherheitsgruppen, die in einer ActiveDirectory-Domäne erstellt wurden, werden in der ActiveDirectory-Datenbank gespeichert und mithilfe von ActiveDirectory-Tools verwaltet. Diese Sicherheitsprinzipale sind Verzeichnisobjekte und können verwendet werden, um den Zugriff auf Domänenressourcen zu verwalten.

Lokale Benutzerkonten und Sicherheitsgruppen werden auf einem lokalen Computer erstellt, und Sie können verwendet werden, um den Zugriff auf Ressourcen auf diesem Computer zu verwalten. Lokale Benutzerkonten und Sicherheitsgruppen werden auf dem lokalen Computer in der Sicherheitskontenverwaltung (Security Accounts Manager, Sam) gespeichert und verwaltet.

Benutzerkonten

Ein Benutzerkonto identifiziert eindeutig eine Person, die ein Computersystem verwendet. Das Konto signalisiert dem System, die entsprechende Autorisierung durchzusetzen, damit der Benutzer Zugriff auf Ressourcen zulässt oder ablehnt. Benutzerkonten können in Active Directory und auf lokalen Computern erstellt werden, und Administratoren verwenden Sie für folgende Zwecke:

- Die Identität eines Benutzers darstellen, identifizieren und authentifizieren. Ein Benutzerkonto ermöglicht einem Benutzer die Anmeldung bei Computern, Netzwerken und Domänen mit einem eindeutigen Bezeichner, der durch den Computer, das Netzwerk oder die Domäne authentifiziert werden kann.
- Autorisieren (gewähren oder verweigern) des Zugriffs auf Ressourcen. Nachdem ein Benutzer

authentifiziert wurde, ist der Benutzer autorisierter Zugriff auf Ressourcen basierend auf den Berechtigungen, die diesem Benutzer für die Ressource zugewiesen sind.

- Überprüfen Sie die Aktionen, die für ein Benutzerkonto durchgeführt werden.

Windows und die Windows Server-Betriebssysteme verfügen über integrierte Benutzerkonten, oder Sie können Benutzerkonten erstellen, um die Anforderungen Ihrer Organisation zu erfüllen.

Sicherheitsgruppen

Eine Sicherheitsgruppe ist eine Sammlung von Benutzerkonten, Computerkonten und anderen Kontengruppen, die aus Sicherheitsgründen als einzelne Einheit verwaltet werden können. In Windowsoperating-Systemen gibt es mehrere integrierte Sicherheitsgruppen, die mit den entsprechenden Rechten und Berechtigungen für die Ausführung bestimmter Aufgaben vorkonfiguriert sind. Darüber hinaus können Sie (und in der Regel auch) eine Sicherheitsgruppe für jede eindeutige Kombination von Sicherheitsanforderungen erstellen, die für mehrere Benutzer in Ihrer Organisation gilt.

Gruppen können auf einem bestimmten Computer ActiveDirectory-basiert oder lokal sein:

- Active Directory-Sicherheitsgruppen werden verwendet, um Rechte und Berechtigungen für Domänenressourcen zu verwalten.
- Lokale Gruppen sind in der SAM-Datenbank auf lokalen Computern (auf allen Windows-basierten Computern) mit Ausnahme von Domänencontrollern vorhanden. Sie verwenden lokale Gruppen, um Rechte und Berechtigungen nur für Ressourcen auf dem lokalen Computer zu verwalten.

Mithilfe von Sicherheitsgruppen, um die Zugriffssteuerung zu verwalten, haben Sie folgende Möglichkeiten:

- Vereinfachung der Verwaltung Sie können einen allgemeinen Satz von Rechten, einen allgemeinen Satz von Berechtigungen oder beides für viele Konten gleichzeitig zuweisen, anstatt Sie jedem Konto einzeln zuzuweisen. Wenn Benutzeraufträge übertragen oder die Organisation verließen, sind Berechtigungen nicht an Ihre Benutzerkonten gebunden, wodurch die erneute Zuweisung oder Entfernung von Berechtigungen vereinfacht wird.
- Implementieren eines rollenbasierten Zugriffssteuerungsmodells Sie können dieses Modell verwenden, um Berechtigungen zu erteilen, indem Sie Gruppen mit unterschiedlichen Bereichen für geeignete Zwecke verwenden. Zu den in Windows verfügbaren Bereichen gehören lokale, globale, lokale und universelle Domänen.
- Minimieren Sie die Größe von Access Control Lists (ACLs) und beschleunigen Sie die Sicherheitsüberprüfung. Eine Sicherheitsgruppe hat eine eigene sid; Daher kann die Gruppen-SID verwendet werden, um Berechtigungen für eine Ressource festzulegen. In einer Umgebung mit mehr als ein paar tausend Benutzern, wenn die SIDs einzelner Benutzerkonten verwendet werden, um den Zugriff auf eine Ressource anzugeben, kann die ACL dieser Ressource unüberschaubar groß werden, und die Zeit, die erforderlich ist, damit das System die Berechtigungen für die Ressource c überprüft ein unakzeptabler werden.

Beschreibungen und Einstellungsinformationen zu den Domänensicherheitsgruppen, die in Active Directory definiert sind, finden Sie unter [Active Directory-Sicherheitsgruppen](#).

Beschreibungen und Einstellungsinformationen zur Gruppe "besondere Identitäten" finden Sie unter [besondere Identitäten](#).

Weitere Informationen:

- [Übersicht über die Zugriffssteuerung](#)

Lokale Konten

15.02.2020 • 20 minutes to read

Gilt für

- Windows 10
- Windows Server 2019
- Windows Server 2016

Dieses Referenzthema für IT-Experten beschreibt die standardmäßigen lokalen Benutzerkonten für Server, einschließlich der Vorgehensweise zum Verwalten dieser integrierten Konten auf einem Mitglied-oder eigenständigen Server.

Informationen zu lokalen Benutzerkonten

Lokale Benutzerkonten werden lokal auf dem Server gespeichert. Diesen Konten können Rechte und Berechtigungen für einen bestimmten Server, aber nur auf diesem Server zugewiesen werden. Lokale Benutzerkonten sind Sicherheitsprinzipale, die zum Sichern und Verwalten des Zugriffs auf die Ressourcen auf einem eigenständigen oder Mitgliedsserver für Dienste oder Benutzer verwendet werden.

In diesem Thema wird Folgendes beschrieben:

- [Lokale Standardbenutzerkonten](#)
 - [Administrator Konto](#)
 - [Gastkonto](#)
 - [Hilfeassistentkonto-Konto \(wird mithilfe einer Remote Unterstützungs Sitzung installiert\)](#)
 - [DefaultAccount](#)
- [Standardkonten für lokales System](#)
- [Verwalten von lokalen Konten](#)
 - [Einschränken und schützen lokaler Konten mit Administratorrechten](#)
 - [Erzwingen von Einschränkungen für lokales Konto für den Remotezugriff](#)
 - [Netzwerkanmeldung für alle lokalen Administrator Konten verweigern](#)
 - [Erstellen von eindeutigen Kennwörtern für lokale Konten mit Administratorrechten](#)

Informationen zu Sicherheitsprinzipalen finden Sie unter [Sicherheitsprinzipale](#).

Lokale Standardbenutzerkonten

Bei den lokalen Standardbenutzerkonten handelt es sich um integrierte Konten, die bei der Installation von Windows automatisch erstellt werden.

Nach der Installation von Windows können die lokalen Standardbenutzerkonten nicht entfernt oder gelöscht werden. Darüber hinaus bieten lokale Standardbenutzerkonten keinen Zugriff auf Netzwerkressourcen.

Standardmäßige lokale Benutzerkonten werden verwendet, um den Zugriff auf die Ressourcen des lokalen Servers auf der Grundlage der Rechte und Berechtigungen zu verwalten, die dem Konto zugewiesen sind. Die lokalen

Standardbenutzerkonten und die lokalen Benutzerkonten, die Sie erstellen, befinden sich im Ordner Benutzer. Der Ordner "Benutzer" befindet sich im Ordner "lokale Benutzer und Gruppen" in der lokalen Computer Verwaltung der Microsoft Management Console (MMC). Bei der Computer Verwaltung handelt es sich um eine Sammlung von Verwaltungstools, mit denen Sie einen einzelnen lokalen oder Remotecomputer verwalten können. Weitere Informationen finden Sie weiter unten in diesem Thema unter [Verwalten von lokalen Konten](#).

Standardmäßige lokale Benutzerkonten werden in den folgenden Abschnitten beschrieben.

Administrator Konto

Das lokale Standardadministratorkonto ist ein Benutzerkonto für den System Administrator. Jeder Computer verfügt über ein Administratorkonto (SID S-1-5-*Domäne*-500, Anzeigename-Administrator). Das Administrator Konto ist das erste Konto, das während der Windows-Installation erstellt wird.

Das Administrator Konto verfügt über die vollständige Kontrolle über die Dateien, Verzeichnisse, Dienste und anderen Ressourcen auf dem lokalen Computer. Das Administrator Konto kann andere lokale Benutzer erstellen, Benutzerrechte zuweisen und Berechtigungen zuweisen. Das Administrator Konto kann die Kontrolle über lokale Ressourcen jederzeit übernehmen, indem Sie einfach die Benutzerrechte und Berechtigungen ändern.

Das Standard Administrator Konto kann nicht gelöscht oder gesperrt werden, es kann jedoch umbenannt oder deaktiviert werden.

Unter Windows 10 und Windows Server 2016 deaktiviert Windows Setup das integrierte Administrator Konto und erstellt ein weiteres lokales Konto, das Mitglied der Gruppe Administratoren ist. Mitglieder der Gruppe Administratoren können apps mit erhöhten Berechtigungen ausführen, ohne die Option "**als Administrator ausführen**" zu verwenden. Die schnelle Benutzerumschaltung ist sicherer als die Verwendung von runas oder einer anderen Benutzeransicht.

Kontogruppen Mitgliedschaft

Standardmäßig ist das Administrator Konto als Mitglied der Gruppe Administratoren auf dem Server installiert. Es empfiehlt sich, die Anzahl der Benutzer in der Gruppe Administratoren zu begrenzen, da Mitglieder der Gruppe Administratoren auf einem lokalen Server über die Berechtigung "Vollzugriff" auf diesem Computer verfügen.

Das Administrator Konto kann nicht aus der Gruppe "Administratoren" gelöscht oder entfernt werden, es kann jedoch umbenannt werden.

Überlegungen zur Sicherheit

Da das Administratorkonto bekanntermaßen in vielen Versionen des Windows-Betriebssystems vorhanden ist, empfiehlt es sich, das Administratorkonto nach Möglichkeit zu deaktivieren, um böswilligen Benutzern den Zugriff auf den Server oder den Clientcomputer zu erschweren.

Sie können das Administrator Konto umbenennen. Ein umbenanntes Administrator Konto verwendet jedoch weiterhin dieselbe automatisch zugewiesene Sicherheits-ID (Security Identifier, SID), die von böswilligen Benutzern erkannt werden kann. Weitere Informationen zum Umbenennen oder Deaktivieren eines Benutzerkontos finden Sie unter [deaktivieren oder Aktivieren eines lokalen Benutzerkontos](#) und [Umbenennen eines lokalen Benutzerkontos](#).

Aus Sicherheitsgründen sollten Sie sich mit Ihrem lokalen (nicht-Administrator-) Konto anmelden und dann "**als Administrator ausführen**" verwenden, um Aufgaben auszuführen, die eine höhere Rechte Ebene erfordern als ein Standardbenutzerkonto. Verwenden Sie das Administrator Konto nicht, um sich bei Ihrem Computer anzuschließen, es sei denn, dies ist völlig erforderlich. Weitere Informationen finden Sie unter [Ausführen eines Programms mit administrativen Anmeldeinformationen](#).

Im Vergleich dazu wird im Windows-Clientbetriebssystem ein Benutzer mit einem lokalen Benutzerkonto, das über Administrator Rechte verfügt, als System Administrator des Clientcomputers betrachtet. Das erste lokale Benutzerkonto, das während der Installation erstellt wird, wird in der lokalen Gruppe Administratoren gespeichert. Wenn jedoch mehrere Benutzer als lokale Administratoren ausgeführt werden, hat das IT-Personal keine Kontrolle

über diese Benutzer oder deren Clientcomputer.

In diesem Fall können Sie mithilfe von Gruppenrichtlinien sichere Einstellungen aktivieren, die die Verwendung der lokalen Gruppe Administratoren automatisch auf jedem Server oder Clientcomputer steuern können. Weitere Informationen zu Gruppenrichtlinien finden Sie unter [Übersicht über Gruppenrichtlinien](#).

Hinweis leere Kennwörter sind in den Versionen, die in der Liste " **gilt für** " am Anfang dieses Themas festgelegt sind, nicht zulässig.

Wichtig auch wenn das Administrator Konto deaktiviert wurde, kann es mithilfe des abgesicherten Modus weiterhin für den Zugriff auf einen Computer verwendet werden. In der Wiederherstellungskonsole oder im abgesicherten Modus wird das Administrator Konto automatisch aktiviert. Wenn der normale Vorgang fortgesetzt wird, ist er deaktiviert.

Gastkonto

Das Gastkonto ist bei der Installation standardmäßig deaktiviert. Mit dem Gastkonto können gelegentliche oder einmal Benutzer, die nicht über ein Konto auf dem Computer verfügen, sich temporär beim lokalen Server oder Clientcomputer mit begrenzter Benutzerberechtigung anmelden. Standardmäßig weist das Gastkonto ein leeres Kennwort auf. Da das Gastkonto anonymen Zugriff bereitstellen kann, handelt es sich um ein Sicherheitsrisiko. Aus diesem Grund ist es empfehlenswert, das Gastkonto deaktiviert zu lassen, es sei denn, die Verwendung ist vollständig erforderlich.

Kontogruppen Mitgliedschaft

Standardmäßig ist das Gastkonto das einzige Mitglied der standardmäßigen guests-Gruppe (SID S-1-5-32-546), mit der sich ein Benutzer bei einem Server anmelden kann. Gelegentlich kann ein Administrator, der ein Mitglied der Gruppe "Administratoren" ist, einen Benutzer mit einem Gastkonto auf einem oder mehreren Computern einrichten.

Überlegungen zur Sicherheit

Gewähren Sie beim Aktivieren des Gastkontos nur begrenzte Rechte und Berechtigungen. Aus Sicherheitsgründen sollte das Gastkonto nicht über das Netzwerk verwendet und anderen Computern zur Verfügung gestellt werden.

Darüber hinaus sollte der Gastbenutzer im Gastkonto nicht in der Lage sein, die Ereignisprotokolle anzuzeigen. Nach der Aktivierung des Gastkontos empfiehlt es sich, das Gastkonto häufig zu überwachen, um sicherzustellen, dass andere Benutzer Dienste und andere Ressourcen nicht verwenden können, beispielsweise Ressourcen, die versehentlich von einem vorherigen Benutzer zur Verfügung gestellt wurden.

Hilfeassistentkonto-Konto (mit einer Remote Unterstützungs Sitzung installiert)

Das Hilfeassistentkonto-Konto ist ein lokales Standardkonto, das bei Ausführung einer Remote Unterstützungs Sitzung aktiviert ist. Dieses Konto wird automatisch deaktiviert, wenn keine Remote Unterstützungsanforderungen ausstehen.

Hilfeassistentkonto ist das primäre Konto, das zum Einrichten einer Remote Unterstützungs Sitzung verwendet wird. Die Remote Unterstützungs Sitzung wird zum Herstellen einer Verbindung mit einem anderen Computer verwendet, auf dem das Windows-Betriebssystem ausgeführt wird, und wird per Einladung initiiert. Für angeforderte Remoteunterstützung sendet ein Benutzer eine Einladung von seinem Computer, per e-Mail oder als Datei an eine Person, die Hilfe leisten kann. Nachdem die Einladung des Benutzers für eine Remote Unterstützungs Sitzung akzeptiert wurde, wird das standardmäßige Hilfeassistentkonto-Konto automatisch erstellt, um der Person, die Unterstützung gewährt, den Zugriff auf den Computer zu ermöglichen. Das Hilfeassistentkonto-Konto wird vom Remote Desktop Help Session Manager-Dienst verwaltet.

Überlegungen zur Sicherheit

Zu den SIDs, die sich auf das standardmäßige Hilfeassistentkonto-Konto beziehen, gehören:

- SID: S-1-5-<Domäne>-13, Anzeigename Terminal Server-Benutzer. Diese Gruppe umfasst alle Benutzer, die sich bei einem Server anmelden und die Remote Desktop Dienste aktiviert sind. Beachten Sie, dass die Remote Desktop Dienste in Windows Server 2008 als Terminal Dienste bezeichnet werden.
- SID: S-1-5-<Domäne>-14, Anzeigename Remote Interactive Logon. Diese Gruppe umfasst alle Benutzer, die eine Verbindung mit dem Computer herstellen, indem Sie eine Remotedesktopverbindung verwenden. Diese Gruppe ist eine Teilmenge der interaktiven Gruppe. Zugriffstoken, die die SID der interaktiven Remote Anmeldung enthalten, enthalten auch die interaktive sid.

Für das Windows Server-Betriebssystem ist die Remote Unterstützung eine optionale Komponente, die nicht standardmäßig installiert wird. Sie müssen die Remote Unterstützung installieren, bevor Sie verwendet werden kann.

Details zu den Attributen des Hilfeassistentkonto-Kontos finden Sie in der folgenden Tabelle.

Hilfeassistentkonto-Kontoattribute

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-13 (Terminal Server Benutzer), s-1-5-<Domäne>-14 (interaktive Remote Anmeldung)
Typ	Benutzer
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Domänengäste Gäste
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, aber wir empfehlen es nicht.
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein

DefaultAccount

Das DefaultAccount, das auch als standardmäßiges System verwaltetes Konto (DSMA) bezeichnet wird, ist ein integriertes Konto, das in Windows 10, Version 1607 und Windows Server 2016, eingeführt wurde. Der DSMA ist ein bekannter Benutzerkontotyp. Es handelt sich um ein Benutzer neutrales Konto, mit dem Prozesse ausgeführt werden können, die entweder mehr Benutzer oder Benutzer unabhängig sind. Die DSMA ist auf den Desktop-SKUs (vollständige Windows-SKUs) und WS 2016 mit dem DesktopStandard mäßig deaktiviert.

Die DSMA hat eine bekannte Rid von 503. Die Sicherheits-ID (Security Identifier, SID) des DSMA hat daher eine bekannte SID im folgenden Format: S-1-5-21--503

DSMA ist ein Mitglied der bekannten Gruppe **System Managed Accounts Group**, die eine bekannte SID von S-1-5-32-581 hat.

Dem DSMA-Alias kann während der Offlinebereitstellung der Zugriff auf Ressourcen gewährt werden, noch bevor das Konto selbst erstellt wurde. Das Konto und die Gruppe werden beim ersten Booten des Computers innerhalb des Security Accounts Manager (Sam) erstellt.

Verwendung von DefaultAccount in Windows

Aus Sicht der Berechtigung ist das DefaultAccount ein Standardbenutzerkonto. Die DefaultAccount ist für die Ausführung von mehr Benutzer Manifest-Apps (Muma-Apps) erforderlich. MUMA-apps werden immer ausgeführt und reagieren auf Benutzer, die sich bei den Geräten anmelden und sich abmelden. Im Gegensatz zum Windows-Desktop, in dem apps im Kontext des Benutzers ausgeführt werden und beendet werden, wenn sich der Benutzer anmeldet, werden Muma-Apps mithilfe von DSMA ausgeführt.

MUMA-apps sind in freigegebenen Sitzungs-SKUs wie Xbox funktionsfähig. Beispielsweise ist Xbox Shell eine Muma-app. Heute meldet sich Xbox automatisch als Gastkonto an, und alle apps werden in diesem Kontext ausgeführt. Alle apps sind Multi-User-fähig und reagieren auf vom Benutzer-Manager ausgelöste Ereignisse. Die apps werden als Gastkonto ausgeführt.

In ähnlicher Weise meldet sich das Telefon automatisch als "DefApps"-Konto an, das dem standardmäßigen Benutzerkonto in Windows, aber mit einigen zusätzlichen Privilegien ähnelt. Broker, einige Dienste und apps werden als dieses Konto ausgeführt.

Im konvergierten Benutzermodell müssen die Multi-User-Aware-apps und die Multi-User-Aware-Broker in einem anderen Kontext als der der Benutzer ausgeführt werden. Zu diesem Zweck erstellt das System DSMA.

So wird die DefaultAccount auf Domänencontrollern erstellt

Wenn die Domäne mit Domänencontrollern erstellt wurde, die Windows Server 2016 ausführen, wird die DefaultAccount auf allen Domänencontrollern in der Domäne vorhanden sein. Wenn die Domäne mit Domänencontrollern erstellt wurde, die eine frühere Version von Windows Server ausführen, wird die DefaultAccount erstellt, nachdem die PDC-Emulator-Rolle an einen Domänencontroller übertragen wurde, auf dem Windows Server 2016 ausgeführt wird. Die DefaultAccount wird dann auf alle anderen Domänencontroller in der Domäne repliziert.

Empfehlungen für die Verwaltung des Standardkontos (DSMA)

Microsoft rät davon ab, die Standardkonfiguration zu ändern, in der das Konto deaktiviert ist. Es besteht kein Sicherheitsrisiko, wenn das Konto im deaktivierten Zustand ist. Das Ändern der Standardkonfiguration kann zukünftige Szenarien behindern, die auf dieses Konto zurückgreifen.

Standardkonten für lokales System

System

Das Systemkonto wird vom Betriebssystem und von Diensten verwendet, die unter Windows ausgeführt werden. Es gibt viele Dienste und Prozesse im Windows-Betriebssystem, die die Möglichkeit zur internen Anmeldung benötigen, beispielsweise während einer Windows-Installation. Das Systemkonto wurde für diesen Zweck entwickelt, und Windows verwaltet die Benutzerrechte des Systemkontos. Es handelt sich um ein internes Konto, das im Benutzer-Manager nicht angezeigt wird und nicht zu Gruppen hinzugefügt werden kann.

Auf der anderen Seite wird das System Konto im Bereich "**Berechtigungen**" im Menü "**Sicherheit**" auf einem NTFS-Dateisystemvolume im Datei-Manager angezeigt. Standardmäßig wird dem System Konto die Berechtigung "Vollzugriff" für alle Dateien auf einem NTFS-Volume gewährt. Hier verfügt das System Konto über dieselben Funktionsrechte und Berechtigungen wie das Administrator Konto.

Hinweis Wenn Sie den Kontenadministratoren die Gruppe "Dateiberechtigungen" erteilen möchten, wird nicht implizit die Berechtigung für das System Konto erteilt. Die Berechtigungen des System Kontos können aus einer Datei entfernt werden, es wird jedoch nicht empfohlen, diese zu entfernen.

Netzwerkdienst

Das Netzwerkdienstkonto ist ein vordefiniertes lokales Konto, das vom Dienststeuerungs-Manager (Service Control Manager) verwendet wird. Ein Dienst, der im Kontext des Netzwerkdienstkontos ausgeführt wird, zeigt die Anmeldeinformationen des Computers für Remoteserver an. Weitere Informationen finden Sie unter [NetworkService-Konto](#).

lokaler Dienst

Das lokale Dienstkonto ist ein vordefiniertes lokales Konto, das vom Dienststeuerungs-Manager verwendet wird. Er verfügt über Mindestberechtigungen auf dem lokalen Computer und stellt anonyme Anmeldeinformationen im Netzwerk dar. Weitere Informationen finden Sie unter [LocalService-Konto](#).

Verwalten von lokalen Benutzerkonten

Die lokalen Standardbenutzerkonten und die lokalen Benutzerkonten, die Sie erstellen, befinden sich im Ordner Benutzer. Der Ordner Benutzer befindet sich in lokalen Benutzern und Gruppen. Weitere Informationen zum Erstellen und Verwalten von lokalen Benutzerkonten finden Sie unter [Verwalten von lokalen Benutzern](#).

Sie können lokale Benutzer und Gruppen verwenden, um Rechte und Berechtigungen auf dem lokalen Server und nur auf diesem Server zuzuweisen, um die Möglichkeit für lokale Benutzer und Gruppen zum Ausführen bestimmter Aktionen zu begrenzen. Ein Recht ermächtigt einen Benutzer, bestimmte Aktionen auf einem Server durchzuführen, beispielsweise das Sichern von Dateien und Ordnern oder das Herunterfahren eines Servers. Bei einer Zugriffsberechtigung handelt es sich um eine Regel, die einem Objekt, in der Regel eine Datei, einen Ordner oder einen Drucker, zugeordnet ist. Sie reguliert, welche Benutzer auf welche Weise auf ein Objekt auf dem Server zugreifen können.

Sie können keine lokalen Benutzer und Gruppen auf einem Domänencontroller verwenden. Sie können jedoch lokale Benutzer und Gruppen auf einem Domänencontroller verwenden, um auf Remotecomputer zuzielen, die keine Domänencontroller im Netzwerk sind.

Hinweis Sie verwenden ActiveDirectory-Benutzer und-Computer zum Verwalten von Benutzern und Gruppen in Active Directory.

Sie können auch lokale Benutzer mithilfe von NET verwalten. EXE-Benutzer und lokale Gruppen mithilfe von NET verwalten. EXE localgroup oder mithilfe einer Vielzahl von PowerShell-Cmdlets und anderen Skripttechnologien.

Einschränken und schützen lokaler Konten mit Administratorrechten

Ein Administrator kann eine Reihe von Vorgehensweisen verwenden, um zu verhindern, dass böswillige Benutzer gestohlene Anmeldeinformationen wie ein gestohlenes Kennwort oder einen Kennwort-Hash verwenden, damit ein lokales Konto auf einem Computer nicht zur Authentifizierung auf einem anderen Computer mit Administratorrechten verwendet wird. Dies wird auch als "Lateral Movement" bezeichnet.

Der einfachste Ansatz ist die Anmeldung bei Ihrem Computer mit einem Standardbenutzerkonto, anstatt das Administrator Konto für Aufgaben zu verwenden, beispielsweise zum Durchsuchen des Internets, Senden von e-Mails oder Verwenden eines Textprozessors. Wenn Sie eine administrative Aufgabe ausführen möchten, beispielsweise um ein neues Programm zu installieren oder um eine Einstellung zu ändern, die sich auf andere Benutzer auswirkt, müssen Sie nicht zu einem Administrator Konto wechseln. Sie können die Benutzerkontensteuerung (User Account Control, UAC) verwenden, um Sie zur Eingabe einer Berechtigung oder eines Administratorkennworts aufzufordern, bevor Sie die Aufgabe ausführen, wie im nächsten Abschnitt beschrieben.

Zu den anderen Ansätzen, die zum einschränken und schützen von Benutzerkonten mit Administratorrechten verwendet werden können, gehören:

- Erzwingen von Einschränkungen für lokales Konto für den Remotezugriff.
- Verweigern Sie die Netzwerkanmeldung allen lokalen Administrator Konten.

- Erstellen Sie eindeutige Kennwörter für lokale Konten mit Administratorrechten.

Jeder dieser Ansätze wird in den folgenden Abschnitten beschrieben.

Hinweis diese Vorgehensweisen gelten nicht, wenn alle administrativen lokalen Konten deaktiviert sind.

Erzwingen von Einschränkungen für lokales Konto für den Remotezugriff

Die Benutzerkontensteuerung (User Account Control, UAC) ist ein Sicherheitsfeature in Windows, das in Windows Server2008 und in Windows Vista verwendet wurde, und die Betriebssysteme, **auf die sich die Liste** bezieht. Mit der UAC können Sie die Kontrolle über Ihren Computer behalten, indem Sie darüber informiert werden, wenn ein Programm eine Änderung vornimmt, die eine Berechtigung auf Administratorebene erfordert. Die UAC funktioniert durch Anpassen der Berechtigungsstufe Ihres Benutzerkontos. Standardmäßig ist UAC so eingestellt, dass Sie benachrichtigt werden, wenn Anwendungen versuchen, Änderungen an Ihrem Computer vorzunehmen, aber Sie können ändern, wie oft UAC Sie benachrichtigt.

Mit der UAC ist es möglich, dass ein Konto mit Administratorrechten als Standardbenutzerkonto ohne Administratorrechte behandelt wird, bis vollständige Rechte, auch als "Elevation" bezeichnet, angefordert und genehmigt werden. Beispielsweise kann ein Administrator während der Benutzersitzung eines nicht-Administrators Anmeldeinformationen eingeben, um gelegentlich administrative Aufgaben auszuführen, ohne die Benutzer wechseln, abmelden oder den Befehl **Ausführen als** verwenden zu müssen.

Darüber hinaus kann die UAC Administratoren dazu verpflichten, Anwendungen ausdrücklich zu genehmigen, die systemweite Änderungen vornehmen, bevor diesen Anwendungen die Berechtigung zum Ausführen gewährt wird, auch in der Benutzersitzung des Administrators.

So wird beispielsweise ein Standardfeature der UAC angezeigt, wenn sich ein lokales Konto über einen Remotecomputer anmeldet, indem Sie die Netzwerkanmeldung verwenden (beispielsweise mithilfe von net. EXE verwenden). In diesem Fall wird ein Standardbenutzertoken ohne Administratorrechte ausgestellt, aber ohne die Möglichkeit, die Höhe anzufordern oder zu empfangen. Folglich können lokale Konten, die sich mit der Netzwerkanmeldung anmelden, nicht auf administrative Freigaben wie C \$ oder Administrator \$ zugreifen oder eine Remoteverwaltung durchführen.

Weitere Informationen zur UAC finden Sie unter [Benutzerkontensteuerung](#).

In der folgenden Tabelle sind die Gruppenrichtlinien- und Registrierungseinstellungen aufgeführt, die verwendet werden, um lokale Kontoeinschränkungen für den Remotezugriff zu erzwingen.

Nein.	Einstellung	Ausführliche Beschreibung
	Richtlinienspeicherort	Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen
1	Richtlinienname	Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen
	Richtlinieneinstellung	Aktiviert

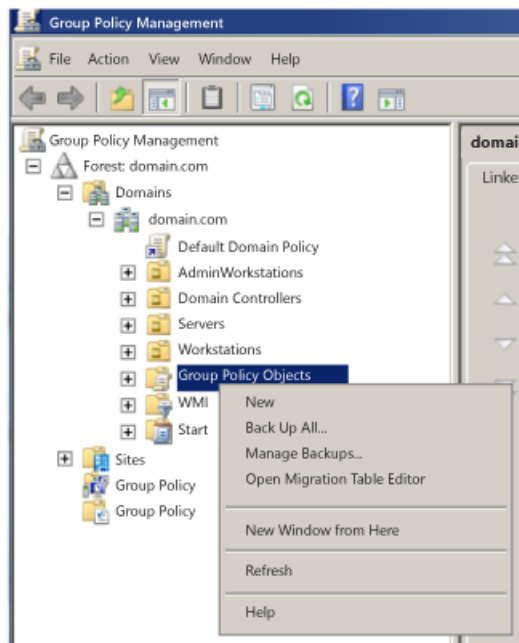
2	Richtlinienspeicherort	Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen
	Richtlinienname	Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen
	Richtlinieneinstellung	Aktiviert
3	Registrierungsschlüssel	HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system
	Name des Registrierungswerts	LocalAccountTokenFilterPolicy
	Registrierungs Werttyp	DWORD
	Registrierungswert Daten	0

NOTE

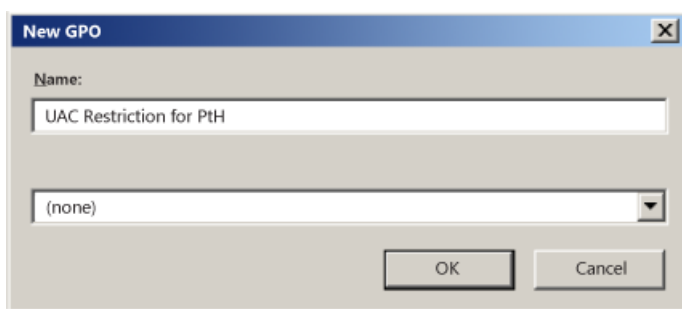
Sie können den Standardwert für LocalAccountTokenFilterPolicy auch erzwingen, indem Sie das benutzerdefinierte ADMX in Sicherheitsvorlagen verwenden.

So erzwingen Sie lokale Kontoeinschränkungen für den Remotezugriff

1. Starten Sie die **Gruppenrichtlinien-Verwaltungskonsolle (Group Policy Management Console, GPMC)**.
2. <Erweitern Sie in der Konsolenstruktur die Domäne< > **Gesamtstruktur>\Domains**, und klicken Sie dann auf ****Gruppenrichtlinienobjekte** , wobei *Gesamtstruktur* der Name der Gesamtstruktur und *Domäne* der Name der Domäne ist, in der Sie das Gruppenrichtlinienobjekt (GPO) festlegen möchten.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** und > dann auf **neu**.



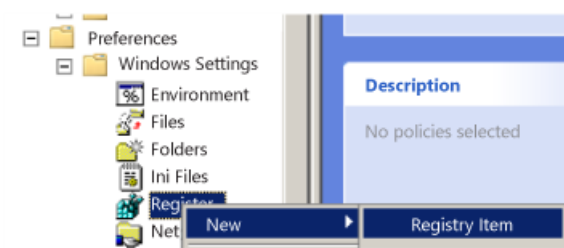
4. Geben <Sie im Dialogfeld **neues GPO** den Namen **GPO _name**>ein > , und klicken Sie auf **OK** , wobei **GPO _name** der Name des neuen Gruppenrichtlinienobjekts ist. Der Name des Gruppenrichtlinienobjekts gibt an, dass das Gruppenrichtlinienobjekt verwendet wird, um zu verhindern, dass lokale Administratorrechte auf einen anderen Computer übertragen werden.



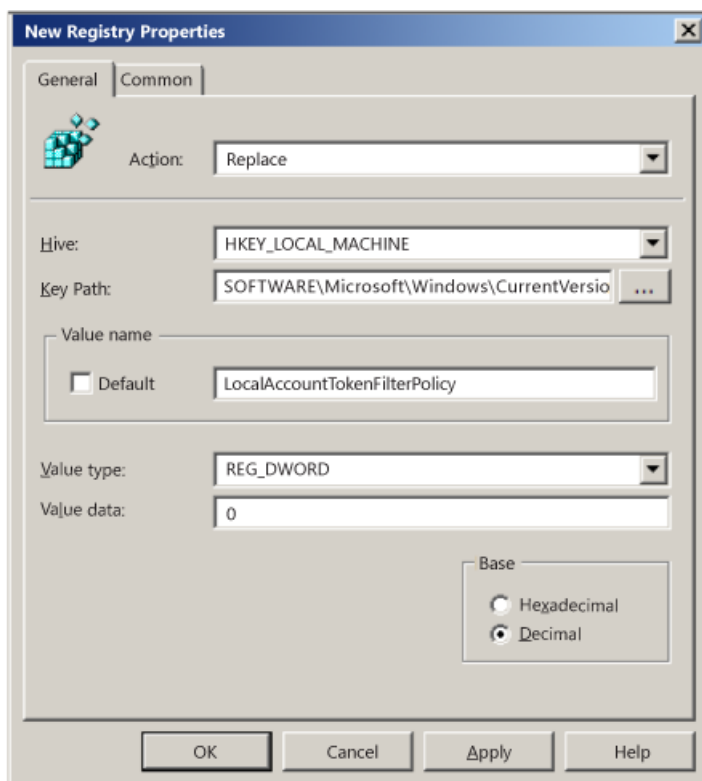
5. Klicken Sie im Detailbereich mit der rechten <Maustaste auf **GPO _name**>und > **Bearbeiten**.



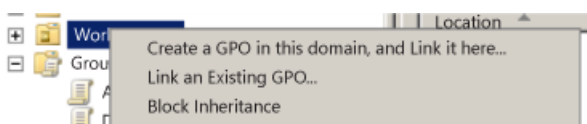
6. Stellen Sie sicher, dass UAC aktiviert ist und dass UAC-Einschränkungen auf das Standard Administrator Konto angewendet werden, indem Sie wie folgt vorgehen:
- Navigieren Sie zum Computer Configuration\Windows Settings\Security Settings\Local Policies, und > wählen Sie **Sicherheitsoptionen**aus.
 - Doppelklicken Sie auf **Benutzerkontensteuerung: alle Administratoren im Administratorgenehmigungsmodus** > ausführen **aktiviert** > **OK**.
 - Doppelklicken Sie auf **Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administrator Konto** > **aktiviert** > **OK**.
7. Führen Sie die folgenden Schritte aus, um sicherzustellen, dass die lokalen Kontoeinschränkungen auf Netzwerkschnittstellen angewendet werden:
- Navigieren Sie zu Computer Configuration\Preferences und Windows-Einstellungen > sowie zur **Registrierung**.
 - Klicken Sie mit **** der rechten Maustaste > auf Registrierung, und wählen Sie **Neues** > **Registrierungselement**aus.



- c. Ändern Sie im Dialogfeld **neue Registrierungseigenschaften** auf der Registerkarte **Allgemein** die Einstellung im Feld **Aktion** auf **ersetzen**.
- d. Stellen Sie sicher, dass das Feld **Hive** auf **HKEY _LOCAL _MACHINE** festgesetzt ist.
- e. Klicken Sie auf (...), navigieren Sie zum folgenden Speicherort für **Schlüsselpfad** > **auswählen** für: **SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
- f. Geben Sie im Bereich **Wertname** den Namen **LocalAccountTokenFilterPolicy** ein.
- g. Wählen Sie im Feld **Werttyp** in der Dropdownliste die Option **reg _DWORD** aus, um den Wert zu ändern.
- h. Stellen Sie im Feld **Wertdaten** sicher, dass der Wert auf **0** festgesetzt ist.
- i. Überprüfen Sie diese Konfiguration > , und klicken Sie auf **OK**.



8. Führen Sie die folgenden Schritte aus, um das Gruppenrichtlinienobjekt mit der ersten **Arbeitsstationen** - Organisationseinheit (OU) zu verknüpfen:
 - a. Navigieren Sie zum <OU-><Pfad der Gesamtstruktur>->\Domains\<Domäne>.
 - b. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **Workstations** , und > **Verknüpfen Sie ein vorhandenes Gruppenrichtlinienobjekt**.



c. Wählen Sie das soeben erstellte Gruppenrichtlinienobjekt aus > , und klicken Sie auf **OK**.

9. Testen Sie die Funktionalität von Enterprise-Anwendungen auf den Arbeitsstationen in dieser ersten Organisationseinheit, und beheben Sie alle Probleme, die durch die neue Richtlinie verursacht werden.

10. Erstellen von Links zu allen anderen OUs, die Workstations enthalten.

11. Erstellen von Links zu allen anderen OUs, die Server enthalten

Netzwerkanmeldung für alle lokalen Administrator Konten verweigern

Lokale Konten ablehnen die Möglichkeit zum Durchführen von Netzwerkanmeldungen kann dazu beitragen, dass der Kennwort-Hash eines lokalen Kontos bei einem böswilligen Angriff wieder verwendet wird. Dieses Verfahren hilft, seitliche Bewegungen zu verhindern, indem Sie sicherstellen, dass die Anmeldeinformationen für lokale Konten, die von einem kompromittierten Betriebssystem gestohlen werden, nicht zum kompromittieren zusätzlicher Computer verwendet werden können, die dieselben Anmeldeinformationen verwenden.

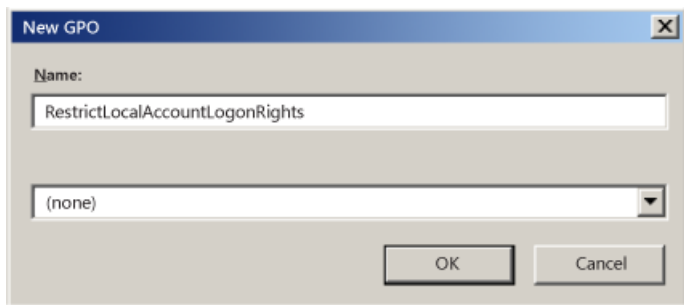
Hinweis um dieses Verfahren ausführen zu können, müssen Sie zunächst den Namen des lokalen Standardadministratorkontos angeben, bei dem es sich möglicherweise nicht um den Standardbenutzernamen "Administrator" handelt, und alle anderen Konten, die Mitglieder der lokalen Gruppe Administratoren sind.

In der folgenden Tabelle sind die Gruppenrichtlinieneinstellungen aufgeführt, die verwendet werden, um die Netzwerkanmeldung für alle lokalen Administrator Konten zu verweigern.

Nein.	Einstellung	Ausführliche Beschreibung
	Richtlinienspeicherort	Computer Computerkonfiguration\Windows-Einstellungen Richtlinien\Zuweisen Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechtezuweisung
1	Richtlinienname	Zugriff vom Netzwerk auf diesen Computer verweigern
	Richtlinieneinstellung	Lokales Konto und Mitglied der Gruppe "Administratoren"
2	Richtlinienspeicherort	Computer Computerkonfiguration\Windows-Einstellungen Richtlinien\Zuweisen Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisen von Benutzerrechtezuweisung
	Richtlinienname	Anmelden über Remotedesktopdienste verweigern
	Richtlinieneinstellung	Lokales Konto und Mitglied der Gruppe "Administratoren"

So verweigern Sie die Netzwerkanmeldung für alle lokalen Administratorkonten

1. Starten Sie die **Gruppenrichtlinien-Verwaltungskonsolle (Group Policy Management Console, GPMC)**.
2. <Erweitern Sie in der Konsolenstruktur die Domäne<> **Gesamtstruktur>\Domains** und dann ****Gruppenrichtlinienobjekte**, wobei *Gesamtstruktur* der Name der Gesamtstruktur und *Domäne* der Name der Domäne ist, in der Sie das Gruppenrichtlinienobjekt (GPO) festlegen möchten.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** und > dann auf **neu**.
4. Geben <Sie im Dialogfeld **Neues Gruppen** Richtlinienobjekt die Zeichenfolge **GPO _name**> ein, und klicken Sie dann > auf **OK**, wobei *GPO _name* der Name des neuen Gruppenrichtlinienobjekts ist, das angibt, dass es verwendet wird, um die lokalen Administratorkonten von der interaktiven Anmeldung beim Computer zu beschränken.



5. Klicken Sie im Detailbereich mit der rechten <Maustaste auf **GPO _name**> und > **Bearbeiten**.



6. Konfigurieren Sie die Benutzerrechte zum Verweigern von Netzwerkanmeldungen für administrative lokale Konten wie folgt:
 - a. Navigieren Sie zum Computer Configuration\Windows Settings\Security Settings\, und > verwenden Sie die **Zuweisung von Benutzerrechten**.
 - b. Doppelklicken Sie auf **Zugriff verweigern für diesen Computer aus dem Netzwerk**.
 - c. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**, geben Sie **Lokales Konto und Mitglied der Gruppe Administratoren** ein, und > klicken Sie auf **OK**.
7. Konfigurieren Sie die Benutzerrechte so, dass Remote Desktop Anmeldungen (Remote Interactive) für administrative lokale Konten wie folgt verweigert werden:
 - a. Navigieren Sie zu Computer Configuration\Policies\Windows-Einstellungen und lokalen Richtlinien, und klicken Sie dann auf **Zuweisung von Benutzerrechten**.
 - b. Doppelklicken Sie auf **Anmeldung über Remote Desktop Dienste verweigern**.
 - c. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**, geben Sie **Lokales Konto und Mitglied der Gruppe Administratoren** ein, und > klicken Sie auf **OK**.
8. Verknüpfen Sie das Gruppenrichtlinienobjekt mit der ersten **Arbeits Stations** -ou wie folgt:
 - a. Navigieren Sie zum <\OU-<Pfad der Gesamtstruktur>-\Domains\<Domäne>.
 - b. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **Workstations**, und > **Verknüpfen Sie ein vorhandenes Gruppenrichtlinienobjekt**.
 - c. Wählen Sie das soeben erstellte Gruppenrichtlinienobjekt aus >, und klicken Sie auf **OK**.

9. Testen Sie die Funktionalität von Enterprise-Anwendungen auf den Arbeitsstationen in dieser ersten Organisationseinheit, und beheben Sie alle Probleme, die durch die neue Richtlinie verursacht werden.
10. Erstellen von Links zu allen anderen OUs, die Workstations enthalten.
11. Erstellen von Links zu allen anderen OUs, die Server enthalten

Hinweis Sie müssen möglicherweise ein separates Gruppenrichtlinienobjekt erstellen, wenn sich der Benutzername des Standard Administrator Kontos auf Workstations und Servern unterscheidet.

Erstellen von eindeutigen Kennwörtern für lokale Konten mit Administratorrechten

Kennwörter sollten für jedes einzelne Konto eindeutig sein. Obwohl dies in der Regel für einzelne Benutzerkonten zutrifft, besitzen viele Unternehmen identische Kennwörter für gängige lokale Konten, beispielsweise das Standard Administrator Konto. Dies geschieht auch, wenn die gleichen Kennwörter für lokale Konten während der Bereitstellung des Betriebssystems verwendet werden.

Kennwörter, die unverändert bleiben oder synchron geändert werden, um Sie identisch zu halten, tragen zu einem erheblichen Risiko für Organisationen bei. Durch das Randomisieren der Kennwörter werden "Pass-the-Hash"-Angriffe durch Verwendung unterschiedlicher Kennwörter für lokale Konten verringert, was die Möglichkeit von böswilligen Benutzern, Kennworthashes dieser Konten zu verwenden, um andere Computer zu gefährden, behindert.

Kennwörter können randomisiert werden durch:

- Einkauf und Implementierung eines Enterprise-Tools, um diese Aufgabe zu erfüllen. Diese Tools werden gemeinhin als Tools für privilegierte Kennwortverwaltung bezeichnet.
- Konfigurieren der [lokalen Administrator Kennwort-Lösung \(Runden\)](#) , um diese Aufgabe auszuführen.
- Erstellen und Implementieren eines benutzerdefinierten Skripts oder einer Lösung zum Randomisieren von Kennwörtern für lokales Konto

Weitere Informationen

Die folgenden Ressourcen bieten zusätzliche Informationen zu Technologien, die sich auf lokale Konten beziehen.

- [Sicherheitsprinzipale](#)
- [Sicherheitskennungen](#)
- [Übersicht über die Zugriffssteuerung](#)

Active Directory-Konten

11.02.2020 • 33 minutes to read

Betrifft

- Windows Server 2016

Windows Server-Betriebssysteme werden mit lokalen Standardkonten installiert. Darüber hinaus können Sie Benutzerkonten erstellen, um die Anforderungen Ihrer Organisation zu erfüllen. Dieses Referenzthema für den IT-Experten beschreibt die lokalen Windows Server-Standardkonten, die lokal auf dem Domänencontroller gespeichert sind und in Active Directory verwendet werden.

Dieses Referenzthema beschreibt keine standardmäßigen lokalen Benutzerkonten für einen Mitglied-oder eigenständigen Server oder für einen Windows-Client. Weitere Informationen finden Sie unter [lokale Konten](#).

Informationen zu diesem Thema

In diesem Thema wird Folgendes beschrieben:

- [Lokale Standardkonten in Active Directory](#)
 - [Administrator Konto](#)
 - [Gastkonto](#)
 - [Hilfeassistentkonto-Konto \(mit einer Remote Unterstützungs Sitzung installiert\)](#)
 - [KRBTGT-Konto](#)
- [Einstellungen für lokale Standardkonten in Active Directory](#)
- [Verwalten von lokalen Standardkonten in Active Directory](#)
- [Einschränken und Schützen vertraulicher Domänenkonten](#)
 - [Trennen von Administratorkonten von Benutzerkonten](#)
 - [Erstellen dedizierter Workstation-Hosts ohne Internet-und e-Mail-Zugriff](#)
 - [Einschränken des Administrator Anmeldezugriffs auf Server und Workstations](#)
 - [Deaktivieren der Konto Delegierungsberechtigung für Administratorkonten](#)
- [Sichern und Verwalten von Domänencontrollern](#)

Lokale Standardkonten in Active Directory

Bei lokalen Standardkonten handelt es sich um integrierte Konten, die automatisch erstellt werden, wenn ein Windows Server-Domänencontroller installiert und die Domäne erstellt wird. Diese lokalen Standardkonten verfügen über Pendants in Active Directory. Diese Konten verfügen auch über einen domänenweiten Zugriff und sind völlig unabhängig von den standardmäßigen lokalen Benutzerkonten für einen Mitglied-oder eigenständigen Server.

Sie können standardmäßigen lokalen Konten auf einem bestimmten Domänencontroller und nur auf diesem Domänencontroller Rechte und Berechtigungen zuweisen. Diese Konten sind lokal für die Domäne. Nachdem die lokalen Standardkonten installiert wurden, werden Sie im Container Benutzer in Active Directory-Benutzer und-

Computer gespeichert. Es empfiehlt sich, die lokalen Standardkonten im Benutzercontainer beizubehalten und nicht zu versuchen, diese Konten beispielsweise in eine andere Organisationseinheit (Organizational Unit, OU) zu verschieben.

Die lokalen Standardkonten im Container Benutzer umfassen: Administrator, Gast und krbtgt. Das Hilfeassistentkonto-Konto wird installiert, wenn eine Remote Unterstützungs Sitzung eingerichtet wird. In den folgenden Abschnitten werden die lokalen Standardkonten und deren Verwendung in Active Directory beschrieben.

In erster Linie führen lokale Standardkonten die folgenden Aktionen aus:

- Lassen Sie die Domäne die Identität des Benutzers, der dem Konto zugewiesen ist, mithilfe eindeutiger Anmeldeinformationen (Benutzername und Kennwort) darstellen, identifizieren und authentifizieren. Es wird empfohlen, die einzelnen Benutzer einem einzigen Konto zuzuweisen, um maximale Sicherheit zu gewährleisten. Mehrere Benutzer sind nicht berechtigt, ein Konto freizugeben. Mit einem Benutzerkonto kann sich ein Benutzer bei Computern, Netzwerken und Domänen mit einem eindeutigen Bezeichner anmelden, der durch den Computer, das Netzwerk oder die Domäne authentifiziert werden kann.
- Autorisieren (gewähren oder verweigern) des Zugriffs auf Ressourcen. Nachdem die Anmeldeinformationen eines Benutzers authentifiziert wurden, ist der Benutzer für den Zugriff auf die Netzwerk- und Domänenressourcen basierend auf den explizit zugewiesenen Berechtigungen des Benutzers für die Ressource autorisiert.
- Überprüfen Sie die Aktionen, die für ein Benutzerkonto durchgeführt werden.

In Active Directory werden von Administratoren standardmäßige lokale Konten verwendet, um Domänen- und Mitgliedsserver direkt und über dedizierte administrative Arbeitsstationen zu verwalten. Active Directory-Konten bieten Zugriff auf Netzwerkressourcen. Active Directory-Benutzerkonten und-Computer Konten können eine physikalische Entität wie einen Computer oder eine Person darstellen oder als dedizierte Dienstkonto für einige Anwendungen fungieren.

Jedes lokale Standardkonto wird automatisch einer Sicherheitsgruppe zugewiesen, die mit den entsprechenden Rechten und Berechtigungen zum Ausführen bestimmter Aufgaben vorkonfiguriert ist. Active Directory-Sicherheitsgruppen sammeln Benutzerkonten, Computerkonten und andere Gruppen in verwaltbare Einheiten. Weitere Informationen finden Sie unter [Active Directory-Sicherheitsgruppen](#).

Auf einem Active Directory-Domänencontroller wird jedes lokale Standardkonto als Sicherheitsprinzipal bezeichnet. Bei einem Sicherheitsprinzipal handelt es sich um ein Verzeichnisobjekt, das zum Sichern und Verwalten von Active Directory-Diensten dient, die Zugriff auf Domänencontrollerressourcen bieten. Ein Sicherheitsprinzipal umfasst Objekte wie Benutzerkonten, Computerkonten, Sicherheitsgruppen oder die Threads oder Prozesse, die im Sicherheitskontext eines Benutzer- oder Computerkontos ausgeführt werden. Weitere Informationen finden Sie unter [Sicherheitsprinzipale](#).

Ein Sicherheitsprinzipal wird durch eine eindeutige Sicherheits-ID (Security Identifier, SID) dargestellt. Die SIDs, die sich auf die einzelnen lokalen Standardkonten in Active Directory beziehen, werden in den folgenden Abschnitten beschrieben.

Einige der lokalen Standardkonten sind durch einen Hintergrundprozess geschützt, der in regelmäßigen Abständen eine bestimmte Sicherheitsbeschreibung überprüft und anwendet. Eine Sicherheitsbeschreibung ist eine Datenstruktur, die Sicherheitsinformationen enthält, die einem geschützten Objekt zugeordnet sind. Durch diesen Vorgang wird sichergestellt, dass alle erfolgreichen unbefugten Versuche, die Sicherheitsbeschreibung für eines der lokalen Standardkonten oder-Gruppen zu ändern, mit den geschützten Einstellungen überschrieben werden.

Diese Sicherheitsbeschreibung ist im AdminSDHolder-Objekt vorhanden. Wenn Sie die Berechtigungen für eine der Dienstadministratorgruppen oder für eines der Mitgliedskonten ändern möchten, müssen Sie die Sicherheitsbeschreibung für das AdminSDHolder-Objekt ändern, um sicherzustellen, dass Sie konsistent

angewendet wird. Achten Sie beim vornehmen dieser Änderungen darauf, dass Sie auch die Standardeinstellungen ändern, die auf alle geschützten Konten angewendet werden.

Administrator Konto

Das Administrator Konto ist ein Standardkonto, das in allen Versionen des Windows-Betriebssystems auf jedem Computer und Gerät verwendet wird. Das Administratorkonto wird vom System Administrator für Aufgaben verwendet, für die Administratoranmeldeinformationen erforderlich sind. Dieses Konto kann nicht gelöscht oder gesperrt werden, aber das Konto kann umbenannt oder deaktiviert werden.

Das Administrator Konto gewährt dem Benutzer vollständigen Zugriff auf die Dateien, Verzeichnisse, Dienste und anderen Ressourcen, die sich auf dem lokalen Server befinden. Das Administrator Konto kann verwendet werden, um lokale Benutzer zu erstellen und Benutzerrechte und Zugriffssteuerungsberechtigungen zuzuweisen. Der Administrator kann auch dazu verwendet werden, die Kontrolle über lokale Ressourcen zu übernehmen, indem die Benutzerrechte und-Berechtigungen geändert werden. Obwohl Dateien und Verzeichnisse vorübergehend vom Administratorkonto geschützt werden können, kann das Administratorkonto diese Ressourcen jederzeit übernehmen, indem die Zugriffsberechtigungen geändert werden.

Kontogruppen Mitgliedschaft

Das Administratorkonto hat die Mitgliedschaft in den Standardsicherheitsgruppen, wie in der Tabelle "Administratorkonto Attribute" weiter unten in diesem Thema beschrieben.

Die Sicherheitsgruppen stellen sicher, dass Sie die Administratorrechte steuern können, ohne die einzelnen Administratorkonten ändern zu müssen. In den meisten Fällen müssen Sie die grundlegenden Einstellungen für dieses Konto nicht ändern. Möglicherweise müssen Sie jedoch die erweiterten Einstellungen ändern, beispielsweise die Mitgliedschaft in bestimmten Gruppen.

Überlegungen zur Sicherheit

Nach der Installation des Server Betriebssystems besteht ihre erste Aufgabe darin, die Administrator Kontoeigenschaften sicher einzurichten. Dazu gehören das Einrichten eines besonders langen, sicheren Kennworts und das Sichern der Profileinstellungen für Remotesteuerung und Remote Desktop Dienste.

Das Administrator Konto kann auch deaktiviert werden, wenn es nicht erforderlich ist. Wenn Sie das Administrator Konto umbenennen oder deaktivieren, ist es für böswillige Benutzer schwieriger, auf das Konto zuzugreifen. Selbst wenn das Administrator Konto deaktiviert ist, kann es jedoch weiterhin verwendet werden, um mithilfe des abgesicherten Modus auf einen Domänencontroller zuzugreifen.

Auf einem Domänencontroller wird das Administrator Konto zum Domänenadministratorkonto. Das Domänenadministratorkonto wird zum Anmelden beim Domänencontroller verwendet, und für dieses Konto ist ein sicheres Kennwort erforderlich. Mit dem Domänenadministratorkonto können Sie auf Domänenressourcen zugreifen.

Hinweis:

Wenn der Domänencontroller zunächst installiert ist, können Sie sich anmelden und mit dem Server-Manager ein lokales Administrator Konto einrichten, das die Rechte und Berechtigungen enthält, die Sie zuweisen möchten. So können Sie beispielsweise ein lokales Administrator Konto zum Verwalten des Betriebssystems verwenden, wenn Sie es zum ersten Mal installieren. Mithilfe dieser Vorgehensweise können Sie das Betriebssystem ohne Sperrung einrichten. Im Allgemeinen müssen Sie das Konto nach der Installation nicht mehr verwenden. Sie können nur lokale Benutzerkonten auf dem Domänencontroller erstellen, bevor Active Directory-Domänendienste installiert werden, und nicht danach.

Wenn Active Directory auf dem ersten Domänencontroller in der Domäne installiert ist, wird das Administrator Konto für Active Directory erstellt. Das Administrator Konto ist das mächtigste Konto in der Domäne. Es erhält domänenweite Zugriffs- und Administratorrechte, um den Computer und die Domäne zu verwalten, und er verfügt über die umfassendsten Rechte und Berechtigungen für die Domäne. Die Person, die die Active Directory-

Domänendienste auf dem Computer installiert, erstellt während der Installation das Kennwort für dieses Konto.

Attribute des Administrator Kontos

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-500
Typ	Benutzer
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	n.v.
Standardmitglied von	Administratoren, Domänenadministratoren, Unternehmensadministratoren und Domänenbenutzer. Beachten Sie, dass die primäre Gruppen-ID aller Benutzerkonten Domänenbenutzer ist. Besitzer von Gruppenrichtlinien Erstellen und Schema Administratoren in Active Directory Gruppe "Domänenbenutzer"
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass Sie die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegieren können?	Nein

Gastkonto

Das Gastkonto ist ein lokales Standardkonto hat nur eingeschränkten Zugriff auf den Computer und ist standardmäßig deaktiviert. Das Gastkonto kann nicht gelöscht oder deaktiviert werden, und der Konto Name kann nicht geändert werden. Standardmäßig bleibt das Kennwort des Gastkontos leer. Mit einem leeren Kennwort kann auf das Gastkonto zugegriffen werden, ohne dass der Benutzer ein Kennwort eingeben muss.

Das Gastkonto ermöglicht gelegentlichen oder einmal Benutzern, die nicht über ein einzelnes Konto auf dem Computer verfügen, die Anmeldung beim lokalen Server oder in der Domäne mit eingeschränkten Rechten und Berechtigungen. Das Gastkonto kann aktiviert werden, und das Kennwort kann bei Bedarf eingerichtet werden, jedoch nur von einem Mitglied der Gruppe Administratoren in der Domäne.

Kontogruppen Mitgliedschaft

Das Gastkonto hat die Mitgliedschaft in den standardmäßigen Sicherheitsgruppen, die in der folgenden Gastkonto-Attributtabelle beschrieben sind. Standardmäßig ist das Gastkonto das einzige Mitglied der standardmäßigen Gruppe "Gäste", mit dem sich ein Benutzer bei einem Server anmelden kann, und die globale Gruppe "Domain guests", mit der sich ein Benutzer bei einer Domäne anmelden kann.

Ein Mitglied der Gruppe "Administratoren" oder "Domänen-Admins" kann einen Benutzer mit einem Gastkonto auf einem oder mehreren Computern einrichten.

Überlegungen zur Sicherheit

Da das Gastkonto anonymen Zugriff bereitstellen kann, handelt es sich um ein Sicherheitsrisiko. Darüber hinaus gibt es eine bekannte SID. Aus diesem Grund ist es empfehlenswert, das Gastkonto deaktiviert zu lassen, es sei denn, die Verwendung ist erforderlich und dann nur mit eingeschränkten Rechten und Berechtigungen für einen sehr begrenzten Zeitraum.

Wenn das Gastkonto erforderlich ist, ist ein Administrator auf dem Domänencontroller zum Aktivieren des Gastkontos erforderlich. Das Gastkonto kann aktiviert werden, ohne dass ein Kennwort erforderlich ist, oder es kann mit einem sicheren Kennwort aktiviert werden. Der Administrator gewährt auch eingeschränkte Rechte und Berechtigungen für das Gastkonto. So verhindern Sie unbefugten Zugriff:

- Gewähren Sie dem Gastkonto nicht das [Systembenutzer Recht Herunterfahren](#) . Wenn ein Computer heruntergefahren oder gestartet wird, ist es möglich, dass ein Gastbenutzer oder jeder mit lokalem Zugriff, beispielsweise ein böswilliger Benutzer, unbefugten Zugriff auf den Computer erlangen kann.
- Stellen Sie dem Gastkonto nicht die Möglichkeit zum Anzeigen der Ereignisprotokolle zur Verfügung. Nach der Aktivierung des Gastkontos empfiehlt es sich, dieses Konto häufig zu überwachen, um sicherzustellen, dass andere Benutzer Dienste und andere Ressourcen nicht verwenden können, beispielsweise Ressourcen, die versehentlich von einem vorherigen Benutzer zur Verfügung gestellt wurden.
- Verwenden Sie das Gastkonto nicht, wenn der Server über einen externen Netzwerkzugriff verfügt oder auf andere Computer zugreifen kann.

Wenn Sie sich entschließen, das Gastkonto zu aktivieren, müssen Sie die Nutzung einschränken und das Kennwort regelmäßig ändern. Wie beim Administrator Konto möchten Sie das Konto möglicherweise als zusätzliche Sicherheitsmaßnahme umbenennen.

Darüber hinaus ist ein Administrator für die Verwaltung des Gastkontos verantwortlich. Der Administrator überwacht das Gastkonto, deaktiviert das Gastkonto, wenn es nicht mehr verwendet wird, und ändert oder entfernt das Kennwort bei Bedarf.

Details zu den Gastkonto Attributen finden Sie in der folgenden Tabelle.

Gast Kontoattribute

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-501
Typ	Benutzer
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Gäste, Domänengäste
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, aber wir empfehlen es nicht.

ATTRIBUT	WERT
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein

Hilfeassistentkonto-Konto (mit einer Remote Unterstützungs Sitzung installiert)

Das Hilfeassistentkonto-Konto ist ein lokales Standardkonto, das bei Ausführung einer Remote Unterstützungs Sitzung aktiviert ist. Dieses Konto wird automatisch deaktiviert, wenn keine Remote Unterstützungsanforderungen ausstehen.

Hilfeassistentkonto ist das primäre Konto, das zum Einrichten einer Remote Unterstützungs Sitzung verwendet wird. Die Remote Unterstützungs Sitzung wird zum Herstellen einer Verbindung mit einem anderen Computer verwendet, auf dem das Windows-Betriebssystem ausgeführt wird, und wird per Einladung initiiert. Für angeforderte Remoteunterstützung sendet ein Benutzer eine Einladung von seinem Computer, per e-Mail oder als Datei an eine Person, die Hilfe leisten kann. Nachdem die Einladung des Benutzers für eine Remote Unterstützungs Sitzung akzeptiert wurde, wird das standardmäßige Hilfeassistentkonto-Konto automatisch erstellt, um der Person, die Unterstützung gewährt, den Zugriff auf den Computer zu ermöglichen. Das Hilfeassistentkonto-Konto wird vom Remote Desktop Help Session Manager-Dienst verwaltet.

Überlegungen zur Sicherheit

Zu den SIDs, die sich auf das standardmäßige Hilfeassistentkonto-Konto beziehen, gehören:

- SID: S-1-5-<Domäne>-13, Anzeigename Terminal Server-Benutzer. Diese Gruppe umfasst alle Benutzer, die sich bei einem Server anmelden und die Remote Desktop Dienste aktiviert sind. Beachten Sie, dass die Remote Desktop Dienste in Windows Server 2008 als Terminal Dienste bezeichnet werden.
- SID: S-1-5-<Domäne>-14, Anzeigename Remote Interactive Logon. Diese Gruppe umfasst alle Benutzer, die eine Verbindung mit dem Computer herstellen, indem Sie eine Remotedesktopverbindung verwenden. Diese Gruppe ist eine Teilmenge der interaktiven Gruppe. Zugriffstoken, die die SID der interaktiven Remote Anmeldung enthalten, enthalten auch die interaktive sid.

Für das Windows Server-Betriebssystem ist die Remote Unterstützung eine optionale Komponente, die nicht standardmäßig installiert wird. Sie müssen die Remote Unterstützung installieren, bevor Sie verwendet werden kann.

Details zu den Attributen des Hilfeassistentkonto-Kontos finden Sie in der folgenden Tabelle.

Hilfeassistentkonto-Kontoattribute

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-13 (Terminal Server Benutzer), s-1-5-<Domäne>-14 (interaktive Remote Anmeldung)
Typ	Benutzer
Standardcontainer	CN = Users, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	Keine
Standardmitglied von	Domänengäste Gäste
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, aber wir empfehlen es nicht.
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein

KRBTGT-Konto

Das krbtgt-Konto ist ein lokales Standardkonto, das als Dienstkonto für den KDC-Dienst (Key Distribution Center) fungiert. Dieses Konto kann nicht gelöscht werden, und der Konto Name kann nicht geändert werden. Das krbtgt-Konto kann in Active Directory nicht aktiviert werden.

KRBTGT ist auch der Name des Sicherheitsprinzips, der vom KDC für eine Windows Server-Domäne verwendet wird, wie in RFC 4120 angegeben. Das krbtgt-Konto ist die Entität für den krbtgt-Sicherheitsprinzipal und wird automatisch erstellt, wenn eine neue Domäne erstellt wird.

Die Windows Server-Kerberos-Authentifizierung wird durch die Verwendung eines speziellen Kerberos-Ticket genehmigenden Tickets (TGT) erreicht, das mit einem symmetrischen Schlüssel verschlüsselt wurde. Dieser Schlüssel wird vom Kennwort des Servers oder Diensts abgeleitet, auf den Access angefordert wird. Das TGT-Kennwort des krbtgt-Kontos ist nur vom Kerberos-Dienst bekannt. Damit Sie ein Sitzungsticket anfordern können, muss das TGT dem KDC angezeigt werden. Der TGT wird vom KDC für den Kerberos-Client ausgestellt.

Überlegungen zur krbtgt-Kontowartung

Dem krbtgt-und Trust-Konto wird automatisch ein sicheres Kennwort zugewiesen. Wie bei allen privilegierten Dienstkontoen sollten Organisationen diese Kennwörter regelmäßig ändern. Das Kennwort für das KDC-Konto wird verwendet, um einen geheimen Schlüssel zum Verschlüsseln und Entschlüsseln der ausgestellten TGT-Anforderungen abzuleiten. Das Kennwort für ein Domänen Vertrauensstellungs Konto wird verwendet, um einen zwischen Bereichs Schlüssel zum Verschlüsseln von Referral Tickets abzuleiten.

Für das Zurücksetzen des Kennworts müssen Sie entweder ein Mitglied der Gruppe der Domänenadministratoren sein oder an die entsprechende Autorität delegiert worden sein. Darüber hinaus müssen Sie Mitglied der lokalen Gruppe Administratoren sein, oder Sie müssen an die entsprechende Autorität delegiert worden sein.

Nachdem Sie das krbtgt-Kennwort zurückgesetzt haben, stellen Sie sicher, dass die Ereignis-ID 9 in der (Kerberos) Key-Distribution-Center-Ereignisquelle in das System Ereignisprotokoll geschrieben wird.

Überlegungen zur Sicherheit

Es ist auch eine bewährte Methode, das Kennwort für das krbtgt-Konto zurückzusetzen, um sicherzustellen, dass ein neu wiederhergestellter Domänencontroller nicht mit einem kompromittierten Domänencontroller repliziert wird. In diesem Fall können Sie in einer umfassenden Gesamtstrukturwiederherstellung, die über mehrere Speicherorte verteilt ist, nicht garantieren, dass alle Domänencontroller heruntergefahren werden, und wenn Sie heruntergefahren werden, können Sie nicht mehr neu gestartet werden, bevor alle entsprechenden Wiederherstellungsschritte durchgeführt wurden. . Nachdem Sie das krbtgt-Konto zurückgesetzt haben, kann ein

anderer Domänencontroller dieses Kontokennwort nicht mithilfe eines alten Kennworts replizieren.

Eine in der Organisation vermutete Domänen Gefährdung des krbtgt-Kontos sollte die Verwendung von professionellen Incident Response Services in Betracht ziehen. Die Auswirkungen auf die Wiederherstellung des Besitzers des Kontos sind domänenweit, und es sollten arbeitsintensive Aktivitäten im Rahmen eines größeren Wiederherstellungs Aufwands unternommen werden.

Das krbtgt-Kennwort ist der Schlüssel, von dem alle Vertrauenswürdigkeit in Kerberos-Ketten bis zu. Das Zurücksetzen des krbtgt-Kennworts ähnelt dem Erneuern des Zertifikats der Stammzertifizierungsstelle mit einem neuen Schlüssel und dem alten Schlüssel unmittelbar nicht, was dazu führt, dass fast alle nachfolgenden Kerberos-Vorgänge betroffen sind.

Für alle Kontotypen (Benutzer, Computer und Dienste)

- Alle TGTs, die bereits ausgestellt und verteilt sind, sind ungültig, da Sie von der DCS abgelehnt werden. Diese Tickets sind mit dem krbtgt verschlüsselt, sodass Sie von jedem DC überprüft werden können. Wenn sich das Kennwort ändert, werden die Tickets ungültig.
- Alle zurzeit authentifizierten Sitzungen, die sich bei Benutzern angemeldet haben (basierend auf Ihren Dienstitickets), an eine Ressource (wie Dateifreigabe, SharePoint-Website oder Exchange-Server) sind gut, bis das Service Ticket erneut authentifiziert werden muss.
- NTLM-authentifizierte Verbindungen sind nicht betroffen

Da es unmöglich ist, die spezifischen Fehler vorherzusagen, die für einen bestimmten Benutzer in einer Produktionsumgebung auftreten werden, müssen Sie davon ausgehen, dass alle Computer und Benutzer davon betroffen sind.

Wichtig

Das Neustarten eines Computers ist die einzige zuverlässige Möglichkeit zum Wiederherstellen von Funktionen, da dies dazu führen kann, dass sich das Computerkonto und die Benutzerkonten wieder anmelden. Bei der erneuten Anmeldung werden neue TGTs angefordert, die mit dem neuen krbtgt gültig sind, wobei alle krbtgt-bezogenen Betriebsprobleme auf diesem Computer behoben werden.

Informationen dazu, wie Sie die Risiken reduzieren können, die mit einem potenziell gefährdeten krbtgt-Konto verbunden sind, finden Sie unter [Kenn Wort Rücksetz Skripts für krbtgt-Konten, die jetzt für Kunden verfügbar sind](#).

Schreibgeschützte Domänencontroller und das krbtgt-Konto

Windows Server 2008 hat den schreibgeschützten Domänencontroller (RODC) eingeführt. Der RODC wird als Schlüssel Verteilungs Center (Key Distribution Center, KDC) für die Zweigstelle angekündigt. Der RODC verwendet ein anderes krbtgt-Konto und-Kennwort als das KDC auf einem beschreibbaren Domänencontroller, wenn es TGT-Anforderungen (Ticket-Granting Ticket) signiert oder verschlüsselt. Nachdem ein Konto erfolgreich authentifiziert wurde, ermittelt der RODC, ob die Anmeldeinformationen eines Benutzers oder die Anmeldeinformationen eines Computers vom schreibbaren Domänencontroller mithilfe der Kennwortreplikationsrichtlinie auf den RODC repliziert werden können.

Nachdem die Anmeldeinformationen auf dem RODC zwischengespeichert wurden, kann der RODC die Anmeldeanforderungen des Benutzers akzeptieren, bis die Anmeldeinformationen geändert wurden. Wenn ein TGT mit dem krbtgt-Konto des RODC signiert ist, erkennt der RODC, dass es eine zwischengespeicherte Kopie der Anmeldeinformationen hat. Wenn ein anderer Domänencontroller das TGT signiert, leitet der RODC Anforderungen an einen beschreibbaren Domänencontroller weiter.

KRBGT-Kontoattribute

Details zu den Attributen des krbtgt-Kontos finden Sie in der folgenden Tabelle.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-502
Typ	Benutzer
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Gruppe "Domänenbenutzer". Beachten Sie, dass die primäre Gruppen-ID aller Benutzerkonten Domänenbenutzer ist.
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, aber wir empfehlen es nicht.
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein

Einstellungen für lokale Standardkonten in Active Directory

Jedes standardmäßige lokale Konto in Active Directory verfügt über eine Reihe von Kontoeinstellungen, die Sie verwenden können, um Kennwordeinstellungen und sicherheitsspezifische Informationen zu konfigurieren, wie in der folgenden Tabelle beschrieben.

Einstellungen für lokale Standardkonten in Active Directory

KONTOEINSTELLUNGEN	BESCHREIBUNG
Der Benutzer muss bei der nächsten Anmeldung das Kennwort ändern.	Erzwingt die Änderung eines Kennworts, wenn sich der Benutzer das nächste Mal beim Netzwerk anmeldet. Verwenden Sie diese Option, wenn Sie sicherstellen möchten, dass der Benutzer die einzige Person ist, die sein Kennwort kennt.
Der Benutzer kann das Kennwort nicht ändern	Verhindert, dass Benutzer das Kennwort ändern. Verwenden Sie diese Option, wenn Sie die Kontrolle über ein Benutzerkonto behalten möchten, beispielsweise für ein Gast-oder ein temporäres Konto.
Kennwort läuft nie ab	Verhindert, dass ein Benutzerkennwort abläuft. Es wird empfohlen, diese Option für Dienstkonto zu aktivieren und sichere Kennwörter zu verwenden.

KONTOEINSTELLUNGEN	BESCHREIBUNG
Kennwörter mit umkehrbarer Verschlüsselung speichern	<p>Bietet Unterstützung für Anwendungen, die Protokolle verwenden, die Kenntnisse der Klartext-Form des Benutzerkennworts für Authentifizierungszwecke erfordern.</p> <p>Diese Option ist erforderlich, wenn CHAP (Challenge Handshake Authentication Protocol) in Internetauthentifizierungsdienste (IAS) und bei Verwendung der Digestauthentifizierung in Internetinformationsdienste (IIS) verwendet wird.</p>
Konto ist deaktiviert	<p>Verhindert, dass sich der Benutzer mit dem ausgewählten Konto anmeldet. Als Administrator können Sie deaktivierte Konten als Vorlagen für allgemeine Benutzerkonten verwenden.</p>
Für die interaktive Anmeldung ist eine Smartcard erforderlich	<p>Erfordert, dass ein Benutzer über eine Smartcard verfügt, um sich interaktiv beim Netzwerk anmelden zu können. Der Benutzer muss auch über einen Smartcard-Leser verfügen, der an seinen Computer angeschlossen ist, und eine gültige persönliche Identifikationsnummer (PIN) für die Smartcard.</p> <p>Wenn dieses Attribut auf das Konto angewendet wird, sieht der Effekt wie folgt aus:</p> <ul style="list-style-type: none"> • Das Attribut beschränkt erst Authentifizierung für interaktive Anmeldung und Remote Desktop Anmeldung. Wenn für die interaktive oder Remote Desktop Anmeldung eine nachfolgende Netzwerkanmeldung erforderlich ist, beispielsweise mit einer Domänenanmeldeinformation, wird ein vom Domänencontroller bereitgestellter NT-Hash verwendet, um den Smartcard-Authentifizierungsprozess abzuschließen. • Jedes Mal, wenn das Attribut für ein Konto aktiviert ist, wird der aktuelle Kennwort-Hashwert des Kontos durch eine Zufallszahl vom 128-Bit ersetzt. Dadurch wird die Verwendung zuvor konfigurierter Kennwörter für das Konto ungültig. Danach ändert sich der Wert erst, wenn ein neues Kennwort festgesetzt oder das Attribut deaktiviert und wieder aktiviert wurde. • Konten mit diesem Attribut können nicht zum Starten von Diensten oder zum Ausführen geplanter Aufgaben verwendet werden.

KONTOEINSTELLUNGEN	BESCHREIBUNG
Konto ist für Delegierungszwecke vertrauenswürdig	Ermöglicht es einem Dienst, der unter diesem Konto ausgeführt wird, Vorgänge im Auftrag anderer Benutzerkonten im Netzwerk durchzuführen. Ein Dienst, der unter einem Benutzerkonto (auch als Dienstkonto bezeichnet) ausgeführt wird, das für die Delegierung als vertrauenswürdig eingestuft wird, kann einen Client für den Zugriff auf Ressourcen entweder auf dem Computer, auf dem der Dienst ausgeführt wird, oder auf anderen Computern anweisen. In einer Gesamtstruktur, die auf die Funktionsebene Windows Server 2003 festgelegt ist, wird diese Einstellung auf der Registerkarte Delegierung gefunden. Sie ist nur für Konten verfügbar, denen Dienstprinzipalnamen (Service Principal Names, SPNs) zugewiesen wurden, die mithilfe des Befehls Setspn in den Windows-Support Tools festgelegt werden. Diese Einstellung ist sicherheitsrelevant und sollte vorsichtig zugewiesen werden.
Das Konto ist vertraulich und kann nicht delegiert werden	Bietet die Kontrolle über ein Benutzerkonto, beispielsweise für ein Gastkonto oder ein temporäres Konto. Diese Option kann verwendet werden, wenn dieses Konto nicht für die Delegierung durch ein anderes Konto zugewiesen werden kann.
Verwenden des Verschlüsselungstyps für dieses Konto	<p>Bietet Unterstützung für den Data Encryption Standard (des). Des unterstützt mehrere Verschlüsselungsebenen, einschließlich Microsoft-Punkt-zu-Punkt-Verschlüsselung (MPPE)-Standard (40-Bit und 56-Bit), MPPE-Standard (56-Bit), MPPE Strong (128-Bit), Internet Protocol Security (IPSec) des (40-Bit), IPSec 56-Bit des und IPSec Triple DES (3DES).</p> <div> <p>Hinweis:</p> <p>DES ist in Windows Server-Betriebssystemen ab Windows Server 2008 R2 oder Windows-Clientbetriebssystemen ab Windows 7 nicht standardmäßig aktiviert. Bei diesen Betriebssystemen werden die Verschlüsselungs Pakete des-CBC-MD5-oder des-CBC-CRC-Computers standardmäßig nicht verwendet. Wenn für die Umgebung des erforderlich ist, kann sich diese Einstellung auf die Kompatibilität mit Clientcomputern oder Diensten und Anwendungen in Ihrer Umgebung auswirken. Weitere Informationen finden Sie unter Hunting Down des, um Kerberos sicher bereitzustellen.</p> </div>
Kerberos-Vorauthentifizierung nicht erforderlich	Bietet Unterstützung für alternative Implementierungen des Kerberos-Protokolls. Da die Vorauthentifizierung zusätzliche Sicherheit bietet, sollten Sie beim Aktivieren dieser Option Vorsicht walten lassen. Beachten Sie, dass Domänencontroller, auf denen Windows 2000 oder Windows Server 2003 ausgeführt wird, andere Mechanismen zum Synchronisieren von Zeit verwenden können.

Verwalten von lokalen Standardkonten in Active Directory

Nachdem die lokalen Standardkonten installiert wurden, befinden sich diese Konten im Container Benutzer in Active Directory-Benutzer und-Computer. Standardmäßige lokale Konten können mithilfe der Microsoft Management Console (MMC) Active Directory-Benutzer und-Computer und mithilfe von Befehlszeilentools erstellt, deaktiviert, zurückgesetzt und gelöscht werden.

Sie können Active Directory-Benutzer und-Computer verwenden, um Rechte und Berechtigungen für einen bestimmten lokalen Domänencontroller und nur für diesen Domänencontroller zuzuweisen, um die Möglichkeit für lokale Benutzer und Gruppen zum Ausführen bestimmter Aktionen zu begrenzen. Ein Recht ermächtigt einen Benutzer, bestimmte Aktionen auf einem Computer durchzuführen, beispielsweise das Sichern von Dateien und Ordnern oder das Herunterfahren eines Computers. Im Gegensatz dazu ist eine Zugriffsberechtigung eine Regel, die einem Objekt zugeordnet ist, in der Regel eine Datei, ein Ordner oder ein Drucker, die regelt, welche Benutzer auf welche Weise auf das Objekt zugreifen können.

Weitere Informationen zum Erstellen und Verwalten von lokalen Benutzerkonten in Active Directory finden Sie unter [Verwalten von lokalen Benutzern](#).

Sie können auch Active Directory-Benutzer und-Computer auf einem Domänencontroller verwenden, um auf Remotecomputer zu Zielen, die keine Domänencontroller im Netzwerk sind.

Sie können Empfehlungen von Microsoft für Domänencontroller Konfigurationen erhalten, die Sie mithilfe des Security Compliance Manager (SCM)-Tools verteilen können. Weitere Informationen finden Sie unter [Microsoft Security Compliance Manager](#).

Einige der lokalen Standardbenutzerkonten sind durch einen Hintergrundprozess geschützt, der in regelmäßigen Abständen eine bestimmte Sicherheitsbeschreibung überprüft und anwendet, bei der es sich um eine Datenstruktur handelt, die Sicherheitsinformationen enthält, die einem geschützten Objekt zugeordnet sind. Diese Sicherheitsbeschreibung ist im AdminSDHolder-Objekt vorhanden.

Das bedeutet, wenn Sie die Berechtigungen für eine Dienstadministratorgruppe oder für eines der Mitgliedskonten ändern möchten, müssen Sie auch die Sicherheitsbeschreibung für das AdminSDHolder-Objekt ändern. Dieser Ansatz stellt sicher, dass die Berechtigungen konsistent angewendet werden. Seien Sie vorsichtig, wenn Sie diese Änderungen vornehmen, da sich diese Aktion auch auf die Standardeinstellungen auswirken kann, die auf alle geschützten Administratorkonten angewendet werden.

Einschränken und Schützen vertraulicher Domänenkonten

Wenn Sie Domänenkonten in ihrer Domänenumgebung einschränken und schützen möchten, müssen Sie den folgenden bewährten Methodenansatz übernehmen und implementieren:

- Beschränken Sie die Mitgliedschaft strikt auf die Gruppen Administratoren, Domänenadministratoren und Unternehmensadministratoren.
- Kontrollieren Sie strikt, wo und wie Domänenkonten verwendet werden.

Mitgliederkonten in den Gruppen Administratoren, Domänenadministratoren und Unternehmensadministratoren in einer Domäne oder Gesamtstruktur sind höchstwertige Ziele für böswillige Benutzer. Es ist eine bewährte Methode, die Mitgliedschaft auf diese Administratorgruppen strikt auf die kleinste Anzahl von Konten zu begrenzen, um eine Gefährdung zu begrenzen. Wenn Sie die Mitgliedschaft in diesen Gruppen einschränken, verringert sich die Möglichkeit, dass ein Administrator diese Anmeldeinformationen versehentlich missbraucht und eine Sicherheitsanfälligkeit schafft, die böswillige Benutzer ausnutzen können.

Darüber hinaus empfiehlt es sich, stringent zu steuern, wo und wie vertrauliche Domänenkonten verwendet werden. Beschränken Sie die Verwendung von Domänenadministratorkonten und anderen Administratorkonten, um zu verhindern, dass Sie für die Anmeldung bei Verwaltungssystemen und Workstations verwendet werden, die auf der gleichen Ebene wie die verwalteten Systeme gesichert sind. Wenn Administratorkonten auf diese Weise

nicht eingeschränkt werden, bietet jede Arbeitsstation, von der ein Domänenadministrator anmeldet, einen anderen Speicherort, den böswillige Benutzer ausnutzen können.

Die Implementierung dieser bewährten Methoden ist in die folgenden Aufgaben aufgeteilt:

- [Trennen von Administratorkonten von Benutzerkonten](#)
- [Erstellen dedizierter Workstation-Hosts für Administratoren](#)
- [Einschränken des Administrator Anmeldezugriffs auf Server und Workstations](#)
- [Deaktivieren der Konto Delegierungsberechtigung für Administratorkonten](#)

Beachten Sie, dass für Fälle, in denen Integrationsherausforderungen mit der Domänenumgebung erwartet werden, jede Aufgabe entsprechend den Anforderungen für eine minimale, bessere und optimale Implementierung beschrieben wird. Wie bei allen bedeutenden Änderungen an einer Produktionsumgebung sollten Sie sicherstellen, dass Sie diese Änderungen gründlich testen, bevor Sie sie implementieren und bereitstellen. Führen Sie dann die Bereitstellung auf eine Weise aus, die ein Rollback der Änderung ermöglicht, falls technische Probleme auftreten.

Trennen von Administratorkonten von Benutzerkonten

Schränken Sie Domänenadministratorkonten und andere vertrauliche Konten ein, um zu verhindern, dass Sie zum Anmelden bei niedrigeren Trust-Servern und-Workstations verwendet werden. Sie können Administratorkonten einschränken und schützen, indem Sie die Administratorkonten von Standardbenutzerkonten trennen, indem Sie administrative Aufgaben von anderen Aufgaben trennen und die Verwendung dieser Konten einschränken. Erstellen Sie dedizierte Konten für Verwaltungspersonal, die Administratoranmeldeinformationen benötigen, um bestimmte administrative Aufgaben auszuführen, und erstellen Sie dann getrennte Konten für andere Standardbenutzer Aufgaben entsprechend den folgenden Richtlinien:

- **Privilegiertes Konto.** Zuweisen von Administratorkonten, um nur die folgenden administrativen Aufgaben auszuführen:
 - **Minimaler Wert.** Erstellen Sie separate Konten für Domänenadministratoren, Unternehmensadministratoren oder das Äquivalent mit den entsprechenden Administratorrechten in der Domäne oder Gesamtstruktur. Verwenden Sie Konten, denen nur vertrauliche Administratorrechte gewährt wurden, um Domänendaten und Domänencontroller zu verwalten.
 - **Besser.** Erstellen Sie separate Konten für Administratoren, die eingeschränkte Administratorrechte haben, beispielsweise Konten für Workstation-Administratoren und Konten mit Benutzerrechten für festgelegte Active Directory-Organisationseinheiten (Organizational Units, OUs).
 - **Ideal.** Erstellen Sie mehrere getrennte Konten für einen Administrator, der über eine Vielzahl von Aufgaben verfügt, die unterschiedliche Vertrauensstufen erfordern. Richten Sie jedes Administratorkonto mit erheblich unterschiedlichen Benutzerrechten ein, beispielsweise für die Verwaltung von Workstations, die Serververwaltung und die Domänenverwaltung, damit sich der Administrator bei bestimmten Workstations, Servern und Domänencontrollern anmelden kann, die auf der Grundlage ausschließlich auf seine Aufgaben Zuständigkeiten.
- **Standard Benutzerkonto.** Erteilen Sie Standardbenutzerrechte für Standardbenutzer Aufgaben wie e-Mail, Web-Browsing und die Verwendung von Branchen Anwendungen. Diesen Konten sollten keine Administratorrechte gewährt werden.

Wichtig

Stellen Sie sicher, dass vertrauliche Administratorkonten nicht auf e-Mails zugreifen oder im Internet surfen können, wie im folgenden Abschnitt beschrieben.

Erstellen dedizierter Workstation-Hosts ohne Internet-und e-Mail-Zugriff

Administratoren müssen Aufgaben verwalten, die vertrauliche Administratorrechte von einer dedizierten

Arbeitsstation erfordern, weil Sie keinen einfachen physischen Zugriff auf die Server haben. Eine Workstation, die mit dem Internet verbunden ist und Zugriff auf e-Mail- und Webbrowsing hat, wird durch Phishing, Herunterladen und andere Arten von Internet-Angriffen regelmäßig gefährdet. Aufgrund dieser Bedrohungen empfiehlt es sich, diese Administratoren auf Workstations einzurichten, die nur für administrative Aufgaben vorgesehen sind, und keinen Zugriff auf das Internet, einschließlich e-Mail und Web-Browsing, zu ermöglichen. Weitere Informationen finden Sie unter [separate Administratorkonten von Benutzerkonten](#).

Hinweis:

Wenn sich die Administratoren in Ihrer Umgebung lokal an verwalteten Servern anmelden und alle Aufgaben ohne erhöhte Rechte oder Domänenrechte von Ihrer Arbeitsstation ausführen können, können Sie diese Aufgabe überspringen.

- **Minimaler Wert.** Erstellen Sie dedizierte administrative Workstations, und blockieren Sie den Internet-Zugriff auf diesen Workstations, einschließlich Web-Browsing und e-Mail. Verwenden Sie die folgenden Methoden zum Blockieren des Internet-Zugriffs:
 - Konfigurieren Sie Authentifizierungs-Grenz-Proxydienste, wenn diese bereitgestellt werden, um zu verhindern, dass Administratorkonten auf das Internet zugreifen.
 - Konfigurieren Sie die Begrenzungs-Firewall oder Proxydienste, um den Internet-Zugriff für die IP-Adressen zu verweigern, die dedizierten administrativen Arbeitsstationen zugewiesen sind.
 - Blockieren Sie den ausgehenden Zugriff auf die Grenz-Proxy-Server in der Windows-Firewall.

Die Anweisungen zum Erfüllen dieser Mindestanforderungen werden im folgenden Verfahren beschrieben.

- **Besser.** Gewähren Sie Administratoren keine Mitgliedschaft in der lokalen Administratorgruppe auf dem Computer, um zu verhindern, dass der Administrator diese Schutzmechanismen umgeht.
- **Ideal.** Schränken Sie Arbeitsstationen auf Netzwerkkonnektivität ein, mit Ausnahme der Domänencontroller und Server, die von den Administratorkonten verwaltet werden. Verwenden Sie alternativ die AppLocker-Anwendungssteuerungsrichtlinien, um alle Anwendungen mit Ausnahme des Betriebssystems und der genehmigten Verwaltungstools und Anwendungen zu begrenzen. Weitere Informationen zu AppLocker finden Sie unter [AppLocker](#).

Im folgenden Verfahren wird beschrieben, wie Sie den Internet-Zugriff blockieren, indem Sie ein Gruppenrichtlinienobjekt erstellen, das eine ungültige Proxyadresse auf administrativen Workstations konfiguriert. Diese Anweisungen gelten nur für Computer mit Internet Explorer und anderen Windows-Komponenten, die diese Proxyeinstellungen verwenden.

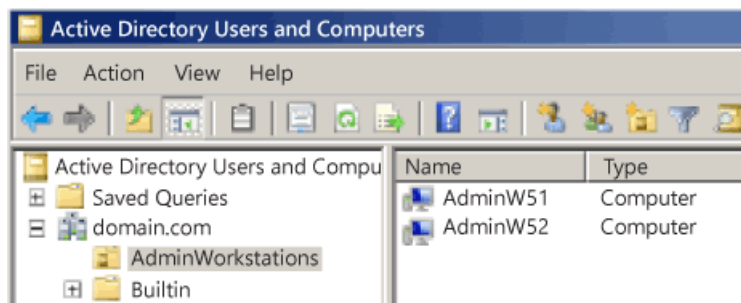
Hinweis:

In diesem Verfahren sind die Arbeitsstationen für Domänenadministratoren reserviert. Indem Sie einfach die Administratorkonten ändern, um Administratoren die Berechtigung zur lokalen Anmeldung zu erteilen, können Sie zusätzliche OUs erstellen, um Administratoren zu verwalten, die weniger Administratorrechte besitzen, um die im folgenden Verfahren beschriebenen Anweisungen zu verwenden.

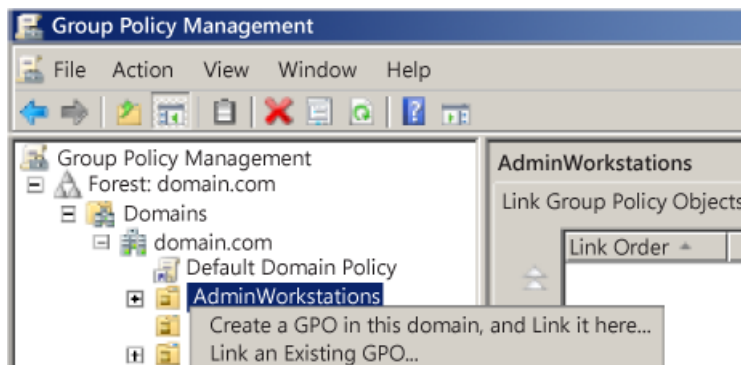
So installieren Sie administrative Arbeitsstationen in einer Domäne und blockieren Internet- und e-Mail-Zugriff (zumindest)

1. Öffnen Sie als Domänenadministrator auf einem Domänencontroller Active Directory-Benutzer und-Computer, und erstellen Sie eine neue Organisationseinheit für administrative Workstations.
2. Erstellen Sie Computerkonten für die neuen Workstations.

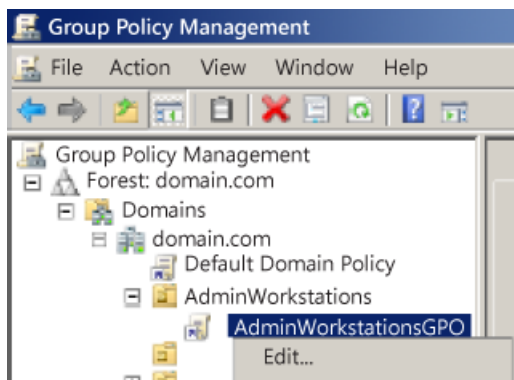
**** Hinweis: Möglicherweise müssen Sie Berechtigungen für die Teilnahme an Computern an die Domäne delegieren, wenn das Konto, das die Arbeitsstationen mit der Domäne verknüpft, diese noch nicht besitzt. Weitere Informationen finden Sie unter [Delegierung der Verwaltung in Active Directory](#).



3. Schließen Sie Active Directory-Benutzer und-Computer.
4. Starten Sie die **Gruppenrichtlinien-Verwaltungskontrolle (Group Policy Management Console, GPMC)**.
5. Klicken Sie mit der rechten Maustaste auf die > neue Organisationseinheit, und **Erstellen Sie ein GPO in dieser Domäne, und verknüpfen Sie es hier.**



6. Benennen Sie das Gruppenrichtlinien > Objekt, und klicken Sie auf **OK**.
7. Erweitern Sie das Gruppenrichtlinienobjekt, klicken Sie mit der rechten > Maustaste auf das neue Gruppenrichtlinienobjekt, und **Bearbeiten**Sie.

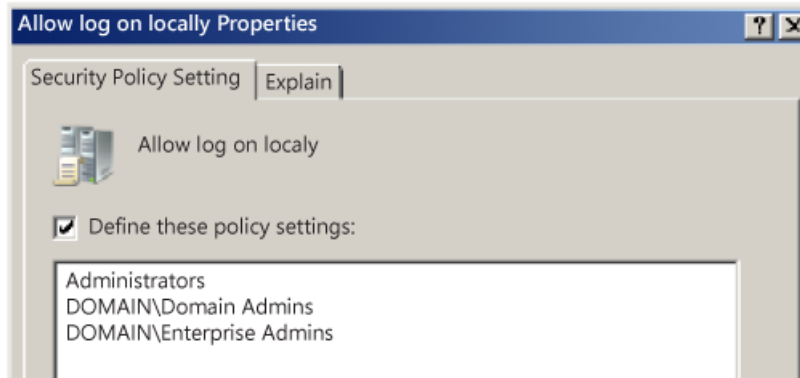


8. Konfigurieren Sie die Mitglieder von Konten, die sich lokal an diesen administrativen Workstations anmelden können, wie folgt:
 - a. Navigieren Sie zu den Richtlinien für Computer Configuration\Policies\Windows Settings\Local, und klicken Sie dann auf **Zuweisen von Benutzerrechten**.
 - b. Doppelklicken Sie auf **Lokal anmelden zulassen**, und aktivieren Sie dann das Kontrollkästchen **Diese Richtlinieneinstellungen definieren**.
 - c. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Unternehmensadministratoren**ein, und klicken Sie auf **OK**.
 - d. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Domänenadministratoren**ein, und klicken Sie auf **OK**.

Wichtig

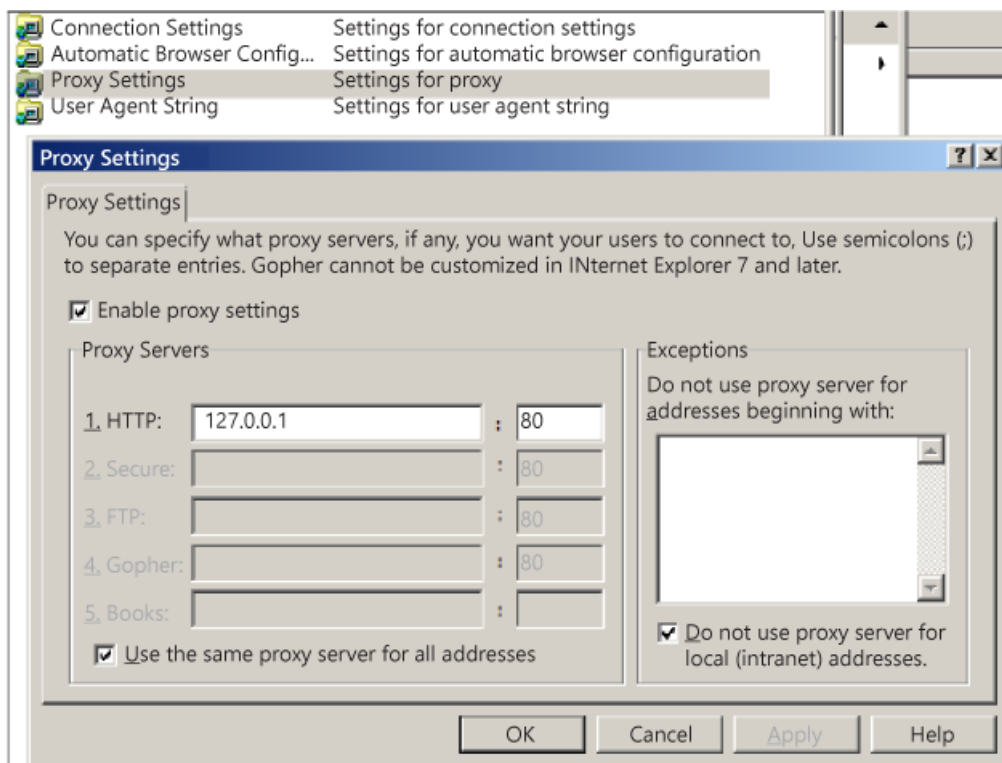
Bei diesen Anweisungen wird davon ausgegangen, dass die Arbeitsstation für Domänenadministratoren reserviert ist.

- e. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**, geben > Sie **Administratoren** ein, und klicken Sie auf **OK**.



9. Konfigurieren Sie die Proxykonfiguration:

- a. Navigieren Sie zu Benutzer Configuration\Policies\Windows Settings\Internet Explorer und > **Verbindung**.
- b. Doppelklicken Sie auf **Proxysteinstellungen**, aktivieren Sie das Kontrollkästchen **Proxysteinstellungen aktivieren**, geben Sie **127.0.0.1** (die IP-Adresse des Netzwerk-Loopbacks >) als Proxy Adresse ein, und klicken Sie auf **OK**.



10. Konfigurieren Sie den Loopbackverarbeitungsmodus so, dass die Einstellung für den Benutzergruppenrichtlinien Proxy wie folgt auf alle Benutzer auf dem Computer angewendet wird:

- a. Navigieren Sie zu Computer Configuration\Policies\Administrative Templates\System und > **Gruppenrichtlinien**.
- b. Doppelklicken Sie auf **Benutzergruppenrichtlinien-Loopback Richtlinien-Verarbeitungsmodus**, und > **aktiviert**.

- c. Wählen Sie **zusammenführungsmodus** und > **OK** aus.

11. Konfigurieren Sie Softwareupdates wie folgt:

- a. Navigieren Sie zu Computer Configuration\Policies\Administrative Templates\Windows-Komponenten, und klicken Sie dann auf **Windows Update**.
- b. Konfigurieren Sie die Windows Update-Einstellungen wie in der folgenden Tabelle beschrieben.

Windows Update-Einstellung	Konfiguration
Sofortiges Installieren von automatischen Updates zulassen	Aktiviert
Automatische Updates konfigurieren	Aktiviert 4 – Automatisches herunterladen und Planen der Installation 0 – jeden Tag 03:00
Aktivieren der Windows Update-Energieverwaltung zum automatischen aufwachen des Systems zum Installieren geplanter Updates	Aktiviert
Angabe des Intranets des Microsoft Update-Dienst Standorts	Aktiviert http://<WSUSServername> http://<WSUSServername> , <wobei> WSUSServername der DNS-Name oder die IP-Adresse der Windows Server Update Services (WSUS) in der Umgebung ist.
Suchhäufigkeit für automatische Updates	6 Stunden
Erneut zu einem Neustart für geplante Installationen auffordern	1 Minute
Verzögerter Neustart für geplante Installationen	5 Minuten

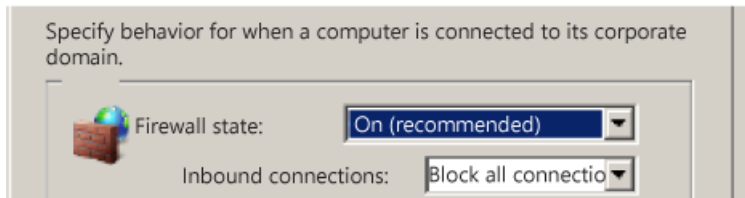
**** Hinweis in diesem Schritt wird davon ausgegangen, dass Windows Server Update Services (WSUS) in der Umgebung installiert und konfiguriert ist. Sie können diesen Schritt überspringen, wenn Sie ein anderes Tool zum Bereitstellen von Softwareupdates verwenden. Wenn der öffentliche Microsoft Windows Update-Dienst nur im Internet verwendet wird, erhalten diese administrativen Workstations keine Updates mehr.

12. Konfigurieren Sie die eingehende Firewall so, dass alle Verbindungen wie folgt blockiert werden:

- a. Klicken Sie mit der rechten Maustaste auf **Windows-Firewall mit erweiterten Sicherheits** **LDAP://Path** und > **Eigenschaften**.



- b. Stellen Sie für jedes Profil sicher, dass die Firewall aktiviert ist und dass eingehende Verbindungen so eingestellt sind, dass **alle Verbindungen blockiert** werden.



- c. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

13. Schließen Sie die Gruppenrichtlinien-Verwaltungskonsole.

14. Installieren Sie das Windows-Betriebssystem auf den Workstations, geben Sie jeder Workstation dieselben Namen wie die Computerkonten, die Ihnen zugewiesen sind, und fügen Sie Sie dann der Domäne bei.

Einschränken des Administrator Anmeldezugriffs auf Server und Workstations

Es empfiehlt sich, die Verwendung von vertraulichen Administratorkonten durch Administratoren zu beschränken, um sich bei Servern und Workstations mit geringer Vertrauenswürdigkeit anzumelden. Diese Einschränkung verhindert, dass Administratoren versehentlich das Risiko von Anmeldeinformationen Diebstahl erhöhen, indem Sie sich bei einem Computer mit niedriger Vertrauenswürdigkeit anmelden.

Wichtig

Stellen Sie sicher, dass Sie entweder über lokalen Zugriff auf den Domänencontroller verfügen oder dass Sie mindestens eine dedizierte administrative Workstation erstellt haben.

Beschränken Sie den Anmeldezugriff auf Server und Workstations mit niedrigeren Vertrauenswürdigkeit mithilfe der folgenden Richtlinien:

- **Minimaler Wert.** Einschränken des Anmeldezugriffs auf Server und Workstations durch Domänenadministratoren. Bevor Sie dieses Verfahren starten, müssen Sie alle OUs in der Domäne identifizieren, die Workstations und Server enthalten. Alle Computer in OUs, die nicht identifiziert werden, schränken Administratoren mit vertraulichen Konten nicht ein, dass Sie sich anmelden.
- **Besser.** Einschränken von Domänenadministratoren von nicht-Domänencontroller-Servern und-Workstations
- **Ideal.** Schränken Sie Serveradministratoren zusätzlich zu Domänenadministratoren von der Anmeldung bei Arbeitsstationen ein.

Hinweis:

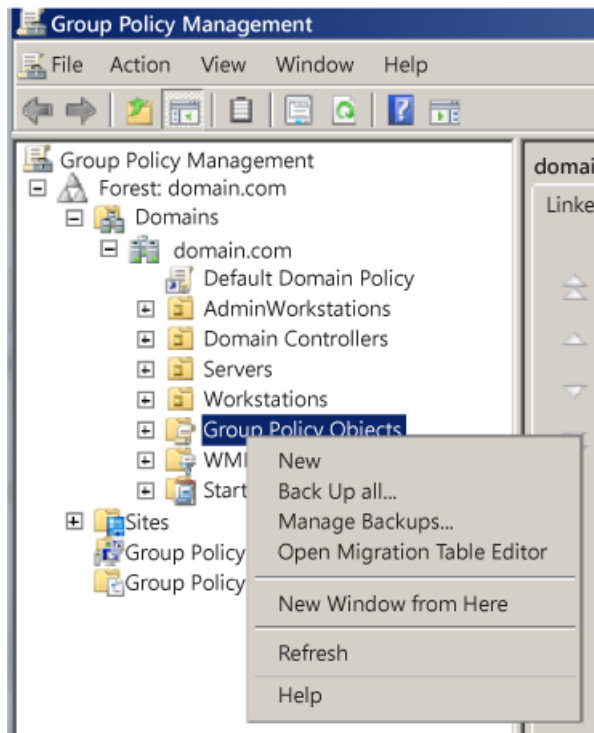
Führen Sie bei dieser Vorgehensweise keine Verknüpfung von Konten mit der Organisationseinheit durch, die Arbeitsstationen für Administratoren enthält, die nur Verwaltungsaufgaben ausführen, und keinen Internet-oder e-Mail-Zugriff bereitstellen. Weitere Informationen finden Sie unter [Erstellen dedizierter Workstation-Hosts für Administratoren](#).

So beschränken Sie Domänenadministratoren auf Workstations (mind.)

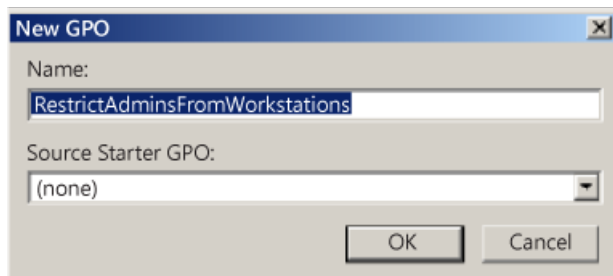
1. Öffnen Sie als Domänenadministrator die Gruppenrichtlinien-Verwaltungskonsole (Group Policy

Management Console, GPMC).

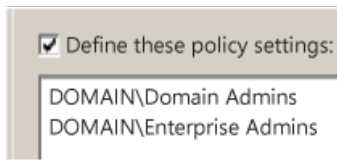
2. Öffnen Sie die **Gruppenrichtlinienverwaltung**, und erweitern * <Sie Gesamtstruktur> -\Domains\<- Domäne>, und erweitern Sie dann zu ****Gruppenrichtlinienobjekten***.
3. Klicken Sie mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** und > dann auf **neu**.



4. Benennen Sie im Dialogfeld **Neues Gruppenrichtlinien** Objekt das Gruppenrichtlinienobjekt, das die Anmeldung von Administratoren auf Workstations > einschränken soll, und klicken Sie auf **OK**.



5. Klicken Sie mit der rechten Maustaste auf **neues GPO**, und > **Bearbeiten** Sie.
6. Konfigurieren Sie Benutzerrechte, um die Anmeldung für Domänenadministratoren lokal zu verweigern.
7. Navigieren Sie zu Computer Configuration\Policies\Windows Settings\Local-Richtlinien, und klicken Sie dann auf **Benutzerrechtezuweisung**, und führen Sie die folgenden Aktionen aus:
 - a. Doppelklicken Sie auf **Anmeldung lokal ablehnen**, > und **definieren Sie diese Richtlinieneinstellungen**.
 - b. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**, klicken Sie auf **Durchsuchen**, > geben Sie **Unternehmensadministratoren** ein, und klicken Sie auf **OK**.
 - c. Klicken Sie auf **Benutzer oder Gruppe hinzufügen**, klicken Sie auf **Durchsuchen**, > geben Sie **Domänenadministratoren** ein, und klicken Sie auf **OK**.



Hinweis:

Sie können optional alle Gruppen hinzufügen, die Serveradministratoren enthalten, die Sie von der Anmeldung bei Workstations einschränken möchten.

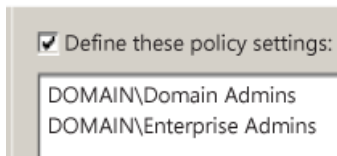
d. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

8. Konfigurieren Sie die Benutzerrechte zum Verweigern von Batch- und Dienst Anmelderechten für Domänenadministratoren wie folgt:

Hinweis:

Wenn Sie diesen Schritt ausführen, können Probleme mit Administratortasken auftreten, die als geplante Aufgaben oder Dienste mit Konten in der Gruppe der Domänenadministratoren ausgeführt werden. Die Praxis der Verwendung von Domänenadministratorkonten zum Ausführen von Diensten und Aufgaben auf Workstations führt zu einem erheblichen Risiko von Diebstahl von Anmeldeinformationen und sollte daher durch alternative Methoden zum Ausführen geplanter Aufgaben oder Dienste ersetzt werden.

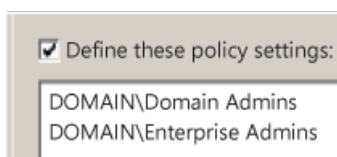
- a. Doppelklicken Sie auf **Anmeldung als Stapelverarbeitungsauftrag ablehnen**, > und **definieren Sie diese Richtlinieneinstellungen**.
- b. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Unternehmensadministratoren** ein, und klicken Sie auf **OK**.
- c. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Domänenadministratoren** ein, und klicken Sie auf **OK**.



Hinweis:

Sie können optional alle Gruppen hinzufügen, die Serveradministratoren enthalten, die Sie von der Anmeldung bei Workstations einschränken möchten.

- d. Doppelklicken Sie auf **Anmeldung als Dienst ablehnen**, und > **definieren Sie diese Richtlinieneinstellungen**.
- e. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Unternehmensadministratoren** ein, und klicken Sie auf **OK**.
- f. Klicken Sie auf **Benutzer hinzufügen oder Gruppe** > **Durchsuchen**, geben Sie > **Domänenadministratoren** ein, und klicken Sie auf **OK**.



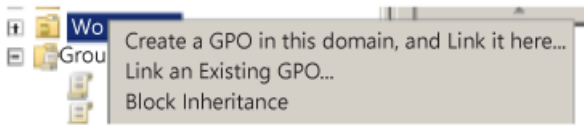
Hinweis:

Sie können optional alle Gruppen hinzufügen, die Serveradministratoren enthalten, die Sie von der Anmeldung bei Workstations einschränken möchten.

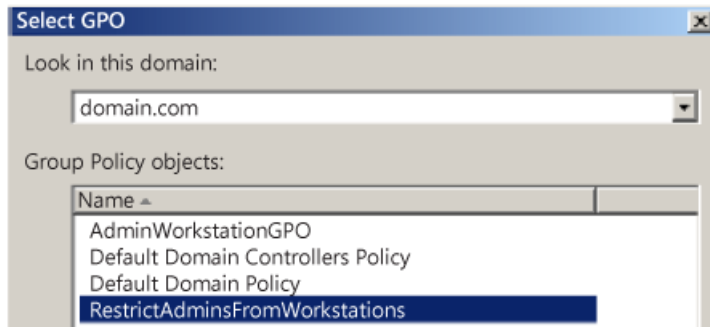
9. Verknüpfen Sie das Gruppenrichtlinienobjekt mit der ersten Arbeitsstations Organisationseinheit.

Navigieren * <Sie zum Pfad>der \Domains*<-Domänen> \OU, und klicken Sie dann auf:

- a. Klicken Sie mit der rechten Maustaste auf die Organisations > Einheit Workstation, und verknüpfen Sie dann **ein vorhandenes Gruppenrichtlinienobjekt**.



- b. Wählen Sie das soeben erstellte Gruppenrichtlinienobjekt aus > , und klicken Sie auf **OK**.



10. Testen Sie die Funktionalität von Enterprise-Anwendungen auf Workstations in der ersten OU, und beheben Sie alle Probleme, die durch die neue Richtlinie verursacht werden.
11. Verknüpfen Sie alle anderen OUs, die Workstations enthalten.

Erstellen Sie jedoch keinen Link zur OU für administrative Workstations, wenn Sie für administrative Workstations erstellt wurde, die nur für Verwaltungsaufgaben vorgesehen sind und die keinen Internet-oder e-Mail-Zugriff aufweisen. Weitere Informationen finden Sie unter [Erstellen dedizierter Workstation-Hosts für Administratoren](#).

Wichtig

Wenn Sie diese Lösung später erweitern, verweigern Sie die Anmelderechte für die Gruppe "

Domänenbenutzer". Die Gruppe "**Domänenbenutzer**" umfasst alle Benutzerkonten in der Domäne, einschließlich Benutzern, Domänenadministratoren und Unternehmensadministratoren.

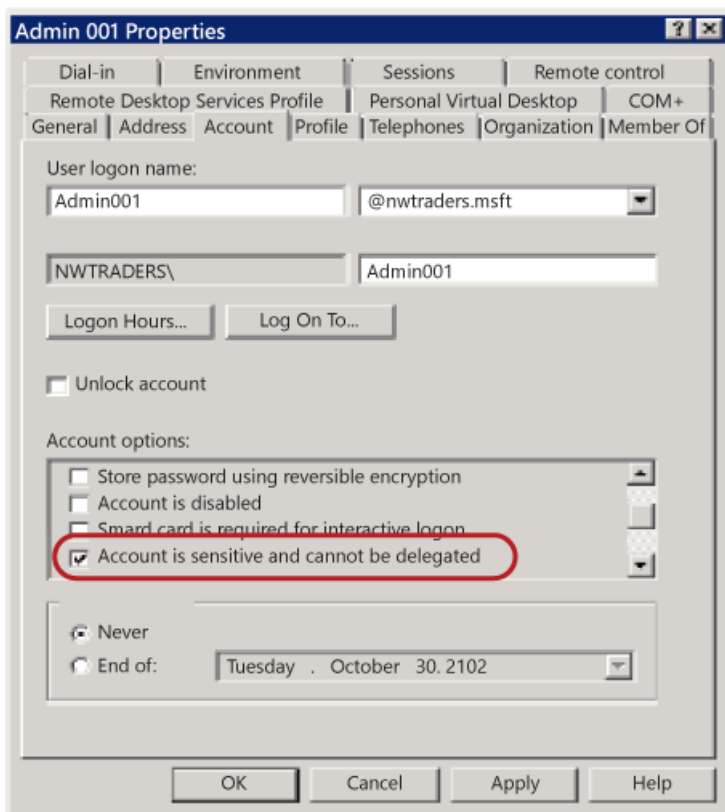
Deaktivieren der Konto Delegierungsberechtigung für vertrauliche Administratorkonten

Obwohl Benutzerkonten nicht standardmäßig für die Delegierung markiert sind, können Konten in einer Active Directory-Domäne für die Delegierung als vertrauenswürdig eingestuft werden. Dies bedeutet, dass ein Dienst oder ein Computer, der für die Delegierung als vertrauenswürdig eingestuft wird, die Identität eines Kontos versichern kann, das sich bei ihm authentifiziert, um auf andere Ressourcen im gesamten Netzwerk zuzugreifen.

Für vertrauliche Konten, beispielsweise für Mitglieder von Administratoren, Domänenadministratoren oder Gruppen für Unternehmensadministratoren in Active Directory, kann die Delegierung ein erhebliches Risiko der Rechteeskalation darstellen. Wenn beispielsweise ein Konto in der Gruppe "Domänen-Admins" verwendet wird, um sich bei einem kompromittierten Mitgliedsserver anzumeldet, der für die Delegierung als vertrauenswürdig eingestuft wird, kann dieser Server den Zugriff auf Ressourcen im Kontext des Domänenadministratorkontos anfordern und die Gefährdung dieses Mitglieds eskalieren. Server zu einer Domänen Kompromittierung.

Es wird empfohlen, die Benutzerobjekte für alle vertraulichen Konten in Active Directory zu konfigurieren, indem Sie das Kontrollkästchen **Konto ist vertraulich und kann nicht delegiert werden** unter **Kontooptionen** aktivieren, um zu verhindern, dass diese Konten delegiert werden. Weitere Informationen finden Sie unter [Festlegen von lokalen Standardkonten in Active Directory](#).

Testen Sie wie bei jeder Konfigurationsänderung diese Einstellung vollständig, um sicherzustellen, dass Sie ordnungsgemäß ausgeführt wird, bevor Sie Sie implementieren.



Sichern und Verwalten von Domänencontrollern

Es ist eine bewährte Methode, Einschränkungen für die Domänencontroller in Ihrer Umgebung strikt durchzusetzen. Dadurch wird sichergestellt, dass die Domänencontroller:

1. Nur erforderliche Software ausführen
2. Die erforderliche Software wird regelmäßig aktualisiert
3. Mit den entsprechenden Sicherheitseinstellungen konfiguriert sind

Ein Aspekt beim Sichern und Verwalten von Domänencontrollern besteht darin, sicherzustellen, dass die lokalen Standardbenutzerkonten vollständig geschützt sind. Es ist von grundlegender Wichtigkeit, alle vertraulichen Domänenkonten zu beschränken und zu schützen, wie in den vorherigen Abschnitten beschrieben.

Da Domänencontroller Anmeldekennwort-Hashwerte aller Konten in der Domäne speichern, handelt es sich um höchstwertige Ziele für böswillige Benutzer. Wenn Domänencontroller mithilfe von Einschränkungen, die streng erzwungen werden, nicht gut verwaltet und gesichert werden, können Sie von böswilligen Benutzern beeinträchtigt werden. Ein böswilliger Benutzer könnte beispielsweise vertrauliche Domänenadministrator Anmeldeinformationen von einem Domänencontroller stehlen und diese dann zum angreifen der Domäne und der Gesamtstruktur verwenden.

Darüber hinaus bieten installierte Anwendungen und Verwaltungs-Agents auf Domänencontrollern möglicherweise einen Pfad für Eskalations Rechte, die böswillige Benutzer verwenden können, um den Verwaltungsdienst oder Administratoren dieses Diensts zu gefährden. Die Verwaltungstools und-Dienste, die Ihre Organisation zum Verwalten von Domänencontrollern und deren Administratoren verwendet, sind für die Sicherheit der Domänencontroller und der Domänenadministrator Konten gleichermaßen wichtig. Stellen Sie sicher, dass diese Dienste und Administratoren mit gleichem Aufwand vollständig abgesichert sind.

Weitere Informationen:

- [Sicherheitsprinzipale](#)
- [Übersicht über die Zugriffssteuerung](#)

Microsoft-Konten

12.09.2019 • 9 minutes to read

Betrifft

- Windows10

In diesem Thema für IT-Experten wird erläutert, wie ein Microsoft-Konto die Sicherheit und den Datenschutz für Benutzer verbessert und wie Sie diesen Verbraucher Kontotyp in Ihrer Organisation verwalten können.

Microsoft-Websites,-Dienste und-Eigenschaften sowie Computer, auf denen Windows 10 ausgeführt wird, können ein Microsoft-Konto verwenden, um einen Benutzer zu identifizieren. Microsoft-Konto wurde zuvor als Windows Live stürzen-ID bezeichnet. Sie hat benutzerdefinierte Geheimnisse und besteht aus einer eindeutigen e-Mail-Adresse und einem Kennwort.

Wenn sich ein Benutzer mit einem Microsoft-Konto anmeldet, wird das Gerät mit Cloud Services verbunden. Viele Einstellungen, Einstellungen und Apps des Benutzers können auf allen Geräten freigegeben werden.

Funktionsweise eines Microsoft-Kontos

Mit dem Microsoft-Konto können sich Benutzer mit einem einzigen Satz von Anmeldeinformationen bei Websites anmelden, die diesen Dienst unterstützen. Die Anmeldeinformationen der Benutzer werden von einem Microsoft-Konto Authentifizierungsserver überprüft, der einer Website zugeordnet ist. Der Microsoft Store ist ein Beispiel für diese Zuordnung. Wenn sich neue Benutzer bei Websites anmelden, die für die Verwendung von Microsoft-Konten aktiviert sind, werden Sie an den nächstgelegenen Authentifizierungsserver weitergeleitet, in dem ein Benutzername und ein Kennwort abgefragt werden. Windows verwendet den SChannel Security Support-Anbieter, um eine TLS/SSL-Verbindung (Transport Level Security/Secure Sockets Layer) für diese Funktion zu öffnen. Benutzer haben dann die Möglichkeit, den Anmelde Informations-Manager zum Speichern Ihrer Anmeldeinformationen zu verwenden.

Wenn sich Benutzer bei Websites anmelden, die für die Verwendung eines Microsoft-Kontos aktiviert sind, wird auf ihren Computern ein Zeit Beschränkungs Cookie installiert, das ein Triple des-verschlüsselte-ID-Tag enthält. Dieser verschlüsselte ID-Tag wurde zwischen dem Authentifizierungsserver und der Website vereinbart. Dieses ID-Tag wird an die Website gesendet, und auf dem Computer des Benutzers wird eine andere zeitbegrenzte verschlüsselte HTTP-Cookie auf der Website gespeichert. Wenn diese Cookies gültig sind, müssen Benutzer keinen Benutzernamen und kein Kennwort angeben. Wenn ein Benutzer sich aktiv von seinem Microsoft-Konto abmeldet, werden diese Cookies entfernt.

Wichtige Funktionen des lokalen Windows-Kontos wurden nicht entfernt, und Sie können in verwalteten Umgebungen weiterhin verwendet werden.

Erstellen von Microsoft-Konten

Um Betrug zu verhindern, überprüft das Microsoft-System die IP-Adresse, wenn ein Benutzer ein Konto erstellt. Ein Benutzer, der versucht, mehrere Microsoft-Konten mit der gleichen IP-Adresse zu erstellen, wird angehalten.

Microsoft-Konten sind nicht für die Erstellung in Batches vorgesehen, beispielsweise für eine Gruppe von Domänenbenutzern innerhalb Ihres Unternehmens.

Es gibt zwei Methoden zum Erstellen eines Microsoft-Kontos:

- **Verwenden Sie eine vorhandene e-Mail-Adresse.**

Benutzer können Ihre gültigen e-Mail-Adressen verwenden, um sich für Microsoft-Konten zu registrieren.

Der Dienst wandelt die e-Mail-Adresse des anfordernden Benutzers in ein Microsoft-Konto um. Benutzer können auch Ihre persönlichen Kennwörter auswählen.

- **Registrieren Sie sich für eine Microsoft-e-Mail-Adresse.**

Benutzer können sich mit den Webmail-Diensten von Microsoft für ein e-Mail-Konto registrieren. Dieses Konto kann zum Anmelden bei Websites verwendet werden, die für die Verwendung von Microsoft-Konten aktiviert sind.

Wie die Microsoft-Kontoinformationen geschützt werden

Anmeldeinformationen werden zwei Mal verschlüsselt. Die erste Verschlüsselung basiert auf dem Kennwort des Kontos. Die Anmeldeinformationen werden erneut verschlüsselt, wenn Sie über das Internet gesendet werden. Die gespeicherten Daten sind für andere Microsoft-oder nicht-Microsoft-Dienste nicht verfügbar.

- **Sicheres Kennwort ist erforderlich.**

Leere Kennwörter sind nicht zulässig.

Weitere Informationen finden Sie unter [Übersicht über die Sicherheit von Microsoft-Konten](#).

- **Sekundärer Identitätsnachweis ist erforderlich.**

Bevor auf einem zweiten unterstützten Windows-Computer zum ersten Mal auf Benutzerprofilinformationen und-Einstellungen zugegriffen werden kann, muss Trust für dieses Gerät eingerichtet werden, indem der sekundäre Identitätsnachweis bereitgestellt wird. Dies kann durch die Bereitstellung von Windows mit einem Code erfolgen, der an eine Mobiltelefonnummer gesendet wird, oder indem Sie die Anweisungen befolgen, die an eine Alternative e-Mail-Adresse gesendet werden, die ein Benutzer in den Kontoeinstellungen angibt.

- **Alle Benutzerprofildaten werden auf dem Client verschlüsselt, bevor Sie in die Cloud übertragen werden.**

Benutzerdaten werden standardmäßig nicht über ein Wireless Wide Area Network (WWAN) durchlaufen, wodurch Profildaten geschützt werden. Alle Daten und Einstellungen, die ein Gerät hinterlassen, werden über das TLS/SSL-Protokoll übertragen.

Microsoft-Konto Sicherheitsinformationen werden hinzugefügt.

Benutzer können Ihren Microsoft-Konten über die **Konten** Schnittstelle auf Computern, auf denen die unterstützten Windows-Versionen ausgeführt werden, Sicherheitsinformationen hinzufügen. Dieses Feature ermöglicht es dem Benutzer, die Sicherheitsinformationen zu aktualisieren, die er beim Erstellen seiner Konten bereitgestellt hat. Diese Sicherheitsinformationen enthalten eine Alternative e-Mail-Adresse oder Telefonnummer, wenn Ihr Kennwort kompromittiert oder vergessen wird, kann ein Verifizierungscode gesendet werden, um seine Identität zu verifizieren. Benutzer können Ihre Microsoft-Konten möglicherweise zum Speichern von Unternehmensdaten in einer persönlichen OneDrive-oder e-Mail-App verwenden, daher ist es sicher, dass der Kontobesitzer diese Sicherheitsinformationen auf dem neuesten Stand halten kann.

Das Microsoft-Konto im Unternehmen

Obwohl das Microsoft-Konto für die Nutzung von Verbrauchern entwickelt wurde, finden Sie möglicherweise Situationen, in denen Ihre Domänenbenutzer in Ihrem Unternehmen über Ihr persönliches Microsoft-Konto profitieren können. Die folgende Liste beschreibt einige Vorteile.

- **Herunterladen von Microsoft Store-Apps:**

Wenn Ihr Unternehmen entscheidet, Software über den Microsoft Store zu verteilen, können die Benutzer Ihre Microsoft-Konten zum herunterladen und verwenden auf bis zu fünf Geräten verwenden, auf denen eine beliebige Version von Windows 10, Windows 8,1, Windows8 oder WindowsRT ausgeführt wird.

- **Einmaliges Anmelden:**

Ihre Benutzer können die Anmeldeinformationen des Microsoft-Kontos verwenden, um sich bei Geräten mit Windows 10, Windows 8,1, Windows8 oder Windows RT anzumelden. In diesem Fall arbeitet Windows mit Ihrer Microsoft Store-App zusammen, um authentifizierte Erfahrungen für Sie bereitzustellen. Benutzer können ein Microsoft-Konto mit den Anmeldeinformationen für Microsoft Store-Apps oder -Websites verknüpfen, damit diese Anmeldeinformationen auf allen Geräten durchlaufen, auf denen diese unterstützten Versionen ausgeführt werden.

- **Synchronisierung der personalisierten Einstellungen:**

Benutzer können die am häufigsten verwendeten Betriebssystem Einstellungen mit einem Microsoft-Konto verknüpfen. Diese Einstellungen sind immer verfügbar, wenn sich ein Benutzer mit diesem Konto auf einem Gerät anmeldet, auf dem eine unterstützte Version von Windows ausgeführt wird und mit der Cloud verbunden ist. Nachdem sich ein Benutzer anmeldet, versucht das Gerät automatisch, die Einstellungen des Benutzers aus der Cloud abzurufen und auf das Gerät anzuwenden.

- **App-Synchronisierung:**

Microsoft Store-Apps können benutzerspezifische Einstellungen speichern, damit diese Einstellungen für jedes Gerät verfügbar sind. Wie bei den Betriebssystemeinstellungen sind diese benutzerspezifischen App-Einstellungen immer verfügbar, wenn sich der Benutzer mit dem gleichen Microsoft-Konto auf einem Gerät anmeldet, auf dem eine unterstützte Version von Windows ausgeführt wird und mit der Cloud verbunden ist. Nachdem sich der Benutzer angemeldet hat, lädt das Gerät die Einstellungen automatisch aus der Cloud herunter und wendet sie auf das Gerät an.

- **Integrierte Social Media-Dienste:**

Die Kontaktinformationen und der Status für die Freunde und Mitarbeiter Ihrer Benutzer bleiben automatisch auf Websites wie Hotmail, Outlook, Facebook, Twitter und LinkedIn auf dem neuesten Stand. Benutzer können auch auf Websites wie OneDrive, Facebook und Flickr auf Fotos, Dokumente und andere Dateien zugreifen und diese freigeben.

Verwalten des Microsoft-Kontos in der Domäne

Je nach Ihren IT- und Geschäftsmodellen kann die Einführung von Microsoft-Konten in Ihrem Unternehmen die Komplexität erhöhen oder Lösungen bieten. Sie sollten die folgenden Überlegungen besprechen, bevor Sie die Verwendung dieser Kontotypen in Ihrem Unternehmen zulassen:

- [Einschränken der Verwendung des Microsoft-Kontos](#)
- [Konfigurieren verbundener Konten](#)
- [Bereitstellen von Microsoft-Konten im Unternehmen](#)
- [Kontoaktivität überwachen](#)
- [Durchführen von Kennwort-zurück setsätzen](#)
- [Einschränken der App-Installation und -Verwendung](#)

Einschränken der Verwendung des Microsoft-Kontos

Die folgenden Gruppenrichtlinieneinstellungen helfen bei der Steuerung der Verwendung von Microsoft-Konten im Unternehmen:

- [Blockieren der Benutzerauthentifizierung für alle Consumer-Microsoft-Konten](#)
- [Konten: Blockieren von Microsoft-Konten](#)

Blockieren der Benutzerauthentifizierung für alle Consumer-Microsoft-Konten

Mit dieser Einstellung wird gesteuert, ob Benutzer Microsoft-Konten zur Authentifizierung für Anwendungen oder

Dienste bereitstellen können.

Wenn diese Einstellung aktiviert ist, werden alle Anwendungen und Dienste auf dem Gerät daran gehindert, Microsoft-Konten zur Authentifizierung zu verwenden. Dies gilt sowohl für vorhandene Benutzer eines Geräts als auch für neue Benutzer, die hinzugefügt werden können.

Alle Anwendungen oder Dienste, die einen Benutzer bereits authentifiziert haben, sind jedoch nicht davon betroffen, wenn Sie diese Einstellung aktivieren, bis der Authentifizierungscache abläuft. Es wird empfohlen, diese Einstellung zu aktivieren, bevor sich ein Benutzer an einem Gerät anmeldet, um zu verhindern, dass zwischengespeicherte Token vorhanden sind.

Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, können Anwendungen und Dienste Microsoft-Konten für die Authentifizierung verwenden. Diese Einstellung ist standardmäßig **deaktiviert**.

Diese Einstellung hat keinen Einfluss darauf, ob sich Benutzer mit Microsoft-Konten bei Geräten anmelden können, oder die Möglichkeit für Benutzer, Microsoft-Konten über den Browser zur Authentifizierung mit webbasierten Anwendungen zur Verfügung zu stellen.

Der Pfad zu dieser Einstellung lautet wie folgt:

Computer-Configuration\Administrative Vorlagen\Windows-Komponenten\Internet Vorlagen\Windows-Komponenten\Microsoft-Konto

Konten: Blockieren von Microsoft-Konten

Mit dieser Einstellung wird verhindert, dass mithilfe der **Einstellungen** -App ein Microsoft-Konto für die SSO-Authentifizierung (Single Sign-on, SSO) für Microsoft-Dienste und einige Hintergrunddienste hinzugefügt oder ein Microsoft-Konto für einmaliges Anmelden bei anderen Anwendungen oder Diensten verwendet wird.

Wenn diese Einstellung aktiviert ist, gibt es zwei Optionen:

- **Benutzer können Microsoft-Konten nicht hinzufügen** bedeutet, dass sich vorhandene verbundene Konten weiterhin beim Gerät anmelden können (und auf dem Anmeldebildschirm angezeigt werden). Benutzer können die **Einstellungen** -App jedoch nicht verwenden, um neue verbundene Konten hinzuzufügen (oder lokale Konten mit Microsoft-Konten zu verbinden).
- **Benutzer können nicht mit Microsoft-Konten hinzufügen oder anmelden** bedeutet, dass Benutzer keine neuen verbundenen Konten hinzufügen (oder lokale Konten mit Microsoft-Konten verbinden) oder vorhandene verbundene Konten über **Einstellungen** verwenden können.

Diese Einstellung hat keinen Einfluss auf das Hinzufügen eines Microsoft-Kontos für die Anwendungsauthentifizierung. Wenn diese Einstellung beispielsweise aktiviert ist, kann ein Benutzer weiterhin ein Microsoft-Konto für die Authentifizierung mit einer Anwendung wie **e-Mail** bereitstellen, aber der Benutzer kann das Microsoft-Konto nicht für die Authentifizierung mit einmaligem Anmelden für andere Anwendungen oder Dienste verwenden (mit anderen Worten: der Benutzer wird aufgefordert, sich für andere Anwendungen oder Dienste zu authentifizieren.)

Diese Einstellung ist standardmäßig **nicht definiert**.

Der Pfad zu dieser Einstellung lautet wie folgt:

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Konfigurieren verbundener Konten

Benutzer können ein Microsoft-Konto mit Ihrem Domänenkonto verbinden und die Einstellungen und Einstellungen zwischen diesen synchronisieren. Dadurch können Benutzer den gleichen Desktop Hintergrund, die App-Einstellungen, den Browserverlauf und die Favoriten sowie andere Microsoft-Kontoeinstellungen auf den anderen Geräten anzeigen.

Benutzer können ein Microsoft-Konto zu einem beliebigen Zeitpunkt wie folgt von Ihrem Domänenkonto trennen:

Tippen oder klicken Sie unter **PC-Einstellungen** auf **Benutzer**, tippen oder klicken Sie auf **trennen**, und tippen oder klicken Sie dann auf **Fertig stellen**.

Hinweis das Verbinden von Microsoft-Konten mit Domänenkonten kann den Zugriff auf einige Aufgaben mit hoher privilegierter Berechtigung in Windows einschränken. So wird beispielsweise vom Aufgabenplaner das verbundene Microsoft-Konto für den Zugriff ausgewertet, und es wird ein Fehler ausgeführt. In diesen Fällen sollte der Kontobesitzer das Konto trennen.

Bereitstellen von Microsoft-Konten im Unternehmen

Microsoft-Konten sind private Benutzerkonten. Microsoft gibt keine Methoden zur Bereitstellung von Microsoft-Konten für ein Unternehmen an. Unternehmen sollten Domänenkonten verwenden.

Kontoaktivität überwachen

Da Microsoft-Konten Internet basiert sind, verfügt Windows nicht über einen Mechanismus, um deren Verwendung zu überwachen, bis das Konto einem Domänenkonto zugeordnet ist. Diese Zuordnung schränkt aber nicht ein, dass der Benutzer die Verbindung mit dem Konto trennt oder von der Domäne getrennt wird. Es ist nicht möglich, die Aktivitäten von Konten zu überwachen, die nicht Ihrer Domäne zugeordnet sind.

Durchführen von Kennwort-zurück setsätzen

Das Kennwort kann nur vom Besitzer des Microsoft-Kontos geändert werden. Kennwörter können im [Anmelde Portal des Microsoft-Kontos](#) geändert werden.

Einschränken der App-Installation und-Verwendung

In Ihrer Organisation können Sie Richtlinien für die Anwendungssteuerung festlegen, um die APP-Installation und-Verwendung für Microsoft-Konten zu regulieren. Weitere Informationen finden Sie unter [AppLocker](#) und [verpackte apps](#) sowie in der [APP-Installationspaket-Regel in AppLocker](#).

Weitere Informationen:

- [Verwalten des Datenschutzes: Verwenden eines Microsoft-Kontos für die Anmeldung und die resultierende Internet Kommunikation](#)
- [Übersicht über die Zugriffssteuerung](#)

Dienstkonten

11.02.2020 • 5 minutes to read

Betrifft

- Windows 10
- Windows Server 2016

In diesem Thema wird für den IT-Experten erläutert, wie Gruppen- und eigenständige verwaltete Dienstkonten und das computerspezifische virtuelle Computerkonto und auf Ressourcen zu diesen Dienstkonten verweist.

Übersicht

Bei einem Dienstkonto handelt es sich um ein Benutzerkonto, das explizit erstellt wird, um einen Sicherheitskontext für Dienste bereitzustellen, die unter Windows Server-Betriebssystemen ausgeführt werden. Der Sicherheitskontext bestimmt, ob der Dienst auf lokale und Netzwerkressourcen zugreifen kann. Die Windows-Betriebssysteme basieren auf Diensten, um verschiedene Funktionen auszuführen. Diese Dienste können über die Anwendungen, das Dienste-Snap-in oder den Task-Manager oder mithilfe von Windows PowerShell konfiguriert werden.

Dieses Thema enthält Informationen zu den folgenden Arten von Dienstkonten:

- [Eigenständige verwaltete Dienstkonten](#)
- [Gruppen verwaltete Dienstkonten](#)
- [Virtuelle Konten](#)

Eigenständige verwaltete Dienstkonten

Ein verwaltetes Dienstkonto soll Domänenkonten in entscheidenden Anwendungen wie Internet Informationsdienste (IIS) isolieren und die Notwendigkeit verhindern, dass ein Administrator den Dienstprinzipalnamen (Service Principal Name, SPN) und die Anmeldeinformationen für die Konten.

Um verwaltete Dienstkonten verwenden zu können, muss auf dem Server, auf dem die Anwendung oder der Dienst installiert ist, mindestens Windows Server 2008 R2 ausgeführt werden. Ein verwaltetes Dienstkonto kann für Dienste auf einem einzelnen Computer verwendet werden. Verwaltete Dienstkonten können nicht von mehreren Computern freigegeben werden, und Sie können nicht in Serverclustern verwendet werden, in denen ein Dienst auf mehreren Clusterknoten repliziert wird. Für dieses Szenario müssen Sie ein Gruppen verwaltetes Dienstkonto verwenden. Weitere Informationen finden Sie unter [Übersicht über Gruppen verwaltete Dienstkonten](#).

Neben der erhöhten Sicherheit, die durch die Nutzung einzelner Konten für wichtige Dienste bereitgestellt wird, gibt es vier wichtige administrative Vorteile, die mit verwalteten Dienstkonten verbunden sind:

- Sie können eine Klasse von Domänenkonten erstellen, die verwendet werden kann, um Dienste auf lokalen Computern zu verwalten und zu verwalten.
- Im Gegensatz zu Domänenkonten, bei denen Administratoren manuell Kennwörter zurücksetzen müssen, werden die Netzwerkkennwörter für diese Konten automatisch zurückgesetzt.
- Sie müssen keine komplexen SPN-Verwaltungsaufgaben ausführen, um verwaltete Dienstkonten verwenden zu können.
- Administrative Aufgaben für verwaltete Dienstkonten können an nicht-Administratoren delegiert werden.

Softwareanforderungen

Verwaltete Dienstkonten gelten für die Windows-Betriebssysteme, die in der Liste "**gilt für**" am Anfang dieses Themas festgelegt sind.

Gruppen verwaltete Dienstkonten

Gruppen verwaltete Dienstkonten sind eine Erweiterung der eigenständigen verwalteten Dienstkonten, die in Windows Server 2008 R2 eingeführt wurden. Hierbei handelt es sich um verwaltete Domänenkonten, die eine automatische Kennwortverwaltung und eine vereinfachte Dienstprinzipalnamen-Verwaltung (SPN) bereitstellen, einschließlich der Delegierung der Verwaltung an andere Administratoren.

Das Group Managed Service-Konto bietet die gleiche Funktionalität wie ein eigenständiges verwaltetes Dienstkonto innerhalb der Domäne, erweitert diese Funktionalität aber auf mehrere Server. Beim Herstellen einer Verbindung mit einem Dienst, der in einer Serverfarm gehostet wird, wie etwa dem Netzwerklastenausgleich, erfordern die Authentifizierungsprotokolle, die die gegenseitige Authentifizierung unterstützen, dass alle Instanzen der Dienste denselben Prinzipal verwenden. Wenn Gruppen verwaltete Dienstkonten als Dienst Prinzipale verwendet werden, verwaltet das Windows Server-Betriebssystem das Kennwort für das Konto, anstatt sich auf den Administrator zu verlassen, um das Kennwort zu verwalten.

Der Microsoft-Schlüssel Verteilungsdienst (kdsvc. dll) stellt den Mechanismus bereit, um den neuesten Schlüssel oder einen bestimmten Schlüssel mit einem Schlüsselbezeichner für ein Active Directory-Konto sicher abzurufen. Dieser Dienst wurde in Windows Server 2012 eingeführt und kann nicht unter vorherigen Versionen des Windows Server-Betriebssystems ausgeführt werden. Der Schlüssel Verteilungsdienst gibt einen geheimen Schlüssel frei, der zum Erstellen von Schlüsseln für das Konto verwendet wird. Diese Tasten werden in regelmäßigen Abständen geändert. Bei einem Group Managed Service-Konto berechnet der Domänencontroller zusätzlich zu anderen Attributen des Gruppen verwalteten Dienstkontos das Kennwort für den Schlüssel, der von den Schlüssel Verteilung Diensten bereitgestellt wird.

Praktische Anwendungsfälle

Gruppen verwaltete Dienstkonten stellen eine einzelne Identitätslösung für Dienste bereit, die in einer Serverfarm ausgeführt werden, oder auf Systemen, die Netzwerklastenausgleich verwenden. Durch die Bereitstellung einer Managed Service Account-Lösung können Dienste für den Gruppen-Managed-Service-Konto Prinzipal konfiguriert werden, und die Kennwortverwaltung wird vom Betriebssystem gehandhabt.

Durch die Verwendung eines Gruppen verwalteten Dienstkontos müssen Dienste oder Dienstadministratoren keine Kennwortsynchronisierung zwischen Dienstinstanzen verwalten. Das Group Managed Service-Konto unterstützt Hosts, die für einen längeren Zeitraum offline aufbewahrt werden, und die Verwaltung von Mitglieds Hosts für alle Instanzen eines Diensts. Das bedeutet, dass Sie eine Serverfarm bereitstellen können, die eine einzelne Identität unterstützt, mit der vorhandene Clientcomputer authentifiziert werden können, ohne die Instanz des Diensts zu kennen, mit dem Sie eine Verbindung herstellen.

Failover-Cluster unterstützen nicht das Group Managed Service-Konto s. Dienste, die auf dem Cluster Dienst ausgeführt werden, können jedoch ein Gruppen verwaltetes Dienstkonto oder ein eigenständiges, verwaltetes Dienstkonto verwenden, wenn es sich um einen Windows-Dienst, einen app-Pool, einen geplanten Task handelt oder wenn er das Gruppen-Managed-Service-Konto oder eigenständige Dienstleistungen nativ unterstützt. verwaltete Dienstkonten.

Softwareanforderungen

Gruppen verwaltete Dienstkonten können nur auf Computern konfiguriert und verwaltet werden, auf denen mindestens Windows Server 2012 ausgeführt wird, Sie können jedoch in Domänen, auf denen noch Domänencontroller mit Betriebssystemen ausgeführt werden, als einzelne Dienst Identitätslösung bereitgestellt werden. als Windows Server 2012. Es gibt keine Anforderungen an die Funktionsebene Domäne oder Gesamtstruktur.

Zum Ausführen der Windows PowerShell-Befehle, die zum Verwalten von Gruppen verwalteten Dienstkonten verwendet werden, ist eine 64-Bit-Architektur erforderlich.

Ein verwaltetes Dienstkonto ist von den von Kerberos unterstützten Verschlüsselungstypen abhängig. Wenn sich ein Clientcomputer mit dem Kerberos-Protokoll bei einem Server authentifiziert, erstellt der Domänencontroller ein Kerberos-Dienstticket, das mit der Verschlüsselung geschützt ist, die vom Domänencontroller und vom Server unterstützt wird. Der Domänencontroller verwendet das **msDS-SupportedEncryptionTypes**-Attribut des Kontos, um zu ermitteln, welche Verschlüsselung vom Server unterstützt wird, und wenn kein Attribut vorhanden ist, wird davon ausgegangen, dass der Clientcomputer keine stärkere Verschlüsselungstypen unterstützt. Der erweiterte Verschlüsselungs Standard (Advanced Encryption Standard, AES) sollte immer explizit für verwaltete Dienstkonten konfiguriert sein. Wenn Computer, die das verwaltete Dienstkonto hosten, so konfiguriert sind, dass Sie RC4 nicht unterstützen, schlägt die Authentifizierung immer fehl.

Hinweis in WindowsServer2008R2 wurde der Data Encryption Standard (des) standardmäßig deaktiviert. Weitere Informationen zu unterstützten Verschlüsselungstypen finden Sie unter [Änderungen bei der Kerberos-Authentifizierung](#).

Gruppen verwaltete Dienstkonten sind unter Windows-Betriebssystemen vor Windows Server 2012 nicht anwendbar.

Virtuelle Konten

Virtuelle Konten wurden in Windows Server2008R2 und Windows7 eingeführt, und es handelt sich um verwaltete lokale Konten, die die folgenden Features zur Vereinfachung der Dienstverwaltung bereitstellen:

- Das virtuelle Konto wird automatisch verwaltet.
- Das virtuelle Konto kann in einer Domänenumgebung auf das Netzwerk zugreifen.
- Es ist keine Kennwortverwaltung erforderlich. Wenn beispielsweise der Standardwert für die Dienstkonten während des SQL Server-Setups unter Windows Server2008R2 verwendet wird, wird ein virtuelles Konto, das den Instanznamen als Dienstname verwendet, im Format NT<SERVICE\ Service>Name eingerichtet.

Dienste, die als virtuelle Konten ausgeführt werden, greifen auf Netzwerkressourcen zu, indem Sie die Anmeldeinformationen <des Computerkontos>\<in der Domäne>Format _name Computer _name \$ verwenden.

Informationen zum Konfigurieren und Verwenden von virtuellen Dienstkonten finden Sie unter [schrittweise Anleitung für Dienstkonten](#).

Softwareanforderungen

Virtuelle Konten gelten für die Windows-Betriebssysteme, die in der Liste "**gilt für**" am Anfang dieses Themas angegeben sind.

Weitere Informationen:

Die folgende Tabelle enthält Links zu weiteren Ressourcen, die sich auf eigenständige verwaltete Dienstkonten, Gruppen verwaltete Dienstkonten und virtuelle Konten beziehen.

INHALTSTYP	VERWEISE
Produktbewertung	Neuerungen bei verwalteten Dienstkonten Erste Schritte mit Gruppen verwalteten Dienstkonten
Bereitstellung	Windows Server2012: Gruppen verwaltete Dienstkonten – Fragen Sie Premier Field Engineering (pfe)-Plattformen-Website Home – TechNet-Blogs
Verwandte Technologien	Sicherheitsprinzipale Neues in Active Directory Domain Services

Active Directory-Sicherheitsgruppen

03.03.2020 • 52 minutes to read

Betreff:

- Windows Server 2016

Dieses Referenzthema für IT-Experten beschreibt die Active Directory-Standardsicherheitsgruppen.

Es gibt zwei Arten von allgemeinen Sicherheitsprinzipalen in Active Directory: Benutzerkonten und Computerkonten. Diese Konten stellen eine physikalische Entität (eine Person oder ein Computer) dar. Benutzerkonten können auch als dedizierte Dienstkonten für einige Anwendungen verwendet werden. Sicherheitsgruppen werden verwendet, um Benutzerkonten, Computerkonten und andere Gruppen in verwaltbaren Einheiten zu erfassen.

Im Windows Server-Betriebssystem gibt es mehrere integrierte Konten und Sicherheitsgruppen, die mit den entsprechenden Rechten und Berechtigungen vorkonfiguriert sind, um bestimmte Aufgaben auszuführen. Für ActiveDirectory gibt es zwei Arten von administrativen Zuständigkeiten:

- **Dienstadministratoren**, die für die Verwaltung und Bereitstellung von Active Directory-Domänendiensten (Adds) verantwortlich sind, einschließlich Verwalten von Domänencontrollern und Konfigurieren des Adds.
- **Datenadministratoren**, die für die Verwaltung der Daten verantwortlich sind, die in Adds- und auf Domänenmitgliedsservern und-Arbeitsstationen gespeichert sind.

Informationen zu Active Directory-Gruppen

Gruppen werden verwendet, um Benutzerkonten, Computerkonten und andere Gruppen in verwaltbaren Einheiten zu erfassen. Das Arbeiten mit Gruppen statt mit einzelnen Benutzern trägt zur Vereinfachung der Netzwerkwartung und-Verwaltung bei.

Es gibt zwei Arten von Gruppen in Active Directory:

- **Verteilerguppen** Dient zum Erstellen von e-Mail-Verteilerlisten.
- **Sicherheitsgruppen** Dient zum Zuweisen von Berechtigungen für freigegebene Ressourcen.

Verteilerguppen

Verteilerguppen können nur mit e-Mail-Anwendungen (wie Exchange Server) verwendet werden, um e-Mails an Benutzer Sammlungen zu senden. Verteilergruppen sind nicht sicherheitsaktiviert, was bedeutet, dass Sie nicht in DACLs (Discretionary Access Control Lists, DACLs) aufgeführt werden können.

Sicherheitsgruppen

Sicherheitsgruppen können eine effiziente Möglichkeit bieten, den Zugriff auf Ressourcen in Ihrem Netzwerk zuzuweisen. Mithilfe von Sicherheitsgruppen können Sie Folgendes tun:

- Zuweisen von Benutzerrechten zu Sicherheitsgruppen in Active Directory.

Benutzerrechte werden einer Sicherheitsgruppe zugewiesen, um zu bestimmen, welche Elemente dieser Gruppe innerhalb des Bereichs einer Domäne oder Gesamtstruktur ausgeführt werden können.

Benutzerrechte werden bei der Installation von ActiveDirectory automatisch einigen Sicherheitsgruppen zugewiesen, damit Administratoren die Administratorrolle einer Person in der Domäne definieren können.

Ein Benutzer, der der Gruppe Sicherungs-Operatoren in ActiveDirectory hinzugefügt wird, hat beispielsweise die Möglichkeit, Dateien und Verzeichnisse, die sich auf jedem Domänencontroller in der Domäne befinden, zu sichern und wiederherzustellen. Dies ist möglich, da standardmäßig die Benutzerrechte- **Sicherungsdateien und-Verzeichnisse** sowie **Dateien und Verzeichnisse wiederherstellen** der Gruppe Sicherungs-Operatoren automatisch zugewiesen werden. Daher erben Mitglieder dieser Gruppe die Benutzerrechte, die dieser Gruppe zugewiesen sind.

Sie können GroupPolicy verwenden, um Sicherheitsgruppen Benutzerrechte zuzuweisen, um bestimmte Aufgaben zu delegieren. Weitere Informationen zum Verwenden von Gruppenrichtlinien finden Sie unter [Zuweisen von Benutzerrechten](#).

- Zuweisen von Berechtigungen zu Sicherheitsgruppen für Ressourcen.

Berechtigungen unterscheiden sich von den Benutzerrechten. Der Sicherheitsgruppe werden Berechtigungen für die freigegebene Ressource zugewiesen. Berechtigungen legen fest, wer auf die Ressource und die Zugriffsebene zugreifen kann, beispielsweise "Vollzugriff". Einige Berechtigungen, die für Domänenobjekte festgelegt sind, werden automatisch zugewiesen, um unterschiedliche Zugriffsebenen für Standardsicherheitsgruppen zu ermöglichen, wie etwa die Gruppe "Konto-Operatoren" oder die Gruppe "Domänen-Admins".

Sicherheitsgruppen sind in DACLs aufgeführt, die Berechtigungen für Ressourcen und Objekte definieren. Beim Zuweisen von Berechtigungen für Ressourcen (Dateifreigaben, Drucker usw.) sollten Administratoren diese Berechtigungen nicht einzelnen Benutzern, sondern einer Sicherheitsgruppe zuweisen. Die Berechtigungen werden der Gruppe einmalig zugewiesen, und zwar nicht mehrmals für jeden einzelnen Benutzer. Jedes Konto, das einer Gruppe hinzugefügt wird, erhält die Rechte, die dieser Gruppe in ActiveDirectory zugewiesen sind, und der Benutzer erhält die Berechtigungen, die für diese Gruppe definiert sind.

Wie Verteilergruppen können Sicherheitsgruppen als e-Mail-Entität verwendet werden. Wenn Sie eine e-Mail-Nachricht an die Gruppe senden, wird die Nachricht an alle Mitglieder der Gruppe gesendet.

Gruppenbereich

Gruppen sind durch einen Bereich gekennzeichnet, der angibt, in welchem Umfang die Gruppe in der Domänenstruktur oder-Gesamtstruktur angewendet wird. Der Bereich der Gruppe definiert, wo der Gruppe Berechtigungen erteilt werden können. Die folgenden drei Gruppenbereiche werden von ActiveDirectory definiert:

- Universelle
- Globalen
- Lokale Domäne

Hinweis zusätzlich zu diesen drei Bereichen verfügen die Standardgruppen im Container **vordefiniert** über einen Gruppenbereich von Builtin local. Dieser Gruppenbereich und Gruppentyp können nicht geändert werden.

In der folgenden Tabelle sind die drei Gruppenbereiche und weitere Informationen zu jedem Bereich für eine Sicherheitsgruppe aufgelistet.

Gruppenbereiche

BEREICH	MÖGLICHE MITGLIEDER	BEREICHS KONVERTIERUNG	KANN BERECHTIGUNGEN ERTEILEN	MÖGLICHES MITGLIED VON
---------	---------------------	------------------------	------------------------------	------------------------

BEREICH	MÖGLICHE MITGLIEDER	BEREICHS KONVERTIERUNG	KANN BERECHTIGUNGEN ERTEILEN	MÖGLICHES MITGLIED VON
Universelle	<p>Konten aus einer beliebigen Domäne in der gleichen Gesamtstruktur</p> <p>Globale Gruppen aus einer beliebigen Domäne in der gleichen Gesamtstruktur</p> <p>Andere universelle Gruppen aus einer beliebigen Domäne in der gleichen Gesamtstruktur</p>	<p>Kann in den lokalen Domänenbereich konvertiert werden</p> <p>Kann in einen globalen Bereich konvertiert werden, wenn die Gruppe kein Mitglied anderer universeller Gruppen ist</p>	<p>In einer beliebigen Domäne in derselben Gesamtstruktur oder in vertrauenswürdigen Gesamtstrukturen</p>	<p>Andere universelle Gruppen in derselben Gesamtstruktur</p> <p>Lokale Domänengruppen in derselben Gesamtstruktur oder vertrauenden Gesamtstrukturen</p> <p>Lokale Gruppen auf Computern in derselben Gesamtstruktur oder vertrauenden Gesamtstrukturen</p>
Globalen	<p>Konten aus der gleichen Domäne</p> <p>Andere globale Gruppen aus derselben Domäne</p>	<p>Kann in den universellen Bereich konvertiert werden, wenn die Gruppe kein Mitglied einer anderen globalen Gruppe ist</p>	<p>In einer beliebigen Domäne in derselben Gesamtstruktur oder vertrauenden Domänen oder Gesamtstrukturen</p>	<p>Universelle Gruppen aus einer beliebigen Domäne in der gleichen Gesamtstruktur</p> <p>Andere globale Gruppen aus derselben Domäne</p> <p>Lokale Domänengruppen aus einer beliebigen Domäne in der gleichen Gesamtstruktur oder aus einer vertrauenswürdigen Domäne</p>

BEREICH	MÖGLICHE MITGLIEDER	BEREICHS KONVERTIERUNG	KANN BERECHTIGUNGEN ERTEILEN	MÖGLICHES MITGLIED VON
Lokale Domäne	<p>Konten aus einer beliebigen Domäne oder einer vertrauenswürdigen Domäne</p> <p>Globale Gruppen aus einer beliebigen Domäne oder einer vertrauenswürdigen Domäne</p> <p>Universelle Gruppen aus einer beliebigen Domäne in der gleichen Gesamtstruktur</p> <p>Andere lokale Domänengruppen aus derselben Domäne</p> <p>Konten, globale Gruppen und universelle Gruppen aus anderen Gesamtstrukturen und aus externen Domänen</p>	Kann in den universellen Bereich konvertiert werden, wenn die Gruppe keine anderen lokalen Domänengruppen enthält	Innerhalb der gleichen Domäne	<p>Andere lokale Domänengruppen aus derselben Domäne</p> <p>Lokale Gruppen auf Computern in der gleichen Domäne, ausgenommen integrierte Gruppen mit bekannten SIDs</p>

Spezielle Identitäts Gruppen

Besondere Identitäten werden im Allgemeinen als Gruppen bezeichnet. Spezielle Identitäts Gruppen verfügen nicht über bestimmte Mitgliedschaften, die geändert werden können, Sie können jedoch je nach Situation verschiedene Benutzer zu unterschiedlichen Zeitpunkten darstellen. Einige dieser Gruppen sind Creator Owner, Batch und authentifizierter Benutzer.

Informationen zu allen speziellen Identitäts Gruppen finden Sie unter [besondere Identitäten](#).

Standardsicherheitsgruppen

Standardgruppen, beispielsweise die Gruppe "Domänen-Admins", sind Sicherheitsgruppen, die beim Erstellen einer ActiveDirectory-Domäne automatisch erstellt werden. Sie können diese vordefinierten Gruppen dazu verwenden, den Zugriff auf freigegebene Ressourcen zu steuern und bestimmte domänenweite Administratorrollen zu delegieren.

Vielen Standardgruppen wird automatisch eine Gruppe von Benutzerrechten zugewiesen, die Mitgliedern der Gruppe das Ausführen bestimmter Aktionen in einer Domäne autorisieren, beispielsweise die Anmeldung an einem lokalen System oder das Sichern von Dateien und Ordnern. Ein Mitglied der Gruppe "Sicherungs-Operatoren" hat beispielsweise das Recht, Sicherungsvorgänge für alle Domänencontroller in der Domäne durchzuführen.

Wenn Sie einen Benutzer zu einer Gruppe hinzufügen, erhält der Benutzer alle Benutzerrechte, die der Gruppe zugewiesen sind, sowie alle Berechtigungen, die der Gruppe für freigegebene Ressourcen zugewiesen sind.

Standardgruppen befinden sich im Container "**BuiltIn**" und im Container "**Benutzer**" in "Active Directory-Benutzer und-Computer". Der Container **BuiltIn** enthält Gruppen, die mit dem lokalen Domänenbereich definiert sind. Die **Benutzer** enthält Gruppen, die mit dem globalen Bereich und Gruppen definiert sind, die mit dem lokalen Domänenbereich definiert sind. Sie können Gruppen, die sich in diesen Containern befinden, in andere Gruppen oder Organisationseinheiten innerhalb der Domäne verschieben, aber nicht in andere Domänen verschieben.

Einige administrative Gruppen, die in diesem Thema aufgelistet sind, und alle Mitglieder dieser Gruppen sind durch einen Hintergrundprozess geschützt, der in regelmäßigen Abständen eine bestimmte Sicherheitsbeschreibung überprüft und anwendet. Dieser Deskriptor ist eine Datenstruktur, die Sicherheitsinformationen enthält, die einem geschützten Objekt zugeordnet sind. Durch diesen Vorgang wird sichergestellt, dass alle erfolgreichen unbefugten Versuche, die Sicherheitsbeschreibung in einem der administrativen Konten oder Gruppen zu ändern, mit den geschützten Einstellungen überschrieben werden.

Die Sicherheitsbeschreibung ist im **AdminSDHolder** -Objekt vorhanden. Das bedeutet, dass Sie die Sicherheitsbeschreibung für das **AdminSDHolder** -Objekt ändern müssen, damit Sie konsistent angewendet wird, wenn Sie die Berechtigungen für eine der Dienstadministratorgruppen oder für eines der Mitgliedskonten ändern möchten. Achten Sie beim Vornehmen dieser Änderungen darauf, dass Sie auch die Standardeinstellungen ändern, die auf alle geschützten Administratorkonten angewendet werden.

Active Directory-Standardsicherheitsgruppen nach Betriebssystemversion

Die folgenden Tabellen enthalten Beschreibungen der Standardgruppen, die sich in den Containern **BuiltIn** und **Users** in jedem Betriebssystem befinden.

STANDARDSICHERHEIT SGRUPPE	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER2008R2
Hilfe Operatoren für die Zugriffssteuerung	Ja	Ja	Ja	
Kontooperatoren	Ja	Ja	Ja	Ja
Administratoren	Ja	Ja	Ja	Ja
Zulässige RODC- Kenn Wort Replikationsgruppe	Ja	Ja	Ja	Ja
Sicherungs- Operatoren	Ja	Ja	Ja	Ja
Zertifikatdienst- DCOM-Zugriff	Ja	Ja	Ja	Ja
CERT- Herausgeber	Ja	Ja	Ja	Ja

STANDARDSICHERHEIT SGRUPPE	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER2008R2
Cloneable- Domänencontroll er	Ja	Ja	Ja	
Kryptografische Operatoren	Ja	Ja	Ja	Ja
Verweigerte RODC-Kenn Wort Replikationsgrupp e	Ja	Ja	Ja	Ja
Gerätebesitzer	Ja	Ja	Ja	Ja
Verteilte com- Benutzer	Ja	Ja	Ja	Ja
DnsUpdateProxy	Ja	Ja	Ja	Ja
DnsAdmins	Ja	Ja	Ja	Ja
Domänenadminis tratoren	Ja	Ja	Ja	Ja
Domänencomput er	Ja	Ja	Ja	Ja
Domänencontroll er	Ja	Ja	Ja	Ja
Domänengäste	Ja	Ja	Ja	Ja
Domänenbenutze r	Ja	Ja	Ja	Ja
Unternehmensad ministratoren	Ja	Ja	Ja	Ja
Enterprise- Schlüssel- Administratoren	Ja			

STANDARDSICHERHEIT SGRUPPE	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER2008R2
Schreibgeschützte Enterprise- Domänencontroll er	Ja	Ja	Ja	Ja
Ereignisprotokoll eser	Ja	Ja	Ja	Ja
Besitzer von Gruppenrichtlinie n Erstellern	Ja	Ja	Ja	Ja
Gäste	Ja	Ja	Ja	Ja
Hyper-V- Administratoren	Ja	Ja	Ja	
IIS_IUSRS	Ja	Ja	Ja	Ja
Eingehende Gesamtstruktur Vertrauensstellun gs-Generatoren	Ja	Ja	Ja	Ja
Schlüssel Administratoren	Ja			
Netzwerk Konfigurations Operatoren	Ja	Ja	Ja	Ja
Leistungsprotokol lbenutzer	Ja	Ja	Ja	Ja
Benutzer des Systemmonitors	Ja	Ja	Ja	Ja
Pre-Windows 2000- kompatibler Zugriff	Ja	Ja	Ja	Ja
Druckoperatoren	Ja	Ja	Ja	Ja

STANDARDSICHERHEIT SGRUPPE	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER2008R2
Geschützte Benutzer	Ja	Ja		
RAS-und IAS- Server	Ja	Ja	Ja	Ja
RDS- Endpunktserver	Ja	Ja	Ja	
RDS- Verwaltungsse- r	Ja	Ja	Ja	
RDS-Remote Zugriffsserver	Ja	Ja	Ja	
Schreibgeschützte Domänencontroll er	Ja	Ja	Ja	Ja
Remote Desktop Benutzer	Ja	Ja	Ja	Ja
Benutzer der Remote Verwaltung	Ja	Ja	Ja	
Replicator	Ja	Ja	Ja	Ja
Schema Administratoren	Ja	Ja	Ja	Ja
Server Operatoren	Ja	Ja	Ja	Ja
Speicher Replikat Administratoren	Ja			
Gruppe "System verwaltete Konten"	Ja			

STANDARDSICHERHEIT SGRUPPE	WINDOWS SERVER 2016	WINDOWS SERVER 2012 R2	WINDOWS SERVER 2012	WINDOWS SERVER2008R2
Terminal Server- Lizenzserver	Ja	Ja	Ja	Ja
Users	Ja	Ja	Ja	Ja
Windows- Autorisierungs Zugriffsgruppe	Ja	Ja	Ja	Ja
WinRMRemoteW MIUsers_		Ja	Ja	

Hilfe Operatoren für die Zugriffssteuerung

Mitglieder dieser Gruppe können Autorisierungs Attribute und Berechtigungen für Ressourcen auf dem Computer Remoteabfragen.

Die Gruppe der Zugriffs Steuerungs Unterstützungs Operatoren bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-579
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Kontooperatoren

Die Gruppe Konten-Operatoren gewährt einem Benutzer begrenzte Konto Erstellungsberechtigungen. Mitglieder dieser Gruppe können die meisten Arten von Konten erstellen und ändern, einschließlich derer von Benutzern, lokalen Gruppen und globalen Gruppen, und Mitglieder können sich lokal bei Domänencontrollern anmelden.

Mitglieder der Gruppe Konten-Operatoren können das Administrator Benutzerkonto, die Benutzerkonten von Administratoren oder die Gruppen [Administratoren](#), [Server Operatoren](#), [Kontooperatoren](#), [Sicherungs-Operatoren](#) oder [Druckoperatoren](#) nicht verwalten. Mitglieder dieser Gruppe können keine Benutzerrechte ändern.

Die Gruppe "Konto-Operatoren" bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis Standardmäßig enthält diese integrierte Gruppe keine Mitglieder, und Sie kann Benutzer und Gruppen in der Domäne erstellen und verwalten, einschließlich ihrer eigenen Mitgliedschaft und der Gruppe der Server Operatoren. Diese Gruppe wird als Dienstadministratorgruppe angesehen, da Sie die Server Operatoren ändern kann, wodurch wiederum die Einstellungen des Domänencontrollers geändert werden können. Als bewährte Methode sollten Sie die Mitgliedschaft in dieser Gruppe leer lassen und Sie nicht für Delegierte Verwaltungszwecke verwenden. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-548
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Lokales anmelden zulassen: SeInteractiveLogonRight

Administratoren

Mitglieder der Gruppe Administratoren haben vollständigen und uneingeschränkten Zugriff auf den Computer, oder wenn der Computer zu einem Domänencontroller heraufgestuft wird, haben Mitglieder uneingeschränkten Zugriff auf die Domäne.

Die Gruppe Administratoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis die Gruppe Administratoren verfügt über integrierte Funktionen, die ihren Mitgliedern die volle Kontrolle über das System bieten. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden. Diese integrierte Gruppe steuert den Zugriff auf alle Domänencontroller in Ihrer Domäne, und Sie kann die Mitgliedschaft aller administrativen Gruppen ändern.

Die Mitgliedschaft kann von Mitgliedern der folgenden Gruppen geändert werden: den standardmäßigen Dienstadministratoren, Domänenadministratoren in der Domäne oder Unternehmensadministratoren. Diese Gruppe hat das besondere Privileg, den Besitz eines beliebigen Objekts im Verzeichnis oder einer beliebigen Ressource auf einem Domänencontroller zu übernehmen. Dieses Konto wird als Dienstadministratorgruppe angesehen, da seine Mitglieder Vollzugriff auf die Domänencontroller in der Domäne haben.

Diese Sicherheitsgruppe umfasst die folgenden Änderungen seit Windows Server 2008:

- Änderungen an den standardmäßigen Benutzerrechten: **Zulassen der Anmeldung über die Terminal Dienste** gab es in Windows Server 2008, und es wurde durch [Allow Log on über Remote Desktop Dienste](#) ersetzt.
- Der [Computer aus der Dockingstation entfernen](#) wurde in Windows Server 2012 R2 entfernt.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-544
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Administrator, Domänenadministratoren, Unternehmensadministratoren
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	<p>Anpassen von Speicherkontingenten für einen Prozess: SeIncreaseQuotaPrivilege</p> <p>Zugriff auf diesen Computer über das Netzwerk: SeNetworkLogonRight</p> <p>Lokales anmelden zulassen: SeInteractiveLogonRight</p> <p>Zulassen der Anmeldung über Remote Desktop Dienste: SeRemoteInteractiveLogonRight</p> <p>Sichern von Dateien und Verzeichnissen: SeBackupPrivilege</p> <p>Umgehen der Durchquerung Überprüfung:</p>

ATTRIBUT	SeChangeNotifyPrivilege WERT
	<p>Ändern der Systemzeit: SeSystemtimePrivilege</p> <p>Ändern der Zeitzone: SeTimeZonePrivilege</p> <p>Erstellen einer AuslagerungsDatei: SeCreatePagefilePrivilege</p> <p>Erstellen globaler Objekte: SeCreateGlobalPrivilege</p> <p>Erstellen symbolischerLinks: SeCreateSymbolicLinkPrivilege</p> <p>Debuggen vonProgrammen: SeDebugPrivilege</p> <p>Aktivieren der Vertrauenswürdigkeit von Computer-und BenutzerKonten für die Delegierung: SeEnableDelegationPrivilege</p> <p>Erzwingen des Herunterfahrens von einem Remote System: SeRemoteShutdownPrivilege</p> <p>Identitätswechsel zwischen einem Client und der Authentifizierung: SeImpersonatePrivilege</p> <p>Erhöhen der PlanungsPriorität: SeIncreaseBasePriorityPrivilege</p> <p>Laden und Entladen von GeräteTreibern: SeLoadDriverPrivilege</p> <p>Anmelden als Stapelverarbeitungsauftrag: SeBatchLogonRight</p> <p>Verwalten von Überwachungs-und Sicherheitsprotokollen: SeSecurityPrivilege</p> <p>Ändern von Firmware-Umgebungswerten: SeSystemEnvironmentPrivilege</p> <p>Durchführen von Volume-Wartungsaufgaben: SeManageVolumePrivilege</p> <p>Profilsystem Leistung: SeSystemProfilePrivilege</p> <p>Profil einzelner Prozess: SeProfileSingleProcessPrivilege</p> <p>Entfernen des Computers aus der Dockingstation: SeUndockPrivilege</p> <p>Wiederherstellen von Dateien und Verzeichnissen: SeRestorePrivilege</p> <p>Herunterfahren des Systems: SeShutdownPrivilege</p> <p>Übernehmen des Besitzes von Dateien oder anderen Objekten: SeTakeOwnershipPrivilege</p>

Zulässige RODC-Kenn Wort Replikationsgruppe

Diese Sicherheitsgruppe dient zum Verwalten einer RODC-Kennwortreplikationsrichtlinie. Diese Gruppe enthält standardmäßig keine Mitglieder und führt zu der Bedingung, dass neue schreibgeschützte Domänencontroller keine Benutzeranmeldeinformationen Zwischenspeichern. Die Gruppe "verweigerte RODC-Kennwortreplikation" enthält eine Reihe von Konten und Sicherheitsgruppen mit hoher Berechtigung. Die Gruppe verweigerte RODC-Kennwortreplikation ersetzt die zulässige RODC-Kenn Wort Replikationsgruppe.

Die Gruppe Zulässige RODC-Kennwortreplikation bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-571
Typ	Lokale Domäne
Standardcontainer	CN = Benutzer DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Sicherungs-Operatoren

Mitglieder der Gruppe Sicherungsoperatoren können unabhängig von den Berechtigungen, die diese Dateien schützen, alle Dateien auf einem Computer sichern und wiederherstellen. Backup-Operatoren können sich auch bei anmelden und den Computer Herunterfahren. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden. Standardmäßig hat diese integrierte Gruppe keine Mitglieder und kann Sicherungs- und Wiederherstellungsvorgänge auf Domänencontrollern durchführen. Die Mitgliedschaft kann durch die folgenden Gruppen geändert werden: Standarddienst Administratoren, Domänenadministratoren in der Domäne oder Unternehmensadministratoren. Die Mitgliedschaft in administrativen Gruppen kann nicht geändert werden. Während Mitglieder dieser Gruppe die Servereinstellungen nicht ändern oder die Konfiguration des Verzeichnisses ändern können, verfügen Sie über die erforderlichen Berechtigungen, um Dateien (einschließlich Betriebssystemdateien) auf Domänencontrollern zu ersetzen. Aus diesem Grund gelten Mitglieder dieser Gruppe als Dienstadministratoren.

Die Gruppe Sicherungs-Operatoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-551
Typ	Builtin local

ATTRIBUT	WERT
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	<p>Lokales anmelden zulassen: SeInteractiveLogonRight</p> <p>Sichern von Dateien und Verzeichnissen: SeBackupPrivilege</p> <p>Anmelden als Stapelverarbeitungsauftrag: SeBatchLogonRight</p> <p>Wiederherstellen von Dateien und Verzeichnissen: SeRestorePrivilege</p> <p>Herunterfahren des Systems: SeShutdownPrivilege</p>

Zertifikatdienst-DCOM-Zugriff

Mitglieder dieser Gruppe können eine Verbindung mit Zertifizierungsstellen im Unternehmen herstellen.

Die DCOM-Zugriffsgruppe Zertifikatdienst gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-<Domäne>-574
Typ	Lokale Domäne
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine

ATTRIBUT	WERT
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

CERT-Herausgeber

Mitglieder der Gruppe "CERT Publishers" sind berechtigt, Zertifikate für Benutzerobjekte in Active Directory zu veröffentlichen.

Die Gruppe "CERT Publishers" bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-517
Typ	Lokale Domäne
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Verweigerte RODC-Kenn Wort Replikationsgruppe
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Cloneable-Domänencontroller

Mitglieder der Gruppe der geklonten Domänencontroller, bei denen es sich um Domänencontroller handelt, können geklont werden. In Windows Server 2012 R2 und Windows Server 2012 können Sie Domänencontroller durch Kopieren eines vorhandenen virtuellen Domänencontrollers bereitstellen. In einer virtuellen Umgebung

müssen Sie nicht mehr wiederholt ein Serverabbild bereitstellen, das mit "Sysprep. exe" vorbereitet wird, den Server zu einem Domänencontroller heraufstufen und dann zusätzliche Konfigurationsanforderungen für die Bereitstellung der einzelnen Domänencontroller erfüllen (einschließlich des Hinzufügens des virtuellen Domänencontrollers zu dieser Sicherheitsgruppe).

Weitere Informationen finden Sie unter [Einführung in die Active Directory-Domänendienste \(AD DS\)-Virtualisierung \(Stufe 100\)](#).

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-522
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Kryptografische Operatoren

Mitglieder dieser Gruppe sind autorisiert, kryptografische Vorgänge durchzuführen. Diese Sicherheitsgruppe wurde in Windows Vista Service Pack 1 (SP1) hinzugefügt, um die Windows-Firewall für IPSec im Modus für allgemeine Kriterien zu konfigurieren.

Die Gruppe kryptografische Operatoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe wurde in WindowsVistaServicePack1 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-569

ATTRIBUT	WERT
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Verweigerte RODC-Kenn Wort Replikationsgruppe

Mitglieder der Gruppe der verweigerten RODC-Kennwortreplikation können Ihre Kennwörter nicht auf einen schreibgeschützten Domänencontroller replizieren.

Diese Sicherheitsgruppe dient zum Verwalten einer RODC-Kennwortreplikationsrichtlinie. Diese Gruppe enthält eine Vielzahl von Konten mit hoher Berechtigung und Sicherheitsgruppen. Die Gruppe verweigerte RODC-Kennwortreplikation ersetzt die [Zulässige RODC-Kenn Wort Replikationsgruppe](#).

Diese Sicherheitsgruppe umfasst die folgenden Änderungen seit Windows Server 2008:

- Windows Server2012 hat die Standard Mitglieder so geändert, dass Sie [CERT-Herausgeber](#)umfassen.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-572
Typ	Lokale Domäne
Standardcontainer	CN = Users, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	CERT-Herausgeber Domänenadministratoren Domänencontroller Unternehmensadministratoren Besitzer von Gruppenrichtlinien Erstellen krbtgt Schreibgeschützte Domänencontroller Schema Administratoren
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Gerätebesitzer

Diese Gruppe wird derzeit nicht in Windows verwendet.

Microsoft rät davon ab, die Standardkonfiguration zu ändern, wenn diese Sicherheitsgruppe keine Mitglieder aufweist. Das Ändern der Standardkonfiguration kann zukünftige Szenarien behindern, die auf diese Gruppe angewiesen sind.

Die Gruppe "Gerätebesitzer" bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-583
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine

ATTRIBUT	WERT
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, wird jedoch nicht empfohlen
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	<p>Lokalesanmelden zulassen: SeInteractiveLogonRight</p> <p>Zugriff auf diesen Computer über dasNetzwerk: SeNetworkLogonRight</p> <p>Umgehen der DurchquerungÜberprüfung: SeChangeNotifyPrivilege</p> <p>Ändern der Zeitzone: SeTimeZonePrivilege</p>

Verteilte com-Benutzer

Mitglieder der Gruppe "verteilte com-Benutzer" dürfen verteilte COM-Objekte auf dem Computer starten, aktivieren und verwenden. Microsoft Component Object Model (com) ist ein plattformunabhängiges, verteiltes objektorientiertes System zum Erstellen binärer Softwarekomponenten, die interagieren können. DCOM (Distributed Component Object Model) ermöglicht die Verteilung von Anwendungen auf Standorte, die für Sie und die Anwendung am sinnvollsten sind. Diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Die Gruppe verteilte com-Benutzer gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-562
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden

ATTRIBUT	WERT
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

DnsUpdateProxy

Mitglieder der DnsUpdateProxy-Gruppe sind DNS-Clients. Sie sind berechtigt, dynamische Updates für andere Clients (wie DHCP-Server) durchzuführen. Ein DNS-Server kann veraltete Ressourceneinträge entwickeln, wenn ein DHCP-Server so konfiguriert ist, dass er Host (a)-und Zeigerressourceneinträge (PTR) im Auftrag von DHCP-Clients dynamisch mithilfe des dynamischen Updates registriert. Das Hinzufügen von Clients zu dieser Sicherheitsgruppe verringert dieses Szenario.

Zum Schutz vor ungesicherten Datensätzen oder zum zulassen, dass Mitglieder der DnsUpdateProxy-Gruppe Datensätze in Zonen registrieren, die nur gesicherte dynamische Updates zulassen, müssen Sie ein dediziertes Benutzerkonto erstellen und DHCP-Server so konfigurieren, dass DNS-dynamische Updates durchgeführt werden. Verwenden der Anmeldeinformationen dieses Kontos (Benutzername, Kennwort und Domäne) Mehrere DHCP-Server können die Anmeldeinformationen eines dedizierten Benutzerkontos verwenden.

Informationen hierzu finden Sie unter [DNS-Eintrags Besitz und die DnsUpdateProxy-Gruppe](#).

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-1103
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

DnsAdmins

Mitglieder der DnsAdmins-Gruppe können auf Netzwerk-DNS-Informationen zugreifen. Die Standardberechtigungen lauten wie folgt: zulassen: lesen, schreiben, alle untergeordneten Objekte erstellen, untergeordnete Objekte löschen, spezielle Berechtigungen.

Weitere Informationen zu Sicherheit und DNS finden Sie unter [DNSSEC in Windows Server 2012](#).

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-1102
Typ	Lokale Domäne
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Domänenadministratoren

Mitglieder der Sicherheitsgruppe "Domänenadministratoren" sind berechtigt, die Domäne zu verwalten. Standardmäßig ist die Gruppe Domänen-Admins ein Mitglied der Gruppe Administratoren auf allen Computern, die einer Domäne beigetreten sind, einschließlich der Domänencontroller. Die Gruppe "Domänen-Admins" ist der Standardbesitzer eines beliebigen Objekts, das von einem Mitglied der Gruppe in ActiveDirectory für die Domäne erstellt wird. Wenn Mitglieder der Gruppe andere Objekte wie Dateien erstellen, ist der Standardbesitzer die Gruppe Administratoren.

Die Gruppe Domänenadministratoren steuert den Zugriff auf alle Domänencontroller in einer Domäne, und Sie kann die Mitgliedschaft aller Administratorkonten in der Domäne ändern. Die Mitgliedschaft kann von Mitgliedern der Dienstadministratorkonten in Ihrer Domäne (Administratoren und Domänenadministratoren) sowie von Mitgliedern der Gruppe Organisations-Admins geändert werden. Hierbei handelt es sich um ein Dienstadministratorkonto, da seine Mitglieder Vollzugriff auf die Domänencontroller in einer Domäne haben.

Die Gruppe Domänen-Admins gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-512
Typ	Domäne Global
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Administrator
Standardmitglied von	Administratoren Verweigerte RODC-Kenn Wort replikationsgroup
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Siehe Administratoren Siehe verweigerte RODC-Kenn Wort Replikationsgruppe

Domänencomputer

Diese Gruppe kann alle Computer und Server enthalten, die der Domäne beigetreten sind, ohne Domänencontroller. Standardmäßig wird jedes Computerkonto, das automatisch erstellt wird, Mitglied dieser Gruppe.

Die Gruppe "Domänencomputer" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-515
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Alle Computer, die mit der Domäne verbunden sind, ohne Domänencontroller

ATTRIBUT	WERT
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja (aber nicht erforderlich)
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

Domänencontroller

Die Gruppe "Domänencontroller" kann alle Domänencontroller in der Domäne umfassen. Neue Domänencontroller werden dieser Gruppe automatisch hinzugefügt.

Die Gruppe Domänencontroller gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-516
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Computer Konten für alle Domänencontroller der Domäne
Standardmitglied von	Verweigerte RODC-Kenn Wort Replikationsgruppe
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Nein
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Domänengäste

Die Gruppe Domain guests enthält das integrierte Gastkonto der Domäne. Wenn sich Mitglieder dieser Gruppe als lokale Gäste auf einem mit der Domäne verbundenen Computer anmelden, wird ein Domänenprofil auf dem lokalen Computer erstellt.

Die Gruppe "Domänengäste" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5- <Domäne> -514
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Gast
Standardmitglied von	Gäste
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann verschoben werden, wird jedoch nicht empfohlen
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Gäste anzeigen

Domänenbenutzer

Die Gruppe "Domänenbenutzer" umfasst alle Benutzerkonten in einer Domäne. Wenn Sie ein Benutzerkonto in einer Domäne erstellen, wird es dieser Gruppe automatisch hinzugefügt.

Standardmäßig wird jedes Benutzerkonto, das in der Domäne erstellt wird, automatisch Mitglied dieser Gruppe. Diese Gruppe kann verwendet werden, um alle Benutzer in der Domäne darzustellen. Wenn Sie beispielsweise möchten, dass alle Domänenbenutzer auf einen Drucker zugreifen können, können Sie dieser Gruppe Berechtigungen für den Drucker zuweisen (oder die Gruppe "Domänenbenutzer" einer lokalen Gruppe auf dem Druckserver hinzufügen, die über die Berechtigungen für den Drucker verfügt).

Die Gruppe "Domänenbenutzer" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5- <Domäne> -513

ATTRIBUT	WERT
Typ	Domäne Global
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Administrator krbtgt
Standardmitglied von	Users
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Benutzer anzeigen

Unternehmensadministratoren

Die Gruppe "Unternehmensadministratoren" existiert nur in der Stammdomäne einer ActiveDirectory-Gesamtstruktur von Domänen. Es handelt sich um eine universelle Gruppe, wenn sich die Domäne im einheitlichen Modus befindet. Wenn sich die Domäne im gemischten Modus befindet, handelt es sich um eine globale Gruppe. Mitglieder dieser Gruppe sind zum Erstellen von gesamtstrukturweiten Änderungen in ActiveDirectory autorisiert, beispielsweise zum Hinzufügen von untergeordneten Domänen.

Standardmäßig ist das einzige Mitglied der Gruppe das Administrator Konto für die Stammdomäne der Gesamtstruktur. Diese Gruppe wird automatisch zur Gruppe Administratoren in jeder Domäne in der Gesamtstruktur hinzugefügt und bietet vollständigen Zugriff für die Konfiguration aller Domänencontroller. Mitglieder in dieser Gruppe können die Mitgliedschaft aller administrativen Gruppen ändern. Die Mitgliedschaft kann nur von den standardmäßigen Dienstadministratorkonten in der Stammdomäne geändert werden. Dies gilt als Dienstadministratorkonto.

Die Gruppe "Unternehmensadministratoren" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21- <root-> Domäne-519
Typ	Universell (wenn sich die Domäne im einheitlichen Modus befindet) else Global

ATTRIBUT	WERT
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Administrator
Standardmitglied von	Administratoren Verweigerte RODC-Kenn Wort Replikationsgruppe
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Siehe Administratoren Siehe verweigerte RODC-Kenn Wort Replikationsgruppe

Enterprise-Schlüssel-Administratoren

Mitglieder dieser Gruppe können administrative Aktionen für Schlüsselobjekte innerhalb der Gesamtstruktur durchführen.

Die Gruppe "Enterprise-Schlüssel-Administratoren" wurde in Windows Server 2016 eingeführt.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-527
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Schreibgeschützte Enterprise-Domänencontroller

Mitglieder dieser Gruppe sind schreibgeschützte Domänencontroller im Unternehmen. Mit Ausnahme von

Kontokennwörtern enthält ein schreibgeschützter Domänencontroller alle ActiveDirectory-Objekte und-Attribute, die ein schreibbarer Domänencontroller besitzt. Änderungen an der Datenbank, die auf dem schreibgeschützten Domänencontroller gespeichert ist, können jedoch nicht vorgenommen werden. Änderungen müssen auf einem schreibbaren Domänencontroller vorgenommen und dann auf den schreibgeschützten Domänencontroller repliziert werden.

Schreibgeschützte Domänencontroller behandeln einige der Probleme, die häufig in Zweigstellen zu finden sind. Diese Speicherorte verfügen möglicherweise nicht über einen Domänencontroller. Oder Sie verfügen möglicherweise über einen beschreibbaren Domänencontroller, aber nicht über die physische Sicherheit, die Netzwerkbandbreite oder lokales Expertenwissen, um es zu unterstützen.

Weitere Informationen finden Sie unter [Was ist ein RODC?](#).

Die Gruppe schreibgeschützte Unternehmens-Domänencontroller gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit WindowsServer2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-498
Typ	Universelle
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Ereignisprotokollleser

Mitglieder dieser Gruppe können Ereignisprotokolle von lokalen Computern lesen. Die Gruppe wird erstellt, wenn der Server zu einem Domänencontroller heraufgestuft wird.

Die Gruppe Ereignisprotokollleser bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-573
Typ	Builtin local
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Besitzer von Gruppenrichtlinien Erstellern

Diese Gruppe ist berechtigt, GroupPolicy-Objekte in der Domäne zu erstellen, zu bearbeiten oder zu löschen. Standardmäßig ist das einzige Mitglied der Gruppe Administrator.

Informationen zu anderen Features, die Sie mit dieser Sicherheitsgruppe verwenden können, finden Sie unter [Übersicht über Gruppenrichtlinien](#).

Die Gruppe der Besitzer von Gruppenrichtlinien Erstellern gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-<Domäne>-520
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Administrator
Standardmitglied von	Verweigerte RODC-Kenn Wort Replikationsgruppe

ATTRIBUT	WERT
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Nein
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Siehe verweigte RODC-Kenn Wort Replikationsgruppe

Gäste

Mitglieder der Gruppe "Gäste" haben standardmäßig denselben Zugriff wie Mitglieder der Gruppe "Benutzer", es sei denn, das Gastkonto hat weitere Einschränkungen. Standardmäßig ist das einzige Mitglied das Gastkonto. Die Gruppe "Gäste" ermöglicht es gelegentlichen oder einmaligen Benutzern, sich mit Einschränkungen für das integrierte Gastkonto eines Computers anzumelden.

Wenn ein Mitglied der Gruppe "Gäste" abmeldet, wird das gesamte Profil gelöscht. Dazu gehören alle Elemente, die im Verzeichnis **% User Profile%** gespeichert sind, einschließlich der Registrierungsstruktur Informationen des Benutzers, benutzerdefinierte Desktopsymbole und andere benutzerspezifische Einstellungen. Dies impliziert, dass ein Gast ein temporäres Profil zur Anmeldung beim System verwenden muss. Diese Sicherheitsgruppe interagiert mit der Gruppenrichtlinieneinstellung "**Benutzer nicht mit temporären Profilen anmelden**", wenn Sie aktiviert ist. Diese Einstellung befindet sich unter dem folgenden Pfad:

Computer Configuration\Administrative Templates\System\User profile

Hinweis ein Gastkonto ist ein Standardmitglied der Sicherheitsgruppe Gäste. Personen, die nicht über ein tatsächliches Konto in der Domäne verfügen, können das Gastkonto verwenden. Ein Benutzer, dessen Konto deaktiviert (aber nicht gelöscht) ist, kann auch das Gastkonto verwenden.

Für das Gastkonto ist kein Kennwort erforderlich. Sie können Rechte und Berechtigungen für das Gastkonto wie in einem beliebigen Benutzerkonto einrichten. Standardmäßig ist das Gastkonto ein Mitglied der integrierten Gruppe Gäste und der globalen Gruppe Domänengäste, mit der sich ein Benutzer bei einer Domäne anmelden kann. Das Gastkonto ist standardmäßig deaktiviert, und es wird empfohlen, dass es deaktiviert bleibt.

Die Gruppe "Gäste" bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-546
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Gast

ATTRIBUT	WERT
Standardmitglied von	Domänengäste Gast
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Hyper-V-Administratoren

Mitglieder der Gruppe "Hyper-v-Administratoren" haben vollständigen und uneingeschränkten Zugriff auf alle Features in Hyper-v. Durch das Hinzufügen von Mitgliedern zu dieser Gruppe können Sie die Anzahl der Mitglieder reduzieren, die in der Gruppe Administratoren erforderlich sind, und den Zugriff weiter voneinander trennen.

Hinweis vor der Windows-Server2012 wurde der Zugriff auf Features in Hyper-V teilweise durch die Mitgliedschaft in der Gruppe Administratoren gesteuert.

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-578
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Nein
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	

ATTRIBUT	WERT
Standardbenutzerrechte	Keine

IIS _IUSRS

IIS _IUSRS ist eine integrierte Gruppe, die von Internet Informationsdiensten ab IIS 7.0 verwendet wird. Ein integriertes Konto und eine integrierte Gruppe werden vom Betriebssystem garantiert, dass immer eine eindeutige SID vorhanden ist. IIS 7.0 ersetzt das IUSR _MachineName-Konto und die IIS _WPG-Gruppe durch die IIS _IUSRS-Gruppe, um sicherzustellen, dass die tatsächlichen Namen, die vom neuen Konto und der Gruppe verwendet werden, nie lokalisiert werden. Unabhängig von der Sprache des Windows-Betriebssystems, das Sie installieren, ist der Name des IIS-Kontos immer IUSR, und der Gruppenname ist IIS _IUSRS.

Weitere Informationen finden Sie unter [Grundlegendes zu integrierten Benutzer-und Gruppenkonten in IIS 7](#).

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-568
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	IUSR
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Eingehende Gesamtstruktur Vertrauensstellungs-Generatoren

Mitglieder der Gruppe "eingehende Gesamtstrukturvertrauensstellung" können eingehende unidirektionale Vertrauensstellungen für diese Gesamtstruktur erstellen. Active Directory bietet Sicherheit für mehrere Domänen oder Gesamtstrukturen über Domänen-und Gesamtstruktur-Vertrauensstellungen. Bevor die Authentifizierung über Vertrauensstellungen erfolgen kann, muss Windows ermitteln, ob die von einem Benutzer, Computer oder Dienst angeforderte Domäne eine Vertrauensstellung mit der Anmeldedomäne des anfordernden Kontos aufweist.

Um diese Feststellung zu treffen, berechnet das Windows-Sicherheitssystem einen Vertrauenspfad zwischen dem Domänencontroller für den Server, der die Anforderung empfängt, und einem Domänencontroller in der Domäne

des anfordernden Kontos. Ein gesicherter Kanal erstreckt sich auf andere Active Directory-Domänen über zwischen Domänen-Vertrauensstellungen. Dieser abgesicherte Kanal wird verwendet, um Sicherheitsinformationen zu erhalten und zu überprüfen, einschließlich Sicherheits-IDs (SIDs) für Benutzer und Gruppen.

Hinweis diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Weitere Informationen finden Sie unter [Funktionsweise von Domänen-und Gesamtstrukturvertrauensstellungen: Domänen-und Gesamtstrukturvertrauensstellungen](#).

Die Gruppe "eingehende Gesamtstrukturvertrauensstellung" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Hinweis diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-557
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Schlüssel Administratoren

Mitglieder dieser Gruppe können administrative Aktionen für Schlüsselobjekte innerhalb der Domäne durchführen.

Die Gruppe "Schlüssel Administratoren" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-526

ATTRIBUT	WERT
Typ	Globalen
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Netzwerk Konfigurations Operatoren

Mitglieder der Gruppe Netzwerkkonfigurations-Operatoren können über die folgenden Administratorrechte verfügen, um die Konfiguration von Netzwerkfeatures zu verwalten:

- Ändern Sie die TCP/IP-Eigenschaften (Transmission Control Protocol/Internet Protocol) für eine LAN-Verbindung (Local Area Network), die die IP-Adresse, die Subnetzmaske, das Standardgateway und die Namensserver umfasst.
- Benennen Sie die LAN-Verbindungen oder RAS-Verbindungen um, die für alle Benutzer verfügbar sind.
- Aktivieren oder Deaktivieren einer LAN-Verbindung.
- Ändern Sie die Eigenschaften aller Remotezugriffsverbindungen von Benutzern.
- Löschen Sie alle RAS-Verbindungen von Benutzern.
- Benennen Sie alle RAS-Verbindungen von Benutzern um.
- Erteilen Sie die Befehle **ipconfig**, **ipconfig/release** oder **ipconfig/renew**.
- Geben Sie den PIN Unblock-Schlüssel (PUK) für mobile Breitbandgeräte ein, die eine SIM-Karte unterstützen.

Hinweis diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Die Gruppe Netzwerkkonfigurations-Operatoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-556

ATTRIBUT	WERT
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

Leistungsprotokollbenutzer

Mitglieder der Gruppe Leistungsprotokollbenutzer können Leistungsindikatoren, Protokolle und Benachrichtigungen lokal auf dem Server und von Remoteclients verwalten, ohne Mitglied der Gruppe Administratoren zu sein. Insbesondere Mitglieder dieser Sicherheitsgruppe:

- Kann alle Features verwenden, die für die Gruppe "System Monitor Benutzer" verfügbar sind.
- Sie können Datensammlungssätze erstellen und ändern, nachdem der Gruppe das Benutzerrecht [Anmelden als Stapelverarbeitungsauftrag](#) zugewiesen wurde.

Warnung Wenn Sie Mitglied der Gruppe Leistungsprotokollbenutzer sind, müssen Sie die von Ihnen erstellten Datensammlungssätze so konfigurieren, dass Sie unter Ihren Anmeldeinformationen ausgeführt werden.

- Der Windows-Kernel-Ablaufverfolgungs-Ereignisanbieter kann in Sammlungssätzen nicht verwendet werden.

Damit Mitglieder der Gruppe Leistungsprotokollbenutzer die Datenprotokollierung initiieren oder Datensammlungssätze ändern können, muss der Gruppe zuerst das Benutzerrecht [Anmelden als Stapelverarbeitungsauftrag](#) zugewiesen werden. Verwenden Sie das lokale Sicherheitsrichtlinien-Snap-in in der Microsoft Management Console, um dieses Benutzerrecht zuzuweisen.

Hinweis diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Die Gruppe Leistungsprotokollbenutzer gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis : dieses Konto kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-559
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Anmelden als Stapelverarbeitungsauftrag: SeBatchLogonRight

Benutzer des Systemmonitors

Mitglieder dieser Gruppe können Leistungsindikatoren auf Domänencontrollern in der Domäne, lokal und von Remoteclients aus überwachen, ohne Mitglied der Gruppen Administratoren oder Leistungsprotokollbenutzer zu sein. Der Windows-System Monitor ist ein MMC-Snap-in (Microsoft Management Console), in dem Tools zum Analysieren der Systemleistung bereitgestellt werden. Über eine einzige Konsole können Sie die Leistung von Anwendungen und Hardware überwachen, die Daten, die Sie in Protokollen sammeln möchten, festlegen, Schwellenwerte für Warnungen und automatische Aktionen definieren, Berichte generieren und vergangene Leistungsdaten auf verschiedene Arten anzeigen.

Insbesondere Mitglieder dieser Sicherheitsgruppe:

- Kann alle Funktionen verwenden, die für die Gruppe "Benutzer" verfügbar sind.
- Kann Echtzeitleistungsdaten im System Monitor anzeigen.

Kann die Anzeigeeigenschaften des Systemmonitors während der Anzeige von Daten ändern.

- Datensammlungssätze können nicht erstellt oder geändert werden.

Warnung Sie können einen Sammlungssatz nicht so konfigurieren, dass er als Mitglied der Gruppe System Monitor Benutzer ausgeführt wird.

Hinweis diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Die Gruppe System Monitor Benutzer gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-558
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

Kompatibler Zugriff vor – 2000-2000

Mitglieder der Gruppe "Pre-Windows 2000-kompatibler Zugriff" verfügen über Lesezugriff für alle Benutzer und Gruppen in der Domäne. Diese Gruppe wird aus Gründen der Abwärtskompatibilität für Computer bereitgestellt, auf denen WindowsNT 4.0 und frühere Versionen ausgeführt werden. Standardmäßig ist die Gruppe besondere Identität, jeder, Mitglied dieser Gruppe. Sie können dieser Gruppe nur dann Benutzer hinzufügen, wenn Sie WindowsNT 4.0 oder früher ausführen.

Warnung diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmastervorgänge oder FSMO bezeichnet) enthält.

Die Gruppe "Pre-2000-kompatibler Zugriff" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-554
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	Wenn Sie den Modus "Pre-Windows 2000-kompatible Berechtigungen" auswählen, sind jeder und Anonymous Mitglieder, und wenn Sie den Modus "nur Windows 2000-Berechtigungen" auswählen, sind authentifizierte Benutzer Mitglieder.
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Zugriff auf diesen Computer über das Netzwerk: SeNetworkLogonRight Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege

Druckoperatoren

Mitglieder dieser Gruppe können Drucker verwalten, erstellen, freigeben und löschen, die mit Domänencontrollern in der Domäne verbunden sind. Sie können auch Active Directory-Druckerobjekte in der Domäne verwalten. Mitglieder dieser Gruppe können sich lokal bei den Domänencontrollern in der Domäne anmelden und diese Herunterfahren.

Diese Gruppe hat keine Standard Mitglieder. Da Mitglieder dieser Gruppe Gerätetreiber auf allen Domänencontrollern in der Domäne laden und entladen können, fügen Sie Benutzer mit Bedacht hinzu. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Die Gruppe "Druckoperatoren" bezieht sich auf Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert. In Windows Server 2008 R2 wurde jedoch die Funktionalität zum Verwalten der Druckverwaltung hinzugefügt. Weitere Informationen finden Sie unter [Zuweisen von Delegierten Druck Administrator- und Drucker Berechtigungseinstellungen in Windows Server 2012](#).

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-550
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Lokales anmelden zulassen: SeInteractiveLogonRight Laden und Entladen von Geräte Treibern: SeLoadDriverPrivilege Herunterfahren des Systems : SeShutdownPrivilege

Geschützte Benutzer

Mitglieder der Gruppe "geschützte Benutzer" haben zusätzlichen Schutz vor der Gefährdung von Anmeldeinformationen während der Authentifizierungsprozesse.

Diese Sicherheitsgruppe wurde als Teil einer Strategie entwickelt, um die Anmeldeinformationen im Unternehmen effektiv zu schützen und zu verwalten. Mitgliedern dieser Gruppe wird automatisch ein nicht konfigurierbarer Schutz auf Ihre Konten zugewiesen. Die Mitgliedschaft in der Gruppe "geschützte Benutzer" soll standardmäßig restriktiv und proaktiv gesichert werden. Die einzige Methode zum Ändern des Schutzes für ein Konto besteht darin, das Konto aus der Sicherheitsgruppe zu entfernen.

Diese domänenbezogene globale Gruppe löst nicht konfigurierbaren Schutz auf Geräten und Hostcomputern aus, beginnend mit den Betriebssystemen Windows Server 2012 R2 und Windows 8,1. Außerdem wird ein nicht konfigurierbarer Schutz auf Domänencontrollern in Domänen mit einem primären Domänencontroller, auf dem Windows Server 2012 R2 oder Windows Server 2016 ausgeführt wird, ausgelöst. Dadurch wird der Speicherbedarf von Anmeldeinformationen erheblich reduziert, wenn sich Benutzer von einem nicht beeinträchtigten Computer bei Computern im Netzwerk anmelden.

Je nach der Domänenfunktionsebene des Kontos sind die Mitglieder der Gruppe "geschützte Benutzer" aufgrund von Verhaltensänderungen in den Authentifizierungsmethoden, die in Windows unterstützt werden, weiter geschützt.

- Mitglieder der Gruppe "geschützte Benutzer" können mithilfe der folgenden Security Support Provider (SSPs) nicht authentifiziert werden: NTLM, Digestauthentifizierung oder CredSSP. Kennwörter werden nicht auf einem Gerät zwischengespeichert, auf dem Windows 8,1 oder Windows 10 ausgeführt wird, sodass sich das Gerät bei einer Domäne nicht authentifizieren kann, wenn das Konto Mitglied der geschützten Benutzergruppe ist.
- Das Kerberos-Protokoll verwendet nicht die schwächeren des oder RC4-Verschlüsselungstypen im vorauthentifizierungs Prozess. Dies bedeutet, dass die Domäne so konfiguriert sein muss, dass Sie mindestens die AES-Verschlüsselungssuite unterstützt.
- Das Konto des Benutzers kann nicht mit einer eingeschränkten oder eingeschränkten Kerberos-

Delegierung delegiert werden. Das bedeutet, dass frühere Verbindungen zu anderen Systemen fehlschlagen können, wenn der Benutzer ein Mitglied der Gruppe "geschützte Benutzer" ist.

- Die Standardeinstellung für das Kerberos-Ticket-Granting Tickets (TGTs) von vier Stunden ist mithilfe von Authentifizierungsrichtlinien und-Silos konfigurierbar, auf die über das Active Directory-Verwaltungs Center zugegriffen werden kann. Das bedeutet, dass der Benutzer sich erneut authentifizieren muss, wenn vier Stunden vergangen sind.

Die Gruppe "geschützte Benutzer" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

Diese Gruppe wurde in Windows Server 2012 R2 eingeführt. Weitere Informationen zur Funktionsweise dieser Gruppe finden Sie unter [Sicherheitsgruppe "geschützte Benutzer"](#).

In der folgenden Tabelle sind die Eigenschaften der Gruppe "geschützte Benutzer" angegeben.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21- <Domäne> -525
Typ	Domäne Global
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

RAS-und IAS-Server

Computer, die Mitglieder der RAS-und IAS-Servergruppe sind, sind bei ordnungsgemäßer Konfiguration berechtigt, RAS-Dienste zu verwenden. Standardmäßig hat diese Gruppe keine Mitglieder. Computer, auf denen der Routing-und RAS-Dienst ausgeführt wird, werden der Gruppe automatisch hinzugefügt, beispielsweise IAS-Server und Netzwerkrichtlinienserver. Mitglieder dieser Gruppe können auf bestimmte Eigenschaften von Benutzerobjekten zugreifen, beispielsweise Lesen von Kontoeinschränkungen, Lesen von Anmeldeinformationen und Lesen von Remote Zugriffsinformationen.

Die Gruppe RAS-und IAS-Server gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-553
Typ	Lokale Domäne
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

RDS-Endpointserver

Server, die Mitglieder der Gruppe "RDS-Endpointserver" sind, können virtuelle Computer und Host Sitzungen ausführen, in denen Benutzer-RemoteApp-Programme und persönliche virtuelle Desktops ausgeführt werden. Diese Gruppe muss auf Servern mit RD-Verbindungs Broker aufgefüllt werden. Die für die Bereitstellung verwendeten Sitzungshost Server und RD Virtualization-Hostserver müssen in dieser Gruppe sein.

Informationen zu Remotedesktopdiensten finden Sie unter [Hosten von Desktopcomputern und apps in Remotedesktopdiensten](#).

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-<Domäne>-576
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine

ATTRIBUT	WERT
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

RDS-Verwaltungsserver

Server, die Mitglieder der Gruppe "RDS-Verwaltungsserver" sind, können verwendet werden, um routinemäßige Verwaltungsaktionen auf Servern auszuführen, auf denen Remote Desktop Dienste ausgeführt werden. Diese Gruppe muss auf allen Servern in einer Remote Desktop Dienste-Bereitstellung aufgefüllt werden. Die Server, auf denen der RDS Central-Verwaltungsdienst ausgeführt wird, müssen in dieser Gruppe enthalten sein.

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-577
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

RDS-Remote Zugriffsserver

Server in der Gruppe RDS-Remote Zugriffsserver ermöglichen Benutzern den Zugriff auf RemoteApp-Programme und persönliche virtuelle Desktops. In Bereitstellungen mit Internet Verbindung werden diese Server in der Regel in einem Edge-Netzwerk bereitgestellt. Diese Gruppe muss auf Servern mit RD-Verbindungs Broker aufgefüllt werden. RD-Gatewayserver und Remote Desktop-Webzugriffs Server, die in der Bereitstellung verwendet werden, müssen sich in dieser Gruppe befinden.

Weitere Informationen finden Sie unter [Hosten von Desktopcomputern und apps in Remote Desktop Diensten](#).

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-575
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Remote Desktop Benutzer

Die Gruppe Remote Desktop Benutzer auf einem RDSession-Hostserver wird verwendet, um Benutzern und Gruppen Berechtigungen für die Remoteverbindung mit einem RDSession-Hostserver zu gewähren. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden. Sie wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Die Gruppe Remote Desktop Benutzer gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-555

ATTRIBUT	WERT
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

Schreibgeschützte Domänencontroller

Diese Gruppe besteht aus den schreibgeschützten Domänencontrollern in der Domäne. Ein schreibgeschützter Domänencontroller ermöglicht Organisationen die einfache Bereitstellung eines Domänencontrollers in Szenarien, in denen die physische Sicherheit nicht gewährleistet werden kann, wie beispielsweise Zweigstellenstandorte oder in Szenarien, in denen die lokale Speicherung aller Domänenkennwörter eine primäre Bedrohung, beispielsweise in einem Extranet oder in einer mit der Anwendung konfrontierten Rolle.

Da die Verwaltung eines schreibgeschützten Domänencontrollers an einen Domänenbenutzer oder eine Sicherheitsgruppe delegiert werden kann, eignet sich ein schreibgeschützter Domänencontroller gut für eine Website, die keinen Benutzer hat, der Mitglied der Gruppe der Domänenadministratoren ist. Ein schreibgeschützter Domänencontroller umfasst die folgenden Funktionen:

- Schreibgeschützte Datenbank hinzugefügt
- Unidirektionale Replikation
- Zwischenspeicherung von Anmeldeinformationen
- Trennung der Administrator Rolle
- Schreibgeschütztes Domain Name System (DNS)

Informationen zum Bereitstellen eines schreibgeschützten Domänencontrollers finden Sie unter [Grundlegendes zur Planung und Bereitstellung für schreibgeschützte Domänencontroller](#).

Diese Sicherheitsgruppe wurde in Windows Server 2008 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-521
Typ	
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Verweigerte RODC-Kenn Wort Replikationsgruppe
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Siehe verweigerte RODC-Kenn Wort Replikationsgruppe

Benutzer der Remote Verwaltung

Mitglieder der Gruppe Remote Verwaltungs Benutzer können über Verwaltungsprotokolle (wie WS-Verwaltung über den Windows-Remote Verwaltungsdienst) auf WMI-Ressourcen zugreifen. Dies gilt nur für WMI-Namespace, die dem Benutzer Zugriff gewähren.

Die Gruppe Remote Verwaltungs Benutzer wird in der Regel verwendet, um Benutzern zu ermöglichen, Server über die Server-Manager-Konsole zu verwalten, während die [WinRMRemoteWMIUsers_](#)-Gruppe Remote ausgeführte Windows PowerShell-Befehle ermöglicht.

Weitere Informationen finden Sie unter [Neuerungen in Mi](#) und [Informationen zu WMI](#).

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-580
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine

ATTRIBUT	WERT
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Replicator

Computer, die Mitglieder der Replicator-Gruppe sind, unterstützen die Dateireplikation in einer Domäne. Windows-Server Betriebssysteme verwenden den Dateireplikationsdienst (File Replication Service, FRS) zum Replizieren von Systemrichtlinien und Anmeldeskripts, die auf dem Systemdatenträger (SYSVOL) gespeichert sind. Jeder Domänencontroller speichert eine Kopie von SYSVOL für Netzwerkclients, auf die Sie zugreifen können. FRS kann auch Daten für das verteilte Datei System (Distributed File System, DFS) replizieren, wobei der Inhalt der einzelnen Mitglieder in einer Replikatgruppe entsprechend der Definition durch DFS synchronisiert wird. FRS kann freigegebene Dateien und Ordner auf mehreren Servern gleichzeitig kopieren und verwalten. Wenn Änderungen auftreten, wird der Inhalt sofort innerhalb von Websites und durch einen Zeitplan zwischen Websites synchronisiert.

Wichtig in Windows Server2008R2 kann FRS nicht zum Replizieren von DFS-Ordern oder benutzerdefinierten (nicht-SYSVOL-) Daten verwendet werden. Ein Windows Server2008R2-Domänencontroller kann weiterhin FRS verwenden, um den Inhalt einer freigegebenen SYSVOL-Ressource in einer Domäne zu replizieren, die FRS zum Replizieren der freigegebenen SYSVOL-Ressource zwischen Domänencontrollern verwendet.

Windows-Server2008R2-Server können FRS jedoch nicht verwenden, um den Inhalt einer Replikatgruppe außer der freigegebenen SYSVOL-Ressource zu replizieren. Der DFS-Replikationsdienst ist ein Ersatz für FRS und kann verwendet werden, um den Inhalt einer freigegebenen SYSVOL-Ressource, DFS-Ordner und anderer benutzerdefinierter (nicht-SYSVOL-) Daten zu replizieren. Sie sollten alle FRS-Replikatsätze, die nicht SYSVOL sind, in die DFS-Replikation migrieren. Weitere Informationen finden Sie unter:

- [Der Dateireplikationsdienst \(FRS\) ist in Windows Server2008R2 \(Windows\) veraltet](#)
- [Übersicht über DFS-Namespaces und DFS-Replikation](#)

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-552
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Schema Administratoren

Mitglieder der Gruppe Schema Administratoren können das Active Directory-Schema ändern. Diese Gruppe ist nur in der Stammdomäne einer ActiveDirectory-Gesamtstruktur von Domänen vorhanden. Es handelt sich um eine universelle Gruppe, wenn sich die Domäne im einheitlichen Modus befindet. Wenn sich die Domäne im gemischten Modus befindet, handelt es sich um eine globale Gruppe.

Die Gruppe ist berechtigt, Schemaänderungen in Active Directory vorzunehmen. Standardmäßig ist das einzige Mitglied der Gruppe das Administrator Konto für die Stammdomäne der Gesamtstruktur. Diese Gruppe verfügt über vollen administrativen Zugriff auf das Schema.

Die Mitgliedschaft in dieser Gruppe kann von allen Dienstadministratorgruppen in der Stammdomäne geändert werden. Dies gilt als Dienstadministratorkonto, da seine Mitglieder das Schema ändern können, das die Struktur und den Inhalt des gesamten Verzeichnisses regelt.

Weitere Informationen finden Sie unter [Was ist das Active Directory-Schema?: Active Directory](#).

Die Gruppe "Schema Administratoren" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5- <root-> Domäne-518
Typ	Universell (wenn sich die Domäne im einheitlichen Modus befindet) else Global
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Administrator

ATTRIBUT	WERT
Standardmitglied von	Verweigerte RODC-Kenn Wort Replikationsgruppe
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Siehe verweigerte RODC-Kenn Wort Replikationsgruppe

Server Operatoren

Mitglieder der Gruppe Server Operatoren können Domänenserver verwalten. Diese Gruppe ist nur auf Domänencontrollern vorhanden. Standardmäßig hat die Gruppe keine Mitglieder. Mitglieder der Gruppe Serveroperatoren können sich interaktiv bei einem Server anmelden, freigegebene Netzwerkressourcen erstellen und löschen, Dienste starten und beenden, Dateien sichern und wiederherstellen, die Festplatte des Computers formatieren und den Computer Herunterfahren. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Standardmäßig hat diese integrierte Gruppe keine Mitglieder und hat Zugriff auf Serverkonfigurationsoptionen auf Domänencontrollern. Die Mitgliedschaft wird von den Dienstadministratorgruppen, Administratoren und Domänenadministratoren in der Domäne und der Gruppe "Unternehmensadministratoren" gesteuert. Mitglieder in dieser Gruppe können keine administrativen Gruppenmitgliedschaften ändern. Hierbei handelt es sich um ein Dienstadministratorkonto, da seine Mitglieder physischen Zugriff auf Domänencontroller haben, Sie Wartungsaufgaben (wie Sicherung und Wiederherstellung) durchführen können, und Sie die Möglichkeit haben, Binärdateien zu ändern, die in der Domäne installiert sind. Controller. Beachten Sie die Standardbenutzerrechte in der folgenden Tabelle.

Die Gruppe Server Operatoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-549
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine

ATTRIBUT	WERT
Geschützt durch ADMINSDHOLDER?	Ja
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	<p>Lokales anmelden zulassen: SeInteractiveLogonRight</p> <p>Sichern von Dateien und Verzeichnissen: SeBackupPrivilege</p> <p>Ändern der Systemzeit: SeSystemtimePrivilege</p> <p>Ändern der Zeitzone: SeTimeZonePrivilege</p> <p>Erzwingen des Herunterfahrens von einem Remote System: SeRemoteShutdownPrivilege</p> <p>Wiederherstellen von Dateien und Verzeichnissen: Wiederherstellen von Dateien und Verzeichnissen SeRestorePrivilege</p> <p>Herunterfahren des Systems: SeShutdownPrivilege</p>

Speicher Replikat Administratoren

Mitglieder dieser Gruppe haben vollständigen und uneingeschränkten Zugriff auf alle Features des Speicher Replikats.

Die Gruppe Speicher Replikat Administratoren gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-582
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Gruppe "System verwaltete Konten"

Mitglieder dieser Gruppe werden vom System verwaltet.

Die Gruppe "System verwaltete Konten" gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle "Active Directory-Standardsicherheitsgruppen"](#) aufgeführt sind.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-581
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Users
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Terminal Server-Lizenzserver

Mitglieder der Gruppe Terminal Server-Lizenzserver können Benutzerkonten in Active Directory mit Informationen zur Lizenzerteilung aktualisieren. Diese wird verwendet, um TS pro Benutzer-CAL-Nutzung zu nachvollziehen und zu melden. Eine TSPer-Benutzer-CAL gibt einem Benutzer das Recht, von einer unbegrenzten Anzahl von Clientcomputern oder-Geräten aus auf einen Terminal Server zuzugreifen. Diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Weitere Informationen zu dieser Sicherheitsgruppe finden Sie unter [Konfiguration der Terminal Dienste-Lizenz Server-Sicherheitsgruppe](#).

Die Gruppe Terminal Server-Lizenzserver gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe gilt nur für Windows Server2003 und Windows Server2008, da die Terminal Dienste in WindowsServer2008R2 durch Remote Desktop Dienste ersetzt wurden.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-561
Typ	Builtin local

ATTRIBUT	WERT
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Geschützt durch ADMINSDHOLDER?	Nein
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

Users

Mitglieder der Gruppe Benutzer werden daran gehindert, zufällige oder absichtliche systemweite Änderungen vorzunehmen, und Sie können die meisten Anwendungen ausführen. Nach der erstmaligen Installation des Betriebssystems ist das einzige Mitglied die Gruppe "authentifizierte Benutzer". Wenn ein Computer einer Domäne Beirtritt, wird die Gruppe "Domänenbenutzer" der Gruppe "Benutzer" auf dem Computer hinzugefügt.

Benutzer können Aufgaben wie das Ausführen von Anwendungen, die Verwendung von lokalen und Netzwerkdruckern, das Herunterfahren des Computers und das Sperren des Computers ausführen. Benutzer können Anwendungen installieren, die nur Sie verwenden dürfen, wenn das Installationsprogramm der Anwendung die Installation pro Benutzer unterstützt. Diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Die Gruppe Benutzer gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Diese Sicherheitsgruppe umfasst die folgenden Änderungen seit Windows Server 2008:

- In Windows Server2008R2 wurde Interactive zur Standard Mitgliederliste hinzugefügt.
- In Windows Server2012 wurde das standardmäßige **Mitglied der** Liste von Domänenbenutzern in None geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-545
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =

ATTRIBUT	WERT
Standard Mitglieder	Authentifizierte Benutzer Domänenbenutzer Interaktive
Standardmitglied von	Domänenbenutzer (diese Mitgliedschaft ist darauf zurückzuführen, dass die primäre Gruppen-ID aller Benutzerkonten Domänenbenutzer ist.)
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Nein
Standardbenutzerrechte	Keine

Windows-Autorisierungs Zugriffsgruppe

Mitglieder dieser Gruppe haben Zugriff auf das berechnete Token-GroupsGlobalAndUniversal-Attribut für Benutzerobjekte. Einige Anwendungen verfügen über Features, die das Token-Groups-Global-and-Universal-Attribut (TGGAU) auf Benutzerkontoobjekten oder auf Computerkontoobjekten in Active Directory-Domänendiensten lesen. Einige Win32-Funktionen machen es einfacher, das TGGAU-Attribut zu lesen. Anwendungen, die dieses Attribut lesen oder eine API aufrufen (die als Funktion bezeichnet wird), die dieses Attribut liest, haben keinen Erfolg, wenn der aufrufende Sicherheitskontext keinen Zugriff auf das Attribut hat. Diese Gruppe wird als SID angezeigt, bis der Domänencontroller als primärer Domänencontroller fungiert und die Betriebsmasterrolle (auch als flexible Einzelmaster-Vorgänge oder FSMO bezeichnet) enthält.

Die Windows-Autorisierungs Zugriffsgruppe gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

Hinweis diese Gruppe kann nicht umbenannt, gelöscht oder verschoben werden.

Diese Sicherheitsgruppe hat sich seit Windows Server 2008 nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-32-560
Typ	Builtin local
Standardcontainer	CN = vordefiniert, DC = <Domäne>, DC =
Standard Mitglieder	Unternehmensdomänencontroller

ATTRIBUT	WERT
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Kann nicht verschoben werden
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	Ja
Standardbenutzerrechte	Keine

WinRMRemoteWMIUsers_

In Windows8 und in Windows Server2012 wurde die Registerkarte **Freigabe** zur Benutzeroberfläche der erweiterten Sicherheitseinstellungen hinzugefügt. Auf dieser Registerkarte werden die Sicherheitseigenschaften einer Remotedateifreigabe angezeigt. Damit diese Informationen angezeigt werden, müssen Sie über die folgenden Berechtigungen und Mitgliedschaften verfügen, wie sinnvoll die Version von Windows Server, auf der der Dateiserver ausgeführt wird.

Die Gruppe WinRMRemoteWMIUsers_ gilt für Versionen des Windows Server-Betriebssystems, die in der [Tabelle Active Directory-Standardsicherheitsgruppen](#) aufgeführt sind.

- Wenn die Dateifreigabe auf einem Server gehostet wird, auf dem eine unterstützte Version des Betriebssystems ausgeführt wird:
 - Sie müssen ein Mitglied der WinRMRemoteWMIUsers__-Gruppe oder der BUILTIN\Administrators-Gruppe sein.
 - Sie benötigen Leseberechtigungen für die Dateifreigabe.
- Wenn die Dateifreigabe auf einem Server gehostet wird, auf dem eine Version von Windows Server ausgeführt wird, die älter als Windows Server2012 ist:
 - Sie müssen ein Mitglied der BUILTIN\Administrators-Gruppe sein.
 - Sie benötigen Leseberechtigungen für die Dateifreigabe.

In Windows Server2012 fügt die Funktion Zugriff verweigerte Unterstützung die Gruppe Authentifizierte Benutzer zur lokalen WinRMRemoteWMIUsers__-Gruppe hinzu. Wenn die Unterstützungsfunktion für Zugriff verweigert aktiviert ist, können alle authentifizierten Benutzer, die über Leseberechtigungen für die Dateifreigabe verfügen, die Dateifreigabeberechtigungen anzeigen.

Hinweis die WinRMRemoteWMIUsers_-Gruppe ermöglicht die Remoteausführung von Windows PowerShell-Befehlen, während die Gruppe [Remote Verwaltungs Benutzer](#) in der Regel verwendet wird, um Benutzern das Verwalten von Servern mithilfe der Server-Manager-Konsole zu ermöglichen.

Diese Sicherheitsgruppe wurde in Windows Server2012 eingeführt und hat sich in späteren Versionen nicht geändert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-21-<Domäne>-1000
Typ	Lokale Domäne
Standardcontainer	CN = Users, DC = <Domäne>, DC =
Standard Mitglieder	Keine
Standardmitglied von	Keine
Geschützt durch ADMINSDHOLDER?	Nein
Sicheres Verschieben des Standardcontainers	Ja
Sicher, dass die Verwaltung dieser Gruppe an nicht-Service-Administratoren delegiert wird?	
Standardbenutzerrechte	Keine

Weitere Informationen

- [Sicherheitsprinzipale](#)
- [Besondere Identitäten](#)
- [Übersicht über die Zugriffssteuerung](#)

Besondere Identitäten

12.09.2019 • 10 minutes to read

Betrifft

- Windows Server 2016

Dieses Referenzthema für den IT-Experten beschreibt die speziellen Identitäts Gruppen (die manchmal als Sicherheitsgruppen bezeichnet werden), die in der Windows-Zugriffssteuerung verwendet werden.

Spezielle Identitäts Gruppen ähneln Active Directory-Sicherheitsgruppen, wie Sie in den Benutzern und integrierten Containern aufgeführt sind. Spezielle Identitäts Gruppen können eine effiziente Möglichkeit bieten, den Zugriff auf Ressourcen in Ihrem Netzwerk zuzuweisen. Mithilfe spezieller Identitäts Gruppen können Sie folgende Aktionen ausführen:

- Zuweisen von Benutzerrechten zu Sicherheitsgruppen in Active Directory.
- Zuweisen von Berechtigungen zu Sicherheitsgruppen zum Zweck des Zugriffs auf Ressourcen.

Auf Servern, auf denen die unterstützten Windows Server-Betriebssysteme ausgeführt werden, die in der Liste "**gilt für**" am Anfang dieses Themas angegeben sind, sind mehrere spezielle Identitäts Gruppen enthalten. Diese speziellen Identitäts Gruppen verfügen nicht über bestimmte Mitgliedschaften, die geändert werden können, Sie können jedoch je nach Situation verschiedene Benutzer zu unterschiedlichen Zeitpunkten darstellen.

Obwohl den speziellen Identitäts Gruppen Rechte und Berechtigungen für Ressourcen zugewiesen werden können, können die Mitgliedschaften nicht geändert oder angezeigt werden. Gruppenbereiche gelten nicht für spezielle Identitäts Gruppen. Benutzer werden diesen speziellen Identitäts Gruppen automatisch zugewiesen, wenn Sie sich anmelden oder auf eine bestimmte Ressource zugreifen.

Informationen zu Sicherheitsgruppen und zum Gruppenbereich finden Sie unter [Active Directory-Sicherheitsgruppen](#).

Die speziellen Identitäts Gruppen werden in den folgenden Tabellen beschrieben:

- [Anonyme Anmeldung](#)
- [Authentifizierter Benutzer](#)
- [Batch](#)
- [Gruppe "Creator"](#)
- [Besitzer des Erstellers](#)
- [Einwahl](#)
- [Digest-Authentifizierung](#)
- [Unternehmensdomänencontroller](#)
- [Jeder](#)
- [Interaktive](#)
- [Lokaler Dienst](#)
- [LocalSystem](#)

- [Netzwerk](#)
- [Netzwerkdienst](#)
- [NTLM-Authentifizierung](#)
- [Andere Organisation](#)
- [Prinzipal selbst](#)
- [Interaktive Remote Anmeldung](#)
- [Beschränkt](#)
- [SChannel-Authentifizierung](#)
- [Dienst](#)
- [Terminal Server-Benutzer](#)
- [Diese Organisation](#)
- [Fenster Manager\Window-Manager-Gruppe](#)

Anonyme Anmeldung

Jeder Benutzer, der über eine anonyme Anmeldung auf das System zugreift, hat die anonyme Anmelde Identität. Diese Identität ermöglicht den anonymen Zugriff auf Ressourcen, beispielsweise auf Webseiten, die auf Unternehmensservern veröffentlicht werden. Die Gruppe Anonymous-Anmeldung ist standardmäßig kein Mitglied der Gruppe Jeder.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-7
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Authentifizierte Benutzer

Jeder Benutzer, der über einen Anmeldeprozess auf das System zugreift, hat die Identität des authentifizierten Benutzers. Diese Identität ermöglicht den Zugriff auf freigegebene Ressourcen in der Domäne, beispielsweise Dateien in einem freigegebenen Ordner, auf die alle Mitarbeiter in der Organisation zugreifen können. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-11
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = System, CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1

ATTRIBUT	WERT
Standardbenutzerrechte	Zugriff auf diesen Computer über das Netzwerk: SeNetworkLogonRight Hinzufügen von Workstations zu einer Domäne: SeMachineAccountPrivilege Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege

Batch

Alle Benutzer oder Prozesse, die auf das System als Stapelverarbeitungsauftrag (oder über die Stapelverarbeitungswarteschlange) zugreifen, weisen die Batch Identität auf. Mit dieser Identität können Stapelverarbeitungsaufträge geplante Aufgaben ausführen, wie etwa ein nächtlicher Cleanup-Auftrag, der temporäre Dateien löscht. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-3
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	keine

Gruppe "Creator"

Die Person, die die Datei oder das Verzeichnis erstellt hat, ist ein Mitglied dieser speziellen Identitäts Gruppe. Windows Server-Betriebssysteme verwenden diese Identität, um dem Ersteller einer Datei oder eines Verzeichnisses automatisch Zugriffsberechtigungen zuzuweisen.

In einem vererbaren Zugriffssteuerungseintrag (ACE) wird eine Platzhalter-Sicherheits-ID (Security Identifier, SID) erstellt. Beim Erben des ACE ersetzt das System diese SID durch die sid für die primäre Gruppe des aktuellen Besitzers des Objekts. Die primäre Gruppe wird nur vom POSIX-Subsystem (Portable Operating System Interface für UNIX) verwendet.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-3-1
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	keine

Besitzer des Erstellers

Die Person, die die Datei oder das Verzeichnis erstellt hat, ist ein Mitglied dieser speziellen Identitäts Gruppe. Windows Server-Betriebssysteme verwenden diese Identität, um dem Ersteller einer Datei oder eines

Verzeichnisses automatisch Zugriffsberechtigungen zuzuweisen. Eine Platzhalter-sid wird in einem vererbbaeren ACE erstellt. Wenn der ACE geerbt wird, ersetzt das System diese SID durch die SID des aktuellen Besitzers des Objekts.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-3-0
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	keine

Einwahl

Jeder Benutzer, der über eine DFÜ-Verbindung auf das System zugreift, verfügt über die DFÜ-Identität. Diese Identität unterscheidet DFÜ-Benutzer von anderen Arten von authentifizierten Benutzern.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-1
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	keine

Digest-Authentifizierung

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-64-21
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	keine

Unternehmensdomänencontroller

Diese Gruppe umfasst alle Domänencontroller in einer Active Directory-Gesamtstruktur. Domänencontroller mit unternehmensweiten Rollen und Zuständigkeiten verfügen über die Identität des Enterprise-Domänencontrollers. Mit dieser Identität können Sie bestimmte Aufgaben im Unternehmen mithilfe von transitiven Vertrauensstellungen durchführen. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-9
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Zugriff auf diesen Computer über das Netzwerk: SeNetworkLogonRight Lokales anmelden zulassen: SeInteractiveLogonRight

Jeder

Alle interaktiven, Netzwerk-, DFÜ- und authentifizierten Benutzer sind Mitglieder der Gruppe Jeder. Diese spezielle Identitäts Gruppe bietet umfassenden Zugriff auf Systemressourcen. Wenn sich ein Benutzer beim Netzwerk anmeldet, wird der Benutzer automatisch zur Gruppe "jeder" hinzugefügt.

Auf Computern, auf denen Windows 2000 und früher ausgeführt wird, enthalten die Gruppe jeder die Gruppe Anonymous-Anmeldung als Standardmitglied, aber ab windowsserver2003 enthält die Gruppe jeder nur authentifizierte Benutzer und Gäste; und es enthält standardmäßig keine anonyme Anmeldung mehr (auch wenn dies geändert werden kann).

Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-1-0
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Zugriff auf diesen Computer über das Netzwerk: SeNetworkLogonRight Als Teil des Betriebssystems fungieren: SeTcbPrivilege Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege

Interaktive

Alle Benutzer, die am lokalen System angemeldet sind, verfügen über die interaktive Identität. Mit dieser Identität können nur lokale Benutzer auf eine Ressource zugreifen. Wenn ein Benutzer auf eine bestimmte Ressource auf dem Computer zugreift, an dem Sie zurzeit angemeldet sind, wird der Benutzer automatisch zur interaktiven Gruppe hinzugefügt. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-4
Objektklasse	Foreign Security Principal

ATTRIBUT	WERT
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Lokaler Dienst

Das lokale Dienstkonto ist mit einem authentifizierten Benutzerkonto vergleichbar. Das lokale Dienstkonto hat dieselbe Zugriffsebene auf Ressourcen und Objekte wie Mitglieder der Gruppe "Benutzer". Durch diesen eingeschränkten Zugriff können Sie Ihr System schützen, wenn einzelne Dienste oder Prozesse gefährdet sind. Dienste, die als Lokales Dienstkonto ausgeführt werden, greifen als NULL-Sitzung mit anonymen Anmeldeinformationen auf Netzwerkressourcen zu. Der Name des Kontos ist NT AUTHORITY\LocalService. Dieses Konto hat kein Kennwort.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-19
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	<p>Anpassen von Speicherkontingenten für einen Prozess: SeIncreaseQuotaPrivilege</p> <p>Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege</p> <p>Ändern der Systemzeit: SeSystemtimePrivilege</p> <p>Ändern der Zeitzone: SeTimeZonePrivilege</p> <p>Erstellen globaler Objekte: SeCreateGlobalPrivilege</p> <p>Generieren von Sicherheitsüberprüfungen: SeAuditPrivilege</p> <p>Identitätswechsel zwischen einem Client und der Authentifizierung: SeImpersonatePrivilege</p> <p>Ersetzen eines Tokens auf Prozessebene: SeAssignPrimaryTokenPrivilege</p>

LocalSystem

Hierbei handelt es sich um ein Dienstkonto, das vom Betriebssystem verwendet wird. Das LocalSystem-Konto ist ein leistungsfähiges Konto mit Vollzugriff auf das System und fungiert als Computer im Netzwerk. Wenn sich ein Dienst beim LocalSystem-Konto auf einem Domänencontroller anmeldet, hat dieser Dienst Zugriff auf die gesamte Domäne. Einige Dienste sind standardmäßig so konfiguriert, dass Sie sich beim LocalSystem-Konto anmelden. Ändern Sie nicht die Standardeinstellung für den Dienst. Der Name des Kontos ist "LocalSystem". Dieses Konto hat kein Kennwort.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-18
Objektklasse	Foreign Security Principal

ATTRIBUT	WERT
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Netzwerk

Diese Gruppe enthält implizit alle Benutzer, die über eine Netzwerkverbindung angemeldet sind. Jeder Benutzer, der über ein Netzwerk auf das System zugreift, hat die Netzwerkidentität. Mit dieser Identität können nur Remotebenutzer auf eine Ressource zugreifen. Wenn ein Benutzer über das Netzwerk auf eine bestimmte Ressource zugreift, wird der Benutzer automatisch zur Gruppe Netzwerk hinzugefügt. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-2
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Netzwerkdienst

Das Netzwerkdienstkonto ist mit einem authentifizierten Benutzerkonto vergleichbar. Das Netzwerkdienstkonto hat dieselbe Zugriffsebene auf Ressourcen und Objekte wie Mitglieder der Gruppe "Benutzer". Durch diesen eingeschränkten Zugriff können Sie Ihr System schützen, wenn einzelne Dienste oder Prozesse gefährdet sind. Dienste, die als Netzwerkdienstkonto ausgeführt werden, greifen mithilfe der Anmeldeinformationen des Computerkontos auf Netzwerkressourcen zu. Der Name des Kontos lautet NTAUTHORITY\NetworkService. Dieses Konto hat kein Kennwort.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-20
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	<p>Anpassen von Speicherkontingenten für einen Prozess: SeIncreaseQuotaPrivilege</p> <p>Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege</p> <p>Erstellen globaler Objekte: SeCreateGlobalPrivilege</p> <p>Generieren von Sicherheitsüberprüfungen: SeAuditPrivilege</p> <p>Identitätswechsel zwischen einem Client und der Authentifizierung: SeImpersonatePrivilege</p> <p>Ersetzen eines Tokens auf Prozessebene: SeAssignPrimaryTokenPrivilege</p>

NTLM-Authentifizierung

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-64-10
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Andere Organisation

Diese Gruppe enthält implizit alle Benutzer, die über eine DFÜ-Verbindung am System angemeldet sind. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-1000
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Prinzipal selbst

Dieser Identifizierer ist ein Platzhalter in einem ACE für ein Benutzer-, Gruppen-oder Computerobjekt in Active Directory. Wenn Sie dem Prinzipal selbst Berechtigungen erteilen, erteilen Sie diesen dem Sicherheitsprinzipal, der durch das Objekt dargestellt wird. Während einer Zugriffsüberprüfung ersetzt das Betriebssystem die sid für Principal Self durch die SID des Sicherheitsprinzipals, der durch das Objekt dargestellt wird.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-10
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Interaktive Remote Anmeldung

Diese Identität stellt alle Benutzer dar, die derzeit mit einer Remote Desktop Verbindung an einem Computer angemeldet sind. Diese Gruppe ist eine Teilmenge der interaktiven Gruppe. Zugriffstoken, die die SID der interaktiven Remote Anmeldung enthalten, enthalten auch die interaktive sid.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-14
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Beschränkt

Benutzer und Computer mit eingeschränkten Funktionen verfügen über die eingeschränkte Identität. Diese Identitäts Gruppe wird von einem Prozess verwendet, der in einem eingeschränkten Sicherheitskontext ausgeführt wird, beispielsweise beim Ausführen einer Anwendung mit dem runas-Dienst. Wenn Code auf der eingeschränkten Sicherheitsstufe ausgeführt wird, wird die eingeschränkte SID dem Zugriffstoken des Benutzers hinzugefügt.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-12
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

SChannel-Authentifizierung

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-64-14
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Dienst

Jeder Dienst, der auf das System zugreift, verfügt über die Dienstidentität. Diese Identitäts Gruppe umfasst alle Sicherheitsprinzipale, die als Dienst angemeldet sind. Diese Identität gewährt Zugriff auf Prozesse, die von Windows Server-Diensten ausgeführt werden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-6
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Erstellen globaler Objekte: SeCreateGlobalPrivilege Identitätswechsel zwischen einem Client und der Authentifizierung: SelpersonatePrivilege

Terminal Server-Benutzer

Jeder Benutzer, der über die Terminaldienste auf das System zugreift, verfügt über die Benutzeridentität des Terminalservers. Diese Identität ermöglicht Benutzern den Zugriff auf Terminalserver Anwendungen und die Ausführung anderer erforderlicher Aufgaben mit Terminalserver Diensten. Die Mitgliedschaft wird vom Betriebssystem gesteuert.

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-13
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Diese Organisation

ATTRIBUT	WERT
Bekannte SID/Rid	S-1-5-15
Objektklasse	Foreign Security Principal
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Keine

Fenster Manager\Window-Manager-Gruppe

ATTRIBUT	WERT
Bekannte SID/Rid	
Objektklasse	

ATTRIBUT	WERT
Standardspeicherort in Active Directory	CN = bekannte Sicherheitsprinzipale, CN = Konfiguration, DC = \ <forestRootDomain \ #a1
Standardbenutzerrechte	Umgehen der Durchquerung Überprüfung: SeChangeNotifyPrivilege Erhöhen des Arbeitssatzes eines Prozesses: SeIncreaseWorkingSetPrivilege

Weitere Informationen:

- [Active Directory-Sicherheitsgruppen](#)
- [Sicherheitsprinzipale](#)
- [Übersicht über die Zugriffssteuerung](#)

Benutzerkontensteuerung

12.09.2019 • 2 minutes to read

Betrifft

- Windows10
- Windows Server2016

Die Benutzerkontensteuerung (User Account Control, UAC) schützt davor, dass Schadsoftware einen PC beschädigt, und unterstützt Unternehmen bei der Bereitstellung einer besser verwalteten Desktopumgebung. Mit der Benutzerkontensteuerung werden Apps und Aufgaben immer im Sicherheitskontext eines Kontos ohne Administratorrechte ausgeführt, es sei denn, ein Administrator autorisiert speziell den Zugriff auf Administratorebene auf das System. Die Benutzerkontensteuerung kann die automatische Installation nicht autorisierter Apps blockieren und unbeabsichtigte Änderungen an Systemeinstellungen verhindern.

Mithilfe der Benutzerkontensteuerung können sich alle Benutzer an ihren Computern mit einem Standardbenutzerkonto anmelden. Mit einem standardmäßigen Benutzertoken gestartete Prozesse führen möglicherweise Aufgaben unter Verwendung von Zugriffsrechten eines Standardbenutzers aus. Windows-Explorer erbt z. B. automatisch Berechtigungen auf Standardbenutzerebene. Außerdem werden alle Apps, die mit Windows-Explorer gestartet werden (z. B. durch Doppelklicken auf eine Verknüpfung), auch mit dem Standardsatz von Benutzerberechtigungen ausgeführt. Viele Apps, auch die im Betriebssystem enthaltenen, können auf diese Weise ordnungsgemäß funktionieren.

Andere Apps, insbesondere solche, die nicht speziell unter Berücksichtigung von Sicherheitseinstellungen konzipiert wurden, benötigen häufig zur erfolgreichen Ausführung zusätzliche Berechtigungen. Diese Arten von Apps werden als Legacy-Apps bezeichnet. Darüber hinaus erfordern Aktionen wie das Installieren neuer Software und Änderungen der Konfiguration in der Windows-Firewall mehr als für die ein Standardbenutzerkonto verfügbaren Berechtigungen.

Wenn eine App mit mehr als den Standardbenutzerrechten ausgeführt werden muss, kann die Benutzerkontensteuerung weitere Benutzergruppen für das Token wiederherstellen. Dies ermöglicht dem Benutzer die explizite Steuerung von Apps, die auf Systemebene Änderungen am Computer oder Gerät vornehmen.

Praktische Anwendungsfälle

Mit dem Administratorgenehmigungsmodus in der Benutzerkontensteuerung wird verhindert, dass Schadsoftware ohne Wissen eines Administrators automatisch installiert wird. Darüber hinaus wird der Schutz vor unbeabsichtigten systemweiten Änderungen sichergestellt. Schließlich kann ein höherer Kompatibilitätsgrad erzwungen werden, beim dem Administratoren jedem administrativen Prozess aktiv zustimmen oder dafür Anmeldeinformationen angeben müssen.

In diesem Abschnitt

THEMA	BESCHREIBUNG
Funktionsweise der Benutzerkontensteuerung	Die Benutzerkontensteuerung (User Account Control, UAC) ist ein grundlegender Baustein der Gesamtsicherheitsvision von Microsoft. UAC hilft dabei, die Auswirkung von Schadsoftware zu verringern.

THEMA	BESCHREIBUNG
Sicherheitsrichtlinieneinstellungen für die Benutzerkontensteuerung	<p>Sie können mithilfe von Sicherheitsrichtlinien die Funktionsweise der Benutzerkontensteuerung in Ihrer Organisation konfigurieren. Diese Richtlinien können lokal über das Snap-In „Lokale Sicherheitsrichtlinie“ (secpol.msc) oder mithilfe der Gruppenrichtlinie für die Domäne, eine Organisationseinheit oder für spezifische Gruppen konfiguriert werden.</p>
Gruppenrichtlinien und Einstellungen für Registrierungsschlüssel zur Benutzerkontensteuerung	<p>Nachstehend finden Sie eine Liste der UAC-Gruppenrichtlinien und der Einstellungen von Registrierungsschlüsseln zur Benutzerkontensteuerung, die Sie zum Verwalten der Benutzerkontensteuerung in Ihrem Unternehmen verwenden können.</p>

Funktionsweise der Benutzerkontensteuerung

12.09.2019 • 13 minutes to read

Betrifft

- Windows 10

Die Benutzerkontensteuerung (User Account Control, UAC) ist ein grundlegender Baustein der Gesamtsicherheitsvision von Microsoft. UAC hilft dabei, die Auswirkung von Schadsoftware zu verringern.

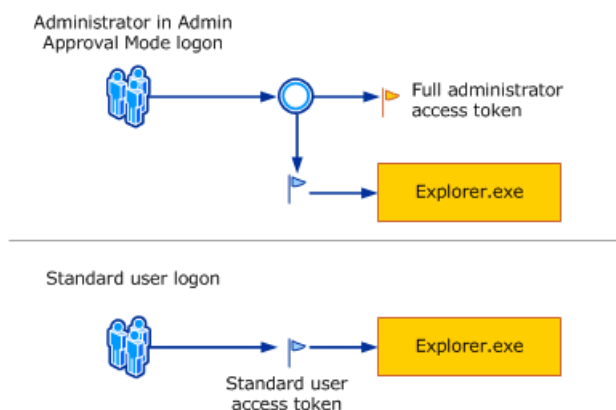
UAC-Prozess und Interaktionen

Jede APP, für die das Administratorzugriffstoken erforderlich ist, muss zur Zustimmung aufgefordert werden. Die einzige Ausnahme ist die Beziehung zwischen über- und untergeordneten Prozessen. Untergeordnete Prozesse erben das Zugriffstoken des Benutzers vom übergeordneten Prozess. Sowohl die übergeordneten als auch die untergeordneten Prozesse müssen jedoch die gleiche Integritätsstufe aufweisen. Windows10 schützt Prozesse durch kennzeichnen ihrer Integritätsstufen. Integritätsstufen sind vertrauenswürdige Maße. Eine "hoch"-Integritäts Anwendung ist eine Anwendung, die Aufgaben ausführt, die Systemdaten wie eine Datenträger Partitionierungs Anwendung ändern, während eine "niedrige" Integritäts Anwendung eine Aufgabe ausführt, die Aufgaben ausführt, die potenziell das Betriebssystem gefährden können, beispielsweise einen Webbrowser. Apps mit niedrigeren Integritätsebenen können Daten in Anwendungen mit höheren Integritätsebenen nicht ändern. Wenn ein Standardbenutzer versucht, eine APP auszuführen, die ein Administratorzugriffstoken erfordert, erfordert UAC, dass der Benutzer gültige Administratoranmeldeinformationen bereitstellt.

Um besser zu verstehen, wie dieser Vorgang erfolgt, sehen wir uns den Windows-Anmeldeprozess an.

Anmeldeprozess

Im folgenden wird gezeigt, wie sich der Anmeldevorgang für einen Administrator vom Anmeldevorgang für einen Standardbenutzer unterscheidet.



Standardbenutzer und-Administratoren greifen standardmäßig auf Ressourcen zu und führen apps im Sicherheitskontext von Standardbenutzern aus. Wenn sich ein Benutzer an einem Computer anmeldet, erstellt das System ein Zugriffstoken für diesen Benutzer. Das Zugriffstoken enthält Informationen über die Zugriffsebene, die dem Benutzer gewährt wird, einschließlich spezifischer Sicherheits-IDs (SIDs) und Windows-Berechtigungen.

Wenn sich ein Administrator anmeldet, werden zwei separate Zugriffstoken für den Benutzer erstellt: ein Standardbenutzerzugriffstoken und ein Administratorzugriffstoken. Das Standardbenutzerzugriffstoken enthält dieselben benutzerspezifischen Informationen wie das Administratorzugriffstoken, aber die Administrator-Windows-Berechtigungen und-SIDs werden entfernt. Das Standardbenutzerzugriffstoken wird verwendet, um apps zu starten, die keine administrativen Aufgaben ausführen (Standardbenutzer-Apps). Das standardmäßige

Benutzerzugriffstoken wird dann verwendet, um den Desktop anzuzeigen (Explorer.exe). Explorer.exe ist der übergeordnete Prozess, aus dem alle anderen vom Benutzer initiierten Prozesse das Zugriffstoken erben. Infolgedessen werden alle Apps als Standardbenutzer ausgeführt, es sei denn, ein Benutzer erteilt eine Zustimmung oder Anmeldeinformationen, um eine App zur Verwendung eines vollständigen administrativen Zugriffstokens zu genehmigen.

Ein Benutzer, der Mitglied der Gruppe Administratoren ist, kann sich bei Verwendung eines Standardbenutzer Zugriffstokens anmelden, im Internet surfen und e-Mails lesen. Wenn der Administrator eine Aufgabe ausführen muss, die das Administratorzugriffstoken erfordert, fordert Windows 10 den Benutzer automatisch zur Genehmigung auf. Diese Aufforderung wird als Eingabeaufforderung für erhöhte Rechte bezeichnet, und ihr Verhalten kann mithilfe des Snap-ins lokale Sicherheitsrichtlinie (secpol.msc) oder der Gruppenrichtlinie konfiguriert werden. Weitere Informationen finden Sie unter [Sicherheitsrichtlinieneinstellungen für die Benutzerkontensteuerung](#).

Die UAC-Benutzeroberfläche

Wenn UAC aktiviert ist, unterscheidet sich die Benutzeroberfläche für Standardbenutzer von den Administratoren im Administratorgenehmigungsmodus. Die empfohlene und sicherere Methode zum Ausführen von Windows 10 besteht darin, das primäre Benutzerkonto zu einem Standardbenutzerkonto zu machen. Die Ausführung als Standardbenutzer hilft, die Sicherheit für eine verwaltete Umgebung zu maximieren. Mit der integrierten UAC-Erweiterungskomponente können Standardbenutzer problemlos eine administrative Aufgabe durchführen, indem Sie gültige Anmeldeinformationen für ein lokales Administratorkonto eingeben. Die standardmäßig integrierte UAC-Erweiterungskomponente für Standardbenutzer ist die Eingabeaufforderung für Anmeldeinformationen.

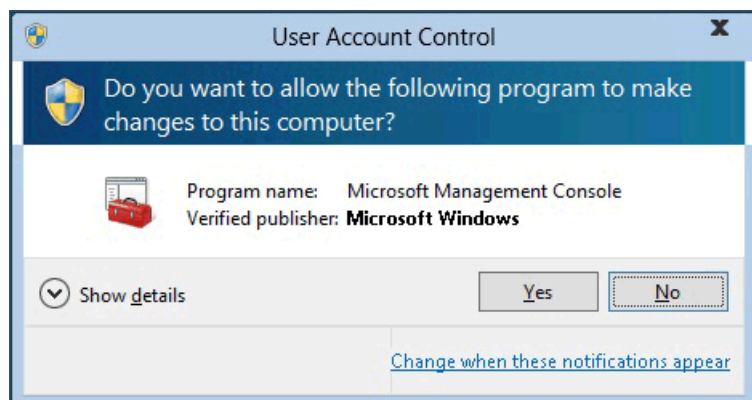
Die Alternative zur Ausführung als Standardbenutzer ist die Ausführung als Administrator im Administratorgenehmigungsmodus. Mit der integrierten UAC-elevations Komponente können Mitglieder der lokalen Administratorengruppe problemlos eine administrative Aufgabe durch eine Genehmigung durchführen. Die standardmäßig integrierte UAC-Erweiterungskomponente für ein Administratorkonto im Administratorgenehmigungsmodus wird als Zustimmungsaufforderung bezeichnet.

Die Eingabeaufforderungen für Zustimmung und Anmeldeinformationen

Wenn UAC aktiviert ist, fordert Windows 10 zur Genehmigung auf oder fordert die Anmeldeinformationen eines gültigen lokalen Administratorkontos an, bevor ein Programm oder eine Aufgabe gestartet wird, für die ein vollständiges Administratorzugriffstoken erforderlich ist. Mit dieser Aufforderung wird sichergestellt, dass keine bösartige Software automatisch installiert werden kann.

Die Zustimmungsaufforderung

Die Eingabeaufforderung zur Zustimmung wird angezeigt, wenn ein Benutzer versucht, eine Aufgabe auszuführen, für die ein Administratorzugriffstoken eines Benutzers erforderlich ist. Der folgende Code ist ein Beispiel für die Eingabeaufforderung zur UAC-Zustimmung.

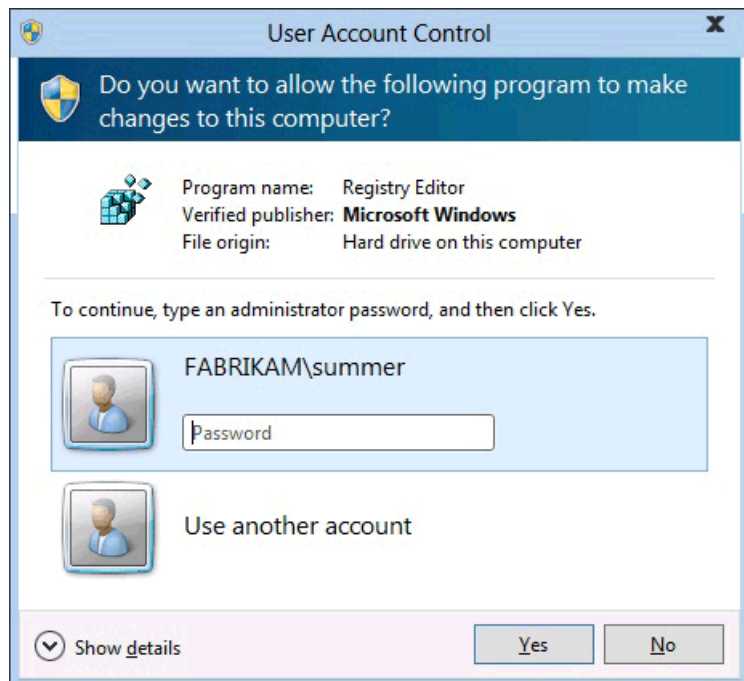


Eingabeaufforderung für Anmeldeinformationen

Die Anmelde Informations Aufforderung wird angezeigt, wenn ein Standardbenutzer versucht, eine Aufgabe

auszuführen, für die ein Administratorzugriffstoken des Benutzers erforderlich ist. Administratoren können auch Ihre Anmeldeinformationen angeben, indem Sie die **Benutzerkontensteuerung: Verhalten der Aufforderung zur Erhöhung der erhöhten Rechte für Administratoren im** Richtlinien Einstellungswert für den Administratorgenehmigungsmodus so festlegen, dass **Anmeldeinformationen angefordert** werden.

Der folgende Code ist ein Beispiel für die Eingabeaufforderung für UAC-Anmeldeinformationen.



UAC-Erweiterungs Ansagen

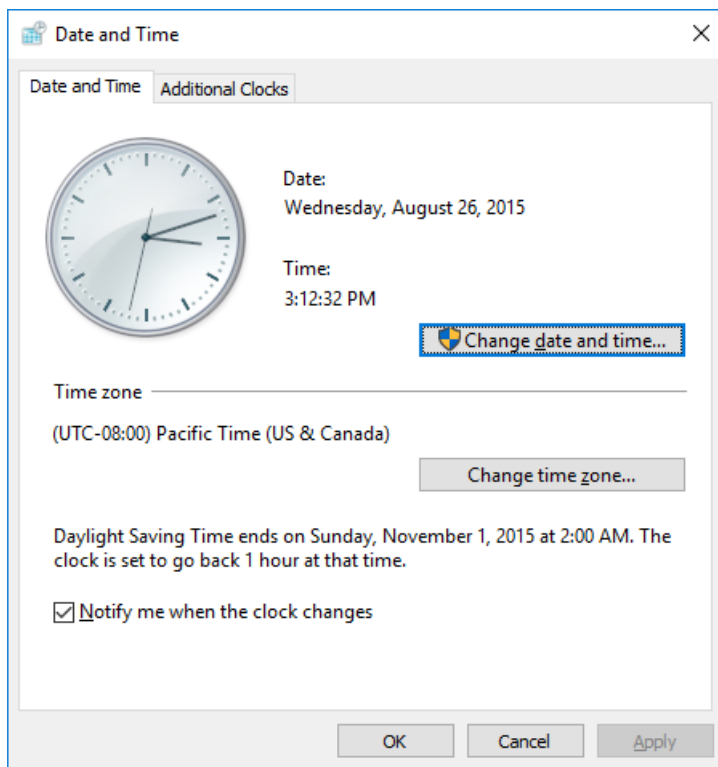
Die UAC-Erhöungs Ansagen sind farbcodiert, um App-spezifisch zu sein, sodass eine sofortige Identifizierung des potenziellen Sicherheitsrisikos einer Anwendung möglich ist. Wenn eine APP versucht, mit dem Vollzugriff-Token eines Administrators auszuführen, analysiert Windows10 zuerst die ausführbare Datei, um den Verleger zu ermitteln. Apps werden zunächst in drei Kategorien aufgeteilt, die auf dem Herausgeber der Datei basieren: Windows10, Herausgeber überprüft (signiert) und Publisher nicht überprüft (nicht signiert). Das folgende Diagramm veranschaulicht, wie Windows10 bestimmt, welche Farb Anhebung für den Benutzer angezeigt werden soll.

Die Farbcodierung für die Eingabeaufforderung mit erhöhten Rechten lautet wie folgt:

- Roter Hintergrund mit einem roten Schild Symbol: die APP wird von der Gruppenrichtlinie blockiert oder stammt von einem blockierten Herausgeber.
- Blauer Hintergrund mit einem blauen und goldenen Schild Symbol: die Anwendung ist eine administrative Windows10-APP, beispielsweise ein Element der Systemsteuerung.
- Blauer Hintergrund mit einem blauen Schild Symbol: die Anwendung wird mit Authenticode signiert und vom lokalen Computer als vertrauenswürdig eingestuft.
- Gelber Hintergrund mit einem gelben Schild Symbol: die Anwendung ist nicht signiert oder signiert, aber vom lokalen Computer noch nicht als vertrauenswürdig eingestuft.

Schildsymbol

Einige Elemente der Systemsteuerung, beispielsweise **Datums-und Uhrzeiteigenschaften**, enthalten eine Kombination aus Administrator-und Standardbenutzervorgängen. Standard Benutzer können die Uhr anzeigen und die Zeitzone ändern, aber ein vollständiges Administratorzugriffstoken ist erforderlich, um die lokale Systemzeit zu ändern. Im folgenden sehen Sie einen Screenshot des Elements " **Datums-und Uhrzeiteigenschaften** ".



Das Symbol "Schild" auf der Schaltfläche "**Datum und Uhrzeit ändern**" gibt an, dass für den Prozess ein vollständiger Administratorzugriffstoken erforderlich ist und eine Eingabeaufforderung zur Erhöhung der UAC angezeigt wird.

Sichern der Eingabeaufforderung für erhöhte Rechte

Der Elevation-Prozess wird weiter gesichert, indem die Eingabeaufforderung an den sicheren Desktop weitergeleitet wird. Die Eingabeaufforderungen für die Zustimmung und die Anmeldeinformationen werden standardmäßig auf dem sicheren Desktop in Windows 10 angezeigt. Nur Windows-Prozesse können auf den sicheren Desktop zugreifen. Für höhere Sicherheit empfiehlt es sich, die **Benutzerkontensteuerung zu verwenden: Wechseln Sie zum sicheren Desktop, wenn Sie aufgefordert werden**, die Einstellung für die Ansichts Richtlinien zu aktivieren.

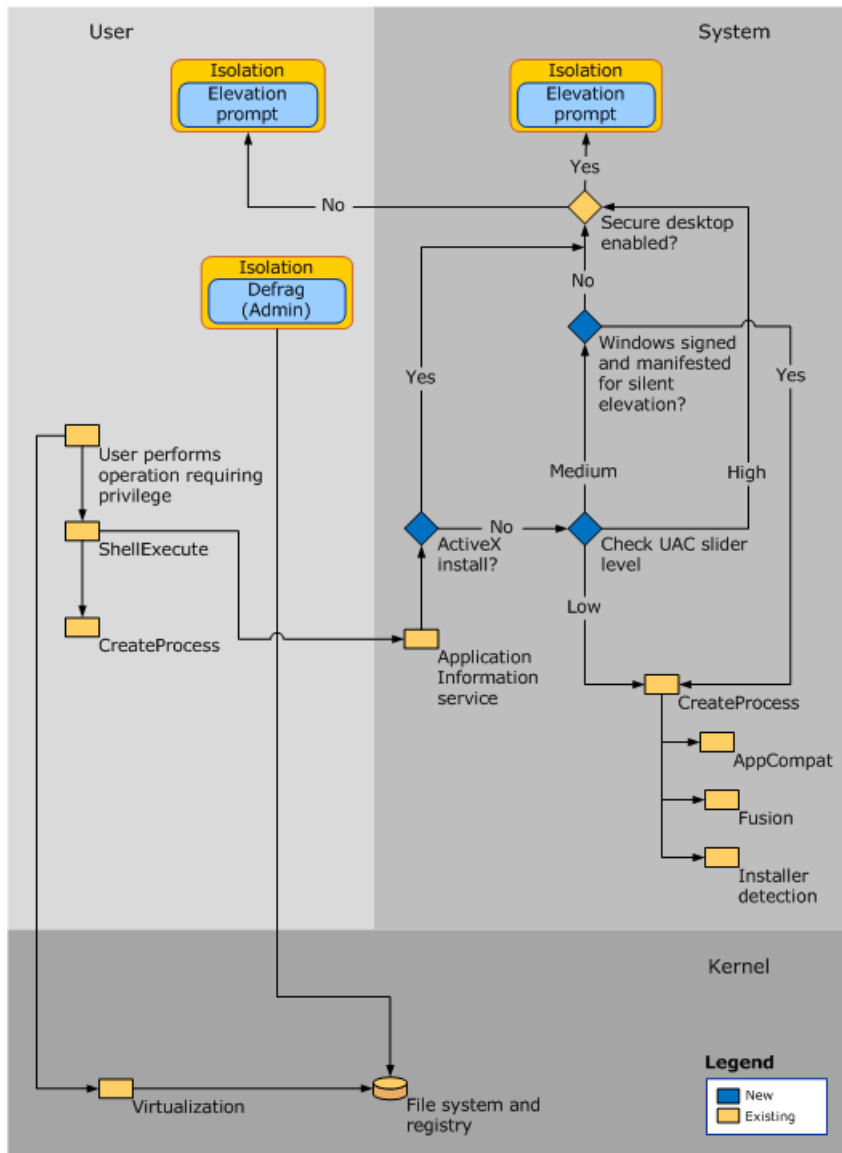
Wenn eine ausführbare Datei eine Anhebung anfordert, wird der interaktive Desktop, auch als Benutzerdesktop bezeichnet, auf den sicheren Desktop umgeschaltet. Der sichere Desktop verdunkelt den Benutzerdesktop und zeigt eine Eingabeaufforderung mit erhöhten Rechten an, auf die Sie Antworten müssen, bevor Sie fortfahren. Wenn der Benutzer auf **Ja** oder **Nein** klickt, wechselt der Desktop wieder zum Benutzerdesktop.

Schadsoftware kann eine Nachahmung des sicheren Desktops darstellen, doch wenn die Richtlinieneinstellung "**Benutzerkontensteuerung" für Administratoren im Administratorgenehmigungsmodus** auf "**Zustimmung bestätigen**" festgelegt ist, erhält die Malware keine Erhöhung. Wenn der Benutzer auf "**Ja**" auf der Nachahmung klickt. Wenn die Richtlinieneinstellung auf **Aufforderung zur Eingabe von Anmeldeinformationen** festgelegt ist, können Malware, die die Anmeldeaufforderung imitiert, möglicherweise die Anmeldeinformationen des Benutzers sammeln. Die Malware erhält jedoch keine erhöhten Rechte, und das System verfügt über andere Schutzmaßnahmen, die Schadsoftware verhindern, dass die Benutzeroberfläche selbst mit einem geernteten Kennwort gesteuert wird.

Während Malware eine Nachahmung des sicheren Desktops darstellen kann, kann dieses Problem nur auftreten, wenn ein Benutzer die Schadsoftware zuvor auf dem PC installiert hat. Da Prozesse, für die ein Administratorzugriffstoken erforderlich ist, nicht automatisch installiert werden können, wenn UAC aktiviert ist, muss der Benutzer ausdrücklich zustimmen, indem er auf **Ja** oder durch die Bereitstellung von Administratoranmeldeinformationen klickt. Das spezifische Verhalten der UAC-Eingabeaufforderung für erhöhte Rechte hängt von der Gruppenrichtlinie ab.

UAC-Architektur

Das folgende Diagramm erläutert die UAC-Architektur.



Wenn Sie die einzelnen Komponenten besser verstehen möchten, lesen Sie die folgende Tabelle:

KOMPONENTE	BESCHREIBUNG
Benutzer	
Der Benutzer führt eine Operation aus, die ein Privileg erfordert	Wenn der Vorgang das Dateisystem oder die Registrierung ändert, wird Virtualisierung aufgerufen. Alle anderen Vorgänge rufen ShellExecute auf.
ShellExecute	ShellExecute ruft CreateProcess auf. ShellExecute sucht nach dem ERROR_ELEVATION_REQUIRED-Fehler von CreateProcess. Wenn der Fehler empfangen wird, ruft ShellExecute den Anwendungsinformationsdienst auf, um zu versuchen, die angeforderte Aufgabe mit der Eingabeaufforderung mit erhöhten Rechten auszuführen.

CreateProcess	Wenn für die Anwendung Elevation erforderlich ist, lehnt CreateProcess den Anruf mit ERROR_ELEVATION_REQUIRED ab.
System	
Anwendungsinformationsdienst	Ein Systemdienst, der das Starten von apps unterstützt, die eine oder mehrere erhöhte Rechte oder Benutzerrechte zum Ausführen erfordern, wie etwa lokale Verwaltungsaufgaben und apps, die höhere Integritätsstufen erfordern. Der Anwendungsinformationsdienst unterstützt Sie beim Starten solcher apps, indem Sie einen neuen Prozess für die Anwendung mit einem Vollzugriffstoken für Administratoren's erstellen, wenn die Höhe erforderlich ist und der Benutzer (je nach Gruppenrichtlinie) die Zustimmung dazu erhält.
Erhöhen einer ActiveX-Installation	Wenn ActiveX nicht installiert ist, überprüft das System die Schieberegler-Ebene des UAC. Wenn ActiveX installiert ist, wird die Benutzerkontensteuerung: zum Sichern des Desktops wechseln, wenn die Gruppenrichtlinieneinstellung für erhöhte Ansicht aufgefordert wird.

UAC verfügt über einen Schieberegler zur Auswahl von vier Benachrichtigungsebenen.

- **Immer benachrichtigen :**

- Sie werden benachrichtigt, wenn Programme versuchen, Software zu installieren oder Änderungen an Ihrem Computer vorzunehmen.
- Sie werden benachrichtigt, wenn Sie Änderungen an den Windows-Einstellungen vornehmen.
- Fixieren Sie andere Aufgaben, bis Sie Antworten.

Empfohlen, wenn Sie häufig neue Software installieren oder unbekannte Websites besuchen.

- **Nur benachrichtigen, wenn Programme versuchen, Änderungen an meinem Computer vorzunehmen:**

- Sie werden benachrichtigt, wenn Programme versuchen, Software zu installieren oder Änderungen an Ihrem Computer vorzunehmen.
- Sie werden nicht benachrichtigt, wenn Sie Änderungen an den Windows-Einstellungen vornehmen.
- Fixieren Sie andere Aufgaben, bis Sie Antworten.

Empfohlen, wenn Sie nicht häufig apps installieren oder unbekannte Websites besuchen.

- **Nur benachrichtigen, wenn Programme versuchen, Änderungen an meinem Computer vorzunehmen (meinen Desktop nicht zu dimmen) :**

- Sie werden benachrichtigt, wenn Programme versuchen, Software zu installieren oder Änderungen an Ihrem Computer vorzunehmen.
- Sie werden nicht benachrichtigt, wenn Sie Änderungen an den Windows-Einstellungen vornehmen.
- Fixieren Sie andere Aufgaben erst, wenn Sie Antworten.

Nicht empfehlenswert. Wählen Sie diese Option nur aus, wenn es lange dauert, den Desktop auf Ihrem Computer zu dimmen.

- **Benachrichtigen Sie niemals (deaktivieren Sie die UAC-Eingabeaufforderungen):**

- Sie werden nicht benachrichtigt, wenn Programme versuchen, Software zu installieren oder Änderungen an Ihrem Computer vorzunehmen.
- Sie werden nicht benachrichtigt, wenn Sie Änderungen an den Windows-Einstellungen vornehmen.
- Fixieren Sie andere Aufgaben erst, wenn Sie Antworten.

Aus Sicherheitsgründen nicht empfohlen.

Sicherer Desktop aktiviert	<p>Die Benutzerkontensteuerung: zum sicheren Desktop wechseln, wenn die Einstellung für die Ansichts Richtlinien Aufforderung aktiviert ist:</p> <ul style="list-style-type: none"> • Wenn der sichere Desktop aktiviert ist, werden alle elevations Anforderungen unabhängig von den Richtlinieneinstellungen für das Verhalten von Eingabeaufforderungen für Administratoren und Standardbenutzer an den sicheren Desktop weitergegeben. • Wenn der sichere Desktop nicht aktiviert ist, werden alle Ansichts Anforderungen auf dem Desktop des interaktiven Benutzers', und die Benutzereinstellungen für Administratoren und Standardbenutzer werden verwendet.
CreateProcess	CreateProcess Ruft die AppCompat-, Fusion-und Installationsprogrammerkennung auf, um festzustellen, ob die APP Elevation erfordert. Die Datei wird dann überprüft, um die angeforderte Ausführungsebene zu ermitteln, die im Anwendungsmanifest für die Datei gespeichert ist. CreateProcess schlägt fehl, wenn die im Manifest angegebene angeforderte Ausführungsebene nicht dem Zugriffstoken entspricht, und gibt einen Fehler (ERROR_ELEVATION_REQUIRED) an ShellExecute zurück.
AppCompat	Die AppCompat-Datenbank speichert Informationen in den Anwendungskompatibilitätskorrektur-Einträgen für eine Anwendung.
Fusion	Die Fusion-Datenbank speichert Informationen aus Anwendungsmanifesten, in denen die Anwendungen beschrieben werden. Das Manifest-Schema wird aktualisiert, um ein neues angeforderte Feld für die Ausführungsebene hinzuzufügen.
Installationsprogrammerkennung	Bei der Installationsprogrammerkennung werden Setupdateien erkannt, wodurch verhindert wird, dass Installationen ausgeführt werden, ohne dass die Kenntnisse und Zustimmung des Benutzers'.
Kernel	
Virtualisierung	Durch die Virtualisierungstechnologie wird sichergestellt, dass nicht konforme apps nicht automatisch ausgeführt werden oder fehlschlagen, sodass die Ursache nicht ermittelt werden kann. UAC bietet auch Datei-und Registrierungs-Virtualisierung und Protokollierung für Anwendungen, die in geschützte Bereiche schreiben.

Dateisystem und Registrierung	Die benutzerspezifische Datei- und Registrierungs-Virtualisierung leitet die Registrierungs- und Datei Schreib Anforderungen pro Computer an gleichwertige Speicherorte für einzelne Benutzer um. Leseanforderungen werden zuerst an den virtualisierten Standort pro Benutzer und an den Standort pro Computer weitergeleitet.
-------------------------------	---

Der Schieberegler schaltet die UAC niemals komplett aus. Wenn Sie die Benachrichtigung so **einstellen**, dass Sie nie benachrichtigt wird, wird Folgendes folgen:

- Führen Sie die Ausführung des UAC-Diensts aus.
- Bewirken, dass alle von Administratoren initiierten Ansichts Anforderungen automatisch genehmigt werden, ohne dass eine UAC-Eingabeaufforderung angezeigt wird.
- Alle elevations Anforderungen für Standardbenutzer werden automatisch verweigert.

Wichtig: Um die UAC vollständig zu deaktivieren, müssen Sie die Richtlinie- **Benutzerkontensteuerung deaktivieren: alle Administratoren im Administratorgenehmigungsmodus ausführen**.

Warnung: Universelle Windows-apps funktionieren nicht, wenn die UAC deaktiviert ist.

Virtualisierung

Da Systemadministratoren in Enterprise-Umgebungen versuchen, Systeme zu sichern, sind viele LOB-Anwendungen für Unternehmen dazu vorgesehen, nur ein Standardbenutzerzugriffstoken zu verwenden. Daher müssen Sie die Mehrzahl der apps nicht ersetzen, wenn UAC aktiviert ist.

Windows10 umfasst Datei- und Registrierungs-Virtualisierungstechnologie für apps, die nicht UAC-kompatibel sind und für die ordnungsgemäße Ausführung des Zugriffstokens eines Administrators erforderlich ist. Wenn eine Verwaltungs-apps, die nicht UAC-kompatibel ist, versucht, in einen geschützten Ordner zu schreiben, wie etwa Programmdateien, gibt die UAC der App eine eigene virtualisierte Ansicht der Ressource, die Sie ändern möchten. Die virtualisierte Kopie wird im Profil des Benutzers verwaltet. Mit dieser Strategie wird eine separate Kopie der virtualisierten Datei für jeden Benutzer erstellt, auf dem die nicht kompatible app ausgeführt wird.

Die meisten App-Aufgaben funktionieren mithilfe von Virtualisierungs-Features ordnungsgemäß. Obwohl die Virtualisierung die Ausführung einer Mehrzahl von Anwendungen ermöglicht, handelt es sich um eine kurzfristige Lösung, die keine langfristige Lösung ist. App-Entwickler sollten Ihre apps so ändern, dass Sie so schnell wie möglich kompatibel sind, anstatt sich auf Datei-, Ordner- und Registrierungs-Virtualisierung zu verlassen.

Virtualisierung ist in den folgenden Szenarien keine Option:

- Virtualisierung gilt nicht für apps, die mit einem vollständigen administrativen Zugriffstoken erhöht und ausgeführt werden.
- Virtualisierung unterstützt nur 32-Bit-apps. Nicht erhöhte 64-Bit-apps erhalten einfach eine Access denied-Meldung, wenn Sie versuchen, ein Handle (einen eindeutigen Bezeichner) für ein Windows-Objekt abzurufen. Systemeigene Windows 64-Bit-apps müssen mit der UAC kompatibel sein und Daten an die richtigen Speicherorte schreiben.
- Virtualisierung ist deaktiviert, wenn die APP ein App-Manifest mit einem angeforderten Attribut für die Ausführungsebene enthält.

Anfordern von Ausführungsebenen

Ein App-Manifest ist eine XML-Datei, die die freigegebenen und privaten parallelen Assemblys beschreibt und identifiziert, an die eine App zur Laufzeit gebunden werden soll. Das App-Manifest enthält Einträge für Kompatibilitätszwecke der UAC-app. Administrative apps, die einen Eintrag im App-Manifest enthalten, geben dem Benutzer die Berechtigung zum Zugriff auf das Zugriffstoken des Benutzers. Obwohl es im App-Manifest keinen

Eintrag gibt, kann die meiste administrative App ohne Änderungen mithilfe von App-Kompatibilitätsfixes ausgeführt werden. Korrekturen der APP-Kompatibilität sind Datenbankeinträge, die Anwendungen ermöglichen, die nicht UAC-kompatibel sind, um ordnungsgemäß zu funktionieren.

Alle UAC-kompatiblen apps sollten eine angeforderte Ausführungsebene zum Anwendungsmanifest hinzugefügt haben. Wenn für die Anwendung Administratorzugriff auf das System erforderlich ist, wird durch das Kennzeichnen der APP mit einer angeforderten Ausführungsebene von "Administrator anfordern" sichergestellt, dass das System dieses Programm als administrative App erkennt und die erforderlichen Höhen Schritte ausführt. Angeforderte Ausführungsebenen geben die für eine APP erforderlichen Berechtigungen an.

Installer-Erkennungstechnologie

Installationsprogramme sind apps, die für die Bereitstellung von Software entwickelt wurden. Die meisten Installationsprogramme schreiben in Systemverzeichnisse und Registrierungsschlüssel. Diese geschützten Systemspeicherorte sind in der Regel nur von einem Administrator in der Installations Erkennungstechnologie zu beschreibbar, was bedeutet, dass Standardbenutzer nicht genügend Zugriff haben, um Programme zu installieren. Windows10 erkennt Installationsprogramme heuristisch und fordert Administratoranmeldeinformationen oder Genehmigung des Administratorbenutzers an, um mit Zugriffsberechtigungen ausgeführt zu werden. Windows10 erkennt auch heuristisch Updates und Programme, die Anwendungen deinstallieren. Eines der Entwurfsziele von UAC besteht darin, zu verhindern, dass Installationen ohne Wissen und Zustimmung des Benutzers ausgeführt werden, da Installationsprogramme in geschützte Bereiche des Dateisystems und der Registrierung schreiben.

Die Installationsprogrammerkennung gilt nur für:

- ausführbare 32-Dateien.
- Anwendungen ohne angeforderte Ausführungsebenen-Attribut.
- Interaktive Prozesse, die als Standardbenutzer mit aktivierter UAC ausgeführt werden.

Bevor ein 32-Bit-Prozess erstellt wird, werden die folgenden Attribute überprüft, um zu ermitteln, ob es sich um ein Installationsprogramm handelt:

- Der Dateiname enthält Schlüsselwörter wie "installieren", "einrichten" oder "Aktualisieren".
- Ressourcenfelder für die Versionsverwaltung enthalten die folgenden Stichwörter: Hersteller, Firmenname, Produktname, Dateibeschreibung, ursprünglicher Dateiname, interner Name und Export Name.
- Schlüsselwörter im nebeneinander liegenden Manifest sind in der ausführbaren Datei eingebettet.
- Schlüsselwörter in bestimmten STRINGTABLE-Einträgen sind in der ausführbaren Datei verknüpft.
- Schlüsselattribute in den Ressourcenskript Daten sind in der ausführbaren Datei verknüpft.
- In der ausführbaren Datei sind gezielte Bytefolge-Sequenzen vorhanden.

Hinweis: Die Schlüsselwörter und Bytesequenzen wurden von den allgemeinen Merkmalen abgeleitet, die von verschiedenen Installationstechnologien beobachtet wurden.

Hinweis: Die Einstellung "Benutzerkontensteuerung: Anwendungsinstallationen erkennen" und "Aufforderung zur Anhebung der Richtlinie" müssen für die Installationsprogrammerkennung aktiviert sein, um Installationsprogramme zu erkennen. Weitere Informationen finden Sie unter [Sicherheitsrichtlinieneinstellungen für die Benutzerkontensteuerung](#).

Sicherheitsrichtlinieneinstellungen für die Benutzerkontensteuerung

11.02.2020 • 5 minutes to read

Betrifft

- Windows 10

Sie können mithilfe von Sicherheitsrichtlinien die Funktionsweise der Benutzerkontensteuerung in Ihrer Organisation konfigurieren. Diese Richtlinien können lokal über das Snap-In „Lokale Sicherheitsrichtlinie“ (secpol.msc) oder mithilfe der Gruppenrichtlinie für die Domäne, eine Organisationseinheit oder für spezifische Gruppen konfiguriert werden.

Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administratorkonto

Diese Richtlinieneinstellung steuert das Verhalten des Administratorgenehmigungsmodus für das integrierte Administrator Konto.

- **Aktiviert** Das integrierte Administratorkonto verwendet den Administratorgenehmigungsmodus. Standardmäßig fordert jeder Vorgang, für den eine Erhöhung der Berechtigung erforderlich ist, den Benutzer zur Genehmigung des Vorgangs auf.
- **Deaktiviert** (Standard) das integrierte Administratorkonto führt alle Anwendungen mit vollständigen Administratorrechten aus.

Benutzerkontensteuerung: zulassen, dass die UIAccess-Anwendung die Anhebung anfordert, ohne den sicheren Desktop zu verwenden

Mit dieser Richtlinieneinstellung wird gesteuert, ob Benutzeroberflächen Barrierefreiheits-Programme (UIAccess oder UIA) den sicheren Desktop automatisch für Elevation-Eingabeaufforderungen deaktivieren können, die von einem Standardbenutzer verwendet werden.

- **Aktiviert** UIA-Programme, einschließlich der Windows-Remote Unterstützung, deaktivieren automatisch den sicheren Desktop für Ansicht Eingabeaufforderungen. Wenn Sie die Richtlinieneinstellung "Benutzerkontensteuerung: zum Sichern des Desktops umschalten" nicht deaktivieren, werden die Eingabeaufforderungen auf dem Desktop des interaktiven Benutzers statt auf dem sicheren Desktop angezeigt.
- **Deaktiviert** (Standard) der sichere Desktop kann nur vom Benutzer des interaktiven Desktops deaktiviert werden, oder durch Deaktivieren der Richtlinieneinstellung "Benutzerkontensteuerung: zum Sichern des Desktops wechseln, wenn eine Eingabeaufforderung zur Erhöhung der Ansicht" angezeigt wird.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus

Diese Richtlinieneinstellung steuert das Verhalten der Aufforderung zur Erhöhung der Höhe für Administratoren.

- **Ohne Aufforderung erhöhen** Ermöglicht privilegierten Konten die Durchführung eines Vorgangs, für den eine Anhebung erforderlich ist, ohne dass Zustimmung oder Anmeldeinformationen erforderlich sind.

Hinweis: verwenden Sie diese Option nur in den am stärksten abhängigen Umgebungen.

- **Anfordern von Anmeldeinformationen auf dem sicheren Desktop** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, einen privilegierten Benutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.
- **Aufforderung zur Genehmigung auf dem sicheren Desktop** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, entweder zulassen oder verweigern auszuwählen. Wenn der Benutzer zulassen auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.
- **Aufforderung zur Eingabe von Anmeldeinformationen** Wenn ein Vorgang eine Anhebung des Privilegs erfordert, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Aufforderung zur Genehmigung** Wenn ein Vorgang eine Anhebung des Privilegs erfordert, wird der Benutzer aufgefordert, entweder zulassen oder verweigern auszuwählen. Wenn der Benutzer zulassen auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.
- **Eingabeaufforderung zur Genehmigung für nicht-Windows-Binärdateien** (Standard) Wenn ein Vorgang für eine nicht von Microsoft ausgeführte Anwendung erhöhte Berechtigungen erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, entweder zulassen oder verweigern auszuwählen. Wenn der Benutzer zulassen auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer

Diese Richtlinieneinstellung steuert das Verhalten der Aufforderung zur Erhöhung der Höhe für Standardbenutzer.

- **Aufforderung zur Eingabe von Anmeldeinformationen** (Standardeinstellung) Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Automatisches ablehnen von elevations Anforderungen** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird eine konfigurierbare Fehlermeldung "Zugriff verweigert" angezeigt. Ein Unternehmen, das Desktops als Standardbenutzer ausführt, kann diese Einstellung auswählen, um Helpdesk-Anrufe zu reduzieren.
- **Anfordern von Anmeldeinformationen auf dem sicheren Desktop** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, einen anderen Benutzernamen und ein anderes Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.

Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern

Diese Richtlinieneinstellung steuert das Verhalten der Anwendungs Installationserkennung für den Computer.

- **Aktiviert** (Standard) Wenn ein App-Installationspaket erkannt wird, für das eine Erhöhung der Berechtigungen erforderlich ist, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Deaktiviert** App-Installationspakete werden nicht erkannt und zur Erhöhung aufgefordert. Unternehmen, die

Standardbenutzerdesktops ausführen und Delegierte Installationstechnologien verwenden, wie etwa Gruppenrichtlinien oder Microsoft Endpoint Configuration Manager, sollten diese Richtlinieneinstellung deaktivieren. In diesem Fall ist die Erkennung des Installationsprogramms nicht erforderlich.

Benutzerkontensteuerung: nur ausführbare Dateien erhöhen, die signiert und validiert sind

Mit dieser Richtlinieneinstellung werden PKI-Signaturüberprüfungen für alle interaktiven Anwendungen erzwungen, die eine Erhöhung der Berechtigungen anfordern. Unternehmensadministratoren können steuern, welche Anwendungen ausgeführt werden dürfen, indem Sie dem Zertifikatspeicher für vertrauenswürdige Herausgeber auf lokalen Computern Zertifikate hinzufügen.

- **Aktiviert** Erzwingt die Validierung des Zertifikat Zertifizierungspfads für eine bestimmte ausführbare Datei, bevor Sie ausgeführt werden darf.
- **Disabled** (Standard) erzwingt die Validierung des Zertifikat Zertifizierungspfads nicht, bevor eine bestimmte ausführbare Datei ausgeführt werden darf.

Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind

Diese Richtlinieneinstellung steuert, ob Anwendungen, die mit einer UIAccess-Integritätsstufe (User Interface Accessibility) ausgeführt werden sollen, an einem sicheren Speicherort im Dateisystem gespeichert werden müssen. Sichere Speicherorte sind auf Folgendes limitiert: - ..\Program-Files\, einschließlich Unterordner - ..\Windows\system32\ - ..\Program-Dateien (x86) \, einschließlich Unterordnern für 64-Bit-Versionen von Windows

Hinweis: Windows erzwingt eine digitale Signaturüberprüfung für jede interaktive APP, die unabhängig vom Zustand dieser Sicherheitseinstellung mit einer UIAccess-Integritätsstufe ausgeführt werden soll.

- **Aktiviert** (Standard) Wenn sich eine APP an einem sicheren Speicherort im Dateisystem befindet, wird Sie nur mit UIAccess-Integrität ausgeführt.
- **Deaktiviert** Eine APP wird mit UIAccess-Integrität ausgeführt, auch wenn Sie sich nicht an einem sicheren Speicherort im Dateisystem befindet.

Benutzerkontensteuerung: Aktivieren des Administratorgenehmigungsmodus

Diese Richtlinieneinstellung steuert das Verhalten aller Richtlinieneinstellungen für die Benutzerkontensteuerung (User Account Control, UAC) für den Computer. Wenn Sie diese Richtlinieneinstellung ändern, müssen Sie Ihren Computer neu starten.

- **Aktiviert** (Standard) Administratorgenehmigungsmodus ist aktiviert. Diese Richtlinie muss aktiviert sein, und die zugehörigen UAC-Richtlinieneinstellungen müssen ebenfalls entsprechend eingestellt werden, damit das integrierte Administrator Konto und alle anderen Benutzer, die Mitglieder der Gruppe "Administratoren" sind, im Administratorgenehmigungsmodus ausgeführt werden können.
- **Deaktiviert** Der Administratorgenehmigungsmodus und alle zugehörigen UAC-Richtlinieneinstellungen sind deaktiviert. Hinweis: Wenn diese Richtlinieneinstellung deaktiviert ist, werden Sie vom Security Center benachrichtigt, dass die allgemeine Sicherheit des Betriebssystems verringert wurde.

Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln

Mit dieser Richtlinieneinstellung wird gesteuert, ob die Aufforderung zur Erhöhung Anforderung auf dem Desktop des interaktiven Benutzers oder auf dem sicheren Desktop angezeigt wird.

- **Aktiviert** (Standard) alle Ansichts Anforderungen werden unabhängig von den Richtlinieneinstellungen für das Verhalten von Eingabeaufforderungen für Administratoren und Standardbenutzer an den sicheren Desktop weitergegeben.
- **Deaktiviert** Alle Höhenanforderungen werden auf dem Desktop des interaktiven Benutzers angezeigt. Richtlinieneinstellungen für das Aufforderungsverhalten für Administratoren und Standardbenutzer werden verwendet.

Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren

Mit dieser Richtlinieneinstellung wird gesteuert, ob Anwendungs Schreibfehler an definierte Registrierungs-und Dateisystemspeicherorte umgeleitet werden. Diese Richtlinieneinstellung verringert Anwendungen, die als Administrator ausgeführt werden, und schreibt Lauf Zeit Anwendungsdaten in % Programme%, % windir%, %windir%\system32 oder HKLM\Software.

- **Enabled** (Standard) app-Schreibfehler werden zur Laufzeit an definierte Benutzerspeicherorte für das Dateisystem und die Registrierung umgeleitet.
- **Deaktiviert** Apps, die Daten in geschützte Speicherorte schreiben, schlagen fehl.

Gruppenrichtlinien und Einstellungen für Registrierungsschlüssel zur Benutzerkontensteuerung

12.09.2019 • 11 minutes to read

Betrifft

- Windows10
- Windows Server 2016

Gruppenrichtlinieneinstellungen

Es gibt 10 Gruppenrichtlinieneinstellungen, die für die Benutzerkontensteuerung (User Account Control, UAC) konfiguriert werden können. In der Tabelle sind die Standardeinstellungen für die einzelnen Richtlinieneinstellungen aufgeführt, und in den folgenden Abschnitten werden die verschiedenen UAC-Richtlinieneinstellungen erläutert und Empfehlungen bereitgestellt. Diese Richtlinieneinstellungen befinden sich unter **Sicherheits Settings\Local Policies\Security Optionen** im Snap-in lokale Sicherheitsrichtlinie. Weitere Informationen zu den einzelnen Gruppenrichtlinieneinstellungen finden Sie in der Gruppenrichtlinien Beschreibung. Informationen zu den Registrierungsschlüsseleinstellungen finden Sie unter [Einstellungen](#) für den Registrierungsschlüssel.

GRUPPENRICHTLINIENEINSTELLUNG	REGISTRIERUNGSSCHLÜSSEL	STANDARD
Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administrator Konto	FilterAdministratorToken	Deaktiviert
Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern	EnableUIADesktopToggle	Deaktiviert
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus	ConsentPromptBehaviorAdmin	Aufforderung zur Genehmigung für nicht-Windows-Binärdateien
Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer	ConsentPromptBehaviorUser	Anfordern von Anmeldeinformationen auf dem sicheren Desktop
Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern	EnableInstallerDetection	Aktiviert (Standard für Start) Deaktiviert (Standard für Enterprise)
Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind	ValidateAdminCodeSignatures	Deaktiviert
Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind	EnableSecureUIAPaths	Aktiviert

GRUPPENRICHTLINIENEINSTELLUNG	REGISTRIERUNGSSCHLÜSSEL	STANDARD
Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen	EnableLUA	Aktiviert
Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln	PromptOnSecureDesktop	Aktiviert
Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren	EnableVirtualization	Aktiviert

Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administrator Konto

Das **Steuerelement "Benutzerkontensteuerung: Administratorgenehmigungsmodus"** für die **Richtlinieneinstellung "integriertes Administratorkonto"** steuert das Verhalten des Administratorgenehmigungsmodus für das integrierte Administratorkonto.

Die Optionen sind:

- **Aktiviert.** Das integrierte Administratorkonto verwendet den Administratorgenehmigungsmodus. Standardmäßig fordert jeder Vorgang, für den eine Erhöhung der Berechtigung erforderlich ist, den Benutzer zur Genehmigung des Vorgangs auf.
- **Deaktiviert.** Standard Das integrierte Administratorkonto führt alle Anwendungen mit vollständigen Administratorrechten aus.

Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern

Die **Benutzerkontensteuerung: zulassen, dass UIAccess-Anwendungen die Anhebung auffordern, ohne die Richtlinieneinstellung für sichere Desktops zu verwenden**, steuert, ob Benutzeroberflächen Barrierefreiheits-Programme (UIAccess oder UIA) den sicheren Desktop automatisch deaktivieren können Eingabeaufforderungen, die von einem Standardbenutzer verwendet werden.

Die Optionen sind:

- **Aktiviert.** UIA-Programme, einschließlich der Windows-Remote Unterstützung, deaktivieren automatisch den sicheren Desktop für Ansichts Eingabeaufforderungen. Wenn Sie die **Benutzerkontensteuerung nicht deaktivieren: Wechseln Sie zum sicheren Desktop, wenn** Sie die Einstellung für die Ansichts Richtlinien anfordern, werden die Eingabeaufforderungen auf dem Desktop des interaktiven Benutzers statt auf dem sicheren Desktop angezeigt.
- **Deaktiviert.** Standard Der sichere Desktop kann nur vom Benutzer des interaktiven Desktops oder durch Deaktivieren der **Benutzerkontensteuerung deaktiviert werden: Wechseln Sie zum sicheren Desktop, wenn Sie für** die Einstellung der Ansichts Richtlinien aufgefordert werden.

UIA-Programme sind für die Interaktion mit Windows-und Anwendungsprogrammen im Auftrag eines Benutzers konzipiert. Diese Richtlinieneinstellung ermöglicht es UIA-Programmen, den sicheren Desktop zu umgehen, um in bestimmten Fällen die Benutzerfreundlichkeit zu verbessern. das zulassen, dass Höhenanforderungen auf dem interaktiven Desktop statt auf dem sicheren Desktop angezeigt werden, kann jedoch Ihr Sicherheitsrisiko erhöhen.

UIA-Programme müssen digital signiert sein, da Sie in der Lage sein müssen, auf Eingabeaufforderungen in Bezug auf Sicherheitsprobleme zu reagieren, beispielsweise die Eingabeaufforderung zur Erhöhung der UAC. Standardmäßig werden UIA-Programme nur in den folgenden geschützten Pfaden ausgeführt:

- ..\Program-Dateien, einschließlich Unterordnern

- ..\Program-Dateien (x86), einschließlich Unterordnern für 64-Bit-Versionen von Windows
- ...\\Windows\\System32

Die **Benutzerkontensteuerung: nur Elevate-UIAccess-Anwendungen, die in der Richtlinieneinstellung für sichere Speicherorte installiert sind**, deaktiviert die Anforderung, von einem geschützten Pfad ausgeführt zu werden.

Obwohl diese Richtlinieneinstellung für ein beliebiges UIA-Programm gilt, wird Sie in erster Linie in bestimmten Remoteunterstützungsszenarien verwendet, einschließlich des Windows-Remote Unterstützungsprogramms in Windows 7.

Wenn ein Benutzer die Remoteunterstützung von einem Administrator anfordert und die Remoteunterstützungssitzung eingerichtet ist, werden alle Erweiterungs Aufforderungen auf dem sicheren Desktop des interaktiven Benutzers angezeigt, und die Remotesitzung des Administrators wird angehalten. Um zu verhindern, dass die Sitzung des Remote Administrators während der Anhebungs Anforderungen angehalten wird, kann der Benutzer beim Einrichten der Remoteunterstützungssitzung das Kontrollkästchen **IT-Experte auf die Eingabeaufforderungen der Benutzerkontensteuerung reagieren zulassen** aktivieren. Wenn Sie dieses Kontrollkästchen aktivieren, muss der interaktive Benutzer jedoch auf dem sicheren Desktop auf eine Eingabeaufforderung mit erhöhten Rechten reagieren. Wenn der interaktive Benutzer ein Standardbenutzer ist, verfügt der Benutzer nicht über die erforderlichen Anmeldeinformationen, um die Höhe zu ermöglichen.

Wenn Sie diese Richtlinieneinstellung aktivieren, werden die Anforderungen für die Erweiterung automatisch an den interaktiven Desktop (nicht an den sicheren Desktop) gesendet und während einer Remoteunterstützungssitzung auch in der Ansicht des Remote Administrators des Desktops angezeigt. Auf diese Weise kann der Remote Administrator die entsprechenden Anmeldeinformationen für die Ansicht bereitstellen.

Mit dieser Richtlinieneinstellung wird das Verhalten der Aufforderung zur Erhöhung der UAC-Höhe für Administratoren nicht geändert.

Wenn Sie beabsichtigen, diese Richtlinieneinstellung zu aktivieren, sollten Sie auch die Auswirkungen der Richtlinieneinstellung **Benutzerkontensteuerung: Verhalten der Aufforderung zur Erhöhung der Standardbenutzer** Einstellungen überprüfen. Wenn Sie als **Automatisches ablehnen von Höhenanforderungen** konfiguriert ist, werden dem Benutzer keine Ansichts Anforderungen angezeigt.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus

Das Verhalten der Aufforderung zur **Eingabeaufforderung für Administratoren im Administratorgenehmigungsmodus für Benutzerkonten Steuerungen** steuert das Verhalten der Aufforderung für erhöhte Rechte für Administratoren.

Die Optionen sind:

- **Ohne Aufforderung erhöhen.** Ermöglicht privilegierten Konten die Durchführung eines Vorgangs, für den eine Anhebung erforderlich ist, ohne dass Zustimmung oder Anmeldeinformationen erforderlich sind.

Hinweis Verwenden Sie diese Option nur in den am stärksten abhängigen Umgebungen.

- **Aufforderung zur Eingabe von Anmeldeinformationen auf dem sicheren Desktop.** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, einen privilegierten Benutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.
- **Aufforderung zur Genehmigung auf dem sicheren Desktop.** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, entweder **zulassen** oder **verweigern** auszuwählen. Wenn der Benutzer **zulassen** auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.

- **Aufforderung zur Eingabe von Anmeldeinformationen** Wenn ein Vorgang eine Anhebung des Privilegs erfordert, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Zur Genehmigung auffordern.** Wenn ein Vorgang eine Anhebung des Privilegs erfordert, wird der Benutzer aufgefordert, entweder **zulassen** oder **verweigern** auszuwählen. Wenn der Benutzer **zulassen** auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.
- **Aufforderung zur Genehmigung für nicht-Windows-Binärdateien** Standard Wenn ein Vorgang für eine nicht von Microsoft ausgeführte Anwendung erhöhte Berechtigungen erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, entweder **zulassen** oder **verweigern** auszuwählen. Wenn der Benutzer **zulassen** auswählt, wird der Vorgang mit dem höchsten verfügbaren Privileg des Benutzers fortgesetzt.

Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer

Die **Benutzerkontensteuerung: das Verhalten der Einstellung Aufforderung zur Erhöhung der Benutzerrechte für Standardbenutzer** steuert das Verhalten der Aufforderung für erhöhte Rechte für Standardbenutzer.

Die Optionen sind:

- **Automatisches ablehnen von Höhenanforderungen** Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird eine konfigurierbare Fehlermeldung "Zugriff verweigert" angezeigt. Ein Unternehmen, das Desktops als Standardbenutzer ausführt, kann diese Einstellung auswählen, um Helpdesk-Anrufe zu reduzieren.
- **Aufforderung zur Eingabe von Anmeldeinformationen auf dem sicheren Desktop.** Standard Wenn ein Vorgang eine Erhöhung der Berechtigung erfordert, wird der Benutzer auf dem sicheren Desktop aufgefordert, einen anderen Benutzernamen und ein anderes Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Aufforderung zur Eingabe von Anmeldeinformationen** Wenn ein Vorgang eine Anhebung des Privilegs erfordert, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.

Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern

Mit der Einstellung "**Benutzerkontensteuerung: Anwendungsinstallationen erkennen**" und "**Eingabeaufforderung für elevations Richtlinien**" wird das Verhalten der Anwendungs Installationserkennung für den Computer gesteuert.

Die Optionen sind:

- **Aktiviert.** (Standardeinstellung für "Start") Wenn ein Anwendungs Installationspaket erkannt wird, für das eine Erhöhung der Berechtigungen erforderlich ist, wird der Benutzer aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben. Wenn der Benutzer gültige Anmeldeinformationen eingibt, wird der Vorgang mit dem entsprechenden Privileg fortgesetzt.
- **Deaktiviert.** (Standard für Enterprise) Anwendungs Installationspakete werden nicht erkannt und zur Erhöhung aufgefordert. Unternehmen, die standardmäßige Benutzerdesktops ausführen und Delegierte Installationstechnologien wie Gruppenrichtlinien-Software Installation oder Systems Management Server (SMS) verwenden, sollten diese Richtlinieneinstellung deaktivieren. In diesem Fall ist die Erkennung des Installationsprogramms nicht erforderlich.

Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind

Die **Benutzerkontensteuerung: nur ausführbare Dateien, die signiert und überprüfte Richtlinieneinstellung sind**, erzwingt öffentliche Schlüsselinfrastruktur (PKI)-Signaturüberprüfungen für alle interaktiven Anwendungen, die eine Erhöhung der Berechtigungen anfordern. Unternehmensadministratoren können steuern, welche Anwendungen ausgeführt werden dürfen, indem Sie dem Zertifikatspeicher für vertrauenswürdige Herausgeber auf lokalen Computern Zertifikate hinzufügen.

Die Optionen sind:

- **Aktiviert.** Erzwingt die Validierung des PKI-Zertifizierungspaths für eine bestimmte ausführbare Datei, bevor Sie ausgeführt werden darf.
- **Deaktiviert.** Standard Erzwingen Sie keine PKI-Zertifizierungspfad Überprüfung, bevor eine bestimmte ausführbare Datei ausgeführt werden darf.

Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind

Die **Benutzerkontensteuerung: nur UIAccess-Anwendungen, die in der Richtlinieneinstellung für sichere Speicherorte installiert sind**, steuert, ob Anwendungen, die mit einer UIAccess-Integritätsstufe (User Interface Accessibility) ausgeführt werden müssen, sich in einem sicheren Speicherort im Dateisystem. Sichere Speicherorte sind auf Folgendes limitiert:

- ..\Program-Dateien, einschließlich Unterordnern
- ...\Windows\system32
- ..\Program-Dateien (x86), einschließlich Unterordnern für 64-Bit-Versionen von Windows

Hinweis Windows erzwingt eine PKI-Signaturüberprüfung für jede interaktive Anwendung, die unabhängig vom Zustand dieser Sicherheitseinstellung mit einer UIAccess-Integritätsstufe ausgeführt werden soll.

Die Optionen sind:

- **Aktiviert.** Standard Wenn sich eine Anwendung an einem sicheren Speicherort im Dateisystem befindet, wird Sie nur mit UIAccess-Integrität ausgeführt.
- **Deaktiviert.** Eine Anwendung wird mit UIAccess-Integrität ausgeführt, auch wenn Sie sich nicht an einem sicheren Speicherort im Dateisystem befindet.

Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen

Die Richtlinieneinstellung **Benutzerkontensteuerung: alle Administratoren des Administrator-Genehmigungsmodus ausführen** steuert das Verhalten aller UAC-Richtlinieneinstellungen für den Computer. Wenn Sie diese Richtlinieneinstellung ändern, müssen Sie Ihren Computer neu starten.

Die Optionen sind:

- **Aktiviert.** Standard Der Administratorgenehmigungsmodus ist aktiviert. Diese Richtlinie muss aktiviert sein, und die zugehörigen UAC-Richtlinieneinstellungen müssen ebenfalls entsprechend eingestellt werden, damit das integrierte Administrator Konto und alle anderen Benutzer, die Mitglieder der Gruppe " **Administratoren** " sind, im Administratorgenehmigungsmodus ausgeführt werden können.
- **Deaktiviert.** Der Administratorgenehmigungsmodus und alle zugehörigen UAC-Richtlinieneinstellungen sind deaktiviert.

Hinweis Wenn diese Richtlinieneinstellung deaktiviert ist, werden Sie vom Security Center benachrichtigt, dass die allgemeine Sicherheit des Betriebssystems verringert wurde.

Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln

Das **Steuerelement "Benutzerkontensteuerung": beim auffordern** der Einstellung für die Richtlinie zum sicheren Desktop wechseln steuert, ob die Aufforderung zur Erhöhungs Anforderung auf dem Desktop des interaktiven Benutzers oder auf dem sicheren Desktop angezeigt wird.

Die Optionen sind:

- **Aktiviert.** Standard Alle elevations Anforderungen werden unabhängig von den Richtlinieneinstellungen des Eingabe Aufforderungs Verhaltens für Administratoren und Standardbenutzer an den sicheren Desktop weitergegeben.
- **Deaktiviert.** Alle Höhenanforderungen werden auf dem Desktop des interaktiven Benutzers angezeigt. Richtlinieneinstellungen für das Aufforderungsverhalten für Administratoren und Standardbenutzer werden

verwendet.

Wenn diese Richtlinieneinstellung aktiviert ist, wird das **Verhalten der Aufforderung zur Erhöhung der Berechtigungen für Administratoren im Administratorgenehmigungsmodus** überschrieben. In der folgenden Tabelle wird das Verhalten der Eingabeaufforderung für erhöhte Rechte für die einzelnen Administrator Richtlinieneinstellungen beschrieben, wenn die **Benutzerkontensteuerung: zum sicheren Desktop wechseln, wenn** die Einstellung für die Ansichts Richtlinien Aufforderung aktiviert oder deaktiviert ist.

ADMINISTRATOR RICHTLINIENEINSTELLUNG	AKTIVIERT	DEAKTIVIERT
Anfordern von Anmeldeinformationen auf dem sicheren Desktop	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.
Aufforderung zur Genehmigung auf dem sicheren Desktop	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.
Aufforderung zur Eingabe von Anmeldeinformationen	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem Desktop des interaktiven Benutzers angezeigt.
Aufforderung zur Genehmigung	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem Desktop des interaktiven Benutzers angezeigt.
Aufforderung zur Genehmigung für nicht-Windows-Binärdateien	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem Desktop des interaktiven Benutzers angezeigt.

Wenn diese Richtlinieneinstellung aktiviert ist, wird die Richtlinieneinstellung **Benutzerkontensteuerung: Verhalten der Aufforderung für erhöhte Rechte für Standardbenutzer** überschrieben. In der folgenden Tabelle wird das Verhalten der Eingabeaufforderung für erhöhte Rechte für die einzelnen Standardbenutzerrichtlinien Einstellungen beschrieben, wenn die **Benutzerkontensteuerung: bei der Eingabeaufforderung für die Einstellung für die elevations Richtlinie auf den sicheren Desktop umschalten** aktiviert oder deaktiviert ist.

STANDARD RICHTLINIENEINSTELLUNG	AKTIVIERT	DEAKTIVIERT
Automatisches ablehnen von elevations Anforderungen	Keine Eingabeaufforderung. Die Anforderung wird automatisch abgelehnt.	Keine Eingabeaufforderung. Die Anforderung wird automatisch abgelehnt.
Anfordern von Anmeldeinformationen auf dem sicheren Desktop	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.
Aufforderung zur Eingabe von Anmeldeinformationen	Die Eingabeaufforderung wird auf dem sicheren Desktop angezeigt.	Die Eingabeaufforderung wird auf dem Desktop des interaktiven Benutzers angezeigt.

Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren

Die **Benutzerkontensteuerung: Virtualisieren von Datei- und Registrierungs Schreibfehlern in der Richtlinie für einzelne Benutzerspeicherorte** steuert, ob Anwendungs Schreibfehler an definierte Registrierungs- und Dateisystemspeicherorte umgeleitet werden. Diese Richtlinieneinstellung verringert Anwendungen, die als Administrator ausgeführt werden, und schreibt Lauf Zeit Anwendungsdaten in%

Programme%,% windir%,%windir%\system32 oder HKLM\Software.

Die Optionen sind:

- **Aktiviert.** Standard Anwendungs Schreibfehler werden zur Laufzeit an definierte Benutzerspeicherorte für das Dateisystem und die Registrierung umgeleitet.
- **Deaktiviert.** Anwendungen, die Daten in geschützte Speicherorte schreiben, schlagen fehl.

Registrierungsschlüsseleinstellungen

Die Registrierungsschlüssel finden Sie unter

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System.

Informationen zu den einzelnen Registrierungsschlüsseln finden Sie in der zugehörigen Gruppenrichtlinien Beschreibung.

REGISTRIERUNGSSCHLÜSSEL	GRUPPENRICHTLINIENEINSTELLUNG	REGISTRIERUNGSEINSTELLUNG
FilterAdministratorToken	Benutzerkontensteuerung: Administratorgenehmigungsmodus für das integrierte Administrator Konto	0 (Standard) = deaktiviert 1 = aktiviert
EnableUIADesktopToggle	Benutzerkontensteuerung: UIAccess-Anwendungen können erhöhte Rechte ohne sicheren Desktop anfordern	0 (Standard) = deaktiviert 1 = aktiviert
ConsentPromptBehaviorAdmin	Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Administratoren im Administratorbestätigungsmodus	0 = ohne Aufforderung erhöhen 1 = Aufforderung zur Eingabe von Anmeldeinformationen auf dem sicheren Desktop 2 = Aufforderung zur Genehmigung auf dem sicheren Desktop 3 = Aufforderung zur Eingabe von Anmeldeinformationen 4 = Aufforderung zur Genehmigung 5 (Standard) = Aufforderung zur Genehmigung für nicht-Windows-Binärdateien
ConsentPromptBehaviorUser	Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer	0 = Automatisches ablehnen von elevations Anforderungen 1 = Aufforderung zur Eingabe von Anmeldeinformationen auf dem sicheren Desktop 3 (Standard) = Aufforderung zur Eingabe von Anmeldeinformationen
EnableInstallerDetection	Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern	1 = aktiviert (Standardeinstellung für Home) 0 = deaktiviert (Standard für Enterprise)
ValidateAdminCodeSignatures	Benutzerkontensteuerung: Nur ausführbare Dateien heraufstufen, die signiert und überprüft sind	0 (Standard) = deaktiviert 1 = aktiviert
EnableSecureUIAPaths	Benutzerkontensteuerung: Erhöhte Rechte nur für UIAccess-Anwendungen, die an sicheren Orten installiert sind	0 = deaktiviert 1 (Standard) = aktiviert

REGISTRIERUNGSSCHLÜSSEL	GRUPPENRICHTLINIENEINSTELLUNG	REGISTRIERUNGSEINSTELLUNG
EnableLUA	Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen	0 = deaktiviert 1 (Standard) = aktiviert
PromptOnSecureDesktop	Benutzerkontensteuerung: Bei Benutzeraufforderung nach erhöhten Rechten zum sicheren Desktop wechseln	0 = deaktiviert 1 (Standard) = aktiviert
EnableVirtualization	Benutzerkontensteuerung: Datei- und Registrierungsschreibfehler an Einzelbenutzerstandorte virtualisieren	0 = deaktiviert 1 (Standard) = aktiviert

Windows Hello for Business




22.01.2020 • 3 minutes to read

In Windows10 ersetzt Windows Hello for Business Kennwörter durch eine starke zweistufige Authentifizierung auf PCs und mobilen Geräten. Diese Authentifizierung besteht aus einer neuen Art von Benutzeranmeldeinformationen, die an ein Gerät gebunden ist und ein biometrisches Merkmal oder eine PIN verwendet.

Mit Windows Hello for Business können Benutzer sich bei einem Active Directory- oder Azure Active Directory-Konto authentifizieren.

Windows Hello behandelt die folgenden Probleme mit Kennwörtern:

- Sichere Kennwörter kann man sich teilweise schlecht merken. Benutzer verwenden deshalb häufig dieselben Kennwörter für mehrere Websites.
- Serververletzungen können symmetrische Netzwerkanmeldeinformationen (Kennwörter) verfügbar machen.
- Kennwörter sind Ziel von [Replay-Angriffen](#).
- Benutzer können versehentlich ihre Kennwörter aufgrund von [Phishing-Angriffen](#) offenlegen.

		
Übersicht	Warum eine PIN besser als ein Kennwort ist	Verwalten von Windows Hello for Business im Unternehmen

Voraussetzungen

Bereitstellung nur in der Cloud

- Windows10, Version 1511 oder höher
- MicrosoftAzure-Konto
- Azure Active Directory
- Azure-mehrstufige Authentifizierung
- Moderne Verwaltung (Intune oder unterstütztes MDM von Drittanbietern) *optional*
- Azure AD Premium-Abonnement – *optional*, erforderlich für die automatische MDM-Registrierung, wenn das Gerät zu Azure Active Directory hinzugefügt wird

Hybridbereitstellungen

Die Tabelle enthält die Mindestanforderungen für jede Bereitstellung. Für die Schlüssel Vertrauensstellung in einer Bereitstellung mit mehreren Domänen/Gesamtstrukturen gelten die folgenden Anforderungen für jede Domäne/Gesamtstruktur, die Windows Hello for Business-Komponenten hostet oder am Kerberos-Verweis Prozess beteiligt ist.

SCHLÜSSELBASIERTES VERTRAUEN VERWALTETE GRUPPENRICHTLINIE	ZERTIFIKATBASIERTES VERTRAUEN GEMISCHT VERWALTET	SCHLÜSSELBASIERTES VERTRAUEN MODERN VERWALTET	ZERTIFIKATBASIERTES VERTRAUEN MODERN VERWALTET
Windows10, Version 1511 oder höher	In Azure AD eingebunden: <i>Minimum:</i> Windows 10, Version 1703 <i>Beste Erfahrung:</i> Windows10, Version 1709 oder höher (unterstützt synchrone Zertifikatregistrierung). In Azure AD eingebunden: Windows10, Version 1511 oder höher	Windows10, Version 1511 oder höher	Windows10, Version 1511 oder höher
Windows Server2016- Schema	Windows Server2016- Schema	Windows Server2016- Schema	Windows Server2016- Schema
Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionse- bene	Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionse- bene	Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionse- bene	Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionse- bene
Windows Server 2016 oder höher-Domänencontroller	Windows Server 2008R2- Domänencontroller oder höher	Windows Server 2016 oder höher-Domänencontroller	Windows Server 2008R2- Domänencontroller oder höher
Windows Server2012- Zertifizierungsstelle oder höher	Windows Server2012- Zertifizierungsstelle oder höher	Windows Server2012- Zertifizierungsstelle oder höher	Windows Server2012- Zertifizierungsstelle oder höher
–	Windows Server2016 AD FS mit KB4088889 Update (in hybride Azure AD eingebundene Clients), und Windows Server2012 Network Device Enrollment Service oder höher (in Azure AD eingebunden)	n.a.	Windows Server2012 Network Device Enrollment Service oder höher
Azure MFA-Mandant oder AD FS mit Azure MFA- Adapter oder AD FS mit Azure MFA- Serveradapter oder AD FS mit MFA-Adapter von Drittanbieter	Azure MFA-Mandant oder AD FS mit Azure MFA- Adapter oder AD FS mit Azure MFA- Serveradapter oder AD FS mit MFA-Adapter von Drittanbieter	Azure MFA-Mandant oder AD FS mit Azure MFA- Adapter oder AD FS mit Azure MFA- Serveradapter oder AD FS mit MFA-Adapter von Drittanbieter	Azure MFA-Mandant oder AD FS mit Azure MFA- Adapter oder AD FS mit Azure MFA- Serveradapter oder AD FS mit MFA-Adapter von Drittanbieter
Azure-Konto	Azure-Konto	Azure-Konto	Azure-Konto
Azure Active Directory	Azure Active Directory	Azure Active Directory	Azure Active Directory
Azure AD Connect	Azure AD Connect	Azure AD Connect	Azure AD Connect

SCHLÜSSELBASIERTES VERTRAUEN VERWALTETE GRUPPENRICHTLINIE	ZERTIFIKATBASIERTES VERTRAUEN GEMISCHT VERWALTET	SCHLÜSSELBASIERTES VERTRAUEN MODERN VERWALTET	ZERTIFIKATBASIERTES VERTRAUEN MODERN VERWALTET
Azure AD Premium, optional	Azure AD Premium, erforderlich für das Zurückschreiben von Geräten	Azure AD Premium, optional für automatische MDM- Registrierung	Azure AD Premium, optional für automatische MDM- Registrierung

IMPORTANT

- Hybrid Bereitstellungen unterstützen den zerstörungsfreien Pin-Reset, der sowohl mit der Zertifikats Vertrauensstellung als auch mit den Schlüssel Vertrauensstellungs Modellen funktioniert.

Anforderungen:

Microsoft Pin-Zurücksetzungs Dienst – Windows 10, Versionen 1709 bis 1809, Enterprise Edition. Es gibt keine Lizenzierungsanforderung für diesen Dienst seit Version 1903

Zurücksetzen über dem Sperrbildschirm (*Ich habe meinen PIN* -Link vergessen)-Windows 10, Version 1903

- Lokale Bereitstellungen unterstützen den destruktiven Pin-Reset, der sowohl mit der Zertifikats Vertrauensstellung als auch mit den Schlüssel Vertrauensstellungs Modellen funktioniert.

Anforderungen:

Zurücksetzen von Einstellungen – Windows 10, Version 1703, professionell

Zurücksetzen über den Sperrbildschirm – Windows 10, Version 1709, professionell

Zurücksetzen über dem Sperrbildschirm (*Ich habe meinen PIN* -Link vergessen)-Windows 10, Version 1903

Lokale Bereitstellungen

Die Tabelle enthält die Mindestanforderungen für jede Bereitstellung.

SCHLÜSSELBASIERTES VERTRAUEN VERWALTETE GRUPPENRICHTLINIE	ZERTIFIKATBASIERTES VERTRAUEN VERWALTETE GRUPPENRICHTLINIE
Windows10, Version 1703 oder höher	Windows10, Version 1703 oder höher
Windows Server2016-Schema	Windows Server2016-Schema
Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionsebene	Windows Server 2008 R2 Domänen- /Gesamtstrukturfunktionsebene
Windows Server 2016 oder höher-Domänencontroller	Windows Server 2008R2-Domänencontroller oder höher
Windows Server2012-Zertifizierungsstelle oder höher	Windows Server2012-Zertifizierungsstelle oder höher
Windows Server 2016 AD FS mit KB4088889 Update	Windows Server 2016 AD FS mit KB4088889 Update
AD FS mit MFA-Adapter von Drittanbieter	AD FS mit MFA-Adapter von Drittanbieter
Azure-Konto, optional für Azure MFA-Abrechnung	Azure-Konto, optional für Azure MFA-Abrechnung

IMPORTANT

Für Windows Hello for Business-Schlüssel Vertrauensstellungs Bereitstellungen ist für jede Domäne mindestens ein Windows Server-Domänen Controller 2016 oder höher erforderlich, wenn Sie über mehrere Domänen verfügen. Weitere Informationen finden Sie im [Planungshandbuch](#).

Schützen abgeleiteter Domänenanmeldeinformationen mit Windows Defender Credential Guard

04.01.2020 • 2 minutes to read

Betrifft:

- Windows 10
- Windows Server2016

In Windows10 Enterprise und Windows Server 2016 wird die Windows Defender-Anmelde Informations Überwachung mithilfe von Virtualisierungs-basierter Sicherheit Geheimnisse isolieren, sodass nur privilegierte System Software darauf zugreifen kann. Ein nicht autorisierter Zugriff auf diese geheimen Schlüssel kann zu Angriffen mit dem Ziel des Diebstahls von Anmeldeinformationen, z.B. Pass-the-Hash oder Pass-The-Ticket, führen. Windows Defender Credential Guard verhindert diese Angriffe durch den Schutz von NTLM-Kennworthashes, Kerberos Ticket Granting Tickets und von Anwendungen als Domänenanmeldeinformationen gespeicherten Anmeldeinformationen.

Durch Aktivieren von Windows Defender Credential Guard werden die folgenden Features und Lösungen bereitgestellt:

- **Hardware-Sicherheit** NTLM, Kerberos und die Anmeldeinformationsverwaltung nutzen die Plattformsicherheitsfeatures, einschließlich des sicheren Starts und der Virtualisierung, um Anmeldeinformationen zu schützen.
- **Virtualisierungsbasierte Sicherheit** Von Windows NTLM und Kerberos abgeleitete Domänenanmeldeinformationen und andere geheime Schlüssel werden in einer geschützten Umgebung isoliert vom Betriebssystem ausgeführt.
- **Verbesserter Schutz gegen fortgeschrittene dauerhafte Bedrohungen** Durch das Sichern von Domänenanmeldeinformationen für die Anmeldeinformationsverwaltung sowie von NTLM und Kerberos abgeleiteten Anmeldeinformationen mithilfe von virtualisierungsbasierter Sicherheit werden die Verfahren und Tools für den Diebstahl von Anmeldeinformationen blockiert, die bei vielen gezielten Angriffen eingesetzt werden. Im Betriebssystem ausgeführte Schadsoftware mit Administratorberechtigungen kann geheime Schlüssel, die durch die virtualisierungsbasierte Sicherheit geschützt sind, nicht extrahieren. Auch wenn Windows Defender Credential Guard eine leistungsstarke Lösung darstellt, werden für dauerhafte Bedrohungen neue Angriffstechniken eingesetzt werden, und Sie sollten daher auch Windows Defender Device Guard und andere Sicherheitsstrategien und -architekturen einbinden.

Verwandte Themen

- [Isolierter Benutzermodus in Windows10 mit Dave Probert \(Channel9\)](#)
- [Isolierte Benutzermodusprozesse und -Features in Windows10 mit Logan Gabriel \(Channel9\)](#)
- [Informationen zu Prozessen und Features im isolierten Benutzermodus von Windows10 mit Dave Probert \(Channel9\)](#)
- [Verringern des Risikos des Diebstahls von Anmeldeinformationen mit dem isolierten Benutzermodus von Windows10 \(Channel9\)](#)
- [Schützen von Kennwörtern mit Windows Defender Credential Guard](#)
- [Aktivieren der strengen KDC-Überprüfung in Windows Kerberos](#)
- [Neuerungen in der Kerberos-Authentifizierung für Windows Server2012](#)

- [Schrittweise Anleitung zur Authentifizierungsmechanismussicherung für AD DS unter Windows Server 2008 R2](#)
- [Trusted Platform Module](#)

Funktionsweise von Windows Defender Credential Guard

31.12.2019 • 2 minutes to read

Gilt für:

- Windows 10
- Windows Server 2016

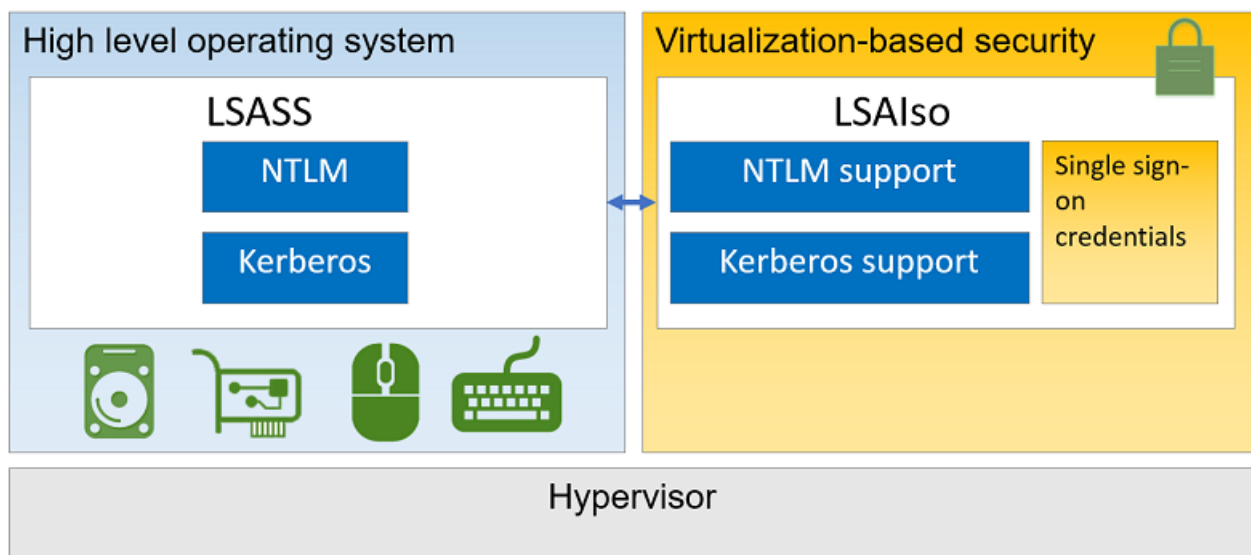
Kerberos, NTLM und die Anmeldeinformationsverwaltung isolieren geheime Schlüssel mithilfe virtualisierungsbasierter Sicherheit. In früheren Windows-Versionen wurden geheime Schlüssel in der lokalen Sicherheitsautorität (LSA) gespeichert. Vor Windows 10 die LSA gespeicherte Geheimnisse, die vom Betriebssystem im Prozess Speicher verwendet werden. Bei Aktivierung von Windows Defender Credential Guard kommuniziert der LSA-Prozess im Betriebssystem mit einer neuen Komponente, die als isolierter LSA-Prozess bezeichnet wird und in der diese geheimen Schlüssel gespeichert und geschützt werden. Im isolierten LSA-Prozess gespeicherte Daten werden durch die virtualisierungsbasierte Sicherheit geschützt, und das restliche Betriebssystem kann darauf nicht zugreifen. Die LSA verwendet Remoteprozeduraufrufe, um mit dem isolierten LSA-Prozess zu kommunizieren.

Aus Sicherheitsgründen hostet der isolierte LSA-Prozess keine Gerätetreiber. Stattdessen enthält er nur eine kleine Teilmenge der Binärdateien des Betriebssystems, die für die Sicherheit nötig sind, und sonst nichts. Alle diese Binärdateien werden mit einem Zertifikat signiert, dem die virtualisierungsbasierte Sicherheit vertraut, und diese Signaturen werden vor dem Starten der Datei in der geschützten Umgebung überprüft.

Wenn Windows Defender Credential Guard aktiviert ist, können NTLMv1, MS-CHAPv2, Digest und CredSSP die angemeldeten Anmeldeinformationen nicht verwenden. Folglich funktioniert einmaliges Anmelden mit diesen Protokollen nicht. Anwendungen können jedoch zur Eingabe der Anmeldeinformationen auffordern, oder im Windows-Tresor gespeicherte Anmeldeinformationen verwenden, die nicht mit einem dieser Protokolle durch Windows Defender Credential Guard geschützt werden. Es wird dringend davon abgeraten, wichtige Informationen wie die Anmeldeinformationen mit einem dieser Protokolle zu verwenden. Wenn die Protokolle von Domänenbenutzern oder Azure AD verwendet werden müssen, sollten für diese Anwendungsfälle sekundäre Anmeldeinformationen bereitgestellt werden.

Wenn Windows Defender Credential Guard aktiviert ist, lässt Kerberos keine nicht eingeschränkte Kerberos-Delegierung bzw. DES-Verschlüsselung zu. Dies gilt nicht nur für angemeldete Anmeldeinformationen, sondern auch für angeforderte oder gespeicherte Anmeldeinformationen.

Im Folgenden finden Sie eine grobe Übersicht darüber, wie die LSA mit der virtualisierungsbasierten Sicherheit isoliert wird:



Weitere Informationen:

Verwandte Videos

[Was ist die Virtualisierungs-basierte Sicherheit?](#)

Windows Defender Credential Guard: Anforderungen

13.02.2020 • 7 minutes to read

Gilt für:

- Windows 10
- Windows Server2016

Damit der Schutz durch Windows Defender-Anmeldeinformationen geschützt wird, müssen die von Ihnen geschützten Computer bestimmte grundlegende Hardware-, Firmware- und Softwareanforderungen erfüllen, die wir als [Hardware- und Softwareanforderungen](#) bezeichnen. Darüber hinaus blockiert Windows Defender Credential Guard spezifische Authentifizierungsfunktionen, sodass Anwendungen, die blockierte Funktionen erfordern, unterbrochen werden. Wir bezeichnen dies als [Anwendungsanforderungen](#). Computer können auch darüber hinausgehende Hardware- und Firmwarequalifikationen erfüllen und mit zusätzlichen Schutzmechanismen ausgestattet werden. Diese Computer sind noch stärker vor bestimmten Bedrohungen geschützt. Ausführliche Informationen zum grundlegenden Schutz und zum Schutz für erhöhte Sicherheit, der mit den in 2015, 2016 und 2017 verfügbaren Hardware- und Firmwareoptionen verknüpft ist, finden Sie in den Tabellen unter [Sicherheitsüberlegungen](#).

Hardware- und Softwareanforderungen

Zum Bereitstellen von grundlegendem Schutz gegen Versuche auf Betriebssystemebene, Domänenanmeldeinformationen für die Anmeldeinformationsverwaltung sowie von NTLM und Kerberos abgeleitete Anmeldeinformationen zu lesen, verwendet Windows Defender Credential Guard Folgendes:

- Unterstützung für virtualisierungsbasierte Sicherheit (erforderlich)
- Sicherer Start (erforderlich)
- TPM 1,2 oder 2,0 (bevorzugt – bietet Bindung an Hardware), entweder diskret oder Firmware
- UEFI-Sperre (bevorzugt – verhindert Deaktivierungen durch Angreifer mit einer einfachen Änderung des Registrierungsschlüssels)

Die virtualisierungsbasierte Sicherheit erfordert Folgendes:

- 64-Bit-CPU
- CPU-Virtualisierungserweiterungen sowie erweiterte Seitentabellen
- Windows-Hypervisor (für die Installation ist keine Hyper-V-Windows-Funktion erforderlich)

Windows Defender Credential Guard-Bereitstellung auf virtuellen Computern

Credential Guard kann geheime Schlüssel auf einem virtuellen Hyper-V-Computer genau wie auf einem physischen Computer schützen. Wenn Sie Credential Guard auf einem virtuellen Computer bereitstellen, werden geheime Schlüssel vor Angriffen innerhalb des virtuellen Computers geschützt. Credential Guard bietet jedoch keinen zusätzlichen Schutz vor Systemangriffen von einem Host mit privilegiertem Zugriff.

Anforderungen für die Ausführung von Windows Defender Credential Guard auf virtuellen Hyper-V-Computern

- Der Hyper-V-Host muss über eine IOMMU verfügen und mindestens Windows Server 2016 oder Windows 10, Version 1607, ausführen.
- Beim virtuellen Hyper-V-Computer muss es sich um einen Computer der Generation2 mit aktiviertem virtuellen TPM handeln, auf dem mindestens Windows Server 2016 oder Windows10 ausgeführt wird.

Informationen zu anderen Hostplattformen finden Sie unter [Aktivieren von Windows Server 2016- und Hyper-V-Virtualisierungs-basierten Sicherheitsfeatures auf anderen Plattformen](#).

Informationen zu den Hardware- und Softwareanforderungen für Windows Defender Remote Credential Guard finden Sie unter [Windows Defender Remote Credential Guard-Anforderungen](#).

Anforderungen an Anwendungen

Wenn Windows Defender Credential Guard aktiviert ist, werden bestimmte Authentifizierungsfunktionen blockiert, sodass Anwendungen, die blockierte Funktionen erfordern, unterbrochen werden. Anwendungen sollten vor der Bereitstellung getestet werden, um die Kompatibilität mit der reduzierten Funktionalität zu gewährleisten.

WARNING

Das Aktivieren von Windows Defender Credential Guard auf Domänencontrollern wird nicht unterstützt. Der Domänencontroller hostet Authentifizierungsdienste, die in isolierte Prozesse integriert werden, wenn Windows Defender Credential Guard aktiviert ist. Dadurch kommt es zu Abstürzen.

NOTE

Windows Defender Credential Guard bietet keinen Schutz für die Active Directory-Datenbank oder die Sicherheitskontenverwaltung (Security Accounts Manager, SAM). Die bei Aktivierung von Windows Defender Credential Guard durch Kerberos und NTLM geschützten Anmeldeinformationen sind auch in der Active Directory-Datenbank (auf Domänencontrollern) und in der SAM (für lokale Konten) enthalten.

Anwendungen werden unterbrochen, wenn sie Folgendes benötigen:

- Kerberos-DES-Verschlüsselungsunterstützung
- Uneingeschränkte Kerberos-Delegierung
- Extrahieren des Kerberos-TGT
- NTLMv1

Anwendungen fordern Anmeldeinformationen an und setzen diese Risiken aus, wenn sie Folgendes benötigen:

- Digestauthentifizierung
- Delegierung von Anmeldeinformationen
- MS-CHAPv2

Anwendungen können zu Leistungsproblemen führen, wenn sie versuchen, den isolierten Windows Defender Credential Guard-Prozess zu verknüpfen.

Dienste oder Protokolle, die auf Kerberos basieren, z.B. Dateifreigaben, Remotedesktop oder BranchCache, funktionieren weiterhin und sind von Windows Defender Credential Guard nicht betroffen.

Sicherheitsaspekte

Alle Computer, die die Hardware-, Firmware- und Softwareanforderungen für grundlegenden Schutz erfüllen, können Windows Defender Credential Guard nutzen. Computer mit zusätzlichen Qualifikationen können erweiterten Schutz bieten, um die Angriffsfläche weiter zu verringern. In den folgenden Tabellen werden grundlegende Schutzmaßnahmen und Schutzmaßnahmen für erhöhte Sicherheit für Hardware- und Firmwareoptionen beschrieben, die 2015, 2016 und 2017 verfügbar sind.

NOTE

Ab Windows10, Version 1607, muss Trusted Platform Module (TPM 2.0) auf neu ausgelieferten Computern standardmäßig aktiviert sein.

Als OEM finden Sie Informationen zu den Anforderungen unter [PC-OEM-Anforderungen für Windows Defender Device Guard und Windows Defender Credential Guard](#).

Grundlegender Schutz

GRUNDLEGENER SCHUTZ	BESCHREIBUNG	SICHERHEITSVORTEILE
Hardware: 64-Bit-CPU	Damit Windows-Hypervisor VBS bereitstellen kann, ist ein 64-Bit-Computer erforderlich.	
Hardware: CPU-Virtualisierungserweiterungen plus EPT (Extended Page Tables)	Anforderungen: Diese Hardwarefeatures sind für VBS erforderlich: Eine der folgenden Virtualisierungserweiterungen: <ul style="list-style-type: none">• VT-x (Intel) oder• AMD-V und: <ul style="list-style-type: none">• EPT (Extended Page Tables), auch als Second Level Address Translation (SLAT) bezeichnet.	VBS isoliert den sicheren Kernel vom normalen Betriebssystem. Aufgrund dieser Isolierung ist es nicht möglich, Sicherheitslücken und Zero-Day-Angriffe im normalen Betriebssystem zu missbrauchen.
Hardware: Trusted Platform Module (TPM)	Anforderung: TPM 1.2 oder TPM 2.0, entweder diskret oder firmwarebasiert. TPM-Empfehlungen	Ein TPM bietet Schutz für VBS-Verschlüsselungsschlüssel, die in der Firmware gespeichert sind. Dadurch ist ein System vor Angriffen durch einen physisch anwesenden Benutzer mit BIOS-Zugriff geschützt.
Firmware: UEFI-Firmwareversion 2.3.1.c oder höher mit „Sicherer Start“ gemäß UEFI	Anforderungen: Siehe folgende Anforderung des Windows-Hardwarekompatibilitätsprogramms: System.Fundamentals.Firmware.UEFISecureBoot	„Sicherer Start“ gemäß UEFI stellt sicher, dass das Gerät nur autorisierten Code startet. Dadurch kann verhindert werden, dass Bootkits und Rootkits installiert werden und zwischen Neustarts erhalten bleiben.
Firmware: Prozess für ein sicheres Firmwareupdate	Anforderungen: UEFI-Firmware muss das sichere Firmwareupdate unterstützen, das unter der folgenden Anforderung des Windows-Hardwarekompatibilitätsprogramms angegeben ist: System.Fundamentals.Firmware.UEFISecureBoot .	UEFI-Firmware kann wie Software Sicherheitsrisiken aufweisen. Falls vorhanden, müssen sie mithilfe von Firmwareupdates gepatcht werden. Die Patches verhindern die Installation von Rootkits.

GRUNDLEGENDER SCHUTZ	BESCHREIBUNG	SICHERHEITSVORTEILE
Software: Qualifiziertes Windows-Betriebssystem	<p>Anforderung: Windows 10 Enterprise, Windows 10 Education, Windows Server 2016 oder Windows 10 Enterprise</p> <div> <p>Wichtig: Als Domänencontroller unterstützt Windows Server 2016 Windows Defender Credential Guard nicht. Mit dieser Konfiguration wird nur Windows Defender Device Guard unterstützt.</p> </div>	Unterstützung von VBS und von Verwaltungsfeatures, welche die Konfiguration von Windows Defender Credential Guard vereinfachen.

IMPORTANT

Die folgenden Tabellen enthalten zusätzliche Qualifikationen für erhöhte Sicherheit. Allerdings wird dringend empfohlen, die Anforderungen für erhöhte Sicherheit einzuhalten, um den Sicherheitsgrad, den Windows Defender Credential Guard gewährleisten kann, deutlich zu erhöhen.

Zusätzliche Sicherheitsqualifikationen 2015 (ab Windows10, Version 1507, und Windows Server2016, Technical Preview 4)

SCHUTZMASSNAHMEN FÜR ERHÖHTE SICHERHEIT	BESCHREIBUNG
Hardware: IOMMU (Input/Output Memory Management Unit, Speicherverwaltungseinheit für die Ein-/Ausgabe)	<p>Anforderung: VT-D oder AMD Vi IOMMU</p> <p>Sicherheitsvorteile: Eine IOMMU kann die Systemresilienz gegenüber Angriffen auf den Arbeitsspeicher verbessern. Weitere Informationen finden Sie unter Tabellen mit ACPI-Beschreibungen.</p>
Firmware: Schützen der Startkonfiguration und -verwaltung	<p>Anforderungen:</p> <ul style="list-style-type: none"> • BIOS-Kennwort oder sicherere Authentifizierung muss unterstützt werden. • In der BIOS-Konfiguration muss die BIOS-Authentifizierung festgelegt sein. • Die geschützte BIOS-Option zum Konfigurieren einer Liste zulässiger Startgeräte (z.B. „Nur von interner Festplatte starten“) und der Reihenfolge von Startgeräten, durch die die vom Betriebssystem vorgenommene BOOTORDER-Änderung überschrieben wird, müssen unterstützt werden. • In der BIOS-Konfiguration müssen sicherheitsbezogene BIOS-Optionen und Startoptionen (Liste zulässiger Startgeräte, Startreihenfolge) geschützt werden, um den Start anderer Betriebssysteme und Änderungen an den BIOS-Einstellungen zu verhindern.
Firmware: Sichere Implementierung von MOR, Version 2	Anforderung: Sichere Implementierung von MOR, Version 2

Zusätzliche Sicherheitsqualifikationen 2016 (ab Windows10, Version 1607, und Windows Server2016)

IMPORTANT

Die folgenden Tabellen enthalten zusätzliche Qualifikationen für erhöhte Sicherheit. Systeme, die diese zusätzlichen Qualifikationen erfüllen, bieten einen stärkeren Schutz.

SCHUTZMASSNAHMEN FÜR ERHÖHTE SICHERHEIT	BESCHREIBUNG	SICHERHEITSVORTEILE
Firmware: Hardware-Vertrauensanker, sicherer Plattformstart	Anforderungen: Startintegrität (sicherer Plattformstart) muss unterstützt werden. Siehe die Anforderungen des Windows-Hardware-Kompatibilitätsprogramms unter System.Fundamentals.Firmware.CS.UEFI SecureBoot.Connected Standby <ul style="list-style-type: none">• HSTI (Hardware Security Test Interface) muss implementiert sein. Siehe Spezifikation zur Prüfbarkeit von Hardwaresicherheit.	Startintegrität (sicherer Plattformstart) nach dem Einschalten bietet Schutzmaßnahmen vor physisch anwesenden Angreifern und eine tiefengestaffelte Verteidigung gegen Schadsoftware. <ul style="list-style-type: none">• HSTI bietet eine zusätzliche Absicherung für ordnungsgemäß geschützte Chip- und Plattformkomponenten.
Firmware: Firmwareupdate über Windows Update	Anforderungen: Die Firmware muss Feldupdates durch Windows Update und UEFI-Kapselungsupdates unterstützen.	Stellt sicher, dass Firmwareupdates schnell, sicher und zuverlässig sind.
Firmware: Schützen der Startkonfiguration und -verwaltung	Anforderungen: <ul style="list-style-type: none">• Erforderliche BIOS-Funktionen: OEMs können während der Fertigung in der Datenbank für „Sicherer Start“ ISV-, OEM- oder Unternehmenszertifikate hinzufügen.• Erforderliche Konfigurationen: Die Microsoft-UEFI-Zertifizierungsstelle muss aus der Datenbank für „Sicherer Start“ entfernt werden. UEFI-Module von Drittanbietern können unterstützt werden, allerdings sollten von ISVs bereitgestellte Zertifikate oder OEM-Zertifikate für die spezifische UEFI-Software genutzt werden.	<ul style="list-style-type: none">• Unternehmen können die Ausführung proprietärer EFI-Treiber/-Anwendungen zulassen.• Durch das Entfernen der Microsoft-UEFI-Zertifizierungsstelle aus der Datenbank für „Sicherer Start“ erhalten Unternehmen die vollständige Kontrolle über Software, die vor dem Betriebssystemstart ausgeführt wird.

Zusätzliche Sicherheitsqualifikationen 2017 (ab Windows10, Version1703)

Die folgende Tabelle enthält die Qualifikationen für Windows10, Version 1703, die zusätzlich zu allen vorherigen Qualifikationen gelten.

SCHUTZMASSNAHMEN FÜR ERHÖHTE SICHERHEIT	BESCHREIBUNG	SICHERHEITSVORTEILE
---	--------------	---------------------

SCHUTZMASSNAHMEN FÜR ERHÖHTE SICHERHEIT	BESCHREIBUNG	SICHERHEITSVORTEILE
<p>Firmware: VBS-Aktivierung von NX-Schutz für UEFI-Laufzeitdienste</p>	<p>Anforderungen:</p> <ul style="list-style-type: none"> • VBS aktiviert NX-Schutz (No-Execute) für Bereiche mit UEFI-Laufzeitdienstcode und -Datenspeicher. UEFI-Laufzeitdienstcode muss Maßnahmen für den schreibgeschützten Seitenschutz unterstützen, und UEFI-Laufzeitdienstdaten dürfen nicht ausführbar sein. • Der UEFI-Laufzeitdienst muss folgende Anforderungen erfüllen: <ul style="list-style-type: none"> – Implementieren von UEFI 2.6 EFI_MEMORY_ATTRIBUTES_TABLE. Alle UEFI-Laufzeitdienstspeicher (Code und Daten) müssen in dieser Tabelle beschrieben werden. – PE-Abschnitte müssen im Speicher seitenausgerichtet sein (nicht erforderlich für nicht flüchtigen Speicher). – Die Tabelle mit Speicherattributen muss Code und Daten ordnungsgemäß als RO/NX für die Konfiguration durch das Betriebssystem markieren: <ul style="list-style-type: none"> – Alle Einträge müssen das Attribut EFI_MEMORY_RO und/oder das Attribut EFI_MEMORY_XP enthalten. – Es dürfen keine Einträge mit einem der oben genannten Attribute verbleiben, die angeben, dass der Speicher sowohl ausführbar als auch beschreibbar ist. Speicher muss entweder lesbar und ausführbar oder beschreibbar und nicht ausführbar sein. <div data-bbox="598 1370 997 1597" style="border: 1px solid black; padding: 5px;"> <p>Hinweise:</p> <ul style="list-style-type: none"> • Dies gilt nur für UEFI-Laufzeitdienstspeicher und nicht für UEFI-Startdienstspeicher. • Dieser Schutz wird von VBS für Betriebssystem-Seitentabellen angewendet. </div> <p>Beachten Sie außerdem Folgendes:</p> <ul style="list-style-type: none"> • Verwenden Sie keine Abschnitte, die sowohl beschreibbar als auch ausführbar sind. • Versuchen Sie nicht, ausführbaren Systemspeicher direkt zu ändern. • Verwenden Sie keinen dynamischen Code. 	<ul style="list-style-type: none"> • Sofern Sicherheitslücken in der UEFI-Laufzeit vorhanden sind, wird verhindert, dass sie VBS gefährden (z.B. in Funktionen wie UpdateCapsule und SetVariable). • Verringert die VBS-Angriffsfläche für Systemfirmware.

SCHUTZMASSNAHMEN FÜR ERHÖHTE SICHERHEIT	BESCHREIBUNG	SICHERHEITSVORTEILE
Firmware: Firmwareunterstützung für SMM-Schutz	<p>Anforderungen: In der WSMT (Windows SMM Security Mitigations Table)-Spezifikation wird eine ACPI (Advanced Configuration and Power Interface)-Tabelle ausführlich beschrieben. Sie wurde zur Verwendung mit Windows-Betriebssystemen erstellt, die Windows-Features für virtualisierungsbasierte Sicherheit (VBS) unterstützen.</p>	<ul style="list-style-type: none"> • Schützt ggf. vor potenziellen Sicherheitsrisiken im UEFI-Laufzeitdienst, und die Gefährdung von VBS (z.B. in Funktionen wie UpdateCapsule und SetVariable) wird verhindert. • Verringert die VBS-Angriffsfläche für Systemfirmware. • Verhindert zusätzliche Sicherheitsangriffe auf SMM.

Verwalten von Windows Defender Credential Guard

20.02.2020 • 9 minutes to read

Betrifft:

- Windows 10
- Windows Server 2016
- Windows Server 2019

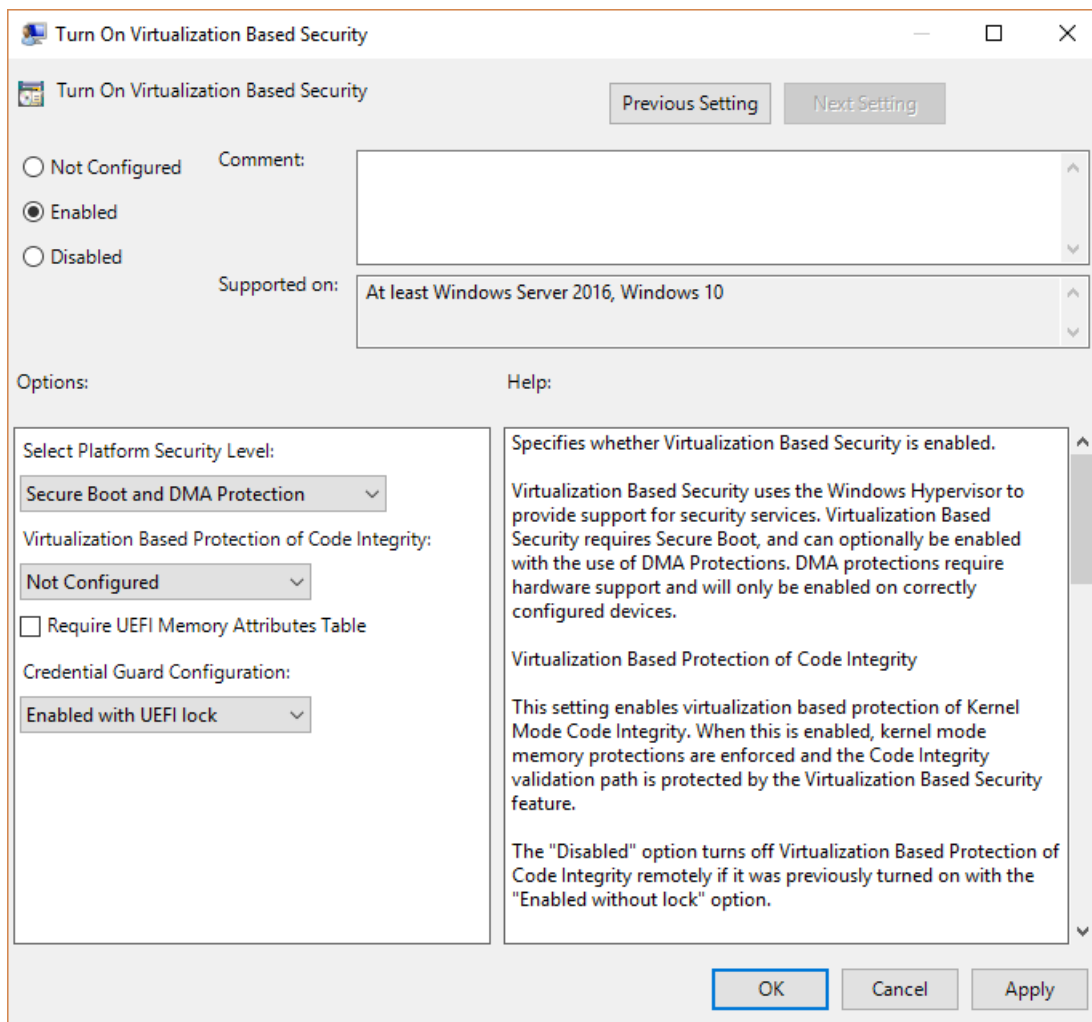
Aktivieren von Windows Defender Credential Guard

Windows Defender Credential Guard kann mit der [Gruppenrichtlinie](#), der [Registrierung](#) oder dem [Hardware-Vorbereitungstool](#) für Windows Defender Device Guard und Windows Defender Credential Guard aktiviert werden. Windows Defender Credential Guard kann geheime Schlüssel auf einem virtuellen Hyper-V-Computer genau wie auf einem physischen Computer schützen. Sie können Windows Defender Credential Guard auf virtuellen Computern auf dieselbe Weise aktivieren wie auf physischen Computern.

Aktivieren von Windows Defender Credential Guard mithilfe der Gruppenrichtlinie

Sie können Gruppenrichtlinien zum Aktivieren von Windows Defender Credential Guard verwenden. Dadurch werden ggf. Funktionen für die virtualisierungsbasierte Sicherheit hinzugefügt und für Sie aktiviert.

1. Wechseln Sie auf der Gruppenrichtlinien-Verwaltungskonsolle zu **Computerkonfiguration** -> **Administrative Vorlagen** -> **System** -> **Device Guard**.
2. Doppelklicken Sie auf **Virtualisierungsbasierte Sicherheit aktivieren**, und klicken Sie dann auf die Option **Aktiviert**.
3. Wählen Sie im Feld **Plattform-Sicherheitsstufe auswählen** die Option **Sicherer Start** oder **Sicherer Start und DMA-Schutz** aus.
4. Klicken Sie im Feld **Credential Guard-Konfiguration** auf **Mit UEFI-Sperre aktiviert**, und klicken Sie dann auf **OK**. Wenn Sie die Möglichkeit zur Remotedeaktivierung von Windows Defender Credential Guard haben möchten, wählen Sie **Ohne Sperre aktiviert** aus.



5. Schließen Sie die Gruppenrichtlinien-Verwaltungskonsole.

Führen Sie `gpupdate /force` aus, um die Verarbeitung der Gruppenrichtlinie zu erzwingen.

Aktivieren von Windows Defender-Anmelde Informationsschutz mithilfe von InTune

1. Von **zu Hause** aus auf **Microsoft InTune** klicken
2. Klicken Sie auf **Gerätekonfiguration**.
3. Klicken Sie auf **profile** > , um den **Windows Defender-Anmelde Informationsschutz** für **Profil** > **Endpunkt** > zu erstellen.

NOTE

Dadurch wird VBS und Secure Boot aktiviert, und Sie können es mit oder ohne UEFI-Sperre tun. Wenn Sie die Berechtigungsüberwachung Remote deaktivieren müssen, aktivieren Sie Sie ohne UEFI-Sperre.

Aktivieren von Windows Defender Credential Guard mithilfe der Registrierung

Wenn Sie keine Gruppenrichtlinien verwenden, können Sie Windows Defender Credential Guard mithilfe der Registrierung aktivieren. Windows Defender Credential Guard verwendet Features für die virtualisierungsbasierte Sicherheit, die bei einigen Betriebssystemen zunächst aktiviert werden müssen.

Hinzufügen der virtualisierungsbasierten Sicherheitsfunktionen

Ab Windows 10, Version 1607, und Windows Server 2016 müssen Windows-Features zur Verwendung der virtualisierungsbasierten Sicherheit nicht aktiviert werden, und dieser Schritt kann daher übersprungen werden.

Wenn Sie Windows 10, Version 1507 (RTM), oder Windows 10, Version 1511, verwenden, müssen Windows-Features aktiviert werden, um die virtualisierungsbasierte Sicherheit zu nutzen. Hierzu können Sie entweder die Systemsteuerung oder das DISM-Tool (Deployment Image Servicing and Management, Abbildverwaltung für die

Bereitstellung) verwenden.

NOTE

Wenn Sie Windows Defender Credential Guard über Gruppenrichtlinien aktivieren, sind die Schritte zum Aktivieren von Windows-Features über die Systemsteuerung oder DISM nicht nötig. Die Gruppenrichtlinien installieren Windows-Funktionen für Sie.

Hinzufügen der virtualisierungsbasierten Sicherheitsfunktionen mit „Programme und Funktionen“

1. Öffnen Sie in der Systemsteuerung „Programme und Funktionen“.
2. Klicken Sie auf die Option **Windows-Features aktivieren oder deaktivieren**.
3. Wählen Sie **Hyper-V** -> **Hyper-V-Plattform**, und aktivieren Sie dann das Kontrollkästchen **Hyper-V-Hypervisor**.
4. Aktivieren Sie auf oberster Ebene der Featureauswahl das Kontrollkästchen **Isolierter Benutzermodus**.
5. Klicken Sie auf **OK**.

Hinzufügen der virtualisierungsbasierten Sicherheitsfunktionen zu einem Offlineimage mit DISM

1. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten.
2. Fügen Sie den Hyper-V-Hypervisor mit dem folgenden Befehl hinzu:

```
dism /image:<WIM file name> /Enable-Feature /FeatureName:Microsoft-Hyper-V-Hypervisor /all
```
3. Fügen Sie das Feature für den isolierten Benutzermodus mit dem folgenden Befehl hinzu:

```
dism /image:<WIM file name> /Enable-Feature /FeatureName:IsolatedUserMode
```

 > [!NOTE] > In Windows 10, Version 1607 und höher, wurde das Feature für den isolierten Benutzermodus in das zentrale Betriebssystem integriert. Die Ausführung des Befehls in Schritt 3 ist daher nicht mehr erforderlich.

NOTE

Sie können diese Features auch einem Onlineimage hinzufügen, indem Sie entweder DISM oder Configuration Manager nutzen.

Aktivieren von virtualisierungsbasierter Sicherheit und Windows Defender Credential Guard

1. Öffnen Sie den Registrierungs-Editor.
2. Aktivieren Sie die virtualisierungsbasierte Sicherheit:
 - Suchen Sie den Eintrag HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Device Guard.
 - Fügen Sie einen neuen DWORD-Wert mit dem Namen **EnableVirtualizationBasedSecurity** hinzu. Legen Sie den Wert dieser Registrierungseinstellung auf 1 fest, um die virtualisierungsbasierte Sicherheit zu aktivieren, und legen Sie den Wert auf 0 fest, um sie zu deaktivieren.
 - Fügen Sie einen neuen DWORD-Wert mit dem Namen **RequirePlatformSecurityFeatures** hinzu. Legen Sie den Wert dieser Registrierungseinstellung auf 1 fest, um nur **Sicherer Start** zu verwenden, oder legen Sie ihn auf 3 fest, um **Sicherer Start und DMA-Schutz** zu verwenden.
3. Aktivieren Sie Windows Defender Credential Guard:
 - Suchen Sie den Eintrag HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA.
 - Fügen Sie einen neuen DWORD-Wert mit dem Namen **LsaCfgFlags** hinzu. Legen Sie den Wert dieser Registrierungseinstellung auf 1 fest, um Windows Defender Credential Guard mit UEFI-Sperre zu aktivieren. Legen Sie ihn auf 2 fest, um Windows Defender Credential Guard ohne Sperre zu aktivieren, und legen Sie ihn zum Deaktivieren auf 0 fest.
4. Schließen Sie den Registrierungs-Editor.

NOTE

Sie können Windows Defender Credential Guard auch aktivieren, indem Sie die Registrierungseinträge in der Einstellung [FirstLogonCommands](#) für die unbeaufsichtigte Installation festlegen.

Aktivieren von Windows Defender Credential Guard mithilfe des Hardware-Vorbereitungstools für Windows Defender Device Guard und Windows Defender Credential Guard

Sie können Windows Defender Credential Guard auch mit dem [Hardware-Vorbereitungstool für Windows Defender Device Guard und Windows Defender Credential Guard](#) aktivieren.

```
DG_Readiness_Tool.ps1 -Enable -AutoReboot
```

IMPORTANT

Bei der Ausführung des Windows Defender Device Guard und des Windows Defender-Anmelde Informationsschutzes für das Hardware-Bereitschafts Tool auf einem nicht englischen Betriebssystem innerhalb des

```
$OSArch = $(gwmi win32_operatingsystem).OSArchitecture
```

 Skripts ändern

```
$OSArch = $((gwmi win32_operatingsystem).OSArchitecture).tolower()
```

 Sie den Namen stattdessen, damit das Tool funktioniert. Dies ist ein bekanntes Problem.

Überprüfen der Leistung von Windows Defender Credential Guard

Wird Windows Defender Credential Guard ausgeführt?

Über Systeminformationen können Sie sicherstellen, dass Windows Defender Credential Guard auf einem PC ausgeführt wird.

1. Klicken Sie auf **Start**, geben Sie **msinfo32.exe** ein, und klicken Sie dann auf **Systeminformationen**.
2. Klicken Sie auf **Systemübersicht**.
3. Überprüfen Sie, ob **Credential Guard** neben **Virtualisierungsbasierte Sicherheitsdienste konfigurieren** angezeigt wird.

Beispiel:

Page title	C:\pageinfo.sys
Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Co
Virtualization-based security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Services Running	

Sie können auch mit dem [Hardware-Vorbereitungstool für Windows Defender Device Guard und Windows Defender Credential Guard](#) überprüfen, ob Windows Defender Credential Guard ausgeführt wird.

```
DG_Readiness_Tool_v3.6.ps1 -Ready
```

IMPORTANT

Bei der Ausführung des Windows Defender Device Guard und des Windows Defender-Anmelde Informationsschutzes für das Hardware-Bereitschafts Tool auf einem nicht englischen Betriebssystem innerhalb des

```
*$OSArch = $(gwmi win32_operatingsystem).OSArchitecture
```

 Skripts ändern

```
$OSArch = $((gwmi win32_operatingsystem).OSArchitecture).tolower()
```

 Sie den Namen stattdessen, damit das Tool funktioniert. Dies ist ein bekanntes Problem.

NOTE

Auf Clientcomputern mit Windows 10 1703 wird Lsalso.exe ausgeführt, wenn die virtualisierungsbasierte Sicherheit für andere Features aktiviert ist.

- Aktivieren Sie deshalb Windows Defender Credential Guard, bevor ein Gerät einer Domäne beitrifft. Wenn Windows Defender Credential Guard auf einem Gerät aktiviert wird, nachdem es einer Domäne beigetreten ist, können die geheimen Schlüssel der Benutzer und Geräte bereits beeinträchtigt worden sein. Anders gesagt trägt das Aktivieren von Credential Guard nicht dazu bei, ein Gerät oder eine Identität, das bzw. die bereits beeinträchtigt wurde, zu sichern. Deshalb wird empfohlen, Credential Guard so früh wie möglich zu aktivieren.
- Sie sollten regelmäßige Überprüfungen der PCs durchführen, für die Windows Defender Credential Guard aktiviert ist. Dies kann mit Sicherheitsüberwachungsrichtlinien oder WMI-Abfragen erfolgen. Suchen Sie nach den folgenden WinInit-Ereignis-IDs:
 - **Ereignis-ID 13** Windows Defender Credential Guard (Lsalso.exe) wurde gestartet und schützt LSA-Anmeldeinformationen.
 - **Ereignis-ID 14** Konfiguration von Windows Defender Credential Guard (Lsalso.exe): 0x1, 0
 - Der erste Variable, 0x1, bedeutet, dass Windows Defender Credential Guard für die Ausführung konfiguriert ist. 0x0 bedeutet, dass er nicht für die Ausführung konfiguriert ist.
 - Die zweite Variable, 0, bedeutet, dass Credential Guard für die Ausführung im geschützten Modus konfiguriert ist. 1 bedeutet, dass sie für die Ausführung im Testmodus konfiguriert ist. Diese Variable sollte immer 0 sein.
 - **Ereignis-ID 15** Windows Defender Credential Guard (Lsalso.exe) ist konfiguriert, aber der sichere Kernel wird nicht ausgeführt; der Vorgang wird ohne Windows Defender Credential Guard fortgesetzt.
 - **Ereignis-ID 16** Fehler beim Starten von Windows Defender Credential Guard (Lsalso.exe): [Fehlercode]
 - **Ereignis-ID 17** Fehler beim Lesen der UEFI-Konfiguration von Windows Defender Credential Guard (Lsalso.exe): [Fehlercode] Sie können auch sicherstellen, dass TPM für den Schlüsselschutz verwendet wird, indem Sie unter der Ereignisquelle **Microsoft** -> **Windows** -> **Kernel-Boot** die Ereignis-ID 51 überprüfen. Wenn die Ausführung mit einem TPM erfolgt, hat der Wert der TPM-PCR-Maske einen anderen Wert als 0.
 - **Ereignis-ID 51** Bereitstellung des VSM-Masterverschlüsselungsschlüssels. Der Status der zwischengespeicherten Kopie wird verwendet: 0x0. Die Versiegelung des Status der zwischengespeicherten Kopie wird aufgehoben: 0x1. Status der Generierung des neuen Schlüssels: 0x1. Versiegelungsstatus: 0x1. TPM-PCR-Maske: 0x0.

Deaktivieren Sie Windows Defender Credential Guard

Zum Deaktivieren der Windows Defender-Anmelde Informationsschutz Funktion können Sie den folgenden Satz von Verfahren oder [das Hardware Readiness Tool für Geräteschutz und Anmeldeinformationen](#) verwenden. Wenn die Anmeldeinformation Guard mit UEFI-Sperre aktiviert wurde, müssen Sie das folgende Verfahren verwenden, da die Einstellungen in EFI-Variablen (Firmware) beibehalten werden und die physische Anwesenheit auf dem Computer erforderlich ist, um eine Funktionstaste zu drücken, um die Änderung zu übernehmen. Wenn die Berechtigungs Überwachung ohne UEFI-Sperre aktiviert wurde, können Sie Sie mithilfe von Gruppenrichtlinien deaktivieren.

1. Wenn Sie Gruppenrichtlinien verwendet haben, deaktivieren Sie die Gruppenrichtlinien-Einstellung, die Sie für die Aktivierung von Windows Defender Credential Guard verwendet haben (**Computerkonfiguration** -> **Administrative Vorlagen** -> **System** -> **Device Guard** -> **Virtualisierungsbasierte Sicherheit aktivieren**).
2. Löschen Sie die folgenden Registrierungseinstellungen:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\LsaCfgFlags
- HKEY _LOCAL _MACHINE \software\policies\microsoft\windows\deviceguard\lsacfgflags

3. Wenn Sie auch die Virtualisierungs-basierte Sicherheit deaktivieren möchten, löschen Sie die folgenden Registrierungseinstellungen:

- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Device Guard\EnableVirtualizationBasedSecurity
- HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Device Guard\RequirePlatformSecurityFeatures > [!IMPORTANT] > Wenn Sie diese Registrierungseinstellungen manuell entfernen, stellen Sie sicher, dass Sie alle löschen. Wenn Sie nicht alle entfernen, kann das Gerät zur BitLocker-Wiederherstellung wechseln.

4. Löschen Sie die EFI-Variablen von Windows Defender Credential Guard mithilfe von bcdedit. Geben Sie in einer Eingabeaufforderung mit erhöhten Rechten die folgenden Befehle ein:

```
mountvol X: /s
copy %WINDIR%\System32\SecConfig.efi X:\EFI\Microsoft\Boot\SecConfig.efi /Y
bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\SecConfig.efi"
bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions DISABLE-LSA-ISO
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:
mountvol X: /d
```

5. Starten Sie den PC neu.

6. Stimmen Sie der Aufforderung zum Deaktivieren von Windows Defender Credential Guard zu.

7. Alternativ können Sie die virtualisierungsbasierten Sicherheitsfunktionen deaktivieren, um Windows Defender Credential Guard zu deaktivieren.

NOTE

Der PC benötigt einen einmaligen Zugriff auf einen Domänencontroller zur Entschlüsselung des Inhalts, z.B. Dateien, die mit EFS verschlüsselt wurden. Wenn Sie sowohl den Windows Defender-Anmelde Informationsschutz als auch die Virtualisierungs-basierte Sicherheit deaktivieren möchten, führen Sie die folgenden bcdedit-Befehle aus, nachdem Sie alle auf Virtualisierung basierenden Sicherheitsgruppen Richtlinien und Registrierungseinstellungen deaktiviert haben:

```
bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions DISABLE-LSA-ISO,DISABLE-VBS
bcdedit /set vsmLaunchType off
```

NOTE

Bei Verwendung von Azure IaaS VMS werden die Anmeldeinformationen Guard und Device Guard zurzeit nicht unterstützt. Diese Optionen werden für Future Generation 2 VMS zur Verfügung gestellt.

Weitere Informationen zur virtualisierungsbasierten Sicherheit und Windows Defender Device Guard finden Sie im [Windows Defender Device Guard-Bereitstellungshandbuch](#).

Deaktivieren von Windows Defender Credential Guard mithilfe des Hardware-Vorbereitungstools für Windows Defender Device Guard und Windows Defender Credential Guard

Sie können Windows Defender Credential Guard auch mit dem [Hardware-Vorbereitungstool für Windows Defender Device Guard und Windows Defender Credential Guard](#) deaktivieren.

```
DG_Readiness_Tool_v3.6.ps1 -Disable -AutoReboot
```

IMPORTANT

Bei der Ausführung des Windows Defender Device Guard und des Windows Defender-Anmelde Informationsschutzes für das Hardware-Bereitschafts Tool auf einem nicht englischen Betriebssystem innerhalb des

```
*$OSArch = $(gwmi win32_operatingsystem).OSArchitecture
```

 Skripts ändern

```
$OSArch = $((gwmi win32_operatingsystem).OSArchitecture).tolower()
```

 Sie den Namen stattdessen, damit das Tool funktioniert. Dies ist ein bekanntes Problem.

Deaktivieren von Windows Defender Credential Guard für einen virtuellen Computer

Vom Host aus können Sie Windows Defender Credential Guard für einen virtuellen Computer deaktivieren:

```
Set-VMSecurity -VMName <VMName> -VirtualizationBasedSecurityOptOut $true
```


Von Windows Defender Credential Guard nicht abdeckte Schutzszenarien

27.12.2019 • 2 minutes to read

Betrifft:

- Windows 10
- Windows Server2016

Einige Methoden zum Speichern von Anmeldeinformationen sind nicht durch Windows Defender Credential Guard geschützt, darunter:

- Software, mit der Anmeldeinformationen außerhalb des Schutzes durch Windows-Features verwaltet werden
- Lokale Konten und Microsoft-Konten
- Windows Defender Credential Guard schützt nicht die auf Windows Server2016-Domänencontrollern ausgeführte Active Directory-Datenbank. Auch Anmeldeinformationen-Eingabepipelines wie Windows Server2016-Server mit Remotedesktopgateway werden nicht geschützt. Wenn Sie einen Windows Server 2016-Server als Client-PC verwenden, erhält er denselben Schutz wie beim Ausführen von Windows10 Enterprise.
- Keylogger
- Physische Angriffe
- Verhindert nicht, dass ein Angreifer mit Schadsoftware auf dem PC die Anmeldeinformationen zugeordneten Privilegien verwendet. Verwenden Sie möglichst dedizierte PCs für besonders wichtige Konten, z.B. für die von IT-Spezialisten und Benutzer mit Zugriff auf wertvolle Ressourcen in Ihrer Organisation.
- Sicherheitspakete von Drittanbietern
- Digest- und CredSSP-Anmeldeinformationen
 - Wenn Windows Defender Credential Guard aktiviert ist, haben weder Digest noch CredSSP Zugriff auf die Anmeldeinformationen von Benutzern. Dies bedeutet keine Verwendung von einmaligem Anmelden für diese Protokolle.
- Für die NTLM-Authentifizierung angegebene Anmeldeinformationen sind nicht geschützt. Wenn ein Benutzer dazu aufgefordert wird und Anmeldeinformationen für die NTLM-Authentifizierung eingibt, sind diese Anmeldeinformationen anfällig für das Lesen aus dem LSASS-Arbeitsspeicher. Beachten Sie, dass dieselben Anmeldeinformationen auch für Keylogger anfällig sind.
- Kerberos-Diensttickets sind nicht durch den Anmelde Informationsschutz geschützt, aber das Kerberos-Ticket-Grant-Ticket (TGT) ist.
- Wenn Windows Defender Credential Guard auf einem virtuellen Computer bereitgestellt wird, schützt Windows Defender Credential Guard geheime Schlüssel vor Angriffen innerhalb des virtuellen Computers. Credential Guard bietet jedoch keinen zusätzlichen Schutz vor Systemangriffen, die von einem Host mit privilegiertem Zugriff stammen.
- Bei Überprüfungen zwischengespeicherter Kennwörter für die Windows-Anmeldung (häufig „zwischengespeicherte Anmeldeinformationen“ genannt) eignen sich nicht als Anmeldeinformationen, weil sie nicht zur Authentifizierung für einen anderen Computer bereitgestellt und nur zur lokalen Überprüfung von Anmeldeinformationen verwendet werden können. Sie werden auf dem lokalen Computer in der Registrierung gespeichert und ermöglichen die Überprüfung von Anmeldeinformationen, wenn ein in die Domäne eingebundener Computer bei der Anmeldung eines Benutzers keine Verbindung mit AD DS herstellen kann. Diese „zwischengespeicherten Anmeldeinformationen“ bzw. zwischengespeicherten Domänenkontoinformationen können mithilfe der folgenden Sicherheitsrichtlinieneinstellung verwaltet

werden: **Interaktive Anmeldung: Anzahl zwischenspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist).**

Weitere Informationen:

Deep Dive into Windows Defender Credential Guard: Themenverwandte Videos

[Microsoft Cyber Stack: erweiterter Identitäts-und Endpunktschutz: Verwalten von Anmeldeinformationen Guard](#)

NOTE

- Hinweis: erfordert das [LinkedIn Learning-Abonnement](#) , um das vollständige Video anzuzeigen

Überlegungen zur Verwendung von Windows Defender Credential Guard

04.12.2019 • 6 minutes to read

Gilt für:

- Windows 10
- Windows Server2016

Kennwörter sind weiterhin unsicher. Wir empfehlen Ihnen daher, in Ihrer Organisation anstelle von Kennwörtern Windows Defender Credential Guard und andere Authentifizierungsmethoden zu verwenden, z.B. physische Smartcards, virtuelle Smartcards oder Windows Hello for Business.

Windows Defender Credential Guard verwendet Hardwaresicherheit, sodass einige Features wie Windows To Go nicht unterstützt werden.

Überlegungen zu WLAN und VPN

Wenn Sie Windows Defender-Anmelde Informationsschutz aktivieren, können Sie die NTLM-klassische Authentifizierung für einmaliges Anmelden nicht mehr verwenden. Sie werden gezwungen, Ihre Anmeldeinformationen einzugeben, um diese Protokolle zu verwenden, und können die Anmeldeinformationen nicht für die spätere Verwendung speichern. Wenn Sie auf MS-CHAPv2 basierende WLAN- und VPN-Endpunkte verwenden, können diese von ähnlichen Angriffen wie NTLMv1 betroffen sein. Für WLAN- und VPN-Verbindungen empfiehlt Microsoft Organisationen, von MSCHAPv2-basierten Verbindungen wie PEAP-MSCHAPv2 und EAP-MSCHAPv2 auf eine zertifikatbasierte Authentifizierung wie PEAP-TLS oder EAP-TLS umzusteigen.

Überlegungen zu Kerberos

Wenn Sie Windows Defender Credential Guard aktivieren, können Sie die uneingeschränkte Kerberos-Delegierung oder DES-Verschlüsselung nicht mehr verwenden. Die uneingeschränkte Delegierung könnte es Angreifern ermöglichen, Kerberos-Schlüssel aus dem isolierten LSA-Prozess zu extrahieren. Sie müssen stattdessen die eingeschränkte oder ressourcenbasierte Kerberos-Delegierung verwenden.

Sicherheitsaspekte bei der Sicherheitsunterstützung von Drittanbietern

Einige Drittanbieter von Sicherheitsunterstützung (SSPs und Zugriffspunkte) sind möglicherweise nicht kompatibel mit Windows Defender Credential Guard, da die Lösung nicht zulässt, dass Drittanbieter-SSPs Kennworthashes von LSA abfragen. SSPs und Zugriffspunkte werden aber weiterhin über das Kennwort informiert, wenn sich ein Benutzer anmeldet bzw. sein Kennwort ändert. Die Verwendung von undokumentierten APIs in benutzerdefinierten SSPs und Zugriffspunkten wird nicht unterstützt. Wir empfehlen, benutzerdefinierte Implementierungen von SSPs/Zugriffspunkten mit Windows Defender Credential Guard zu testen. SSPs und Zugriffspunkte, die auf einem undokumentierten oder nicht unterstützten Verhalten basieren, werden nicht akzeptiert. Beispielsweise wird die Verwendung der KerberosQuerySupplementalCredentialsMessage-API nicht unterstützt. Ersetzen Sie NTLM- oder Kerberos-SSPs durch benutzerdefinierte SSPs und Zugriffspunkte. Weitere Informationen finden Sie unter [Beschränkungen für das Registrieren und Installieren eines Sicherheitspakets](#) auf der MSDN-Website.

Überlegungen zu Upgrades

Da die von der Windows Defender-Anmeldeinformation Guard bereitgestellten tiefen-und breiten Schutzbestimmungen erhöht werden, können sich nachfolgende Versionen von Windows10 mit Windows Defender-Anmeldeinformationen Guard auf die in der Vergangenheit ausgeführten Szenarien auswirken. Möglicherweise blockiert Windows Defender Credential Guard die Verwendung eines bestimmten Typs von Anmeldedaten oder eine bestimmte Komponente, damit Schadsoftware keine Sicherheitslücken ausnutzen kann. Testen Sie Szenarien, die für Vorgänge in einer Organisation wichtig sind, vor dem Upgrade eines Geräts mit Windows Defender Credential Guard.

Windows-Anmeldedaten geschützt gespeichert

Beginnend mit Windows10, Version 1511, werden Domänenanmeldeinformationen, die mit dem Anmelde Informations-Manager gespeichert sind, mit Windows Defender-Anmelde Informationsschutz geschützt. Mit der Anmeldeinformationsverwaltung können Sie drei Typen von Anmeldedaten speichern: Windows-Anmeldedaten, zertifikatbasierte Anmeldedaten und generische Anmeldedaten. Generische Anmeldedaten, z.B. Benutzernamen und Kennwörter, die Sie zur Anmeldung bei Websites verwenden, sind nicht geschützt, da die Anwendungen Ihr Kennwort im Klartext benötigen. Wenn die Anwendung keine Kopie des Kennworts benötigt, können Sie Anmeldedaten für die Domäne als Windows-Anmeldeidaten speichern, die geschützt sind. Windows-Anmeldedaten werden verwendet, um eine Verbindung mit anderen Computern in einem Netzwerk herzustellen. Für den Windows Defender Credential Guard-Schutz für die Anmeldeinformationsverwaltung sollten Sie Folgendes berücksichtigen:

- Von Remotedesktop-Client gespeicherte Windows-Anmeldedaten können nicht an einen Remotehost gesendet werden. Versuche, gespeicherte Windows-Anmeldedaten zu verwenden, schlagen fehl. Die Fehlermeldung „Anmeldeversuch ist fehlgeschlagen.“ wird angezeigt.
- Anwendungen, die Windows-Anmeldedaten extrahieren, funktionieren nicht.
- Wenn die Anmeldedaten auf einem PC gesichert sind, auf dem Windows Defender Credential Guard aktiviert ist, können die Windows-Anmeldedaten nicht wiederhergestellt werden. Wenn Sie Ihre Anmeldedaten sichern müssen, müssen Sie dies tun, bevor Sie Windows Defender Credential Guard aktivieren. Andernfalls können Sie diese Anmeldedaten nicht wiederherstellen.

Überlegungen zum Löschen des TPM

Virtualisierungsbasierte Sicherheit (VBS) verwendet das TPM, um den Schlüssel zu schützen. Wird das TPM gelöscht, geht der vom TPM geschützte Schlüssel zum Verschlüsseln der VBS-Geheimnisse verloren.

WARNING

Das Löschen des TPM führt zu einem Verlust der geschützten Daten für alle Features, die VBS verwenden, um Daten zu schützen.

Nachdem ein TPM gelöscht ist, können sämtliche Features, die VBS verwenden, um Daten zu schützen, ihre geschützten Daten nicht mehr entschlüsseln.

Dementsprechend kann auch Credential Guard geschützte Daten nicht mehr entschlüsseln. VBS erstellt einen neuen, von TPM geschützten Schlüssel für Credential Guard. Credential Guard verwendet den neuen Schlüssel, um neue Daten zu schützen. Alle vorher geschützten Daten sind unwiederbringlich verloren.

NOTE

Credential Guard erhält den Schlüssel während der Initialisierung. Somit betrifft der Datenverlust nur persistente Daten und tritt erst nach dem nächsten Systemstart ein.

Von der Anmeldeinformationsverwaltung gesicherte Windows-Anmeldedaten

Da die Anmeldeinformationsverwaltung gespeicherten Windows-Anmeldedaten nicht entschlüsseln kann, werden

diese gelöscht. Anwendungen sollten zur Eingabe von Anmeldedaten auffordern, die zuvor gespeichert wurden. Nachdem sie erneut gespeichert wurden, sind die Windows-Anmeldedaten durch Credential Guard geschützt.

Automatisch bereitgestellte öffentliche Schlüssel für Geräte in einer Domäne

Ab Windows 10 und Windows Server 2016 stellen Domänengeräte automatisch einen gebundenen öffentlichen Schlüssel bereit. Weitere Informationen über die automatische öffentliche Schlüsselbereitstellung finden Sie unter [Domain-joined Device Public Key Authentication](#).

Da Credential Guard den geschützten privaten Schlüssel nicht entschlüsseln kann, verwendet Windows das Kennwort des zur Domäne gehörenden Computers zur Authentifizierung in der Domäne. Solange keine zusätzlichen Richtlinien bereitgestellt werden, gibt es keinen Funktionalitätsverlust. Wenn ein Gerät so konfiguriert wurde, dass es nur öffentliche Schlüssel verwendet, ist eine Authentifizierung per Kennwort erst nach der Deaktivierung dieser Richtlinie möglich. Weitere Informationen zum Konfigurieren von Geräten, die nur öffentliche Schlüssel verwenden, finden Sie unter [Domain-joined Device Public Key Authentication](#).

Ebenfalls fehlschlagen werden Zugriffsprüfungen (einschließlich Authentifizierungsrichtlinien), die voraussetzen, dass Geräte über die bekannten SIDs KEY TRUST IDENTITY (S-1-18-4) oder FRESH PUBLIC KEY IDENTITY (S-1-18-3) verfügen. Weitere Informationen über Authentifizierungsrichtlinien finden Sie unter [Authentifizierungsrichtlinien und Authentifizierungsrichtliniensilos](#). Weitere Informationen zu bekannten SIDs finden Sie unter [\[MS-DTYP\] Section 2.4.2.4 Well-known SID Structures](#).

DPAPI auf Geräte in einer Domäne

Auf den zu einer Domäne gehörenden Geräten kann DPAPI Schlüssel des Benutzers mit einem Domänencontroller aus der Domäne des Benutzers wiederherstellen. Wenn ein Domänengerät über keine Verbindung mit einem Domänencontroller verfügt, ist die Wiederherstellung nicht möglich.

IMPORTANT

Das Löschen eines TPM auf einem Domänengerät sollte daher in einem Netzwerk mit Konnektivität zu Domänencontrollern erfolgen. Dadurch ist sichergestellt, dass DPAPI-Funktionen ausgeführt werden und der Benutzer kein ungewöhnliches Verhalten bemerkt.

Die automatische VPN-Konfiguration ist durch Benutzer-DPAPI geschützt. Benutzer können VPN möglicherweise nicht verwenden, um Verbindungen zu Domänencontrollern herzustellen, da die VPN-Konfigurationen verloren gegangen sind.

Wenn Sie das TPM auf einem Domänengerät ohne Verbindung zu den Domänencontrollern löschen müssen, sollten Sie Folgendes beachten.

Benutzeranmeldung auf einem Domänengerät nach dem Löschen eines TPM für die Zeit, in der keine Verbindung mit einem Domänencontroller besteht:

ANMELEDATENTYP	WINDOWS10-VERSION	VERHALTEN
Zertifikat (Smartcard oder Windows Hello for Business)	Alle	Alle mit der Benutzer DPAPI geschützten Daten sind nicht mehr verwendbar, und die Benutzer-DPAPI funktioniert nicht mehr.
Kennwort	Windows10 v1709 oder eine spätere Versionen	Wenn sich Benutzer vor dem Löschen des TPM mit einem Zertifikat oder einem Kennwort angemeldet haben, können sie sich mit Kennwort anmelden, und die Benutzer-DPAPI ist nicht betroffen.

ANMELDEDATENTYP	WINDOWS10-VERSION	VERHALTEN
Kennwort	Windows10 v1703	Wenn sich Benutzer vor dem Löschen des TPM mit einem Kennwort angemeldet haben, können sie sich mit diesem Kennwort anmelden und sind nicht betroffen.
Kennwort	Windows10 v1607 oder früher	Vorhandene DPAPI-geschützte Benutzerdaten sind nicht mehr verwendbar. Benutzer-DPAPI kann neue Daten schützen.

Nachdem das Gerät über Konnektivität zum Domänencontroller verfügt, stellt DPAPI den Schlüssel des Benutzers wieder her, und vor dem Löschen des TPM geschützte Daten können entschlüsselt werden.

Auswirkungen eines DPAPI-Ausfalls auf Windows Information Protection

Wenn die per Benutzer-DPAPI geschützten Daten unbrauchbar sind, verliert der Benutzer den Zugriff auf alle von Windows Information Protection geschützten Arbeitsdaten. Zu den Auswirkung gehört: Outlook 2016 kann nicht gestartet und geschützte Arbeitsdokumente können nicht geöffnet werden. Wenn DPAPI funktioniert, werden neu erstellte Arbeitsdaten geschützt und können abgerufen werden.

Problemumgehung: Benutzer können das Problem beheben, indem Sie ihr Gerät mit der Domäne verbinden und neu starten oder ihr Data Recovery Agent-Zertifikat für das Encrypting File System verwenden. Weitere Informationen über das Recovery Agent-Zertifikat für das Encrypting File System finden Sie unter [Erstellen und Überprüfen eines Datenwiederherstellungs-Agent \(DRA\)-Zertifikats des verschlüsselnden Dateisystems \(Encrypting File System, EFS\)](#).

Weitere Informationen

Verwandte Videos

[Was ist die Virtualisierungs-basierte Sicherheit?](#)

Weitere Risikominderungen

23.12.2019 • 18 minutes to read

Windows Defender Credential Guard kann das Risiko von Angriffen auf abgeleitete Anmeldeinformationen mindern und die Verwendung von gestohlenen Anmeldeinformationen an anderer Stelle verhindern. PCs können trotzdem weiterhin anfällig für bestimmte Angriffe sein, auch wenn die abgeleiteten Anmeldeinformationen durch Windows Defender Credential Guard geschützt werden. Zu diesen Angriffen zählen der Missbrauch von Berechtigungen und die Verwendung von abgeleiteten Anmeldeinformationen direkt von einem manipulierten Gerät, die erneute Verwendung von vor dem Einsatz von Windows Defender Device Guard gestohlenen Anmeldeinformationen sowie der Missbrauch von Verwaltungstools und unsichere Anwendungskonfigurationen. Aus diesem Grund müssen weitere Risikominderungen bereitgestellt werden, um die Domänenumgebung stabiler zu machen.

Beschränken des Domänenbenutzerzugriffs auf bestimmte in die Domäne eingebundene Geräte

Angriffe mit dem Ziel des Diebstahls von Anmeldeinformationen ermöglichen es dem Angreifer, geheime Schlüssel von einem Gerät zu stehlen und auf einem anderen Gerät zu verwenden. Wenn sich ein Benutzer auf mehreren Geräten anmelden kann, können von jedem dieser Geräte Anmeldeinformationen gestohlen werden. Wie wird sichergestellt, dass sich Benutzer nur mit Geräten anmelden, auf denen Windows Defender Credential Guard aktiviert ist? Durch die Bereitstellung von Authentifizierungsrichtlinien, die die Anmeldung auf ein bestimmtes, in die Domäne eingebundenes Gerät beschränken. Die Richtlinien werden in Windows Defender Credential Guard konfiguriert. Damit der Domänencontroller weiß, von welchem Gerät sich ein Benutzer anmeldet, muss der Kerberos-Schutz verwendet werden.

Kerberos-Schutz

Der Kerberos-Schutz ist Teil des Standards RFC 6113. Wenn der Kerberos-Schutz von einem Gerät unterstützt wird, wird der Besitzernachweis des Benutzers mittels TGT geschützt, um Angriffe auf das Offlinewörterbuch abzuwehren. Der Kerberos-Schutz bietet als weiteren Vorteil signierte KDC-Fehler. Dadurch können Manipulationen abgewehrt werden, die möglicherweise zu Downgradeangriffen führen.

So aktivieren Sie den Kerberos-Schutz, um den Domänenbenutzerzugriff auf bestimmte, in die Domäne eingebundene Geräte zu beschränken

- Benutzer müssen Domänen angehören, in denen Windows Server 2012 R2 oder höher ausgeführt wird.
- Alle Domänencontroller in diesen Domänen müssen für die Unterstützung des Kerberos-Schutzes konfiguriert werden. Legen Sie die Gruppenrichtlinieneinstellung **Unterstützung des Kerberos-Domänencontrollers für Ansprüche, Verbundauthentifizierung und Kerberos-Schutz** auf **Unterstützt** oder **Immer Ansprüche liefern** fest.
- Alle Geräte mit Windows Defender Credential Guard, für die der Benutzerzugriff beschränkt wird, müssen für die Unterstützung des Kerberos-Schutzes konfiguriert werden. Aktivieren Sie die Gruppenrichtlinieneinstellungen **Unterstützung des Kerberos-Clients für Ansprüche, Verbundauthentifizierung und Kerberos-Schutz** unter **Computerkonfiguration -> Administrative Vorlagen -> System -> Kerberos**.

Schützen geheimer Schlüssel von Geräten, die in die Domäne eingebunden sind

Da in die Domäne eingebundene Geräte zudem gemeinsame geheime Schlüssel für die Authentifizierung verwenden, können Angreifer diese geheimen Schlüssel auch stehlen. Durch die Bereitstellung von Gerätezertifikaten mit Windows Defender Credential Guard kann der private Schlüssel geschützt werden. Die

Authentifizierungsrichtlinien können voraussetzen, dass sich Benutzer bei Geräten anmelden, bei denen die Authentifizierung über diese Zertifikate erfolgt. Dies verhindert, dass gemeinsame vom Gerät gestohlene, geheime Schlüssel mit gestohlenen Benutzeranmeldeinformationen verwendet werden, um eine Benutzeranmeldung vorzunehmen.

Für die Zertifikatauthentifizierung eines in die Domäne eingebundenen Geräts ist Folgendes erforderlich:

- Die Gerätekonten müssen mindestens Windows Server2012 als Domänenfunktionsebene aufweisen.
- Alle Domänencontroller dieser Domänen müssen über KDC-Zertifikate verfügen, die strenge Zertifikatanforderungen bei der KDC-Überprüfung erfüllen:
 - Die erweiterte Schlüsselverwendung für das KDC muss vorhanden sein.
 - Der DNS-Domänenname muss dem DNSName-Feld der Erweiterung SubjectAltName (SAN) entsprechen.
- Windows10-Geräte verfügen über die Zertifizierungsstelle, auf der die Domänencontrollerzertifikate im Enterprise Store ausgestellt werden.
- Ein Prozess wird eingerichtet, um die Identität und die Vertrauenswürdigkeit des Geräts auf ähnliche Weise sicherzustellen, wie Sie die Identität und Vertrauenswürdigkeit eines Benutzers feststellen würden, bevor Sie ihm eine Smartcard zuweisen.

Bereitstellen von Zertifikaten für Geräte, die in die Domäne eingebunden sind

Um sicherzustellen, dass nur Zertifikate mit der erforderlichen Ausstellungsrichtlinie auf den für die Benutzer vorgesehenen Geräten installiert werden, müssen die Zertifikate auf jedem Gerät manuell bereitgestellt werden. Die Sicherheitsverfahren, die für das Ausstellen von Smartcards für Benutzer gelten, sollten auch auf Gerätezertifikate angewendet werden.

Nehmen wir beispielsweise an, Sie möchten die Richtlinie "Hohe Zusicherung" nur auf diesen Geräten verwenden. Sie würden dann mithilfe einer Windows Server Enterprise-Zertifizierungsstelle eine neue Vorlage erstellen.

Erstellen einer neuen Zertifikatvorlage

1. Klicken Sie in der Zertifikatverwaltungs-Konsole mit der rechten Maustaste auf **Zertifikatvorlagen**, und klicken Sie dann auf **Verwalten**.
2. Klicken Sie mit der rechten Maustaste auf **Arbeitsstationsauthentifizierung**, und klicken Sie dann auf **Vorlage duplizieren**.
3. Klicken Sie mit der rechten Maustaste auf die neue Vorlage, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Erweiterungen** auf **Anwendungsrichtlinien** und dann auf **Bearbeiten**.
5. Klicken Sie auf **Clientauthentifizierung** und dann auf **Entfernen**.
6. Fügen Sie die ID-PKInit-KPClientAuth ECU hinzu. Klicken Sie auf **Hinzufügen**, klicken Sie auf **Neu**, und geben Sie dann die folgenden Werte an:
 - Name: Kerberos Client Auth
 - Objekt-ID: 1.3.6.1.5.2.3.4
7. Klicken Sie auf der Registerkarte **Erweiterungen** auf **Ausstellungsrichtlinien** und dann auf **Bearbeiten**.
8. Klicken Sie unter **Ausstellungsrichtlinien** auf **Hohe Zusicherung**.
9. Deaktivieren Sie auf der Registerkarte **Antragstellernamen** das Kontrollkästchen **DNS-Name**, und aktivieren Sie dann das Kontrollkästchen **Benutzerprinzipalname (UPN)**.

Registrieren Sie dann auf Geräten, auf denen Windows Defender Credential Guard ausgeführt wird, die Geräte mithilfe des soeben erstellten Zertifikats.

Registrieren von Geräten in einem Zertifikat

Führen Sie den folgenden Befehl aus:

NOTE

Sie müssen das Gerät nach der Registrierung des Computerauthentifizierungszertifikats neu starten.

Verwenden einer Zertifikatausstellungsrichtlinie für die Zugriffssteuerung

Ab der Domänenfunktionsebene Windows Server2008 R2 bietet die Domänencontrollerunterstützung zur Authentifizierungsmechanismussicherung eine Möglichkeit, um OIDs der Zertifikatausstellungsrichtlinie und universelle Sicherheitsgruppen einander zuzuordnen. Windows Server2012-Domänencontroller, die Ansprüche unterstützen, ermöglichen die Zuordnung zu Ansprüchen. Informationen zur Authentifizierungsmechanismussicherung finden Sie unter [Schrittweise Anleitung zur Authentifizierungsmechanismussicherung für AD DS unter Windows Server2008R2](#) auf TechNet.

So zeigen Sie die verfügbaren Ausstellungsrichtlinien an

- Das Skript [get-IssuancePolicy.ps1](#) zeigt alle Ausstellungsrichtlinien, die für die Zertifizierungsstelle verfügbar sind. Führen Sie an der Windows PowerShell-Eingabeaufforderung den folgenden Befehl aus:

```
.\get-IssuancePolicy.ps1 -LinkedToGroup:All
```

So verknüpfen Sie eine Ausstellungsrichtlinie mit einer universellen Sicherheitsgruppe

- Das Skript [set-IssuancePolicyToGroupLink.ps1](#) erstellt eine universelle Sicherheitsgruppe sowie eine Organisationseinheit und verknüpft die Ausstellungsrichtlinie mit dieser universellen Sicherheitsgruppe. Führen Sie an der Windows PowerShell-Eingabeaufforderung den folgenden Befehl aus:

```
.\set-IssuancePolicyToGroupLink.ps1 -IssuancePolicyName:"<name of issuance policy>" -groupOU:"<Name of OU to create>" -groupName:"<name of Universal security group to create>"
```

Beschränken der Benutzeranmeldung

Bisher haben wir folgende Schritte ausgeführt:

- Es wurde eine spezielle Zertifikatausstellungsrichtlinie zur Identifizierung der Geräte erstellt, die die Bereitstellungskriterien erfüllen, die für die Benutzeranmeldung erforderlich sind.
- Die Richtlinie wurde einer universellen Sicherheitsgruppe oder einem Anspruch zugeordnet.
- Es wurde eine Methode bereitgestellt, wie Domänencontroller während der Benutzeranmeldung mit Kerberos-Schutz Geräteautorisierungsdaten abrufen. Als letzter Schritt muss jetzt nur noch die Zugriffsprüfung für Domänencontroller konfiguriert werden. Dies erfolgt mithilfe von Authentifizierungsrichtlinien.

Für Authentifizierungsrichtlinien gelten folgende Anforderungen:

- Die Benutzerkonten müssen mindestens die Domänenfunktionsebene Windows Server2012 aufweisen.

Erstellen einer Authentifizierungsrichtlinie, die Benutzer auf die spezifische universelle Sicherheitsgruppe beschränkt

1. Öffnen Sie das Active Directory-Verwaltungscenter.
2. Klicken Sie erst auf **Authentifizierung**, dann auf **Neu** und zuletzt auf **Authentifizierungsrichtlinie**.
3. Geben Sie im Feld **Anzeigename** einen Namen für diese Authentifizierungsrichtlinie ein.
4. Klicken Sie unter der Überschrift **Konten** auf **Hinzufügen**.
5. Geben Sie im Dialogfeld **Benutzer-, Computer- oder Dienstkonten auswählen** den Namen des

- Benutzerkontos ein, für das der Zugriff eingeschränkt werden soll, und klicken Sie dann auf **OK**.
6. Klicken Sie unter der Überschrift **Benutzeranmeldung** auf die Schaltfläche **Bearbeiten**.
 7. Klicken Sie auf **Bedingung hinzufügen**.
 8. Überprüfen Sie, ob im Feld **Zugriffssteuerungsbedingungen bearbeiten** die Elemente **Benutzer > Gruppe > Mitglied von allen Elementen > Wert** enthalten sind, und klicken Sie dann auf **Elemente hinzufügen**.
 9. Geben Sie im Dialogfeld **Benutzer-, Computer- oder Dienstkonten auswählen** den Namen der universellen Sicherheitsgruppe ein, die Sie mit dem Skript set-IssuancePolicyToGroupLink erstellt haben, und klicken Sie dann auf **OK**.
 10. Klicken Sie auf **OK**, um das Feld **Zugriffssteuerungsbedingungen bearbeiten** zu schließen.
 11. Klicken Sie auf **OK**, um die Authentifizierungsrichtlinie zu erstellen.
 12. Schließen Sie das Active Directory-Verwaltungscenter.

NOTE

Wenn Richtlinieneinschränkungen von der Authentifizierungsrichtlinie erzwungen werden, sind die Benutzer nicht in der Lage, sich über Geräte anzumelden, für die kein Zertifikat mit der entsprechenden Ausstellungsrichtlinie bereitgestellt wurde. Dies gilt für: die lokale und die Remoteanmeldung. Daher wird dringend empfohlen, zunächst nur Richtlinieneinschränkungen zu überprüfen, damit keine unerwarteten Fehler auftreten.

Ermitteln von Authentifizierungsfehlern aufgrund von Authentifizierungsrichtlinien

Wenn Sie die Nachverfolgung von Authentifizierungsfehlern aufgrund von Authentifizierungsrichtlinien vereinfachen möchten, können Sie ein Betriebsprotokoll verwenden, das nur diese Ereignisse enthält. Um die Protokolle auf den Domänencontrollern zu aktivieren, navigieren Sie in der Ereignisanzeige zu **Anwendungs- und Dienstprotokolle\Microsoft\Windows\Authentifizierung**, klicken Sie mit der rechten Maustaste auf „AuthenticationPolicyFailures-DomainController“, und klicken Sie dann auf **Protokoll aktivieren**.

Weitere Informationen zu Ereignissen von Authentifizierungsrichtlinien finden Sie unter [Authentifizierungsrichtlinien](#) und [Authentifizierungsrichtliniensilos](#).

Anhang: Skripts

Im Folgenden finden Sie eine Liste von Skripten, die in diesem Thema beschrieben werden.

Abrufen der verfügbaren Ausstellungsrichtlinien für die Zertifizierungsstelle

Speichern Sie diese Skriptdatei unter dem Namen get-IssuancePolicy.ps1.

```
#####
##      Parameters to be defined      ##
##      by the user                    ##
#####
Param (
$Identity,
$LinkedToGroup
)
#####
##      Strings definitions            ##
#####
Data getIP_strings {
# culture="en-US"
ConvertFrom-StringData -stringdata @"
help1 = This command can be used to retrieve all available Issuance Policies in a forest. The forest of the
currently logged on user is targeted.
help2 = Usage:
help3 = The following parameter is mandatory:
help4 = -LinkedToGroup:<yes|no|all>
help5 = "yes" will return only Issuance Policies that are linked to groups. Checks that the linked Issuance
Policies are linked to valid groups.
```

```

help6 = "no" will return only Issuance Policies that are not currently linked to any group.
help7 = "all" will return all Issuance Policies defined in the forest. Checks that the linked Issuance policies
are linked to valid groups.
help8 = The following parameter is optional:
help9 = -Identity:<Name, Distinguished Name or Display Name of the Issuance Policy that you want to retrieve>.
If you specify an identity, the option specified in the "-LinkedToGroup" parameter is ignored.
help10 = Output: This script returns the Issuance Policy objects meeting the criteria defined by the above
parameters.
help11 = Examples:
errorIPNotFound = Error: no Issuance Policy could be found with Identity "{0}"
ErrorNotSecurity = Error: Issuance Policy "{0}" is linked to group "{1}" which is not of type "Security".
ErrorNotUniversal = Error: Issuance Policy "{0}" is linked to group "{1}" whose scope is not "Universal".
ErrorHasMembers = Error: Issuance Policy "{0}" is linked to group "{1}" which has a non-empty membership. The
group has the following members:
LinkedIPs = The following Issuance Policies are linked to groups:
displayName = displayName : {0}
Name = Name : {0}
dn = distinguishedName : {0}
    InfoName = Linked Group Name: {0}
    InfoDN = Linked Group DN: {0}
NonLinkedIPs = The following Issuance Policies are NOT linked to groups:
'@
}
##Import-LocalizedData getIP_strings
import-module ActiveDirectory
#####
##          Help          ##
#####
function Display-Help {
    ""
    $getIP_strings.help1
    ""
$getIP_strings.help2
""
$getIP_strings.help3
"    " + $getIP_strings.help4
"    " + $getIP_strings.help5
"    " + $getIP_strings.help6
"    " + $getIP_strings.help7
""
$getIP_strings.help8
"    " + $getIP_strings.help9
""
    $getIP_strings.help10
""
""
$getIP_strings.help11
"    " + '$' + "myIPs = .\get-IssuancePolicy.ps1 -LinkedToGroup:All"
"    " + '$' + "myLinkedIPs = .\get-IssuancePolicy.ps1 -LinkedToGroup:yes"
"    " + '$' + "myIP = .\get-IssuancePolicy.ps1 -Identity:""Medium Assurance""
""
}
$root = get-adrootdse
$domain = get-addomain -current loggedonuser
$configNCDN = [String]$root.configurationNamingContext
if ( !($Identity) -and !($LinkedToGroup) ) {
display-Help
break
}
if ($Identity) {
    $OIDs = get-adobject -Filter {(objectclass -eq "msPKI-Enterprise-Oid") -and ((name -eq $Identity) -or
(displayname -eq $Identity) -or (distinguishedName -like $Identity)) } -searchBase $configNCDN -properties *
    if ($OIDs -eq $null) {
$errormsg = $getIP_strings.ErrorIPNotFound -f $Identity
write-host $errmsg -ForegroundColor Red
    }
    foreach ($OID in $OIDs) {
        if ($OID."msDS-OIDToGroupLink") {
# In case the Issuance Policy is linked to a group, it is good to check whether there is any problem with the

```

```
mapping.
    $groupDN = $OID."msDS-OIDToGroupLink"
    $group = get-adgroup -Identity $groupDN
    $groupName = $group.Name
# Analyze the group
    if ($group.groupCategory -ne "Security") {
$errorrmgs = $getIP_strings.ErrorNotSecurity -f $Identity, $groupName
        write-host $errorrmgs -ForegroundColor Red
    }
    if ($group.groupScope -ne "Universal") {
        $errorrmgs = $getIP_strings.ErrorNotUniversal -f $Identity, $groupName
write-host $errorrmgs -ForegroundColor Red
    }
    $members = Get-ADGroupMember -Identity $group
    if ($members) {
        $errorrmgs = $getIP_strings.ErrorHasMembers -f $Identity, $groupName
write-host $errorrmgs -ForegroundColor Red
        foreach ($member in $members) {
            write-host "                " $member -ForeGroundColor Red
        }
    }
}
return $OIDs
break
}
if (($LinkedToGroup -eq "yes") -or ($LinkedToGroup -eq "all")) {
    $LDAPFilter = "&(objectClass=msPKI-Enterprise-Oid)(msDS-OIDToGroupLink=*)(flags=2))"
    $LinkedOIDs = get-adobject -searchBase $configNCDN -LDAPFilter $LDAPFilter -properties *
    write-host ""
    write-host "*****"
    write-host $getIP_strings.LinkedIPs
    write-host "*****"
    write-host ""
    if ($LinkedOIDs -ne $null){
        foreach ($OID in $LinkedOIDs) {
# Display basic information about the Issuance Policies
            ""

            $getIP_strings.displayName -f $OID.displayName
            $getIP_strings.Name -f $OID.Name
            $getIP_strings.dn -f $OID.distinguishedName
# Get the linked group.
            $groupDN = $OID."msDS-OIDToGroupLink"
            $group = get-adgroup -Identity $groupDN
            $getIP_strings.InfoName -f $group.Name
            $getIP_strings.InfoDN -f $groupDN
# Analyze the group
            $OIDName = $OID.displayName
            $groupName = $group.Name
            if ($group.groupCategory -ne "Security") {
                $errorrmgs = $getIP_strings.ErrorNotSecurity -f $OIDName, $groupName
                write-host $errorrmgs -ForegroundColor Red
            }
            if ($group.groupScope -ne "Universal") {
                $errorrmgs = $getIP_strings.ErrorNotUniversal -f $OIDName, $groupName
                write-host $errorrmgs -ForegroundColor Red
            }
            $members = Get-ADGroupMember -Identity $group
            if ($members) {
                $errorrmgs = $getIP_strings.ErrorHasMembers -f $OIDName, $groupName
                write-host $errorrmgs -ForegroundColor Red
                foreach ($member in $members) {
                    write-host "                " $member -ForeGroundColor Red
                }
            }
            write-host ""
        }
    }else{
write-host "There are no issuance policies that are mapped to a group"
```

```

    }
    if ($LinkedToGroup -eq "yes") {
        return $LinkedOIDs
        break
    }
}
if (($LinkedToGroup -eq "no") -or ($LinkedToGroup -eq "all")) {
    $LDAPFilter = "(&(objectClass=msPKI-Enterprise-Oid)(!(msDS-OIDToGroupLink=*)))(flags=2)"
    $NonLinkedOIDs = get-adobject -searchBase $configNCDN -LDAPFilter $LDAPFilter -properties *
    write-host ""
    write-host "*****"
    write-host $getIP_strings.NonLinkedIPs
    write-host "*****"
    write-host ""
    if ($NonLinkedOIDs -ne $null) {
        foreach ($OID in $NonLinkedOIDs) {
            # Display basic information about the Issuance Policies
            write-host ""
            $getIP_strings.displayName -f $OID.displayName
            $getIP_strings.Name -f $OID.Name
            $getIP_strings.dn -f $OID.distinguishedName
            write-host ""
        }
    }else{
        write-host "There are no issuance policies which are not mapped to groups"
    }
    if ($LinkedToGroup -eq "no") {
        return $NonLinkedOIDs
        break
    }
}
}

```

NOTE

Wenn bei der Ausführung dieses Skripts Probleme auftreten, sollten Sie das einfache Anführungszeichen nach dem Parameter ConvertFrom-StringData ersetzen.

Verknüpfen einer Ausstellungsrichtlinie mit einer Gruppe

Speichern Sie die Skriptdatei unter dem Namen set-IssuancePolicyToGroupLink.ps1.

```

#####
##      Parameters to be defined      ##
##      by the user                   ##
#####
Param (
    $IssuancePolicyName,
    $groupOU,
    $groupName
)
#####
##      Strings definitions           ##
#####
Data ErrorMsg {
    # culture="en-US"
    ConvertFrom-StringData -stringdata @"
help1 = This command can be used to set the link between a certificate issuance policy and a universal security
group.
help2 = Usage:
help3 = The following parameters are required:
help4 = -IssuancePolicyName:<name or display name of the issuance policy that you want to link to a group>
help5 = -groupName:<name of the group you want to link the issuance policy to>. If no name is specified, any
existing link to a group is removed from the Issuance Policy.
help6 = The following parameter is optional:
help7 = -groupOU:<Name of the Organizational Unit dedicated to the groups which are linked to issuance

```

policies>. If this parameter is not specified, the group is looked for or created in the Users container.

help8 = Examples:

help9 = This command will link the issuance policy whose display name is "High Assurance" to the group "HighAssuranceGroup" in the Organizational Unit "OU_FOR_IPol_linked_groups". If the group or the Organizational Unit do not exist, you will be prompted to create them.

help10 = This command will unlink the issuance policy whose name is "402.164959C40F4A5C12C6302E31D5476062" from any group.

MultipleIPs = Error: Multiple Issuance Policies with name or display name "{0}" were found in the subtree of "{1}"

NoIP = Error: no issuance policy with name or display name "{0}" could be found in the subtree of "{1}".

IPFound = An Issuance Policy with name or display name "{0}" was successfully found: {1}

MultipleOUs = Error: more than 1 Organizational Unit with name "{0}" could be found in the subtree of "{1}".

confirmOUcreation = Warning: The Organizational Unit that you specified does not exist. Do you want to create it?

OUCreationSuccess = Organizational Unit "{0}" successfully created.

OUcreationError = Error: Organizational Unit "{0}" could not be created.

OUFoundSuccess = Organizational Unit "{0}" was successfully found.

multipleGroups = Error: More than one group with name "{0}" was found in Organizational Unit "{1}".

confirmGroupCreation = Warning: The group that you specified does not exist. Do you want to create it?

groupCreationSuccess = Universal Security group "{0}" successfully created.

groupCreationError = Error: Universal Security group "{0}" could not be created.

GroupFound = Group "{0}" was successfully found.

confirmLinkDeletion = Warning: The Issuance Policy "{0}" is currently linked to group "{1}". Do you really want to remove the link?

UnlinkSuccess = Certificate issuance policy successfully unlinked from any group.

UnlinkError = Removing the link failed.

UnlinkExit = Exiting without removing the link from the issuance policy to the group.

IPNotLinked = The Certificate issuance policy is not currently linked to any group. If you want to link it to a group, you should specify the -groupName option when starting this script.

ErrorNotSecurity = Error: You cannot link issuance Policy "{0}" to group "{1}" because this group is not of type "Security".

ErrorNotUniversal = Error: You cannot link issuance Policy "{0}" to group "{1}" because the scope of this group is not "Universal".

ErrorHasMembers = Error: You cannot link issuance Policy "{0}" to group "{1}" because it has a non-empty membership. The group has the following members:

ConfirmLinkReplacement = Warning: The Issuance Policy "{0}" is currently linked to group "{1}". Do you really want to update the link to point to group "{2}"?

LinkSuccess = The certificate issuance policy was successfully linked to the specified group.

LinkError = The certificate issuance policy could not be linked to the specified group.

ExitNoLinkReplacement = Exiting without setting the new link.

'@

}

import-localizeddata ErrorMsg

function Display-Help {

""

write-host \$ErrorMsg.help1

""

write-host \$ErrorMsg.help2

""

write-host \$ErrorMsg.help3

write-host "`t" \$ErrorMsg.help4

write-host "`t" \$ErrorMsg.help5

""

write-host \$ErrorMsg.help6

write-host "`t" \$ErrorMsg.help7

""

""

write-host \$ErrorMsg.help8

""

write-host \$ErrorMsg.help9

".\Set-IssuancePolicyToGroupMapping.ps1 -IssuancePolicyName ""High Assurance"" -groupOU

""OU_FOR_IPol_linked_groups"" -groupName ""HighAssuranceGroup"" "

""

write-host \$ErrorMsg.help10

'.\Set-IssuancePolicyToGroupMapping.ps1 -IssuancePolicyName "402.164959C40F4A5C12C6302E31D5476062" -groupName

\$null '

""

}

Assumption: The group to which the Issuance Policy is going

```

#         to be linked is (or is going to be created) in
#         the domain the user running this script is a member of.
import-module ActiveDirectory
$root = get-adrootdse
$domain = get-addomain -current loggedonuser
if ( !($IssuancePolicyName) ) {
display-Help
break
}
#####
##      Find the OID object          ##
##      (aka Issuance Policy)        ##
#####
$searchBase = [String]$root.configurationnamingcontext
$OID = get-adobject -searchBase $searchBase -Filter { ((displayName -eq $IssuancePolicyName) -or (name -eq
$IssuancePolicyName)) -and (objectClass -eq "msPKI-Enterprise-Oid")} -properties *
if ($OID -eq $null) {
$tmp = $ErrorMsg.NoIP -f $IssuancePolicyName, $searchBase
write-host $tmp -ForegroundColor Red
break;
}
elseif ($OID.GetType().IsArray) {
$tmp = $ErrorMsg.MultipleIPs -f $IssuancePolicyName, $searchBase
write-host $tmp -ForegroundColor Red
break;
}
else {
$tmp = $ErrorMsg.IPFound -f $IssuancePolicyName, $OID.distinguishedName
write-host $tmp -ForegroundColor Green
}
#####
##      Find the container of the group ##
#####
if ($groupOU -eq $null) {
# default to the Users container
$groupContainer = $domain.UsersContainer
}
else {
$searchBase = [string]$domain.DistinguishedName
$groupContainer = get-adobject -searchBase $searchBase -Filter { (Name -eq $groupOU) -and (objectClass -eq
"organizationalUnit")}
if ($groupContainer.count -gt 1) {
$tmp = $ErrorMsg.MultipleOUs -f $groupOU, $searchBase
write-host $tmp -ForegroundColor Red
break;
}
elseif ($groupContainer -eq $null) {
$tmp = $ErrorMsg.confirmOUCreation
write-host $tmp " ( (y)es / (n)o )" -ForegroundColor Yellow -nonewline
$userChoice = read-host
if ( ($userChoice -eq "y") -or ($userChoice -eq "yes") ) {
new-adobject -Name $groupOU -displayName $groupOU -Type "organizationalUnit" -ProtectedFromAccidentalDeletion
$true -path $domain.distinguishedName
if ($?){
$tmp = $ErrorMsg.OUCreationSuccess -f $groupOU
write-host $tmp -ForegroundColor Green
}
}
else{
$tmp = $ErrorMsg.OUCreationError -f $groupOU
write-host $tmp -ForegroundColor Red
break;
}
}
$groupContainer = get-adobject -searchBase $searchBase -Filter { (Name -eq $groupOU) -and (objectClass -eq
"organizationalUnit")}
}
else {
break;
}
}
}

```

```

else {
$tmp = $ErrorMsg.OUFoundSuccess -f $groupContainer.name
write-host $tmp -ForegroundColor Green
}
}
#####
## Find the group ##
#####
if (($groupName -ne $null) -and ($groupName -ne "")){
##$searchBase = [String]$groupContainer.DistinguishedName
$searchBase = $groupContainer
$group = get-adgroup -Filter { (Name -eq $groupName) -and (objectClass -eq "group") } -searchBase $searchBase
if ($group -ne $null -and $group.gettype().isArray) {
$tmp = $ErrorMsg.multipleGroups -f $groupName, $searchBase
write-host $tmp -ForegroundColor Red
break;
}
elseif ($group -eq $null) {
$tmp = $ErrorMsg.confirmGroupCreation
write-host $tmp " ( (y)es / (n)o )" -ForegroundColor Yellow -nonewline
$userChoice = read-host
if ( ($userChoice -eq "y") -or ($userChoice -eq "yes") ) {
new-adgroup -samAccountName $groupName -path $groupContainer.distinguishedName -GroupScope "Universal" -
GroupCategory "Security"
if ($?){
$tmp = $ErrorMsg.GroupCreationSuccess -f $groupName
write-host $tmp -ForegroundColor Green
}else{
$tmp = $ErrorMsg.groupCreationError -f $groupName
write-host $tmp -ForegroundColor Red
break
}
}
$group = get-adgroup -Filter { (Name -eq $groupName) -and (objectClass -eq "group") } -searchBase $searchBase
}
else {
break;
}
}
else {
$tmp = $ErrorMsg.GroupFound -f $group.Name
write-host $tmp -ForegroundColor Green
}
}
else {
#####
## If the group is not specified, we should remove the link if any exists
#####
if ($OID."msDS-OIDToGroupLink" -ne $null) {
$tmp = $ErrorMsg.confirmLinkDeletion -f $IssuancePolicyName, $OID."msDS-OIDToGroupLink"
write-host $tmp " ( (y)es / (n)o )" -ForegroundColor Yellow -nonewline
$userChoice = read-host
if ( ($userChoice -eq "y") -or ($userChoice -eq "yes") ) {
set-adobject -Identity $OID -Clear "msDS-OIDToGroupLink"
if ($?) {
$tmp = $ErrorMsg.UnlinkSuccess
write-host $tmp -ForegroundColor Green
}else{
$tmp = $ErrorMsg.UnlinkError
write-host $tmp -ForegroundColor Red
}
}
}
else {
$tmp = $ErrorMsg.UnlinkExit
write-host $tmp
break
}
}
else {
$tmp = $ErrorMsg.IPNotLinked

```



```

write-host $tmp -ForegroundColor Yellow
}
break;
}
#####
## Verify that the group is ##
## Universal, Security, and ##
## has no members ##
#####
if ($group.GroupScope -ne "Universal") {
$tmp = $ErrorMsg.ErrorNotUniversal -f $IssuancePolicyName, $groupName
write-host $tmp -ForegroundColor Red
break;
}
if ($group.GroupCategory -ne "Security") {
$tmp = $ErrorMsg.ErrorNotSecurity -f $IssuancePolicyName, $groupName
write-host $tmp -ForegroundColor Red
break;
}
$members = Get-ADGroupMember -Identity $group
if ($members -ne $null) {
$tmp = $ErrorMsg.ErrorHasMembers -f $IssuancePolicyName, $groupName
write-host $tmp -ForegroundColor Red
foreach ($member in $members) {write-host " $member.name" -ForegroundColor Red}
break;
}
#####
## We have verified everything. We ##
## can create the link from the ##
## Issuance Policy to the group. ##
#####
if ($OID."msDS-OIDToGroupLink" -ne $null) {
$tmp = $ErrorMsg.ConfirmLinkReplacement -f $IssuancePolicyName, $OID."msDS-OIDToGroupLink",
$group.distinguishedName
write-host $tmp "( (y)es / (n)o )" -ForegroundColor Yellow -nonewline
$userChoice = read-host
if ( ($userChoice -eq "y") -or ($userChoice -eq "yes") ) {
$tmp = @{'msDS-OIDToGroupLink' = $group.DistinguishedName}
set-adobject -Identity $OID -Replace $tmp
if ($?) {
$tmp = $ErrorMsg.LinkSuccess
write-host $tmp -ForegroundColor Green
}else{
$tmp = $ErrorMsg.LinkError
write-host $tmp -ForegroundColor Red
}
} else {
$tmp = $ErrorMsg.ExitNoLinkReplacement
write-host $tmp
break
}
}
else {
$tmp = @{'msDS-OIDToGroupLink' = $group.DistinguishedName}
set-adobject -Identity $OID -Add $tmp
if ($?) {
$tmp = $ErrorMsg.LinkSuccess
write-host $tmp -ForegroundColor Green
}else{
$tmp = $ErrorMsg.LinkError
write-host $tmp -ForegroundColor Red
}
}
}

```

NOTE

Wenn bei der Ausführung dieses Skripts Probleme auftreten, sollten Sie das einfache Anführungszeichen nach dem Parameter ConvertFrom-StringData ersetzen.

Windows Defender Credential Guard – bekannte Probleme

12.09.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows Server2016

Für Windows Defender Credential Guard gelten bestimmte Anwendungsanforderungen. Windows Defender Credential Guard blockiert bestimmte Authentifizierungsfunktionen. Anwendungen, die solche Funktionen verwenden, funktionieren daher nicht, wenn die Lösung aktiviert ist. Weitere Informationen finden Sie unter [Anwendungsanforderungen](#).

Das folgende bekannte Problem wurde im [kumulativen Sicherheitsupdate für November 2017](#) behoben:

- Geplante Aufgaben mit gespeicherten Anmeldeinformationen werden nicht ausgeführt, wenn Credential Guard aktiviert ist. Die Aufgabe schlägt fehl und meldet die Ereignis-ID 104 mit folgender Meldung:
"Task Scheduler konnte sich nicht auf "\Test" anmelden.
Fehler im 'LogonUserExEx'.
Benutzeraktion: Stellen Sie sicher, dass die Anmeldeinformationen für die Aufgabe richtig angegeben wurden.
Zusätzliche Daten: Fehlerwert: 2147943726. 2147943726: ERROR_LOGON_FAILURE. (Der Nutzernamen oder das Passwort sind falsch)."

Die folgenden bekannten Probleme wurden mit den Wartungsaktualisierungen in den kumulativen Sicherheitsupdates für April 2017 behoben:

- [KB4015217: Eine falsche Kennworteingabe zählt in Windows Defender Credential Guard auf in die Active Directory-Domäne eingebundenen Windows 10-Computern doppelt](#)

Dieses Problem kann zu unerwarteten Kontosperrungen führen. Siehe auch Microsoft® Knowledge Base-Artikel [KB4015219](#) und [KB4015221](#)

- [KB4033236 Zwei fehlerhafte Anmeldeversuche werden nach der Installation von Windows Defender Credential Guard unter Windows10 an Active Directory gesendet](#)

Dieses Problem kann zu unerwarteten Kontosperrungen führen. Das Problem wurde in Wartungsupdates für jedes der folgenden Betriebssysteme behoben:

- Windows 10 Version 1607 und Windows Server 2016: [KB4015217 \(BS-Build 14393.1066 und 14393.1083\)](#)
- Windows 10 Version 1511: [KB4015219 \(BS-Build 10586.873\)](#)
- Windows 10 Version 1507: [KB4015221 \(BS-Build 10240.17354\)](#)

Bekannte Probleme im Zusammenhang mit Drittanbieteranwendungen

Das folgende Problem betrifft die Java-GSS-API. Informationen finden Sie im folgenden Datenbankartikel von Oracle-Fehlern:

- [JDK-8161921: Windows10 Windows Defender Credential Guard lässt keine Freigabe von TGT mit Java zu](#)

Wenn Windows Defender Credential Guard in Windows10 aktiviert ist, wird Java-GSS-API nicht authentifiziert.

Dieses Verhalten ist erwartet, da Windows Defender Credential Guard bestimmte Authentifizierungsfunktionen blockiert und unabhängig von den Registrierungsschlüsseleinstellungen keinen TGT-Sitzungsschlüssel für Anwendungen bereitstellt. Weitere Informationen finden Sie unter [Anwendungsanforderungen](#).

Das folgende Problem betrifft Cisco AnyConnect Secure Mobility Client:

- [Bluescreen auf Windows10-Computern mit Windows Defender Device Guard und Windows Defender Credential Guard mit Cisco Anyconnect 4.3.04027 *](#)

*Dieser Artikel ist nur für registrierte Benutzer verfügbar.

Das folgende Problem betrifft McAfee Application and Change Control (MACC):

- [KB88869 Hohe Prozessorauslastung auf Windows 10-Computern mit McAfee Application and Change Control \(MACC\)-Installation bei Aktivierung von Windows Defender Credential Guard ^{\[1\]}](#)

Das folgende Problem betrifft AppSense Environment Manager. Weitere Informationen finden Sie im folgenden KnowledgeBase-Artikel:

- [Die Installation von AppSense Environment Manager auf Windows 10-Computern führt dazu, dass LSAISO.exe eine hohe Prozessorauslastung aufweist, wenn Windows Defender Credential Guard aktiviert ist ^{\[1\]}](#)
**

Das folgende Problem betrifft Citrix-Anwendungen:

- Hohe Prozessorauslastung auf Windows10-Computern mit installierten Citrix-Anwendungen, wenn Windows Defender Credential Guard aktiviert ist. ^[1]

^[1] Produkte, sich mit Prozessen verbinden, die mit der virtualisierungsbasierten Sicherheit (VBS) geschützt werden, können dazu führen, dass auf Windows10- oder Windows Server 2016-Computern mit aktiviertem Windows Defender Credential Guard eine hohe Prozessorauslastung auftritt. Weitere technische Informationen und Informationen zur Problembehandlung finden Sie im folgenden Microsoft KnowledgeBase-Artikel:

- [KB4032786 Hohe Prozessorauslastung im LSAISO-Prozess in Windows10 oder Windows Server2016](#)

Weitere technische Informationen zu LSAISO.exe finden Sie im MSDN-Artikel [Isolierte Benutzermodusprozesse](#)

** Dieser Artikel ist nur für registrierte Benutzer verfügbar.

Anbieterunterstützung

Informationen zur Citrix-Unterstützung für den sicheren Start finden Sie in folgendem Artikel:

- [Citrix-Unterstützung für den sicheren Start](#)

Windows Defender Credential Guard wird von den folgenden Produkten, Produktversionen, Computersystemen oder Windows10-Versionen nicht unterstützt:

- Hinweise zu Windows Defender Credential Guard auf Windows 10 mit McAfee-Verschlüsselungsprodukten finden Sie unter: [Unterstützung für Windows Defender Device Guard und Windows Defender Credential Guard unter Windows10 mit McAfee-Verschlüsselungsprodukten](#)
- Hinweise zu Windows Defender Credential Guard auf Windows 10 mit Check Point Endpoint Security-Client finden Sie unter: [Unterstützung im Check Point Endpoint Security-Client für Microsoft Windows 10 Windows Defender Credential Guard- und Windows Defender Device Guard-Funktionen](#)
- Hinweise zu Windows Defender Credential Guard auf Windows 10 mit VMWare Workstation finden Sie unter: [Fehler in Windows 10-Host bei der Ausführung von VMWare Workstation mit aktiviertem Windows Defender Credential Guard](#)

- Hinweise zu Windows Defender Credential Guard auf Windows 10 mit bestimmten Lenovo ThinkPad-Versionen finden Sie unter: [ThinkPad-Unterstützung für Windows Defender Device Guard und Windows Defender Credential Guard in Microsoft Windows 10 – ThinkPad](#)
- Hinweise zu Windows Defender Credential Guard auf Windows 10 mit Symantec Endpoint Protection finden Sie unter: [Windows 10 mit Windows Defender Credential Guard und Symantec Endpoint Protection 12.1](#)

Diese Liste ist nicht vollständig. Überprüfen Sie, ob Ihr Produhersteller, Ihre Produktversion oder Ihr Computersystem Windows Defender Credential Guard auf Systemen mit Windows10 oder bestimmten Versionen von Windows10 unterstützt. Bestimmte Modelle von Computersystemen sind möglicherweise nicht mit Windows Defender Credential Guard kompatibel.

Microsoft empfiehlt Drittanbietern, zu dieser Seite beitragen, indem sie relevante Produktinformationen und Links zu den Informationen zur Unterstützung ihrer eigenen Produkte hinzufügen.

Schützen von Remote Desktop Anmeldeinformationen mit Windows Defender Remote Credential Guard

12.09.2019 • 8 minutes to read

Betrifft

- Windows10
- Windows Server 2016

Eingeführt in Windows 10, Version 1607, hilft Ihnen Windows Defender Remote Credential Guard, Ihre Anmeldeinformationen über eine Remote Desktop Verbindung zu schützen, indem Kerberos-Anforderungen zurück an das Gerät umgeleitet werden, das die Verbindung anfordert. Darüber hinaus bietet es einmaliges Anmelden für Remote Desktop Sitzungen.

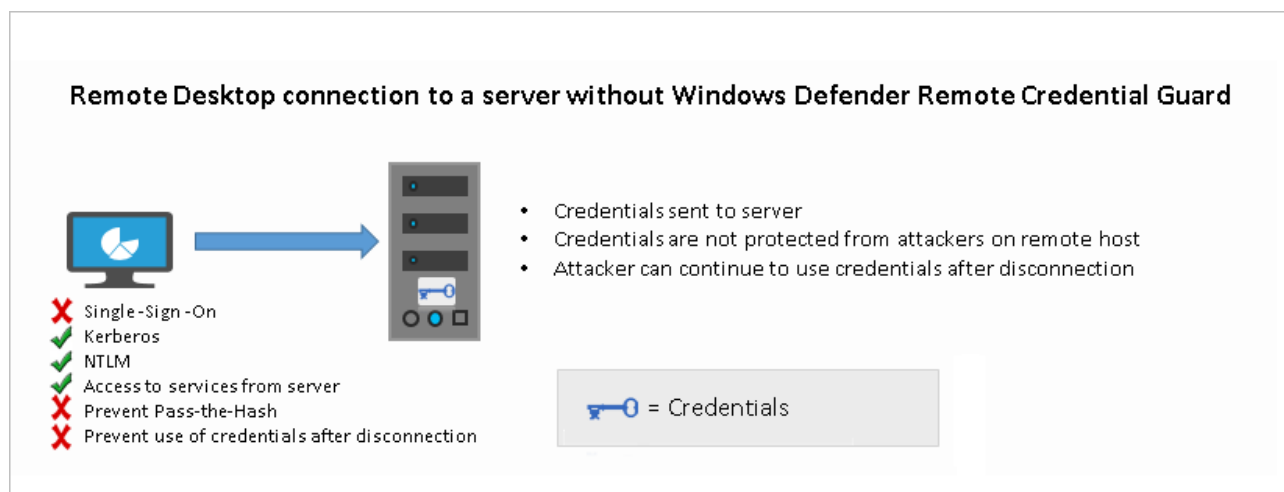
Die Administrator Anmeldeinformationen sind sehr privilegiert und müssen geschützt werden. Wenn Sie die Windows Defender-Remoteanmeldeinformationen für die Verbindung während einer Remote Desktop Sitzung verwenden und das Zielgerät kompromittiert wird, werden Ihre Anmeldeinformationen nicht verfügbar gemacht, da sowohl Anmeldeinformationen als auch Anmeldeinformationen nicht über das Netzwerk an das Ziel übergeben werden. Gerät.

IMPORTANT

Informationen zu Remote Desktop-Verbindungsszenarien mit Helpdesk-Unterstützung finden Sie in diesem Artikel unter [Szenarien für Remotedesktopverbindungen und Helpdesk-Support](#).

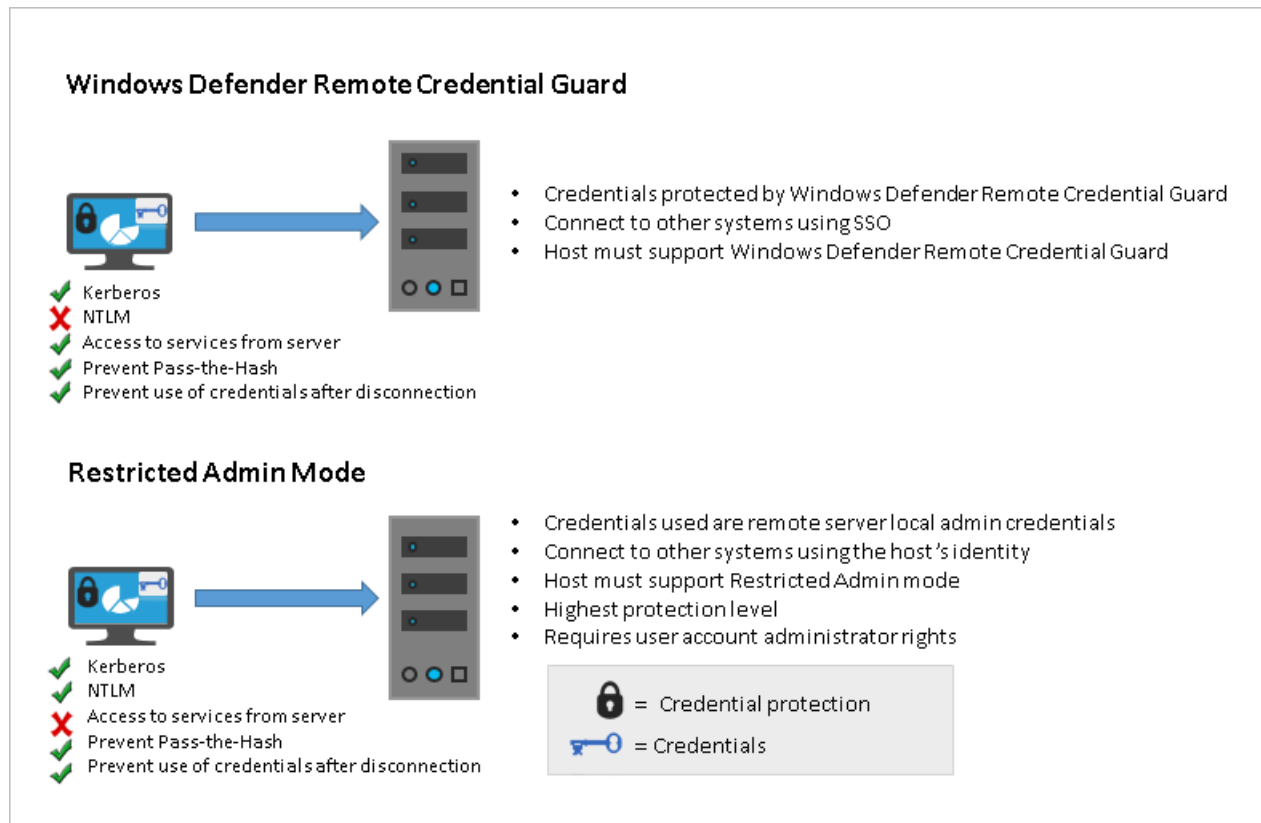
Vergleich von Windows Defender Remote Credential Guard mit anderen Remote Desktop-Verbindungsoptionen

Das folgende Diagramm hilft Ihnen zu verstehen, wie eine standardmäßige Remote Desktop Sitzung zu einem Server ohne Windows Defender Remote Credential Guard funktioniert:



Das folgende Diagramm hilft Ihnen, die Funktionsweise von Windows Defender Remote Credential Guard zu

verstehen und zu schützen, und vergleicht sie mit der Option [eingeschränkter Administratormodus](#) :



Wie in Abbildung dargestellt, blockiert Windows Defender Remote Credential Guard NTLM (nur Kerberos), verhindert Pass-the-Hash-Angriffe (Durchkontaktierungen) und verhindert auch die Verwendung von Anmeldeinformationen nach der Trennung.

Mit der folgenden Tabelle können Sie verschiedene Sicherheitsoptionen für Remote Desktop Verbindungen vergleichen:

FEATURE	REMOTEDESKTOP	WINDOWS DEFENDER-REMOTE ANMELDE INFORMATIONSSCHUTZ	EINGESCHRÄNKTER ADMINISTRATORMODUS
Schutz Vorteile	Die Anmeldeinformationen auf dem Server sind nicht vor Pass-the-Hash-Angriffen geschützt.	Benutzeranmeldeinformationen verbleiben auf dem Client. Ein Angreifer kann <i>nur</i> im Namen des Benutzers handeln, wenn die Sitzung fortgesetzt wird.	Der Benutzer meldet sich beim Server als lokaler Administrator an, sodass ein Angreifer nicht im Namen des "Domänenbenutzers" agieren kann. Jeder Angriff ist lokal auf dem Server.

FEATURE	REMOTEDESKTOP	WINDOWS DEFENDER-REMOTE ANMELDE INFORMATIONSSCHUTZ	EINGESCHRÄNKTER ADMINISTRATORMODUS
Versionsunterstützung	Auf dem Remotecomputer kann ein beliebiges Windows-Betriebssystem ausgeführt werden	Sowohl auf dem Client als auch auf dem Remotecomputer muss mindestens Windows 10, Version 1607 oder Windows Server 2016 ausgeführt werden.	Auf dem Remotecomputer muss mindestens ein gepatchter Windows 7- oder gepatchter Windows Server 2008 R2 ausgeführt werden. Weitere Informationen zu Patches (Softwareupdates) im Zusammenhang mit dem eingeschränkten Administratormodus finden Sie unter Microsoft Security Advisory 2871997 .
Hilft zu verhindern	N/A	<ul style="list-style-type: none"> • Pass-the-Hash • Verwendung von Anmeldeinformationen nach dem Verbindungsaufbau 	<ul style="list-style-type: none"> • Pass-the-Hash • Verwendung der Domänenidentität während der Verbindung
Vom Remote Desktop Clientgerät unterstützte Anmeldeinformationen	<ul style="list-style-type: none"> • Anmeldeinformationen angemeldet • Angegebene Anmeldeinformationen • Gespeicherte Anmeldeinformationen 	<ul style="list-style-type: none"> • Nur Anmeldeinformationen angemeldet 	<ul style="list-style-type: none"> • Anmeldeinformationen angemeldet • Angegebene Anmeldeinformationen • Gespeicherte Anmeldeinformationen
Access	Benutzer zulässig , also Mitglieder der Gruppe Remote Desktop Benutzer des Remotehosts.	Benutzer zulässig , also Mitglieder von Remote Desktop Benutzern des Remotehosts.	Nur Administratoren , das heißt, nur Mitglieder der Gruppe Administratoren des Remotehosts.
Netzwerkidentität	Die Remote Desktop Sitzung stellt eine Verbindung mit anderen Ressourcen als angemeldeter Benutzer her .	Die Remote Desktop Sitzung stellt eine Verbindung mit anderen Ressourcen als angemeldeter Benutzer her .	Die Remote Desktop Sitzung stellt eine Verbindung mit anderen Ressourcen als Identität des Remotehosts her .
Multi-Hop	Über den Remote Desktop können Sie eine Verbindung über den Remote Desktop mit einem anderen Computer herstellen .	Über den Remote Desktop können Sie eine Verbindung über den Remote Desktop mit einem anderen Computer herstellen .	Für Benutzer nicht zulässig, während die Sitzung als lokales Host Konto ausgeführt wird
Unterstützte Authentifizierung	Alle verhandelbaren Protokolle.	Nur Kerberos.	Alle verhandelbaren Protokolle

Weitere technische Informationen finden Sie unter [Remote Desktop Protokoll](#) und [Funktionsweise von Kerberos](#).

Szenarien für Remote Desktop Verbindungen und Helpdesk-Support

Für Helpdesk-Support Szenarien, in denen Personaladministrator Zugriff benötigt, um Computerbenutzern Remoteunterstützung über Remote Desktop Sitzungen bereitzustellen, empfiehlt Microsoft, dass Windows Defender Remote Credential Guard nicht in diesem Kontext verwendet werden sollte. Wenn eine RDP-Sitzung an einen kompromittierten Client initiiert wird, den ein Angreifer bereits steuert, kann der Angreifer diesen geöffneten Kanal verwenden, um Sitzungen im Namen des Benutzers zu erstellen (ohne die Anmeldeinformationen zu kompromittieren), um auf die Ressourcen eines Benutzers zuzugreifen. begrenzte Zeit (einige Stunden), nachdem die Sitzung getrennt wurde.

Daher empfehlen wir stattdessen, dass Sie die Option eingeschränkter Administratormodus verwenden. Für Helpdesk-Support Szenarien sollten RDP-Verbindungen nur mithilfe des/RestrictedAdmin-Schalters initiiert werden. Dadurch wird sichergestellt, dass Anmeldeinformationen und andere Benutzer Ressourcen nicht für kompromittierte Remotehosts verfügbar gemacht werden. Weitere Informationen finden Sie unter [mildernder Pass-the-Hash und anderer Identitätsdiebstahl v2](#).

Um die Sicherheit weiter zu verhärten, empfehlen wir außerdem, dass Sie eine lokale Administratorkennwort-Lösung (Laps) implementieren, eine in Windows 8,1 eingeführte Gruppenrichtlinien-clientseitige Erweiterung (CSE), die die Kennwortverwaltung des lokalen Administrators automatisiert. Runden verringert das Risiko einer lateralen Eskalation und anderer Cyberattacken erleichtert, wenn Kunden dieselbe administrative lokale Konto- und Kennwortkombination auf allen ihren Computern verwenden. Sie können [hier](#)runden herunterladen und installieren.

Weitere Informationen zu runden finden Sie unter [Microsoft Security Advisory 3062591](#).

Anforderungen für Remote-Anmeldeinformationen

Für die Verwendung von Windows Defender Remote Credential Guard müssen der Remote Desktop Client und der Remote Host die folgenden Anforderungen erfüllen:

Das Remote Desktop-Clientgerät:

- Muss mindestens Windows 10, Version 1703, ausgeführt werden, um Anmeldeinformationen angeben zu können, die an das Remotegerät gesendet werden. Dadurch können Benutzer als unterschiedliche Benutzer ausgeführt werden, ohne Anmeldeinformationen an den Remotecomputer senden zu müssen.
- Muss mindestens Windows 10, Version 1607 oder Windows Server 2016 ausgeführt werden, um die Anmeldeinformationen des Benutzers zu verwenden. Dazu muss sich das Konto des Benutzers sowohl beim Clientgerät als auch beim Remote Host anmelden können.
- Muss die klassische Windows-Anwendung "Remote Desktop" ausführen. Die universelle Windows-Plattform-App für Remote Desktop unterstützt keine Windows Defender-Remoteanmeldeinformationen.
- Sie müssen die Kerberos-Authentifizierung verwenden, um eine Verbindung mit dem Remote Host herzustellen. Wenn der Client keine Verbindung mit einem Domänencontroller herstellen kann, versucht RDP, auf NTLM zurückzugreifen. Windows Defender Remote Credential Guard lässt keine NTLM-Fallbacks zu, da dadurch die Anmeldeinformationen für das Risiko verfügbar gemacht werden.

Der Remote Desktop-Remote Host:

- Muss mindestens Windows 10, Version 1607 oder Windows Server 2016 ausgeführt werden.
- Es müssen eingeschränkte Administratorverbindungen zugelassen werden.
- Muss dem Domänenbenutzer des Clients den Zugriff auf Remote Desktop Verbindungen gestatten.
- Es muss eine Delegierung nicht exportierbarer Anmeldeinformationen zugelassen werden.

Es gibt keine Hardwareanforderungen für Windows Defender Remote Credential Guard.

NOTE

Auf Remote Desktop-Clientgeräten, auf denen frühere Versionen unter Windows 10, Version 1607, ausgeführt werden, werden nur Anmeldeinformationen unterstützt, sodass das Clientgerät auch mit einer Active Directory-Domäne verbunden sein muss. Sowohl der Remote Desktop Client als auch der Server müssen der gleichen Domäne angehören, oder der Remotedesktopserver kann mit einer Domäne verbunden werden, die über eine Vertrauensstellung zur Domäne des Clientgeräts verfügt.

- Damit Windows Defender Remote Credential Guard unterstützt wird, muss sich der Benutzer über die Kerberos-Authentifizierung beim Remote Host authentifizieren.
- Auf dem Remote Host muss mindestens Windows 10, Version 1607, oder Windows Server 2016 ausgeführt werden.
- Die klassische Windows-App für Remote Desktop ist erforderlich. Die universelle Windows-Plattform-App für Remote Desktop unterstützt keine Windows Defender-Remoteanmeldeinformationen.

Aktivieren von Windows Defender Remote Credential Guard

Sie müssen den eingeschränkten Administrator oder den Windows Defender-Remote Anmelde Informationsschutz auf dem Remote Host mithilfe der Registrierung aktivieren.

1. Öffnen Sie den Registrierungs-Editor auf dem Remote Host.
2. Aktivieren des eingeschränkten Administrator- und Windows Defender-Remote Anmelde Informationsschutzes:
 - Wechseln Sie zu HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa.
 - Fügen Sie einen neuen DWORD-Wert mit dem Namen **DisableRestrictedAdmin** hinzu.
 - Wenn Sie den eingeschränkten Administrator und die Windows Defender-Remoteanmeldeinformationen aktivieren möchten, legen Sie den Wert dieser Registrierungseinstellung auf 0 fest, um Windows Defender Remote Credential Guard zu aktivieren.
3. Schließen Sie den Registrierungs-Editor.

Sie können dies hinzufügen, indem Sie an einer Eingabeaufforderung mit erhöhten Rechten den folgenden Befehl ausführen:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0 /t REG_DWORD
```

Verwenden von Windows Defender Remote Credential Guard

Ab Windows 10, Version 1703, können Sie Windows Defender Remote Credential Guard auf dem Clientgerät aktivieren, entweder mithilfe von Gruppenrichtlinien oder mithilfe eines Parameters mit der Remote Desktop Verbindung.

Aktivieren von Windows Defender Remote Credential Guard mithilfe von Gruppenrichtlinien

1. Wechseln Sie in der Gruppenrichtlinien-Verwaltungskonsolle zu **Computer Configuration -> Administrative Templates -> System -> Credentials Delegation**.
2. Doppelklicken Sie auf **Delegation von Anmeldeinformationen auf Remoteserver einschränken**.

3. Unter **verwenden Sie den folgenden eingeschränkten Modus:**

- Wenn Sie entweder den [eingeschränkten Administratormodus](#) oder den Windows Defender-Remote Anmelde Informationsschutz anfordern möchten, wählen Sie **Windows Defender Remote Credential Guard bevorzugen** aus. In dieser Konfiguration wird Windows Defender Remote Credential Guard bevorzugt, es wird jedoch der eingeschränkte Administratormodus (sofern unterstützt) verwendet, wenn die Windows Defender-Remoteanmeldeinformationen nicht verwendet werden kann.

Hinweis: Weder Windows Defender Remote Credential Guard noch eingeschränkter Administratormodus sendet Anmeldeinformationen in Klartext an den Remote Desktop Server.

- Wenn Sie Windows Defender Remote Credential Guard anfordern möchten, wählen Sie **Windows Defender-Remoteanmeldeinformationen anfordern** aus. Bei dieser Einstellung kann eine Remote Desktop Verbindung nur erfolgreich ausgeführt werden, wenn der Remotecomputer die [Anforderungen](#) erfüllt, die weiter oben in diesem Thema aufgeführt sind.
- Wenn Sie den eingeschränkten Administratormodus anfordern möchten, wählen Sie **eingeschränkter Administrator erforderlich** aus. Informationen zum eingeschränkten Administratormodus finden Sie in der Tabelle unter [Vergleich der Windows Defender-Remoteanmeldeinformationen mit anderen Remote Desktop-Verbindungsoptionen](#) weiter oben in diesem Thema.

4. Klicken Sie auf **OK**.

5. Schließen Sie die Gruppenrichtlinien-Verwaltungskonsole.
6. Führen Sie an einer Eingabeaufforderung **gpupdate. exe Force** aus, um sicherzustellen, dass das Gruppenrichtlinienobjekt angewendet wird.

Verwenden von Windows Defender Remote Credential Guard mit einem Parameter für die Remote Desktop Verbindung

Wenn Sie in Ihrer Organisation keine Gruppenrichtlinien verwenden oder wenn nicht alle Ihre Remotehosts die Remoteanmeldeinformationen unterstützen, können Sie den remoteGuard-Parameter hinzufügen, wenn Sie die Remote Desktop Verbindung starten, um die Windows Defender-Remoteanmeldeinformationen für diese Verbindung zu aktivieren. .

```
mstsc.exe /remoteGuard
```

NOTE

Der Benutzer muss Teil der Gruppe "Administratoren" sein.

Überlegungen bei der Verwendung von Windows Defender Remote Credential Guard

- Windows Defender Remote Credential Guard unterstützt keine Verbundauthentifizierung. Wenn Sie beispielsweise versuchen, auf einen Dateiserver von einem Remote Host zuzugreifen, der einen Geräte Anspruch erfordert, wird der Zugriff verweigert.
- Die Windows Defender-Remote Anmeldeinformationen können nur verwendet werden, wenn eine Verbindung mit einem Gerät hergestellt wird, das mit einer Windows Server Active Directory-Domäne verbunden ist, einschließlich von AD-Domänen verbundenen Servern, die als Azure Virtual Machines (VMS) ausgeführt werden. Die Windows Defender-Remote Anmelde Informations Überwachung kann nicht verwendet werden, wenn eine Verbindung zu Remotegeräten hergestellt wird, die mit Azure Active Directory verbunden sind.
- Der Remote Desktop-Anmelde Informationsschutz funktioniert nur mit dem RDP-Protokoll.
- Es werden keine Anmeldeinformationen an das Zielgerät gesendet, das Zielgerät erhält jedoch weiterhin Kerberos-Service Tickets für sich.
- Der Server und der Client müssen sich mit Kerberos authentifizieren.

Technische Referenz für Smartcards

04.01.2020 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

Die Smartcard-Technische Referenz beschreibt die Windows-Smartcard-Infrastruktur für physische Smartcards und die Funktionsweise von Smartcard-bezogenen Komponenten in Windows. Dieses Dokument enthält auch Informationen zu Tools, die IT-Entwickler und-Administratoren zur Problembehandlung, zum Debuggen und zur Bereitstellung von Smartcard-basierter starker Authentifizierung im Unternehmen verwenden können.

Zielgruppe

In diesem Dokument wird erläutert, wie die Windows-Smartcard-Infrastruktur funktioniert. Wenn Sie diese Informationen verstehen möchten, sollten Sie über grundlegende Kenntnisse der Infrastruktur öffentlicher Schlüssel (PKI) und Smartcard-Konzepte verfügen. Dieses Dokument richtet sich an:

- IT-Entwickler,-Manager und-Mitarbeiter in Unternehmen, die beabsichtigen, Smartcards in Ihrer Organisation bereitzustellen oder zu verwenden.
- Smartcard-Anbieter, die Smartcard-Minitreiber oder Anmeldeinformationsanbieter schreiben.

Was sind Smartcards?

Smartcards sind manipulationssichere tragbare Speichergeräte, mit denen die Sicherheit von Aufgaben wie Authentifizierung von Clients, Signieren von Code, Sichern von e-Mails und Anmelden mit einem Windows-Domänenkonto verbessert werden kann.

Smartcards bieten:

- Manipulations resistenter Speicher zum Schutz privater Schlüssel und anderer Formen personenbezogener Informationen.
- Isolierung sicherheitsrelevanter Berechnungen, die Authentifizierung, digitale Signaturen und Schlüsselaustausch aus anderen Teilen des Computers beinhalten. Diese Berechnungen werden auf der Smartcard durchgeführt.
- Portabilität von Anmeldeinformationen und anderen privaten Informationen zwischen Computern am Arbeitsplatz, zu Hause oder unterwegs.

Smartcards können nur zum Anmelden bei Domänenkonten und nicht zu lokalen Konten verwendet werden.

Wenn Sie ein Kennwort für die interaktive Anmeldung an einem Domänenkonto verwenden, verwendet Windows das Kerberos-Protokollversion 5 (V5) für die Authentifizierung. Wenn Sie eine Smartcard verwenden, verwendet das Betriebssystem die Kerberos V5-Authentifizierung mit X. 509 v3-Zertifikaten.

Virtuelle Smartcards wurden in Windows Server 2012 und Windows 8 eingeführt, um die Notwendigkeit einer physischen Smartcard, des Smartcard-Readers und der zugehörigen Verwaltung dieser Hardware zu verringern. Informationen zur Virtual Smartcard-Technologie finden Sie unter [Übersicht über virtuelle Smartcards](#).

In dieser technischen Referenz

Dieser Bezug enthält die folgenden Themen:

- [Funktionsweise der Smartcardanmeldung in Windows](#)

- Smartcardarchitektur
- Zertifikatanforderungen und Enumeration
- Smartcard und Remotedesktopdienste
- Smartcards für den Windows-Dienst
- Zertifikatverteilungsdienst
- Dienst „Richtlinie zum Entfernen der Smartcard“
- Tools und Einstellungen für Smartcards
 - Smartcards-Debuginformationen
 - Gruppenrichtlinien- und Registrierungseinstellungen für Smartcards
 - Smartcardereignisse

Funktionsweise der Smartcardanmeldung in Windows

12.09.2019 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT Professional finden Sie Links zu Ressourcen zur Implementierung von Smartcard-Technologien im Windows-Betriebssystem. Sie umfasst die folgenden Ressourcen zur Architektur, zur Zertifikatsverwaltung und zu Diensten, die sich auf die Verwendung von Smartcards beziehen:

- [Smartcard-Architektur](#): Hier erfahren Sie, wie Sie die Kommunikation mit Smartcards und Smartcard-Lesern aktivieren, die je nach Anbieter unterschiedlich sein können.
- [Zertifikatanforderungen und-Enumeration](#): erfahren Sie mehr über die Anforderungen für Smartcard-Zertifikate basierend auf dem Betriebssystem und über die Vorgänge, die vom Betriebssystem ausgeführt werden, wenn eine Smartcard in den Computer eingefügt wird.
- [Smartcard-und Remotedesktopdienste](#): erfahren Sie, wie Sie Smartcards für Remotedesktopverbindungen verwenden.
- [Smartcards für Windows-Dienst](#): erfahren Sie, wie der Smart Cards für Windows-Dienst implementiert ist.
- [Zertifikat Propagations Dienst](#): erfahren Sie, wie der Zertifikat Propagations Dienst funktioniert, wenn eine Smartcard auf einem Computer eingefügt wird.
- [Richtlinien-Dienst](#) für die Smartcard-Entfernung: erfahren Sie, wie Sie mithilfe von Gruppenrichtlinien steuern können, was geschieht, wenn ein Benutzer eine Smartcard entfernt.

Smartcardarchitektur

12.09.2019 • 18 minutes to read

Gilt für: Windows 10, Windows Server 2016

Dieses Thema für IT-Experten beschreibt die Systemarchitektur, die Smartcards im Windows-Betriebssystem unterstützt, einschließlich Architektur des Anmeldeinformationsanbieters und der Architektur des Smart Card-Subsystems.

Bei der Authentifizierung handelt es sich um einen Prozess zur Überprüfung der Identität eines Objekts oder einer Person. Wenn Sie ein Objekt, beispielsweise eine Smartcard, authentifizieren, besteht das Ziel darin, zu überprüfen, ob das Objekt echt ist. Wenn Sie eine Person authentifizieren, besteht das Ziel darin, zu überprüfen, ob es sich nicht um einen Betrüger handelt.

In einem Netzwerk Kontext stellt die Authentifizierung den Akt dar, bei dem eine Netzwerkanwendung oder-Ressource Identität bewiesen wird. In der Regel wird Identität durch einen kryptografischen Vorgang bewiesen, der einen Schlüssel verwendet, der nur dem Benutzer bekannt ist (beispielsweise mit der Kryptografie mit öffentlichen Schlüsseln) oder einem freigegebenen Schlüssel. Die Serverseite des Authentifizierungs Austauschs vergleicht die signierten Daten mit einem bekannten kryptografischen Schlüssel, um den Authentifizierungsversuch zu überprüfen. Das Speichern der kryptografischen Schlüssel an einem sicheren zentralen Speicherort macht den Authentifizierungsprozess skalierbar und verwaltbar.

Für Smartcards unterstützt Windows eine Anbieter Architektur, die die Anforderungen der sicheren Authentifizierung erfüllt und erweiterbar ist, sodass Sie benutzerdefinierte Anmeldeinformationsanbieter einbeziehen können. Dieses Thema enthält Informationen zu folgenden Themen:

- [Anmeldeinformationsanbieter-Architektur](#)
- [Architektur des Smart Card-Subsystems](#)

Anmeldeinformationsanbieter-Architektur

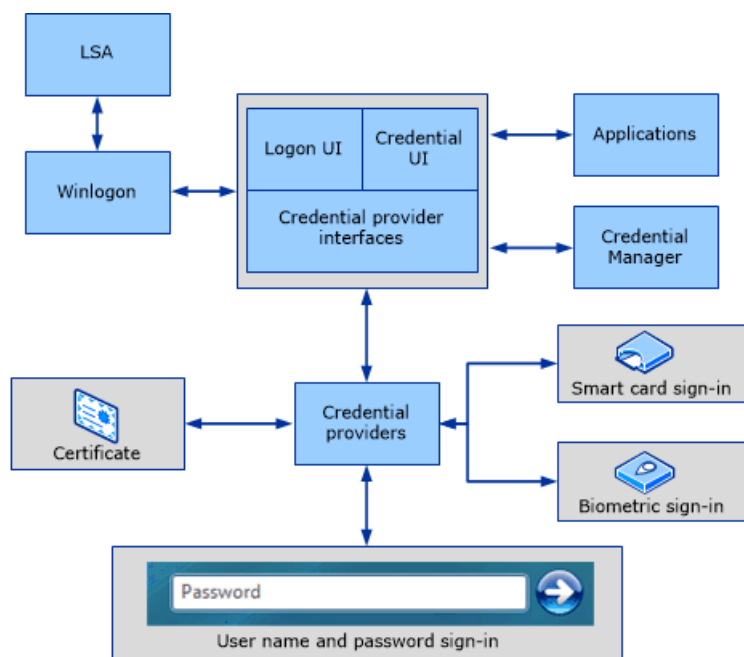
In der folgenden Tabelle sind die Komponenten aufgelistet, die in der interaktiven Anmeldearchitektur von Windows Server und Windows-Betriebssystemen enthalten sind.

KOMPONENTE	BESCHREIBUNG
Winlogon	Bietet eine interaktive Anmelde Infrastruktur.
Anmeldebenutzeroberfläche	Bietet ein interaktives UI-Rendering.
Anmeldeinformationsanbieter (Kennwort und Smartcard)	Beschreibt Anmeldeinformationen und das Serialisieren von Anmeldeinformationen.
Local Security Authority (LSA)	Verarbeitet Anmeldeinformationen.
Authentifizierungspakete	Enthält NTLM und das Kerberos-Protokoll. Kommuniziert mit Server Authentifizierungspaketen, um Benutzer zu authentifizieren.

Die interaktive Anmeldung in Windows beginnt, wenn der Benutzer STRG + ALT + ENTF drückt. Die Tastenkombination STRG + ALT + ENTF wird als Secure Attention Sequence (SAS) bezeichnet. Damit andere

Programme und Prozesse weiterhin verwendet werden können, registriert Winlogon diese Sequenz während des Startvorgangs.

Nach dem Empfang der SAS generiert die Benutzeroberfläche dann die Anmelde Kachel aus den Informationen, die von den registrierten Anmeldeinformationsanbietern empfangen wurden. Die folgende Abbildung zeigt die Architektur für Anmeldeinformationsanbieter im Windows-Betriebssystem.



*** Abbildung1 -*Anmeldeinformationsanbieter-Architektur**

In der Regel muss ein Benutzer, der sich mit einem lokalen Konto oder einem Domänenkonto bei einem Computer anmeldet, einen Benutzernamen und ein Kennwort eingeben. Diese Anmeldeinformationen werden verwendet, um die Identität des Benutzers zu überprüfen. Bei der Smartcard-Anmeldung sind die Anmeldeinformationen eines Benutzers auf dem Sicherheitschip der Smartcard enthalten. Mit einem Smartcard-Lesegerät kann der Computer mit dem Sicherheitschip auf der Smartcard interagieren. Wenn sich Benutzer mit einer Smartcard anmelden, geben Sie anstelle eines Benutzernamens und Kennworts eine persönliche Identifikationsnummer (PIN) ein.

Anmeldeinformationsanbieter sind in-Process-COM-Objekte, die auf dem lokalen System ausgeführt werden und zum Sammeln von Anmeldeinformationen verwendet werden. Die Benutzeroberfläche für die Anmeldung bietet interaktive Benutzeroberflächen Wiedergabe, Winlogon bietet interaktive Anmelde Infrastruktur, und Anmeldeinformationsanbieter arbeiten mit diesen beiden Komponenten zusammen, um die Anmeldeinformationen zu erfassen und zu verarbeiten.

Winlogon weist die Anmeldebenutzeroberfläche an, die Kacheln des Anmeldeinformationsanbieters anzuzeigen, nachdem ein SAS-Ereignis empfangen wurde. Die Anmeldebenutzeroberfläche fragt jeden Anmeldeinformationsanbieter nach der Anzahl der Anmeldeinformationen ab, die er auflisten möchte. Anmeldeinformationsanbieter haben die Möglichkeit, eine dieser Kacheln als Standard anzugeben. Nachdem alle Anbieter Ihre Kacheln aufgelistet haben, zeigt die Anmeldebenutzeroberfläche Sie dem Benutzer an. Der Benutzer interagiert mit einer Kachel, um die richtigen Anmeldeinformationen bereitzustellen. Die Anmeldebenutzeroberfläche sendet diese Anmeldeinformationen zur Authentifizierung.

In Kombination mit der unterstützenden Hardware können Anmeldeinformationsanbieter das Windows-Betriebssystem so erweitern, dass Benutzer sich mithilfe von Biometrie (beispielsweise Fingerabdruck, Netzhaut oder Spracherkennung), Kennwort, PIN, Smartcard-Zertifikat oder beliebige benutzerdefinierte Anmeldungen anmelden können. Authentifizierungspaket. Unternehmen und IT-Experten können benutzerdefinierte Authentifizierungsmechanismen für alle Domänenbenutzer entwickeln und bereitstellen, und Sie können Benutzer ausdrücklich dazu verpflichten, diesen benutzerdefinierten Anmeldemechanismus zu verwenden.

**** Hinweis Anbieter von Anmeldeinformationen sind keine Erzwingungsmechanismen. Sie werden zum Sammeln und Serialisieren von Anmeldeinformationen verwendet. Die LSA- und Authentifizierungspakete erzwingen Sicherheit.

Anmeldeinformationsanbieter können zur Unterstützung der einmaligen Anmeldung (Single Sign-in, SSO) entwickelt werden. In diesem Verfahren authentifizieren Sie Benutzer mit einem sicheren Netzwerkzugriffspunkt (mithilfe von RADIUS und anderen Technologien) für die Anmeldung beim Computer.

Anmeldeinformationsanbieter sind auch für die Unterstützung der anwendungsspezifischen Erfassung von Anmeldeinformationen konzipiert und können für die Authentifizierung für Netzwerkressourcen, das Hinzufügen von Computern zu einer Domäne oder die Genehmigung des Administrators für die Benutzerkontensteuerung (UAC) verwendet werden.

Mehrere Anmeldeinformationsanbieter können auf einem Computer koexistieren.

Anmeldeinformationsanbieter müssen auf einem Computer mit Windows registriert sein und für folgende Aufgaben verantwortlich sein:

- Beschreibung der Anmeldeinformationen, die für die Authentifizierung erforderlich sind.
- Behandeln von Kommunikation und Logik mit externen Authentifizierungs Behörden
- Verpacken von Anmeldeinformationen für interaktive und Netzwerkanmeldungen

**** Hinweis die API des Anmeldeinformationsanbieters rendert die Benutzeroberfläche nicht. Sie beschreibt, was gerendert werden muss.

Nur der Anmeldeinformationsanbieter für Kennwörter steht im abgesicherten Modus zur Verfügung.

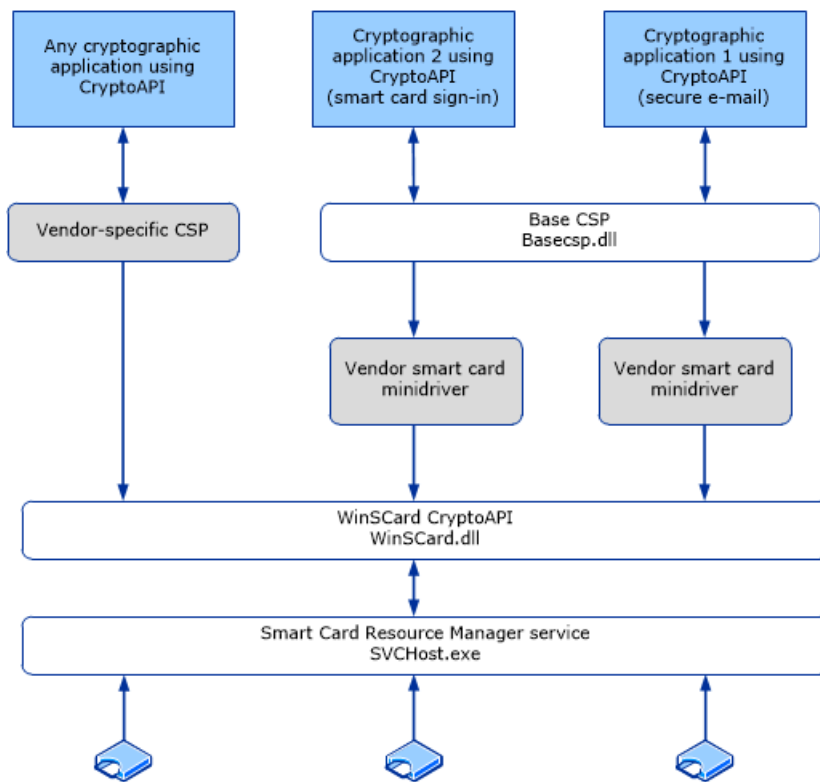
Der Anbieter von Smartcard-Anmeldeinformationen steht während des Netzwerkbetriebs im abgesicherten Modus zur Verfügung.

Architektur des Smart Card-Subsystems

Anbieter bieten Smartcards und Smartcard-Leser an, und in vielen Fällen unterscheiden sich die Anbieter von Smartcards und Smartcard-Lesern. Treiber für Smartcard-Leser werden in den [Standard für Personal Computer/Smartcard \(PC/SC\)](#) geschrieben. Jede Smartcard muss einen Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) aufweisen, der die CryptoAPI-Schnittstellen verwendet, um kryptografische Vorgänge zu ermöglichen, und die winscard-APIs, um die Kommunikation mit Smartcard-Hardware zu ermöglichen.

Basis-CSP und Smartcard-Mini Driver-Architektur

Bild2 veranschaulicht die Beziehung zwischen CryptoAPI, Kryptografiedienstanbieter, dem Smartcard-Basis-Kryptografiedienstanbieter (Cryptographic Service Provider, Base CSP) und Smartcard-Minitreiber.



* **Bild2** *-Basis-CSP und Smartcard-Mini Driver-Architektur

Zwischenspeicherung mit Basis-CSP und Smartcard KSP

Bei der Smartcard-Architektur werden zwischen Speichungs Mechanismen verwendet, um die Optimierung von Vorgängen zu unterstützen und den Zugriff eines Benutzers auf eine PIN zu verbessern.

- **Datenzwischenspeicherung:** der Datencache bietet einen einzelnen Prozess zum Minimieren von e/a-Vorgängen für Smartcards.
- **Pin-Zwischenspeicherung:** der PIN-Cache hilft dem Benutzer, jedesmal eine PIN erneut einzugeben, wenn die Smartcard nicht authentifiziert wird.

Datenzwischenspeicherung

Jeder CSP implementiert den aktuellen Smartcard-Datencache separat. Der Basis-CSP implementiert einen robusten Zwischenspeichermechanismus, mit dem ein einzelner Prozess die e/a-Vorgänge von Smartcards minimieren kann.

Der vorhandene globale Cache funktioniert wie folgt:

1. Die Anwendung fordert einen kryptografischen Vorgang an. Beispielsweise soll ein Benutzerzertifikat von der Smartcard gelesen werden.
2. Der CSP überprüft seinen Cache auf das Element.
3. Wenn das Element im Cache nicht gefunden wird oder wenn das Element zwischengespeichert ist, aber nicht auf dem neuesten Stand ist, wird das Element von der Smartcard gelesen.
4. Nachdem ein Element von der Smartcard gelesen wurde, wird es dem Cache hinzugefügt. Alle vorhandenen veralteten Kopien dieses Elements werden ersetzt.

Drei Arten von Objekten oder Daten werden vom CSP zwischengespeichert: Pins (Weitere Informationen finden Sie unter [Zwischenspeichern von Pins](#)), Zertifikate und Dateien. Wenn sich die zwischengespeicherten Daten ändern, wird das entsprechende Objekt in aufeinanderfolgenden Vorgängen aus der Smartcard gelesen. Wenn beispielsweise eine Datei auf die Smartcard geschrieben wird, wird der CSP-Cache für die Dateien veraltet, und andere Prozesse lesen die Smartcard mindestens einmal, um den CSP-Cache zu aktualisieren.

Der globale Datencache wird im Smart Cards für Windows-Dienst gehostet. Windows umfasst zwei öffentliche Smartcard-API-Aufrufe, SCardWriteCache und SCardReadCache. Mithilfe dieser API-Aufrufe können Anwendungen globale Daten Zwischenspeicherungsfunktionen zur Verfügung stellen. Jede Smartcard, die der Mini Driver-Spezifikation für Smartcards entspricht, verfügt über eine 16-Byte-Kartenkennung. Dieser Wert wird verwendet, um zwischengespeicherte Daten, die zu einer bestimmten Smartcard gehören, eindeutig zu identifizieren. Der standardmäßige Windows-GUID-Typ wird verwendet. Diese APIs ermöglichen einer Anwendung das Hinzufügen und Lesen von Daten aus dem globalen Cache.

Zwischenspeichern von Pins

Der PIN-Cache schützt den Benutzer vor der Eingabe einer PIN, wenn die Smartcard nicht authentifiziert wird. Nachdem eine Smartcard authentifiziert wurde, wird Sie nicht zwischen hostseitigen Anwendungen unterschieden – jede Anwendung kann auf private Daten auf der Smartcard zugreifen.

Um dies zu vermeiden, wechselt die Smartcard in einen exklusiven Zustand, wenn sich eine Anwendung bei der Smartcard authentifiziert. Dies bedeutet jedoch, dass andere Anwendungen nicht mit der Smartcard kommunizieren können und blockiert werden. Daher werden solche exklusiven Verbindungen minimiert. Das Problem besteht darin, dass für ein Protokoll (wie das Kerberos-Protokoll) mehrere Signierung Vorgänge erforderlich sind. Daher erfordert das Protokoll exklusiven Zugriff auf die Smartcard über einen längeren Zeitraum, oder es sind mehrere Authentifizierungsvorgänge erforderlich. Hier wird der PIN-Cache verwendet, um die ausschließliche Verwendung der Smartcard zu minimieren, ohne dass der Benutzer mehrmals eine PIN eingeben muss.

Im folgenden Beispiel wird gezeigt, wie das funktioniert. In diesem Szenario gibt es zwei Anwendungen: Outlook und Internet Explorer. Die Anwendungen verwenden Smartcards für unterschiedliche Zwecke.

1. Der Benutzer startet Outlook und versucht, eine signierte e-Mail-Nachricht zu senden. Der private Schlüssel befindet sich auf der Smartcard.
2. Outlook fordert den Benutzer auf, die Smartcard-PIN einzugeben. Der Benutzer gibt die richtige PIN ein.
3. E-Mail-Daten werden für den Signaturvorgang an die Smartcard gesendet. Der Outlook-Client formatiert die Antwort und sendet die e-Mail.
4. Der Benutzer öffnet Internet Explorer und versucht, auf eine geschützte Website zuzugreifen, die TLS-Authentifizierung (Transport Layer Security) für den Client erfordert.
5. Internet Explorer fordert den Benutzer auf, die Smartcard-PIN einzugeben. Der Benutzer gibt die richtige PIN ein.
6. Der TLS-bezogene private Schlüssel Vorgang erfolgt auf der Smartcard, und der Benutzer wird authentifiziert und angemeldet.
7. Der Benutzer kehrt zu Outlook zurück, um eine weitere signierte e-Mail zu senden. Dieses Mal wird der Benutzer nicht aufgefordert, eine PIN einzugeben, da die PIN aus dem vorherigen Vorgang zwischengespeichert wurde. Auch wenn der Benutzer Internet Explorer für einen anderen Vorgang erneut verwendet, fordert Internet Explorer den Benutzer nicht auf, eine PIN einzugeben.

Der Basis-CSP verwaltet intern einen Cache für einzelne Prozesse der PIN. Die PIN wird verschlüsselt und im Arbeitsspeicher gespeichert. Die zum Sichern der PIN verwendeten Funktionen sind RtlEncryptMemory, RtlDecryptMemory und RtlSecureZeroMemory, wodurch Puffer, die die PIN enthielten, leer sind.

Smartcard-Auswahl

In den folgenden Abschnitten in diesem Thema wird beschrieben, wie Windows die Smartcard-Architektur zur Auswahl der richtigen Smartcard-Lesesoftware, des Anbieters und der Anmeldeinformationen für eine erfolgreiche Smartcard-Anmeldung nutzt:

- [Container-Spezifikations Ebenen](#)

- Container Operationen
- Kontext-Flags
- Erstellen eines neuen Containers im Hintergrund
- Auswahlverhalten für intelligente Karten
- Anpassen einer Smartcard-Sprachausgabe
- Erstellen einer Smartcard-Übereinstimmung
- Öffnen eines vorhandenen Standardcontainers (kein Reader angegeben)
- Öffnen eines vorhandenen GUID-benannten Containers (kein Reader angegeben)
- Erstellen eines neuen Containers (kein Reader angegeben)
- Löschen eines Containers

Container-Spezifikations Ebenen

Als Antwort auf einen CryptAcquireContext-Aufruf in CryptoAPI versucht der Basis-CSP, dem Container zu entsprechen, den der Aufrufer auf eine bestimmte Smartcard und einen bestimmten Leser angibt. Der Aufrufer kann einen Containernamen mit unterschiedlichen Spezifitäten bereitstellen, wie in der folgenden Tabelle dargestellt, und von den meisten spezifischen zu den am wenigsten spezifischen Anforderungen sortiert werden.

Ebenso versucht die Smartcard KSP als Antwort auf einen NCryptOpenKey-Aufruf in CNG, den Container auf die gleiche Weise abzugleichen, und es wird dasselbe Containerformat verwendet, wie in der folgenden Tabelle dargestellt.

Hinweis Bevor Sie einen Schlüssel mithilfe der Smartcard KSP öffnen, muss ein Aufruf von NCryptOpenStorageProvider (MS_SMART_CARD_KEY_STORAGE_PROVIDER) erfolgen.

TYP	NAME	FORMAT
I	Leser Name und Container Name	\\.\ <Reader Name>\<Container Name>
II	Leser Name und Container Name (null)	\\.\ <Reader Name>
III	Nur Container Name	<Container Name>
IV	Nur Standard Container (null)	NULL

Der Basis-CSP und die Smartcard KSP-Cache-Smartcard behandeln Informationen zum Aufruf Prozess und zu den Smartcards, auf die der Prozess zugegriffen hat. Bei der Suche nach einem Smartcard-Container überprüft der Basis-CSP oder die Smartcard KSP zunächst den Cache des Prozesses. Wenn das zwischengespeicherte Handle ungültig ist oder keine Übereinstimmung gefunden wird, wird die SCardUIDlg-API aufgerufen, um das Kartenhandle abzurufen.

Container Operationen

Die folgenden drei Container Vorgänge können mithilfe von CryptAcquireContext angefordert werden:

1. Erstellen Sie einen neuen Container. (Das CNG-Äquivalent von CryptAcquireContext mit dwFlags, das auf CRYPT_NEWKEYSET eingestellt ist, ist NCryptCreatePersistedKey.)
2. Öffnen Sie einen vorhandenen Container. (Das CNG-Äquivalent von CryptAcquireContext zum Öffnen des Containers lautet NCryptOpenKey.)

3. Löschen eines Containers (Das CNG-Äquivalent von CryptAcquireContext mit dwFlags, das auf CRYPT_DELETEKEYSET eingestellt ist, ist NCryptDeleteKey.)

Die Heuristik, die verwendet wird, um einem kryptografischen handle eine bestimmte Smartcard und einen bestimmten Leser zuzuordnen, basiert auf dem angeforderten Container Vorgang und der verwendeten Container Spezifikation.

Die folgende Tabelle enthält die Einschränkungen für den Container Erstellungsvorgang.

SPEZIFIKATION	EINSCHRÄNKUNG
Kein Hintergrund	Die Erstellung von Schlüsselcontainern muss immer in der Lage sein, die Benutzeroberfläche anzuzeigen, beispielsweise die PIN-Eingabeaufforderung.
Kein Überschreiben vorhandener Container	Wenn der angegebene Container bereits auf der ausgewählten Smartcard vorhanden ist, wählen Sie eine andere Smartcard aus, oder brechen Sie den Vorgang ab.

Kontext-Flags

Die folgende Tabelle zeigt die Kontext-Flags, die als Einschränkungen für den Container Erstellungsvorgang verwendet werden.

FLAG	BESCHREIBUNG
CRYPT_SILENT	Während dieses Vorgangs kann keine Benutzeroberfläche angezeigt werden.
CRYPT_MACHINE_KEYSET	Während dieses Vorgangs sollten keine zwischengespeicherten Daten verwendet werden.
CRYPT_VERIFYCONTEXT	Auf die Smartcard kann nur auf öffentliche Daten zugegriffen werden.

Zusätzlich zu Container Vorgängen und Container Spezifikationen müssen Sie während der Smartcard-Auswahl andere Benutzeroptionen wie die CryptAcquireContext-Flags berücksichtigen.

**** Wichtig das CRYPT_SILENT-Flag kann nicht zum Erstellen eines neuen Containers verwendet werden.

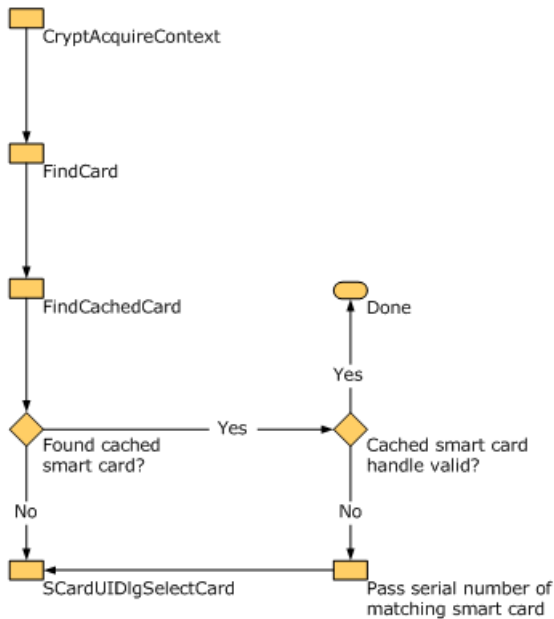
Erstellen eines neuen Containers im Hintergrund

Anwendungen können den Basis-CSP mit CRYPT_DEFAULT_CONTAINER_OPTIONAL aufrufen, die PIN im Silent-Kontext fest legen und dann einen neuen Container im Silent-Kontext erstellen. Dieser Vorgang erfolgt wie folgt:

1. Rufen Sie CryptAcquireContext auf, indem Sie den Namen des Smartcard-Lesers als Container Spezifikationsebene Typ II übergeben und das CRYPT_DEFAULT_CONTAINER_OPTIONAL-Flag angeben.
2. Rufen Sie CryptSetProvParam auf, indem Sie PP_KEYEXCHANGE_PIN oder PP_SIGNATURE_PIN und eine NULL-terminierte ASCII-PIN angeben.
3. Freigeben des in Schritt 1 erworbenen Kontexts
4. Rufen Sie CryptAcquireContext mit CRYPT_NEWKEYSET auf, und geben Sie die Container Spezifikationsebene Typ I an.
5. Rufen Sie CryptGenKey auf, um den Schlüssel zu erstellen.

Auswahlverhalten für intelligente Karten

In einigen der folgenden Szenarien kann der Benutzer zum Einfügen einer Smartcard aufgefordert werden. Wenn der Benutzerkontext stumm ist, schlägt dieser Vorgang fehl, und es wird keine Benutzeroberfläche angezeigt. Andernfalls kann der Benutzer als Antwort auf die Benutzeroberfläche eine Smartcard einfügen oder auf **"Abbrechen"** klicken. Wenn der Benutzer den Vorgang abbricht, schlägt der Vorgang fehl. Das Flussdiagramm in Figure3 zeigt die Auswahlsschritte an, die vom Windows-Betriebssystem ausgeführt werden.



*** Figure3 -*Auswahlverhalten für Smartcards**

Im Allgemeinen wird das Auswahlverhalten von Smartcards von der SCardUIDlgSelectCard-API gehandhabt. Der Basis-CSP interagiert mit dieser API, indem er direkt aufgerufen wird. Der Basis-CSP sendet auch Rückruffunktionen, die zum Filtern und Zuordnen von Kandidaten-Smartcards dienen. Anrufer von CryptAcquireContext bieten Informationen zur Smartcard-Übereinstimmung. Intern verwendet der Basis-CSP eine Kombination aus Smartcard-Seriennummern, Leser Namen und Containernamen, um bestimmte Smartcards zu finden.

Jeder Anruf an SCardUI \ * kann dazu führen, dass weitere Informationen von einer Kandidaten-Smartcard gelesen werden. Die Basis-CSP-Auswahl Rückrufe für Smartcards Zwischenspeichern diese Informationen.

Anpassen einer Smartcard-Sprachausgabe

Bei den Container Spezifikations Ebenen Typ I und Typ II ist der Auswahlprozess für die Smartcards nicht so komplex, da nur die Smartcard im benannten Reader als Übereinstimmung angesehen werden kann. Der Vorgang zum Abgleich einer Smartcard mit einem Smartcard-Lesegerät lautet wie folgt:

1. Suchen Sie den gewünschten Smartcard-Leser. Wenn Sie nicht gefunden werden kann, schlägt der Prozess fehl. (Dazu ist eine Cache Suche nach Leser Name erforderlich.)
2. Wenn sich keine Smartcard im Reader befindet, wird der Benutzer aufgefordert, eine Smartcard einzufügen. (Dies ist nur im nicht stummen Modus; Wenn der Anruf im unbeaufsichtigten Modus erfolgt, schlägt er fehl.)
3. Nur bei der Container Spezifikationsstufe II wird der Name des Standardcontainers auf der ausgewählten Smartcard bestimmt.
4. Suchen Sie den angegebenen Container, um einen vorhandenen Container zu öffnen oder einen vorhandenen Container zu löschen. Wenn der angegebene Container auf dieser Smartcard nicht gefunden werden kann, wird der Benutzer aufgefordert, eine Smartcard einzufügen.
5. Wenn das System versucht, einen neuen Container zu erstellen, schlägt der Prozess fehl, wenn der angegebene Container auf dieser Smartcard bereits vorhanden ist.

Erstellen einer Smartcard-Übereinstimmung

Für Container Spezifikations Ebenen III und IV wird eine breitere Methode verwendet, um eine geeignete Smartcard mit einem Benutzerkontext zu vergleichen, da mehrere zwischengespeicherte Smartcards die angegebenen Kriterien erfüllen können.

Öffnen eines vorhandenen Standardcontainers (kein Reader angegeben)

**** Hinweis dieser Vorgang setzt voraus, dass Sie die Smartcard mit dem Basis-CSP verwenden.

1. Für jede Smartcard, auf die der Basis-CSP zugegriffen hat und die Handle-und Container Informationen zwischengespeichert sind, sucht der Basis-CSP nach einem gültigen Standardcontainer. Es wird versucht, die Gültigkeit des zwischengespeicherten SCARDHANDLE zu überprüfen. Wenn das Smartcard-Handle nicht gültig ist, sucht der Basis-CSP weiterhin nach einer neuen Smartcard.
2. Wenn im Basis-CSP-Cache keine übereinstimmende Smartcard gefunden wird, werden die Basis-CSP-Aufrufe an das Smartcard-Subsystem durchgestellt. SCardUIDlgSelectCard () wird zusammen mit einem geeigneten Rückruf Filter verwendet, um eine passende Smartcard mit einem gültigen Standardcontainer zu finden.

Öffnen eines vorhandenen GUID-benannten Containers (kein Reader angegeben)

**** Hinweis dieser Vorgang setzt voraus, dass Sie die Smartcard mit dem Basis-CSP verwenden.

1. Suchen Sie für jede Smartcard, die bereits beim Basis-CSP registriert ist, nach dem angeforderten Container. Versuchen Sie, die Gültigkeit des zwischengespeicherten SCARDHANDLE zu überprüfen. Wenn das Smartcard-Handle nicht gültig ist, wird die Seriennummer der Smartcard an die SCardUI \ *-API übergeben, um weiterhin nach dieser bestimmten Smartcard zu suchen (und nicht nur eine allgemeine Übereinstimmung für den Containernamen).
2. Wenn keine übereinstimmende Smartcard im Basis-CSP-Cache gefunden wird, wird ein Anruf an das Smartcard-Subsystem durchgeführt. SCardUIDlgSelectCard () wird zusammen mit einem geeigneten Rückruf Filter verwendet, um eine passende Smartcard mit dem angeforderten Container zu finden. Wenn die Seriennummer einer Smartcard aus der Suche in Schritt 1 resultierte, versucht der Rückruf Filter, die Seriennummer und nicht den Containernamen zu erfüllen.

Erstellen eines neuen Containers (kein Reader angegeben)

**** Hinweis dieser Vorgang setzt voraus, dass Sie die Smartcard mit dem Basis-CSP verwenden.

Wenn die PIN nicht zwischengespeichert wird, ist für die Container Erstellung kein CRYPT_SILENT zulässig, da der Benutzer mindestens aufgefordert werden muss, eine PIN einzugeben.

Für andere Vorgänge kann der Aufrufer möglicherweise einen "verify"-Kontext für den Standardcontainer (CRYPT_DEFAULT_CONTAINER_OPTIONAL) erwerben und dann einen Aufruf mit CryptSetProvParam durchführen, um die Benutzer-PIN für nachfolgende Vorgänge zwischenzuspeichern.

1. Aktualisieren Sie für jede Smartcard, die bereits vom CSP bekannt ist, die gespeicherte SCARDHANDLE, und führen Sie die folgenden Überprüfungen durch:
 - a. Wenn die Smartcard entfernt wurde, fahren Sie mit der Suche fort.
 - b. Wenn die Smartcard vorhanden ist, aber bereits über den benannten Container verfügt, fahren Sie mit der Suche fort.
 - c. Wenn die Smartcard verfügbar ist, aber ein Aufruf von CardQueryFreeSpace angibt, dass die Smartcard nicht genügend Speicherplatz für einen zusätzlichen Schlüsselcontainer aufweist, fahren Sie mit der Suche fort.

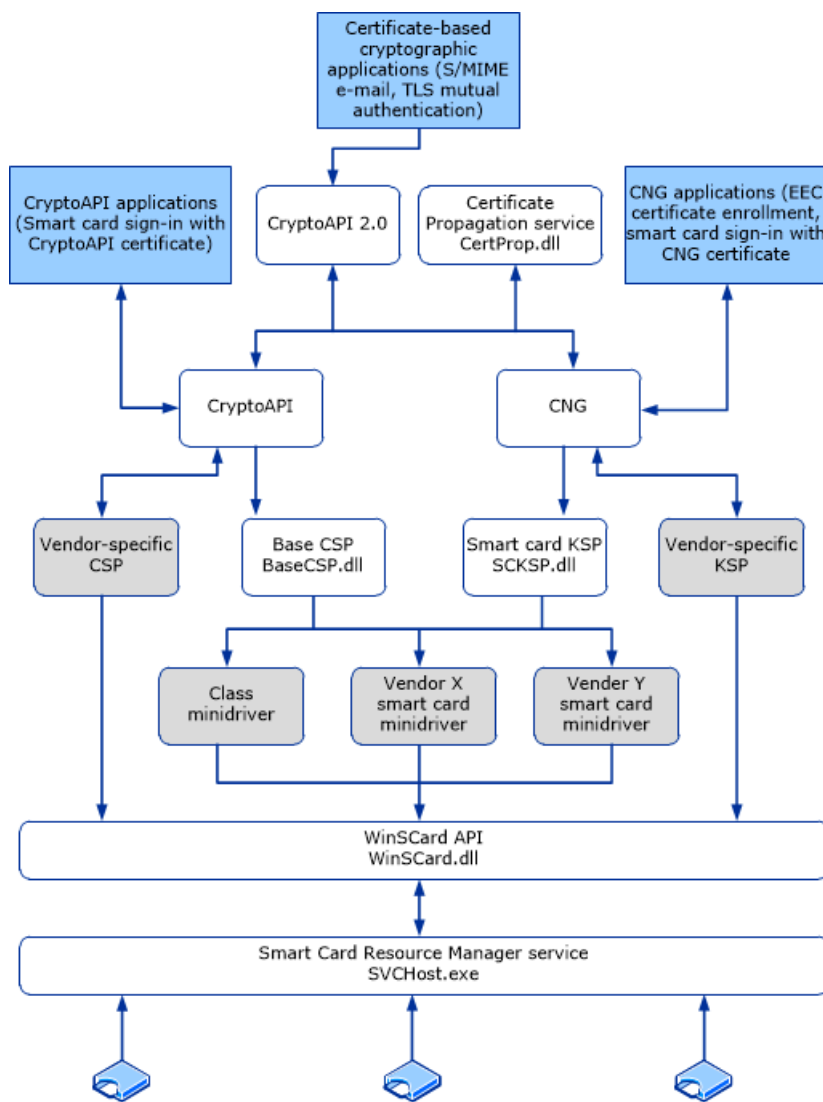
- d. Verwenden Sie andernfalls die erste verfügbare Smartcard, die die obigen Kriterien für die Container Erstellung erfüllt.
2. Wenn keine übereinstimmende Smartcard im CSP-Cache gefunden wird, führen Sie einen Anruf an das Smartcard-Subsystem durch. Der Rückruf, der zum Filtern von aufgelisteten Smartcards verwendet wird, überprüft, ob eine potenzielle Smartcard nicht bereits über den benannten Container verfügt, und dass CardQueryFreeSpace angibt, dass die Smartcard genügend Speicherplatz für einen zusätzlichen Container aufweist. Wenn keine geeignete Smartcard gefunden wird, wird der Benutzer aufgefordert, eine Smartcard einzufügen.

Löschen eines Containers

1. Wenn der angegebene Containername NULL ist, wird der Standardcontainer gelöscht. Das Löschen des Standardcontainers bewirkt, dass ein neuer Standardcontainer willkürlich ausgewählt wird. Aus diesem Grund wird dieser Vorgang nicht empfohlen.
2. Aktualisieren Sie für jede Smartcard, die bereits vom CSP bekannt ist, die gespeicherte SCARDHANDLE, und führen Sie die folgenden Überprüfungen durch:
 - a. Wenn die Smartcard nicht über den benannten Container verfügt, fahren Sie mit der Suche fort.
 - b. Wenn die Smartcard über den benannten Container verfügt, das Smartcard-handle aber nicht mehr gültig ist, speichern Sie die Seriennummer der entsprechenden Smartcard, und übergeben Sie Sie an SCardUI \ *.
3. Wenn keine übereinstimmende Smartcard im CSP-Cache gefunden wird, führen Sie einen Anruf an das Smartcard-Subsystem durch. Der Rückruf, der zum Filtern von aufgelisteten Smartcards verwendet wird, sollte überprüfen, ob eine Kandidaten-Smartcard den benannten Container aufweist. Wenn eine fortlaufende Zahl als Ergebnis der vorherigen Cache Suche bereitgestellt wurde, sollte der Rückruf die aufgelisteten Smartcards auf Seriennummer und nicht auf Container Übereinstimmungen filtern. Wenn der Kontext nicht geräuschlos ist und keine geeignete Smartcard gefunden wird, wird die Benutzeroberfläche angezeigt, in der der Benutzer zum Einfügen einer Smartcard aufgefordert wird.

Basis-CSP und KSP-basierte Architektur in Windows

Bild4 zeigt die Kryptografie-Architektur, die vom Windows-Betriebssystem verwendet wird.



* **Bild4 -Kryptografie-Architektur**

Basis-CSP-und Smartcard-KSP-Eigenschaften in Windows

Die folgenden Eigenschaften werden in Windows-Versionen unterstützt, die in der Liste " **gilt für** " am Anfang dieses Themas angegeben sind.

**** Hinweis die API-Definitionen befinden sich in Wincrypt. h und winscard. h.

EIGENSCHAFT	BESCHREIBUNG
PP_USER_CERTSTORE	<ul style="list-style-type: none"> – Wird verwendet, um eine HCERTSTORE zurückzugeben, die alle Benutzerzertifikate auf der Smartcard enthält. -Schreibgeschützt (nur von CryptGetProvParam verwendet) -Anrufer, der für das Schließen des Zertifikatspeichers verantwortlich ist – Mit PKCS_7_ASN_ENCODING oder X509_ASN_ENCODING codiertes Zertifikat -CSP sollte KEY_PROV_INFO für Zertifikate einrichten – Der Zertifikatspeicher sollte als speicherresidenter Speicher angesehen werden. – Zertifikate sollten über ein gültiges CRYPT_KEY_PROV_INFO als Eigenschaft verfügen

EIGENSCHAFT	BESCHREIBUNG
PP_ROOT_CERTSTORE	<ul style="list-style-type: none"> – Lesen und schreiben (wird von CryptGetProvParam und CryptSetProvParam verwendet) – Wird verwendet, um eine Sammlung von Stammzertifikaten auf die Smartcard zu schreiben oder HCERTSTORE zurückzugeben, das Stammzertifikate von der Smartcard enthält. – Wird in erster Linie für die Teilnahme an einer Domäne mithilfe einer Smartcard verwendet -Anrufer, der für das Schließen des Zertifikatspeichers verantwortlich ist
PP_SMARTCARD_READER	<ul style="list-style-type: none"> -Schreibgeschützt (nur von CryptGetProvParam verwendet) – Gibt den Namen des Smartcard-Readers als ANSI-Zeichenfolge zurück, die zum Erstellen eines vollqualifizierten Container namens verwendet wird (also ein Smartcard-Lesegerät und ein Container).
PP_SMARTCARD_GUID	<ul style="list-style-type: none"> -Zurückgeben der Smartcard-GUID (auch als fortlaufende Nummer bezeichnet), die für jede Smartcard eindeutig sein sollte -Wird vom Certificate Propagation Service verwendet, um die Quelle eines Stammzertifikats zu überwachen
PP_UI_PROMPT	<ul style="list-style-type: none"> – Wird verwendet, um die Suchzeichenfolge für das Dialogfeld "SCardUIDlgSelectCard-Karten Einfügung" einzustellen. -Persistent für den gesamten Prozess, wenn er eingerichtet ist -Schreibgeschützt (nur von CryptSetProvParam verwendet)

Auswirkungen auf Kryptografiedienstanbieter in Windows

Kryptografiedienstanbieter (Cryptographic Service Providers, LSP), einschließlich benutzerdefinierter Smartcard-Kryptografiedienstanbieter, werden weiterhin unterstützt, aber dieser Ansatz wird nicht empfohlen. Die Verwendung des vorhandenen Basis-CSP und der Smartcard KSP mit dem Smartcard-Mini Driver-Modell für Smartcards bietet beträchtliche Vorteile in Bezug auf die Leistung sowie die Zwischenspeicherung von Pins und Daten. Ein Mini Driver kann für die Arbeit unter CryptoAPI- und CNG-Ebenen konfiguriert werden. Dies bietet Vorteile von erweiterter kryptografischer Unterstützung, einschließlich elliptischer Kurvenverschlüsselung und AES.

Wenn eine Smartcard von einem CSP und einer Smartcard-Mini Driver registriert wurde, wird die zuletzt installierte Version für die Kommunikation mit der Smartcard verwendet.

Schreiben einer Smartcard-Mini Driver,-CSP oder-KSP

Kryptografiedienstanbieter und KSPs sollten nur geschrieben werden, wenn bestimmte Funktionen in der aktuellen Smartcard-Mini Driver-Architektur nicht zur Verfügung stehen. Beispielsweise unterstützt die Smartcard-Mini Driver-Architektur Hardwaresicherheitsmodule, sodass ein Mini Driver für ein Hardwaresicherheitsmodul geschrieben werden kann und ein CSP oder KSP möglicherweise nicht erforderlich ist, es sei denn, dies ist erforderlich, um Algorithmen zu unterstützen, die nicht in der Basis implementiert sind. CSP oder Smartcard KSP.

Weitere Informationen zum Schreiben einer Smartcard-Mini Driver,-CSP oder-KSP finden Sie unter [Smartcard-Minitreiber](#).

Zertifikatanforderungen und Enumeration

06.03.2020 • 17 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für Entwickler von IT-Experten und Smartcards wird beschrieben, wie Zertifikate verwaltet und für die Smartcard-Anmeldung verwendet werden.

Wenn eine Smartcard eingefügt wird, werden die folgenden Schritte ausgeführt.

**** Hinweis wenn nichts anderes angegeben ist, werden alle Vorgänge im Hintergrund ausgeführt (Crypt _SILENT an CryptAcquireContext übergeben).

1. Die Datenbank des Smartcard-Ressourcen-Managers sucht nach dem Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) der Smartcard.
2. Ein qualifizierter Containername wird mit dem Namen des Smartcard-Readers erstellt und an den CSP übergeben. Das Format ist *\\ . \ <Leser Name> *\\
3. CryptAcquireContext wird aufgerufen, um einen Kontext für den Standardcontainer abzurufen. Wenn ein Fehler auftritt, ist die Smartcard für die Smartcard-Anmeldung unbrauchbar.
4. Der Name des Containers wird mithilfe des PP _CONTAINER-Parameters mit CryptGetProvParam abgerufen.
5. Mithilfe des in Schritt 3 erworbenen Kontexts wird der CSP nach dem Parameter PP _User _CERTSTORE abgefragt (in Windows Vista hinzugefügt). Weitere Informationen finden Sie unter [Smartcard-Architektur](#). Wenn der Vorgang erfolgreich ist, wird der Name eines Zertifikatspeichers zurückgegeben, und der Programmablauf springt zu Schritt 8.
6. Wenn der Vorgang in Schritt 5 fehlschlägt, wird der Standardcontainer Kontext aus Schritt 3 für den at _KEYEXCHANGE-Schlüssel abgefragt.
7. Das Zertifikat wird dann mithilfe von kp _CERTIFICATE aus dem Schlüssel Kontext abgefragt. Das Zertifikat wird einem speicherinternen Zertifikatspeicher hinzugefügt.
8. Für jedes Zertifikat im Zertifikatspeicher aus Schritt 5 oder Schritt 7 werden die folgenden Prüfungen durchgeführt:
 - a. Das Zertifikat muss gültig sein, basierend auf der Systemuhr des Computers (nicht abgelaufen oder gültig mit einem zukünftigen Datum).
 - b. Das Zertifikat darf sich nicht im at _SIGNATURE-Teil eines Containers befinden.
 - c. Das Zertifikat muss einen gültigen Benutzerprinzipalnamen (User Principal Name, UPN) aufweisen.
 - d. Das Zertifikat muss die Verwendung des digitalen Signaturschlüssels aufweisen.
 - e. Das Zertifikat muss die EKU für die Smartcard-Anmeldung aufweisen.

Jedes Zertifikat, das diese Anforderungen erfüllt, wird dem Benutzer mit dem UPN des Zertifikats (oder einer e-Mail-Adresse oder einem Betreff) angezeigt, je nach dem vorhanden sein der Zertifikaterweiterungen.

**** Beachten Sie, dass diese Anforderungen mit denen in Windows Server 2003 identisch sind, Sie

aber ausgeführt werden, bevor der Benutzer die PIN eingibt. Sie können viele davon mithilfe von Gruppenrichtlinieneinstellungen außer Kraft setzen.

9. Der Prozess wählt dann ein Zertifikat aus, und die PIN wird eingegeben.
10. LogonUI.exe Pakete die Informationen und sendet Sie an Lsass.exe, um den Anmeldeversuch zu verarbeiten.
11. Wenn dies erfolgreich ist, wird logonui.exe geschlossen. Dies bewirkt, dass der in Schritt 3 abgerufene kontextfrei gegeben wird.

Informationen zur Zertifikat Unterstützung für Kompatibilität

Obwohl Windows-Versionen vor Windows Vista Unterstützung für Smartcards enthalten, sind die Typen von Zertifikaten, die Smartcards enthalten können, limitiert. Die Einschränkungen lauten wie folgt:

- Jedes Zertifikat muss über einen Benutzerprinzipalnamen (User Principal Name, UPN) und die Smartcard-Anmeldeobjekt-ID (auch bekannt als OID) im Attributfeld Enhanced Key Usage (EKU) verfügen. Es gibt eine Gruppenrichtlinieneinstellung, mit der die Verwendung von ECC-Zertifikaten für die Anmeldung und Authentifizierung ermöglicht wird, um die ECU optional zu machen.
- Jedes Zertifikat muss im Bereich at _KEYEXCHANGE des Standard-CryptoAPI-Containers gespeichert werden, und nicht standardmäßige CryptoAPI-Container werden nicht unterstützt.

In der folgenden Tabelle sind die Zertifikat Unterstützung in älteren Versionen des Windows-Betriebssystems aufgeführt.

BETRIEBSSYSTEM	ZERTIFIKAT UNTERSTÜTZUNG
Windows Server 2008 R2 und Windows 7	<p>Unterstützung für die Smartcard-Anmeldung mit ECC-basierten Zertifikaten. Die ECC-Smartcard-Anmeldung wird über Gruppenrichtlinien aktiviert.</p> <p>ECDH _P256 ECDH Curve P-256 von FIPS 186-2</p> <p>ECDsa _P256 ECDsa Curve P-256 von FIPS 186-2</p> <p>ECDH _P384 ECDH Curve P-384 von FIPS 186-2</p> <p>ECDH _P521 ECDH Curve P-521 von FIPS 186-2</p> <p>ECDsa _P256 ECDH Curve P-256 von FIPS 186-2</p> <p>ECDsa _P384 ECDsa Curve P-384 von FIPS 186-2</p> <p>ECDsa _P521 ECDsa Curve P-384 von FIPS 186-2</p>

BETRIEBSSYSTEM	ZERTIFIKAT UNTERSTÜTZUNG
Windows Server 2008 und Windows Vista	<p>Gültige Zertifikate werden auf allen Smartcards aufgelistet und angezeigt und dem Benutzer präsentiert.</p> <p>Schlüssel sind nicht mehr auf den Standardcontainer beschränkt, und Zertifikate in verschiedenen Containern können ausgewählt werden.</p> <p>ECC-basierte Zertifikate (elliptische Kurve) werden für die Smartcard-Anmeldung nicht unterstützt.</p>

Smartcard-Anmelde Fluss in Windows

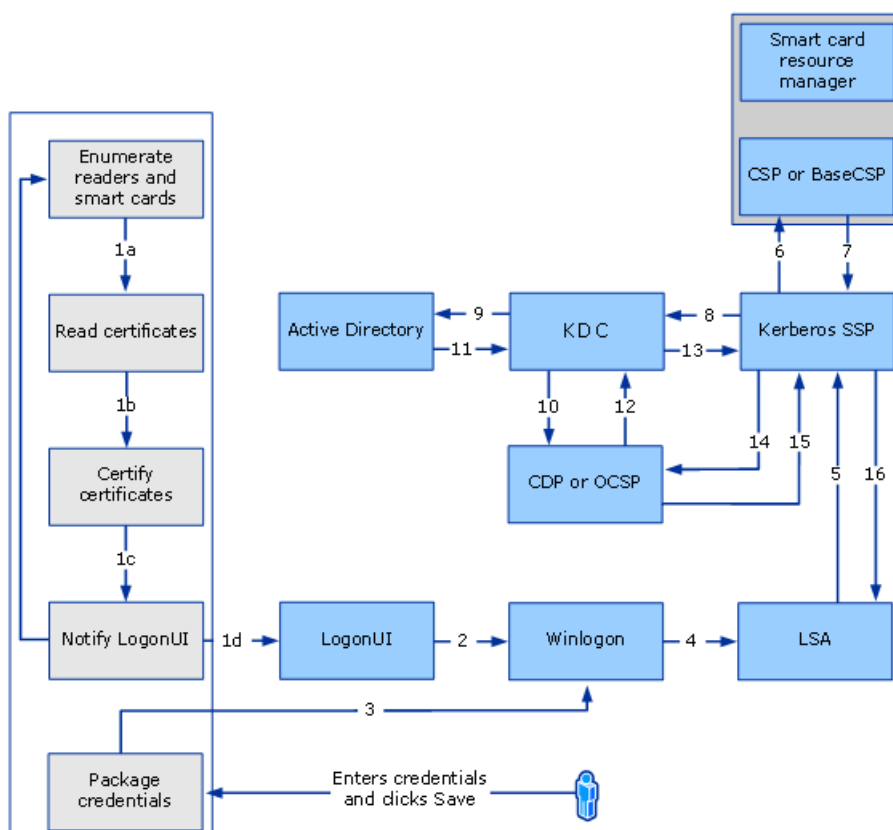
Die meisten Probleme während der Authentifizierung treten aufgrund von Änderungen des Sitzungs Verhaltens auf. Wenn Änderungen auftreten, übernimmt die Local Security Authority (LSA) den Sitzungskontext nicht erneut. Sie beruht stattdessen auf dem kryptografischen Dienstanbieter, um die Sitzungsänderung zu verarbeiten.

In den unterstützten Windows-Versionen, die in der Liste **betrifft zu** Beginn dieses Themas angegeben sind, können Clientzertifikate, die keinen UPN im **subjectAltName** (San)-Feld des Zertifikats enthalten, für die Anmeldung aktiviert werden, die eine größere Auswahl an Zertifikaten unterstützt und mehrere Anmelde Zertifikate auf derselben Karte unterstützt.

Die Unterstützung mehrerer Zertifikate auf derselben Karte ist standardmäßig aktiviert. Neue Zertifikattypen müssen über Gruppenrichtlinien aktiviert werden.

Wenn Sie die für die Anmeldeinformationsanbieter-Richtlinie **gültige Signaturschlüssel zulassen** aktivieren, werden auf dem Anmeldebildschirm alle auf der Smartcard verfügbaren Zertifikate mit einem Signaturschlüssel angezeigt. Dadurch können Benutzer ihre Anmelde Erfahrung auswählen. Wenn die Richtlinie deaktiviert oder nicht konfiguriert ist, werden auf dem Anmeldebildschirm keine Smartcard-Signaturschlüssel basierten Zertifikate angezeigt.

Das folgende Diagramm zeigt, wie die Smartcard-Anmeldung in den unterstützten Windows-Versionen funktioniert.



Anmelde Fluss für Smartcards

Im folgenden werden die Schritte beschrieben, die während einer Smartcard-Anmeldung ausgeführt werden:

1. Winlogon fordert die Anmeldeinformationen für Anmeldebenutzer Oberflächen an.
2. Der Smartcard-Ressourcen-Manager wird asynchron gestartet, und der Smartcard-Anmeldeinformationsanbieter führt die folgenden Aktionen aus:
 - a. Ruft Anmeldeinformationen (eine Liste bekannter Anmeldeinformationen oder wenn keine Anmeldeinformationen vorhanden sind, die Informationen für den Smartcard-Leser ab, die von Windows erkannt wurden).
 - b. Ruft eine Liste von Smartcard-Lesern ab (mithilfe der WinSCard-API) und die Liste der in die einzelnen Karten eingefügten Smartcards.
 - c. Listet jede Karte auf, um zu überprüfen, ob ein Anmeldezertifikat vorhanden ist, das von Gruppenrichtlinien gesteuert wird. Wenn das Zertifikat vorhanden ist, wird es vom Smartcard-Anmeldeinformationsanbieter in einen temporären, sicheren Cache auf dem Computer oder Terminal kopiert.

**** Hinweis Smartcard-Cacheeinträge werden für Zertifikate mit einem Antragstellernamen oder mit einem Betreff-Schlüsselbezeichner erstellt. Wenn das Zertifikat einen Antragstellernamen aufweist, wird es mit einem Index gespeichert, der auf dem Antragstellernamen und dem Aussteller des Zertifikats basiert. Wenn ein anderes Zertifikat mit dem gleichen Antragstellernamen und Zertifikataussteller verwendet wird, wird der vorhandene zwischengespeicherte Eintrag ersetzt. Eine Änderung in diesem Verhalten nach Windows Vista ermöglicht die Bedingung, wenn das Zertifikat keinen Antragstellernamen aufweist, der Cache wird mit einem Index erstellt, der auf dem Subject-Schlüsselbezeichner und dem Zertifikataussteller basiert. Wenn ein anderes Zertifikat über denselben Betreff-Schlüsselbezeichner und Zertifikataussteller verfügt, wird der Cacheeintrag ersetzt. Wenn Zertifikate weder einen Antragstellernamen noch einen Betreff-Schlüsselbezeichner aufweisen, wird kein zwischengespeicherter Eintrag erstellt.

- a. Benachrichtigt die Anmeldebenutzeroberfläche, dass Sie neue Anmeldeinformationen hat.
3. Die Anmeldebenutzeroberfläche fordert die neuen Anmeldeinformationen vom Anbieter von Smartcard-Anmeldeinformationen an. Als Antwort stellt der Smartcard-Anmeldeinformationsanbieter jedes Anmeldezertifikat für die Anmeldebenutzeroberfläche bereit, und entsprechende Anmelde Kacheln werden angezeigt. Der Benutzer wählt eine Smartcard-basierte Anmeldungs Zertifikat Kachel aus, und Windows zeigt das Dialogfeld "Pin" an.
4. Der Benutzer gibt die PIN ein und drückt dann die EINGABETASTE. Der Smartcard-Anmeldeinformationsanbieter verschlüsselt die PIN.
5. Der Anmeldeinformationsanbieter, der sich im LogonUI-System befindet, sammelt die PIN. Als Teil der Anmeldeinformationen für die Verpackung des Smartcard-Anmeldeinformationsanbieters werden die Daten in einem Bordstein _CERTIFICATE _LOGON Struktur gepackt. Der Hauptinhalt der _CERTIFICATE _LOGON Struktur sind die Smartcard-PIN, CSP-Daten (wie Leser Name und Containername), Benutzername und Domänenname. Der Benutzername ist erforderlich, wenn sich die Anmeldedomäne nicht in derselben Gesamtstruktur befindet, da ein Zertifikat mehreren Benutzerkonten zugeordnet werden kann.
6. Der Anmeldeinformationsanbieter umschließt die Daten (wie die verschlüsselte PIN, den Containernamen, den Leser Namen und die Kartenschlüssel Spezifikation) und sendet Sie an LogonUI zurück.
7. Winlogon zeigt die Daten aus LogonUI der LSA mit den Benutzerinformationen in LsaLogonUser an.
8. LSA Ruft das Kerberos-Authentifizierungspaket (Kerberos-SSP) auf, um eine Kerberos-

Authentifizierungsdiensteanforderung (KRB _AS _REQ) zu erstellen, die einen vorauthentifizierungs Dienst enthält (wie in RFC 4556: [Kryptografie mit öffentlichen Schlüsseln für die erste Authentifizierung in Kerberos \(PKINIT\)](#) angegeben).

Wenn die Authentifizierung mithilfe eines Zertifikats durchgeführt wird, das eine digitale Signatur verwendet, bestehen die Vorauthentifizierungsdaten aus dem öffentlichen Zertifikat des Benutzers und dem Zertifikat, das mit dem zugehörigen privaten Schlüssel digital signiert ist.

Wenn die Authentifizierung mithilfe eines Zertifikats durchgeführt wird, das Schlüssel Verschlüsselung verwendet, bestehen die Vorauthentifizierungsdaten aus dem öffentlichen Zertifikat des Benutzers und dem Zertifikat, das mit dem zugehörigen privaten Schlüssel verschlüsselt wurde.

9. Wenn Sie die Anforderung digital signieren möchten (gemäß RFC 4556), wird ein Anruf an den entsprechenden CSP für einen privaten Schlüssel Vorgang durchgeführt. Da der private Schlüssel in diesem Fall auf einer Smartcard gespeichert ist, wird das Smartcard-Subsystem aufgerufen, und der erforderliche Vorgang ist abgeschlossen. Das Ergebnis wird an den Kerberos-Security-Support-Anbieter (SSP) zurückgesendet.
10. Der Kerberos-SSP sendet eine Authentifizierungsanforderung für ein Ticket-Granting-Ticket (TGT) (pro RFC 4556) an den KDC-Dienst (Key Distribution Center), der auf einem Domänencontroller ausgeführt wird.
11. Das KDC findet das Kontoobjekt des Benutzers in den Active Directory-Domänendiensten (AD DS), wie in den [Client Zertifikatanforderungen und-Zuordnungen](#) beschrieben, und verwendet das Zertifikat des Benutzers, um die Signatur zu überprüfen.
12. Das KDC überprüft das Zertifikat des Benutzers (Zeit, Pfad und Sperrungsstatus), um sicherzustellen, dass das Zertifikat aus einer vertrauenswürdigen Quelle stammt. Das KDC verwendet CryptoAPI zum Erstellen eines Zertifizierungspfads aus dem Zertifikat des Benutzers zu einem Stammzertifizierungsstellen-Zertifikat, das sich im Stammspeicher des Domänencontrollers befindet. Das KDC verwendet dann CryptoAPI, um die digitale Signatur auf dem signierten Authentifikator zu überprüfen, der in den Datenfeldern für die Vorauthentifizierung enthalten war. Der Domänencontroller überprüft die Signatur und verwendet den öffentlichen Schlüssel aus dem Zertifikat des Benutzers, um zu beweisen, dass die Anforderung vom Besitzer des privaten Schlüssels stammt, der dem öffentlichen Schlüssel entspricht. Das KDC überprüft auch, ob der Aussteller vertrauenswürdig ist und im NTAUTH-Zertifikatspeicher angezeigt wird.
13. Der KDC-Dienst ruft Benutzerkontoinformationen aus AD DS ab. Das KDC erstellt einen TGT, der auf den Benutzerkontoinformationen basiert, die er aus AD DS abrufen. Zu den Autorisierungsdaten Feldern des TGT gehören die Sicherheits-ID (Security Identifier, SID) des Benutzers, die SIDs für universelle und globale Domänengruppen, zu denen der Benutzer gehört, und (in einer Mehrdomänenumgebung) die SIDs für universelle Gruppen, für die der Benutzer Mitglied ist.
14. Der Domänencontroller gibt den TGT als Teil der krb _AS _REP Antwort an den Client zurück.

**** Hinweis das krb _AS _REP-Paket besteht aus:

- Berechtigungsattribut Zertifikat (PAC)
- SID des Benutzers
- SIDs einer Gruppe, deren Mitglied der Benutzer ist
- Eine Anforderung für den Ticket-Granting-Service (TGS)
- Vorauthentifizierungsdaten

TGT wird mit dem Hauptschlüssel des KDC verschlüsselt, und der Sitzungsschlüssel wird mit einem temporären Schlüssel verschlüsselt. Dieser temporäre Schlüssel wird basierend auf RFC 4556 abgeleitet. Mit CryptoAPI wird der temporäre Schlüssel entschlüsselt. Wenn sich der private Schlüssel als Teil des Entschlüsselungsprozesses auf einer Smartcard befindet, wird ein Anruf an das Smartcard-Subsystem

durchgeführt, wobei der angegebene CSP zum Extrahieren des Zertifikats dient, das dem öffentlichen Schlüssel des Benutzers entspricht. (Programmgesteuerte Aufrufe für das Zertifikat umfassen CryptAcquireContext, CryptSetProvParam mit der PIN, CryptgetUserKey und CryptGetKeyParam.) Nachdem der temporäre Schlüssel abgerufen wurde, entschlüsselt der Kerberos-SSP den Sitzungsschlüssel.

15. Der Client überprüft die Antwort vom KDC (Zeit, Pfad und Sperrungsstatus). Sie überprüft zunächst die Signatur des KDC durch die Erstellung eines Zertifizierungspfads vom KDC-Zertifikat zu einer vertrauenswürdigen Stammzertifizierungsstelle und verwendet dann den öffentlichen Schlüssel des KDC, um die Antwort Signatur zu überprüfen.
16. Nachdem nun eine TGT abgerufen wurde, erhält der Client ein Service Ticket, das zum Anmelden beim lokalen Computer verwendet wird.
17. Mit Erfolg speichert LSA die Tickets und gibt eine Erfolgsmeldung an LsaLogonUser zurück. Nachdem diese Erfolgsmeldung ausgegeben wurde, wird das Benutzerprofil für das Gerät ausgewählt und eingestellt, die Gruppenrichtlinienaktualisierung instanziiert und andere Aktionen ausgeführt.
18. Nachdem das Benutzerprofil geladen wurde, erkennt der Certification Propagation Service (CertPropSvc) dieses Ereignis, liest die Zertifikate von der Smartcard (einschließlich der Stammzertifikate) und füllt Sie dann im Zertifikatspeicher des Benutzers (myStore) auf.
19. CSP für die Smartcard-Ressourcen-Manager-Kommunikation erfolgt im LRPC-Kanal.
20. Bei erfolgreicher Authentifizierung werden Zertifikate vom Zertifikat propagierdienst (Certificate Propagation Service, CertPropSvc) asynchron an den Speicher des Benutzers weitergegeben.
21. Wenn die Karte entfernt wird, werden Zertifikate im temporären sicheren Cachespeicher entfernt. Die Zertifikate sind nicht mehr für die Anmeldung verfügbar, verbleiben aber im Zertifikatspeicher des Benutzers.

**** Hinweis eine SID wird für jeden Benutzer oder jede Gruppe erstellt, wenn ein Benutzerkonto oder ein Gruppenkonto in der lokalen Sicherheitskontendatenbank oder in AD DS erstellt wird. Die SID ändert sich nie, auch wenn das Benutzer-oder Gruppenkonto umbenannt wurde.

Weitere Informationen zum Kerberos-Protokoll finden Sie unter [Microsoft Kerberos](#).

Standardmäßig wird vom KDC überprüft, ob das Zertifikat des Clients das EKU-szOID _KP_SMARTCARD_LOGON der Smartcard-Clientauthentifizierung enthält. Wenn die Gruppenrichtlinieneinstellung **Zertifikate ohne erweiterte Schlüssel Verwendungs Zertifikat zulassen** aktiviert ist, kann das KDC die SC-Logon-EKU jedoch nicht anfordern. Die SC-Logon-EKU ist für Kontozuordnungen, die auf dem öffentlichen Schlüssel basieren, nicht erforderlich.

KDC-Zertifikat

Active Directory-Zertifikatdienste bietet drei Arten von Zertifikatvorlagen:

- Domänencontroller
- Domänencontrollerauthentifizierung
- Kerberos-Authentifizierung

Je nach Konfiguration des Domänencontrollers wird einer dieser Zertifikattypen als Teil des AS_REP-Pakets gesendet.

Anforderungen und Zuordnungen für Client Zertifikate

Die Zertifikatanforderungen sind nach Versionen des Windows-Betriebssystems aufgeführt. Zertifikatzuordnung beschreibt, wie Informationen aus dem Zertifikat dem Benutzerkonto zugeordnet werden.

Zertifikatanforderungen

Das Smartcard-Zertifikat hat bestimmte Formatanforderungen, wenn es mit Windows XP und älteren Betriebssystemen verwendet wird. Sie können festlegen, dass ein beliebiges Zertifikat für den Smartcard-Anmeldeinformationsanbieter sichtbar sein soll.

KOMPONENTE	VORAUSSETZUNGEN FÜR WINDOWS 8,1, WINDOWS 8, WINDOWS 7, WINDOWS VISTA UND WINDOWS 10	VORAUSSETZUNGEN FÜR WINDOWS XP
Speicherort des CRL-Verteilungspunkts	Nicht erforderlich	Der Speicherort muss angegeben werden, Online und verfügbar sein, beispielsweise: \ [1] CRL-Verteilungspunkt Name des Verteilungspunkts: Vollständiger Name: URL = http://server1.contoso.com/CertEnroll/caname.crl
Schlüsselverwendung	Digitale Signatur	Digitale Signatur
Grundlegende Einschränkungen	Nicht erforderlich	\ [Subject Type = End Entity; Path length Constraint = None] (optional)
Erweiterte Schlüsselverwendung (EKU)	Die Smartcard-Anmeldeobjekt-ID ist nicht erforderlich. **** Hinweis wenn eine EKU vorhanden ist, muss Sie die Registrierungs-EKU für Smartcards enthalten. Zertifikate ohne EKU können für die Anmeldung verwendet werden.	-Client Authentifizierung (1.3.6.1.5.5.7.3.2) Die Client Authentifizierungs Objekt-ID ist nur erforderlich, wenn ein Zertifikat für die SSL-Authentifizierung verwendet wird. -Smartcard-Anmeldung (1.3.6.1.4.1.311.20.2.2)
Alternativer Antragstellername	Für die Smartcard-Anmeldung ist keine e-Mail-ID erforderlich.	Anderer Name: Principal Name = (UPN), beispielsweise: UPN=user1@contoso.com Der UPN OtherName-Objektbezeichner lautet 1.3.6.1.4.1.311.20.2.3. Der UPN OtherName-Wert muss eine ASN1-codierte UTF8-Zeichenfolge sein.
Antragsteller	Nicht erforderlich	Distinguished Name des Benutzers. Dieses Feld ist eine obligatorische Erweiterung, aber die Auffüllung dieses Felds ist optional.
Schlüsselaustausch (at _KEYEXCHANGE Feld)	Nicht erforderlich für Anmelde Zertifikate für Smartcards, wenn eine Gruppenrichtlinieneinstellung aktiviert ist. (Standardmäßig sind die Gruppenrichtlinieneinstellungen nicht aktiviert.)	Nicht erforderlich
CRL	Nicht erforderlich	Nicht erforderlich

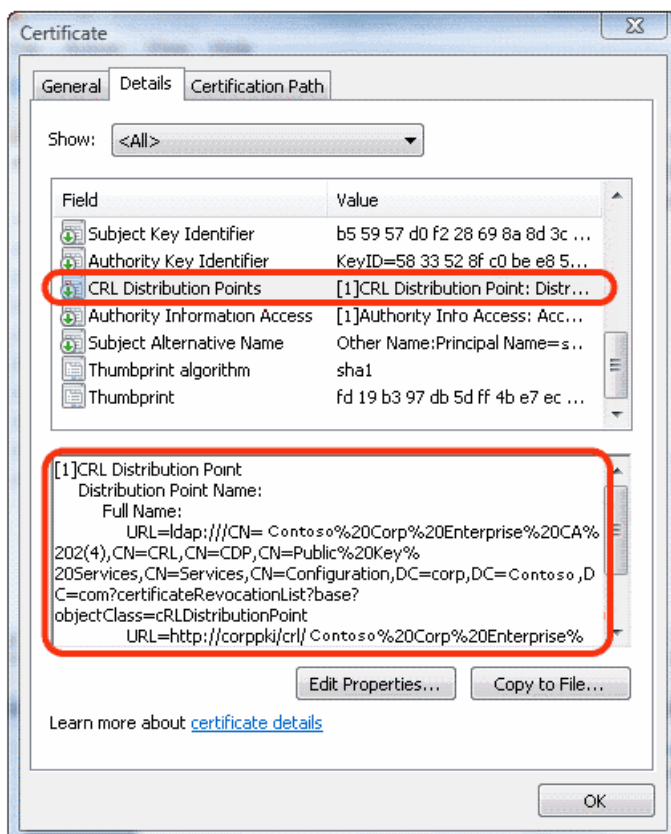
KOMPONENTE	VORAUSSETZUNGEN FÜR WINDOWS 8,1, WINDOWS 8, WINDOWS 7, WINDOWS VISTA UND WINDOWS 10	VORAUSSETZUNGEN FÜR WINDOWS XP
UPN	Nicht erforderlich	Nicht erforderlich
Anmerkungen	Sie können festlegen, dass ein beliebiges Zertifikat für den Smartcard-Anmeldeinformationsanbieter sichtbar sein soll.	Es gibt zwei vordefinierte Typen privater Schlüssel. Diese Tasten sind nur Signatur (at _SIGNATURE) und Schlüsselaustausch (at _KEYEXCHANGE). Für Smartcard-Anmelde Zertifikate muss ein Schlüsselaustausch (at _KEYEXCHANGE)-privater Schlüsseltyp vorhanden sein.

Client Zertifikatzuordnungen

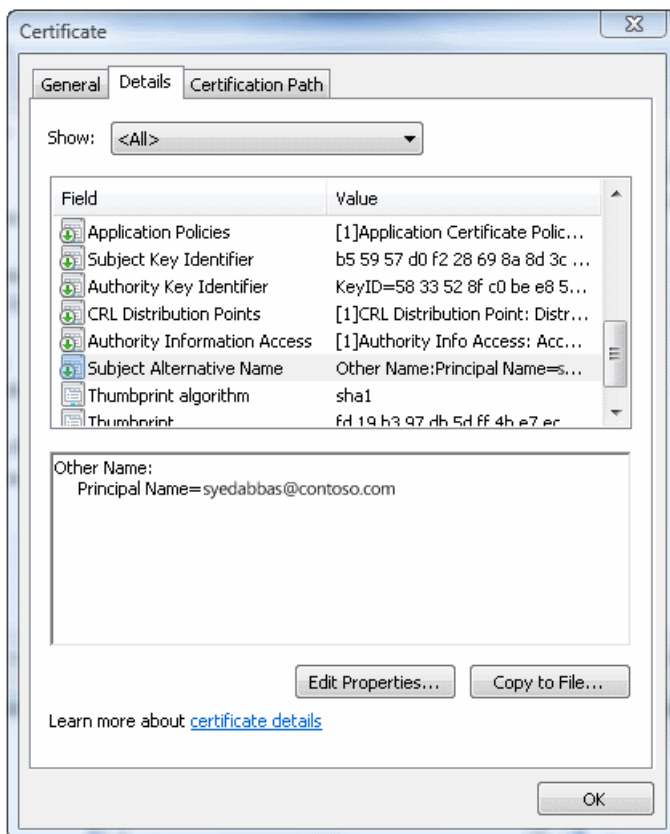
Die Zertifikatzuordnung basiert auf dem UPN, der im Feld subjectAltName (San) des Zertifikats enthalten ist. Client Zertifikate, die keine Informationen im San-Feld enthalten, werden ebenfalls unterstützt.

SSL/TLS kann Zertifikate zuordnen, die kein San aufweisen, und die Zuordnung erfolgt mithilfe der AltSecID-Attribute in Clientkonten. Das <x509-AltSecID, das von der SSL/TLS-Clientauthentifizierung verwendet wird, hat den <Betreffnamen>"X509: I>"< <Ausstellernamen>"S>". Der * <Ausstellernamen> * und * <der Name> des Antragstellers* werden aus dem Clientzertifikat übernommen, wobei "\r" und "\n" durch ";" ersetzt werden.

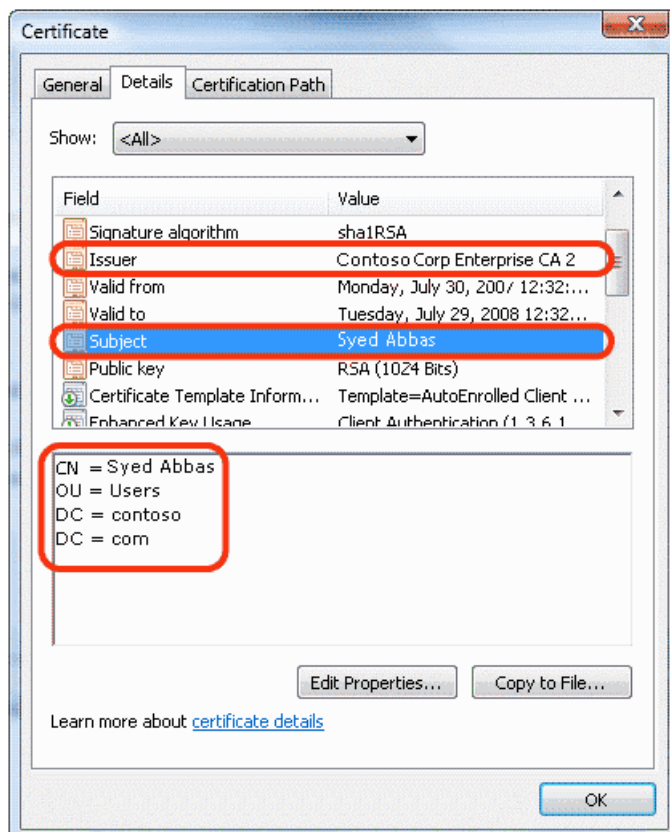
Verteilungspunkte für Zertifikatssperlisten



UPN im Feld "alternativer Antragsteller Name"

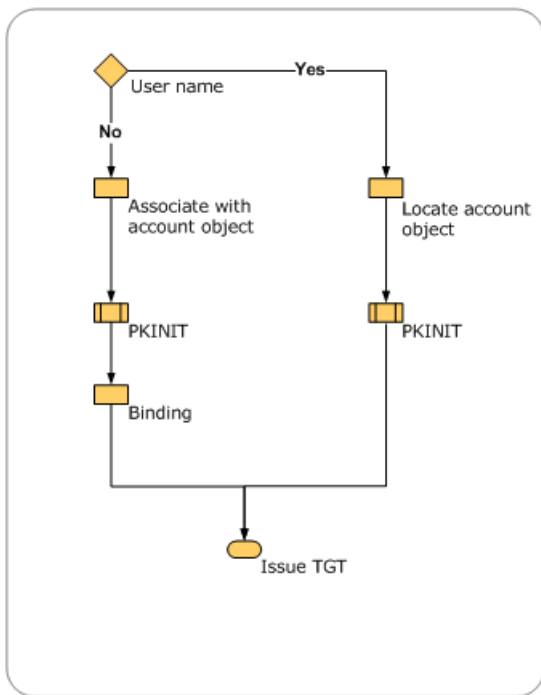


Subject und Issuer-Felder



Diese Kontozuordnung wird neben sechs anderen Zuordnungsmethoden vom KDC unterstützt. Die folgende Abbildung zeigt einen Fluss der Benutzerkonto-Zuordnungslogik, die vom KDC verwendet wird.

Ablauf der Zertifikat Verarbeitung auf hoher Ebene für die Anmeldung



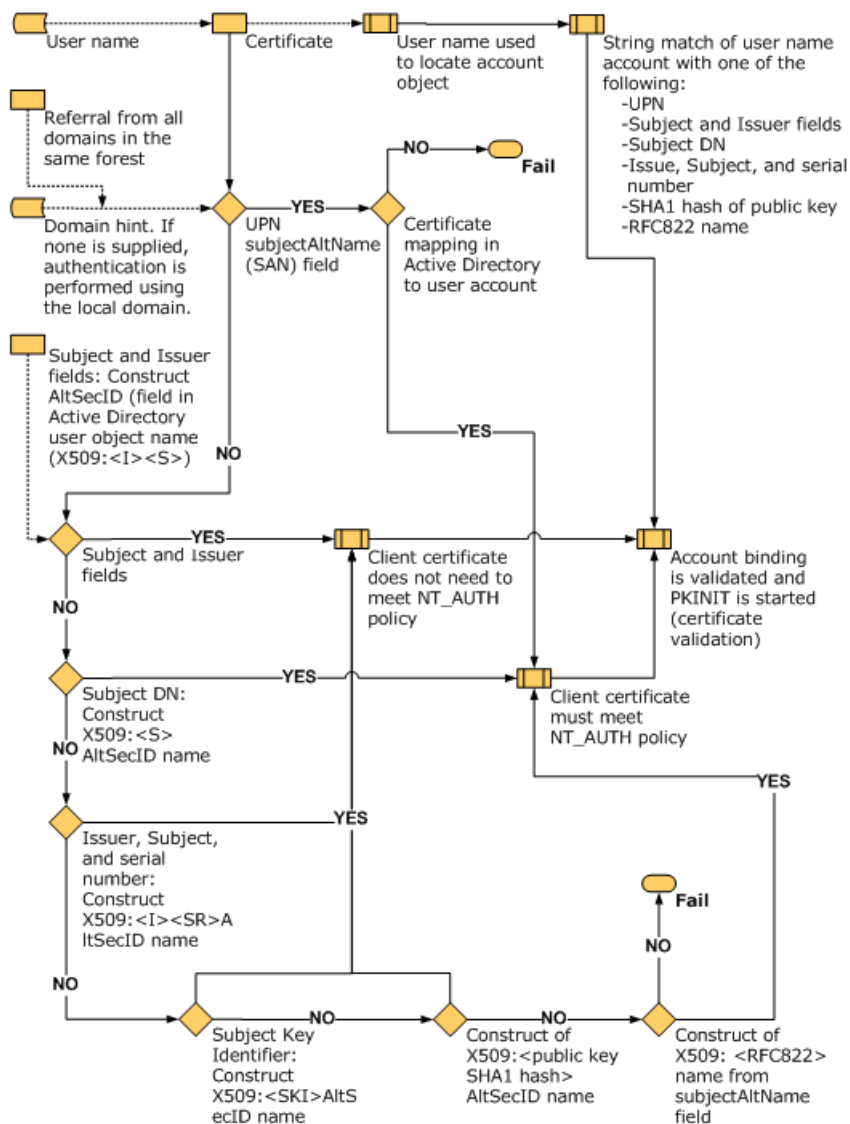
Das Certificate-Objekt wird analysiert, um nach Inhalten zu suchen, um eine Benutzerkonten Zuordnung durchzuführen.

- Wenn ein Benutzername mit dem Zertifikat bereitgestellt wird, wird der Benutzername verwendet, um das Kontoobjekt zu finden. Dieser Vorgang ist am schnellsten, da der Zeichenfolgenabgleich erfolgt.
- Wenn nur das Certificate-Objekt bereitgestellt wird, erfolgt eine Reihe von Vorgängen, um nach dem Benutzernamen zu suchen, um den Benutzernamen einem Kontoobjekt zuzuordnen.
- Wenn keine Domäneninformationen zur Authentifizierung zur Verfügung stehen, wird standardmäßig die lokale Domäne verwendet. Wenn eine andere Domäne für die Suche verwendet werden soll, sollte ein Domänennamen Hinweis bereitgestellt werden, um die Zuordnung und Bindung durchzuführen.

Die Zuordnung auf der Grundlage generischer Attribute ist nicht möglich, da keine generische API zum Abrufen von Attributen aus einem Zertifikat vorhanden ist. Zurzeit beendet die erste Methode, die ein Konto sucht, die Suche erfolgreich. Ein Konfigurationsfehler tritt jedoch auf, wenn zwei Methoden dasselbe Zertifikat verschiedenen Benutzerkonten zuordnen, wenn der Client den Clientnamen nicht über die Zuordnungs Hinweise bereitstellt.

Die folgende Abbildung zeigt den Vorgang der Zuordnung von Benutzerkonten für die Anmeldung im Verzeichnis, indem verschiedene Einträge im Zertifikat angezeigt werden.

Zertifikat Verarbeitungslogik



Die Richtlinie "NT _AUTH" wird am besten im Abschnitt "CERT _CHAIN _POLICY _NT _AUTH Parameter" der CertVerifyCertificateChainPolicy-Funktion beschrieben. Weitere Informationen finden Sie unter [CertVerifyCertificateChainPolicy](#).

Smartcard-Anmeldung für einen einzelnen Benutzer mit einem Zertifikat in mehrere Konten

Ein einzelnes Benutzerzertifikat kann mehreren Konten zugeordnet werden. Beispielsweise kann sich ein Benutzer bei einem Benutzerkonto anmelden und sich auch als Domänenadministrator anmelden. Die Zuordnung erfolgt mithilfe der konstruierten AltSecID basierend auf Attributen aus Clientkonten. Informationen dazu, wie diese Zuordnung ausgewertet wird, finden Sie unter [Client Zertifikatanforderungen und-Zuordnungen](#).

*** Hinweis : Da jedes Konto einen anderen Benutzernamen aufweist, empfehlen wir, dass Sie die Gruppenrichtlinieneinstellung *Benutzernamen Hinweis zulassen (X509HintsNeeded - Registrierungsschlüssel) aktivieren, um die optionalen Felder bereitzustellen, mit denen Benutzer ihre Benutzernamen und Domäneninformationen zur Anmeldung eingeben können.**

Basierend auf den Informationen, die im Zertifikat zur Verfügung stehen, sind die Anmeldebedingungen:

1. Wenn im Zertifikat kein UPN vorhanden ist:
 - a. Die Anmeldung kann in der lokalen Gesamtstruktur oder in einer anderen Gesamtstruktur erfolgen, wenn sich ein einzelner Benutzer mit einem Zertifikat bei verschiedenen Konten anmelden muss.

- b. Ein Hinweis muss angegeben werden, wenn die Zuordnung nicht eindeutig ist (Wenn beispielsweise mehrere Benutzer demselben Zertifikat zugeordnet sind).
2. Wenn ein UPN im Zertifikat vorhanden ist:
- a. Das Zertifikat kann nicht mehreren Benutzern in der gleichen Gesamtstruktur zugeordnet werden.
 - b. Das Zertifikat kann mehreren Benutzern in verschiedenen Gesamtstrukturen zugeordnet werden.
Damit sich ein Benutzer bei anderen Gesamtstrukturen anmelden kann, muss ein X509-Hinweis für den Benutzer bereitgestellt werden.

Smartcard-Anmeldung für mehrere Benutzer in einem einzigen Konto

Eine Gruppe von Benutzern meldet sich möglicherweise bei einem einzelnen Konto an (beispielsweise einem Administratorkonto). Für dieses Konto werden Benutzerzertifikate so zugeordnet, dass Sie für die Anmeldung aktiviert sind.

Mehrere unterschiedliche Zertifikate können einem einzelnen Konto zugeordnet werden. Damit dies ordnungsgemäß funktioniert, kann das Zertifikat nicht über UPNs.

Wenn Certificate1 beispielsweise über CN = CNName1, Certificate2 über cn = Benutzer1 verfügt und Certificate3 über CN = User2 verfügt, kann die AltSecID dieser Zertifikate mithilfe der Namen Zuordnung Active Directory-Benutzer und-Computer einem einzelnen Konto zugeordnet werden.

Smartcard-Anmeldung über Gesamtstrukturen hinweg

Damit die Kontozuordnung für Gesamtstrukturen verwendet werden kann, insbesondere in Fällen, in denen nicht genügend Informationen für das Zertifikat verfügbar sind, kann der Benutzer einen Hinweis in Form eines Benutzernamens eingeben, beispielsweise *domain\user*, oder einen vollqualifizierten UPN *wieuser@contoso.com*.

*** Hinweis damit das Hinweisfeld während der Smartcard-Anmeldung angezeigt wird, muss die Gruppenrichtlinieneinstellung *Benutzername Hinweis zulassen (X509HintsNeeded - Registrierungsschlüssel) auf dem Client aktiviert sein.**

OCSP-Unterstützung für PKINIT

Das in RFC 2560 definierte Online Certificate Status Protocol (OCSP) ermöglicht es Anwendungen, rechtzeitig Informationen über den Sperrungsstatus eines Zertifikats zu erhalten. Da OCSP-Antworten klein und gut gebunden sind, möchten abhängige Clients möglicherweise OCSP verwenden, um die Gültigkeit der Zertifikate für Kerberos auf dem KDC zu überprüfen, um die Übertragung großer CRLs zu vermeiden und die Bandbreite in abhängigen Netzwerken zu sparen. Informationen zu CRL-Registrierungsschlüsseln finden Sie unter [Smartcard-Gruppenrichtlinien und Registrierungseinstellungen](#).

Die KDCs in Windows versuchen, OCSP-Antworten abzurufen und bei Verfügbarkeit zu verwenden. Dieses Verhalten kann nicht deaktiviert werden. CryptoAPI für OCSP speichert OCSP-Antworten und den Status der Antworten zwischen. Das KDC unterstützt nur OCSP-Antworten für das Signaturgeber Zertifikat.

Windows-Clientcomputer versuchen, die OCSP-Antworten anzufordern und in der Antwort zu verwenden, wenn Sie verfügbar sind. Dieses Verhalten kann nicht deaktiviert werden.

Smartcard-Stammzertifikat Anforderungen für die Verwendung mit der Domänenanmeldung

Damit die Anmeldung in einer Smartcard-basierten Domäne ausgeführt werden kann, muss das Smartcard-Zertifikat die folgenden Bedingungen erfüllen:

- Das KDC-Stammzertifikat auf der Smartcard muss einen HTTP-CRL-Verteilungspunkt aufweisen, der im Zertifikat aufgeführt ist.
- Für das Smartcard-Anmeldezertifikat muss der http-CRL-Verteilungspunkt im Zertifikat aufgeführt sein.
- Der CRL-Verteilungspunkt muss, falls zutreffend, eine gültige CRL sowie eine Delta-CRL veröffentlichen, auch wenn der CRL-Verteilungspunkt leer ist.
- Das Smartcard-Zertifikat muss eine der folgenden Angaben enthalten:
 - Ein Subject-Feld, das den DNS-Domännennamen im Distinguished Name enthält. Wenn dies nicht der Fall ist, schlägt die Lösung für eine geeignete Domäne fehl, sodass die Remote Desktop Dienste und die Domänenanmeldung bei der Smartcard fehlschlagen.
 - Ein UPN, in dem der Domänenname in die eigentliche Domäne aufgelöst wird. Wenn beispielsweise der Domänenname "Engineering. Corp. contoso" lautet, lautet der UPN username@Engineering.Corp.contoso.com. Wenn ein Teil des Domännennamens ausgelassen wird, kann der Kerberos-Client die entsprechende Domäne nicht finden.

Obwohl die http-CRL-Verteilungspunkte in Windows Server 2008 standardmäßig aktiviert sind, umfassen nachfolgende Versionen des Windows Server-Betriebssystems keine http-CRL-Verteilungspunkte. Gehen Sie wie folgt vor, um die Smartcard-Anmeldung bei einer Domäne in diesen Versionen zu ermöglichen:

1. Aktivieren von http-CRL-Verteilungspunkten auf der Zertifizierungsstelle
2. Starten Sie die Zertifizierungsstelle neu.
3. Stellen Sie das KDC-Zertifikat erneut aus.
4. Das Smartcard-Anmeldezertifikat wird ausgestellt oder erneut ausgestellt.
5. Verteilen Sie das aktualisierte Stammzertifikat an die Smartcard, die Sie für die Domänenanmeldung verwenden möchten.

Die Problemumgehung besteht darin, die Gruppenrichtlinieneinstellung "**Benutzernamen Hinweis zulassen**" (**X509HintsNeeded** -Registrierungsschlüssel) zu aktivieren, die es dem Benutzer ermöglicht, einen Hinweis auf der Benutzeroberfläche für Anmeldeinformationen für die Domäne anzugeben.

Wenn der Clientcomputer nicht der Domäne beigetreten ist oder wenn er einer anderen Domäne beigetreten ist, kann der Clientcomputer die Server Domäne nur auflösen, indem der Distinguished Name auf dem Zertifikat und nicht der UPN betrachtet wird. Damit dieses Szenario funktioniert, erfordert das Zertifikat einen vollständigen Betreff, einschließlich DC =<Domain Controller> Name, für die Domännennamensauflösung.

Zum Bereitstellen von Stammzertifikaten auf einer Smartcard für die derzeit verbundene Domäne können Sie den folgenden Befehl verwenden:

certutil-scroots-Update

Weitere Informationen zu dieser Option für das Befehlszeilentool finden Sie unter [-SCRoots](#).

Weitere Informationen

[Funktionsweise der Smartcardanmeldung in Windows](#)

Smartcard und Remotedesktopdienste

12.09.2019 • 5 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten wird das Verhalten von Remote Desktop Diensten beschrieben, wenn Sie die Smartcard-Anmeldung implementieren.

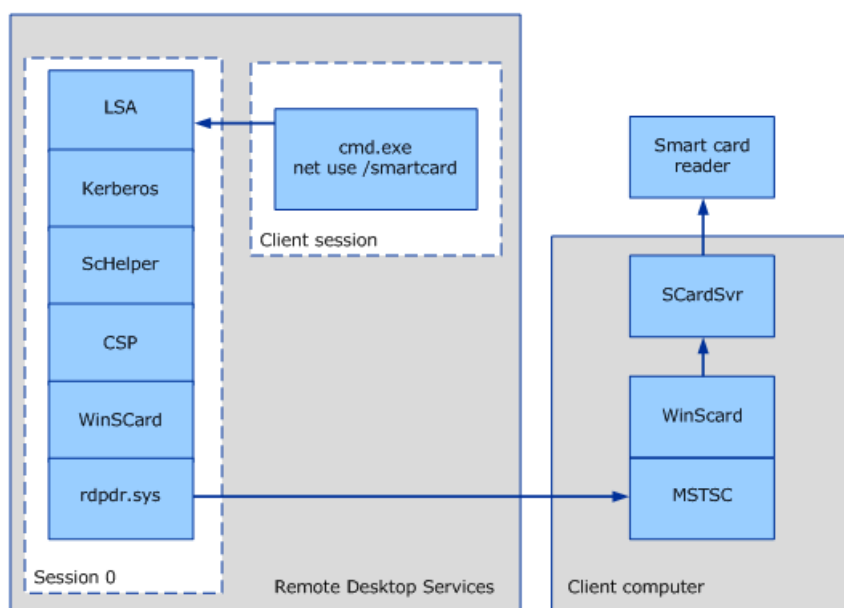
Der Inhalt in diesem Thema bezieht sich auf die Windows-Versionen, die in der Liste "**gilt für**" am Anfang dieses Themas angegeben sind. In diesen Versionen werden die Smartcard-Umleitungs Logik und die **winscard** -API kombiniert, um mehrere umgeleitete Sitzungen in einem einzigen Prozess zu unterstützen.

Um viele Szenarien für Remote Desktop Dienste aktivieren zu können, ist eine Smartcard-Unterstützung erforderlich. Dazu zählen:

- Verwenden der schnellen Benutzerumschaltung oder der Remote Desktop Dienste. Ein Benutzer kann keine umgeleitete Smartcard-basierte Remotedesktopverbindung einrichten. Das bedeutet, dass der Verbindungsversuch beim schnellen Benutzerwechsel oder bei einer Remote Desktop Dienste-Sitzung nicht erfolgreich ist.
- Aktivieren von EFS (Encrypting File System) zum Auffinden des Smartcard-Readers des Benutzers aus dem LSA-Prozess (Local Security Authority) bei der schnellen Benutzerumschaltung oder in einer Remote Desktop Dienste-Sitzung. Wenn EFS nicht in der Lage ist, den Smartcard-Leser oder das Zertifikat zu finden, kann EFS keine Benutzer Dateien entschlüsseln.

Umleitung von Remote Desktop Diensten

In einem Szenario mit Remote Desktop verwendet ein Benutzer einen Remoteserver für die Ausführung von Diensten, und die Smartcard ist lokal auf dem Computer, den der Benutzer verwendet. Bei einem Smartcard-Anmeldeszenario wird der smartcarddienst auf dem Remoteserver an den Smartcard-Leser umgeleitet, der mit dem lokalen Computer verbunden ist, auf dem der Benutzer sich anmelden möchte.



Remote Desktop Umleitung

Hinweise zum Umleitungs Modell:

1. Bei diesem Szenario handelt es sich um eine Remote Anmeldesitzung auf einem Computer mit Remote Desktop Diensten. In der Remotesitzung (mit der Bezeichnung "Client Sitzung") wird der Benutzer **net use/Smartcard**.
2. Pfeile stellen den Fluss der PIN dar, nachdem der Benutzer die PIN an der Eingabeaufforderung eingibt, bis er die Smartcard des Benutzers in einem Smartcard-Leser erreicht, der mit dem RDC-Clientcomputer (Remote Desktop Connection) verbunden ist.
3. Die Authentifizierung wird von der LSA in Sitzung 0 durchgeführt.
4. Die CryptoAPI-Verarbeitung wird im LSA (Lsass.exe) ausgeführt. Dies ist möglich, da der RDP-Redirector (Rdpdr.sys) pro Sitzung und nicht pro Prozesskontext zulässt.
5. Die WinScard- und SCRedir-Komponenten, die separate Module in Betriebssystemen früher als Windows Vista, sind jetzt in einem Modul enthalten. Die SchHelper-Bibliothek ist ein für das Kerberos-protokollspezifischer CryptoAPI-Wrapper.
6. Die Umleitungs Entscheidung erfolgt basierend auf der Sitzung des Threads, der den SCardEstablishContext-Aufruf ausführt, auf Grundlage einer Smartcard-Kontext Basis.
7. Änderungen an der winscard.dll-Implementierung wurden in Windows Vista vorgenommen, um die Smartcard-Umleitung zu verbessern.

Einmaliges anmeldeerlebnis für Remote Desktop-Sitzungs Host Server

Im Rahmen der Common Criteria-Compliance muss der RDC-Client konfigurierbar sein, damit er das Kennwort oder die Smartcard-PIN des Benutzers mithilfe des Anmelde-Managers abrufen und speichern kann. Die Compliance für allgemeine Kriterien setzt voraus, dass Anwendungen keinen direkten Zugriff auf das Kennwort oder die PIN des Benutzers haben.

Common Criteria-Kompatibilität erfordert ausdrücklich, dass das Kennwort oder die PIN die LSA niemals unverschlüsselt belassen. In einem verteilten Szenario sollte das Kennwort oder die PIN zwischen einer vertrauenswürdigen LSA und einer anderen Person Reisen, und Sie kann während der Übertragung nicht entschlüsselt werden.

Wenn für Remote Desktop Dienste-Sitzungen eine Smartcard-aktivierte einmalige Anmeldung (Single Sign-in, SSO) verwendet wird, müssen sich die Benutzer bei jeder neuen Remotedesktopdienste-Sitzung anmelden. Der Benutzer wird jedoch nicht mehrmals zur Eingabe einer PIN aufgefordert, um eine Remote Desktop Dienste-Sitzung einzurichten. Nachdem der Benutzer beispielsweise auf ein Microsoft Word-Dokumentsymbol, das sich auf einem Remotecomputer befindet, doppelklickt, wird der Benutzer aufgefordert, eine PIN einzugeben. Diese PIN wird mithilfe eines sicheren Kanals gesendet, den der Anmelde Informations-SSP eingerichtet hat. Die PIN wird über den sicheren Kanal zurück an den RDC-Client weitergeleitet und an Winlogon gesendet. Der Benutzer erhält keine weiteren Eingabeaufforderungen für die PIN, es sei denn, die PIN ist falsch oder es gibt Fehler mit Smartcards.

Remote Desktop Dienste und Smartcard-Anmeldung

Mithilfe der Remote Desktop Dienste können sich Benutzer mit einer Smartcard anmelden, indem Sie eine PIN auf dem RDC-Clientcomputer eingeben und diese an den Host für Remotedesktopsitzungen-Server senden, ähnlich der Authentifizierung, die auf Benutzername und Kennwort basiert.

Darüber hinaus müssen Gruppenrichtlinieneinstellungen, die für Remote Desktop Dienste spezifisch sind, für die Smartcard-basierte Anmeldung aktiviert werden.

Um die Smartcard-Anmeldung bei einem Host für Remotedesktopsitzungen-Server (RD-Sitzungshost) zu aktivieren, muss das Schlüssel Verteilungs Center-Zertifikat auf dem RDC-Clientcomputer vorhanden sein. Wenn sich der Computer nicht in der gleichen Domäne oder Arbeitsgruppe befindet, kann der folgende Befehl zum Bereitstellen des Zertifikats verwendet werden:

certutil-dspublish NTAAuthCA "DSCDPContainer"

Der *DSCDPContainer* Common Name (CN) ist in der Regel der Name der Zertifizierungsstelle.

Beispiel:

certutil-dspublish NTAAuthCA<certdatei> "CN = NTAAuthCertificates, CN = Public Key Services, CN = Services, CN = Configuration, DC = Engineering, DC = contoso, DC = com"

Informationen zu dieser Option für das Befehlszeilentool finden Sie unter [-dsPublish](#).

Remote Desktop Dienste und Smartcard-Anmeldung über Domänen hinweg

Um den Remotezugriff auf Ressourcen in einem Unternehmen zu aktivieren, muss das Stammzertifikat für die Domäne auf der Smartcard bereitgestellt werden. Führen Sie auf einem Computer, der mit einer Domäne verbunden ist, den folgenden Befehl in der Befehlszeile aus:

certutil-scroots-Update

Informationen zu dieser Option für das Befehlszeilentool finden Sie unter [-SCRoots](#).

Für Remote Desktop Dienste zwischen Domänen muss das KDC-Zertifikat des Servers mit dem Host für Remotedesktopsitzungen auch im NTAUTH-Speicher des Clientcomputers vorhanden sein. Führen Sie den folgenden Befehl in der Befehlszeile aus, um den Store hinzuzufügen:

certutil-addstore-Enterprise-NTAUTH<certdatei>

Dabei <> ist *certdatei* das Stammzertifikat des KDC-Zertifikatausstellers.

Informationen zu dieser Option für das Befehlszeilentool finden Sie unter [-addstore](#).

*** Hinweis Wenn Sie den Anmelde Informations-SSP auf Computern verwenden, auf denen die unterstützten Versionen des Betriebssystems ausgeführt werden, die in der Liste " *gilt für " am Anfang dieses Themas festgelegt sind: so können Sie sich mit einer Smartcard von einem Computer anmelden, der nicht mit einer Domäne verbunden ist, muss die Smartcard die Stammzertifizierung des Domänencontrollers enthalten. Ein sicherer Kanal für die öffentliche Schlüsselinfrastruktur (PKI) kann nicht ohne die Stammzertifizierung des Domänencontrollers eingerichtet werden.**

Die Anmeldung bei Remote Desktop Diensten über eine Domäne funktioniert nur, wenn der UPN im Zertifikat das folgende Formular verwendet: <Client>@<NameDomainDNSName>

Der UPN im Zertifikat muss eine Domäne enthalten, die aufgelöst werden kann. Andernfalls kann das Kerberos-Protokoll nicht ermitteln, welche Domäne kontaktiert werden soll. Sie können dieses Problem beheben, indem Sie Gruppenrichtlinienobjekte-X509-Domänen Hinweise aktivieren. Weitere Informationen zu dieser Einstellung finden Sie unter [Gruppenrichtlinie für Smartcards und Registrierungseinstellungen](#).

Weitere Informationen:

[Funktionsweise der Smartcardanmeldung in Windows](#)

Smartcards für den Windows-Dienst

12.09.2019 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für Entwickler von IT-Experten und Smartcards wird beschrieben, wie der Smart Cards für Windows-Dienst (früher als Smartcard-Ressourcen-Manager bezeichnet) Leser und Anwendungs Interaktionen verwaltet.

Der Smart Cards für Windows-Dienst stellt die grundlegende Infrastruktur für alle anderen Smartcard-Komponenten bereit, während er Smartcard-Leser und Anwendungs Interaktionen auf dem Computer verwaltet. Sie ist vollständig mit den Spezifikationen kompatibel, die von der PC/SC-Arbeitsgruppe festgesetzt werden. Informationen zu diesen Spezifikationen finden Sie auf der [Website für PC/SC-Arbeitsgruppen Spezifikationen](#).

Der Smart Cards für Windows-Dienst wird im Kontext eines lokalen Diensts ausgeführt und als gemeinsamer Dienst des Diensthospzesses (SVCHOST) implementiert. Der Smart Cards für Windows-Dienst, scardsvr, enthält die folgende Dienstbeschreibung:

```

<serviceData
  dependOnService="PlugPlay"
  description="@%SystemRoot%\System32\SCardSvr.dll, -5"
  displayName="@%SystemRoot%\System32\SCardSvr.dll, -1"
  errorControl="normal"
  group="SmartCardGroup"
  imagePath="%SystemRoot%\system32\svchost.exe -k LocalServiceAndNoImpersonation"
  name="SCardSvr"
  objectName="NT AUTHORITY\LocalService"
  requiredPrivileges="SeCreateGlobalPrivilege,SeChangeNotifyPrivilege"
  sidType="unrestricted"
  start="demand"
  type="win32ShareProcess"
  >
<failureActions resetPeriod="900">
  <actions>
    <action
      delay="120000"
      type="restartService"
    />
    <action
      delay="300000"
      type="restartService"
    />
    <action
      delay="0"
      type="none"
    />
  </actions>
</failureActions>
<securityDescriptor name="ServiceXSecurity"/>
</serviceData>

<registryKeys buildFilter="">
  <registryKey keyName="HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SCardSvr\Parameters">
    <registryValue
      name="ServiceDll"
      value="%SystemRoot%\System32\SCardSvr.dll"
      valueType="REG_EXPAND_SZ"
    />
    <registryValue
      name="ServiceMain"
      value="CalaisMain"
      valueType="REG_SZ"
    />
    <registryValue
      name="ServiceDllUnloadOnStop"
      value="1"
      valueType="REG_DWORD"
    />
  </registryKey>
</registryKeys>

```

*** Hinweis damit winscard.dll als das richtige Klasseninstallationsprogramm aufgerufen wird, muss die INF-Datei für einen Smartcard-Reader für *Class -und ClassGUID Folgendes angeben:**

```
Class=SmartCardReader
```

```
ClassGuid={50DD5230-BA8A-11D1-BF5D-0000F805F530}
```

Standardmäßig ist der Dienst für den manuellen Modus konfiguriert. Entwickler von Smartcard-Lese Treibern müssen ihre INFs so konfigurieren, dass Sie den Dienst automatisch starten, und winscard.dll-Dateien einen vordefinierten Einstiegspunkt aufrufen, um den Dienst während der Installation zu starten. Der Einstiegspunkt wird als Teil der **SmartCardReader** -Klasse definiert und nicht direkt aufgerufen. Wenn ein Gerät sich selbst als Teil dieser Klasse ankündigt, wird der Einstiegspunkt automatisch aufgerufen, um den Dienst zu starten, wenn das

Gerät eingefügt wird. Durch die Verwendung dieser Methode wird sichergestellt, dass der Dienst bei Bedarf aktiviert wird, er ist aber auch für Benutzer deaktiviert, die keine Smartcards verwenden.

Wenn der Dienst gestartet wird, führt er mehrere Funktionen aus:

1. Sie registriert sich selbst für Dienst Benachrichtigungen.
2. Sie registriert sich selbst für Plug & Play-Benachrichtigungen (PNP) im Zusammenhang mit dem Entfernen und Hinzufügen von Geräten.
3. Er initialisiert seinen Datencache und ein globales Ereignis, das signalisiert, dass der Dienst gestartet wurde.

Hinweis für Smartcard-Implementierungen sollten Sie die gesamte Kommunikation unter Windows-Betriebssystemen mit Smartcard-Lesern über den Smartcards für Windows-Dienst senden. Dadurch wird eine Schnittstelle zum nachvollziehen, auswählen und kommunizieren mit allen Treibern bereitgestellt, die Mitglieder der Smartcard-Lesegerät-Gerätegruppe deklarieren.

Der Smart Cards für Windows-Dienst kategorisiert jeden Smartcard-Leser Steckplatz als eindeutigen Leser, und jeder Steckplatz wird unabhängig von den physikalischen Eigenschaften des Geräts ebenfalls separat verwaltet. Der Smart Cards für Windows-Dienst behandelt die folgenden Aktionen auf höherer Ebene:

- Geräte Einführung
- Reader-Initialisierung
- Benachrichtigen von Kunden über neue Leser
- Serialisieren des Zugriffs auf Leser
- Zugriff auf Smartcards
- Tunneln von Reader-spezifischen Befehlen

Weitere Informationen:

[Funktionsweise der Smartcardanmeldung in Windows](#)

Zertifikatverteilungsdienst

12.09.2019 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

Dieses Thema für IT-Experten beschreibt den Certificate Propagation Service (CertPropSvc), der in der Smartcard-Implementierung verwendet wird.

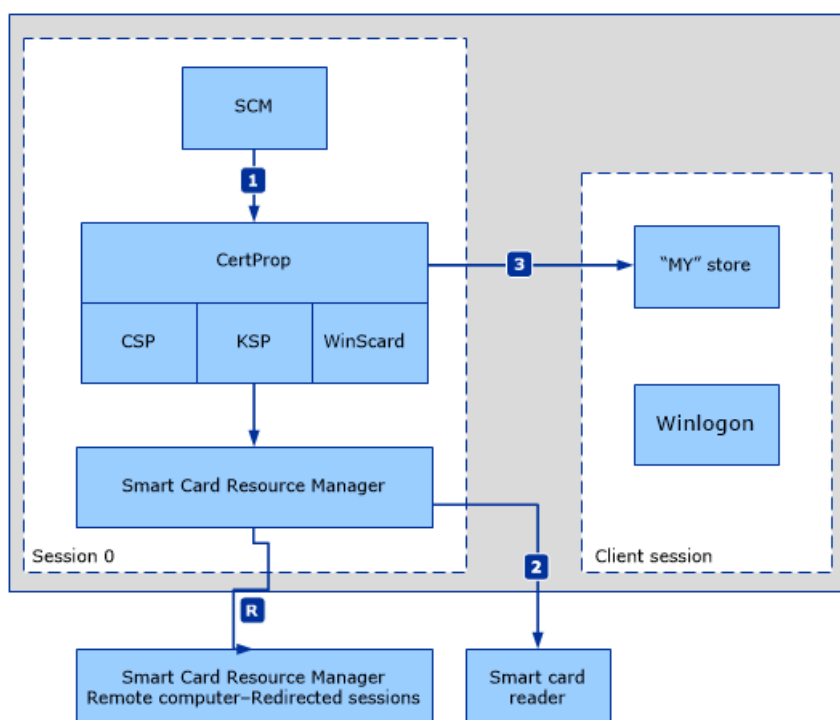
Der Zertifikat Propagations Dienst wird aktiviert, wenn ein angemeldeter Benutzer eine Smartcard in einen Leser einfügt, der an den Computer angefügt ist. Diese Aktion bewirkt, dass das Zertifikat von der Smartcard gelesen wird. Die Zertifikate werden dann dem persönlichen Store des Benutzers hinzugefügt. Dienstaktionen für die Zertifikat Propagierung werden mithilfe von Gruppenrichtlinien gesteuert. Weitere Informationen finden Sie unter [Gruppenrichtlinie für Smartcards und Registrierungseinstellungen](#).

**** Hinweis der Zertifikat Propagations Dienst muss ausgeführt werden, damit die Smartcard-Plug & Play-Funktion funktioniert.

Die folgende Abbildung zeigt den Fluss des Zertifikats Propagations Diensts. Die Aktion beginnt, wenn ein angemeldeter Benutzer eine Smartcard einfügt.

1. Der Pfeil mit der Bezeichnung **1** gibt an, dass der Dienststeuerungs-Manager (SCM) den Certificate Propagation Service (CertPropSvc) benachrichtigt, wenn sich ein Benutzer anmeldet, und CertPropSvc beginnt, die Smartcards in der Benutzersitzung zu überwachen.
2. Der Pfeil mit der Bezeichnung **R** steht für die Möglichkeit einer Remotesitzung und die Verwendung der Smartcard-Umleitung.
3. Der Pfeil mit der Bezeichnung **2** gibt die Zertifizierung für den Leser an.
4. Der Pfeil mit der Bezeichnung **3** gibt den Zugriff auf den Zertifikatspeicher während der Clientsitzung an.

Zertifikat Propagations Dienst



1. Ein angemeldeter Benutzer fügt eine Smartcard ein.
2. CertPropSvc wird benachrichtigt, dass eine Smartcard eingefügt wurde.
3. CertPropSvc liest alle Zertifikate von allen eingefügten Smartcards. Die Zertifikate werden in den persönlichen Zertifikatspeicher des Benutzers geschrieben.

**** Hinweis der Zertifikat Propagations Dienst wird als Remote Desktop Dienste-Abhängigkeit gestartet.

Zu den Eigenschaften des Zertifikats propagierten Diensts gehören:

- CERT_STORE_ADD_REPLACE_EXISTING_INHERIT_PROPERTIES fügt dem persönlichen Speicher eines Benutzers Zertifikate hinzu.
- Wenn das Zertifikat über die CERT_ENROLLMENT_PROP_ID-Eigenschaft verfügt (wie von Wincrypt. h definiert), werden leere Anforderungen gefiltert und im Anforderungs Speicher des aktuellen Benutzers platziert, aber nicht an den privaten Speicher des Benutzers weitergegeben.
- Der Dienst gibt keine Computerzertifikate an den privaten Speicher eines Benutzers weiter, oder es werden Benutzerzertifikate an einen Computerspeicher weitergegeben.
- Der Dienst propagiert Zertifikate entsprechend den festgelegten Gruppenrichtlinienoptionen, die Folgendes umfassen können:
 - **Aktivieren der Zertifikat Propagierung von der Smartcard** gibt an, ob das Zertifikat eines Benutzers weitergegeben werden soll.
 - **Aktivieren der Stammzertifikat Propagierung von Smartcard** gibt an, ob Stammzertifikate propagiert werden sollen.
 - **Konfigurieren der Stammzertifikat Bereinigung** gibt an, wie Stammzertifikate entfernt werden.

Stammzertifikat-Propagations Dienst

Die Stammzertifikat Propagierung ist für die folgenden Smartcard-Bereitstellungsszenarien verantwortlich, wenn noch keine PKI-Vertrauensstellung (Public Key Infrastructure) eingerichtet wurde:

- Beitreten zur Domäne
- Remotezugriff auf ein Netzwerk

In beiden Fällen ist der Computer nicht mit einer Domäne verbunden, und daher wird die Vertrauensstellung nicht von der Gruppenrichtlinie verwaltet. Das Ziel ist jedoch die Authentifizierung bei einem Remoteserver wie dem Domänencontroller. Die Stammzertifikat Propagierung bietet die Möglichkeit, die Smartcard zum Einbeziehen der fehlenden Vertrauenskette zu verwenden.

Wenn die Smartcard eingefügt wird, gibt der Zertifikat Verteilungsdienst alle Stammzertifikate auf der Karte an die Zertifikatspeicher der vertrauenswürdigen Smartcard-Stammcomputer weiter. Dieser Prozess richtet eine Vertrauensstellung mit den Enterprise-Ressourcen ein. Sie können auch eine nachfolgende Bereinigungsaktion verwenden, wenn die Smartcard des Benutzers aus dem Reader entfernt wird oder wenn sich der Benutzer abmeldet. Dies kann mit Gruppenrichtlinien konfiguriert werden. Weitere Informationen finden Sie unter [Gruppenrichtlinie für Smartcards und Registrierungseinstellungen](#).

Weitere Informationen zu den Anforderungen für Stammzertifikate finden Sie unter [Anforderungen für Smartcard-Stammzertifikate für die Verwendung mit der Domänenanmeldung](#).

Weitere Informationen:

Dienst „Richtlinie zum Entfernen der Smartcard“

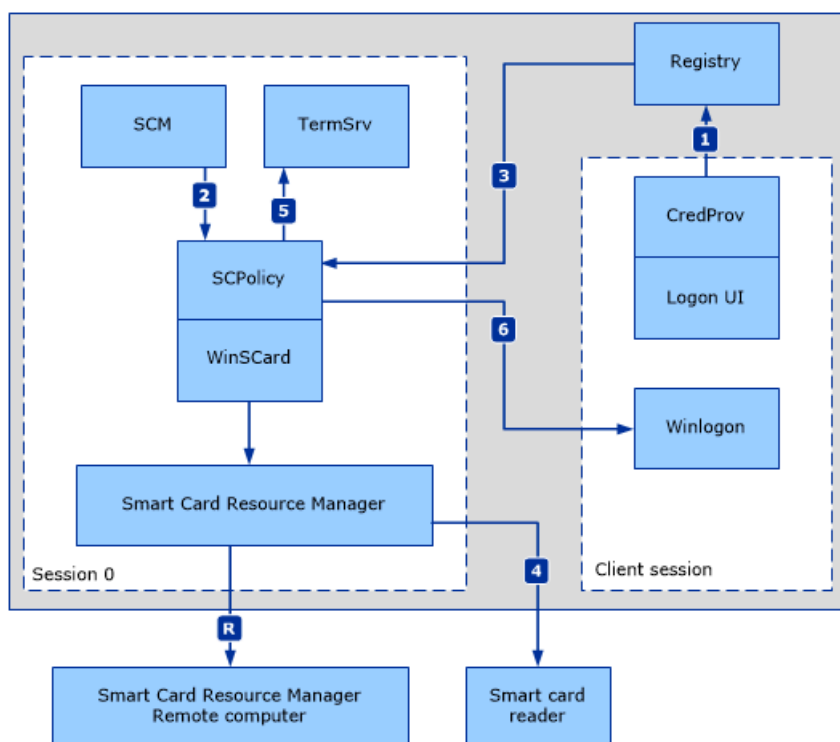
12.09.2019 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten wird die Rolle des Richtlinien-Deinstallations Richtlinien Diensts (ScPolicySvc) in der Smartcard-Implementierung beschrieben.

Der Richtlinien Dienst für die Smartcard-Entfernung gilt, wenn sich ein Benutzer mit einer Smartcard angemeldet hat und diese Smartcard anschließend aus dem Reader entfernt. Die Aktion, die ausgeführt wird, wenn die Smartcard entfernt wird, wird durch die Gruppenrichtlinieneinstellungen gesteuert. Weitere Informationen finden Sie unter [Gruppenrichtlinie für Smartcards und Registrierungseinstellungen](#).

Richtlinien-Service für die Smartcard-Entfernung



Die Zahlen in der vorherigen Abbildung stellen die folgenden Aktionen dar:

1. Winlogon ist nicht direkt an der Überwachung von Smartcard-Entfernungs Ereignissen beteiligt. Die Abfolge von Schritten, die beim Entfernen einer Smartcard involviert sind, beginnt mit dem Smartcard-Anmeldeinformationsanbieter im Anmelde UI-Prozess. Wenn sich ein Benutzer erfolgreich mit einer Smartcard anmeldet, erfasst der Smartcard-Anmeldeinformationsanbieter den Leser Namen. Diese Informationen werden dann in der Registrierung mit der Sitzungs-ID gespeichert, in der die Anmeldung initiiert wurde.
2. Der Smartcard-Ressourcen-Manager-Dienst benachrichtigt den Richt Liniendienst für die Smartcard-Entfernung, dass eine Anmeldung aufgetreten ist.
3. ScPolicySvc Ruft die Smartcard-Informationen ab, die der Smartcard-Anmeldeinformationsanbieter in der Registrierung gespeichert hat. Dieser Anruf wird umgeleitet, wenn sich der Benutzer in einer Remotesitzung befindet. Wenn die Smartcard entfernt wird, wird ScPolicySvc benachrichtigt.
4. ScPolicySvc ruft Remote Desktop Dienste auf, um die entsprechende Aktion auszuführen, wenn sich die Anforderung zum Abmelden des Benutzers oder zum Trennen der Sitzung des Benutzers eignet, was zu

einem Datenverlust führen kann. Wenn die Einstellung so konfiguriert ist, dass der Computer gesperrt wird, wenn die Smartcard entfernt wird, sendet ScPolicySvc eine Nachricht an Winlogon, um den Computer zu sperren.

Weitere Informationen:

[Funktionsweise der Smartcardanmeldung in Windows](#)

Tools und Einstellungen für Smartcards

12.09.2019 • 2 minutes to read

Gilt für: Windows 10, Windows Server 2016

Dieses Thema enthält Links zu Informationen zum Debuggen von Smartcards, zu Einstellungen und Ereignissen für den Entwickler von IT-Experten und Smartcards.

Dieser Abschnitt der technischen Referenz für Smartcards enthält Informationen zu folgenden Themen:

- [Informationen zum Debuggen von Smartcards](#): erfahren Sie mehr über Tools und Dienste in unterstützten Windows-Versionen, um Zertifikatprobleme zu identifizieren.
- [Gruppenrichtlinien und Registrierungseinstellungen für Smartcards](#): erfahren Sie mehr über Smartcard-bezogene Gruppenrichtlinieneinstellungen und Registrierungsschlüssel, die pro Computer festgelegt werden können, einschließlich der Vorgehensweise zum Bearbeiten und Anwenden von Gruppenrichtlinieneinstellungen auf lokale oder Domänencomputer.
- [Smartcard-Ereignisse](#): erfahren Sie mehr zu Ereignissen, die zum Verwalten von Smartcards in einer Organisation verwendet werden können, einschließlich der Überwachung der Installation, Verwendung und Fehler.

Weitere Informationen:

[Technische Referenz für Smartcards](#)

Smartcards-Debuginformationen

12.09.2019 • 6 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema werden die Tools und Dienste erläutert, mit denen Smartcard-entwicklerzertifikat Probleme bei der Bereitstellung von Smartcards identifizieren können.

Das Debuggen und Nachverfolgen von Smartcard-Problemen erfordert eine Vielzahl von Tools und Ansätzen. Die folgenden Abschnitte enthalten Anleitungen zu Tools und Methoden, die Sie verwenden können.

- [Certutil](#)
- [Debuggen und Ablaufverfolgung mit WPP](#)
- [Kerberos-Protokoll, KDC-und NTLM-Debugging und-Ablaufverfolgung](#)
- [Smartcard-Service](#)
- [Smartcard-Leser](#)
- [CryptoAPI 2,0-Diagnose](#)

Certutil

Eine vollständige Beschreibung von certutil, einschließlich Beispielen, die zeigen, wie es zu verwenden ist, finden Sie unter [certutil \ \[W2012 \]](#).

Auf der Smartcard verfügbare Listen Zertifikate

Wenn Sie auf der Smartcard Verfügbare Zertifikate auflisten möchten, geben Sie certutil-scinfo.

**** Hinweis die Eingabe einer PIN ist für diesen Vorgang nicht erforderlich. Sie können ESC drücken, wenn Sie aufgefordert werden, eine PIN einzugeben.

Löschen von Zertifikaten auf der Smartcard

Jedes Zertifikat ist in einem Container eingeschlossen. Wenn Sie ein Zertifikat auf der Smartcard löschen, löschen Sie den Container für das Zertifikat.

Um den Container Wert zu finden, geben Sie certutil-scinfo.

Wenn Sie einen Container löschen möchten, geben Sie **certutil-delkey-CSP "Microsoft Base Smart Card Crypto Provider" <"containerwert">** ein.

Debuggen und Ablaufverfolgung mit WPP

Windows-Software-Ablauf Verfolgungs Präprozessor (WPP) vereinfacht das Nachverfolgen des Vorgangs des Ablaufverfolgungsanbieters und stellt einen Mechanismus bereit, mit dem der Ablaufverfolgungsanbieter Echt Zeit binäre Nachrichten protokollieren kann. Protokollierte Nachrichten können anschließend in eine menschlich lesbare Spur des Vorgangs des Ablaufverfolgungsanbieters konvertiert werden. Weitere Informationen zu WPP finden Sie unter [Diagnose mit WPP – dem NDIS-Blog](#).

Aktivieren der Ablaufverfolgung

Verwenden Sie in WPP einen der folgenden Befehle, um die Ablaufverfolgung zu aktivieren:

- **tracelog.exe-KD-RT-Start** << ** > < ** > ** <> ** ***** ** FriendlyName-GUID \ # GUID-f. \ \ LogFileName. ETL-Flags Flags-Ft 1>
- **logman Start** < * ** > < > > < ** ***** ** *FriendlyName-ETS-p {GUID}-Flags **-Ft 1-RT-o. \ \ LogFileName> *ETL-Modus 0x00080000 **

Sie können die Parameter in der folgenden Tabelle verwenden.

ANZEIGENAME	GUID	FLAGS
scardsvr	13038e47-ffec-425d-bc69-5707708075fe	0xFFFF
winscard	3fce7c5f-fb3b-4bce-a9d8-55cc0ce1cf01	0xFFFF
basecsp	133a980d-035d-4e2d-b250-94577ad8fced	0x7
scksp	133a980d-035d-4e2d-b250-94577ad8fced	0x7
msclmd	fb36caf4-582b-4604-8841-9263574c4f2c	0x7
credprov	dba0e0e0-505a-4ab6-aa3f-22f6f743b480	0xFFFF
certprop	30eae751-411f-414c-988b-a8bfa8913f49	0xFFFF
scfilter	eed7f3c9-62ba-400e-a001-658869df9a91	0xFFFF
wudfusbccid	a3c09ba3-2f62-4be5-a50f-8278a646ac9d	0xFFFF

Beispiele

So aktivieren Sie die Ablaufverfolgung für den scardsvr-Dienst:

- **tracelog.exe-KD-RT-startscardsvr-GUID \ #13038e47-ffec-425d-bc69-5707708075fe-f. \ \ scardsvr. ETL-flags0xffff-FT1**
- **logmanstartscardsvr-ETS-p {13038e47-ffec-425d-bc69-5707708075fe} 0xFFFF-FT1-RT-o. \ \ scardsvr. ETL-mode0x00080000**

So aktivieren Sie die Ablaufverfolgung für scfilter.sys:

tracelog.exe-KD-RT-startscfilter-GUID \ #eed7f3c9 -62ba-400e-A001-658869df9a91-f. \ \ scfilter. ETL-flags0xffff-FT1

Beenden der Ablaufverfolgung

Verwenden Sie mit WPP einen der folgenden Befehle, um die Ablaufverfolgung zu beenden:

- **tracelog.exe – beenden** < FriendlyName >
- **logman-Stopp** FriendlyName -ETS ** <>

Beispiele

So beenden Sie eine Ablaufverfolgung:

- `tracelog. exe – beenden von scardsvr`
- `logman-stop scardsvr-ETS`

Kerberos-Protokoll, KDC-und NTLM-Debugging und-Ablaufverfolgung

Sie können die folgenden Ressourcen verwenden, um mit der Problembehandlung dieser Protokolle und des KDC zu beginnen:

- [Tipps zur Problembehandlung für Kerberos und LDAP](#)
- [Windows Driver Kit \(WDK\) und Debugging Tools für Windows \(WinDbg\)](#) Sie können das Tool "Ablaufverfolgungsprotokoll" in diesem SDK verwenden, um Kerberos-Authentifizierungsfehler zu debuggen.

Wenn Sie mit der Ablaufverfolgung beginnen möchten, können Sie `tracelog` verwenden. Verschiedene Komponenten verwenden unterschiedliche Steuerelement-GUIDs, wie in den folgenden Beispielen erläutert. Weitere Informationen finden Sie unter [tracelog](#).

NTLM

Führen Sie Folgendes in der Befehlszeile aus, um die Ablaufverfolgung für die NTLM-Authentifizierung zu aktivieren:

```
tracelog. exe-KD-RT-Start NTLM-GUID \ #5BBB6C18-AA45-49b1-A15F-085F7ED0AA90-f.\ntlm.ETL-Flags 0x15003-Ft 1
```

Führen Sie in der Befehlszeile Folgendes aus, um die Ablaufverfolgung für die NTLM-Authentifizierung zu beenden:

```
tracelog-Beenden von NTLM
```

Kerberos-Authentifizierung

Führen Sie die folgenden Schritte in der Befehlszeile aus, um die Ablaufverfolgung für die Kerberos-Authentifizierung zu aktivieren:

```
tracelog. exe-KD-RT-Start Kerb-GUID \ #6B510852-3583-4e2d-Affe-A67F9F223438-f.\kerb.ETL-Flags 0x43-Ft 1
```

Führen Sie die folgenden Schritte in der Befehlszeile aus, um die Ablaufverfolgung für die Kerberos-Authentifizierung zu beenden:

```
tracelog. exe – Stopp Kerb
```

KDC

Führen Sie die folgenden Schritte in der Befehlszeile aus, um die Ablaufverfolgung für das Key Distribution Center (KDC) zu aktivieren:

```
tracelog. exe-KD-RT-Start KDC-GUID \ #1BBA8B19-7F31-43c0-9643-6E911F79A06B-f.\kdc.ETL-Flags 0x803-Ft 1
```

Führen Sie in der Befehlszeile Folgendes aus, um die Ablaufverfolgung für das KDC zu beenden:

```
tracelog. exe – KDC beenden
```

Wenn Sie die Ablaufverfolgung von einem Remotecomputer beenden möchten, führen Sie Folgendes in der Befehlszeile aus: `logman. exe-s * <Computername>*`.

*** Hinweis der Standardspeicherort für logman.exe ist %SystemRoot%\System32\ . Verwenden Sie die Option *-s , um einen Computernamen anzugeben.**

Konfigurieren der Ablaufverfolgung mit der Registrierung

Sie können die Ablaufverfolgung auch konfigurieren, indem Sie die in der folgenden Tabelle aufgeführten Kerberos-Registrierungswerte bearbeiten.

ELEMENT	REGISTRIERUNGSSCHLÜSSELEINSTELLUNG
NTLM	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 Wertname: NtLmInfoLevel Werttyp: DWORD Wertdaten: c0015003
Kerberos	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos Wertname: LogToFile Werttyp: DWORD Wertdaten: 00000001 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters Wertname: KerbDebugLevel Werttyp: DWORD Wertdaten: c0000043 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters Wertname: LogToFile Werttyp: DWORD Wertdaten: 00000001
KDC	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc Wertname: KdcDebugLevel Werttyp: DWORD Wertdaten: c0000803

Wenn Sie tracelog verwendet haben, suchen Sie im aktuellen Verzeichnis nach der folgenden Protokolldatei: Kerb. ETL/KDC. ETL/NTLM. ETL.

Wenn Sie die in der vorherigen Tabelle gezeigten Registrierungsschlüsseleinstellungen verwendet haben, suchen Sie in den folgenden Speicherorten nach den generierten Ablaufverfolgungs-Protokolldateien:

- NTLM:%systemroot%\tracing\msv1_0
- Kerberos:%systemroot%\tracing\kerberos
- KDC:%systemroot%\tracing\kdcsvc

Zum Decodieren von Ereignisablauf Verfolgungs Dateien können Sie tracefmt (tracefmt.exe) verwenden. Tracefmt ist ein Befehlszeilentool, mit dem nach Verfolgungs Nachrichten aus einer Ereignisablaufverfolgungsprotokoll Datei (ETL) oder einer echt Zeitablauf Verfolgungs Sitzung formatiert und angezeigt werden. Tracefmt kann die Nachrichten im Eingabeaufforderungsfenster anzeigen oder in einer Textdatei speichern. Sie befindet sich im \tools\tracing-Unterverzeichnis des Windows Driver Kit (WDK). Weitere Informationen finden Sie unter [tracefmt](#).

Smartcard-Service

Der Dienst Smartcard-Ressourcen-Manager wird im Kontext eines lokalen Diensts ausgeführt und als gemeinsamer Dienst des Diensthostprozesses (SVCHOST) implementiert.

So überprüfen Sie, ob der Smart Card-Dienst ausgeführt wird

1. Drücken Sie STRG + ALT + ENTF, und klicken Sie dann auf **Task-Manager starten**.
2. Klicken Sie im Dialogfeld **Windows-Task-Manager** auf die Registerkarte **Dienste**.
3. Klicken Sie auf die Spalte **Name**, um die Liste alphabetisch zu sortieren, und geben Sie dann **sein**.
4. Suchen Sie in der Spalte **Name** nach **scardsvr**, und suchen Sie dann in der Spalte **Status** nach, ob der Dienst ausgeführt oder beendet wird.

So starten Sie den Smartcard-Dienst neu

1. Führen Sie an der Eingabeaufforderung als Administrator aus.
2. Wenn das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, vergewissern Sie sich, dass die angezeigte Aktion Ihren Vorstellungen entspricht, und klicken Sie dann auf **Ja**.
3. Geben Sie an der Eingabeaufforderung **net stop scardsvr** ein.
4. Geben Sie an der Eingabeaufforderung **net Start scardsvr**.

Sie können an der Eingabeaufforderung den folgenden Befehl verwenden, um zu überprüfen, ob der Dienst ausgeführt wird: **SC QUERYEX scardsvr**.

Im folgenden Beispiel wird die Ausgabe dieses Befehls ausgeführt:

```
SERVICE_NAME: scardsvr
  TYPE       : 20 WIN32_SHARE_PROCESS
  STATE      : 4 RUNNING
              (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
  WIN32_EXIT_CODE : 0 (0x0)
  SERVICE_EXIT_CODE : 0 (0x0)
  CHECKPOINT    : 0x0
  WAIT_HINT    : 0x0
  PID          : 1320
  FLAGS       :
C:\>
```

Smartcard-Leser

Wie bei allen Geräten, die mit einem Computer verbunden sind, kann der Geräte-Manager zum Anzeigen von Eigenschaften und zum Starten des Debug-Vorgangs verwendet werden.

So überprüfen Sie, ob der Smartcard-Leser funktioniert

1. Navigieren Sie zu **Computer**.
2. Klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie unter **Aufgaben** auf **Geräte-Manager**.
4. Erweitern Sie im Geräte-Manager die Option **Smartcard-Leser**, wählen Sie den Namen des Smartcard-Readers aus, den Sie überprüfen möchten, und klicken Sie dann auf **Eigenschaften**.

*** Hinweis wenn der Smartcard-Leser nicht im Geräte-Manager aufgeführt ist, klicken Sie im Menü**
***Aktion auf nach Hardwareänderungen suchen.**

CryptoAPI 2,0-Diagnose

Die CryptoAPI 2,0-Diagnose ist ein Feature, das in Windows-Betriebssystemen zur Unterstützung von CryptoAPI 2,0 zur Verfügung steht. Dieses Feature kann Ihnen bei der Behandlung von Problemen mit der PKI (Public Key Infrastructure) helfen.

Die CryptoAPI 2,0-Diagnose protokolliert Ereignisse im Windows-Ereignisprotokoll, die detaillierte Informationen zur Zertifikatsketten Überprüfung, zu Zertifikatspeicher Vorgängen und zur Signaturüberprüfung enthalten. Diese Informationen machen es einfacher, die Ursachen von Problemen zu erkennen und die für die Diagnose benötigte Zeit zu verringern.

Weitere Informationen zur CryptoAPI 2,0-Diagnose finden Sie unter [Problembehandlung bei einer Enterprise-PKI](#).

Weitere Informationen:

[Technische Referenz für Smartcards](#)

Gruppenrichtlinien- und Registrierungseinstellungen für Smartcards

20.12.2019 • 18 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für den IT-Experten und den Smartcard-Entwickler werden die Gruppenrichtlinieneinstellungen, Registrierungsschlüsseleinstellungen, Einstellungen für lokale Sicherheitsrichtlinien und Richtlinieneinstellungen für die Delegierung von Anmeldeinformationen beschrieben, die für die Konfiguration von Smartcards verfügbar sind.

In den folgenden Abschnitten und Tabellen sind die Smartcard-bezogenen Gruppenrichtlinieneinstellungen und Registrierungsschlüssel aufgeführt, die pro Computer festgelegt werden können. Wenn Sie Gruppenrichtlinienobjekte (Domain Group Policy Objects, GPOs) verwenden, können Sie Gruppenrichtlinieneinstellungen auf lokale oder Domänencomputer bearbeiten und anwenden.

- **Primäre Gruppenrichtlinieneinstellungen für Smartcards**
 - Zertifikate ohne erweitertes Schlüssel Verwendungs Zertifikat-Attribut zulassen
 - Zulassen, dass ECC-Zertifikate für die Anmeldung und Authentifizierung verwendet werden
 - Anzeige der integrierten Blockierungs Anzeige zum Zeitpunkt der Anmeldung
 - Zulassen von Signaturschlüsseln, die für die Anmeldung gültig sind
 - Zeit für ungültige Zertifikate zulassen
 - Benutzernamen Hinweis zulassen
 - Konfigurieren des Cleanups von Stammzertifikaten
 - Zeichenfolge anzeigen, wenn Smartcard blockiert ist
 - Filtern doppelter Anmelde Zertifikate
 - Erzwingen des Auslesens aller Zertifikate von der Smartcard
 - Benachrichtigen des Benutzers über eine erfolgreiche Installation des Smartcard-Treibers
 - Verhindern des Zurückgebens von Klartext-Pins durch den Anmelde Informations-Manager
 - Umkehren des in einem Zertifikat gespeicherten Antragstellernamens beim Anzeigen
 - Aktivieren der Zertifikat Propagierung von einer Smartcard
 - Aktivieren der Stammzertifikat Propagierung von einer Smartcard
 - Aktivieren des Smartcard-Plug & Play-Diensts
- Basis-CSP und Smartcard KSP-Registrierungsschlüssel
- CRL-Überprüfung der Registrierungsschlüssel
- Zusätzliche Gruppenrichtlinieneinstellungen und Registrierungsschlüssel für Smartcards

Primäre Gruppenrichtlinieneinstellungen für Smartcards

Die folgenden Gruppenrichtlinieneinstellungen für Smartcards befinden sich auf der Computer Configuration\Administrative Templates\Windows Components\Smart-Karte.

Die Registrierungsschlüssel sind an den folgenden Speicherorten gespeichert:

- HKEY _LOCAL _MACHINE \software\policies\microsoft\windows\scnpn\enablescnpn
- HKEY _LOCAL _MACHINE \software\policies\microsoft\windows\smartcardcredentialprovider
- HKEY _LOCAL _MACHINE \software\policies\microsoft\windows\certprop

**** Hinweis die Registrierungsinformationen des Smartcard-Readers befinden sich in HKEY _LOCAL _MACHINE \software\microsoft\cryptography\calais\readers.
Informationen zur Smartcard-Registrierung finden Sie unter HKEY _LOCAL _MACHINE \software\microsoft\cryptography\calais\smartcards.

In der folgenden Tabelle sind die Standardwerte für diese GPO-Einstellungen aufgelistet. Variationen sind unter den Richtlinien Beschreibungen in diesem Thema dokumentiert.

SERVERTYP ODER GRUPPENRICHTLINIENOBJEKT	STANDARDWERT
Standarddomänenrichtlinie	Nicht konfiguriert
Standardrichtlinie für Domänen Controller	Nicht konfiguriert
Standardeinstellungen für eigenständige Server	Nicht konfiguriert
Effektive Standardeinstellungen für Domänen Controller	Deaktiviert
Effektive Standardeinstellungen für Mitglieds Server	Deaktiviert
Effektive Standardeinstellungen für Client Computer	Deaktiviert

Zertifikate ohne erweitertes Schlüssel Verwendungs Zertifikat-Attribut zulassen

Mit dieser Richtlinieneinstellung können Zertifikate ohne erweiterte Schlüsselverwendung für die Anmeldung verwendet werden.

**** Hinweis erweiterte Schlüsselverwendung Certificate-Attribut wird auch als erweiterte Schlüsselverwendung bezeichnet.

In Windows-Versionen vor Windows Vista erfordern Smartcard-Zertifikate, die zum Anmelden verwendet werden, eine EKU-Erweiterung mit einer Smartcard-Anmeldeobjekt-ID. Diese Richtlinieneinstellung kann verwendet werden, um diese Einschränkung zu ändern.

Wenn diese Richtlinieneinstellung aktiviert ist, können Zertifikate mit den folgenden Attributen auch zur Anmeldung mit einer Smartcard verwendet werden:

- Zertifikate ohne EKU
- Zertifikate mit einer Allzweck-EKU
- Zertifikate mit einer EKU für die Client Authentifizierung

Wenn diese Richtlinieneinstellung deaktiviert oder nicht konfiguriert ist, können nur Zertifikate, die die Smartcard-Anmeldeobjekt-ID enthalten, zur Anmeldung mit einer Smartcard verwendet werden.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	AllowCertificatesWithNoEKU
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Zulassen, dass ECC-Zertifikate für die Anmeldung und Authentifizierung verwendet werden

Mit dieser Richtlinieneinstellung können Sie steuern, ob ECC-Zertifikate (Elliptische Kurven Kryptographie) auf einer Smartcard zum Anmelden bei einer Domäne verwendet werden können. Wenn diese Einstellung aktiviert ist, können ECC-Zertifikate auf einer Smartcard zum Anmelden bei einer Domäne verwendet werden. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, können keine ECC-Zertifikate auf einer Smartcard zum Anmelden bei einer Domäne verwendet werden.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	EnumerateECCerts
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Diese Richtlinieneinstellung wirkt sich nur auf die Möglichkeit des Benutzers aus, sich bei einer Domäne anzumelden. ECC-Zertifikate auf einer Smartcard, die für andere Anwendungen wie das Signieren von Dokumenten verwendet werden, sind von dieser Richtlinieneinstellung nicht betroffen. Wenn Sie einen ECDSA-Schlüssel für die Anmeldung verwenden, müssen Sie auch über einen zugehörigen ECDH-Schlüssel verfügen, um die Anmeldung zuzulassen, wenn Sie nicht mit dem Netzwerk verbunden sind.

Anzeige der integrierten Blockierungs Anzeige zum Zeitpunkt der Anmeldung

Mit dieser Richtlinieneinstellung können Sie feststellen, ob das integrierte Blockierungs Feature auf der Anmeldebenutzeroberfläche (UI) zur Verfügung steht. Das Feature wurde als Standardfeature in den Anbieter von Anmeldeinformationen für Sicherheitsunterstützung in Windows Vista eingeführt.

Wenn diese Einstellung aktiviert ist, steht die integrierte Blockierungsfunktion zur Verfügung. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, ist das Feature nicht verfügbar.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	AllowIntegratedUnblock
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent

ELEMENT	BESCHREIBUNG
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Wenn Sie die integrierte Blockierungsfunktion verwenden möchten, muss Sie von der Smartcard unterstützt werden. Erkundigen Sie sich beim Hardwarehersteller, ob diese Funktion von der Smartcard unterstützt wird. Sie können eine benutzerdefinierte Nachricht erstellen, die angezeigt wird, wenn die Smartcard blockiert ist, indem Sie die Anzeigezeichenfolge für die Richtlinieneinstellung konfigurieren, Wenn Smartcard blockiert ist .

Zulassen von Signaturschlüsseln, die für die Anmeldung gültig sind

Mit dieser Richtlinieneinstellung können Sie Signaturschlüssel basierte Zertifikate auflisten und für die Anmeldung verfügbar machen. Wenn diese Einstellung aktiviert ist, werden alle auf der Smartcard verfügbaren Zertifikate mit einem nur-Signatur-Schlüssel auf dem Anmeldebildschirm angezeigt. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, werden auf der Smartcard Verfügbare Zertifikate mit einem nur-Signatur-Schlüssel nicht auf dem Anmeldebildschirm angezeigt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	AllowSignatureOnlyKeys
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Zeit für ungültige Zertifikate zulassen

Diese Richtlinieneinstellung ermöglicht es, abgelaufene oder noch nicht gültige Zertifikate für die Anmeldung anzuzeigen.

Vor Windows Vista mussten Zertifikate eine gültige Zeit enthalten und nicht ablaufen. Damit das Zertifikat verwendet werden kann, muss es vom Domänencontroller akzeptiert werden. Diese Richtlinieneinstellung steuert nur, welche Zertifikate auf dem Clientcomputer angezeigt werden.

Wenn diese Einstellung aktiviert ist, werden Zertifikate auf dem Anmeldebildschirm angezeigt, unabhängig davon, ob Sie eine ungültige Zeit oder ihre Gültigkeitsdauer abgelaufen sind. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, werden Zertifikate, die abgelaufen oder noch nicht gültig sind, nicht auf dem Anmeldebildschirm angezeigt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	AllowTimeInvalidCertificates
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent

ELEMENT	BESCHREIBUNG
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Benutzernamen Hinweis zulassen

Mit dieser Richtlinieneinstellung können Sie bestimmen, ob ein optionales Feld während der Anmeldung angezeigt wird, und es wird ein anschließender elevations Prozess bereitgestellt, mit dem Benutzer Ihren Benutzernamen oder Benutzernamen und Ihre Domäne eingeben können, die dem Benutzer ein Zertifikat zuordnet. Wenn diese Einstellung aktiviert ist, wird ein optionales Feld angezeigt, mit dem Benutzer Ihren Benutzernamen oder Benutzernamen und Ihre Domäne eingeben können. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird das Feld nicht angezeigt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	X509HintsNeeded
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Konfigurieren des Cleanups von Stammzertifikaten

Mit dieser Richtlinieneinstellung können Sie das Bereinigungs Verhalten von Stammzertifikaten verwalten. Zertifikate werden mithilfe einer Vertrauenskette überprüft, und der Vertrauensstellungs Anker für das digitale Zertifikat ist die Stammzertifizierungsstelle (Certification Authority, ca). Eine Zertifizierungsstelle kann mehrere Zertifikate mit dem Stammzertifikat als oberstes Zertifikat der Baumstruktur ausgeben. Ein privater Schlüssel wird verwendet, um andere Zertifikate zu signieren. Dadurch wird eine geerbte Vertrauenswürdigkeit für alle Zertifikate unmittelbar unter dem Stammzertifikat erstellt. Wenn diese Einstellung aktiviert ist, können Sie die folgenden Bereinigungsoptionen festlegen:

- **Keine Bereinigung.** Wenn der Benutzer die Smartcard abmeldet oder entfernt, bleiben die während der Sitzung verwendeten Stammzertifikate auf dem Computer bestehen.
- **Bereinigen Sie Zertifikate beim Entfernen von Smartcards.** Wenn die Smartcard entfernt wird, werden die Stammzertifikate entfernt.
- **Bereinigen Sie Zertifikate beim Abmelden.** Wenn sich der Benutzer von Windows abmeldet, werden die Stammzertifikate entfernt.

Wenn diese Richtlinieneinstellung deaktiviert oder nicht konfiguriert ist, werden Stammzertifikate automatisch entfernt, wenn sich der Benutzer von Windows abmeldet.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	RootCertificateCleanupOption

ELEMENT	BESCHREIBUNG
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Zeichenfolge anzeigen, wenn Smartcard blockiert ist

Wenn diese Richtlinieneinstellung aktiviert ist, können Sie die angezeigte Nachricht erstellen und verwalten, die dem Benutzer angezeigt wird, wenn eine Smartcard blockiert ist. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist (und die integrierte Blockierungsfunktion ebenfalls aktiviert ist), wird dem Benutzer die Standardmeldung des Systems angezeigt, wenn die Smartcard blockiert ist.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	IntegratedUnblockPromptString
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: diese Richtlinieneinstellung ist nur wirksam, wenn der Bildschirm integrierte Blockierung zulassen zum Zeitpunkt der Anmelderichtlinie angezeigt werden aktiviert ist.
Notizen und Ressourcen	

Filtern doppelter Anmelde Zertifikate

Mit dieser Richtlinieneinstellung können Sie einen Filterprozess verwenden, um zu konfigurieren, welche gültigen Anmelde Zertifikate angezeigt werden. Während des Zertifikats Erneuerungszeitraums kann die Smartcard eines Benutzers mehrere gültige Anmelde Zertifikate aufweisen, die von der gleichen Zertifikatvorlage ausgestellt wurden, wodurch Verwirrung darüber entstehen kann, welches Zertifikat ausgewählt werden muss. Dieses Verhalten kann auftreten, wenn ein Zertifikat erneuert und das alte Zertifikat noch nicht abgelaufen ist.

Zwei Zertifikate werden als identisch festgelegt, wenn Sie von derselben Vorlage mit der gleichen Hauptversion ausgestellt werden und für denselben Benutzer gelten (Dies wird durch den UPN festgelegt). Wenn diese Richtlinieneinstellung aktiviert ist, erfolgt die Filterung, damit der Benutzer nur die aktuellsten gültigen Zertifikate sehen kann, aus denen Sie auswählen können. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, werden alle Zertifikate für den Benutzer angezeigt.

Diese Richtlinieneinstellung wird auf den Computer angewendet, nachdem die Richtlinieneinstellung [ungültige Zertifikate zulassen](#) angewendet wurde.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	FilterDuplicateCerts

ELEMENT	BESCHREIBUNG
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Wenn zwei oder mehr der gleichen Zertifikate auf einer Smartcard vorhanden sind und diese Richtlinieneinstellung aktiviert ist, wird das Zertifikat angezeigt, das für die Anmeldung bei Computern mit Windows 2000, Windows XP oder Windows Server 2003 verwendet wird. Andernfalls wird das Zertifikat mit der am weitesten entfernten Ablaufzeit angezeigt.

Erzwingen des Auslesens aller Zertifikate von der Smartcard

Mit dieser Richtlinieneinstellung können Sie verwalten, wie Windows alle Zertifikate von der Smartcard zur Anmeldung liest. Während der Anmeldung liest Windows nur das Standardzertifikat von der Smartcard, es sei denn, es unterstützt das Abrufen aller Zertifikate in einem einzelnen Anruf. Diese Richtlinieneinstellung zwingt Windows, alle Zertifikate von der Smartcard zu lesen.

Wenn diese Richtlinieneinstellung aktiviert ist, versucht Windows, unabhängig von der CSP-Funktionsgruppe alle Zertifikate von der Smartcard zu lesen. Wenn deaktiviert oder nicht konfiguriert, versucht Windows, nur das Standardzertifikat von Smartcards zu lesen, die das Abrufen aller Zertifikate in einem einzelnen Anruf nicht unterstützen. Für die Anmeldung sind keine anderen Zertifikate als der Standard verfügbar.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	ForceReadingAllCertificates
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine **** Wichtig das Aktivieren dieser Richtlinieneinstellung kann sich negativ auf die Leistung während des Anmeldevorgangs in bestimmten Situationen auswirken.
Notizen und Ressourcen	Wenden Sie sich an den Smartcard-Anbieter, um festzustellen, ob Ihre Smartcard und der zugehörige CSP das erforderliche Verhalten unterstützen.

Benachrichtigen des Benutzers über eine erfolgreiche Installation des Smartcard-Treibers

Mit dieser Richtlinieneinstellung können Sie steuern, ob dem Benutzer eine Bestätigungsmeldung angezeigt wird, wenn ein Smartcard-Gerätetreiber installiert ist. Wenn diese Richtlinieneinstellung aktiviert ist, wird beim Installieren eines Smartcard-Gerätetreibers eine Bestätigungsmeldung angezeigt. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, wird keine Smartcard-Gerätetreiber-Installationsnachricht angezeigt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	ScPnPNotification
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Diese Richtlinieneinstellung gilt nur für Smartcard-Treiber, die das WHQL-Testverfahren (Windows Hardware Quality Labs) bestanden haben.

Verhindern des Zurückgebens von Klartext-Pins durch den Anmelde Informations-Manager

Mit dieser Richtlinieneinstellung wird verhindert, dass der Anmelde-Manager Klartext-Pins zurückgibt. Der Anmelde Informations-Manager wird vom Benutzer auf dem lokalen Computer gesteuert, und er speichert die Anmeldeinformationen aus unterstützten Browsern und Windows-Anwendungen. Die Anmeldeinformationen werden in speziellen verschlüsselten Ordnern auf dem Computer unter dem Profil des Benutzers gespeichert. Wenn diese Richtlinieneinstellung aktiviert ist, gibt der Anmelde Informations-Manager keine Klartext-PIN zurück. Wenn diese Einstellung deaktiviert oder nicht konfiguriert ist, können die Klartext-Pins vom Anmelde Informations-Manager zurückgegeben werden.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	DisallowPlaintextPin
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Wenn diese Richtlinieneinstellung aktiviert ist, funktionieren einige Smartcards möglicherweise nicht auf Computern unter Windows. Wenden Sie sich an den Smartcard-Hersteller, um festzustellen, ob diese Richtlinieneinstellung aktiviert werden soll.

Umkehren des in einem Zertifikat gespeicherten Antragstellernamens beim Anzeigen

Wenn diese Richtlinieneinstellung aktiviert ist, wird die Anzeige des Antragstellernamens so umgekehrt, wie er im Zertifikat während des Anmeldeprozesses gespeichert ist.

Damit Benutzer ein Zertifikat von einem anderen unterscheiden können, werden standardmäßig der Benutzerprinzipalname (User Principal Name, UPN) und der allgemeine Name angezeigt. Wenn diese Einstellung beispielsweise aktiviert ist, wenn der Zertifikats Betreff cn = Benutzer1, ou = users, DN = example, DN = com und der UPN user1@example.com ist, wird "Benutzer1" mit "user1@example.com" angezeigt. Wenn der UPN nicht vorhanden ist, wird der gesamte Name des Antragstellers angezeigt. Diese Einstellung steuert die Darstellung des Antragstellernamens und muss möglicherweise für Ihre Organisation angepasst werden.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	ReverseSubject
Standardwerte	Keine Änderungen pro Betriebssystemversion Deaktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	

Aktivieren der Zertifikat Propagierung von einer Smartcard

Mit dieser Richtlinieneinstellung können Sie die Zertifikat Propagierung verwalten, die beim Einfügen einer Smartcard eintritt. Der Zertifikat Propagations Dienst wird angewendet, wenn ein angemeldeter Benutzer eine Smartcard in einen Leser einfügt, der an den Computer angeschlossen ist. Diese Aktion bewirkt, dass das Zertifikat von der Smartcard gelesen wird. Die Zertifikate werden dann dem persönlichen Store des Benutzers hinzugefügt.

Wenn Sie diese Richtlinieneinstellung aktivieren oder nicht konfigurieren, erfolgt die Zertifikat Propagierung, wenn der Benutzer die Smartcard einfügt. Wenn diese Einstellung deaktiviert ist, tritt keine Zertifikat Propagierung auf, und die Zertifikate werden für Anwendungen wie Outlook nicht zur Verfügung gestellt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	CertPropEnabled
Standardwerte	Keine Änderungen pro Betriebssystemversion Aktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: diese Richtlinieneinstellung muss aktiviert sein, damit die Aktivierung der Stammzertifikat Propagierung von der Smart Card -Einstellung auf funktionieren kann, wenn Sie aktiviert ist.
Notizen und Ressourcen	

Aktivieren der Stammzertifikat Propagierung von einer Smartcard

Mit dieser Richtlinieneinstellung können Sie die Stammzertifikat Propagierung verwalten, die auftritt, wenn eine Smartcard eingefügt wird. Der Zertifikat Propagations Dienst wird angewendet, wenn ein angemeldeter Benutzer eine Smartcard in einen Leser einfügt, der an den Computer angeschlossen ist. Diese Aktion bewirkt, dass das Zertifikat von der Smartcard gelesen wird. Die Zertifikate werden dann dem persönlichen Store des Benutzers hinzugefügt. Wenn diese Richtlinieneinstellung aktiviert oder nicht konfiguriert ist, tritt die Stammzertifikat Propagierung auf, wenn der Benutzer die Smartcard einfügt.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	EnableRootCertificate-Propagierung
Standardwerte	Keine Änderungen pro Betriebssystemversion Aktiviert und nicht konfiguriert sind äquivalent

ELEMENT	BESCHREIBUNG
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: damit diese Richtlinieneinstellung funktioniert, muss auch die Option " Zertifikat Propagierung aus Smartcard -Richtlinieneinstellung aktivieren" aktiviert sein.
Notizen und Ressourcen	

Aktivieren des Smartcard-Plug & Play-Diensts

Mit dieser Richtlinieneinstellung können Sie steuern, ob die Smartcard-Plug & Play-Funktion aktiviert ist. Das bedeutet, dass Ihre Benutzer Smartcards von Anbietern verwenden können, die ihre Treiber über Windows Update veröffentlicht haben, ohne spezielle Middleware zu benötigen. Diese Treiber werden auf die gleiche Weise wie Treiber für andere Geräte in Windows heruntergeladen. Wenn ein geeigneter Treiber nicht über Windows Update verfügbar ist, wird für diese Karten ein PIV-kompatibles Mini Driver verwendet, das in einer der unterstützten Versionen von Windows enthalten ist.

Wenn die Smartcard-Plug & Play-Richtlinieneinstellung aktiviert oder nicht konfiguriert ist und das System versucht, einen Smartcard-Gerätetreiber zu installieren, wenn eine Smartcard zum ersten Mal in einen Smartcard-Leser eingefügt wird. Wenn diese Richtlinieneinstellung deaktiviert ist, wird ein Gerätetreiber nicht installiert, wenn eine Smartcard in einen Smartcard-Leser eingefügt wird.

ELEMENT	BESCHREIBUNG
Registrierungsschlüssel	EnableScnPp
Standardwerte	Keine Änderungen pro Betriebssystemversion Aktiviert und nicht konfiguriert sind äquivalent
Richtlinienverwaltung	Neustartanforderung: keine Abmeldeanforderung: keine Richtlinienkonflikte: keine
Notizen und Ressourcen	Diese Richtlinieneinstellung gilt nur für Smartcard-Treiber, die das WHQL-Testverfahren (Windows Hardware Quality Labs) bestanden haben.

Basis-CSP und Smartcard KSP-Registrierungsschlüssel

Die folgenden Registrierungsschlüssel können für den Basis-Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) und den Smartcard-Schlüsselspeicheranbieter (KSP) konfiguriert werden. In den folgenden Tabellen sind die Schlüssel aufgeführt. Alle Schlüssel verwenden den DWORD-Typ.

Die Registrierungsschlüssel für den Basis-CSP befinden sich in der Registrierung in HKEY _LOCAL _MACHINE \software\microsoft\cryptography\defaults\provider\microsoft Base Smartcard Crypto-Anbieter.

Die Registrierungsschlüssel für die Smartcard KSP befinden sich in HKEY _LOCAL _MACHINE \system\controlset001\control\cryptography\providers\microsoft-Smartcard-Schlüsselspeicheranbieter.

Registrierungsschlüssel für den Basis-CSP und die Smartcard KSP

REGISTRIERUNGSSCHLÜSSEL	BESCHREIBUNG
-------------------------	--------------

REGISTRIERUNGSSCHLÜSSEL	BESCHREIBUNG
AllowPrivateExchangeKeyImport	Mit einem Wert ungleich NULL können RSA-Exchange- (beispielsweise Verschlüsselungs-) private Schlüssel für die Verwendung in Schlüssel Archivierungsszenarien importiert werden. Standardwert: 00000000
AllowPrivateSignatureKeyImport	Mit einem Wert ungleich NULL können RSA-Signatur-private Schlüssel für die Verwendung in Schlüssel Archivierungsszenarien importiert werden. Standardwert: 00000000
DefaultPrivateKeyLenBits	Definiert die Standardlänge für private Schlüssel, falls gewünscht. Standardwert: 00000400 Standardparameter für die Schlüsselerzeugung: 1024-Bit-Schlüssel
RequireOnCardPrivateKeyGen	Mit diesem Schlüssel wird die Kennzeichnung festgelegt, die die Generierung von privaten Schlüsseln auf Karten erfordert (Standard). Wenn dieser Wert gesetzt ist, kann ein auf einem Host generierter Schlüssel in die Smartcard importiert werden. Dies wird für Smartcards verwendet, die die Schlüsselerzeugung auf dem Kartenspeicher nicht unterstützen, oder wenn ein Schlüssel-Escrow erforderlich ist. Standardwert: 00000000
TransactionTimeoutMilliseconds	Mit Standardtimeoutwerten können Sie angeben, ob Transaktionen, die über mäßig viel Zeit in Anspruch nehmen, fehlschlagen. Standardwert: 000005dc1500 Das Standardtimeout für das Speichern von Transaktionen auf der Smartcard beträgt 1,5 Sekunden.

Zusätzliche Registrierungsschlüssel für die Smartcard KSP

REGISTRIERUNGSSCHLÜSSEL	BESCHREIBUNG
AllowPrivateECDHEKeyImport	Mit diesem Wert können ephemere elliptische Curve Diffie-Hellman (ECDHE)-private Schlüssel für die Verwendung in Schlüssel Archivierungsszenarien importiert werden. Standardwert: 00000000
AllowPrivateECDSAKeyImport	Mit diesem Wert können ECDSA-private Schlüssel (elliptische Kurve) für die Verwendung in Schlüssel Archivierungsszenarien importiert werden. Standardwert: 00000000

CRL-Überprüfung der Registrierungsschlüssel

In der folgenden Tabelle sind die Schlüssel und die entsprechenden Werte aufgeführt, um die CRL-Prüfung (Certificate Revocation List, CRL) beim Key Distribution Center (KDC) oder Client zu deaktivieren. Zum Verwalten der CRL-Überprüfung müssen Sie die Einstellungen für das KDC und den Client konfigurieren.

CRL-Überprüfung der Registrierungsschlüssel

REGISTRIERUNGSSCHLÜSSEL	DETAILS
HKEY _LOCAL _MACHINE \system\ccs\services\kdc\usecachedcrloonlyandignorerrevocatio nunknownerrors	Typ = DWORD Wert = 1
HKEY _LOCAL _MACHINE \system\ccs\control\lsa\kerberos\parameters\usecachedcrlo yandignorerrevocationunknownerrors	Typ = DWORD Wert = 1

Zusätzliche Gruppenrichtlinieneinstellungen und Registrierungsschlüssel für Smartcards

Bei einer Smartcard-Bereitstellung können zusätzliche Gruppenrichtlinieneinstellungen verwendet werden, um die Benutzerfreundlichkeit oder Sicherheit zu verbessern. Zwei dieser Richtlinieneinstellungen, die eine Smartcard-Bereitstellung ergänzen können, sind:

- Deaktivieren der Delegierung für Computer
- Interaktive Anmeldung: keine STRG + ALT + ENTF erforderlich (nicht empfohlen)

Die folgenden Smartcard-bezogenen Gruppenrichtlinieneinstellungen befinden sich unter Computer Configuration\Windows Settings\Security Settings\Local Policies\Security-Optionen.

Einstellungen für lokale Sicherheitsrichtlinien

GRUPPENRICHTLINIENEINSTELLUNG UND REGISTRIERUNGSSCHLÜSSEL	STANDARD	BESCHREIBUNG
Interaktive Anmeldung: Smartcard erforderlich scforceoption	Deaktiviert	Für diese Sicherheitsrichtlinieneinstellung müssen sich die Benutzer mit einer Smartcard bei einem Computer anmelden. Aktiviert Benutzer können sich nur mithilfe einer Smartcard beim Computer anmelden. Deaktiviert Benutzer können sich mit einer beliebigen Methode beim Computer anmelden.

GRUPPENRICHTLINIENEINSTELLUNG UND REGISTRIERUNGSSCHLÜSSEL	STANDARD	BESCHREIBUNG
Interaktive Anmeldung: Verhalten beim Entfernen von Smartcards scremoveoption	Diese Richtlinieneinstellung ist nicht definiert, was bedeutet, dass Sie vom System als keine Aktion behandelt wird.	Diese Einstellung bestimmt, was passiert, wenn die Smartcard für einen signierten Benutzer aus dem Smartcard-Lesegerät entfernt wird. Die Optionen sind: Keine Aktion Arbeitsstation sperren: die Arbeitsstation ist gesperrt, wenn die Smartcard entfernt wird, sodass Benutzer den Bereich belassen, Ihre Smartcard mitnehmen und weiterhin eine geschützte Sitzung verwalten können. Abmelden Erzwingen: der Benutzer wird automatisch abgemeldet, wenn die Smartcard entfernt wird. Trennen der Verbindung, Wenn eine Remote Desktop Dienste-Sitzung: durch Entfernen der Smartcard wird die Sitzung getrennt, ohne dass der Benutzer sich abmeldet. Auf diese Weise kann der Benutzer die Smartcard erneut einfügen und die Sitzung später oder auf einem anderen Computer, der mit einem Smartcard-Lesegerät ausgestattet ist, fortsetzen, ohne sich erneut anmelden zu müssen. Wenn die Sitzung lokal ist, funktioniert diese Richtlinieneinstellung identisch mit der Option " Workstation Sperren ". **** Hinweis Remote Desktop Dienste wurden in früheren Versionen von Windows Server als Terminal Dienste bezeichnet.

Im lokalen Sicherheitsrichtlinien-Editor (secpol. msc) können Sie Systemrichtlinien bearbeiten und anwenden, um die Delegierung von Anmeldeinformationen für lokale oder Domänencomputer zu verwalten.

Die folgenden Smartcard-bezogenen Gruppenrichtlinieneinstellungen befinden sich in der Computer Configuration\Administrative Templates\System\Credentials-Delegierung.

Registrierungsschlüssel befinden sich in HKEY _LOCAL _MACHINE
\system\controlset001\control\lsa\credssp\policydefaults.

**** Hinweis in der folgenden Tabelle sind die neuen Anmeldeinformationen so, dass Sie beim Ausführen einer Anwendung dazu aufgefordert werden.

Richtlinieneinstellungen für die Delegierung von Anmeldeinformationen

GRUPPENRICHTLINIENEINSTELLUNG UND REGISTRIERUNGSSCHLÜSSEL	STANDARD	BESCHREIBUNG
---	----------	--------------

GRUPPENRICHTLINIENEINSTELLUNG UND REGISTRIERUNGSSCHLÜSSEL	STANDARD	BESCHREIBUNG
<p>Zulassen, dass neue Anmeldeinformationen delegiert werden</p> <p>AllowFreshCredentials</p>	<p>Nicht konfiguriert</p>	<p>Diese Richtlinieneinstellung gilt: Wenn die Serverauthentifizierung über ein vertrauenswürdiges X509-Zertifikat oder ein Kerberos-Protokoll erfolgt ist. Für Anwendungen, die die CredSSP-Komponente verwenden (beispielsweise Remote Desktop Dienste).</p> <p>Aktiviert: Sie können die Server angeben, auf die die neuen Anmeldeinformationen des Benutzers delegiert werden können.</p> <p>Nicht konfiguriert: nach der richtigen gegenseitigen Authentifizierung ist die Delegierung von neuen Anmeldeinformationen für Remote Desktop Dienste auf jedem Computer zulässig.</p> <p>Deaktiviert: die Delegierung von neuen Anmeldeinformationen auf einen beliebigen Computer ist nicht zulässig.</p> <p><i>*** Hinweis diese Richtlinieneinstellung kann auf einen oder mehrere Dienstprinzipalnamen (Service Principal Names, SPNs) festgelegt werden. Der SPN steht für den Zielservice, auf dem die Benutzeranmeldeinformationen delegiert werden können. Bei der Angabe des SPN ist ein einzelnes Platzhalterzeichen zulässig, beispielsweise:</i></p> <p><i>Verwenden Sie \ * termsrv/\ * \ * für den Remote Desktop-Sitzungshost (RD-Sitzungshost), der auf einem beliebigen Computer ausgeführt wird. Verwenden Sie *termsrv/Host. HumanResources.fabrikam.com für RD-Sitzungshost, der auf dem Host.HumanResources.fabrikam.com-Computer ausgeführt wird. Verwenden Sie termsrv/\ *. HumanResources.fabrikam.com für RD-Sitzungs Host, der auf allen Computern in. HumanResources.fabrikam.com ausgeführt wird.</i></p>

GRUPPENRICHTLINIENEINSTELLUNG UND REGISTRIERUNGSSCHLÜSSEL	STANDARD	BESCHREIBUNG
<p>Zulassen der erneuten Übertragung von neuen Anmeldeinformationen mit NTLM-Server Authentifizierung</p> <p>AllowFreshCredentialsWhenNTLMOnly</p>	Nicht konfiguriert	<p>Diese Richtlinieneinstellung gilt: Wenn die Serverauthentifizierung mithilfe von NTLM erreicht wurde. Für Anwendungen, die die CredSSP-Komponente verwenden (beispielsweise Remote Desktop).</p> <p>Aktiviert: Sie können die Server angeben, auf die die neuen Anmeldeinformationen des Benutzers delegiert werden können.</p> <p>Nicht konfiguriert: nach der richtigen gegenseitigen Authentifizierung ist die Delegierung von neuen Anmeldeinformationen für den Remote Desktop-Sitzungs Host auf einem beliebigen Computer zulässig (termsrv/\).</p> <p><i>Deaktiviert: die Delegierung von neuen Anmeldeinformationen ist für jeden Computer nicht zulässig.</i></p> <p>Hinweis diese Richtlinieneinstellung kann auf einen oder mehrere SPNs festgelegt werden. Der SPN steht für den Zielservers, auf dem die Benutzeranmeldeinformationen delegiert werden können. Bei der Angabe des SPN ist ein einzelnes Platzhalterzeichen (\ *) zulässig. Beispiele finden Sie in der Richtlinie zum *Delegieren der neuen Anmeldeinformationen für die Richtlinieneinstellung zulassen.</p>
<p>Ablehnen der erneuten Delegierung neuer Anmeldeinformationen</p> <p>DenyFreshCredentials</p>	Nicht konfiguriert	<p>Diese Richtlinieneinstellung gilt für Anwendungen, die die CredSSP-Komponente verwenden (beispielsweise Remote Desktop).</p> <p>Aktiviert: Sie können die Server angeben, bei denen die neuen Anmeldeinformationen des Benutzers nicht delegiert werden können.</p> <p>Deaktiviert oder nicht konfiguriert: Es wurde kein Server angegeben.</p> <p>* Hinweis diese Richtlinieneinstellung kann auf einen oder mehrere SPNs festgelegt werden. Der SPN steht für den Zielservers, auf dem die Benutzeranmeldeinformationen nicht delegiert werden können. Bei der Angabe des SPN ist ein einzelnes Platzhalterzeichen (\ *) zulässig. Beispiele finden Sie in der Richtlinie zum *Delegieren der neuen Anmeldeinformationen für die Richtlinieneinstellung zulassen.</p>

Wenn Sie Remote Desktop Dienste mit Smartcard-Anmeldung verwenden, können Sie keine standardmäßigen und gespeicherten Anmeldeinformationen delegieren. Die Registrierungsschlüssel in der folgenden Tabelle, die sich unter HKEY \ _LOCAL \ _MACHINE \ system \ controlset001 \ control \ Isa \ credssp \ policydefaults befinden, und die entsprechenden Gruppenrichtlinieneinstellungen werden ignoriert.

REGISTRIERUNGSSCHLÜSSEL	ENTSPRECHENDE GRUPPENRICHTLINIENEINSTELLUNG
AllowDefaultCredentials	Delegieren von Standardanmeldeinformationen zulassen
AllowDefaultCredentialsWhenNTLMOnly	Zulassen der Delegierung von Standardanmeldeinformationen mit der NTLM-Server Authentifizierung
AllowSavedCredentials	Delegieren gespeicherter Anmeldeinformationen zulassen
AllowSavedCredentialsWhenNTLMOnly	Zulassen der Delegierung gespeicherter Anmeldeinformationen mit der NTLM-Server Authentifizierung

Weitere Informationen

[Technische Referenz für Smartcards](#)

Smartcardereignisse

04.12.2019 • 12 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für den IT-Experten und den Smartcard-Entwickler werden Ereignisse beschrieben, die sich auf die Bereitstellung und Entwicklung von Smartcards beziehen.

Eine Reihe von Ereignissen kann verwendet werden, um Smartcard-Aktivitäten auf einem Computer zu überwachen, einschließlich Installation, Verwendung und Fehler. In den folgenden Abschnitten werden die Ereignisse und Informationen beschrieben, die zum Verwalten von Smartcards in einer Organisation verwendet werden können.

- [Name des Smartcard-Lesers](#)
- [Warnungseignisse für Smartcards](#)
- [Smartcard-Fehlerereignisse](#)
- [Plug & Play-Ereignisse für Smartcards](#)

Name des Smartcard-Lesers

Der Smartcard-Ressourcen-Manager verwendet nicht den Gerätenamen aus dem Geräte-Manager, um einen Smartcard-Leser zu beschreiben. Stattdessen wird der Name aus drei Geräte Attributen erstellt, die direkt vom Treiber für Smartcard-Leser abgefragt werden.

Die folgenden drei Attribute werden verwendet, um den Namen des Smartcard-Lesers zu erstellen:

- Herstellername
- Benutzeroberflächen-Gerätetyp
- Geräteeinheit

Der Gerätenamen des Smartcard-Readers wird im Format `<VendorName><Type><DeviceUnit>` erstellt. So wird beispielsweise "Contoso-Smartcard-Leser 0" aus den folgenden Informationen erstellt:

- Herstellername: contoso
- Benutzeroberflächen-Gerätetyp: Smartcard-Leser
- Geräteeinheit: 0

Warnungseignisse für Smartcards

Hinweis: `ioctl` in der folgenden Tabelle bezieht sich auf die Eingabe- und Ausgabesteuerung.

EREIGNIS-ID	WARNMELDUNG	BESCHREIBUNG
-------------	-------------	--------------

EREIGNIS-ID	WARNMELDUNG	BESCHREIBUNG
620	Der Smartcard-Ressourcen-Manager konnte die IOCTL %3 für den Leser "%2" nicht stornieren: %1. Der Leser reagiert möglicherweise nicht mehr. Wenn dieser Fehler weiterhin auftritt, funktioniert Ihre Smartcard oder Ihr Lesegerät möglicherweise nicht ordnungsgemäß. % n% nbefehl-Kopfzeile: %4	<p>Dies tritt auf, wenn der Ressourcen-Manager versucht, einen Befehl an den Smartcard-Leser abzubreaken, wenn der Smartcard-Dienst heruntergefahren wird oder nachdem eine Smartcard aus dem Smartcard-Leser entfernt wurde und der Befehl nicht abgebrochen werden konnte. Dadurch kann der Smartcard-Leser in einem unbrauchbaren Zustand bleiben, bis er vom Computer entfernt oder der Computer neu gestartet wird.</p> <p>%1 = Windows-Fehlercode %2 = Name des Smartcard-Lesers %3 = IOCTL wird abgebrochen %4 = erste 4 Bytes des Befehls, der an die Smartcard gesendet wurde</p>
619	Der Smartcard-Leser "%2" hat in %1 Sekunden nicht auf IOCTL %3 geantwortet. Wenn dieser Fehler weiterhin auftritt, funktioniert Ihre Smartcard oder Ihr Lesegerät möglicherweise nicht ordnungsgemäß. % n% nbefehl-Kopfzeile: %4	<p>Dies tritt auf, wenn ein Reader nach einer ungewöhnlich langen Zeitspanne nicht auf ein IOCTL-Ereignis geantwortet hat. Zurzeit wird dieser Fehler gesendet, nachdem ein Leser 150 Sekunden lang nicht reagiert hat. Dadurch kann der Smartcard-Leser in einem unbrauchbaren Zustand bleiben, bis er vom Computer entfernt oder der Computer neu gestartet wird.</p> <p>%1 = Anzahl der Sekunden, die der IOCTL gewartet hat %2 = Name des Smartcard-Lesers %3 = ioctl gesendet %4 = erste 4 Bytes des Befehls, der an die Smartcard gesendet wurde</p>

Smartcard-Fehlerereignisse

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
202	Fehler beim Initialisieren der Server Anwendung	Es ist ein Fehler aufgetreten, und der Dienst kann nicht ordnungsgemäß initialisiert werden. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.
203	Das Server Steuerelement verfügt über keinen Speicher für das Reader-Referenzobjekt.	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
204	Fehler beim Erstellen des Shutdown-Ereignisses durch das Server Steuerelement: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
205	Reader-Objekt hat doppelten Namen: %1	Es gibt zwei Smartcard-Leser mit dem gleichen Namen. Entfernen Sie den Smartcard-Leser, der diese Fehlermeldung verursacht. %1 = Name des duplizierten Smartcard-Readers
206	Fehler beim Erstellen des globalen Leser Änderungsereignisses.	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.
401	Ausnahme zum Herunterfahren des Leseegeräts vom Befehl "Smartcard Auswerfen"	Ein Smartcard-Leser konnte keine Smartcard auswerfen, während der Smartcard-Leser heruntergefahren wurde.
406	Reader-Objekt kann Gerät nicht identifizieren	Ein Smartcard-Leser reagierte nicht ordnungsgemäß auf eine Anforderung von Informationen über das Gerät, die für die Erstellung des Smartcard-Leser namens erforderlich ist. Der Smartcard-Leser wird vom Dienst erst erkannt, wenn er vom Computer entfernt und erneut eingefügt wird oder bis der Computer neu gestartet wird.
502	Fehler beim Initialisieren des kritischen Abschnitts des Dienst Status	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.
504	Der Ressourcen-Manager kann das Ereignis-Flag für das Herunterfahren nicht erstellen: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
506	Fehler beim Registrieren des Diensts für den Smartcard-Ressourcen-Manager: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
506	Der Smartcard-Ressourcen-Manager hat eine unerwartete Ausnahme vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Reader hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
507	Kein Arbeitsspeicher für wichtigen Dienst Status Abschnitt verfügbar	Es steht nicht genügend Systemarbeitsspeicher zur Verfügung. Dadurch wird verhindert, dass der Dienst den Status verwaltet. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.
508	Der Smartcard-Ressourcen-Manager hat eine unerwartete Ausnahme vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Reader hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
509	Der Smartcard-Ressourcen-Manager hat eine unerwartete Ausnahme vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Reader hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
510	Der Smartcard-Ressourcen-Manager hat das NULL-Handle vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Smartcard-Leser hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
511	Der Smartcard-Ressourcen-Manager hat eine unerwartete Ausnahme vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Reader hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
512	Der Smartcard-Ressourcen-Manager hat das NULL-Handle vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Smartcard-Leser hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
513	Der Smartcard-Ressourcen-Manager hat eine unerwartete Ausnahme vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Reader hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
514	Fehler beim Hinzufügen des Lesebereichs des Smartcard-Ressourcen-Managers %2: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode %2 = Name des Smartcard-Lesers
515	Fehler beim Deklarieren des Status des Smartcard-Ressourcen-Managers: %1	Hierbei handelt es sich um einen internen nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Der Smart Card-Dienst funktioniert möglicherweise nicht ordnungsgemäß. Das Problem kann durch einen Neustart des Diensts oder Computers behoben werden. %1 = Windows-Fehlercode
516	Das Herunterfahren des Smartcard-Ressourcen-Managers konnte nicht deklariert werden: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Der Smartcard-Dienst kann möglicherweise nicht beendet werden. Wenn Sie den Computer neu starten, kann dieses Problem möglicherweise behoben werden. %1 = Windows-Fehlercode

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
517	Der Smartcard-Ressourcen-Manager hat unerwartete Ausnahmen beim Hinzufügen des Readers %1 erhalten.	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Name des Smartcard-Lesers
521	Der Smartcard-Ressourcen-Manager hat das NULL-Handle vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Smartcard-Leser hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
523	Der Smartcard-Ressourcen-Manager hat das NULL-Handle vom PNP-Ereignis %1 erhalten.	Fehler beim Versuch, einen Plug & Play-Smartcard-Leser hinzuzufügen. Das Gerät ist möglicherweise bereits in Betrieb oder fehlerhaft. Um diese Fehlermeldung zu beheben, versuchen Sie, das Gerät erneut hinzuzufügen, oder starten Sie den Computer neu. %1 = Name des betroffenen Handles
602	Die Treiberinitialisierung des WDM-Lesegeräts kann das Lesegerät nicht öffnen: %1	Der Dienst kann keinen Kommunikationskanal mit dem Smartcard-Lesegerät öffnen. Sie können den Smartcard-Leser erst dann verwenden, wenn das Problem behoben ist. %1 = Windows-Fehlercode
603	Die Treiberinitialisierung für WDM-Reader hat keinen verfügbaren Arbeitsspeicher zum Steuern des Geräts %1	Es steht nicht genügend SystemArbeitsspeicher zur Verfügung. Dadurch wird verhindert, dass der Dienst den hinzugefügten Smartcard-Leser verwaltet. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Name des betroffenen Readers
604	Das Server Steuerelement kann das Entfernen von Lese Ereignissen nicht festlegen: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
605	Fehler beim Erstellen eines Overlapped-Ereignisses durch das Reader-Objekt: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
606	Das readerobjekt konnte das Entfernungs Ereignis nicht erstellen: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
607	Das Lese Objekt konnte den Monitorthread nicht starten: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
608	Fehler beim Erstellen des Power Down-Zeitgebers durch den Lesermonitor: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode
609	Fehler beim Erstellen eines Overlapped-Ereignisses durch den Lesermonitor: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
610	Der Smartcard-Leser "%2" hat ioctl %3: %1 abgelehnt. Wenn dieser Fehler weiterhin auftritt, funktioniert Ihre Smartcard oder Ihr Lesegerät möglicherweise nicht ordnungsgemäß. % n% nbefehl-Kopfzeile: %4	Der Leser kann den angegebenen ioctl nicht erfolgreich an die Smartcard übertragen. Dies kann auf einen Hardwarefehler hindeuten, dieser Fehler kann aber auch auftreten, wenn eine Smartcard oder ein Smartcard-Lesegerät aus dem System entfernt wird, während ein Vorgang ausgeführt wird. %1 = Windows-Fehlercode %2 = Name des Smartcard-Lesers %3 = IOCTL, die gesendet wurde %4 = erste 4 Bytes des Befehls, der an die Smartcard gesendet wird Diese Ereignisse werden durch Legacyfunktionen im Smartcard-Stapel verursacht. Sie kann ignoriert werden, wenn es in den Szenarien für die Smartcard-Nutzung keinen nennenswerten Fehler gibt.
611	Fehler bei der Initialisierung des Smartcard-Readers	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann dieses Problem möglicherweise behoben werden.
612	Fehler beim Wiederholungs Schwellenwert für Reader-insertions Monitor erreicht: %1	Dies tritt auf, wenn ein Smartcard-Lesegerät mehrmals fehlschlägt, um ordnungsgemäß auf den ioctl zu reagieren, was angibt, ob eine Smartcard im Reader vorhanden ist. Der Smartcard-Leser ist als fehlerhaft markiert und wird vom Dienst erst erkannt, wenn er vom Computer entfernt und erneut eingefügt wird oder bis der Computer neu gestartet wird. %1 = Windows-Fehlercode
615	Fehler beim Wiederholungs Schwellenwert für Reader-Entfernungs Überwachung erreicht: %1	Dies tritt auf, wenn ein Smartcard-Lesegerät mehrmals fehlschlägt, um ordnungsgemäß auf den ioctl zu reagieren, was angibt, ob eine Smartcard im Reader vorhanden ist. Der Smartcard-Leser ist als fehlerhaft markiert und wird vom Dienst erst erkannt, wenn er vom Computer entfernt und erneut eingefügt wird oder bis der Computer neu gestartet wird. %1 = Windows-Fehlercode

EREIGNIS-ID	FEHLERMELDUNG	BESCHREIBUNG
616	Der Lesemonitor "%2" hat nicht abgefangenen Fehlercode erhalten: %1	Dies tritt auf, wenn ein Smartcard-Lesegerät mehrmals fehlschlägt, um ordnungsgemäß auf den ioctl zu reagieren, was angibt, ob eine Smartcard im Reader vorhanden ist. Der Smartcard-Leser ist als fehlerhaft markiert und wird vom Dienst erst erkannt, wenn er vom Computer entfernt und erneut eingefügt wird oder bis der Computer neu gestartet wird. %1 = Windows-Fehlercode %2 = Leser Name
617	Reader-Monitor "%1"-Ausnahme--Thread wird beendet	Beim Überwachen eines Smartcard-Readers für Smartcard-Einfügungen und-Entfernungen ist ein unbekannter Fehler aufgetreten. Der Smartcard-Leser ist als fehlerhaft markiert und wird vom Dienst erst erkannt, wenn er vom Computer entfernt und erneut eingefügt wird oder bis der Computer neu gestartet wird. %1 = Name des Smartcard-Lesers
618	Für den Smartcard-Ressourcen-Manager ist ein nicht behebbarer interner Fehler aufgetreten.	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden.
621	Fehler beim Zugriff auf das Startereignis des Server Steuerelements: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode Diese Ereignisse werden durch Legacyfunktionen im Smartcard-Stapel verursacht. Sie kann ignoriert werden, wenn es in den Szenarien für die Smartcard-Nutzung keinen nennenswerten Fehler gibt.
622	Fehler beim Zugriff auf das Stop-Ereignis des Server Steuerelements: %1	Hierbei handelt es sich um einen internen, nicht behebbaren Fehler, der auf einen Fehler im smartcarddienst hindeutet. Die häufigste Ursache sind begrenzte Computerressourcen. Wenn Sie den Computer neu starten, kann das Problem möglicherweise behoben werden. %1 = Windows-Fehlercode

Plug & Play-Ereignisse für Smartcards

EREIGNIS-ID	EREIGNISTYP	EREIGNISMELDUNG	BESCHREIBUNG
1000	Fehler	Die Geräte-ID für Smartcard konnte in Reader %1 nicht abgerufen werden. Der Rückgabecode lautet %2.	Die Geräte-ID für die Smartcard konnte nicht von Smartcard-Plug & Play abgerufen werden. Diese Informationen sind erforderlich, um den richtigen Treiber zu ermitteln. Die Smartcard ist möglicherweise fehlerhaft. %1 = Name des Smartcard-Lesers %2 = Windows-Fehlercode
1001	Information	Software, die erfolgreich für Smartcard im Leser %1 installiert wurde. Der Smartcard-Name lautet %2.	Smartcard-Plug & Play hat erfolgreich eine Mini Driver für die eingefügte Karte installiert. %1 = Name des Smartcard-Lesers %2 = Name des neuen Smartcard-Geräts

Weitere Informationen

[Technische Referenz für Smartcards](#)

Übersicht über virtuelle Smartcards

24.12.2019 • 8 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten finden Sie eine Übersicht über die von Microsoft entwickelte virtuelle Smartcard-Technologie sowie [Links zu weiteren Themen](#), die Ihnen beim evaluieren, planen, bereitstellen und Verwalten virtueller Smartcards helfen.

Meinten Sie...

- [Smartcards](#)

NOTE

[Windows Hello for Business](#) ist die moderne zweistufige Authentifizierung für Windows 10. Microsoft ist in Zukunft nicht mehr in der Lage, virtuelle Smartcards zu deaktivieren, aber zurzeit wurde kein Datum gesetzt. Kunden, die Windows 10 und virtuelle Smartcards verwenden, sollten zu Windows Hello for Business wechseln. Microsoft wird das Datum frühzeitig veröffentlichen, um sicherzustellen, dass die Kunden genügend Zeit für den Wechsel zu Windows Hello for Business haben. Wir empfehlen, dass neue Windows 10-Bereitstellungen Windows Hello for Business verwenden. Virtuelle Smartcards bleiben für Windows 7 und Windows 8 unterstützt.

Featurebeschreibung

Die virtuelle Smartcard-Technologie von Microsoft bietet mithilfe der zweistufigen Authentifizierung vergleichbare Sicherheitsvorteile für physische Smartcards. Virtuelle Smartcards emulieren die Funktionalität von physikalischen Smartcards, verwenden aber den TPM-Chip (Trusted Platform Module), der auf Computern in vielen Organisationen zur Verfügung steht, anstatt die Verwendung einer separaten physischen Smartcard und eines Lesegeräts zu erfordern. Virtuelle Smartcards werden im TPM erstellt, in dem die für die Authentifizierung verwendeten Schlüssel in kryptografisch gesicherter Hardware gespeichert werden.

Durch die Verwendung von TPM-Geräten, die die gleichen kryptografischen Funktionen wie physische Smartcards bereitstellen, führen virtuelle Smartcards die drei wichtigsten Eigenschaften aus, die für Smartcards erwünscht sind: keine Exportfähigkeit, isolierte Kryptografie und Anti-hämmern.

Praktische Anwendungsfälle

Virtuelle Smartcards ähneln physikalischen Smartcards und werden in Windows als Smartcards angezeigt, die immer eingefügt werden. Virtuelle Smartcards können für die Authentifizierung für externe Ressourcen, den Datenschutz durch sichere Verschlüsselung und die Integrität durch zuverlässige Signierung verwendet werden. Sie können problemlos mithilfe von internen Methoden oder einer gekauften Lösung bereitgestellt werden, und Sie können zu einem vollständigen Ersatz für andere Methoden der starken Authentifizierung in einer Unternehmenseinstellung jeder Größenordnung werden.

Authentifizierungs Anwendungsfälle

Zweistufiger authentication\2012based-Remotezugriff

Nachdem ein Benutzer über eine voll funktionsfähige virtuelle TPM-Smartcard verfügt, die mit einem Anmeldezertifikat bereitgestellt wurde, wird das Zertifikat verwendet, um einen stark authentifizierten Zugriff auf Unternehmensressourcen zu erhalten. Wenn das richtige Zertifikat auf die virtuelle Karte bereitgestellt wird, muss der Benutzer nur die PIN für die virtuelle Smartcard angeben, als ob es sich um eine physikalische Smartcard

handelt, um sich bei der Domäne anzumeldet.

In der Praxis ist dies so einfach wie das Eingeben eines Kennworts für den Zugriff auf das System. Technisch gesehen ist es weitaus sicherer. Die Verwendung der virtuellen Smartcard für den Zugriff auf das System erweist sich in der Domäne, dass der Benutzer, der die Authentifizierung beantragt, über den Personal Computer verfügt, auf dem die Karte bereitgestellt wurde, und die virtuelle Smartcard-PIN kennt. Da diese Anforderung möglicherweise nicht von einem anderen System als dem System stammt, das von der Domäne für den Zugriff dieses Benutzers zertifiziert wurde, und der Benutzer die Anforderung nicht ohne Kenntnis der PIN initiiert haben konnte, wird eine starke zweistufige Authentifizierung eingerichtet.

Client Authentifizierung

Virtuelle Smartcards können auch mithilfe von Secure Socket Layer (SSL) oder einer ähnlichen Technologie für die Clientauthentifizierung verwendet werden. Ähnlich wie der Domänenzugriff mit einer virtuellen Smartcard kann ein Authentifizierungszertifikat für die virtuelle Smartcard bereitgestellt werden, die für einen Remotedienst bereitgestellt wird, wie im Client Authentifizierungsprozess angefordert. Dies entspricht den Grundsätzen der zweistufigen Authentifizierung, da auf das Zertifikat nur von dem Computer aus zugegriffen werden kann, auf dem die virtuelle Smartcard gehostet wird, und der Benutzer muss die PIN für den ersten Zugriff auf die Karte eingeben.

Virtuelle Smartcard-Umleitung für Remotedesktopverbindungen

Das Konzept der zweistufigen Authentifizierung, das mit virtuellen Smartcards verbunden ist, basiert auf der Nähe der Benutzer zu den Computern, über die Sie auf Domänenressourcen zugreifen. Wenn ein Benutzer eine Remoteverbindung mit einem Computer herstellt, auf dem virtuelle Smartcards gehostet werden, können die virtuellen Smartcards, die sich auf dem Remotecomputer befinden, daher während der Remotesitzung nicht verwendet werden. Die virtuellen Smartcards, die auf dem Verbindungs Computer gespeichert sind (die unter physischer Kontrolle des Benutzers liegen), werden jedoch auf den Remotecomputer geladen, und Sie können so verwendet werden, als ob Sie mithilfe des TPM des Remotecomputers installiert wurden. Dadurch werden die Berechtigungen eines Benutzers für den Remotecomputer erweitert, wobei die Grundsätze der zweistufigen Authentifizierung beibehalten werden.

Windows to go und virtuelle Smartcards

Virtuelle Smartcards funktionieren gut mit Windows to go, in dem ein Benutzer von einem kompatiblen Wechselspeichergerät in eine unterstützte Version von Windows booten kann. Für den Benutzer kann eine virtuelle Smartcard erstellt und an das TPM auf dem physikalischen Hostcomputer gebunden werden, mit dem das Wechselmedium verbunden ist. Wenn der Benutzer das Betriebssystem von einem anderen physikalischen Computer bootet, ist die virtuelle Smartcard nicht verfügbar. Dies kann für Szenarien verwendet werden, in denen ein einzelner physischer Computer von vielen Benutzern freigegeben wird. Jedem Benutzer kann ein Wechselspeichergerät für Windows to go zugewiesen werden, für das eine virtuelle Smartcard für den Benutzer bereitgestellt wurde. Auf diese Weise können Benutzer nur auf Ihre persönliche virtuelle Smartcard zugreifen.

Vertraulichkeits Use Cases

S/MIME-e-Mail-Verschlüsselung

Physische Smartcards sind für private Schlüssel vorgesehen, die für die e-Mail-Verschlüsselung und-Entschlüsselung verwendet werden können. Diese Funktionalität ist auch in virtuellen Smartcards vorhanden. Durch die Verwendung von S/MIME mit dem öffentlichen Schlüssel des Benutzers zum Verschlüsseln von e-Mails kann der Absender einer e-Mail sicher sein, dass nur die Person mit dem zugehörigen privaten Schlüssel die e-Mail entschlüsseln kann. Diese Zusicherung ist ein Ergebnis der nicht exportierbaren privaten Schlüssel. Sie ist nie innerhalb der Reichweite von Schadsoftware vorhanden und bleibt durch das TPM geschützt – auch während der Entschlüsselung.

BitLocker für Daten-Volumes

Die sBitLocker-Laufwerk Verschlüsselungstechnologie nutzt symmetrische Schlüssel Verschlüsselung, um den

Inhalt der Festplatte eines Benutzers zu schützen. Dadurch wird sichergestellt, dass ein Gegner nicht in der Lage ist, Daten vom Laufwerk zu lesen, wenn der physische Besitz einer Festplatte beeinträchtigt wird. Der Schlüssel, der zum Verschlüsseln des Laufwerks verwendet wird, kann in einer virtuellen Smartcard gespeichert werden, die Kenntnisse über die virtuelle Smartcard-PIN benötigt, um auf das Laufwerk und den Besitz des Computers zuzugreifen, auf dem die virtuelle TPM-Smartcard gehostet wird. Wenn das Laufwerk ohne Zugriff auf das TPM abgerufen wird, das die virtuelle Smartcard hostet, ist jeder Brute-Force-Angriff sehr schwierig.

BitLocker kann auch verwendet werden, um tragbare Laufwerke zu verschlüsseln, wozu die Speicherung von Schlüsseln in virtuellen Smartcards gehört. In diesem Szenario (im Gegensatz zur Verwendung von BitLocker mit einer physischen Smartcard) kann das verschlüsselte Laufwerk nur verwendet werden, wenn es mit dem Host für die virtuelle Smartcard verbunden ist, die zum Verschlüsseln des Laufwerks verwendet wird, da der BitLocker-Schlüssel nur von diesem Computer aus zugänglich ist. Diese Methode kann jedoch hilfreich sein, um die Sicherheit von Backup-Laufwerken und persönlichen Speicher außerhalb der Hauptfestplatte zu gewährleisten.

Anwendungsfall der Datenintegrität

Signieren von Daten

Um die Autorschaft von Daten zu überprüfen, kann ein Benutzer ihn unter Verwendung eines privaten Schlüssels signieren, der auf der virtuellen Smartcard gespeichert ist. Digitale Signaturen bestätigen die Integrität und den Ursprung der Daten. Wenn der Schlüssel in einem verfügbaren Betriebssystem gespeichert ist, kann ein böswilliger Benutzer darauf zugreifen und ihn zum Ändern bereits signierter Daten oder zum Spoofing der Identität des Schlüsselbesitzers verwenden. Wenn dieser Schlüssel jedoch auf einer virtuellen Smartcard gespeichert ist, kann er nur zum Signieren von Daten auf dem Hostcomputer verwendet werden. Sie kann nicht auf andere Systeme (absichtlich oder unbeabsichtigt, beispielsweise mit Malware Diebstahl) exportiert werden. Auf diese Weise sind digitale Signaturen weitaus sicherer als andere Methoden für den privaten Schlüsselspeicher.

Neue und geänderte Funktionen ab Windows 8,1

Verbesserungen in Windows 8,1 ermöglichten Entwicklern, Microsoft Store-Apps zum Erstellen und Verwalten virtueller Smartcards zu erstellen.

Die DCOM-Schnittstellen für das TPM-Protokoll Device Management Protocol (Trusted Platform Module) bieten eine DCOM-Remote Protokollschnittstelle, die zum Erstellen und Vernichten virtueller Smartcards verwendet wird. Bei einer virtuellen Smartcard handelt es sich um ein Gerät, das eine Geräteschnittstelle darstellt, die mit der PC/SC-Spezifikation für PC-angeschlossene Schnittstellengeräte mit der Betriebssystemplattform (Host Operating System) konform ist. Dieses Protokoll übernimmt nichts über die zugrunde liegende Implementierung von virtuellen Smartcard-Geräten. Insbesondere ist es zwar in erster Linie für die Verwaltung virtueller Smartcards basierend auf TPMs vorgesehen, kann aber auch zum Verwalten anderer Typen virtueller Smartcards verwendet werden.

Welchen Nutzen bietet diese Änderung?

Ab Windows 8,1 können Anwendungsentwickler in Ihre apps die folgenden virtuellen Smartcard-Wartungsfunktionen einbauen, um einen Teil ihrer administrativen Lasten zu verringern.

- Erstellen Sie eine neue virtuelle Smartcard, oder wählen Sie eine virtuelle Smartcard aus der Liste der verfügbaren virtuellen Smartcards im System aus. Ermitteln Sie die Person, mit der die Anwendung arbeiten soll.
- Personalisieren der virtuellen Smartcard
- Ändern Sie den Administrator-Schlüssel.
- Diversifizieren Sie den Administrator-Schlüssel, der es dem Benutzer ermöglicht, die PIN in einem Szenario mit PIN-Blockierung aufzuheben.
- Ändern Sie die PIN.

- Zurücksetzen oder Entsperren der PIN
- Zerstören Sie die virtuelle Smartcard.

Worin bestehen die Unterschiede?

Ab Windows 8,1 können Microsoft Store-App-Entwickler apps erstellen, die den Benutzer zum Zurücksetzen oder Aufheben der Blockierung sowie zum Ändern einer virtuellen Smartcard-PIN auffordern. Dadurch wird dem Benutzer mehr Verantwortung für die Verwaltung der virtuellen Smartcard zugewiesen, er kann aber auch eine konsistentere Benutzererfahrung und Verwaltungserfahrung in Ihrer Organisation bereitstellen.

Weitere Informationen zum Entwickeln von Microsoft Store-Apps mit diesen Funktionen finden Sie unter [Virtuelles Smartcard-Verwaltungsprotokoll für Trusted Platform Module](#).

Weitere Informationen zum Verwalten dieser Funktionen in virtuellen Smartcards finden Sie unter [Grundlegendes zu virtuellen Smartcards und auswerten](#).

Hardwareanforderungen

Um die virtuelle Smartcard-Technologie verwenden zu können, muss TPM 1,2 für Computer mit Windows 10 oder Windows Server 2016 mindestens erforderlich sein.

Softwareanforderungen

Um die virtuelle Smartcard-Technologie verwenden zu können, müssen auf Computern eines der folgenden Betriebssysteme ausgeführt werden:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 10
- Windows8.1
- Windows 8

Weitere Informationen:

- [Grundlagen und Evaluierung virtueller Smartcards](#)
- [Erste Schritte mit virtuellen Smartcards: Handbuch mit exemplarischer Vorgehensweise](#)
- [Verwenden virtueller Smartcards](#)
- [Bereitstellen virtueller Smartcards](#)
- [Bewerten der Sicherheit virtueller Smartcards](#)
- [Tpmvscmgr](#)

Grundlagen und Evaluierung virtueller Smartcards

04.01.2020 • 13 minutes to read

Gilt für: Windows 10, Windows Server 2016

Dieses Thema für IT-Experten beschreibt die von Microsoft entwickelte virtuelle Smartcard-Technologie. schlägt vor, wie es in Ihr Authentifizierungs Design passen kann. und enthält Links zu weiteren Ressourcen, die Sie zum Entwerfen, bereitstellen und behandeln von virtuellen Smartcards verwenden können.

Bei der virtuellen Smartcard-Technologie werden kryptografische Schlüssel verwendet, die auf Computern gespeichert sind, auf denen das TPM (Trusted Platform Module) installiert ist. Virtuelle Smartcards bieten mit zweistufiger Authentifizierung vergleichbare Sicherheitsvorteile für herkömmliche Smartcards. Die Technologie bietet auch mehr Benutzerfreundlichkeit und geringere Kosten für die Bereitstellung. Durch die Verwendung von TPM-Geräten, die die gleichen kryptografischen Funktionen wie herkömmliche Smartcards bereitstellen, führen virtuelle Smartcards die drei wichtigsten Eigenschaften aus, die für Smartcards erwünscht sind: keine Exportfähigkeit, isolierte Kryptografie und Anti-Hämmern.

Virtuelle Smartcards funktionieren ähnlich wie physische Smartcards. Sie werden als immer eingefügte Smartcards angezeigt, und Sie können für die Authentifizierung für externe Ressourcen, den Datenschutz durch sichere Verschlüsselung und die Integrität durch zuverlässige Signierung verwendet werden. Da die TPM-fähige Hardware leicht verfügbar ist und virtuelle Smartcards problemlos mithilfe vorhandener Zertifikatregistrierungsmethoden bereitgestellt werden können, können virtuelle Smartcards zu einem vollständigen Ersatz für andere Methoden der starken Authentifizierung in einer Unternehmenseinstellung werden. beliebiger Skalierung.

Dieses Thema enthält die folgenden Abschnitte:

- [Vergleich virtueller Smartcards mit physischen Smartcards](#): vergleicht Eigenschaften, Funktionsaspekte, Sicherheit und Kosten.
- [Authentifizierungs Entwurfsoptionen](#): Beschreibt, wie Kennwörter, Smartcards und virtuelle Smartcards zum Erreichen von Authentifizierungs Zielen in Ihrer Organisation verwendet werden können.
- [Siehe auch](#): Links zu anderen Themen, die Ihnen beim Entwerfen, bereitstellen und behandeln von virtuellen Smartcards helfen können.

Vergleich virtueller Smartcards mit physischen Smartcards

Virtuelle Smartcards funktionieren ähnlich wie physische Smartcards, unterscheiden sich jedoch dadurch, dass Sie private Schlüssel schützen, indem Sie das TPM des Computers anstelle von Smartcard-Medien verwenden.

Eine virtuelle Smartcard wird Anwendungen als herkömmliche Smartcard angezeigt. Private Schlüssel auf der virtuellen Smartcard sind geschützt, nicht durch Isolierung des physikalischen Speichers, sondern durch die kryptografischen Funktionen des TPM. Alle vertraulichen Informationen werden mit dem TPM verschlüsselt und dann auf der Festplatte in verschlüsselter Form gespeichert.

Alle kryptografischen Vorgänge erfolgen in der sicheren, isolierten Umgebung des TPM, und die unverschlüsselten privaten Schlüssel werden niemals außerhalb dieser Umgebung verwendet. So wie physische Smartcards bleiben virtuelle Smartcards vor jeder Malware auf dem Host sicher. Wenn die Festplatte in irgendeiner Weise gefährdet ist, kann ein böswilliger Benutzer auch nicht auf Schlüssel zugreifen, die auf der virtuellen Smartcard gespeichert sind, da Sie mit dem TPM sicher verschlüsselt sind. Schlüssel können auch durch die BitLocker-Laufwerkverschlüsselung geschützt werden.

Virtuelle Smartcards verwalten die drei wichtigsten Eigenschaften von physikalischen Smartcards:

- **Nicht exportierbare Daten:** da alle privaten Informationen auf der virtuellen Smartcard mithilfe des TPM auf dem Hostcomputer verschlüsselt werden, können Sie nicht auf einem anderen Computer mit einem anderen TPM verwendet werden. Darüber hinaus sind TPMs so konzipiert, dass Sie manipulationssicher und nicht exportierbar sind, sodass ein böswilliger Benutzer kein identisches TPM zurückentwickeln oder dasselbe TPM auf einem anderen Computer installieren kann. Weitere Informationen finden Sie unter [bewerten der virtuellen Smartcard-Sicherheit](#).
- **Isolierte Kryptografie:** TPMs bietet dieselben Eigenschaften der isolierten Kryptografie, die von physischen Smartcards bereitgestellt werden, und wird von virtuellen Smartcards verwendet. Unverschlüsselte Kopien privater Schlüssel werden nur innerhalb des TPM und nie in den Arbeitsspeicher geladen, auf den das Betriebssystem zugreifen kann. Alle kryptografischen Vorgänge mit diesen privaten Schlüsseln treten innerhalb des TPM auf.
- **Anti-hämmern:** Wenn ein Benutzer eine PIN falsch eingibt, reagiert die virtuelle Smartcard mithilfe der antihämmer-Logik des TPMs, die weitere Versuche für einen bestimmten Zeitraum ablehnt, anstatt die Karte zu blockieren. Dies wird auch als "Lockout" bezeichnet. Weitere Informationen finden Sie unter [bewerten der virtuellen Smartcard-Sicherheit](#).

Die folgenden Unterabschnitte vergleichen die Funktionalität, Sicherheit und Kosten von virtuellen Smartcards und physischen Smartcards.

Funktion

Das von Microsoft entworfene virtuelle Smartcard-System ahmt die Funktionalität herkömmlicher Smartcards genau nach. Der bemerkenswerteste Unterschied für den Endbenutzer besteht darin, dass die virtuelle Smartcard im Wesentlichen eine Smartcard ist, die immer in den Computer eingefügt wird. Es gibt keine Methode zum Exportieren der virtuellen Smartcard des Benutzers zur Verwendung auf anderen Computern, was zur Sicherheit virtueller Smartcards beiträgt. Wenn ein Benutzer Zugriff auf Netzwerkressourcen auf mehreren Computern benötigt, können mehrere virtuelle Smartcards für diesen Benutzer ausgestellt werden. Darüber hinaus kann ein Computer, der von mehreren Benutzern gemeinsam genutzt wird, mehrere virtuelle Smartcards für verschiedene Benutzer hosten.

Die grundlegende Benutzeroberfläche für eine virtuelle Smartcard ist so einfach wie die Verwendung eines Kennworts für den Zugriff auf ein Netzwerk. Da die Smartcard standardmäßig geladen wird, muss der Benutzer einfach die PIN eingeben, die an die Karte gebunden ist, um Zugriff zu erhalten. Die Benutzer sind nicht mehr verpflichtet, Karten und Leser zu tragen oder physische Maßnahmen zur Nutzung der Karte zu ergreifen.

Obwohl die antihämmerfunktion der virtuellen Smartcard ebenso sicher ist wie eine physische Smartcard, müssen virtuelle Smartcard-Benutzer niemals einen Administrator kontaktieren, um die Blockierung der Karte zu blockieren. Stattdessen warten Sie einfach einen bestimmten Zeitraum (abhängig von den TPM-Spezifikationen), bevor Sie erneut versuchen, die PIN einzugeben. Alternativ kann der Administrator die Sperrung zurücksetzen, indem er dem TPM auf dem Hostcomputer Besitzer Authentifizierungsdaten bereitstellt.

Sicherheit

Physische Smartcards und virtuelle Smartcards bieten vergleichbare Sicherheitsstufen. Beide implementieren zweistufige Authentifizierung für die Verwendung von Netzwerkressourcen. Sie unterscheiden sich jedoch in bestimmten Aspekten, einschließlich physischer Sicherheit und der Praktikabilität eines Angriffs. Aufgrund ihres kompakten und tragbaren Designs werden herkömmliche Smartcards am häufigsten in engem Kontakt mit dem beabsichtigten Nutzer gehalten. Sie bieten kaum Möglichkeiten für den Kauf eines potenziellen Gegners, sodass jede Art von Interaktion mit der Karte schwierig ist, ohne eine Vielzahl von Diebstählen zu verpflichten.

Virtuelle TPM-Smartcards befinden sich jedoch auf dem Computer eines Benutzers, der häufig unbeaufsichtigt bleiben kann, wodurch eine Möglichkeit für böswillige Benutzer zum Hämmern des TPMs bietet. Obwohl virtuelle Smartcards vollständig vor dem hämmern geschützt sind (ebenso wie physische Smartcards), macht diese

Barrierefreiheit die Logistik eines Angriffs etwas einfacher. Darüber hinaus unterscheidet sich das antihämmerverfahren einer TPM-Smartcard dadurch, dass es lediglich eine Zeitverzögerung als Reaktion auf wiederholte Pin-Fehler darstellt, im Gegensatz zur vollständigen Blockierung des Benutzers.

Es gibt jedoch mehrere Vorteile, die virtuelle Smartcards bieten, um diese geringen Sicherheitslücken zu verringern. Am wichtigsten ist, dass eine virtuelle Smartcard viel seltener verloren geht. Virtuelle Smartcards sind in Computer und Geräte integriert, die der Benutzer bereits für andere Zwecke besitzt und die für einen sicheren Schutz sorgen. Wenn der Computer oder das Gerät, auf dem sich die virtuelle Smartcard befindet, verloren geht oder gestohlen wird, kann der Benutzer den Verlust eines physischen Smartcards mehr sofort feststellen. Wenn ein Computer oder Gerät als verloren erkannt wird, kann der Benutzer den Administrator des Systems Benachrichtigen, der das Zertifikat widerrufen kann, das der virtuellen Smartcard auf diesem Gerät zugeordnet ist. Dies schließt jeglichen zukünftigen unbefugten Zugriff auf diesem Computer oder Gerät aus, wenn die PIN für die virtuelle Smartcard beeinträchtigt wird.

Kosten

Wenn ein Unternehmen physische Smartcards bereitstellen möchte, müssen Sie Smartcards und Smartcard-Leser für alle Mitarbeiter erwerben. Obwohl relativ kostengünstige Optionen gefunden werden können, sind Optionen, die die drei wichtigsten Eigenschaften von Smartcard-Sicherheit (insbesondere die Nichtexportierbarkeit) sicherstellen, teurer. Wenn Mitarbeiter über Computer mit integriertem TPM verfügen, können virtuelle Smartcards ohne zusätzliche Materialkosten bereitgestellt werden. Diese Computer und Geräte sind im Markt relativ üblich.

Darüber hinaus sind die Wartungskosten virtueller Smartcards kleiner als die für physische Smartcards, die einfach verloren gehen, gestohlen oder vom normalen Verschleiß beschädigt werden. Virtuelle TPM-Smartcards gehen nur verloren, wenn der Hostcomputer oder das Gerät verloren geht oder beschädigt ist, was in den meisten Fällen viel seltener der Fall ist.

Vergleichszusammenfassung

PHYSISCHE SMARTCARDS	VIRTUELLE TPM-SMARTCARDS
Schützt private Schlüssel mithilfe der integrierten kryptografischen Funktionalität der Karte.	Schützt private Schlüssel mithilfe der kryptografischen Funktionalität des TPM.
Speichert private Schlüssel in isoliertem, nicht flüchtigem Speicher auf der Karte, was bedeutet, dass der Zugriff auf private Schlüssel nur von der Karte erfolgt und der Zugriff auf das Betriebssystem nie gestattet ist.	Speichert verschlüsselte private Schlüssel auf der Festplatte. Durch die Verschlüsselung wird sichergestellt, dass diese Schlüssel nur im TPM entschlüsselt und verwendet werden können, nicht im barrierefreien Arbeitsspeicher des Betriebssystems.
Gewährleistet die Nichtexportierbarkeit über den Kartenhersteller, der die Isolierung privater Informationen vom Zugriff auf das Betriebssystem umfasst.	Gewährleistet keine Exportfähigkeit über den TPM-Hersteller, der die Unfähigkeit eines Gegners zum Replizieren oder Entfernen des TPMs umfasst.
Führt und isoliert kryptografische Vorgänge innerhalb der integrierten Funktionen der Karte.	Führt und trennt kryptografische Vorgänge im TPM des Computers oder Geräts des Benutzers.
Bietet Anti-hämmern über die Karte. Nach einer bestimmten Anzahl von fehlgeschlagenen PIN-Eingabeversuchen blockiert die Karte weiteren Zugriff, bis eine administrative Aktion ausgeführt wird.	Bietet Anti-hämmern über das TPM. Bei aufeinander folgenden fehlgeschlagenen versuchen wird die Geräte Sperr Zeit erhöht (die Zeit, die der Benutzer warten muss, bevor er erneut versucht). Dies kann von einem Administrator zurückgesetzt werden.
Setzt voraus, dass Benutzer Ihre Smartcard und ihren Smartcard-Leser für den Zugriff auf Netzwerkressourcen mit sich führen.	Ermöglicht Benutzern den Zugriff auf Ihre TPM-fähigen Computer oder Geräte und den Zugriff auf das Netzwerk ohne zusätzliche Geräte.

PHYSISCHE SMARTCARDS	VIRTUELLE TPM-SMARTCARDS
Ermöglicht die Portabilität von Anmeldeinformationen, indem die Smartcard in Smartcard-Leser eingefügt wird, die an andere Computer angefügt sind.	Verhindert das Exportieren von Anmeldeinformationen von einem bestimmten Computer oder Gerät. Virtuelle Smartcards können jedoch mithilfe zusätzlicher Zertifikate für denselben Benutzer auf mehreren Computern oder Geräten ausgestellt werden.
Ermöglicht es mehreren Benutzern, über denselben Computer auf Netzwerkressourcen zuzugreifen, indem Sie Ihre persönlichen Smartcards einfügen.	Ermöglicht es mehreren Benutzern, über denselben Computer oder ein Gerät auf Netzwerkressourcen zuzugreifen, indem Sie für jeden Benutzer auf diesem Computer oder Gerät eine virtuelle Smartcard ausgeben.
Erfordert, dass der Benutzer die Karte trägt, wodurch es für einen Angreifer erschwert wird, auf das Gerät zuzugreifen und einen Hämmervorgang zu starten.	Speichert die virtuelle Smartcard auf dem Computer des Benutzers, die möglicherweise unbeaufsichtigt bleibt und ein größeres Risiko Fenster für das Hämmern von versuchen ermöglicht.
Stellt ein im allgemeinen einmaliges Gerät bereit, das explizit zum Zweck der Authentifizierung durchgeführt wird. Die Smartcard kann problemlos verlegt oder vergessen werden.	Installiert die virtuelle Smartcard auf einem Gerät, das anderen Zwecken für den Benutzer dient, damit der Benutzer mehr Anreiz hat, für den Computer oder das Gerät verantwortlich zu sein.
Benachrichtigt Benutzer, dass Ihre Karte verloren geht oder gestohlen wird, wenn Sie sich anmelden müssen und feststellen, dass Sie nicht vorhanden ist.	Installiert die virtuelle Smartcard auf einem Gerät, das der Benutzer wahrscheinlich zu anderen Zwecken benötigt, damit die Benutzer den Verlust viel schneller feststellen können. Dadurch wird das zugeordnete Risiko Fenster reduziert.
Verlangt von Unternehmen, in Smartcards und Smartcard-Leser für alle Mitarbeiter zu investieren.	Erfordert, dass Unternehmen sicherstellen, dass alle Mitarbeiter über TPM-fähige Computer verfügen, die relativ häufig sind.
Ermöglicht die Verwendung einer Richtlinie zum Entfernen von Smartcards, um das Verhalten des Systems beim Entfernen der Smartcard zu beeinflussen. Beispielsweise kann die Richtlinie diktieren, ob die Anmeldesitzung des Benutzers gesperrt oder beendet wird, wenn der Benutzer die Karte entfernt.	Beseitigt die Notwendigkeit einer Richtlinie für die Smartcard-Entfernung, da eine virtuelle TPM-Smartcard immer vorhanden ist und nicht vom Computer entfernt werden kann.

Optionen für das Authentifizierungs Design

Im folgenden Abschnitt werden verschiedene häufig verwendete Optionen und ihre jeweiligen Stärken und Schwächen vorgestellt, die Organisationen für die Authentifizierung in Frage stellen können.

Kennwörter

Bei einem Kennwort handelt es sich um eine geheime Zeichenfolge, die mit den Identifikations Anmeldeinformationen für das Konto eines Benutzers verknüpft ist. Dadurch wird die Identität des Benutzers festgelegt. Obwohl Kennwörter die am häufigsten verwendete Form der Authentifizierung sind, sind Sie auch die schwächsten. In einem System, in dem Kennwörter als alleinige Methode zur Benutzerauthentifizierung verwendet werden, gelten nur Personen, die ihre Kennwörter kennen, als gültige Benutzer.

Die Kennwortauthentifizierung legt dem Benutzer eine große Verantwortung. Kennwörter müssen hinreichend komplex sein, damit Sie nicht einfach zu erraten sind, aber Sie müssen einfach genug sein, um in den Arbeitsspeicher zu übertragen und nicht an einem physikalischen Ort gespeichert zu werden. Auch wenn dieses Gleichgewicht erfolgreich erreicht wird, gibt es eine Vielzahl von Angriffen (wie Brute-Force-Angriffe, Lauschangriffe und Social-Engineering-Taktiken), in denen ein böswilliger Benutzer das Kennwort eines Benutzers erwerben und die Identität dieser Person annehmen kann. Ein Benutzer wird häufig nicht erkennen, dass das

Kennwort kompromittiert wurde, wodurch es für böswillige Benutzer einfach ist, den Zugriff auf ein System aufrechtzuerhalten, wenn ein gültiges Kennwort abgerufen wurde.

Einmalkennwörter

Ein Einmalkennwort (OTP) ähnelt einem herkömmlichen Kennwort, ist aber sicherer, da es nur einmal zur Authentifizierung eines Benutzers verwendet werden kann. Die Methode zum Ermitteln jedes neuen Kennworts variiert je nach Implementierung. Wenn jedoch eine sichere Bereitstellung jedes neuen Kennworts vorliegt, hat OTPs gegenüber dem klassischen Kennwortmodell der Authentifizierung mehrere Vorteile. Besonders wichtig: Wenn ein bestimmtes OTP-Token in der Übertragung zwischen dem Benutzer und dem System abgefangen wird, kann der Interceptor es nicht für zukünftige Transaktionen verwenden. Wenn ein böswilliger Benutzer das OTP eines gültigen Benutzers erhält, hat der Interceptor auf ähnliche Weise nur Zugriff auf das System (nur eine Sitzung).

Smartcards

Smartcards sind physikalische Authentifizierungsgeräte, die das Konzept eines Kennworts verbessern, indem Sie festlegen, dass Benutzer tatsächlich über Ihr Smartcard-Gerät verfügen, um auf das System zuzugreifen, und außerdem die PIN kennen, die Zugriff auf die Smartcard bietet. Smartcards verfügen über drei wichtige Eigenschaften, die zur Wahrung ihrer Sicherheit beitragen:

- **Nicht exportierbare Daten:** auf der Karte gespeicherte Informationen, beispielsweise die privaten Schlüssel des Benutzers, können nicht von einem Gerät extrahiert und in einem anderen Medium verwendet werden.
- **Isolierte Kryptografie:** alle kryptografischen Vorgänge, die mit der Karte verknüpft sind (wie sichere Verschlüsselung und Entschlüsselung von Daten), treten in einem kryptografischen Prozessor auf der Karte auf, sodass die Transaktionen nicht von bössartiger Software auf dem Hostcomputer beobachtet werden können.
- **Anti-hämmern:** um den Zugriff auf die Karte durch einen Brute-Force-Angriff zu verhindern, blockiert eine festgelegte Anzahl aufeinanderfolgender erfolgloser PIN-Eingabeversuche die Karte, bis eine administrative Aktion ausgeführt wird.

Smartcards bieten eine erheblich verbesserte Sicherheit für Kennwörter allein, da es für böswillige Benutzer viel schwieriger ist, den Zugriff auf ein System zu erhalten und zu verwalten. Vor allem erfordert der Zugriff auf ein Smartcardsystem, dass Benutzer über eine gültige Karte verfügen und dass Sie die PIN kennen, die den Zugriff auf diese Karte ermöglicht. Es ist extrem schwierig für einen Dieb, die Karte und die PIN zu erwerben.

Zusätzliche Sicherheit wird durch die singuläre Art der Karte erreicht, da nur eine Kopie der Karte vorhanden ist, nur eine Person die Anmeldeinformationen verwenden kann, und die Benutzer werden schnell feststellen, ob die Karte verloren gegangen oder gestohlen wurde. Dadurch wird das Risiko Fenster des Diebstahls von Anmeldeinformationen im Vergleich zur Verwendung eines Kennworts erheblich reduziert.

Diese zusätzliche Sicherheit ist leider mit zusätzlichen Material- und Supportkosten verbunden. Herkömmliche Smartcards sind teuer zu kaufen (Karten- und Kartenleser müssen den Mitarbeitern zur Verfügung gestellt werden), und Sie können auch problemlos verlegt oder gestohlen werden.

Virtuelle Smartcards

Um diese Probleme zu beheben, emulieren virtuelle Smartcards die Funktionalität herkömmlicher Smartcards, doch anstatt den Kauf zusätzlicher Hardware zu erfordern, verwenden Sie Technologien, die Benutzer bereits besitzen und mit denen Sie häufiger zu tun haben. Theoretisch kann jedes Gerät, das die drei wichtigsten Eigenschaften von Smartcards bereitstellen kann (keine Exportmöglichkeit, isolierte Kryptografie und Anti-hämmern), als virtuelle Smartcard in Auftrag gegeben werden. Die von Microsoft entwickelte virtuelle Smartcard-Plattform ist derzeit jedoch auf die Verwendung des TPM-Chips (Trusted Platform Module) limitiert, der auf den meisten modernen Computern installiert ist.

Virtuelle Smartcards, die ein TPM verwenden, bieten die drei wichtigsten Sicherheitsprinzipien herkömmlicher Smartcards (Nichtexportierbarkeit, isolierte Kryptografie und Anti-hämmern). Außerdem sind Sie günstiger zu implementieren und für Benutzer bequemer. Da viele Unternehmens Computer bereits über ein integriertes TPM verfügen, sind beim Kauf neuer Hardware keine Kosten verbunden. Der Besitz des Benutzers an einem Computer oder Gerät entspricht dem Besitz einer Smartcard, und die Identität eines Benutzers kann von keinem anderen Computer oder Gerät ohne administrative Bereitstellung weiterer Anmeldeinformationen übernommen werden. Daher wird die zweistufige Authentifizierung erreicht, da der Benutzer über einen Computer verfügen muss, der mit einer virtuellen Smartcard eingerichtet ist und die PIN für die Verwendung der virtuellen Smartcard kennt.

Weitere Informationen:

- [Erste Schritte mit virtuellen Smartcards: Handbuch mit exemplarischer Vorgehensweise](#)
- [Verwenden virtueller Smartcards](#)
- [Bereitstellen virtueller Smartcards](#)
- [Bewerten der Sicherheit virtueller Smartcards](#)

Erste Schritte mit virtuellen Smartcards: Handbuch mit exemplarischer Vorgehensweise

12.09.2019 • 5 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten wird beschrieben, wie Sie eine grundlegende Testumgebung für die Verwendung von virtuellen TPM-Smartcards einrichten.

Virtuelle Smartcards sind eine Technologie von Microsoft, die vergleichbare Sicherheitsvorteile bei der zweistufigen Authentifizierung für physische Smartcards bietet. Darüber hinaus bieten Sie mehr Benutzerfreundlichkeit und geringere Kosten für Organisationen zur Bereitstellung. Durch die Verwendung von TPM-Geräten (Trusted Platform Module), die die gleichen kryptografischen Funktionen wie physische Smartcards bereitstellen, führen virtuelle Smartcards die drei wichtigsten Eigenschaften aus, die von Smartcards gewünscht werden: keine Exportfähigkeit, isolierte Kryptografie und Anti-Hämmern.

Diese schrittweise Anleitung zeigt, wie Sie eine grundlegende Testumgebung für die Verwendung von virtuellen TPM-Smartcards einrichten. Nach Abschluss dieser exemplarischen Vorgehensweise haben Sie eine funktionelle virtuelle Smartcard auf dem Windows-Computer installiert.

Zeitanforderungen

Sie sollten in der Lage sein, diese exemplarische Vorgehensweise in weniger als einer Stunde abzuschließen, ohne Software zu installieren und die Testdomäne einzurichten.

Exemplarische Vorgehensweisen

- [Voraussetzungen](#)
- [Schritt 1: Erstellen der Zertifikatvorlage](#)
- [Schritt 2: Erstellen der virtuellen TPM-Smartcard](#)
- [Schritt 3: Registrieren des Zertifikats auf der virtuellen TPM-Smartcard](#)

**** Wichtig diese grundlegende Konfiguration dient nur zu Testzwecken. Sie ist nicht für die Verwendung in einer Produktionsumgebung vorgesehen.

Voraussetzungen

Sie benötigen:

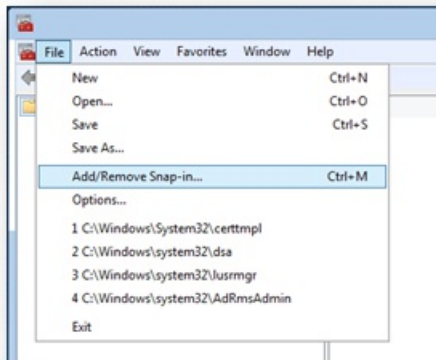
- Ein Computer unter Windows 10 mit einem installierten und voll funktionsfähigen TPM (Version 1,2 oder Version 2,0).
- Eine Testdomäne, zu der der oben aufgeführte Computer verknüpft werden kann.
- Zugriff auf einen Server in dieser Domäne mit einer vollständig installierten und ausgeführten Zertifizierungsstelle (Certification Authority, ca).

Schritt 1: Erstellen der Zertifikatvorlage

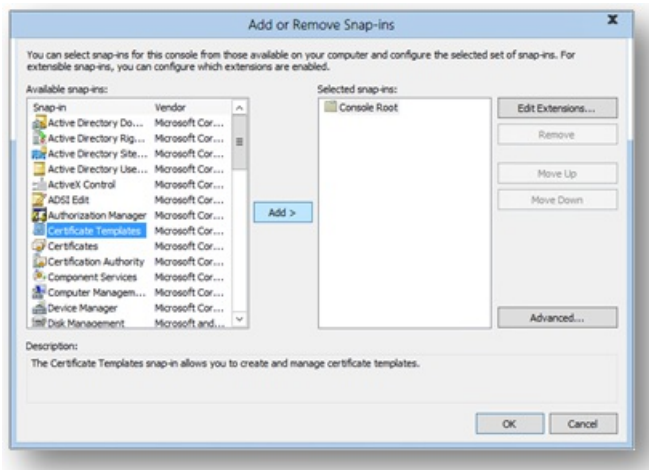
Auf dem Domänenserver müssen Sie eine Vorlage für das Zertifikat erstellen, das Sie für die virtuelle Smartcard anfordern werden.

So erstellen Sie die Zertifikatvorlage

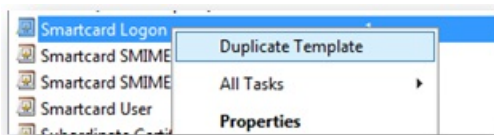
1. Öffnen Sie auf dem Server die Microsoft Management Console (MMC). Eine Möglichkeit besteht darin, im **Startmenü MMC.exe** einzugeben, mit der rechten Maustaste auf **MMC.exe** zu klicken und dann auf **als Administrator ausführen** zu klicken.
2. Klicken Sie auf **Datei** und dann auf **Snap-In hinzufügen/entfernen**.



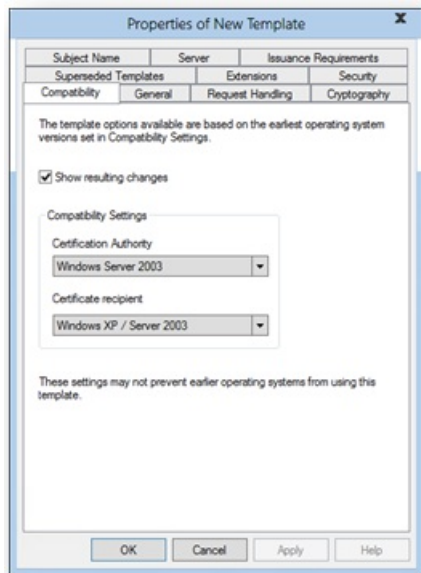
3. Klicken Sie in der Liste Verfügbare Snap-Ins auf **Zertifikatvorlagen**, und klicken Sie dann auf **Hinzufügen**.



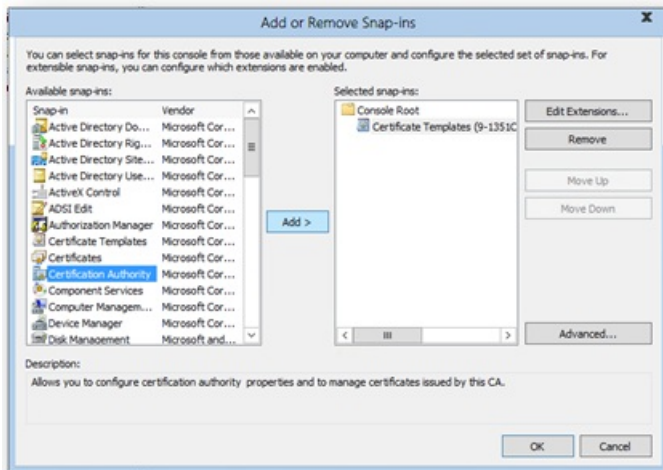
4. Zertifikatvorlagen befindet sich jetzt unter **Konsolenstamm** in der MMC. Doppelklicken Sie darauf, um alle verfügbaren Zertifikatvorlagen anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf die **Smartcard-Anmelde** Vorlage, und klicken Sie auf **Vorlage duplizieren**.



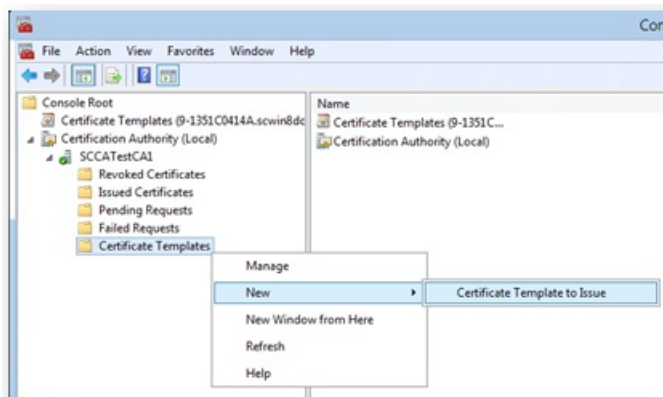
6. Überprüfen Sie auf der Registerkarte **Kompatibilität** unter **Zertifizierungsstelle** die Auswahl, und ändern Sie sie bei Bedarf.



7. Auf der Registerkarte "**Allgemein**":
 - a. Geben Sie einen Namen wie die **virtuelle TPM-Smartcard-Anmeldungen**.
 - b. Stellen Sie den Gültigkeitszeitraum auf den gewünschten Wert ein.
8. Auf der Registerkarte "**Anforderungsbehandlung**":
 - a. Stellen Sie den **Zweck** auf **Signatur und Smartcard-Anmeldung** ein.
 - b. Klicken Sie auf **Benutzer während der Registrierung auffordern**.
9. Klicken Sie auf der Registerkarte **Kryptografie** auf:
 - a. Setzen Sie die minimale Schlüsselgröße auf 2048.
 - b. Klicken Sie auf **Anforderungen müssen einen der folgenden Anbieter verwenden**, und wählen Sie dann **Microsoft Base Smartcard Crypto-Anbieter** aus.
10. Fügen Sie auf der Registerkarte **Sicherheit** die Sicherheitsgruppe hinzu, auf die Sie den **Registrierungs** Zugriff gewähren möchten. Wenn Sie beispielsweise allen Benutzern den Zugriff gewähren möchten, wählen Sie die Gruppe **Authentifizierte Benutzer** aus, und wählen Sie dann Berechtigungen für diese Benutzer **registrieren** aus.
11. Klicken Sie auf **OK**, um die Änderungen abzuschließen und die neue Vorlage zu erstellen. Ihre neue Vorlage sollte nun in der Liste der Zertifikatvorlagen angezeigt werden.
12. Wählen Sie **Datei** aus, und klicken Sie dann auf **Snap-in hinzufügen/entfernen**, um das Zertifizierungsstellen-Snap-in zur MMC-Konsole hinzuzufügen. Wenn Sie den Computer, den Sie verwalten möchten, gefragt haben, wählen Sie den Computer aus, auf dem sich die Zertifizierungsstelle befindet, wahrscheinlich **lokaler Computer**.

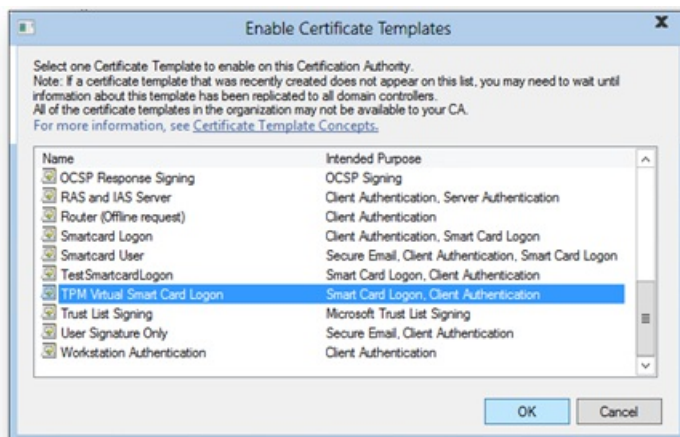


13. Erweitern Sie im linken Bereich der MMC **Zertifizierungsstelle (local)**, und erweitern Sie dann Ihre Zertifizierungsstelle in der Liste Zertifizierungsstelle.
14. Klicken Sie mit der rechten Maustaste auf **Zertifikatvorlagen**, klicken Sie auf **neu**, und klicken Sie dann auf **Zertifikatvorlage zum ausgeben**.



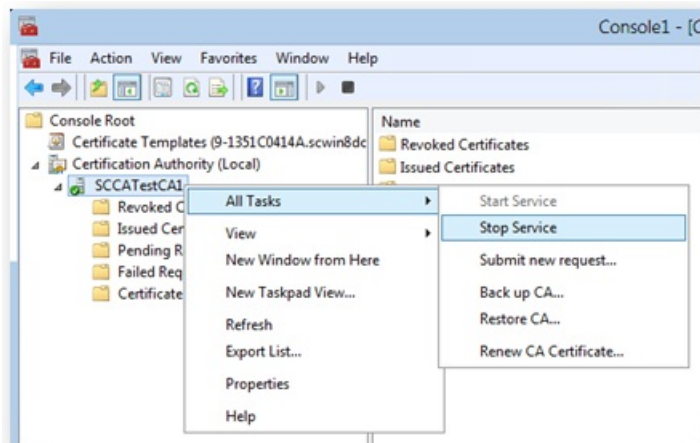
15. Wählen Sie in der Liste die neue Vorlage aus, die Sie soeben erstellt haben (**virtuelle TPM-Smartcard-Anmeldung**), und klicken Sie dann auf **OK**.

**** Hinweis es kann einige Zeit dauern, bis Ihre Vorlage auf alle Server repliziert wird und in dieser Liste verfügbar ist.



16. Klicken Sie nach dem Replizieren der Vorlage in der MMC mit der rechten Maustaste in die Liste Zertifizierungsstelle, klicken Sie auf **alle Aufgaben**, und klicken Sie dann auf **Dienst beenden**. Klicken Sie dann erneut mit der rechten Maustaste auf den Namen der Zertifizierungsstelle, klicken Sie auf **alle**

Aufgaben, und klicken Sie dann auf **Dienst starten**.

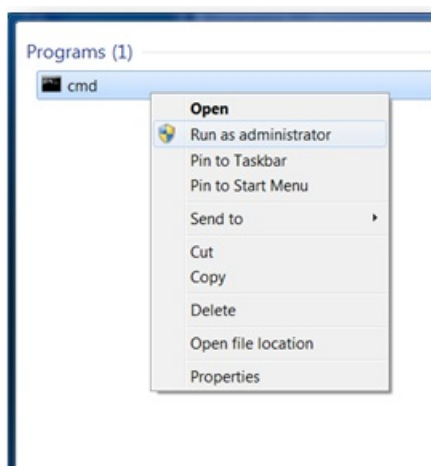


Schritt 2: Erstellen der virtuellen TPM-Smartcard

In diesem Schritt erstellen Sie die virtuelle Smartcard auf dem Clientcomputer mithilfe des Befehlszeilentools [Tpmvscmgr.exe](#).

So erstellen Sie die virtuelle TPM-Smartcard

1. Öffnen Sie auf einem Computer, der mit der Domäne verbunden ist, ein Eingabeaufforderungsfenster mit administrativen Anmeldeinformationen.



2. Geben Sie an der Eingabeaufforderung Folgendes ein, und drücken Sie dann die EINGABETASTE:

```
tpmvscmgr.exe create /name TestVSC /pin default /adminkey random /generate
```

Dadurch wird eine virtuelle Smartcard mit dem Namen **TestVSC** erstellt, der Unlock-Schlüssel ausgelassen und das Dateisystem auf der Karte generiert. Die PIN wird auf die Standardeinstellung 12345678 festgesetzt. Wenn Sie zur Eingabe einer PIN aufgefordert werden möchten, können Sie anstelle der **/Pin-Standard Eingabeaufforderung/Pin** eingeben.

Weitere Informationen zum Tpmvscmgr-Befehlszeilentool finden Sie unter [Verwenden virtueller Smartcards](#) und [Tpmvscmgr](#).

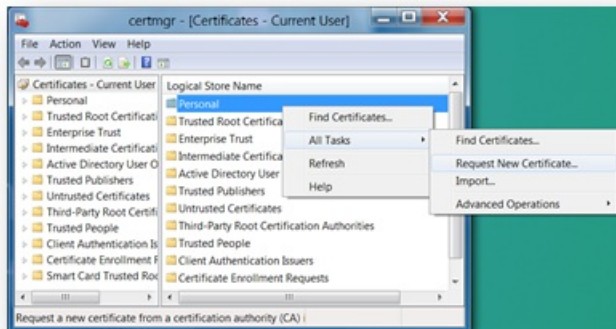
3. Warten Sie einige Sekunden, bis der Vorgang abgeschlossen ist. Nach der Fertigstellung stellt Ihnen Tpmvscmgr.exe die Geräteinstanz-ID für die virtuelle TPM-Smartcard zur Verfügung. Speichern Sie diese ID für spätere Verweise, da Sie diese zum Verwalten oder Entfernen der virtuellen Smartcard benötigen.

Schritt 3: Registrieren des Zertifikats auf der virtuellen TPM-Smartcard

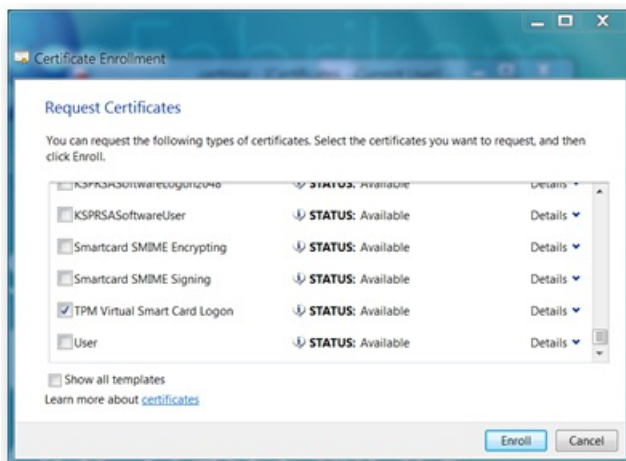
Die virtuelle Smartcard muss mit einem Anmeldezertifikat bereitgestellt werden, damit Sie voll funktionsfähig ist.

So registrieren Sie das Zertifikat

1. Öffnen Sie die Konsole Zertifikate, indem Sie im **Startmenü Certmgr. msc** eingeben.
2. Klicken Sie mit der rechten Maustaste auf **persönlich**, klicken Sie auf **alle Aufgaben**, und klicken Sie dann auf **Neues Zertifikat anfordern**.



3. Folgen Sie den Eingabeaufforderungen, und wenn eine Liste mit Vorlagen angeboten wird, aktivieren Sie das Kontrollkästchen **virtuelle TPM-Smartcard-Anmeldung** (oder was auch immer Sie die Vorlage in Schritt 1 genannt haben).



4. Wenn Sie zur Eingabe eines Geräts aufgefordert werden, wählen Sie die virtuelle Microsoft-Smartcard aus, die der im vorherigen Abschnitt erstellten Version entspricht. Sie wird als **Identitäts Gerät (Microsoft-Profil)** angezeigt.
5. Geben Sie die PIN ein, die beim Erstellen der virtuellen TPM-Smartcard festgelegt wurde, und klicken Sie dann auf **OK**.
6. Warten Sie, bis die Registrierung abgeschlossen ist, und klicken Sie dann auf **Fertig stellen**.

Die virtuelle Smartcard kann nun als Alternative Anmeldeinformationen für die Anmeldung bei Ihrer Domäne verwendet werden. Wenn Sie überprüfen möchten, ob die virtuelle Smartcard-Konfiguration und die Zertifikatregistrierung erfolgreich waren, melden Sie sich bei Ihrer aktuellen Sitzung ab, und melden Sie sich an. Wenn Sie sich anmelden, wird das Symbol für die neue virtuelle TPM-Smartcard auf dem Bildschirm Secure Desktop (anmelden) angezeigt, oder Sie werden automatisch an das TPM-Dialogfeld Smartcard-Anmeldung weitergeleitet. Klicken Sie auf das Symbol, geben Sie Ihre PIN ein (falls erforderlich), und klicken Sie dann auf **OK**. Sie sollten bei Ihrem Domänenkonto angemeldet sein.

Weitere Informationen:

- [Grundlagen und Evaluierung virtueller Smartcards](#)

- Verwenden virtueller Smartcards
- Bereitstellen virtueller Smartcards

Verwenden virtueller Smartcards

11.02.2020 • 4 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten werden die Anforderungen für virtuelle Smartcards, die Verwendung virtueller Smartcards und Tools beschrieben, die Ihnen beim Erstellen und Verwalten von Smartcards helfen.

Anforderungen, Einschränkungen und Einschränkungen

BEREICH	ANFORDERUNGEN UND DETAILS
Unterstützte Betriebssysteme	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows 10 Windows 8.1 Windows 8
Unterstütztes Trusted Platform Module (TPM)	Jedes TPM, das die TPM-Hauptspezifikationen für Version 1,2 oder Version 2,0 (wie von der vertrauenswürdigen Computergruppe festgelegte) erfüllt, wird für die Verwendung als virtuelle Smartcard unterstützt. Weitere Informationen finden Sie in der TPM-Hauptspezifikation .
Unterstützte virtuelle Smartcards pro Computer	<p>Zehn Smartcards können gleichzeitig mit einem Computer oder Gerät verbunden werden. Dazu gehören physische und virtuelle Smartcards kombiniert.</p> <p>Hinweis: Sie können mehrere virtuelle Smartcards erstellen; nach dem Erstellen von mehr als vier virtuellen Smartcards können Sie jedoch die Leistungsverschlechterung bemerken. Da alle Smartcards so angezeigt werden, als ob Sie immer eingefügt werden, wenn mehr als eine Person einen Computer oder ein Gerät freigibt, kann jede Person alle virtuellen Smartcards sehen, die auf diesem Computer oder Gerät erstellt wurden. Wenn der Benutzer die PIN-Werte für alle virtuellen Smartcards kennt, kann er ebenfalls verwendet werden.</p>
Unterstützte Anzahl von Zertifikaten auf einer virtuellen Smartcard	Eine einzelne virtuelle TPM-Smartcard kann 30 unterschiedliche Zertifikate mit den entsprechenden privaten Schlüsseln enthalten. Benutzer können weiterhin Zertifikate auf der Karte verlängern, bis die Gesamtzahl der Zertifikate auf einer Karte 90 überschreitet. Der Grund dafür, dass die Gesamtzahl der Zertifikate von der Gesamtzahl der privaten Schlüssel abweicht, besteht darin, dass die Verlängerung manchmal mit demselben privaten Schlüssel erfolgen kann – in diesem Fall wird kein neuer privater Schlüssel generiert.

BEREICH	ANFORDERUNGEN UND DETAILS
PIN, PIN-Entriegelungstaste (PUK) und administrative Schlüsselanforderungen	Die PIN und die PUK müssen mindestens acht Zeichen umfassen, die Zahlen, alphabetische Zeichen und Sonderzeichen enthalten können. Der administrative Schlüssel muss als 48-Hexadezimalzeichen eingegeben werden. Es handelt sich um eine 3-Tasten-Triple des mit ISO/IEC 9797-Padding-Methode 2 im CBC-Verkettungsmodus.

Verwenden von "Tpmvscmgr. exe"

Zum Erstellen und Löschen von virtuellen TPM-Smartcards für Endbenutzer wird das Tpmvscmgr-Befehlszeilentool als Befehlszeilentool mit dem Betriebssystem hinzugefügt. Sie können die Parameter **Create** und **Delete** verwenden, um virtuelle Smartcards auf lokalen oder Remotecomputern zu verwalten. Informationen zur Verwendung dieses Tools finden Sie unter [Tpmvscmgr](#).

Programmgesteuertes Erstellen und Löschen virtueller Smartcards

Virtuelle Smartcards können auch mithilfe von APIs erstellt und gelöscht werden. Weitere Informationen finden Sie in den folgenden Klassen und Schnittstellen:

- [TpmVirtualSmartCardManager](#)
- [RemoteTpmVirtualSmartCardManager](#)
- [ITpmVirtualSmartCardManager](#)
- [ITPMVirtualSmartCardManagerStatusCallBack](#)

Sie können APIs verwenden, die im Windows. Device. Smartcards-Namespace in Windows Server2012R2 und Windows 8.1 eingeführt wurden, um Microsoft Store-Apps zu erstellen, um den gesamten Lebenszyklus virtueller Smartcards zu verwalten. Informationen dazu, wie Sie eine APP dazu erstellen, finden Sie unter [starke Authentifizierung: Erstellen von apps, die virtuelle Smartcards in Enterprise-, BYOD-und Consumer-Umgebungen nutzen | Build 2013 | Kanal 9](#).

In der folgenden Tabelle werden die Features beschrieben, die in einer Microsoft Store-App entwickelt werden können:

FEATURE	PHYSISCHE SMARTCARD	VIRTUELLE SMARTCARDS
Abfragen und Überwachen von Smartcard-Lesern	Ja	Ja
Auflisten von verfügbaren Smartcards in einem Reader und Abrufen des Karten namens und der Karten-ID	Ja	Ja
Überprüfen, ob der Administratorschlüssel einer Karte richtig ist	Ja	Ja
Bereitstellen (oder Neuformatieren) einer Karte mit einer bestimmten Karten-ID	Ja	Ja

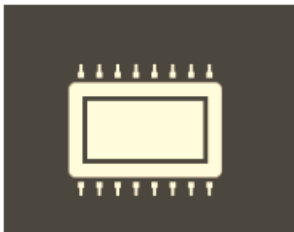
FEATURE	PHYSISCHE SMARTCARD	VIRTUELLE SMARTCARDS
Ändern Sie die PIN, indem Sie die alte PIN eingeben und eine neue PIN angeben.	Ja	Ja
Ändern des administrativen Schlüssels, Zurücksetzen der PIN oder Aufheben der Blockierung der Smartcard mithilfe einer Abfrage/Antwort-Methode	Ja	Ja
Erstellen einer virtuellen Smartcard	Nicht zutreffend	Ja
Löschen einer virtuellen Smartcard	Nicht zutreffend	Ja
PIN-Richtlinien setzen	Nein	Ja

Weitere Informationen zu diesen Windows-APIs finden Sie unter:

- [Windows. Devices. Smartcards-Namespace \(Windows\)](#)
- [Windows. Security. Cryptography. Certificates-Namespace \(Windows\)](#)

Unterscheiden von TPM-basierten virtuellen Smartcards von physischen Smartcards

Um Benutzern die visuelle Unterscheidung einer TPM-basierten virtuellen Smartcard (Trusted Platform Module) von physischen Smartcards zu ermöglichen, weist die virtuelle Smartcard ein anderes Symbol auf. Das folgende Symbol wird während der Anmeldung und auf anderen Bildschirmen angezeigt, in denen der Benutzer die PIN für eine virtuelle Smartcard eingeben muss.



Eine TPM-basierte virtuelle Smartcard ist auf der Benutzeroberfläche mit dem Namen " **Sicherheitsgerät** " gekennzeichnet.

Ändern der PIN

Die PIN für virtuelle Smartcards kann geändert werden, indem Sie STRG + ALT + ENTF drücken und dann unter **Anmeldeoptionen** die virtuelle TPM-Smartcard auswählen.

Beheben von Problemen

TPM nicht bereitgestellt

Damit eine TPM-basierte virtuelle Smartcard ordnungsgemäß funktioniert, muss ein bereitgestelltes TPM auf dem Computer verfügbar sein. Wenn das TPM im BIOS deaktiviert ist oder nicht mit vollständigem Besitz und dem Speicherstammschlüssel bereitgestellt wird, schlägt die virtuelle TPM-Smartcard-Erstellung fehl.

Wenn das TPM nach dem Erstellen einer virtuellen Smartcard initialisiert wird, funktioniert die Karte nicht mehr, und Sie muss neu erstellt werden.

Wenn der TPM-Besitz in einer Windows Vista-Installation eingerichtet wurde, ist das TPM nicht bereit, virtuelle Smartcards zu verwenden. Der System Administrator muss das TPM löschen und initialisieren, damit es für die Erstellung von virtuellen TPM-Smartcards geeignet ist.

Wenn das Betriebssystem neu installiert wird, sind vorherige virtuelle TPM-Smartcards nicht mehr verfügbar und müssen neu erstellt werden. Wenn das Betriebssystem aktualisiert wurde, stehen frühere virtuelle TPM-Smartcards für die Verwendung im aktualisierten Betriebssystem zur Verfügung.

TPM im Sperrzustand

Manchmal kann das TPM aufgrund häufiger fehlerhafter PIN-Versuche eines Benutzers in den Sperrzustand wechseln. Um die Verwendung der virtuellen TPM-Smartcard fortzusetzen, müssen Sie die Sperrung für das TPM zurücksetzen, indem Sie das Kennwort des Besitzers verwenden oder warten, bis die Sperrung abläuft. Durch das Aufheben der Blockierung der Benutzer-PIN wird die Sperrung im TPM nicht zurückgesetzt. Wenn das TPM gesperrt wird, wird die virtuelle TPM-Smartcard so angezeigt, als ob Sie blockiert ist. Wenn das TPM in den Sperrzustand wechselt, weil der Benutzer zu oft eine falsche PIN eingegeben hat, kann es erforderlich sein, die Benutzer-PIN mithilfe der virtuellen Smartcard-Verwaltungstools wie Tpmvscmgr-Befehlszeilentool zurückzusetzen.

Weitere Informationen:

Informationen zu Authentifizierungs-, Vertraulichkeits- und Daten Integritäts Anwendungsfällen finden Sie unter [Übersicht über virtuelle Smartcards](#).

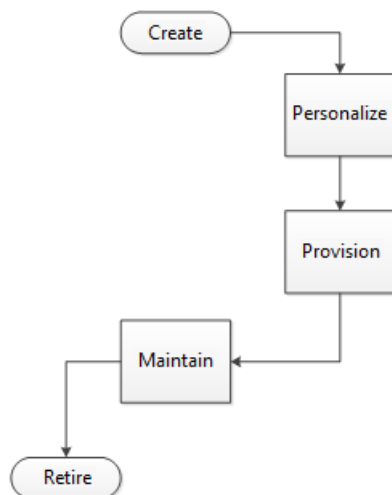
Bereitstellen virtueller Smartcards

12.09.2019 • 23 minutes to read

Gilt für: Windows 10, Windows Server 2016

In diesem Thema für IT-Experten werden die Faktoren erörtert, die bei der Bereitstellung einer virtuellen Smartcard-Authentifizierungslösung zu berücksichtigen sind.

Herkömmliche Identitäts Geräte wie physische Smartcards folgen einem vorhersagbaren Lebenszyklus in jeder Bereitstellung, wie in der folgenden Abbildung dargestellt.



Physische Geräte werden von einem dedizierten Hersteller erstellt und dann vom Unternehmen erworben, das ihn letztendlich bereitstellt. Das Gerät durchläuft die Personalisierungs Phase, in der seine eindeutigen Eigenschaften eingestellt sind. In Smartcards sind diese Eigenschaften der Administratorschlüssel, die persönliche Identifikationsnummer (PIN), die PIN-Entriegelungstaste (PUK) und Ihr physikalisches Aussehen. Zur Bereitstellung des Geräts werden die erforderlichen Zertifikate wie ein Anmeldezertifikat geladen. Nachdem Sie das Gerät bereitgestellt haben, kann es verwendet werden. Das Gerät muss einfach gewartet werden. Sie müssen beispielsweise Karten ersetzen, wenn Sie verloren gehen oder gestohlen werden, und Pins zurücksetzen, wenn Sie von Benutzern vergessen werden. Schließlich werden Sie Geräte zurückziehen, wenn Sie die beabsichtigte Lebensdauer überschreiten oder wenn Mitarbeiter das Unternehmen verlässt.

Dieses Thema enthält Informationen zu den folgenden Phasen in einem virtuellen Smartcard-Lebenszyklus:

- [Erstellen und personalisieren virtueller Smartcards](#)
- [Bereitstellen virtueller Smartcards](#)
- [Verwalten virtueller Smartcards](#)

Erstellen und personalisieren virtueller Smartcards

Ein Unternehmen erwirbt die Geräte, die dann bereitgestellt werden. Das Gerät durchläuft die Personalisierungs Phase, in der seine eindeutigen Eigenschaften eingestellt sind. In Smartcards sind diese Eigenschaften der Administratorschlüssel, die persönliche Identifikationsnummer (PIN), die PIN-Entriegelungstaste (PUK) und Ihr physikalisches Aussehen. Die Sicherheit, die für eine virtuelle TPM-Smartcard bereitgestellt wird, ist im TPM des Hosts vollständig bereitgestellt.

Bereitschaft des vertrauenswürdigen Plattform Moduls

Der TPM-Bereitstellungs-Assistent, der über die **TPM-Verwaltungskonsolle** gestartet wird, führt den Benutzer durch alle Schritte, um das TPM für die Verwendung vorzubereiten.

Wenn Sie virtuelle Smartcards erstellen, sollten Sie im TPM die folgenden Aktionen ausführen:

- **Aktivieren und aktivieren:** TPMs sind in vielen industrietauglichen Computern integriert, sind aber häufig nicht standardmäßig aktiviert und aktiviert. In einigen Fällen muss das TPM aktiviert und über das BIOS aktiviert werden. Weitere Informationen finden Sie unter Initialisieren und Konfigurieren des Besitzes für das TPM.
- **Übernehmen des Besitzes:** Wenn Sie das TPM bereitstellen, legen Sie ein Besitzerkennwort für die zukünftige Verwaltung des TPMs fest, und Sie legen den Speicherstammschlüssel fest. Um den Schutz gegen Hämmer für virtuelle Smartcards zu gewährleisten, muss der Benutzer oder ein Domänenadministrator das TPM-Besitzerkennwort zurücksetzen können. Für die Unternehmens-Nutzung von virtuellen TPM-Smartcards empfiehlt es sich, dass der Domänenadministrator des Unternehmens den Zugriff auf das TPM-Besitzerkennwort durch Speichern in Active Directory und nicht in der lokalen Registrierung einschränken kann. Wenn TPM-Besitz in Windows Vista eingestellt ist, muss das TPM gelöscht und neu initialisiert werden. Weitere Informationen finden Sie unter Übersicht über Trusted Platform Module Technology.
- **Verwalten:** Sie können den Besitz einer virtuellen Smartcard verwalten, indem Sie das Besitzerkennwort ändern, und Sie können die Anti-Hämmer-Logik verwalten, indem Sie die Sperr Zeit zurücksetzen. Weitere Informationen finden Sie unter Verwalten der TPM-Sperrung.

Ein TPM funktioniert möglicherweise im Modus mit eingeschränkter Funktionalität. Dies kann beispielsweise vorkommen, wenn das Betriebssystem nicht feststellen kann, ob das Besitzerkennwort für den Benutzer verfügbar ist. In diesen Fällen kann das TPM zum Erstellen einer virtuellen Smartcard verwendet werden, es wird jedoch dringend empfohlen, das TPM in einen vollständig bereitgestellten Zustand zu versetzen, damit unerwartete Umstände den Benutzer nicht von der Verwendung des Computers blockieren lassen.

Die Verwaltungstools für die Smartcard-Bereitstellung, die eine Statusüberprüfung eines TPMs erfordern, bevor Sie versuchen, eine virtuelle TPM-Smartcard zu erstellen, können dies über die TPM-WMI-Schnittstelle tun.

Je nach dem Setup des Computers, der für die Installation von virtuellen TPM-Smartcards vorgesehen ist, muss möglicherweise das TPM bereitgestellt werden, bevor die Bereitstellung virtueller Smartcards fortgesetzt wird. Weitere Informationen zur Bereitstellung finden Sie unter [Verwenden virtueller Smartcards](#).

Weitere Informationen zum Verwalten von TPMs mithilfe integrierter Tools finden Sie Untergruppen Richtlinienereinstellungen für Trusted Platform Module Services.

Erstellung

Eine virtuelle TPM-Smartcard simuliert eine physikalische Smartcard und verwendet das TPM, um die gleiche Funktionalität wie physische Smartcard-Hardware bereitzustellen. Eine virtuelle Smartcard wird im Betriebssystem als physische Smartcard angezeigt, die immer eingefügt wird. Unterstützte Versionen des Windows-Betriebssystems präsentieren einem virtuellen Smartcard-Leser und einer virtuellen Smartcard Anwendungen mit der gleichen Schnittstelle wie physische Smartcards, aber Nachrichten an und von der virtuellen Smartcard werden in TPM-Befehle übersetzt. Durch diesen Vorgang wird die Integrität der virtuellen Smartcard durch die drei Eigenschaften der Smartcard-Sicherheit sichergestellt:

- **Nicht exportierbare Daten:** da alle privaten Informationen auf der virtuellen Smartcard mithilfe des TPM auf dem Hostcomputer verschlüsselt werden, können Sie nicht auf einem anderen Computer mit einem anderen TPM verwendet werden. Darüber hinaus sind TPMs so konzipiert, dass Sie manipulationssicher und nicht exportierbar sind, sodass ein böswilliger Benutzer kein identisches TPM zurückentwickeln oder dasselbe TPM auf einem anderen Computer installieren kann. Weitere Informationen finden Sie unter [bewerten der virtuellen Smartcard-Sicherheit](#).

- **Isolierte Kryptografie:** TPMs bietet die gleichen Eigenschaften der isolierten Kryptografie, die von physischen Smartcards bereitgestellt wird, und wird von virtuellen Smartcards verwendet. Unverschlüsselte Kopien privater Schlüssel werden nur innerhalb des TPM und nie in den Arbeitsspeicher geladen, auf den das Betriebssystem zugreifen kann. Alle kryptografischen Vorgänge mit diesen privaten Schlüsseln treten innerhalb des TPM auf.
- **Anti-hämmern:** Wenn ein Benutzer eine PIN falsch eingibt, reagiert die virtuelle Smartcard mithilfe der antihämmer-Logik des TPMs, die weitere Versuche für einen bestimmten Zeitraum ablehnt, anstatt die Karte zu blockieren. Dies wird auch als "Lockout" bezeichnet. Weitere Informationen finden Sie unter [Blockierte virtuelle Smartcards](#) und [Auswerten der virtuellen Smartcard-Sicherheit](#).

Je nach Größe der Bereitstellung und des Budgets der Organisation gibt es mehrere Optionen zum Erstellen virtueller Smartcards. Die günstigste Option ist die Verwendung von Tpmvscmgr. exe zum individuellen Erstellen von Karten auf den Computern der Benutzer. Alternativ können Sie eine virtuelle Smartcard-Verwaltungslösung erwerben, um die virtuelle Smartcard-Erstellung auf eine größere Skala zu vereinfachen und in weiteren Phasen der Bereitstellung zu unterstützen. Virtuelle Smartcards können auf Computern erstellt werden, die für einen Mitarbeiter bereitgestellt werden sollen, oder für Personen, die bereits im Besitz eines Mitarbeiters sind. In beiden Ansätzen sollte eine zentrale Kontrolle über Personalisierung und Bereitstellung vorhanden sein. Wenn ein Computer für die Verwendung durch mehrere Mitarbeiter vorgesehen ist, können mehrere virtuelle Smartcards auf einem Computer erstellt werden.

Informationen zum Befehlszeilentool TPM Virtual Smartcard finden Sie unter [Tpmvscmgr](#).

Personalisierung

Während der Personalisierung virtueller Smartcards werden die Werte für den Administratorschlüssel, die PIN und die PUK zugewiesen. Wie bei einer physischen Karte ist es wichtig, den Administratorschlüssel zu kennen, um die PIN zurückzusetzen oder die Karte in Zukunft zu löschen. (Wenn ein PUK festgesetzt wird, kann der Administratorschlüssel nicht mehr verwendet werden, um die PIN zurückzusetzen.)

Da der Administratorschlüssel für die Sicherheit der Karte von entscheidender Bedeutung ist, ist es wichtig, die Bereitstellungsumgebung zu beachten und die richtige Strategie für den Administratorschlüssel festzulegen. Zu den Optionen für diese Strategien gehören:

- **Uniform:** der Administrator Schlüssel für alle virtuellen Smartcards, die in der Organisation bereitgestellt werden, sind identisch. Obwohl dies die Wartungsinfrastruktur vereinfacht (nur ein Schlüssel muss gespeichert werden), ist sie höchst unsicher. Diese Strategie kann für sehr kleine Organisationen ausreichen, wenn aber der Administratorschlüssel kompromittiert ist, müssen alle virtuellen Smartcards, die diesen Schlüssel verwenden, erneut ausgestellt werden.
- **Random, not stored:** Administrator Schlüssel werden nach dem Zufallsprinzip für alle virtuellen Smartcards zugewiesen, und Sie werden nicht aufgezeichnet. Dies ist eine gültige Option, wenn die bereitstellungsadministratoren keine Möglichkeit zum Zurücksetzen von Pins benötigen und stattdessen virtuelle Smartcards löschen und erneut ausgeben möchten. Dies kann auch eine realisierbare Strategie sein, wenn der Administrator die PUK-Werte für die virtuellen Smartcards festlegen und dann diesen Wert zum Zurücksetzen von Pins verwenden möchte, falls dies erforderlich ist.
- **Random, gespeichert:** Administrator Schlüssel werden nach dem Zufallsprinzip zugewiesen und an einem zentralen Speicherort gespeichert. Die Sicherheit jeder Karte ist unabhängig von den anderen. Dies ist in großem Umfang sicher, es sei denn, die Administratorschlüssel Datenbank ist kompromittiert.
- **Deterministisch:** Administrator Schlüssel sind das Ergebnis einiger Funktionen oder bekannter Informationen. Beispielsweise kann die Benutzer-ID verwendet werden, um Daten nach dem Zufallsprinzip zu generieren, die mithilfe eines geheimen Verschlüsselungsalgorithmus weiterverarbeitet werden können. Dieser Administratorschlüssel kann bei Bedarf ebenfalls neu erstellt werden und muss nicht gespeichert werden. Die Sicherheit dieser Methode basiert auf der Sicherheit des verwendeten geheimen Geheimnisses.

Obwohl die Methoden "PUK" und "Administratorschlüssel" das entsperren und Zurücksetzen von Funktionen ermöglichen, tun Sie dies auf unterschiedliche Weise. Bei der PUK handelt es sich um eine PIN, die einfach auf dem Computer eingegeben wird, um einen Benutzer-Pin-Reset zu ermöglichen.

Bei der Methode des Administrator Schlüssels wird ein Challenge-Response-Ansatz verwendet. Die Karte stellt eine Reihe von Zufallsdaten bereit, nachdem Benutzer ihre Identität beim Bereitstellungsadministrator überprüft haben. Der Administrator verschlüsselt die Daten dann mit dem Administratorschlüssel und übergibt die verschlüsselten Daten an den Benutzer zurück. Wenn die verschlüsselten Daten übereinstimmen, die von der Karte während der Überprüfung erstellt wurden, wird die PIN-Zurücksetzung zugelassen. Da der Administratorschlüssel nie von einem anderen Benutzer als dem Bereitstellungsadministrator zugänglich ist, kann er nicht von einer anderen Partei (einschließlich Mitarbeitern) abgefangen oder aufgezeichnet werden. Dies bietet beträchtliche Sicherheitsvorteile, die über die Verwendung eines PUK hinausgehen, was während des Personalisierungsprozesses wichtig ist.

Virtuelle TPM-Smartcards können individuell personalisiert werden, wenn Sie mit dem Tpmvscmgr-Befehlszeilentool erstellt werden. Oder Organisationen können eine Verwaltungslösung erwerben, die die Personalisierung in eine automatisierte Routine einbeziehen kann. Ein weiterer Vorteil einer solchen Lösung ist die automatisierte Erstellung von Administrator Schlüsseln. Mit Tpmvscmgr.exe können Benutzer eigene Administratorschlüssel erstellen, was sich negativ auf die Sicherheit der virtuellen Smartcards auswirken kann.

Bereitstellen virtueller Smartcards

Die Bereitstellung ist der Vorgang des Ladens bestimmter Anmeldeinformationen auf einer virtuellen TPM-Smartcard. Diese Anmeldeinformationen bestehen aus Zertifikaten, die erstellt werden, um Benutzern den Zugriff auf einen bestimmten Dienst, beispielsweise die Domänenanmeldung, zu ermöglichen. Auf jeder virtuellen Smartcard sind maximal 30 Zertifikate zulässig. Wie bei physischen Smartcards müssen für die Bereitstellungsstrategie verschiedene Entscheidungen getroffen werden, die sich auf die Umgebung der Bereitstellung und die gewünschte Sicherheitsstufe beziehen.

Ein hohes Maß an sicherer Bereitstellung erfordert absolute Gewissheit über die Identität der Person, die das Zertifikat erhält. Daher nutzt eine Methode für die Bereitstellung mit hoher Sicherheit zuvor bereitgestellte starke Anmeldeinformationen, beispielsweise eine physikalische Smartcard, um die Identität während der Bereitstellung zu überprüfen. In-Person-Proofing an Registrierungsstellen ist eine weitere Option, da eine Person ihre Identität einfach und sicher mit einem Reisepass oder Führerschein belegen kann, obwohl dies in einem größeren Maßstab undurchführbar werden kann. Um eine ähnliche Zuverlässigkeitsstufe zu erreichen, kann eine große Organisation eine Strategie zur "Registrierung im Auftrag von" implementieren, in der die Mitarbeiter von einem Vorgesetzten, der Ihre Identitäten persönlich verifizieren kann, mit Ihren Anmeldeinformationen registriert sind. Dadurch wird eine Vertrauenskette geschaffen, die sicherstellt, dass einzelne Personen gegen ihre vorgeschlagenen Identitäten überprüft werden, jedoch ohne den administrativen Aufwand für die Bereitstellung aller virtuellen Smartcards von einer einzelnen zentralen Registrierungsstelle aus.

Sie können Self-Service-Lösungen für Bereitstellungen verwenden, bei denen es sich nicht um ein wichtiges Problem mit hoher Sicherheit handelt. Diese können die Verwendung eines Online Portals zum Abrufen von Anmeldeinformationen oder das einfache registrieren für Zertifikate mithilfe von Certificate Manager, abhängig von der Bereitstellung, umfassen. Bedenken Sie, dass die virtuelle Smartcard-Authentifizierung nur so stark ist wie die Bereitstellungsmethode. Wenn beispielsweise schwache Domänenanmeldeinformationen (beispielsweise ein Kennwort) verwendet werden, um das Authentifizierungszertifikat anzufordern, entspricht die virtuelle Smartcard-Authentifizierung der Verwendung des Kennworts, und die Vorteile der zweistufigen Authentifizierung gehen verloren.

Informationen zum Verwenden des Zertifikats-Managers zum Konfigurieren virtueller Smartcards finden Sie unter [Erste Schritte mit virtuellen Smartcards: Exemplarische Vorgehensweise](#).

Für die Bereitstellung von Smartcards mit hoher Sicherheit und Self-Service-Lösungen gehen Sie davon aus, dass der Computer des Benutzers vor der Bereitstellung virtueller Smartcards ausgestellt wurde, dies ist jedoch nicht

immer der Fall. Wenn virtuelle Smartcards mit neuen Computern bereitgestellt werden, können Sie auf dem Computer erstellt, personalisiert und bereitgestellt werden, bevor der Benutzer Kontakt mit diesem Computer hat.

In diesem Fall wird die Bereitstellung relativ einfach, doch es müssen Identitätsprüfungen durchgeführt werden, um sicherzustellen, dass der Empfänger des Computers die Person ist, die während der Bereitstellung erwartet wurde. Dies kann geschehen, wenn der Mitarbeiter die Initiale PIN unter der Aufsicht des Bereitstellungsadministrators oder-Managers festlegen muss.

Wenn Sie Ihre Computer bereitstellen, sollten Sie auch die Langlebigkeit von Anmeldeinformationen berücksichtigen, die für virtuelle Smartcards bereitgestellt werden. Diese Wahl muss auf der Risikoschwelle der Organisation basieren. Obwohl mehr geübte Anmeldeinformationen günstiger sind, sind Sie auch wahrscheinlicher, dass Sie während ihrer Lebensdauer beeinträchtigt werden. Um die angemessene Lebensdauer für Anmeldeinformationen zu bestimmen, muss die Bereitstellungsstrategie die Anfälligkeit ihrer Kryptografie berücksichtigen (wie lange es dauern kann, die Anmeldeinformationen zu knacken) und die Wahrscheinlichkeit eines Angriffs.

Wenn eine virtuelle Smartcard kompromittiert ist, sollten Administratoren in der Lage sein, die zugehörigen Anmeldeinformationen zu widerrufen, wie dies bei einem verloren gegangenen oder gestohlenen Laptop der Fall wäre. Dies erfordert einen Datensatz, dessen Anmeldeinformationen mit dem Benutzer und Computer übereinstimmen, was Funktionalität ist, die in Windows nicht nativ vorhanden ist. Bereitstellungsadministratoren möchten möglicherweise Add-on-Lösungen in Frage stellen, um einen solchen Eintrag beizubehalten.

Virtuelle Smartcards auf Consumer-Geräten, die für den Unternehmens Zugriff verwendet werden

Es gibt Techniken, mit denen Mitarbeiter virtuelle Smartcards bereitstellen und Zertifikate registrieren können, die für die Authentifizierung der Benutzer verwendet werden können. Dies ist hilfreich, wenn Mitarbeiter versuchen, von Geräten aus auf Unternehmensressourcen zuzugreifen, die nicht mit der Unternehmensdomäne verbunden sind. Diese Geräte können weiter definiert werden, damit Benutzer keine Anwendungen aus anderen Quellen als dem Windows Store herunterladen und ausführen können (beispielsweise Geräte, auf denen WindowsRT ausgeführt wird).

Sie können APIs verwenden, die in Windows Server2012R2 und Windows 8.1 eingeführt wurden, um Windows Store-Apps zu erstellen, mit denen Sie den gesamten Lebenszyklus virtueller Smartcards verwalten können. Weitere Informationen finden Sie unter [Programmgesteuertes Erstellen und Löschen virtueller Smartcards](#).

TPM-ownerAuth in der Registrierung

Wenn ein Gerät oder Computer nicht mit einer Domäne verbunden ist, wird das TPM-ownerAuth in der Registrierung unter HKEY_LOCAL_MACHINE. gespeichert. Dadurch werden einige Bedrohungen verfügbar gemacht. Die meisten Bedrohungs Vektoren sind durch BitLocker geschützt, aber nicht geschützte Bedrohungen sind:

- Ein böswilliger Benutzer verfügt über ein Gerät mit einer aktiven lokalen Anmeldesitzung, bevor das Gerät gesperrt wird. Der böswillige Benutzer kann einen Brute-Force-Angriff auf die virtuelle Smartcard-PIN versuchen und dann auf die Unternehmensgeheimnisse zugreifen.
- Ein böswilliger Benutzer verfügt über ein Gerät mit einer aktiven VPN-Sitzung (virtuelles privates Netzwerk). Das Gerät wird dann kompromittiert.

Die vorgeschlagene Abschwächung für die vorherigen Szenarien ist die Verwendung von Exchange ActiveSync-Richtlinien (EAS), um die automatische Sperrungszeit von fünf Minuten auf 30 Sekunden Inaktivität zu verringern. Richtlinien für die automatische Sperrung können während der Bereitstellung virtueller Smartcards eingestellt werden. Wenn eine Organisation mehr Sicherheit wünscht, kann Sie auch eine Einstellung konfigurieren, um die ownerAuth vom lokalen Gerät zu entfernen.

Konfigurationsinformationen zum TPM-ownerAuth-Registrierungsschlüssel finden Sie in der Gruppenrichtlinieneinstellung konfigurieren der Ebene der TPM-Besitzer Autorisierungsinformationen, die für das Betriebssystem verfügbar sind.

Informationen zu EAS-Richtlinien finden Sie unter [Übersicht über das Exchange ActiveSync-Richtlinienmodul](#).

Verwaltete und nicht verwaltete Karten

In der folgenden Tabelle werden die wichtigen Unterschiede zwischen verwalteten und nicht verwalteten virtuellen Smartcards beschrieben, die auf Consumer-Geräten vorhanden sind:

VORGANG	VERWALTETE UND NICHT VERWALTETE KARTEN	NICHT VERWALTETE KARTEN
PIN zurücksetzen, wenn der Benutzer die PIN vergisst	Ja	Nein, die Karte muss gelöscht und erneut erstellt werden.
Zulassen, dass Benutzer die PIN ändern	Ja	Nein, die Karte muss gelöscht und erneut erstellt werden.

Verwaltete Karten

Eine verwaltete virtuelle Smartcard kann vom IT-Administrator oder einer anderen Person in dieser benannten Rolle gewartet werden. Sie ermöglicht es dem IT-Administrator, Einfluss zu haben oder die vollständige Kontrolle über bestimmte Aspekte der virtuellen Smartcard von der Erstellung bis zum Löschen zu haben. Zum Verwalten dieser Karten ist häufig ein virtuelles Smartcard-Bereitstellungs Verwaltungstool erforderlich.

Erstellung verwalteter Karten

Ein Benutzer kann eine leere virtuelle Smartcard mithilfe des Tpmvscmgr-Befehlszeilentools erstellen, bei dem es sich um ein integriertes Tool handelt, das über eine Eingabeaufforderung mit erhöhten Rechten mit administrativen Anmeldeinformationen ausgeführt wird. Diese virtuelle Smartcard muss mit bekannten Parametern (wie Standardwerten) erstellt werden, und Sie sollte unformatiert bleiben (insbesondere sollte die Option **/Generate** nicht angegeben werden).

Mit dem folgenden Befehl wird eine virtuelle Smartcard erstellt, die später von einem auf einem anderen Computer gestarteten Smartcard-Verwaltungstool verwaltet werden kann (wie im nächsten Abschnitt erläutert):

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey DEFAULT /PIN PROMPT
```

Anstatt einen standardmäßigen Administratorschlüssel zu verwenden, kann ein Benutzer auch einen Administratorschlüssel in der Befehlszeile eingeben:

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey PROMPT /PIN PROMPT
```

In beiden Fällen muss das Kartenverwaltungssystem den anfänglichen Administratorschlüssel beachten, der verwendet wird, um den Besitz der virtuellen Smartcard zu übernehmen und den Administratorschlüssel in einen Wert zu ändern, auf den nur über das Karten Verwaltungstool zugegriffen werden kann. vom IT-Administrator. Wenn beispielsweise der Standardwert verwendet wird, ist der Administratorschlüssel auf Folgendes eingestellt:

```
10203040506070801020304050607080102030405060708
```

Informationen zur Verwendung dieses Befehlszeilentools finden Sie unter [Tpmvscmgr](#).

Verwaltung verwalteter Karten

Nachdem die virtuelle Smartcard erstellt wurde, muss der Benutzer eine Remotedesktopverbindung mit einer Registrierungsstelle öffnen, beispielsweise auf einem Computer, der der Domäne beigetreten ist. Virtuelle Smartcards, die einem Clientcomputer zugeordnet sind, stehen für die Verwendung in der Remotedesktopverbindung zur Verfügung. Der Benutzer kann ein Karten Verwaltungstool innerhalb der Remotesitzung öffnen, das den Besitz der Karte übernehmen und für die Verwendung durch den Benutzer bereitstellen kann. Dazu ist es erforderlich, dass ein Benutzer eine Remotedesktopverbindung von einem Computer ohne Domäne zu einem Computer mit einem Domänenbeitritt herstellt. Dies erfordert möglicherweise eine bestimmte Netzwerkkonfiguration, beispielsweise über IPSec-Richtlinien.

Wenn Benutzer eine PIN zurücksetzen oder ändern müssen, müssen Sie die Remotedesktopverbindung verwenden, um diese Vorgänge abzuschließen. Sie können die integrierten Tools für die PIN-Sperrung und die PIN-Änderung oder das Smart Card-Verwaltungstool verwenden.

Zertifikatverwaltung für verwaltete Karten

Ähnlich wie bei physischen Smartcards erfordern virtuelle Smartcards die Zertifikatregistrierung.

Zertifikatausstellung

Benutzer können Zertifikate in einer Remotedesktopsitzung registrieren, die für die Bereitstellung der Karte eingerichtet wurde. Dieser Vorgang kann auch vom Smartcard-Verwaltungstool verwaltet werden, das der Benutzer über die Remotedesktopverbindung ausführt. Dieses Modell eignet sich für Bereitstellungen, die erfordern, dass der Benutzer eine Registrierungsanforderung mithilfe einer physischen Smartcard signiert. Der Treiber für die physische Smartcard muss nicht auf dem Clientcomputer installiert werden, wenn er auf dem Remotecomputer installiert ist. Dies wird durch die in windowsserver2003 eingeführte Smartcard-Umleitungsfunktion ermöglicht, die sicherstellt, dass Smartcards, die mit dem Clientcomputer verbunden sind, während einer Remotesitzung zur Verwendung zur Verfügung stehen.

Alternativ können Benutzer keine Remotedesktopverbindung einrichten, sondern können sich über die Certificate Management Console (certmgr.msc) auf einem Clientcomputer für Zertifikate registrieren. Benutzer können auch eine Anforderung erstellen und Sie über eine benutzerdefinierte Zertifikat Registrierungsanwendung (beispielsweise eine Registrierungsstelle) an einen Server übermitteln, die Zugriff auf die Zertifizierungsstelle kontrolliert. Dazu sind spezifische Unternehmenskonfiguration und-Bereitstellungen für Zertifikats Registrierungsrichtlinien (CEP) und Certificate Enrollment Services (CES) erforderlich.

Zertifikatlebenszyklus Verwaltung

Sie können Zertifikate über Remotedesktopverbindungen, Zertifikatregistrierungsrichtlinien oder Zertifikat Registrierungsdienste verlängern. Die Erneuerungsanforderungen können sich von den anfänglichen Ausstellungsanforderungen unterscheiden, die auf der Erneuerungsrichtlinie basieren.

Für die Zertifikatsperrung ist eine sorgfältige Planung erforderlich. Wenn Informationen über das zu wider rufende Zertifikat zuverlässig verfügbar sind, kann das jeweilige Zertifikat problemlos widerrufen werden. Wenn Informationen zu dem zu wider rufenden Zertifikat nicht einfach zu ermitteln sind, müssen möglicherweise alle Zertifikate, die dem Benutzer unter der Richtlinie ausgestellt wurden, die für die Ausstellung des Zertifikats verwendet wurde, widerrufen werden. Dies kann beispielsweise vorkommen, wenn ein Mitarbeiter ein verlorenes oder kompromittiertes Gerät meldet und Informationen, die dem Gerät ein Zertifikat zuordnen, nicht zur Verfügung stehen.

Nicht verwaltete Karten

Nicht verwaltete virtuelle Smartcards können von einem IT-Administrator nicht gewartet werden. Nicht verwaltete Karten sind möglicherweise geeignet, wenn ein Organisation nicht über ein ausgeklügeltes Verwaltungstool für die Smartcard-Bereitstellung verfügt und die Verwendung von Remotedesktopverbindungen zum Verwalten der Karte nicht erwünscht ist. Da nicht verwaltete Karten vom IT-Administrator nicht gewartet werden können, wenn ein Benutzer Hilfe bei einer virtuellen Smartcard benötigt (beispielsweise das Zurücksetzen oder Entsperren einer PIN), besteht die einzige Option, die dem Benutzer zur Verfügung steht, darin, die Karte zu löschen und erneut zu erstellen. Dies führt zu einem Verlust der Anmeldeinformationen des Benutzers, und er muss sich erneut registrieren.

Erstellung von nicht verwalteten Karten

Ein Benutzer kann eine virtuelle Smartcard mithilfe des Tpmvscmgr-Befehlszeilentools erstellen, das über eine Eingabeaufforderung mit erhöhten Rechten mit administrativen Anmeldeinformationen ausgeführt wird. Mit dem folgenden Befehl wird eine nicht verwaltete Karte erstellt, mit der Zertifikate registriert werden können:

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey RANDOM /PIN PROMPT /generate
```


Mit diesem Befehl wird eine Karte mit einem randomisierten Administratorschlüssel erstellt. Der Schlüssel wird nach der Erstellung der Karte automatisch verworfen. Wenn Benutzer Ihre PIN vergessen oder ändern möchten, müssen Sie die Karte löschen und erneut erstellen. Zum Löschen der Karte kann der Benutzer den folgenden Befehl ausführen:

```
tpmvmcgr.exe destroy /instance <instance ID>
```

wobei <Instanz-> ID der Wert ist, der auf dem Bildschirm gedruckt wird, wenn der Benutzer die Karte erstellt. Insbesondere bei der ersten erstellten Karte ist die Instanz-ID ROOT\SMARTCARDREADER\0000).

Zertifikatverwaltung für nicht verwaltete Karten

Je nach den für eine Organisation eindeutigen Sicherheitsanforderungen können Benutzer zunächst Zertifikate über die Certificate Management Console (certmgr. msc) oder in benutzerdefinierten Zertifikat Registrierungsanwendungen registrieren. Die letztere Methode kann eine Anforderung erstellen und Sie an einen Server übermitteln, der Zugriff auf die Zertifizierungsstelle hat. Dazu sind spezifische organisatorische Konfigurationen und Bereitstellungen für Zertifikats Registrierungsrichtlinien und Zertifikat Registrierungsdienste erforderlich. Windows-has-integrierte Tools, insbesondere "Certreq. exe" und "Certutil. exe", die von Skripten verwendet werden können, um die Registrierung über die Befehlszeile durchzuführen.

Anfordern des Zertifikats, indem nur Domänenanmeldeinformationen bereitgestellt werden

Die einfachste Möglichkeit für Benutzer, Zertifikate anzufordern, besteht darin, ihre Domänenanmeldeinformationen über ein Skript bereitzustellen, das die Registrierung über integrierte Komponenten durchführen kann, die Sie für Zertifikatanforderungen eingerichtet haben.

Alternativ kann eine Anwendung (wie eine Branchen-APP) auf dem Computer installiert werden, um die Registrierung durchführen einer Anforderung auf dem Client durchzuführen. Die Anforderung wird an einen HTTP-Server übermittelt, der Sie an eine Registrierungsstelle weiterleiten kann.

Eine weitere Möglichkeit besteht darin, dass der Benutzer auf ein Registrierungs Portal zugreifen kann, das über Internet Explorer zur Verfügung steht. Auf der Webseite können die Skript-APIs verwendet werden, um die Zertifikatregistrierung durchzuführen.

Signieren der Anforderung mit einem anderen Zertifikat

Sie können Benutzern über eine PFX-Datei (Personal Information Exchange) ein kurz Zeit Zertifikat zur Verfügung stellen. Sie können die PFX-Datei generieren, indem Sie eine Anforderung von einem Computer mit Domänenbeitritt initiieren. In der PFX-Datei können zusätzliche Richtlinieneinschränkungen erzwungen werden, um die Identität des Benutzers zu bestätigen.

Der Benutzer kann das Zertifikat in den **My** Store (den Zertifikatspeicher des Benutzers) importieren. Und Ihre Organisation kann dem Benutzer ein Skript präsentieren, das verwendet werden kann, um die Anforderung für das kurz Zeit Zertifikat zu signieren und eine virtuelle Smartcard anzufordern.

Für Bereitstellungen, für die Benutzer eine physikalische Smartcard zum Signieren der Zertifikatanforderung verwenden müssen, können Sie die folgende Vorgehensweise verwenden:

1. Benutzer initiieren eine Anforderung auf einem Computer, der einer Domäne beigetreten ist.
2. Die Benutzer führen die Anforderung mit einer physischen Smartcard aus, um die Anforderung zu signieren.
3. Benutzer laden die Anforderung auf die virtuelle Smartcard auf dem Clientcomputer herunter.

Verwenden eines Einmalkennworts für die Registrierung

Eine weitere Möglichkeit, um sicherzustellen, dass Benutzer vor der Ausstellung von virtuellen Smartcard-Zertifikaten stark authentifiziert werden, besteht darin, einem Benutzer ein einmaliges Kennwort per SMS, e-Mail oder Telefon zu senden. Der Benutzer gibt dann das Einmalkennwort während der Zertifikatregistrierung von einer Anwendung oder einem Skript auf einem Desktop ein, das integrierte Befehlszeilentools aufruft.

Zertifikatslebenszyklus Verwaltung

Die Zertifikaterneuerung kann über die gleichen Tools erfolgen, die für die erstmalige Zertifikatregistrierung verwendet werden. Zertifikatregistrierungsrichtlinien und Zertifikat Registrierungsdienste können auch verwendet werden, um die automatische Verlängerung durchzuführen.

Für die Zertifikatsperrung ist eine sorgfältige Planung erforderlich. Wenn Informationen über das zu wider rufende Zertifikat zuverlässig verfügbar sind, kann das jeweilige Zertifikat problemlos widerrufen werden. Wenn Informationen zu dem zu wider rufenden Zertifikat nicht einfach zu ermitteln sind, müssen möglicherweise alle Zertifikate, die dem Benutzer unter der Richtlinie ausgestellt wurden, die für die Ausstellung des Zertifikats verwendet wurde, widerrufen werden. Dies kann beispielsweise vorkommen, wenn ein Mitarbeiter ein verlorenes oder kompromittiertes Gerät meldet und Informationen, die dem Gerät ein Zertifikat zuordnen, nicht zur Verfügung stehen.

Verwalten virtueller Smartcards

Wartung ist ein wichtiger Teil des virtuellen Smartcard-Lebenszyklus und eine der wichtigsten Überlegungen aus Sicht des Managements. Nachdem virtuelle Smartcards erstellt, personalisiert und bereitgestellt wurden, können Sie für eine bequeme zweistufige Authentifizierung verwendet werden. Bereitstellungsadministratoren müssen sich mit mehreren gängigen administrativen Szenarien vertraut machen, die mithilfe einer gekauften virtuellen Smartcard-Lösung oder von Fall zu Fall mit internen Methoden erreicht werden können.

Erneuerung: das erneuern virtueller Smartcard-Anmeldeinformationen ist eine reguläre Aufgabe, die erforderlich ist, um die Sicherheit einer virtuellen Smartcard-Bereitstellung zu gewährleisten. Die Erneuerung ist das Ergebnis einer signierten Anforderung eines Benutzers, die das für die neuen Anmeldeinformationen gewünschte Schlüsselpaar angibt. Je nach Auswahl oder Bereitstellungs Spezifikation des Benutzers kann der Benutzeranmeldeinformationen mit demselben Schlüsselpaar anfordern, wie zuvor verwendet, oder ein neu generiertes Schlüsselpaar auswählen.

Beim verlängern mit einem zuvor verwendeten Schlüssel sind keine zusätzlichen Schritte erforderlich, da ein starkes Zertifikat mit diesem Schlüssel während der anfänglichen Bereitstellung ausgestellt wurde. Wenn der Benutzer jedoch ein neues Schlüsselpaar anfordert, müssen Sie dieselben Schritte ausführen, die während der Bereitstellung verwendet wurden, um die Stärke der Anmeldeinformationen zu gewährleisten. Die Erneuerung mit neuen Schlüsseln sollte in regelmäßigen Abständen erfolgen, um anspruchsvollen langfristigen versuchen durch böswillige Benutzer entgegenzuwirken, das System zu infiltrieren. Wenn neue Schlüssel zugewiesen werden, müssen Sie sicherstellen, dass die neuen Schlüssel von den erwarteten Personen auf denselben virtuellen Smartcards verwendet werden.

Zurücksetzen von Pins: das Zurücksetzen virtueller Smartcard-Pins ist auch häufig notwendig, weil Mitarbeiter ihre Pins vergessen. Es gibt zwei Möglichkeiten, dies zu erreichen, je nachdem, welche Entscheidungen zuvor in der Bereitstellung getroffen wurden: Verwenden Sie einen PUK (wenn die PUK eingestellt ist), oder verwenden Sie einen Challenge-Response-Ansatz mit dem Administrations Schlüssel. Bevor die PIN zurückgesetzt wird, muss die Identität des Benutzers mit einigen anderen Mitteln als der Karte überprüft werden – höchstwahrscheinlich die Überprüfungsmethode, die Sie während der ersten Bereitstellung (beispielsweise in-Person-Proofing) verwendet haben. Dies ist in Benutzer Fehlerszenarien notwendig, wenn Benutzer ihre Pins vergessen. Sie sollten jedoch nie eine PIN zurücksetzen, wenn Sie kompromittiert wurde, weil die Sicherheitsanfälligkeit, nach der die PIN verfügbar gemacht wurde, schwer zu erkennen ist. Die gesamte Karte sollte erneut ausgestellt werden.

Sperrungs Zurücksetzung: eine häufige Vorstufe zum Zurücksetzen einer PIN besteht darin, dass die TPM-Sperrungszeit zurückgesetzt werden muss, da die TPM-antihammer-Logik mit mehreren Pin-Eintrags Fehlern für eine virtuelle Smartcard belegt wird. Dies ist derzeit gerätespezifisch.

Ausscheiden von **Karten:** der letzte Aspekt der virtuellen smartcardverwaltung ist das Abziehen von Karten, wenn Sie nicht mehr benötigt werden. Wenn ein Mitarbeiter das Unternehmen verlässt, ist es wünschenswert, den Domänenzugriff zu widerrufen. Das Sperren von Anmeldeinformationen von der Zertifizierungsstelle

(Certification Authority, ca) führt zum Erreichen dieses Ziels.

Die Karte sollte erneut ausgestellt werden, wenn derselbe Computer von anderen Mitarbeitern verwendet wird, ohne das Betriebssystem neu zu installieren. Durch die erneute Verwendung der ehemaligen Karte kann der ehemalige Mitarbeiter die PIN nach dem Verlassen der Organisation ändern und dann die dem neuen Benutzer gehörenden Zertifikate entführen, um nicht autorisierten Domänenzugriff zu erhalten. Wenn der Mitarbeiter jedoch den virtuellen Smartcard-fähigen Computer verwendet, müssen die auf der virtuellen Smartcard gespeicherten Zertifikate nur widerrufen werden.

Notfallbereitschaft

Kartenausgabe

Das häufigste Szenario in einer Organisation ist die erneute Ausgabe virtueller Smartcards, die erforderlich sein können, wenn das Betriebssystem neu installiert wird oder die virtuelle Smartcard in irgendeiner Weise gefährdet ist. Bei der Neuausstellung handelt es sich im Wesentlichen um die Wiederherstellung der Karte, bei der ein neuer PIN- und Administratorschlüssel eingerichtet und eine neue Gruppe zugehöriger Zertifikate bereitgestellt wird. Dies ist eine sofortige Notwendigkeit, wenn eine Karte kompromittiert wird, beispielsweise, wenn der virtuelle Smartcard-geschützte Computer einem Gegner zur Verfügung gestellt wird, der möglicherweise Zugriff auf die richtige PIN hat. Die Neuausstellung ist die sicherste Antwort auf eine unbekannte Gefährdung der Privatsphäre einer Karte. Darüber hinaus ist die erneute Veröffentlichung nach der erneuten Installation eines Betriebssystems erforderlich, da das virtuelle Smartcard-Geräteprofil bei der Neuinstallation des Betriebssystems mit allen anderen Benutzerdaten entfernt wird.

Virtuelle Smartcard blockiert

Das Anti-hämmern-Verhalten einer virtuellen TPM-Smartcard unterscheidet sich von der einer physischen Smartcard. Eine physikalische Smartcard blockiert sich selbst, nachdem der Benutzer einige Male die falsche PIN eingegeben hat. Eine virtuelle TPM-Smartcard wechselt eine zeitgesteuerte Verzögerung, nachdem der Benutzer einige Male die falsche PIN eingegeben hat. Wenn sich das TPM im Modus mit verzögerter Verzögerung befindet, wenn der Benutzer versucht, die virtuelle TPM-Smartcard zu verwenden, wird der Benutzer benachrichtigt, dass die Karte blockiert ist. Wenn Sie die integrierte Sperrungs Funktion aktivieren, kann der Benutzer zudem die Benutzeroberfläche sehen, um die virtuelle Smartcard zu entsperren und die PIN zu ändern. Durch das Entsperren der virtuellen Smartcard wird die TPM-Sperrung nicht zurückgesetzt. Der Benutzer muss einen zusätzlichen Schritt durchführen, um die TPM-Sperrung zurückzusetzen, oder auf das Ablaufen der zeitlich verzögerten Verzögerung warten.

Weitere Informationen zum Festlegen der Richtlinie "integrierte Blockierung zulassen" finden Sie unter [zulassen](#), dass der [integrierte Blockierungs Bildschirm zum Zeitpunkt der Anmeldung angezeigt wird](#).

Weitere Informationen:

[Grundlagen und Evaluierung virtueller Smartcards](#)

[Erste Schritte mit virtuellen Smartcards: Handbuch mit exemplarischer Vorgehensweise](#)

[Verwenden virtueller Smartcards](#)

[Bewerten der Sicherheit virtueller Smartcards](#)

[Tpmvscmgr](#)

12.09.2019 • 3 minutes to read

In diesem Thema für IT-Experten werden Sicherheitsmerkmale und Überlegungen beim Bereitstellen von virtuellen TPM-Smartcards beschrieben.

Ein entscheidender Aspekt von virtuellen TPM-Smartcards ist die Möglichkeit, geheime Daten sicher zu speichern und zu verwenden, insbesondere, dass die gesicherten Daten nicht exportierbar sind. Daten können im virtuellen Smartcardsystem aufgerufen und verwendet werden, sind aber außerhalb der beabsichtigten Umgebung bedeutungslos. In virtuellen TPM-Smartcards ist die Sicherheit mit einer sicheren Schlüsselhierarchie gewährleistet, die mehrere Verschlüsselungsketten umfasst. Dieser stammt aus dem TPM-Speicherstammschlüssel, der im TPM generiert und gespeichert und nicht außerhalb des Chips verfügbar gemacht wird. Die TPM-Schlüsselhierarchie wurde entwickelt, um die Verschlüsselung von Benutzerdaten mit dem Speicherstammschlüssel zu ermöglichen, aber Sie autorisiert die Entschlüsselung mit der Benutzer-PIN so, dass die Änderung der PIN keine erneute Verschlüsselung der Daten erfordert.

Diagram illustrating the User Key Access Process:

- SRK** (System Recovery Key) is used to **Encrypt** the **User Key** and the **User Cert**.
- The **User Key** is encrypted to $E_{SRKPub}(UserKey) | AuthKey$.
- The **User Cert** is encrypted to $E_{SRKPub}(AuthKey) | PIN$.
- The **SRK** is used to **Encrypt** the **Auth Key** to produce $E_{SRKPub}(AuthKey)$.
- The **Auth Key** is used to **Encrypt** the **SC Key** to produce $E_{SRKPub}(SCKey) | PIN$.
- The **SC Key** is used to **Encrypt** the **SRK** to produce $E_{SRKPub}(SRK) | PIN$.

To access User Key:

$$SCKey = D_{SRKPub}(SCKeyBlob) | PIN$$

$$AuthKey = D_{SCKeyPriv}(AuthKeyBlob)$$

$$UserKey = D_{SRKPub}(UserKeyBlob) | AuthKey$$

Orange highlighted components: Managed and stored by TPM based virtual smart card reader

- Benutzertaste
- Smartcard-Schlüssel, der mit dem Speicherstammschlüssel verschlüsselt wird
- Autorisierungsschlüssel für die Benutzerschlüssel Entschlüsselung, die durch den öffentlichen Teil des Smartcard-Schlüssels verschlüsselt wird

Wenn der Benutzer eine PIN eingibt, wird die Verwendung des entschlüsselten Smartcard-Schlüssels mit dieser Pin autorisiert. Wenn diese Autorisierung erfolgreich ist, wird der Schlüssel für die entschlüsselte Smartcard

verwendet, um den auth-Schlüssel zu entschlüsseln. Der auth-Schlüssel wird dann für das TPM bereitgestellt, um die Entschlüsselung und Verwendung des Benutzerschlüssels zu autorisieren, der auf der virtuellen Smartcard gespeichert ist.

Der auth-Schlüssel ist die einzige vertrauliche Daten, die als nur-Text-Funktion außerhalb des TPM verwendet wird, deren Anwesenheit im Arbeitsspeicher jedoch durch die Microsoft-Datenschutz-API (DPAPI) geschützt ist, sodass Sie vor dem Speichern in irgendeiner Weise verschlüsselt ist. Alle anderen Daten als der auth-Schlüssel werden nur als Klartext innerhalb des TPM verarbeitet, das komplett vom externen Zugriff isoliert ist.

Details zu den virtuellen Smartcard-Anti-hämmern

Die Anti-Hämmer-Funktion von virtuellen Smartcards basiert auf der antihämmerfunktion des TPM, das die virtuelle Smartcard aktiviert. Die TPM-Version 1.2 und die nachfolgenden Spezifikationen (wie von der Gruppe Trusted Computing entwickelt) bieten jedoch sehr flexible Richtlinien für die Reaktion auf das Hämmern. Die Spezifikation erfordert nur, dass das TPM den Schutz vor Test-und Fehler-Attacken auf die Benutzer-PIN, den PUK und den Challenge/Response-Mechanismus implementiert.

Die Gruppe "vertrauenswürdige Computer" gibt auch an, dass das TPM die Ausführung der autorisierten TPM-Befehle verhindern muss, wenn die Antwort auf Angriffe die ordnungsgemäße Funktion des TPMs für einen bestimmten Zeitraum oder bis zu einer administrativen Aktion unterbricht. Das TPM kann die Ausführung von TPM-Befehlen bis zum Beenden der Angriffs Antwort verhindern. Neben einer Zeitverzögerung oder einer administrativen Aktion kann ein TPM auch einen Neustart erzwingen, wenn ein Angriff erkannt wird. Die Trusted Computing-Gruppe ermöglicht Herstellern eine Kreativitäts Stufe bei der Wahl der Implementierung. Welche Methodologie von den TPM-Herstellern ausgewählt wird, bestimmt die Anti-Hämmer-Reaktion von virtuellen TPM-Smartcards. Einige typische Aspekte des Schutzes vor Angriffen sind:

1. Erlauben Sie nur eine begrenzte Anzahl falscher PIN-Versuche, bevor Sie eine Sperrung aktivieren, die eine Zeitverzögerung erzwingt, bevor weitere Befehle vom TPM akzeptiert werden.

**** Hinweis in Windows Server2012R2 und Windows 8.1 wurde die Karte blockiert, wenn der Benutzer fünf aufeinanderfolgende Male eine falsche PIN für eine virtuelle Smartcard eingibt (die zusammen mit dem TPM funktioniert). Wenn die Karte blockiert ist, muss Sie mit dem Administrator- oder PUK-Schlüssel freigegeben werden.

2. Erhöhen Sie die Zeitverzögerung exponentiell, wenn der Benutzer die falsche PIN eingibt, damit eine übermäßige Anzahl falscher PIN-Versuche schnell lange Verzögerungen beim Akzeptieren von Befehlen auslösen kann.
3. Führen Sie einen Fehler-Leckage-Mechanismus aus, damit das TPM die zeitverzögerten Verzögerungen über einen bestimmten Zeitraum zurücksetzen kann. Dies ist hilfreich in Fällen, in denen ein gültiger Benutzer die falsche PIN gelegentlich eingegeben hat, beispielsweise aufgrund der Komplexität der PIN.

Als Beispiel wird es 14 Jahre dauern, bis eine 8-stellige PIN für ein TPM erraten wird, das den folgenden Schutz implementiert:

1. Anzahl der zulässigen falschen Pins vor dem Eintritt in die Sperrung (Schwelle): 9
2. Zeitpunkt, zu dem das TPM gesperrt wird, nachdem der Schwellenwert erreicht ist: 10 Sekunden
3. Zeitgesteuerte Verzögerung verdoppelt für jede falsche PIN, nachdem der Schwellenwert erreicht wurde

Weitere Informationen:

[Grundlagen und Evaluierung virtueller Smartcards](#)

Tpmvscmgr

11.02.2020 • 4 minutes to read

Gilt für: Windows 10, Windows Server 2016

Mit dem Tpmvscmgr-Befehlszeilentool können Benutzer mit administrativen Anmeldeinformationen TPM-virtuelle Smartcards auf einem Computer erstellen und löschen. Beispiele für die Verwendung dieses Befehls finden Sie unter [Beispiele](#).

Syntax

```
Tpmvscmgr create [/quiet] /name <name> /AdminKey {DEFAULT | PROMPT | RANDOM} [/PIN {DEFAULT | PROMPT}] [/PUK {DEFAULT | PROMPT}] [/generate] [/machine <machine name>] [/pinpolicy [policy options]] [/attestation {AIK_AND_CERT | AIK_ONLY}] [/?]
```

```
Tpmvscmgr destroy [/quiet] [/instance <device instance ID>] [/machine <machine name>] [/?]
```

Parameter für Create (Befehl)

Der Befehl "erstellen" richtet neue virtuelle Smartcards auf dem System des Benutzers ein. Die Instanz-ID der neu erstellten Karte wird für spätere Verweise zurückgegeben, wenn eine Löschung erforderlich ist. Die Instanz-ID befindet sich im Format ROOT\SMARTCARDREADER\000n, wobei n von 0 beginnt und bei jeder Erstellung einer neuen virtuellen Smartcard um 1 erhöht wird.

PARAMETER	BESCHREIBUNG
/Name	Erforderlich. Gibt den Namen der neuen virtuellen Smartcard an.
/AdminKey	<p>Gibt den gewünschten Administratorschlüssel an, der verwendet werden kann, um die PIN der Karte zurückzusetzen, wenn der Benutzer die PIN vergisst.</p> <p>Standardwert Gibt den Standardwert von 010203040506070801020304050607080102030405060708 an.</p> <p>* Aufforderung fordert den Benutzer auf, einen Wert für den Administratorschlüssel einzugeben.</p> <p>* Zufällige Ergebnisse in einer Zufalls Einstellung für den Administratorschlüssel für eine Karte, die nicht an den Benutzer zurückgegeben wird. Dadurch wird eine Karte erstellt, die möglicherweise nicht über die Smartcard-Verwaltungstools verwaltbar ist. Bei der Generierung mit Random muss der Administratorschlüssel als 48-Hexadezimalzeichen eingegeben werden.</p>
/PIN	<p>Zeigt den gewünschten Benutzer-PIN-Wert an.</p> <p>* Standard gibt die Standard-PIN von 12345678 an.</p> <p>* Aufforderung fordert den Benutzer auf, in der Befehlszeile eine PIN einzugeben. Die PIN muss mindestens acht Zeichen lang sein, und Sie kann Zahlen, Zeichen und Sonderzeichen enthalten.</p>

PARAMETER	BESCHREIBUNG
/PUK	<p>Gibt den gewünschten PUK-Wert (PIN Unlock Key) an. Der PUK-Wert muss mindestens acht Zeichen lang sein und kann Zahlen, Zeichen und Sonderzeichen enthalten. Wenn der Parameter ausgelassen wird, wird die Karte ohne PUK erstellt.</p> <p>* <i>Standard gibt die Standard-PUK von 12345678 an.</i></p> <p>* Aufforderung fordert den Benutzer auf, einen PUK in der Befehlszeile einzugeben.</p>
/generate	<p>Generiert die Dateien im Speicher, die für die Funktion der virtuellen Smartcard erforderlich sind. Wenn der/Generate-Parameter ausgelassen wird, entspricht dies dem Erstellen einer Karte ohne dieses Dateisystem. Eine Karte ohne Dateisystem kann nur von einem Smartcard-Verwaltungssystem wie dem Microsoft Endpoint Configuration Manager verwaltet werden.</p>
/Machine	<p>Ermöglicht es Ihnen, den Namen eines Remotecomputers anzugeben, auf dem die virtuelle Smartcard erstellt werden kann. Dies kann nur in einer Domänenumgebung verwendet werden und basiert auf DCOM. Damit der Befehl beim Erstellen einer virtuellen Smartcard auf einem anderen Computer erfolgreich ausgeführt werden kann, muss der Benutzer, der diesen Befehl ausführt, ein Mitglied der lokalen Gruppe Administratoren auf dem Remotecomputer sein.</p>
/pinpolicy	<p>Wenn /PIN-Aufforderung verwendet wird, können Sie mit /pinpolicy die folgenden Pin-Richtlinienoptionen angeben:</p> <p>minlen <minimale PIN-Länge> Wenn nicht angegeben, wird standardmäßig 8 verwendet. Die untere Grenze ist 4.</p> <p>maxlen <maximale PIN-Länge> Wenn nicht angegeben, wird standardmäßig 127. Die obere Grenze ist 127.</p> <p>Großbuchstaben können zugelassen, nicht zulässig oder erforderlich sein. Standard ist zulässig.</p> <p>Kleinbuchstaben können zugelassen, **** unzulässig oder erforderlich sein. Standard ist zulässig.</p> <p>* Ziffern können *zugelassen, nicht zulässig oder erforderlich sein. Standard ist zulässig.</p> <p>* SpecialChars können *zugelassen, nicht zulässig oder erforderlich sein. Standard ist zulässig.</p> <p>Bei Verwendung von /pinpolicy müssen PIN-Zeichen druckbare ASCII-Zeichen sein.</p>
/attestation	<p>Konfiguriert die Bescheinigung (nur Betreff). Diese Bescheinigung verwendet ein AIK-Zertifikat (certificateing Identity Key) als Vertrauensanker, um zu bestätigen, dass die virtuellen Smartcard-Schlüssel und-Zertifikate wirklich Hardware gebunden sind. Die Bescheinigungs Methoden lauten wie folgt:</p> <p>* <i>AIK_AND_CERT erstellt ein AIK und ruft ein AIK-Zertifikat von der Microsoft-Cloud-Zertifizierungsstelle (Certification Authority, ca) ab. Dazu muss das Gerät ein TPM mit einem EK- Zertifikat aufweisen. Wenn diese Option angegeben ist und keine Netzwerkkonnektivität vorhanden ist, kann es vorkommen, dass die virtuelle Smartcard nicht erstellt wird.</i></p> <p>* AIK_ONLY erstellt ein AIK, erhält aber kein AIK-Zertifikat.</p>

PARAMETER	BESCHREIBUNG
/?	Zeigt Hilfe für diesen Befehl an.

Parameter für "Destroy" (Befehl)

Mit dem Befehl "zerstören" wird eine virtuelle Smartcard sicher von einem Computer gelöscht.

WARNING

Wenn eine virtuelle Smartcard gelöscht wird, kann Sie nicht wiederhergestellt werden.

PARAMETER	BESCHREIBUNG
/instance	Gibt die Instanz-ID der virtuellen Smartcard an, die entfernt werden soll. Die Instanceld wurde als Ausgabe von Tpmvscmgr.exe generiert, als die Karte erstellt wurde. Der /instance -Parameter ist ein erforderliches Feld für den Befehl Destroy.
/Machine	Ermöglicht es Ihnen, den Namen eines Remotecomputers anzugeben, auf dem die virtuelle Smartcard gelöscht wird. Dies kann nur in einer Domänenumgebung verwendet werden und basiert auf DCOM. Damit der Befehl beim Löschen einer virtuellen Smartcard auf einem anderen Computer erfolgreich ausgeführt werden kann, muss der Benutzer, der diesen Befehl ausführt, ein Mitglied der lokalen Gruppe Administratoren auf dem Remotecomputer sein.
/?	Zeigt Hilfe für diesen Befehl an.

Hinweise

Die Mitgliedschaft in der Gruppe Administratoren (oder gleichwertig) auf dem Zielcomputer ist das Mindestgebot, das zum Ausführen aller Parameter dieses Befehls erforderlich ist.

Bei alphanumerischen Eingaben ist der vollständige 127-Zeichensatz ASCII zulässig.

Beispiele

Der folgende Befehl zeigt, wie Sie eine virtuelle Smartcard erstellen, die später von einem auf einem anderen Computer gestarteten Smartcard-Verwaltungstool verwaltet werden kann.

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey DEFAULT /PIN PROMPT
```

Alternativ können Sie anstelle eines standardmäßigen Administrator Schlüssels einen Administratorschlüssel in der Befehlszeile erstellen. Der folgende Befehl zeigt, wie Sie einen Administratorschlüssel erstellen.

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey PROMPT /PIN PROMPT
```

Mit dem folgenden Befehl wird die nicht verwaltete virtuelle Smartcard erstellt, die zum Registrieren von Zertifikaten verwendet werden kann.


```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /AdminKey RANDOM /PIN PROMPT /generate
```

Mit dem vorhergehenden Befehl wird eine virtuelle Smartcard mit einem randomisierten Administratorschlüssel erstellt. Der Schlüssel wird automatisch verworfen, nachdem die Karte erstellt wurde. Das bedeutet, dass der Benutzer die Karte löschen und erneut erstellen muss, wenn der Benutzer die PIN vergisst oder die PIN ändern möchte. Zum Löschen der Karte kann der Benutzer den folgenden Befehl ausführen.

```
tpmvscmgr.exe destroy /instance <instance ID>
```

wobei <Instanz-> ID der Wert ist, der auf dem Bildschirm gedruckt wird, wenn der Benutzer die Karte erstellt hat. Insbesondere bei der ersten erstellten Karte ist die Instanz-ID ROOT\SMARTCARDREADER\0000.

Mit dem folgenden Befehl wird eine virtuelle TPM-Smartcard mit dem Standardwert für den Administratorschlüssel und einer angegebenen PIN-Richtlinie und-Bestätigungsmethode erstellt:

```
tpmvscmgr.exe create /name "VirtualSmartCardForCorpAccess" /PIN PROMPT /pinpolicy minlen 4 maxlen 8 /AdminKey  
DEFAULT /attestation AIK_AND_CERT /generate
```

Weitere Verweise

- [Übersicht über virtuelle Smartcards](#)

Anheften von Enterprise-Zertifikaten

12.09.2019 • 11 minutes to read

Gilt für

- Windows 10

Das Anheften von Enterprise-Zertifikaten ist ein Feature von Windows zum Speichern oder "anheften" einer Stammzertifizierungsstelle, einer ausstellenden Zertifizierungsstelle oder eines Endeinheitenzertifikats zu einem bestimmten Domänennamen. Das Anheften von Enterprise-Zertifikaten kann Man-in-the-Middle-Angriffe reduzieren. Sie können Ihre internen Domänennamen davor schützen, unerwünschte oder fälschlich ausgestellte Zertifikate zu verketteten.

NOTE

Externe Domänennamen, deren Zertifikat von einer öffentlichen Zertifizierungsstelle ausgestellt wurde, eignen sich nicht für das Anheften von Enterprise-Zertifikaten.

Windows-Zertifikat-APIs (CertVerifyCertificateChainPolicy und WinVerifyTrust) werden aktualisiert, um zu überprüfen, ob die Serverauthentifizierungs-Zertifikatkette der Website einer eingeschränkten Gruppe von Zertifikaten entspricht. Diese Einschränkungen sind in einer Zertifikatvertrauensliste (Certificate Trust List, CTL) mit Pin-Regeln gekapselt, die auf Windows10-PCs bereitgestellt und konfiguriert wird. Wenn ein Websitezertifikat einen Namenskonflikt auslöst, schreibt Windows ein Ereignis in das CAPI2-Ereignisprotokoll und verhindert, dass der Benutzer die Website mit Microsoft Edge oder Internet Explorer aufrufen kann.

Bereitstellung

Sie können das Anheften von Enterprise-Zertifikaten auf die folgende Weise bereitstellen:

- Erstellen einer korrekt formatierten XML-Datei mit Regeln für das Anheften von Zertifikaten
- Erstellen einer Zertifikatvertrauensliste mit Pin-Regeln aus der XML-Datei
- Übernehmen der Zertifikatvertrauensliste mit Pin-Regeln auf einem administrativen Referenzcomputer
- Stellen Sie die Registrierungskonfiguration auf dem Referenzcomputer mit der Gruppenrichtlinien-Verwaltungskonsole (GPMC) bereit, die in den [Remoteserver-Verwaltungstools \(RSAT\)](#) enthalten ist.

Erstellen einer XML-Datei mit Pin-Regeln

Die XML-basierte Datei mit Pin-Regeln besteht aus einer Sequenz von PinRule-Elementen. Jedes PinRule-Element enthält eine Sequenz von mindestens einem Site-Element und eine Sequenz von null oder mehreren Certificate-Elementen.

```

<PinRules ListIdentifier="PinRulesExample" Duration="P28D">

  <PinRule Name="AllCertificateAttributes" Error="None" Log="true">
    <Certificate File="Single.cer"/>
    <Certificate File="Multiple.p7b"/>
    <Certificate File="Multiple.sst"/>
    <Certificate Directory="Multiple"/>
    <Certificate Base64="MIIBY ... QFzuM"/>
    <Certificate File="WillExpire.cer" EndDate="2015-05-12T00:00:00Z"/>
    <Site Domain="xyz.com"/>
  </PinRule>

  <PinRule Name="MultipleSites" Log="false">
    <Certificate File="Root.cer"/>
    <Site Domain="xyz.com"/>
    <Site Domain=".xyz.com"/>
    <Site Domain="*.abc.xyz.com" AllSubdomains="true"/>
    <Site Domain="WillNormalize.com"/>
  </PinRule>

</PinRules>

```

PinRules-Element

Das PinRules-Element kann die folgenden Attribute enthalten. Hilfe bei der Formatierung von Pin-Regeln finden Sie unter [Darstellen eines Datums in XML](#) oder [Darstellen einer Zeitdauer in XML](#).

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
Duration oder NextUpdate	Gibt an, wenn die Anheftungseglern ablaufen. Eines der beiden Elemente ist erforderlich. NextUpdate hat Vorrang, wenn beide Elemente angegeben werden. Duration , dargestellt als XML-TimeSpan-Datentyp, darf keine Jahre und Monate enthalten. Das NextUpdate -Attribut wird als XML-DateTime-Datentyp in UTC angegeben.	Erforderlich? Ja Mindestens ein Element ist erforderlich.
LogDuration oder LogEndDate	Konfiguriert die Überwachung ggf. über das Ablaufdatum für die Umsetzung der Pin-Regeln hinaus. LogEndDate , dargestellt als XML-DateTime-Datentyp in UTC, hat Vorrang, wenn beide Elemente angegeben werden. LogDuration wird als XML-TimeSpan-Datentyp angegeben. Jahre und Monate sind nicht zulässig. Wenn keines der Attribute angegeben ist, wird das Attribut Duration oder NextUpdate für die Dauer der Überwachung verwendet.	Nein.
ListIdentifier	Ein Anzeigenname für die Liste der Pin-Regeln. Windows verwendet dieses Attribut nicht für die Umsetzung der Anheftung von Zertifikaten. Es wird jedoch mit angegeben, wenn die Pin-Regeln in eine Zertifikatvertrauensliste (CTL) konvertiert werden.	Nein.

PinRule-Element

Das **PinRule**-Element kann die folgenden Attribute aufweisen.

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
Name	Eindeutiger Bezeichner für die PinRule . Windows verwendet dieses Attribut, um das Element bei Analysefehlern oder für die ausführliche Ausgabe zu identifizieren. Das Attribut ist nicht in der generierten Zertifikatvertrauensliste (CTL) enthalten.	Ja.
Error	Beschreibt die Aktion, die Windows ausführt, wenn ein PIN-Konflikt auftritt. Sie können aus folgenden Zeichenfolgenwerten auswählen: <ul style="list-style-type: none">- Revoked - Windows meldet das Zertifikat, das die Website schützt, so, als wäre es gesperrt. Auf diese Weise wird normalerweise verhindert, dass der Benutzer die Website aufrufen kann.- InvalidName - Windows meldet, dass der Name des Zertifikats, das die Website schützt, nicht mit dem Namen der Website übereinstimmt. Dies führt normalerweise dazu, dass der Benutzer eine Bestätigungsmeldung erhält, bevor die Website aufgerufen wird.- None - Der Standardwert. Es wird kein Fehler zurückgegeben. Mit dieser Einstellung können Sie die Pin-Regeln überwachen, ohne die Benutzer zu beeinträchtigen.	Nein.
Log	Ein boolescher Wert, dargestellt als true oder false . Standardmäßig ist die Protokollierung aktiviert (true).	Nein.

Certificate-Element

Das **Certificate**-Element kann die folgenden Attribute aufweisen.

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
File	Pfad zu einer Datei mit einem oder mehreren Zertifikaten. Die Zertifikate können codiert werden als: <ul style="list-style-type: none">- Einzelzertifikat- p7b- sst Diese Dateien können auch mit Base64-Formatierung angegeben werden. Alle Site -Elemente innerhalb eines PinRule -Elements können mit jedem dieser Zertifikate übereinstimmen.	Ja (File, Directory oder Base64 muss vorhanden sein).
Directory	Pfad zu einem Verzeichnis mit mindestens einer der oben genannten Zertifikatsdateien. Überspringt alle Dateien, die keine Zertifikate enthalten.	Ja (File, Directory oder Base64 muss vorhanden sein).

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
Base64	<p>Base64-codierte Zertifikate. Die Zertifikate können codiert werden als:</p> <ul style="list-style-type: none"> - Einzelzertifikat - p7b - sst <p>Auf diese Weise können die Zertifikate ohne Abhängigkeit von einem Dateiverzeichnis in der XML-Datei angegeben werden.</p> <p>Hinweis:</p> <p>Sie können certutil -encode verwenden, um eine CER-Datei in base64 zu konvertieren. Anschließend können Sie den Editor verwenden, um das base64-codierte Zertifikat zu kopieren und in die Pin-Regel einzufügen.</p>	Ja (File, Directory oder Base64 muss vorhanden sein).
EndDate	<p>Konfigurieren Sie ein Ablaufdatum, ab dem das Zertifikat nicht mehr in der Pin-Regel gültig ist.</p> <p>Während der Umstellung auf eine neue Stammzertifizierungsstelle oder ZS können Sie EndDate festlegen, um den Abgleich mit den Zertifikaten in diesem Element zu erlauben.</p> <p>Nach Ablauf des in EndDate festgelegten Datums gibt der Parser bei der Erstellung der Zertifikatvertrauensliste (CTL) eine Warnmeldung aus und schließt die Zertifikate aus der Pin-Regel aus der generierten CTL aus.</p> <p>Hilfe bei der Formatierung von Pin-Regeln finden Sie unter Darstellen eines Datums in XML.</p>	Nein.

Site-Element

Das **Site**-Element kann die folgenden Attribute aufweisen.

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
Domain	<p>Enthält den DNS-Namen für den Abgleich mit dieser Pin-Regel. Beim Erstellen der Zertifikatvertrauensliste normalisiert der Parser den Eingabenamen wie folgt:</p> <ul style="list-style-type: none"> - Wenn der DNS-Name ein vorangestelltes "*" enthält, wird dieses Element entfernt. - Nicht-ASCII-DNS-Namen werden zu ASCII-Puny Code konvertiert. - ASCII-Großbuchstaben werden zu Kleinbuchstaben konvertiert. <p>Wenn der normalisierte Name ein vorangestelltes "." enthält, wird der Platzhalterabgleich mit links stehenden Bezeichnungen aktiviert. ". xyz.com" stimmt beispielsweise mit "abc.xyz.com" überein.</p>	Ja.

ATTRIBUT	BESCHREIBUNG	ERFORDERLICH
----------	--------------	--------------

AllSubdomains	Der Platzhalterabgleich mit links stehenden Bezeichnern ist standardmäßig auf einen einzigen links stehenden Bezeichner beschränkt. Dieses Attribut kann auf "true" festgelegt werden, um den Platzhalterabgleich für alle links stehenden Bezeichner zu aktivieren. In diesem Fall würde der Domänenwert ". xyz.com" auch mit "123.abc.xyz.com" übereinstimmen.	Nein.
----------------------	--	-------

Erstellen einer Zertifikatvertrauensliste für Pin-Regeln

Das Befehlszeilenprogramm **Certutil.exe** enthält das **generatePinRulesCTL**-Argument, mit dem Sie die XML-Datei analysieren und die codierte Zertifikatvertrauensliste (CTL) generieren können, die Sie auf Ihren Referenzcomputern mit Windows 10 Version 1703 hinzufügen und anschließend bereitstellen. Die Syntax lautet:

```
CertUtil [Options] -generatePinRulesCTL XMLFile CTLFile [SSTFile]
Generate Pin Rules CTL
XMLFile -- input XML file to be parsed.
CTLFile -- output CTL file to be generated.
SSTFile -- optional .sst file to be created.
          The .sst file contains all of the certificates
          used for pinning.

Options:
-f          -- Force overwrite
-v          -- Verbose operation
```

Ein Zertifikat kann in mehreren **PinRule**-Elementen enthalten sein. Eine Domäne kann in mehreren **PinRule**-Elementen enthalten sein. Certutil führt diese in der resultierenden Zertifikatvertrauensliste für Pin-Regeln zusammen.

Certutil.exe führt keine strikte Erzwingung der XML-Schemadefinition durch. Das Programm führt die folgenden Aktionen aus, damit andere Tools ihre eigenen Elemente und Attribute hinzufügen bzw. aufnehmen können:

- Elemente vor und nach dem **PinRules**-Element werden übersprungen.
- Alle Element innerhalb des **PinRules**-Elements, die nicht mit **Certificate** oder **Site** übereinstimmen, werden übersprungen.

- Alle Attribute, die mit den oben angegebenen Namen für die einzelnen Elementtypen übereinstimmen, werden übersprungen.

Verwenden Sie den **Certutil**-Befehl mit dem Argument **GeneratePinRulesCTL** und Ihrer XML-Datei, die Ihre Regeln zum Anheften von Zertifikaten enthält. Geben Sie zuletzt den Namen der Ausgabedatei an, die Ihre Regeln zum Anheften von Zertifikaten in Form einer Zertifikatvertrauensliste enthalten soll.

```
certutil -generatePinRulesCTL certPinRules.xml pinrules.stl
```

Anwenden von Regeln zum Anheften von Zertifikaten auf einem Referenzcomputer

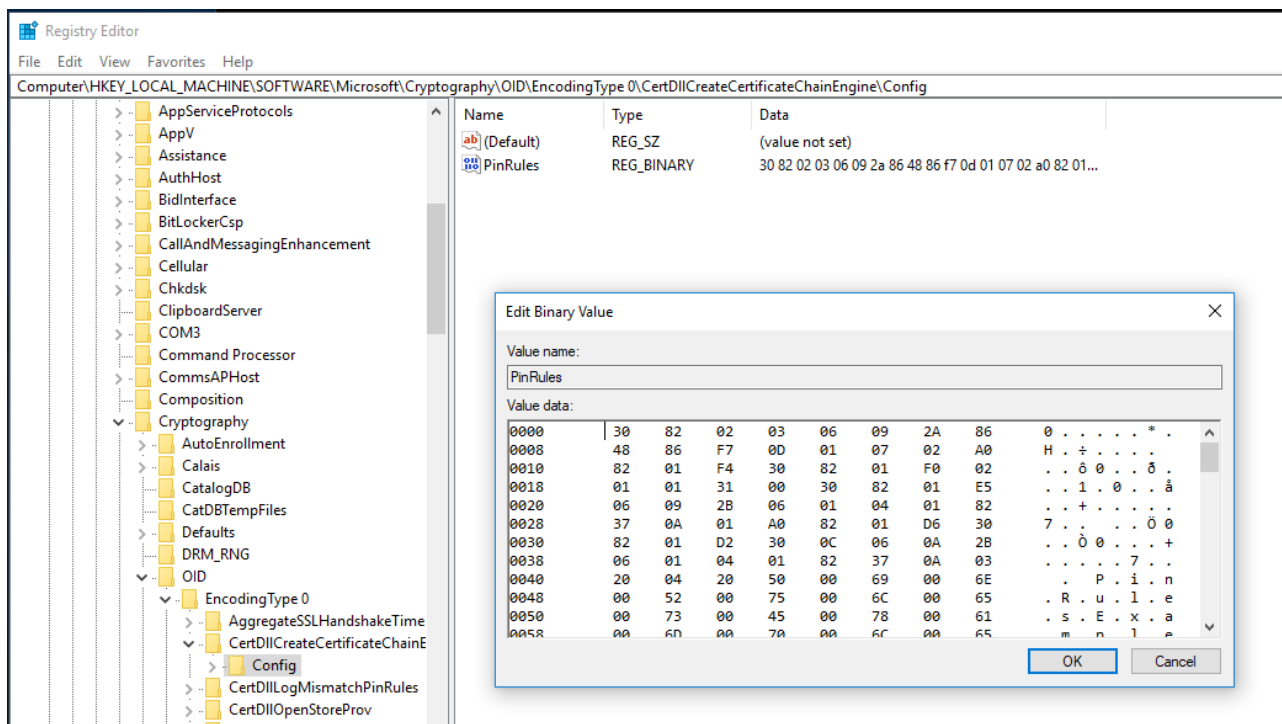
Wenn Ihre Regeln zum Anheften von Zertifikaten in Form einer Zertifikatvertrauensliste vorliegen, müssen Sie die Einstellungen auf einem Referenzcomputer anwenden, um sie in Ihrem Unternehmen bereitstellen zu können. Um die Konfiguration der Bereitstellung zu vereinfachen, können Sie die Regeln zum Anheften von Zertifikaten auf einem Computer mit der Gruppenrichtlinien-Verwaltungskonsolle (GPMC) anwenden, die in der Remoteserver-Verwaltungstools (RSAT) enthalten ist.

Verwenden Sie **certutil.exe** mit dem Argument **setreg**, um Ihre Regeln zum Anheften von Zertifikaten auf Ihrem Referenz-Computer zu übernehmen. Das Argument **Setreg** nimmt ein zweites Argument entgegen, in dem Sie angeben können, an welchen Ort certutil die Zertifikatregeln schreiben soll. Das zweite Argument heißt **Chain\PinRules**. Im letzten Argument geben Sie den Namen der Datei an, die Ihre Regeln zum Anheften von Zertifikaten in Form einer Zertifikatvertrauensliste (.stl) enthält. Sie können den Namen der Datei im letzten Argument übergeben. Der Name der Datei muss wie im folgenden Beispiel gezeigt mit dem Präfix "@" angegeben werden. Führen Sie diesen Befehl über eine Eingabeaufforderung mit erhöhten Rechten aus.

```
Certutil -setreg chain\PinRules @pinrules.stl
```

Certutil schreibt die Binärdaten an den folgenden Ort in der Registrierung:

NAME	WERT
Schlüssel	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType0\CertDllCreateCertificateChainEngine\Config
Name	PinRules
Value	Binärinhalt der Datei mit der Zertifikatvertrauensliste für Pin-Regeln
Datentyp	REG_BINARY



Bereitstellen von Enterprise-Einstellungen für Pin-Regeln mit einer Gruppenrichtlinie

Sie haben eine XML-Datei mit Regeln zum Anheften von Zertifikaten erstellt. Anhand der XML-Datei haben Sie eine Datei mit einer Zertifikatvertrauensliste erstellt und den Inhalt dieser Datei auf Ihrem Referenzcomputer angewendet, auf dem Sie die Gruppenrichtlinien-Verwaltungskonsolle ausführen können. Anschließend müssen Sie eine Gruppenrichtlinie konfigurieren, um die angewendeten Einstellungen zum Anheften von Zertifikaten zu integrieren und in Ihrer Umgebung bereitzustellen.

Melden Sie sich als Domänenadministrator auf dem Referenzcomputer an.

1. Starten Sie die **Gruppenrichtlinien-Verwaltungskonsolle** (gpmc.msc).
2. Erweitern Sie den Gesamtstrukturknoten und anschließend den Domänenknoten im Navigationsbereich.
3. Erweitern Sie den Knoten, der Ihren Active Directory-Domännennamen enthält.
4. Wählen Sie den Knoten **Gruppenrichtlinienobjekte** aus. Klicken Sie mit der rechten Maustaste auf den Knoten **Gruppenrichtlinienobjekte**, und klicken Sie auf **Neu**.
5. Geben Sie im Dialogfeld **Neues Gruppenrichtlinienobjekt** den Text *Enterprise-Regeln zum Anheften von Zertifikaten* in das Textfeld **Name** ein, und klicken Sie auf **OK**.
6. Klicken Sie im Inhaltsbereich mit der rechten Maustaste auf das Gruppenrichtlinienobjekt **Enterprise-Regeln zum Anheften von Zertifikaten**, und klicken Sie auf **Bearbeiten**.
7. Erweitern Sie im Navigationsbereich im **Gruppenrichtlinienverwaltungs-Editor** den Knoten **Einstellungen** unter **Computerkonfiguration**. Erweitern Sie **Windows-Einstellungen**.
8. Klicken Sie mit der rechten Maustaste auf den Knoten **Registrierung**, und klicken Sie auf **Neu**.
9. Wählen Sie im Dialogfeld **Neue Registrierungseigenschaften** den Wert **Update** in der Liste **Aktion** aus. Wählen Sie **HKEY_LOCAL_MACHINE** in der Liste **Struktur** aus.
10. Klicken Sie neben **Schlüsselpfad** auf **...**, um den **Registrierungselementbrowser** zu starten. Navigieren Sie zum folgenden Registrierungsschlüsselwert, und wählen Sie den Registrierungswertnamen **PinRules** aus:

HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType0\CertDllCreateCertificateChainEngine\Config

Klicken Sie auf **Auswählen**, um den **Registrierungselementbrowser** zu schließen.

11. Der **Schlüsselpfad** sollte jetzt den ausgewählten Registrierungsschlüssel enthalten. Unter **Wertname** sollte der jetzt der Name des Registrierungsschlüssels **PinRules** stehen. **Werttyp** sollte den Wert **REG_BINARY**

haben, und **Wertdaten** sollte eine lange Hexadezimalzeichenfolge (Ziffern 0-9 und Buchstaben A-F) enthalten. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

PinRules Properties

General Common

Action: Update

Hive: HKEY_LOCAL_MACHINE

Key Path: SOFTWARE\Microsoft\Cryptography\OID\Enc...

Value name: ☐ Default PinRules

Value type: REG_BINARY

Value data: 3082020306092A864886F70D010702A08201F4308:

OK Cancel Apply Help

- Schließen Sie den **Gruppenrichtlinienverwaltungs-Editor** um Ihre Einstellungen zu speichern.
- Verknüpfen Sie das Gruppenrichtlinienobjekt **Enterprise-Regeln zum Anheften von Zertifikaten** und wenden Sie es auf den Computern in Ihrem Unternehmen an, auf denen Windows 10 Version 1703 ausgeführt wird. Wenn diese Domänencomputer die Gruppenrichtlinie anwenden, wird werden die im Gruppenrichtlinienobjekt konfigurierten Registrierungsinformationen auf dem jeweiligen Computer angewendet.

Zusätzliche Protokollierung für Pin-Regeln

Als Hilfe bei der Erstellung Regeln zum Anheften von Zertifikaten können Sie die Einstellung **PinRulesLogDir** unter dem Registrierungsschlüssel für die Konfiguration von Zertifikatketten konfigurieren, um ein übergeordnetes Verzeichnis für die Protokollierung von Pin-Regeln anzugeben.

NAME	WERT
Schlüssel	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType0\CertDllCreateCertificateChainEngine\Config
Name	PinRulesLogDir
Wert	Das übergeordnete Verzeichnis, in dem Windows die zusätzlichen Protokolle für Pin-Regeln erstellen soll
Datentyp	REG_SZ

Berechtigung für den Protokollordner für Pin-Regeln

Der Ordner, in dem Windows die zusätzlichen Protokolle für Pin-Regeln schreibt, muss allen Benutzern und Apps vollen Zugriff erlauben. Sie können die folgenden Befehle in einer Eingabeaufforderung mit erhöhten Rechten ausführen, um die entsprechenden Berechtigungen einzurichten.

```
set PinRulesLogDir=c:\PinRulesLog
mkdir %PinRulesLogDir%
icacls %PinRulesLogDir% /grant *S-1-15-2-1:(OI)(CI)(F)
icacls %PinRulesLogDir% /grant *S-1-1-0:(OI)(CI)(F)
icacls %PinRulesLogDir% /grant *S-1-5-12:(OI)(CI)(F)
icacls %PinRulesLogDir% /inheritance:e /setintegritylevel (OI)(CI)L
```

Wenn eine Anwendung eine TLS/SSL-Zertifikatkette überprüft, deren Servername mit einem DNS-Namen im Serverzertifikat übereinstimmt, schreibt Windows eine .p7b-Datei mit allen Zertifikaten in der Kette des Servers in einen der drei Unterordner:

- AdminPinRules: Übereinstimmung mit einer Website in den Enterprise-Regeln zum Anheften von Zertifikaten.
- AutoUpdatePinRules: Übereinstimmung mit einer Website in den von Microsoft verwalteten Pin-Regeln.
- NoPinRules: Keine Übereinstimmung mit den Websites in den Regeln zum Anheften von Zertifikaten.

Der Name der Ausgabedatei besteht aus den ersten acht ASCII-Hex-Stellen des SHA1-Fingerabdrucks der Stammzertifizierungsstelle, gefolgt vom Namen des Servers. Beispiele:

- D4DE20D0_xsi.outlook.com.p7b
- DE28F4A4_www.yammer.com.p7b

Bei einem Konflikt mit einer Enterprise-Regel zum Anheften von Zertifikaten oder einer Pin-Regel von Microsoft schreibt Windows die .p7b-Datei in den Unterordner **MismatchPinRules**. Wenn die Pin-Regeln abgelaufen sind, schreibt Windows die .p7b-Datei in den Unterordner **ExpiredPinRules**.

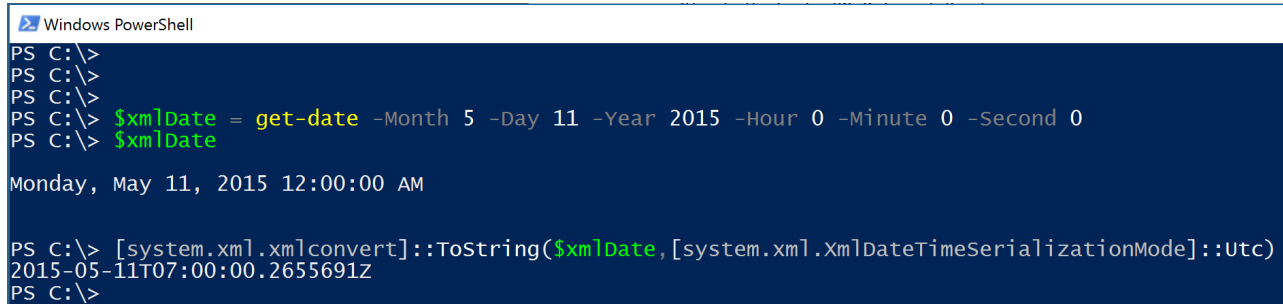
Darstellen eines Datums in XML

Viele Attribute in der XML-Datei mit den Pin-Regeln sind Datumsangaben.

Diese Daten müssen korrekt formatiert und in UTC angegeben werden.

Sie können Windows PowerShell verwenden, um diese Daten zu formatieren.

Anschließend können Sie die Ausgabe des Cmdlets kopieren und in die XML-Datei einfügen.



```
Windows PowerShell
PS C:\>
PS C:\>
PS C:\>
PS C:\> $xmlDate = get-date -Month 5 -Day 11 -Year 2015 -Hour 0 -Minute 0 -Second 0
PS C:\> $xmlDate
Monday, May 11, 2015 12:00:00 AM
PS C:\> [system.xml.xml]convert>::ToString($xmlDate,[system.xml.XmlDateTimeSerializationMode]::Utc)
2015-05-11T07:00:00.2655691Z
PS C:\>
```

Der Einfachheit halber können Sie nach das Dezimaltrennzeichen (.) und die nachfolgenden Nummern weglassen. Achten Sie jedoch darauf, den Großbuchstaben "Z" an das Ende der XML-Datumszeichenfolge anzufügen.

```
2015-05-11T07:00:00.2655691Z
2015-05-11T07:00:00Z
```

Konvertieren eines XML-Datums

Sie können Windows PowerShell auch verwenden, um ein XML-Datum in ein für Menschen lesbares Datum zu konvertieren und zu überprüfen, ob das Datum korrekt ist.

```
Windows PowerShell
PS C:\>
PS C:\>
PS C:\> [system.xml.xmlconvert]::ToDateTime("2015-05-11T07:00:00Z", [system.xml.xmlDateTimeSerializationMode]::Local)
Monday, May 11, 2015 12:00:00 AM
PS C:\>
```

Darstellen einer Zeitdauer in XML

Manche Elemente können eine Zeitdauer anstatt eines Datums enthalten. In diesen Fällen müssen Sie die Dauer als XML-Timespan-Datentyp angeben. Sie können Windows PowerShell verwenden, um eine Zeitdauer (Timespan) korrekt zu formatieren und in Ihre XML-Datei einzufügen.

Windows PowerShell

```
PS C:\>
PS C:\>
PS C:\>
PS C:\> $ts = New-Timespan -Days 45
PS C:\> $ts

Days                : 45
Hours               : 0
Minutes            : 0
Seconds            : 0
Milliseconds        : 0
Ticks               : 3888000000000000
TotalDays           : 45
TotalHours          : 1080
TotalMinutes        : 64800
TotalSeconds        : 3888000
TotalMilliseconds   : 3888000000

PS C:\> [system.xml.xmlconvert]::ToString($ts)
P45D
PS C:\>
```

Konvertieren eine XML-Zeitdauer

Sie können eine Zeitspanne aus dem XML-Format in ein für Menschen lesbares Format konvertieren.

```
Windows PowerShell
PS C:\>
PS C:\>
PS C:\>
PS C:\> [system.xml.xmlconvert]::ToTimeSpan("P45D")

Days           : 45
Hours          : 0
Minutes        : 0
Seconds        : 0
Milliseconds   : 0
Ticks          : 388800000000000
TotalDays      : 45
TotalHours     : 1080
TotalMinutes   : 64800
TotalSeconds   : 3888000
TotalMilliseconds : 3888000000
```

XML-Schemadefinition (XSD) der Zertifikatvertrauensliste

```

<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="PinRules">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PinRule" maxOccurs="unbounded" minOccurs="1">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Certificate" maxOccurs="unbounded" minOccurs="0">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:dateTime" name="EndDate" use="optional"/>
                      <xs:attribute type="xs:string" name="File" use="optional"/>
                      <xs:attribute type="xs:string" name="Directory" use="optional"/>
                      <xs:attribute type="xs:base64Binary" name="Base64" use="optional"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
              <xs:element name="Site" maxOccurs="unbounded" minOccurs="1">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute type="xs:string" name="Domain"/>
                      <xs:attribute type="xs:boolean" name="AllSubdomains" use="optional" default="false"/>
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
            <xs:attribute type="xs:string" name="Name"/>
            <xs:attribute name="Error" use="optional" default="None">
              <xs:simpleType>
                <xs:restriction base="xs:string">
                  <xs:enumeration value="Revoked"/>
                  <xs:enumeration value="InvalidName"/>
                  <xs:enumeration value="None"/>
                </xs:restriction>
              </xs:simpleType>
            </xs:attribute>
            <xs:attribute type="xs:boolean" name="Log" use="optional" default="true"/>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute type="xs:duration" name="Duration" use="optional"/>
      <xs:attribute type="xs:duration" name="LogDuration" use="optional"/>
      <xs:attribute type="xs:dateTime" name="NextUpdate" use="optional"/>
      <xs:attribute type="xs:dateTime" name="LogEndDate" use="optional"/>
      <xs:attribute type="xs:string" name="ListIdentifier" use="optional"/>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

Installieren digitaler Zertifikate unter Windows 10 Mobile

12.09.2019 • 3 minutes to read

Gilt für:

- Windows 10 Mobile

Mit digitalen Zertifikaten wird die Identität eines Benutzers oder Computers an ein Schlüsselpaar gebunden, das zum Verschlüsseln und Signieren von digitalen Informationen verwendet werden kann. Zertifikate werden von einer Zertifizierungsstelle (ZS) ausgestellt, von der die Identität des Zertifikatinhabers bestätigt wird. Außerdem ermöglichen sie die sichere Clientkommunikation mit Websites und Diensten.

Zertifikate in Windows10 Mobile werden in erster Linie für die folgenden Zwecke verwendet:

- Erstellen eines sicheren Kanals per Secure Sockets Layer (SSL) zwischen einem Smartphone und einem Webserver oder -dienst
- Authentifizieren eines Benutzers für einen Reverseproxy, der zum Aktivieren von Microsoft Exchange ActiveSync (EAS) für E-Mails verwendet wird
- Installieren und Lizenzieren von Anwendungen (aus dem Windows Phone Store oder der Distributionswebsite eines Unternehmens)

WARNING

Wenn auf dem Gerät mehrere Zertifikate bereitgestellt wurden und für das bereitgestellte WLAN-Profil keine strengen Filterkriterien gelten, werden unter Windows10 (Version 1607) beim Herstellen einer WLAN-Verbindung unter Umständen Verbindungsfehler angezeigt. [Erfahren Sie mehr über dieses bekannte Problem in Version 1607.](#)

Installieren von Zertifikaten mit Microsoft Edge

Ein Zertifikat kann auf einer Website bereitgestellt und für Benutzer über eine per Gerät zugängliche URL verfügbar gemacht werden, die zum Herunterladen des Zertifikats verwendet werden kann. Wenn ein Benutzer auf die Seite zugreift und auf das Zertifikat tippt, wird es auf dem Gerät geöffnet. Der Benutzer kann das Zertifikat überprüfen, und wenn Sie den Vorgang fortsetzen auswählen, wird das Zertifikat auf dem mobilen Windows10-Gerät installiert.

Installieren von Zertifikaten per E-Mail

Das Windows10-Installationsprogramm für Mobile Zertifikate unterstützt CER-, P7B-, PEM- und PFX-Dateien. Einige E-Mail-Programme blockieren CER-Dateien aus Gründen der Sicherheit. Wenn dies in Ihrer Organisation der Fall ist, verwenden Sie eine alternative Methode, um das Zertifikat bereitzustellen. Zertifikate, die per E-Mail gesendet werden, werden als Anlagen angezeigt. Beim Empfang eines Zertifikats kann ein Benutzer den Inhalt per Tippen überprüfen und dann auf die Option zum Installieren des Zertifikats tippen. Beim Installieren eines Identitätszertifikats wird der Benutzer meist zum Eingeben eines Kennworts (oder einer Passphrase) aufgefordert, mit dem das Zertifikat geschützt ist.

Installieren von Zertifikaten mit der Verwaltung mobiler Geräte (MDM)

Windows10 Mobile unterstützt root-, ca- und Clientzertifikate, die über MDM konfiguriert werden. Mit der

Verwaltung mobiler Geräte kann ein Administrator Stamm- und ZS-Zertifikate direkt hinzufügen, löschen oder abfragen und das Gerät so konfigurieren, dass ein Clientzertifikat bei einem Zertifikatregistrierungsserver registriert wird, der das Simple Certificate Enrollment Protocol (SCEP) unterstützt. Per SCEP registrierte Clientzertifikate werden in den Bereichen WLAN, VPN, E-Mail und Browser für die zertifikatbasierte Clientauthentifizierung verwendet. Ein MDM-Server kann per SCEP registrierte Clientzertifikate (einschließlich der von Benutzern installierten Zertifikate) auch abfragen und löschen oder eine neue Registrierungsanforderung auslösen, bevor das aktuelle Zertifikat abläuft.

WARNING

Verwenden Sie SCEP nicht für Verschlüsselungszertifikate für S/MIME. Sie müssen ein pfx-Zertifikat Profil verwenden, um S/MIME auf Windows10 Mobile zu unterstützen. Eine Anleitung zum Erstellen eines PFX-Zertifikatprofils in Microsoft Intune finden Sie unter [Aktivieren des Zugriffs auf Unternehmensressourcen mithilfe von Zertifikatprofilen in Microsoft Intune](#).

Verarbeiten installierter Zertifikate per MDM

1. Der MDM-Server generiert die erste Anforderung der Zertifikatregistrierung, einschließlich Anfragekennwort, SCEP-Server-URL und anderer Parameter für die Registrierung.
2. Die Richtlinie wird in eine OMA-DM-Anforderung konvertiert und an das Gerät gesendet.
3. Das vertrauenswürdige ZS-Zertifikat wird während der MDM-Anforderung direkt installiert.
4. Das Gerät akzeptiert die Zertifikatregistrierungsanforderung.
5. Das Gerät generiert ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel.
6. Das Gerät stellt eine Verbindung mit dem für die Internetverbindung bestimmten Punkt her, der vom MDM-Server verfügbar gemacht wird.
7. Der MDM-Server erstellt ein Zertifikat, das mit einem korrektem CA-Zertifikat signiert ist, und gibt es an das Gerät zurück.

NOTE

Das Gerät unterstützt die Wartefunktion („Ausstehend“), damit auf der Serverseite weitere Überprüfungsschritte ausgeführt werden können, bevor das Zertifikat ausgestellt wird. In diesem Fall wird der Status „Ausstehend“ zurück an das Gerät gesendet. Das Gerät nimmt regelmäßig Kontakt mit dem Server auf. Die Häufigkeit hängt von den vorkonfigurierten Parametern für die Wiederholungsanzahl und den Wiederholungszeitraum ab. Die Wiederholungsversuche enden, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Empfang eines Zertifikats vom Server ist erfolgreich.
- Der Server gibt einen Fehler zurück.
- Die Anzahl der Wiederholungsversuche erreicht die vorkonfigurierte Obergrenze.

8. Das Zertifikat wird auf dem Gerät installiert. Browser, WLAN, VPN, E-Mail und andere Erstanbieteranwendungen haben Zugriff auf dieses Zertifikat.

NOTE

Wenn per MDM angefordert wurde, dass der private Schlüssel im Trusted Platform Module (TPM) gespeichert wird (das während der Registrierungsanforderung konfiguriert wurde), wird der private Schlüssel im TPM gespeichert. Beachten Sie, dass per SCEP registrierte Zertifikate, die mit TPM geschützt sind, nicht über eine PIN verfügen. Wird das Zertifikat aber in den Windows Hello for Business-KSP (Key Storage Provider) importiert, ist es mit der Hello-PIN geschützt.

Verwandte Themen

Windows 10-Leitfaden für die Diebstahl Minderung von Anmeldeinformationen

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10

Dieses Thema enthält eine Zusammenfassung des Windows 10-Ratgebers zur Einführung von Anmeldeinformationen zum Diebstahl, der aus dem [Microsoft Download Center](#) heruntergeladen werden kann. In diesem Leitfaden wird erläutert, wie Angriffe auf Identitätsdiebstahl und die Strategien und Gegenmaßnahmen, die Sie durchführen können, nach diesen Sicherheitsstufen durchgeführt werden:

- Identifizieren von Ressourcen mit hoher Qualität
- Schutz vor bekannten und unbekannten Bedrohungen
- Erkennen von Pass-the-Hash und zugehörigen Angriffen
- Reagieren auf verdächtige Aktivitäten
- Wiederherstellen nach einem Verstoß



Angriffe, die Anmeldeinformationen stehlen

Informieren Sie sich über die verschiedenen Arten von Angriffen, die zum stehlen von Anmeldeinformationen verwendet werden, und die Faktoren, die Ihrer Organisation ein Risiko geben können. Die folgenden Arten von Angriffen sind abgedeckt:

- Übergeben des Hashs
- Kerberos übergibt das Ticket
- Goldenes Kerberos-Ticket und Silver-Ticket
- Keylogger
- Schulter Surfen

Schutzstrategien für Anmeldeinformationen

Dieser Teil des Handbuchs hilft Ihnen, die Denkweise des Angreifers zu unterstützen, mit normativen Anleitungen zum Priorisieren von Konten mit hoher Leistung und Computern. Sie erfahren, wie Sie eine Verteidigung gegen den Diebstahl von Anmeldeinformationen entwerfen:

- Einrichten eines Kapselungs Modells für Konto Privilegien
- Härten und Einschränken von administrativen Hosts

- Sicherstellen, dass Sicherheitskonfigurationen und bewährte Methoden implementiert sind

Technische Gegenmaßnahmen zum Diebstahl von Anmeldeinformationen

Für jede dieser Gegenmaßnahmen fallen Ziele und erwartete Ergebnisse an:

- Verwenden von Windows 10 mit Credential Guard
- Einschränken und schützen von Domänenkonten mit hoher Berechtigung
- Einschränken und schützen lokaler Konten mit Administratorrechten
- Einschränken des eingehenden Netzwerkverkehrs

Viele andere Gegenmaßnahmen werden ebenfalls behandelt, beispielsweise die Verwendung von Microsoft Passport und Windows Hello oder die mehrstufige Authentifizierung.

Erkennen von Anmeldeinformationen-Angriffen

In diesem Abschnitt wird beschrieben, wie Sie die Verwendung von gestohlenen Anmeldeinformationen erkennen und wie Sie Computerereignisse sammeln, um den Diebstahl von Anmeldeinformationen zu erkennen.

Reagieren auf verdächtige Aktivitäten

Informieren Sie sich über die Empfehlungen von Microsoft für die Reaktion auf Vorfälle, einschließlich der Wiederherstellung der Steuerung von kompromittierten Konten, der Untersuchung von Angriffen und der Wiederherstellung nach einem Verstoß.

Konfigurieren von S/MIME für Windows 10 und Windows 10 Mobile

04.01.2020 • 3 minutes to read

Betrifft:

- Windows 10
- Windows 10 Mobile

S/MIME steht für „Secure/Multipurpose Internet Mail Extensions“ und stellt eine zusätzliche Sicherheitsschicht für E-Mails bereit, die an ein Exchange ActiveSync-Konto (EAS) bzw. von diesem Konto gesendet werden. In Windows 10 können Benutzer ausgehende Nachrichten und Anlagen von S/MIME verschlüsseln, sodass nur beabsichtigte Empfänger, die über eine digitale Identifikation (ID) verfügen, die auch als Zertifikat bezeichnet wird, diese lesen können. Benutzer können eine Nachricht digital signieren. So haben Empfänger eine Möglichkeit, die Identität des Absenders zu überprüfen und sicherzustellen, dass die Nachricht nicht manipuliert wurde.

Informationen zur Verschlüsselung von Nachrichten

Benutzer können verschlüsselte Nachrichten an Personen in ihrem Unternehmen und Personen außerhalb des Unternehmens senden, wenn diese über die richtigen Verschlüsselungszertifikate verfügen. Benutzer, die die Windows 10-Mail-App verwenden, können jedoch nur verschlüsselte Nachrichten lesen, wenn die Nachricht in Ihrem Exchange-Konto empfangen wurde und entsprechende Entschlüsselungsschlüssel vorhanden sind.

Verschlüsselte Nachrichten können nur von Empfängern gelesen werden, die über ein Zertifikat verfügen. Wenn Sie versuchen, eine verschlüsselte Nachricht an Empfänger zu senden, deren Verschlüsselungszertifikate nicht verfügbar sind, werden Sie von der App aufgefordert, diese Empfänger vor dem Senden der E-Mail zu entfernen.

Informationen zu digitalen Signaturen

Bei einer digital signierten Nachricht kann der Empfänger sicher sein, dass die Nachricht nicht manipuliert wurde, und er kann die Identität des Absenders überprüfen. Empfänger können die digitale Signatur nur überprüfen, wenn sie einen E-Mail-Client verwenden, der S/MIME unterstützt.

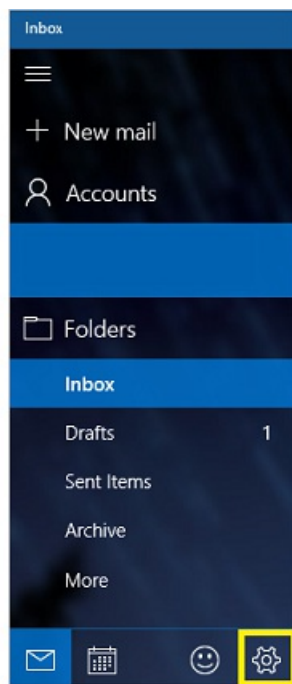
Voraussetzungen

- [S/MIME ist für Exchange-Konten aktiviert](#) (lokal und Office 365). Benutzer können die S/MIME-Signierung und -Verschlüsselung nicht mit einem persönlichen Konto verwenden, z. B. Outlook.com.
- Gültige Zertifikate vom Typ „Privater Informationsaustausch (PFX)“ sind auf dem Gerät installiert.
 - [Erstellen von PFX-Zertifikatprofilen in Configuration Manager](#)
 - [Aktivieren des Zugriffs auf Unternehmensressourcen per Zertifikatprofil mit Microsoft Intune](#)
 - [Installieren digitaler Zertifikate unter Windows 10 Mobile](#)

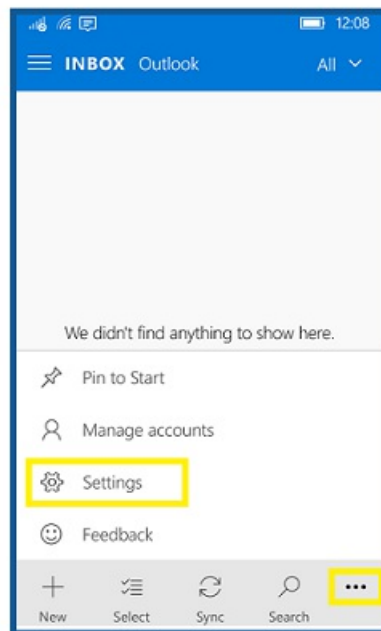
Auswählen von S/MIME-Einstellungen

Führen Sie auf dem Gerät die folgenden Schritte aus: (Ausgewähltes Zertifikat hinzufügen)

1. Öffnen Sie die Mail-App. (In Windows 10 Mobile ist die APP Outlook-e-Mail.)
2. Öffnen Sie **Einstellungen**, indem Sie auf einem PC auf das Zahnradsymbol bzw. auf einem Smartphone auf die Auslassungspunkte (...) und dann auf das Zahnradsymbol tippen.

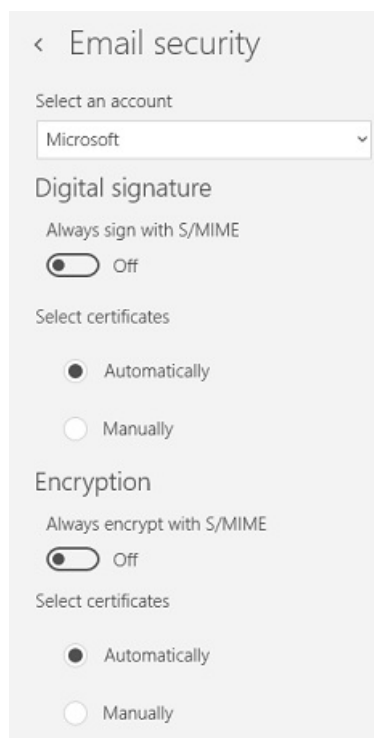


Desktop app



Phone app

3. Tippen Sie auf **E-Mail-Sicherheit**.



4. Wählen Sie unter **Konto auswählen** das Konto aus, für das Sie S/MIME-Optionen konfigurieren möchten.

5. Wählen Sie ein Zertifikat für die digitale Signatur und die Verschlüsselung aus.

- Wählen Sie **Automatisch**, um das Zertifikat von der App auswählen zu lassen.
- Wählen Sie **Manuell**, wenn Sie das Zertifikat selbst aus der Liste mit den gültigen Zertifikaten auf dem Gerät auswählen möchten.

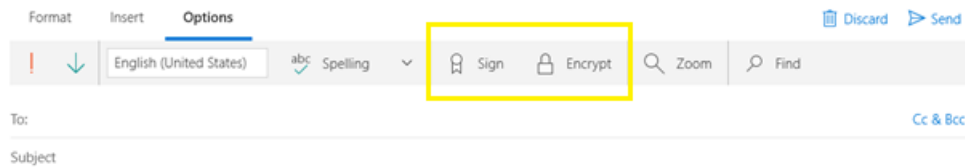
6. (Optional) Wählen Sie **Immer mit S/MIME signieren**, **Immer mit S/MIME verschlüsseln** oder beide Optionen aus, wenn alle ausgehenden Nachrichten digital signiert bzw. verschlüsselt werden sollen.

Hinweis: die Option zum Signieren oder verschlüsseln kann für einzelne Nachrichten geändert werden, es sei denn, EAS-Richtlinien verhindern dies.

7. Tippen Sie auf den Zurück-Pfeil.

Verschlüsseln oder Signieren einzelner Nachrichten

1. Wählen Sie beim Verfassen einer Nachricht im Menüband **Optionen**. Auf dem Telefon können Sie auf **Optionen** zugreifen, indem Sie auf die Auslassungspunkte (...) tippen.
2. Verwenden Sie die Symbole **Signieren** und **Verschlüsseln**, um die digitale Signatur und die Verschlüsselung für diese Nachricht zu aktivieren.



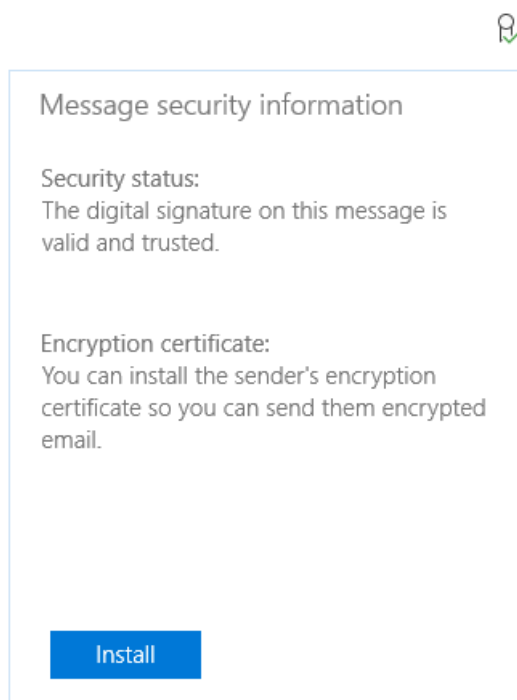
Lesen signierter oder verschlüsselter Nachrichten

Wenn Sie eine verschlüsselte Nachricht erhalten, wird von der Mail-App überprüft, ob auf dem Computer ein Zertifikat verfügbar ist. Wenn ein Zertifikat verfügbar ist, wird die Nachricht beim Öffnen entschlüsselt. Wenn Ihr Zertifikat auf einer Smartcard gespeichert ist, werden Sie aufgefordert, zum Lesen der Nachricht die Smartcard einzulegen. Für die Smartcard kann auch eine PIN erforderlich sein, um auf das Zertifikat zuzugreifen.

Installieren von Zertifikaten aus einer empfangenen Nachricht

Wenn Sie eine signierte E-Mail erhalten, können Sie die App-Features verwenden, um das entsprechende Verschlüsselungszertifikat auf Ihrem Gerät zu installieren, sofern das Zertifikat verfügbar ist. Dieses Zertifikat kann dann verwendet werden, um verschlüsselte E-Mails an die jeweilige Person zu senden.

1. Öffnen Sie eine signierte E-Mail.
2. Tippen oder klicken Sie im Lesebereich auf das Symbol für die digitale Signatur.
3. Tippen Sie auf **Installieren**.



Technische VPN-Anleitung für Windows10

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows10Mobile

In diesem Handbuch werden die Entscheidungen erläutert, die Sie für Windows10-Clients in Ihrer VPN-Unternehmenslösung treffen. Darüber hinaus erfahren Sie, wie Sie Ihre Bereitstellung konfigurieren. Dieses Handbuch verweist auf den [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#) und enthält Konfigurationsanweisungen für die Verwaltung mobiler Geräte (MDM) unter Verwendung von Microsoft Intune und der VPN-Profilvorlage für Windows 10.

Create a New Policy

Select a template for the new policy

Select the template that includes the settings you want to manage with the new policy.

VPN Profile (Windows 10 Desktop and Mobile and later)

NOTE

In diesem Handbuch wird nicht die Serverbereitstellung erläutert.

Inhalt dieser Anleitung

THEMA	BESCHREIBUNG
VPN-Verbindungstypen	Auswählen eines VPN-Clients und eines Tunnelingprotokolls
VPN-Routingentscheidungen	Wählen zwischen einer Konfiguration mit geteiltem oder mit erzwungenem Tunneling
VPN-Authentifizierungsoptionen	Auswählen einer Methode für die EAP-Authentifizierung (Extensible Authentication-Protokoll)
VPN und bedingter Zugriff	Festlegen von Zugriffsrichtlinien für VPN-Verbindungen mithilfe der Azure Active Directory-Richtlinienbewertung
VPN-Namensauflösung	Festlegen der Funktionsweise der Namensauflösung
Automatisch ausgelöste VPN-Profiloptionen	Hier wird ein VPN-Profil so festgelegt, dass die Verbindung automatisch nach App oder Name hergestellt wird, dass die Verbindung immer aktiviert ist oder dass VPN für vertrauenswürdige Netzwerke nicht ausgelöst wird.
VPN-Sicherheitsfeatures	Festlegen eines Sperrmodus-VPN-Profiles, Konfigurieren der Datenverkehrsfilterung und Verbinden des VPN-Profiles mit Windows Information Protection (WIP)

THEMA	BESCHREIBUNG
VPN-Profiloptionen	Zusammenfassen der Einstellungen in einem einzelnen VPN-Profil mit XML

Weitere Informationen

- [VPN-Verbindungen in Microsoft Intune](#)

VPN-Verbindungstypen

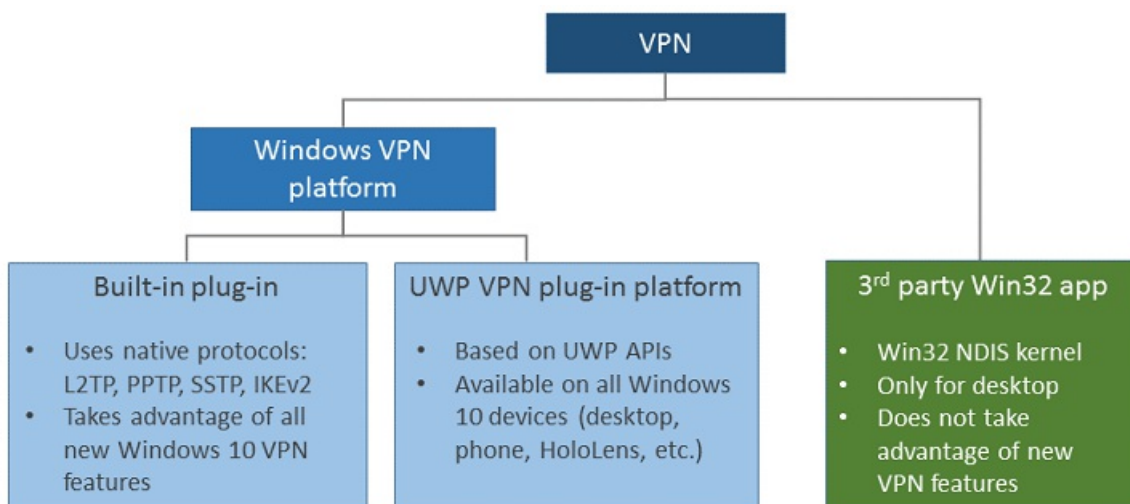
12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Virtuelle private Netzwerke (VPNs) sind Punkt-zu-Punkt-Verbindungen über ein privates oder öffentliches Netzwerk, z.B. das Internet. Ein VPN-Client verwendet spezielle TCP/IP- oder UDP-basierte Protokolle (sogenannte *Tunnelingprotokolle*), um virtuell einen virtuellen Port eines VPN-Servers aufzurufen. In einer typischen VPN-Bereitstellung initiiert ein Client eine virtuelle Punkt-zu-Punkt-Verbindung mit einem RAS-Server über das Internet. Der RAS-Server beantwortet den Aufruf, authentifiziert den Aufrufer und überträgt Daten zwischen dem VPN-Client und dem privaten Netzwerk der Organisation.

Es gibt zahlreiche Optionen für VPN-Clients. Unter Windows 10 basieren das integrierte Plug-In und die VPN-Plug-In-Plattform der universellen Windows-Plattform (Universal Windows Platform, UWP) auf der Windows-VPN-Plattform. Der Schwerpunkt dieses Handbuchs liegt auf den Windows-VPN-Plattformclients und den Features, die konfiguriert werden können.



Integrierter VPN-Client

- Tunnelingprotokolle
 - [Version 2 des Internetschlüsselaustauschs \(Internet Key Exchange version 2, IKEv2\)](#)

Konfigurieren Sie die IPsec/IKE-Tunnelkryptografieeigenschaften mithilfe der Einstellung **Cryptography Suite** unter [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#).

- [L2TP](#)

L2TP mit der Authentifizierung mithilfe eines vordefinierten Schlüssels (Pre-Shared Key, PSK) kann mithilfe der Einstellung **L2tpPsk** unter [VPNv2-CSP](#) konfiguriert werden.

- [PPTP](#)
- [SSTP](#)

SSTP wird nur für Windows-Desktop-Editionen unterstützt. SSTP kann nicht mit der Verwaltung

mobiler Geräte (MDM) konfiguriert werden. Es ist jedoch eines der Protokolle, die in der Option **Automatisch** ausprobiert werden.

- Automatisch

Mit der Option **Automatisch** probiert das Gerät alle integrierten Tunnelingprotokolle aus, bis eines erfolgreich ist. Dabei beginnt die Option mit dem sichersten Protokoll und arbeitet sich dann ggf. zu weniger sicheren Protokollen vor.

Konfigurieren Sie **Automatisch** für die Einstellung **NativeProtocolType** unter [VPNv2-CSP](#).

VPN-Plug-In der universellen Windows-Plattform

Die UWP-VPN-Plug-Ins wurden in Windows10 eingeführt. Anfangs waren jedoch Versionen für die Windows 8.1 Mobile- und die Windows 8.1-PC-Plattform verfügbar. Bei Verwendung der UWP-Plattform können VPN-Drittanbieter App-Container-Plug-Ins mithilfe von WinRT-APIs erstellen. Dies macht Schreibvorgänge in Treiber auf Systemebene unproblematischer und weniger komplex.

Es gibt eine Reihe von UWP-VPN-Anwendungen, etwa Pulse Secure, Cisco AnyConnect, F5 Access, Sonicwall Mobile Connect und Check Point Capsule. Wenn Sie ein UWP-VPN-Plug-In verwenden möchten, wenden Sie sich an den Hersteller, falls Sie benutzerdefinierte Einstellungen zum Konfigurieren der VPN-Lösung benötigen.

Konfigurieren des Verbindungstyps

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

Die folgende Abbildung zeigt Verbindungsoptionen in einer VPN-Profilkonfigurationsrichtlinie mit Microsoft Intune.

VPN Settings

Connection

* VPN connection name (displayed to users):

Example

Connection type:

▼

Pulse Secure

* F5 Edge Client

Dell SonicWALL Mobile Connect

Check Point Capsule VPN

Automatic

IKEv2

L2TP

PPTP

} UWP VPN plug-in connection types

} Built-in VPN connection types

In Intune können Sie auch benutzerdefiniertes XML für Plug-In-Profil von Drittanbietern einfügen.

Custom XML (Third party only):

<xml/>

Verwandte Themen

- Technische VPN-Anleitung
- VPN-Routingentscheidungen
- VPN-Authentifizierungsoptionen
- VPN und bedingter Zugriff
- VPN-Namensauflösung
- Automatisch ausgelöste VPN-Profiloptionen
- VPN-Sicherheitsfeatures
- VPN-Profiloptionen

VPN-Routingentscheidungen

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Netzwerkrouen sind erforderlich, damit der Stapel nachvollziehen kann, welche Schnittstelle für ausgehenden Datenverkehr verwendet werden soll. Einer der wichtigsten Entscheidungspunkte für die VPN-Konfiguration ist, ob Sie alle Daten über VPN (*erzwungenes Tunneling*) oder nur einige Daten über VPN (*geteiltes Tunneling*) senden möchten. Diese Entscheidung wirkt sich auf die Konfiguration und die Kapazitätsplanung sowie die Sicherheitserwartungen aus, die Sie an die Verbindung haben.

Konfiguration mit geteiltem Tunneling

In einer Konfiguration mit geteiltem Tunneling kann angegeben werden, dass Routen über VPN geleitet werden und der gesamte andere Datenverkehr die physische Schnittstelle passiert.

Routen können mit der Einstellung „VPNv2/ProfileName/RouteList“ im [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#) konfiguriert werden.

Für jedes Routenelement in der Liste kann Folgendes angegeben werden:

- **Adresse:** VPNv2/ProfileName/RouteList/routeRowId/Address
- **Präfixgröße:** VPNv2/ProfileName/RouteList/routeRowId/Prefix
- **Ausschlussroute:** VPNv2/ProfileName/RouteList/routeRowId/ExclusionRoute

Die Windows-VPN-Plattform unterstützt nun die Option zur Angabe von Ausschlussrouten, die ausdrücklich nicht über die physische Schnittstelle geleitet werden sollen.

Routen können auch beim Herstellen einer Verbindung über den Server für UWP-VPN-Apps hinzugefügt werden.

Konfiguration mit erzwungenem Tunneling

In einer Konfiguration mit erzwungenem Tunneling wird der gesamte Datenverkehr über VPN geleitet. Diese Standardkonfiguration wird angewendet, wenn keine Routen angegeben werden.

Die einzige Auswirkung dieser Einstellung besteht in der Änderung von Routingeinträgen. Bei einer Tunnelerzwingung werden VPN-V4- und -V6-Standardrouten (z.B. 0.0.0.0/0) der Routingtabelle mit einer niedrigeren Metrik als für andere Schnittstellen hinzugefügt. Dadurch wird Datenverkehr über das VPN gesendet, solange keine bestimmte Route an der physischen Schnittstelle selbst vorliegt.

Bei integriertem VPN wird diese Entscheidung mithilfe der MDM-Einstellung **VPNv2/ProfileName/NativeProfile/RoutingPolicyType** gesteuert.

Bei einem UWP-VPN-Plug-In wird diese Eigenschaft direkt von der App gesteuert. Wenn das VPN-Plug-In die Standardroute für IPv4 und IPv6 als die beiden einzigen Einschlussrouten angibt, kennzeichnet die VPN-Plattform die Verbindung als Verbindung mit Tunnelerzwingung.

Konfigurieren des Routings

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

Beim Konfigurieren eines VPN-Profiles in Microsoft Intune aktivieren Sie ein Kontrollkästchen, um die Konfiguration für geteiltes Tunneling zu aktivieren.

VPN Settings

Connection

* VPN connection name (displayed to users):

Connection type:

* Server list:

Server description	IP address or FQDN
--------------------	--------------------

Default server:

☒ Enable split tunneling

Als Nächstes fügen Sie unter **Unternehmensgrenzen** die Routen hinzu, die die VPN-Verbindung verwenden sollen.

Corporate Boundaries

Configure rules that specify the type of network traffic that can use this connection:

Rule name	Rule scope
-----------	------------

Specify the routes for this VPN connection (optional for third-party providers):

Destination Prefix	Prefix Size
--------------------	-------------

Add or edit VPN route

* Destination prefix (IPv4/v6 addresses):

* Prefix size:

Enter a valid route

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Authentifizierungsoptionen](#)
- [VPN und bedingter Zugriff](#)

- VPN-Namensauflösung
- Automatisch ausgelöste VPN-Profiloptionen
- VPN-Sicherheitsfeatures
- VPN-Profiloptionen

VPN-Authentifizierungsoptionen

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Zusätzlich zu älteren und weniger sicheren kennwortbasierten Authentifizierungsmethoden (die vermieden werden sollten) verwendet die integrierte VPN-Lösung zertifikatbasierte Methoden sowie das Extensible Authentication-Protokoll (EAP), um eine sichere Authentifizierung mithilfe von Benutzername und Kennwort bereitzustellen. Sie können die EAP-basierte Authentifizierung nur konfigurieren, wenn Sie einen integrierten VPN-Typ (IKEv2, L2TP, PPTP oder Automatisch) auswählen.

Windows unterstützt eine Reihe von EAP-Authentifizierungsmethoden.

METHODE	DETAILS
EAP-Microsoft Challenge Handshake Authentication-Protokoll, Version 2 (EAP-MSCHAPv2)	<ul style="list-style-type: none">• Authentifizierung mit Benutzername und Kennwort• Anmeldeinformationen für die Windows-Anmeldung: Kann die Authentifizierung mit Computeranmeldeinformationen angeben.
EAP-Transport Layer Security (EAP-TLS)	<ul style="list-style-type: none">• Unterstützt die folgenden Arten der Zertifikatauthentifizierung.<ul style="list-style-type: none">◦ Zertifikat mit Schlüsseln im Software-Schlüsselspeicheranbieter (Key Storage Provider, KSP)◦ Zertifikat mit Schlüsseln im TPM-KSP (Trusted Platform Module)◦ Smartcardzertifikate◦ Windows Hello for Business-Zertifikat• Zertifikatfilterung<ul style="list-style-type: none">◦ Die Zertifikatfilterung kann aktiviert werden, um nach einem bestimmten Zertifikat für die Authentifizierung zu suchen.◦ Sie können nach Aussteller oder der erweiterten Schlüsselverwendung (Enhanced Key Usage, EKU) filtern.• Serverüberprüfung: Mit TLS kann die Serverüberprüfung ein- und ausgeschaltet werden.<ul style="list-style-type: none">◦ Servername: Geben Sie den zu überprüfenden Server an.◦ Serverzertifikat: Vertrauenswürdiges Stammzertifikat zur Überprüfung des Servers◦ Benachrichtigung: Geben Sie an, ob der Benutzer in einer Benachrichtigung gefragt werden soll, ob der Server als vertrauenswürdig eingestuft werden soll.

METHODE	DETAILS
Protected Extensible Authentication-Protokoll (PEAP)	<ul style="list-style-type: none"> • Serverüberprüfung: Mit PEAP kann die Serverüberprüfung ein- und ausgeschaltet werden. <ul style="list-style-type: none"> ◦ Servername: Geben Sie den zu überprüfenden Server an. ◦ Serverzertifikat: Vertrauenswürdiges Stammzertifikat zur Überprüfung des Servers ◦ Benachrichtigung: Geben Sie an, ob der Benutzer in einer Benachrichtigung gefragt werden soll, ob der Server als vertrauenswürdig eingestuft werden soll. • Innere Methode: Die äußere Methode erstellt einen sicheren Tunnel, während die innere Methode zum Abschließen der Authentifizierung verwendet wird. <ul style="list-style-type: none"> ◦ EAP-MSCHAPv2 ◦ EAP-TLS • Schnelle Wiederherstellung der Verbindung: Verringert die Verzögerung zwischen einer Authentifizierungsanforderung von einem Client und der Antwort des Netzwerkrichtlinienservers (Network Policy Server, NPS) oder einem anderen RADIUS-Server (Remote Authentication Dial-in User Service). Dadurch werden Ressourcenanforderungen für Client und Server verringert, und die Häufigkeit, mit der Benutzer zur Eingabe von Anmeldeinformationen aufgefordert werden, wird minimiert. • Kryptografiebindung: Durch Ableiten und Austauschen von Werten aus dem PEAP-Schlüsselmateriale der Phase1 (Tunnelschlüssel) und aus dem PEAP-Schlüsselmateriale der Phase2 der inneren EAP-Methode (Innerer Sitzungsschlüssel) kann nachgewiesen werden, dass die beiden Authentifizierungen an den beiden gleich Entitäten (PEAP-Peer und PEAP-Server) beendet werden. Dieser als Kryptografiebindung bezeichnete Prozess wird zum Schutz der PEAP-Aushandlung vor Man-in-the-Middle-Angriffen verwendet.
Tunneled Transport Layer Security (TTLS)	<ul style="list-style-type: none"> • Innere Methode <ul style="list-style-type: none"> ◦ Nicht EAP <ul style="list-style-type: none"> ◦ Password Authentication-Protokoll (PAP) ◦ CHAP ◦ MSCHAP ◦ MSCHAPv2 ◦ EAP <ul style="list-style-type: none"> ◦ MSCHAPv2 ◦ TLS • Serverüberprüfung: Bei TTLS muss der Server überprüft werden. Folgendes kann konfiguriert werden: <ul style="list-style-type: none"> ◦ Servername ◦ Vertrauenswürdiges Stammzertifikat für Serverzertifikat ◦ Senden von Benachrichtigungen zur Serverüberprüfung

Bei einem UWP-VPN-Plug-In steuert der App-Anbieter die zu verwendende Authentifizierungsmethode. Die folgenden Arten von Anmeldeinformationen können verwendet werden:

- Smartcard
- Zertifikat
- Windows Hello for Business
- Benutzername und Kennwort
- Einmalkennwort
- Benutzerdefinierter Typ von Anmeldeinformationen

Konfigurieren der Authentifizierung

Informationen zur EAP-XML-Konfiguration finden Sie unter [EAP-Konfiguration](#).

NOTE

Führen Sie zum Konfigurieren der Windows Hello for Business-Authentifizierung die Schritte unter [EAP-Konfiguration](#) aus, um ein Smartcardzertifikat zu erstellen. [Weitere Informationen zu Windows Hello for Business](#)

Die folgende Abbildung zeigt das Feld für EAP-XML in einem Microsoft Intune-VPN-Profil. Das Feld für EAP-XML wird nur angezeigt, wenn Sie als Typ die integrierte Verbindung (Automatisch, IKEv2, L2TP, PPTP) auswählen.

Authentication

Authentication method:
Certificates ▼

☐ Remember the user credentials at each logon

* Select a client certificate for client authentication (Identity Certificate):
 Select...

☐ Enable conditional access for this VPN connection

* EAP XML:

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN und bedingter Zugriff](#)
- [VPN-Namensauflösung](#)
- [Automatisch ausgelöste VPN-Profiloptionen](#)
- [VPN-Sicherheitsfeatures](#)
- [VPN-Profiloptionen](#)

VPN und bedingter Zugriff

20.12.2019 • 4 minutes to read

Gilt für: Windows10 und Windows10 Mobile

Der VPN-Client kann nun in die cloudbasierte Plattform für den bedingten Zugriff integriert werden, um eine Gerätekompatibilitätsoption für Remoteclients bereitzustellen. Beim bedingten Zugriff handelt es sich um ein richtlinienbasiertes Auswertungsmodul, mit dem Sie Zugriffsregeln für alle mit Azure Active Directory (Azure AD) verknüpften Anwendungen erstellen können.

NOTE

Der bedingte Zugriff ist ein Azure AD Premium-Feature.

Zu den für die Gerätekompatibilität verwendeten Komponenten der Plattform für den bedingten Zugriff zählen folgende cloudbasierte Dienste:

- [Conditional Access Framework](#)
- [Azure AD Connect Health](#)
- [Windows-Integritätsnachweisdienst \(Health Attestation Service\)](#) (optional)
- Azure AD-Zertifizierungsstelle: Das für die cloudbasierte Gerätekompatibilitätslösung verwendete Zertifikat muss von einer auf Azure Active Directory basierenden Zertifizierungsstelle ausgestellt werden. Bei einer Azure AD-Zertifizierungsstelle handelt es sich im Grunde um einen Cloudmandanten für eine sehr kleine Zertifizierungsstelle in Azure. Die Azure AD-Zertifizierungsstelle kann nicht als Teil einer lokalen Unternehmenszertifizierungsstelle konfiguriert werden.
- Von Azure AD ausgegebene Zertifikate mit kurzer Laufzeit: Bei einem VPN-Verbindungsversuch kommuniziert der Azure AD-Tokenbroker auf dem lokalen Gerät mit dem Azure Active Directory-Dienst, der dann basierend auf Kompatibilitätsregeln die Integrität überprüft. Bei bestätigter Kompatibilität sendet Azure AD ein Zertifikat mit kurzer Laufzeit zurück, das zum Authentifizieren des VPN verwendet wird. Beachten Sie, dass Zertifikatauthentifizierungsmethoden wie etwa EAP-TLS verwendet werden können. Wenn das Zertifikat abläuft, überprüft der Client erneut mit Azure AD die Integritätsüberprüfung, bevor ein neues Zertifikat ausgestellt wird.
- [Gerätekompatibilitätsrichtlinien in Microsoft Intune](#): Die cloudbasierte Gerätekompatibilität nutzt Microsoft Intune-Kompatibilitätsrichtlinien, die den Gerätestatus abfragen und Kompatibilitätsregeln u.a. für Folgendes festlegen können:
 - Antivirusstatus
 - Status automatischer Updates und Updatekompatibilität
 - Kompatibilität von Kennwortrichtlinien
 - Verschlüsselungskompatibilität
 - Zustand des Geräteintegritätsnachweises (überprüft mit dem Nachweisdienst nach der Abfrage)

Die folgenden clientseitigen Komponenten sind ebenfalls erforderlich:

- [HealthAttestation-Konfigurationsdienstanbieter \(Configuration Service Provider, CSP\)](#)
- [VPNv2-CSP](#): DeviceCompliance-Knoteneinstellungen

- Trusted Platform Module (TPM)

VPN-Gerätekompatibilität

Zu diesem Zeitpunkt enthalten die für Benutzer ausgestellten Azure AD-Zertifikate keinen CRL-Verteilungspunkt (CDP) und eignen sich nicht für Key Distribution Center (KDCs), um Kerberos-Token auszustellen. Damit Benutzer Zugriff auf lokale Ressourcen wie Dateien auf einer Netzwerkfreigabe erhalten, müssen Clientauthentifizierungszertifikate für die Windows-Profile der Benutzer bereitgestellt werden, und ihre VPNv2-Profile müssen den <SSO> -Abschnitt enthalten.

Anforderungen in Bezug auf die serverseitige Infrastruktur zur Unterstützung der VPN-Gerätekompatibilität:

- Der VPN-Server sollte für die Zertifikatauthentifizierung konfiguriert sein.
- Der VPN-Server muss der mandantenspezifischen Azure AD-Zertifizierungsstelle vertrauen.
- Für den Clientzugriff mit Kerberos/NTLM wird ein Domänen vertrauenswürdigen Zertifikat auf dem Clientgerät bereitgestellt und für die Verwendung für einmaliges Anmelden (SSO) konfiguriert.

Nach der Einrichtung der serverseitigen Infrastruktur können VPN-Administratoren die Richtlinieneinstellungen für bedingten Zugriff mithilfe des VPNv2-DeviceCompliance-Knotens zum VPN-Profil hinzufügen.

Für die VPN-Gerätekompatibilität werden zwei clientseitige Konfigurationsdienstanbieter genutzt.

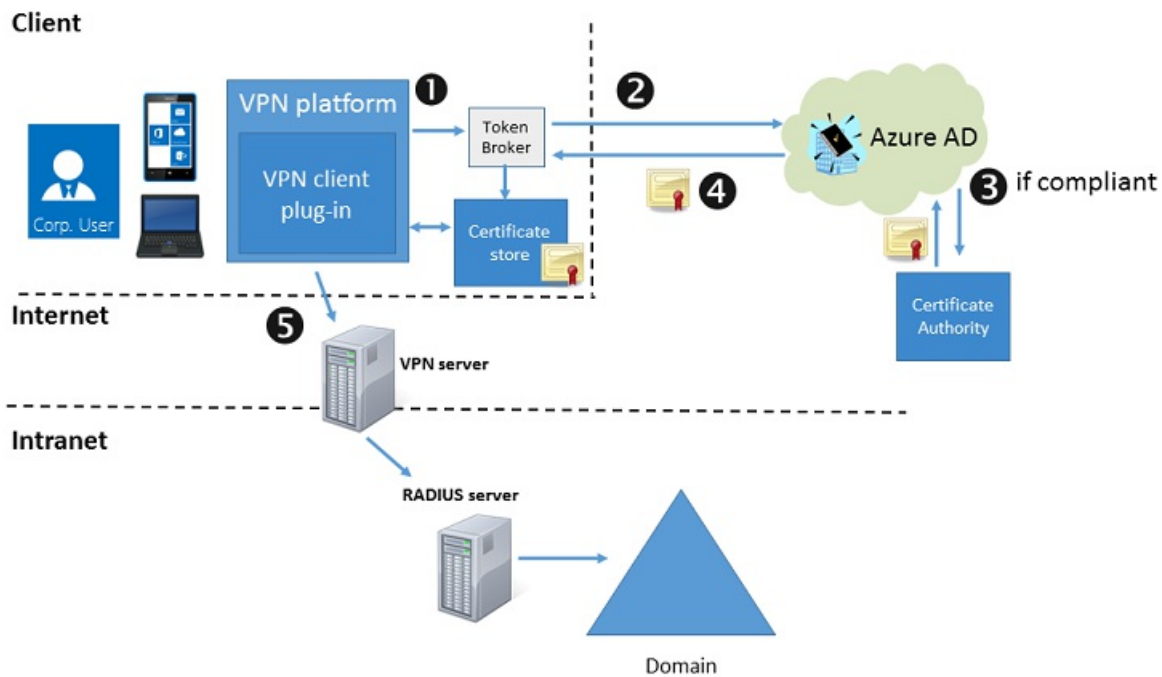
- VPNv2-CSP-DeviceCompliance-Einstellungen
 - **Enabled:** Aktiviert den Gerätekompatibilitätsfluss vom Client. Wenn als **wahr** markiert, versucht der VPN-Client, mit Azure AD zu kommunizieren, um ein Zertifikat für die Authentifizierung zu erhalten. Das VPN sollte für die Verwendung der Zertifikatauthentifizierung eingerichtet werden, und der VPN-Server muss dem von AzureAD zurückgegebenen Server vertrauen.
 - **SSO:** Einträge unter SSO sollten verwendet werden, um den VPN-Client dazu zu verleiten, ein anderes Zertifikat als das VPN-Authentifizierungszertifikat zu verwenden, wenn auf Ressourcen zugegriffen wird, die Kerberos-Authentifizierung erfordern.
 - **SSO/Enabled:** Wenn dieses Feld auf "**true**" festgelegt ist, sucht der VPN-Client nach einem separaten Zertifikat für die Kerberos-Authentifizierung.
 - **Sso/IssuerHash:** Hashes für den VPN-Client, um nach dem richtigen Zertifikat für die Kerberos-Authentifizierung zu suchen.
 - **Sso/Eku:** Eine durch Komma getrennte Liste mit EKU-Erweiterungen (Enhanced Key Usage, erweiterte Schlüsselerweiterung) für den VPN-Client, um nach dem richtigen Zertifikat für die Kerberos-Authentifizierung zu suchen.
- HealthAttestation-CSP (keine Voraussetzung) – vom HealthAttestation-CSP ausgeführte Funktionen:
 - Sammeln von TPM-Daten, mit denen Integritätszustände überprüft werden
 - Weiterleitung der Daten an den Integritätsnachweisdienst (Health Attestation Service, HAS)
 - Bereitstellen des vom HAS empfangenen Integritätsnachweiszertifikats
 - Auf Anforderung werden das (vom HAS erhaltene) Integritätsnachweiszertifikat und zugehörige Laufzeitinformationen zur Überprüfung an den MDM-Server weitergeleitet.

NOTE

Derzeit ist es erforderlich, dass Zertifikate von einer lokalen Zertifizierungsstelle ausgestellt werden und dass SSO im VPN-Profil des Benutzers aktiviert wird. Auf diese Weise kann der Benutzer Kerberos-Tickets abrufen, um auf Ressourcen lokal zuzugreifen. Kerberos unterstützt derzeit nicht die Verwendung von Azure AD-Zertifikaten.

Clientverbindungsfluss

Der VPN-clientseitige Verbindungs Fluss funktioniert wie folgt:



Wenn ein VPNv2-Profil mit `\\ true< /Enabled>` der VPN-Client diesen Verbindungs Fluss verwendet:

1. Der VPN-Client ruft den Azure AD-Token-Broker von Windows 10 auf und identifiziert sich selbst als VPN-Client.
2. Der Azure AD-Tokenbroker authentifiziert sich bei Azure AD und stellt Informationen zu dem Gerät bereit, das versucht, eine Verbindung herzustellen. Der Azure AD-Server prüft, ob das Gerät die Richtlinien erfüllt.
3. Falls ja, fordert Azure AD ein Zertifikat mit kurzer Laufzeit an.
4. Azure AD übergibt über den Tokenbroker ein Zertifikat mit kurzer Laufzeit an den Zertifikatspeicher. Der Tokenbroker gibt anschließend zur weiteren Verbindungsverarbeitung die Steuerung zurück an den VPN-Client.
5. Der VPN-Client nutzt das von Azure AD ausgegebene Zertifikat für die Authentifizierung beim VPN-Server.

Konfigurieren des bedingten Zugriffs

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

Weitere Informationen zu bedingtem Zugriff und Azure AD Health

- [Bedingter Zugriff in Azure Active Directory](#)
- [Erste Schritte mit bedingtem Zugriff in Azure Active Directory](#)
- [Kontrollieren der Integrität Windows10-basierter Geräte](#)
- [Tipps und Tricks: Das Conditional Access Framework und Gerätecompliance für VPN \(Teil 1\)](#)
- [Tipps und Tricks: Das Conditional Access Framework und Gerätecompliance für VPN \(Teil 2\)](#)
- [Tipps und Tricks: Das Conditional Access Framework und Gerätecompliance für VPN \(Teil 3\)](#)
- [Tipps und Tricks: Das Conditional Access Framework und Gerätecompliance für VPN \(Teil 4\)](#)

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN-Authentifizierungsoptionen](#)

- [VPN-Namensauflösung](#)
- [Automatisch ausgelöste VPN-Profiloptionen](#)
- [VPN-Sicherheitsfeatures](#)
- [VPN-Profiloptionen](#)

VPN-Namensauflösung

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Wenn der VPN-Client eine Verbindung mit dem VPN-Server herstellt, empfängt der VPN-Client die Client-IP-Adresse. Der Client erhält unter Umständen auch die IP-Adresse des DNS-Servers (Domain Name System) und die IP-Adresse des WINS-Servers (Windows Internet Name Service).

Die Einstellung für die Namensauflösung im VPN-Profil konfiguriert, wie die Namensauflösung für das System erfolgt, wenn eine VPN-Verbindung besteht. Der Netzwerkstapel sucht zunächst in der Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT) nach Übereinstimmungen und probiert im Falle einer Übereinstimmung die Auflösung. Wird keine Übereinstimmung gefunden, wird das DNS-Suffix für die bevorzugte Schnittstelle basierend auf der Schnittstellenmetrik an den Namen angehängt (im Fall eines Kurznamens). Zudem wird eine DNS-Abfrage an die bevorzugte Schnittstelle gesendet. Tritt bei der Abfrage eine Zeitüberschreitung auf, wird die DNS-Suffixsuchliste der Reihenfolge nach durchgegangen, und DNS-Abfragen werden für alle Schnittstellen gesendet.

Richtlinientabelle für die Namensauflösung (Name Resolution Policy Table, NRPT)

Die NRPT ist eine Tabelle mit Namespaces, die das Verhalten des DNS-Clients beim Ausgeben von Abfragen zur Namensauflösung und beim Verarbeiten von Antworten bestimmt. Hier sucht der Stapel zuerst nach „DNSCache“.

Es gibt drei Arten von übereinstimmenden Namen, die für NRPT eingerichtet werden können:

- Vollqualifizierter Domänenname (FQDN), der für die direkte Zuordnung zu einem Namen verwendet werden kann
- Eine Suffixübereinstimmung führt entweder zu einem Vergleich der Suffixe (zur FQDN-Auflösung) oder zum Anfügen des Suffixes (im Fall eines Kurznamens).
- Bei jeder Auflösung sollte zunächst versucht werden, die Auflösung mit dem Proxyserver/DNS-Server mit diesem Eintrag auszuführen.

NRPT wird mithilfe des [VPNv2 CSP](#)-Knotens **VPNv2/ProfileName/DomainNameInformationList** festgelegt. Dieser Knoten konfiguriert auch den Webproxyserver oder Domänennamenserver.

[Weitere Informationen zur NRPT](#)

DNS-Suffix

Mit dieser Einstellung werden das primäre DNS-Suffix für die VPN-Schnittstelle und die Suffixsuchliste konfiguriert, nachdem die VPN-Verbindung eingerichtet wurde.

Das primäre DNS-Suffix wird mithilfe des Knotens **VPNv2/ProfileName/DnsSuffix** festgelegt.

[Weitere Informationen zum primären DNS-Suffix](#)

Permanent

Sie können auch Regeln für die *permanente* Namensauflösung konfigurieren. Die Namensauflösung für bestimmte Elemente erfolgt ausschließlich per VPN.

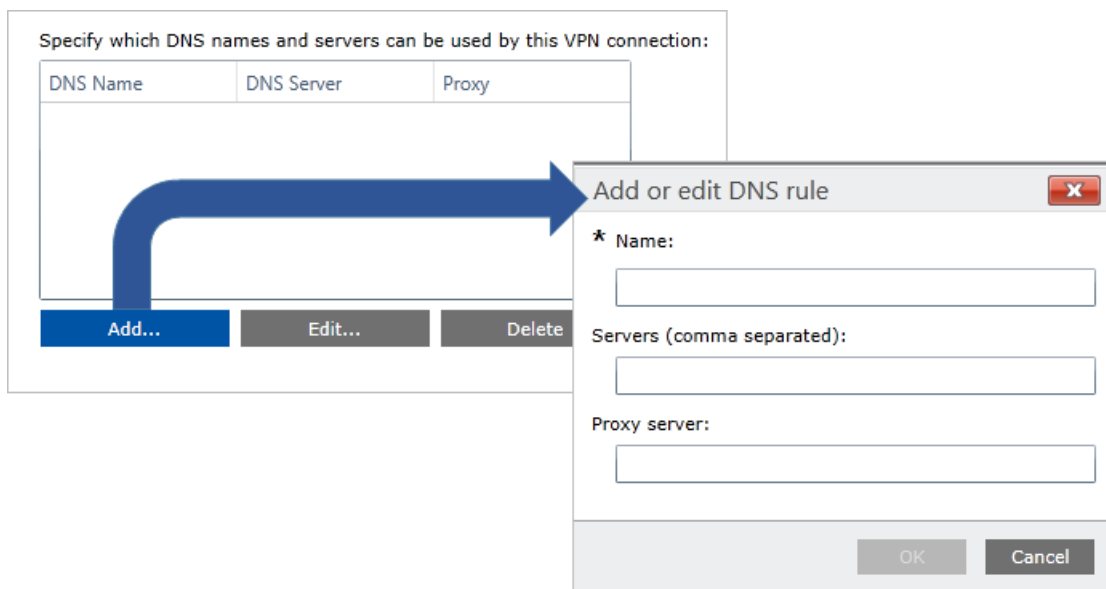
Die permanente Namensauflösung wird mithilfe des Knotens

VPNv2/ProfileName/DomainNameInformationList/dniRowId/Persistent festgelegt.

Konfigurieren der Namensauflösung

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

Die folgende Abbildung zeigt Namensauflösungsoptionen in einer VPN-Profilkonfigurationsrichtlinie mit Microsoft Intune.



Die Felder im Dialogfeld **DNS-Regel hinzufügen oder bearbeiten** im Intune-Profil entsprechen den XML-Einstellungen in der folgenden Tabelle:

FELD	XML
Name	VPNv2/ProfileName/DomainNameInformationList/dniRowId/DomainName
Server (durch Komma getrennt)	VPNv2/ProfileName/DomainNameInformationList/dniRowId/DnsServers
Proxyserver	VPNv2/ProfileName/DomainNameInformationList/dniRowId/WebServers

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN-Authentifizierungsoptionen](#)
- [VPN und bedingter Zugriff](#)
- [Automatisch ausgelöste VPN-Profiloptionen](#)
- [VPN-Sicherheitsfeatures](#)

- [VPN-Profiloptionen](#)

Automatisch ausgelöste VPN-Profiloptionen

12.09.2019 • 3 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Unter Windows 10 wurde eine Reihe von Features für die automatische VPN-Auslösung hinzugefügt, sodass Benutzer nicht manuell eine Verbindung herstellen müssen, wenn VPN für den Zugriff auf erforderliche Ressourcen benötigt wird. Es gibt drei verschiedene Arten von Regeln für die automatische Auslösung:

- App-Auslöser
- Namenbasierter Auslöser
- Always On

App-Auslöser

VPN-Profile in Windows 10 können so konfiguriert werden, dass beim Start eines angegebenen Satzes von Anwendungen automatisch eine Verbindung hergestellt wird. Sie können Desktop-Apps oder Apps für die universelle Windows-Plattform (UWP) für die Auslösung einer VPN-Verbindung konfigurieren. Außerdem können Sie App-basiertes VPN konfigurieren und bestimmte Datenverkehrsregeln für jede App angeben. Weitere Details finden Sie unter [Datenverkehrsfilter](#).

Bei der App-ID für eine Desktop-App handelt es sich um einen Dateipfad. Die App-ID für eine UWP-App ist ein Paketfamilienname.

[Suchen eines Paketfamiliennamens \(PFN\) für eine Konfiguration mit VPN pro App](#)

Namenbasierter Auslöser

Sie können eine auf dem Domänennamen basierende Regel konfigurieren, sodass ein bestimmter Domänenname die VPN-Verbindung auslöst.

Der namenbasierte automatische Auslöser kann mithilfe der Einstellung „VPNv2/ProfileName/DomainNameInformationList/dniRowId/AutoTrigger“ unter [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#) konfiguriert werden.

Es gibt vier Arten von namenbasierten Auslösern:

- Kurzname: Wenn **HRweb** beispielsweise als Auslöser konfiguriert wird und der Stapel eine DNS-Auflösungsanforderung für **HRweb** erkennt, wird die VPN-Verbindung ausgelöst.
- Vollqualifizierter Domänenname (FQDN): Wenn **HRweb.corp.contoso.com** beispielsweise als Auslöser konfiguriert wird und der Stapel eine DNS-Auflösungsanforderung für **HRweb.corp.contoso.com** erkennt, wird die VPN-Verbindung ausgelöst.
- Suffix: Wenn **.corp.contoso.com** beispielsweise als Auslöser konfiguriert wird und der Stapel eine DNS-Auflösungsanforderung mit einem übereinstimmenden Suffix (z.B. **HRweb.corp.contoso.com**) erkennt, wird die VPN-Verbindung ausgelöst. Bei jeder Auflösung eines Kurznamens wird die VPN-Verbindung ausgelöst, und der DNS-Server wird auf **ShortName.corp.contoso.com** abgefragt.
- Alle: In diesem Fall sollte jede DNS-Auflösung ein VPN auslösen.

Always On

Always On ist ein Feature in Windows 10, mit dem das aktive VPN-Profil für die folgenden Auslöser automatisch eine Verbindung herstellen kann:

- Benutzeranmeldung
- Netzwerkänderung
- Einschalten des Gerätebildschirms

Beim Auslösen des Auslösers versucht das VPN, eine Verbindung herzustellen. Wenn ein Fehler auftritt oder eine Benutzereingabe erforderlich ist, wird dem Benutzer eine Pop-upbenachrichtigung zur weiteren Interaktion angezeigt.

Wenn ein Gerät über mehrere Profile mit Always On-Auslösern verfügt, kann der Benutzer das aktive Profil in **Einstellungen > Netzwerk und Internet > VPN > VPN-Profil** angeben, indem er das Kontrollkästchen **Apps automatisch diese VPN-Verbindung verwenden lassen** aktiviert. Das erste mit MDM konfigurierte Profil ist standardmäßig als **Aktiv** gekennzeichnet. Geräte mit mehreren Benutzern haben die gleiche Einschränkung: nur ein Profil und daher kann nur ein Benutzer die immer auf-Trigger verwenden.

Beibehalten des Benutzers immer nach Wunsch

Windows verfügt über ein Feature, um die AlwaysOn-Einstellung eines Benutzers beizubehalten. Für den Fall, dass ein Benutzer das Kontrollkästchen "automatisch verbinden" deaktiviert, speichert Windows diese Benutzereinstellung für diesen Profilnamen, indem der Profilname dem Wert AutoTriggerDisabledProfilesList hinzugefügt wird.

Wenn ein Verwaltungstool denselben Profilnamen wieder entfernt/hinzugefügt und AlwaysOn auf "true" festgelegt hat, wird das Feld nicht aktiviert, wenn der Profilname im folgenden Registrierungswert vorhanden ist, um die Benutzereinstellungen beizubehalten. Schlüssel:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Config-Wert:

AutoTriggerDisabledProfilesList-Typ: REG_MULTI_SZ

Erkennen vertrauenswürdiger Netzwerke

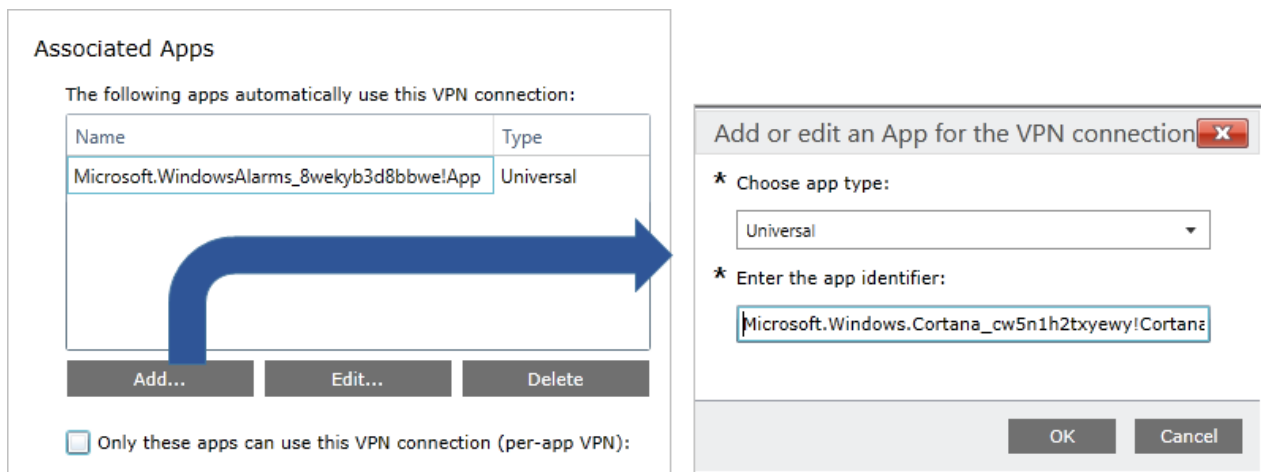
Mit diesem Feature wird das VPN so konfiguriert, dass es nicht ausgelöst wird, wenn sich ein Benutzer in einem vertrauenswürdigen Unternehmensnetzwerk befindet. Der Wert für diese Einstellung ist eine Liste mit DNS-Suffixen. Der VPN-Stapel überprüft das DNS-Suffix auf der physischen Schnittstelle. Wenn es mit einem Suffix in der konfigurierten Liste übereinstimmt und das Netzwerk privat ist oder von MDM bereitgestellt wird, wird das VPN nicht ausgelöst.

Die Erkennung vertrauenswürdiger Netzwerke kann mithilfe der Einstellung „VPNv2/ProfileName/TrustedNetworkDetection“ unter [VPNv2-CSP](#) konfiguriert werden.

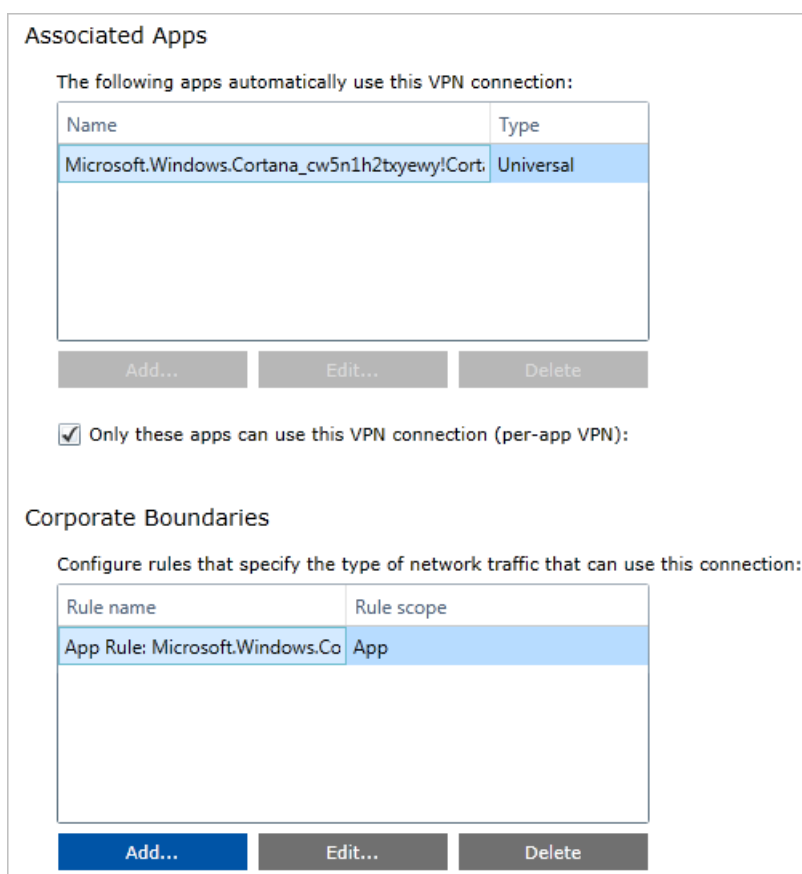
Konfigurieren eines durch Apps ausgelösten VPN

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

In der folgenden Abbildung wird gezeigt, wie eine App mithilfe von Microsoft Intune einer VPN-Verbindung in einer VPN-Profilkonfigurationsrichtlinie zugeordnet wird.



Wenn Sie eine zugeordnete App hinzugefügt haben und das Kontrollkästchen **Nur diese Apps können diese VPN-Verbindung verwenden (VPN pro App)**: aktivieren, ist die App unter **Unternehmensgrenzen** verfügbar. Dort können Sie Regeln für die App konfigurieren. Weitere Details finden Sie unter [DatenverkehrsfILTER](#).



Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN-Authentifizierungsoptionen](#)
- [VPN und bedingter Zugriff](#)
- [VPN-Namensauflösung](#)
- [VPN-Sicherheitsfeatures](#)
- [VPN-Profiloptionen](#)

VPN-Sicherheitsfeatures

12.09.2019 • 2 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

VPN-Sperrmodus

Ein mit Sperrmodus konfiguriertes VPN-Profil schützt das Gerät, indem nur Netzwerkdatenverkehr über die VPN-Schnittstelle zugelassen wird. Es verfügt über die folgenden Features:

- Das System versucht, das VPN jederzeit verbunden zu halten.
- Der Benutzer kann die VPN-Verbindung nicht trennen.
- Der Benutzer kann das VPN-Profil nicht löschen oder ändern.
- Das VPN-Sperrmodus-Profil verwendet eine erzwungene Tunnelverbindung.
- Wenn die VPN-Verbindung nicht verfügbar ist, wird der ausgehende Netzwerkdatenverkehr blockiert.
- Auf einem Gerät ist nur ein VPN-Sperrmodus-Profil zulässig.

NOTE

Für integriertes VPN ist der VPN-Sperrmodus nur für den Verbindungstyp von Version2 des Internetschlüsselaustauschs (Internet Key Exchange Version 2, IKEv2) verfügbar.

Stellen Sie dieses Feature mit Bedacht bereit, da die resultierende Verbindung keinen Netzwerkdatenverkehr senden oder empfangen kann, wenn keine VPN-Verbindung besteht.

WIP-Integration (Windows Information Protection) in VPN

Dank der Funktionen von Windows Information Protection können Unternehmensdaten separat gehandhabt und vor der Offenlegung sowohl auf geschäftlichen als auch privaten Geräten geschützt werden, ohne dass dazu zusätzliche Änderungen an den Umgebungen oder den Apps selbst erforderlich sind. Darüber hinaus kann WIP bei Verwendung in Verbindung mit Rights Management Services (RMS) zum lokalen Schutz von Unternehmensdaten beitragen.

Der Knoten **EdpModelId** unter [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#) ermöglicht einem Windows10-VPN-Client die Integration in WIP, wodurch die Funktionen auch auf Remotegeräte ausgeweitet werden.

Anwendungsfälle für WIP:

- Kernfunktionen: Dateiverschlüsselung und Blockierung des Dateizugriffs
- UX-Richtlinienerzwingung: Einschränken von Vorgängen zum Kopieren/Einfügen, Ausführen von Drag & Drop und Freigeben
- WIP-Netzwerkrichtlinienerzwingung: Schützen von Intranetressourcen über das Unternehmensnetzwerk und VPN
- Netzwerkrichtlinienerzwingung: Schützen von SMB- und Internetcloudressourcen über das Unternehmensnetzwerk und VPN

Der Wert von **EdpModelId** ist eine Unternehmens-ID. Der Netzwerkstapel sucht im App-Token nach dieser ID, um zu ermitteln, ob das VPN für diese bestimmte App ausgelöst werden sollte.

Beim Herstellen einer Verbindung mit WIP muss der Administrator zudem in diesem Profil die AppTriggerList- und die TrafficFilterList-Regel nicht separat angeben (sofern keine komplexere Konfiguration erforderlich ist), da die WIP-Richtlinien und App-Listen automatisch wirksam werden.

[Weitere Informationen zu Windows Information Protection](#)

Datenverkehrsfilter

Mit Datenverkehrsfiltern können Unternehmen anhand von Richtlinien festlegen, welche Art von Datenverkehr im Unternehmensnetzwerk zugelassen wird. Effektives Hinzufügen von schnittstellenspezifischen Firewallregeln für die VPN-Schnittstelle durch Netzwerkadministratoren. Es gibt zwei Arten von Regeln für Datenverkehrsfilter:

- App-basierte Regeln. Mit anwendungsbasierten Regeln kann eine Anwendungsliste so gekennzeichnet werden, dass nur von diesen Anwendungen stammender Datenverkehr die VPN-Schnittstelle passieren darf.
- Datenverkehrs-basierte Regeln. Datenverkehrs-basierte Regeln sind 5-Tupel-Richtlinien (Ports, Adressen, Protokoll), die so festgelegt werden können, dass nur diesen Regeln entsprechender Datenverkehr die VPN-Schnittstelle passieren darf.

Es können mehrere Regelsätze mit OR verknüpft werden. In jedem Satz können anwendungs- und datenverkehrs-basierte Regeln vorhanden sein. Alle Eigenschaften innerhalb des Satzes werden mit „AND“ verknüpft. Darüber hinaus können diese Regeln App-basiert oder gerätebasiert angewendet werden.

Beispielsweise kann ein Administrator Regeln definieren, die Folgendes angeben:

- Die Contoso HR-App muss das VPN passieren dürfen und nur auf Port 4545 zugreifen.
- Die Contoso Finance-Apps dürfen das VPN passieren und nur auf die Remote-IP-Bereiche 10.10.0.40 bis 10.10.0.201 an Port 5889 zugreifen.
- Alle anderen Apps auf dem Gerät dürfen nur auf die Ports 80 und 443 zugreifen.

Konfigurieren von Datenverkehrsfiltern

Informationen zur XML-Konfiguration finden Sie unter [VPN-Profiloptionen](#) und [VPNv2-CSP](#).

Die folgende Abbildung zeigt die Schnittstelle zum Konfigurieren von Datenverkehrsregeln in einer VPN-Profilkonfigurationsrichtlinie mit Microsoft Intune:

The screenshot shows a dialog box titled "Add or edit a traffic rule" with a close button (X) in the top right corner. The dialog contains several input fields for configuring a traffic rule:

- Rule name:** A text input field with a red asterisk (*) indicating it is required.
- Protocols (0-255):** A text input field.
- Local port range (comma separated):** A text input field.
- Remote port range (comma separated):** A text input field.
- Local address range (comma separated):** A text input field.
- Remote address range (comma separated):** A text input field.

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN-Authentifizierungsoptionen](#)
- [VPN und bedingter Zugriff](#)
- [VPN-Namensauflösung](#)
- [Automatisch ausgelöste VPN-Profiloptionen](#)
- [VPN-Profiloptionen](#)

VPN-Profiloptionen

11.02.2020 • 4 minutes to read

Betrifft

- Windows 10
- Windows 10 Mobile

Die meisten VPN-Einstellungen in Windows 10 können mithilfe von Microsoft Intune oder Microsoft Endpoint Configuration Manager in VPN-Profilen konfiguriert werden. Alle VPN-Einstellungen in Windows 10 können mithilfe des **ProfileXML** -Knotens im [VPNv2-Konfigurationsdienstanbieter \(CSP\)](#) konfiguriert werden.

NOTE

Wenn Sie mit CSPs nicht vertraut sind, lesen Sie zunächst die Informationen unter [Einführung in Konfigurationsdienstanbieter \(Configuration Service Providers, CSPs\)](#).

In der folgenden Tabelle sind die VPN-Einstellungen und eine Angabe dazu aufgeführt, ob die Einstellung in Intune und Configuration Manager oder ausschließlich mithilfe von **ProfileXML** konfiguriert werden kann.

PROFILEINSTELLUNG	KANN IN INTUNE UND CONFIGURATION MANAGER KONFIGURIERT WERDEN
Verbindungsart	ja
Routing: Routen mit geteiltem Tunneling	Ja, mit Ausnahme von Ausschlussrouten
Routing: erzwungenes Tunneling	ja
Authentifizierung (EAP)	Ja, wenn der Verbindungstyp integriert ist
Bedingter Zugriff	ja
Proxyeinstellungen	Ja, mit PAC-/WPAD-Datei oder mit Server und Port
Namensauflösung: NRPT	ja
Namensauflösung: DNS-Suffix	nein
Namensauflösung: permanent	nein
Automatische Auslösung: App-Trigger	ja
Automatische Auslösung: Namensauslöser	Ja
Automatische Auslösung: Always On	ja
Automatische Auslösung: Erkennen vertrauenswürdiger Netzwerke	Nein

PROFILEEINSTELLUNG	KANN IN INTUNE UND CONFIGURATION MANAGER KONFIGURIERT WERDEN
Sperrmodus	Nein
Windows Information Protection (WIP)	ja
Datenverkehrsfilter	Ja

Der ProfileXML-Knoten wurde dem VPNv2-CSP hinzugefügt, um Benutzern die Bereitstellung eines VPN-Profiles als einzelnes Blob zu ermöglichen. Dies ist besonders hilfreich für die Bereitstellung von Profilen mit Features, die von MDMs noch nicht unterstützt werden. Weitere Beispiele finden Sie im Thema [ProfileXML-XSD](#).

Beispiel für ein natives VPN-Profil

Hier sehen Sie ein Beispiel für ein natives VPN-Profil. Dieses Blob fällt unter den ProfileXML-Knoten.

```
<VPNProfile>
  <ProfileName>TestVpnProfile</ProfileName>
  <NativeProfile>
    <Servers>testServer.VPN.com</Servers>
    <NativeProtocolType>IKEv2</NativeProtocolType>

    <!--Sample EAP profile (PEAP)-->
    <Authentication>
      <UserMethod>Eap</UserMethod>
      <MachineMethod>Eap</MachineMethod>
    <Eap>
      <Configuration>
        <EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
          <EapMethod>
            <Type xmlns="http://www.microsoft.com/provisioning/EapCommon">25</Type>
            <VendorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorId>
            <VendorType xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorType>
            <AuthorId xmlns="http://www.microsoft.com/provisioning/EapCommon">0</AuthorId>
          </EapMethod>
          <Config xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
            <Eap xmlns="http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1">
              <Type>25</Type>
              <EapType xmlns="http://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV1">
                <ServerValidation>
                  <DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
                  <ServerNames></ServerNames>
                  <TrustedRootCA>d2 d3 8e ba 60 ca a1 c1 20 55 a2 e1 c8 3b 15 ad 45 01 10 c2
                </TrustedRootCA>
                  <TrustedRootCA>d1 76 97 cc 20 6e d2 6e 1a 51 f5 bb 96 e9 35 6d 6d 61 0b 74
                </TrustedRootCA>
                </ServerValidation>
                <FastReconnect>true</FastReconnect>
                <InnerEapOptional>false</InnerEapOptional>
              <Eap xmlns="http://www.microsoft.com/provisioning/BaseEapConnectionPropertiesV1">
                <Type>13</Type>
                <EapType xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV1">
                  <CredentialsSource>
                    <CertificateStore>
                      <SimpleCertSelection>true</SimpleCertSelection>
                    </CertificateStore>
                  </CredentialsSource>
                  <ServerValidation>
                    <DisableUserPromptForServerValidation>true</DisableUserPromptForServerValidation>
                    <ServerNames></ServerNames>
                    <TrustedRootCA>d2 d3 8e ba 60 ca a1 c1 20 55 a2 e1 c8 3b 15 ad 45 01 10 c2
```

```

</TrustedRootCA>
    <TrustedRootCA>d1 76 97 cc 20 6e d2 6e 1a 51 f5 bb 96 e9 35 6d 6d 61 0b 74
</TrustedRootCA>
    </ServerValidation>
    <DifferentUsername>false</DifferentUsername>
    <PerformServerValidation
xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">true</PerformServerValidation>
    <AcceptServerName
xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">false</AcceptServerName>
    <TLSExtensions
xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV2">
    <FilteringInfo
xmlns="http://www.microsoft.com/provisioning/EapTlsConnectionPropertiesV3">
        <EKUMapping>
            <EKUMap>
                <EKUName>AAD Conditional Access</EKUName>
                <EKUOID>1.3.6.1.4.1.311.87</EKUOID>
            </EKUMap>
        </EKUMapping>
        <ClientAuthEKUList Enabled="true">
            <EKUMapInList>
                <EKUName>AAD Conditional Access</EKUName>
            </EKUMapInList>
        </ClientAuthEKUList>
    </FilteringInfo>
    </TLSExtensions>
</EapType>
</Eap>
<EnableQuarantineChecks>false</EnableQuarantineChecks>
<RequireCryptoBinding>true</RequireCryptoBinding>
<PeapExtensions>
    <PerformServerValidation
xmlns="http://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">true</PerformServerValidation>
    <AcceptServerName
xmlns="http://www.microsoft.com/provisioning/MsPeapConnectionPropertiesV2">false</AcceptServerName>
</PeapExtensions>
</EapType>
</Eap>
</Config>
</EapHostConfig>
</Configuration>
</Eap>
</Authentication>

<!--Sample routing policy: in this case, this is a split tunnel configuration with two routes
configured-->
    <RoutingPolicyType>SplitTunnel</RoutingPolicyType>
    <DisableClassBasedDefaultRoute>true</DisableClassBasedDefaultRoute>
</NativeProfile>
    <Route>
        <Address>192.168.0.0</Address>
        <PrefixSize>24</PrefixSize>
    </Route>
    <Route>
        <Address>10.10.0.0</Address>
        <PrefixSize>16</PrefixSize>
    </Route>

<!--VPN will be triggered for the two apps specified here-->
<AppTrigger>
    <App>
        <Id>Microsoft.MicrosoftEdge_8wekyb3d8bbwe</Id>
    </App>
</AppTrigger>
<AppTrigger>
    <App>
        <Id>C:\windows\system32\ping.exe</Id>
    </App>
</AppTrigger>

```



```

    <!--Example of per-app VPN. This configures traffic filtering rules for two apps. Internet Explorer is
    configured for force tunnel, meaning that all traffic allowed through this app must go over VPN. Microsoft
    Edge is configured as split tunnel, so whether data goes over VPN or the physical interface is dictated by
    the routing configuration.-->
    <TrafficFilter>
      <App>
        <Id>%ProgramFiles%\Internet Explorer\iexplore.exe</Id>
      </App>
      <Protocol>6</Protocol>
      <LocalPortRanges>10,20-50,100-200</LocalPortRanges>
      <RemotePortRanges>20-50,100-200,300</RemotePortRanges>
      <RemoteAddressRanges>30.30.0.0/16,10.10.10.10-20.20.20.20</RemoteAddressRanges>
      <RoutingPolicyType>ForceTunnel</RoutingPolicyType>
    </TrafficFilter>
    <TrafficFilter>
      <App>
        <Id>Microsoft.MicrosoftEdge_8wekyb3d8bbwe</Id>
      </App>
      <LocalAddressRanges>3.3.3.3/32,1.1.1.1-2.2.2.2</LocalAddressRanges>
    </TrafficFilter>

    <!--Name resolution configuration. The AutoTrigger node configures name-based triggering. In this
    profile, the domain "hrs.site.corporate.contoso.com" triggers VPN.-->
    <DomainNameInformation>
      <DomainName>hrs.site.corporate.contoso.com</DomainName>
      <DnsServers>1.2.3.4,5.6.7.8</DnsServers>
      <WebProxyServers>5.5.5.5</WebProxyServers>
      <AutoTrigger>true</AutoTrigger>
    </DomainNameInformation>
    <DomainNameInformation>
      <DomainName>.corp.contoso.com</DomainName>
      <DnsServers>10.10.10.10,20.20.20.20</DnsServers>
      <WebProxyServers>100.100.100.100</WebProxyServers>
    </DomainNameInformation>

    <!--EDPMode is turned on for the enterprise ID "corp.contoso.com". When a user accesses an app with that
    ID, VPN will be triggered.-->
    <EdpModeId>corp.contoso.com</EdpModeId>
    <RememberCredentials>true</RememberCredentials>

    <!--Always On is turned off, and triggering VPN for the apps and domain name specified earlier in the
    profile will not occur if the user is connected to the trusted network "contoso.com".-->
    <AlwaysOn>false</AlwaysOn>
    <DnsSuffix>corp.contoso.com</DnsSuffix>
    <TrustedNetworkDetection>contoso.com</TrustedNetworkDetection>
    <Proxy>
      <Manual>
        <Server>HelloServer</Server>
      </Manual>
      <AutoConfigUrl>Helloworld.Com</AutoConfigUrl>
    </Proxy>

    <!--Device compliance is enabled and an alternate certificate is specified for domain resource
    authentication.-->
    <DeviceCompliance>
      <Enabled>true</Enabled>
      <Sso>
        <Enabled>true</Enabled>
        <Eku>This is my Eku</Eku>
        <IssuerHash>This is my issuer hash</IssuerHash>
      </Sso>
    </DeviceCompliance>
  </VPNProfile>

```

Beispiel für ein Plug-In- VPN-Profil

Hier sehen Sie ein Beispiel für ein Plug-In-VPN-Profil. Dieses Blob fällt unter den ProfileXML-Knoten.

```
<VPNProfile>
  <ProfileName>TestVpnProfile</ProfileName>
  <PluginProfile>
    <ServerUrlList>testserver1.contoso.com;testserver2.contoso..com</ServerUrlList>
    <PluginPackageFamilyName>JuniperNetworks.JunosPulseVpn_cw5n1h2txyewy</PluginPackageFamilyName>
    <CustomConfiguration>&lt;pulse-
schema&gt;&lt;isSingleSignOnCredential&gt;true&lt;/isSingleSignOnCredential&gt;&lt;/pulse-schema&gt;
</CustomConfiguration>
  </PluginProfile>
  <Route>
    <Address>192.168.0.0</Address>
    <PrefixSize>24</PrefixSize>
  </Route>
  <Route>
    <Address>10.10.0.0</Address>
    <PrefixSize>16</PrefixSize>
  </Route>
  <AppTrigger>
    <App>
      <Id>Microsoft.MicrosoftEdge_8wekyb3d8bbwe</Id>
    </App>
  </AppTrigger>
  <AppTrigger>
    <App>
      <Id>%ProgramFiles%\Internet Explorer\iexplore.exe</Id>
    </App>
  </AppTrigger>
  <TrafficFilter>
    <App>
      <Id>%ProgramFiles%\Internet Explorer\iexplore.exe</Id>
    </App>
    <Protocol>6</Protocol>
    <LocalPortRanges>10,20-50,100-200</LocalPortRanges>
    <RemotePortRanges>20-50,100-200,300</RemotePortRanges>
    <RemoteAddressRanges>30.30.0.0/16,10.10.10.10-20.20.20.20</RemoteAddressRanges>
    <!--<RoutingPolicyType>ForceTunnel</RoutingPolicyType-->
  </TrafficFilter>
  <TrafficFilter>
    <App>
      <Id>Microsoft.MicrosoftEdge_8wekyb3d8bbwe</Id>
    </App>
    <LocalAddressRanges>3.3.3.3/32,1.1.1.1-2.2.2.2</LocalAddressRanges>
  </TrafficFilter>
  <TrafficFilter>
    <App>
      <Id>Microsoft.MicrosoftEdge_8wekyb3d8bbwe</Id>
    </App>
    <Claims>0:SYG:SYD:(A;;CC;;;AU)</Claims>
    <!--<RoutingPolicyType>SplitTunnel</RoutingPolicyType-->
  </TrafficFilter>
  <DomainNameInformation>
    <DomainName>corp.contoso.com</DomainName>
    <DnsServers>1.2.3.4,5.6.7.8</DnsServers>
    <WebProxyServers>5.5.5.5</WebProxyServers>
    <AutoTrigger>false</AutoTrigger>
  </DomainNameInformation>
  <DomainNameInformation>
    <DomainName>corp.contoso.com</DomainName>
    <DnsServers>10.10.10.10,20.20.20.20</DnsServers>
    <WebProxyServers>100.100.100.100</WebProxyServers>
  </DomainNameInformation>
  <!--<EdpModeId>corp.contoso.com</EdpModeId-->
  <RememberCredentials>true</RememberCredentials>
  <AlwaysOn>false</AlwaysOn>
  <DnsSuffix>corp.contoso.com</DnsSuffix>
  <TrustedNetworkDetection>contoso.com,test.corp.contoso.com</TrustedNetworkDetection>
</VPNProfile>
```

```

<Proxy>
  <Manual>
    <Server>HelloServer</Server>
  </Manual>
  <AutoConfigUrl>Helloworld.Com</AutoConfigUrl>
</Proxy>
</VPNProfile>

```

Anwenden von ProfileXML mithilfe von Intune

Nachdem Sie die gewünschten Einstellungen mit „ProfileXML“ konfiguriert haben, können Sie den Knoten mit Intune und der Richtlinie **Benutzerdefinierte Konfiguration (Windows 10 Desktop und Mobile und höher)** anwenden.

1. Anmelden beim [Azure-Portal](#)
2. Wechseln Sie zu **InTune > Device Configuration > profile**.
3. Klicken Sie auf **Profil erstellen**.
4. Geben Sie einen Namen und (optional) eine Beschreibung ein.
5. Wählen Sie **Windows 10 und höher** als Plattform aus.
6. Wählen Sie **Benutzerdefiniert** als Profiltyp aus, und klicken Sie auf **Hinzufügen**.
7. Geben Sie einen Namen und (optional) eine Beschreibung ein.
8. Geben Sie den OMA-URI **/User/Vendor/MSFT/VPNv2/-VPN-Profilnamen/ProfileXML** ein.
9. Legen Sie den Datentyp auf **String (XML-Datei)**.
10. Laden Sie die Profil-XML-Datei hoch.
11. Klicken Sie auf **OK**.

The screenshot displays three panels from the Microsoft Intune console:

- Create profile:** Shows the 'Name' field set to 'Custom VPN Profile for Windows 10', 'Platform' set to 'Windows 10 and later', and 'Profile type' set to 'Custom'.
- Custom OMA-URI Settings:** Shows a table with columns NAME, DESCRIPTION, OMA-URI, and VALUE. The table is currently empty with the message 'No settings'.
- Add Row:** Shows the 'Name' field set to 'VPNProfileXML', 'OMA-URI' set to '/User/vendor/MSFT/VPN profile name/ProfileXML', and 'Data type' set to 'String (XML file)'. Below this, the 'File contents' section displays the XML configuration for a VPN profile.

The XML configuration shown is:

```

<VPNProfile>
  <ProfileName>TestVpnProfile</ProfileName>
  <NativeProfile>
    <Servers>testServer.VPN.com</Servers>
    <NativeProtocolType>IKEv2</NativeProtocolType>
  </NativeProfile>
  <!--Sample EAP profile (PEAP)-->
  <Authentication>
    <UserMethod>Eap</UserMethod>
    <MachineMethod>Eap</MachineMethod>
  </Authentication>
  <Configuration>
    <EapHostConfig xmlns="http://www.microsoft.com/provisioning/EapHostConfig">
      <EapMethod>
        <Type xmlns="http://www.microsoft.com/provisioning/EapCommon">25</Type>
        <VendorId>
          xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorId>
        <VendorType>
          xmlns="http://www.microsoft.com/provisioning/EapCommon">0</VendorType>
        <AuthId>

```

12. Klicken Sie auf **OK** und dann auf **Erstellen**.
13. Weisen Sie das Profil zu.

Weitere Informationen

- [Informationen zum Konfigurieren von VPN-Verbindungen in Microsoft Intune](#)
- [Referenz zum VPNv2-Konfigurationsdienstanbieter](#)
- [Erstellen von VPN-Profilen in Configuration Manager](#)

Verwandte Themen

- [Technische VPN-Anleitung](#)
- [VPN-Verbindungstypen](#)
- [VPN-Routingentscheidungen](#)
- [VPN-Authentifizierungsoptionen](#)
- [VPN und bedingter Zugriff](#)
- [VPN-Namensauflösung](#)
- [Automatisch ausgelöste VPN-Profiloptionen](#)
- [VPN-Sicherheitsfeatures](#)

So konfigurieren Sie ein Diffie-Hellman-Protokoll über IKEv2-VPN-Verbindungen

12.09.2019 • 2 minutes to read

Gilt für: Windows Server (Semi-Annual Channel), Windows Server 2016, Windows 10

Bei IKEv2-VPN-Verbindungen ist die Standardkonfiguration für die Diffie-Hellman-Gruppe 2. Diese ist für einen IKE-Austausch nicht sicher. Um die Verbindungen zu sichern, aktualisieren Sie die Konfiguration des VPN-Servers und des Clients durch das Ausführen von VPN-Cmdlets.

VPN-Server

Für VPN-Server, auf denen Windows Server 2012 R2 oder höher ausgeführt wird, müssen Sie [Set-VpnServerConfiguration](#) ausführen, um den Tunneltyp zu konfigurieren. Dadurch verwendet der IKE Austausch auf dem IKEv2-Tunnel die sichere Konfiguration.

```
Set-VpnServerConfiguration -TunnelType IKEv2 -CustomPolicy
```

Führen Sie auf den früheren Versionen von Windows Server [Set-VpnServerIPsecConfiguration](#) aus. Da

`Set-VpnServerIPsecConfiguration` nicht über `-TunnelType` verfügt, wirkt sich die Konfiguration auf alle Tunneltypen auf dem Server aus.

```
Set-VpnServerIPsecConfiguration -CustomPolicy
```

VPN-Client

Bei VPN-Clients müssen Sie jede VPN-Verbindung konfigurieren. Führen Sie z.B. [Set-VpnConnectionIPsecConfiguration \(Version 4.0\)](#) aus und geben Sie den Namen der Verbindung an:

```
Set-VpnConnectionIPsecConfiguration -ConnectionName <String>
```

Einmaliges Anmelden (SSO) über VPN- und WLAN-Verbindungen

12.09.2019 • 4 minutes to read

In diesem Thema werden die Anforderungen erläutert, mit denen einmaliges Anmelden (Single Sign-on, SSO) für lokale Domänenressourcen über WLAN- oder VPN-Verbindungen ermöglicht wird. Das Szenario lautet:

- Sie stellen eine Verbindung mit einem Netzwerk über WLAN oder VPN her.
- Sie möchten die Anmeldeinformationen, die Sie für die WLAN- oder VPN-Authentifizierung verwenden, auch zum Authentifizieren von Anforderungen für den Zugriff auf eine Domänenressource verwenden, mit der Sie eine Verbindung herstellen, ohne dass Sie separat zur Eingabe Ihrer Domänenanmeldeinformationen aufgefordert werden.

So möchten Sie beispielsweise eine Verbindung mit einem Unternehmensnetzwerk herstellen und auf eine interne Website zugreifen, für die die Windows-integrierte Authentifizierung erforderlich ist.

Auf einem hohen Niveau ist die Art und Weise, wie dies funktioniert, dass die Anmeldeinformationen, die für die Verbindungsauthentifizierung verwendet werden, im Anmelde Informations-Manager als Standardanmeldeinformationen für die Anmeldesitzung abgelegt werden. Der Anmelde Informations-Manager ist ein Ort, an dem Anmeldeinformationen im Betriebssystem für bestimmte Domänenressourcen basierend auf dem TargetName der Ressource gespeichert werden können. Bei VPN speichert der VPN-Stapel seine Anmeldeinformationen als Standard für die Sitzung. Für WLAN funktioniert EAP.

Die Anmeldeinformationen werden in Credential Manager als Anmeldeinformationen für "\ * Session" abgelegt. Eine "\ * Session"-Anmeldeinformation impliziert, dass Sie für die aktuelle Benutzersitzung gültig ist. Die Anmeldeinformationen werden auch bereinigt, wenn die WLAN- oder VPN-Verbindung getrennt wird.

Wenn der Benutzer versucht, auf eine Domänenressource zuzugreifen, beispielsweise mit Edge, verfügt Edge über die richtige Unternehmens Authentifizierungsfunktion, damit [WinInet](#) die Anmeldeinformationen freigeben kann, die er vom Anmelde Informations Manager für den SSP erhält, der ihn anfordert. Weitere Informationen zur Enterprise-Authentifizierungsfunktion finden Sie unter [Deklarationen der App-Funktionen](#).

Die lokale Sicherheitsautorität sieht sich die Geräteanwendung an, beispielsweise eine Anwendung für die universelle Windows-Plattform (UWP), um festzustellen, ob Sie die richtige Funktion besitzt. Wenn die APP nicht UWP ist, ist es unerheblich. Wenn es sich um eine UWP-App handelt, wird die Gerätefunktion für die Unternehmensauthentifizierung untersucht. Wenn Sie über diese Funktion verfügt und die Ressource, auf die Sie zugreifen möchten, in der Intranetzone in den Internet Optionen (ZoneMap) vorhanden ist, werden die Anmeldeinformationen freigegeben. Dieses Verhalten verhindert, dass Anmeldeinformationen von nicht vertrauenswürdigen Drittanbietern missbraucht werden können.

Intranetzone

Für die Intranetzone können standardmäßig nur Namen mit einzelnen Bezeichnungen wie [Http://finance](#). Wenn für die Ressource, auf die zugegriffen werden muss, mehrere Domänen Beschriftungen verfügbar sind, besteht die Problemumgehung darin, den [Registrierungs-CSP](#) zu verwenden.

Festlegen des ZoneMap

Die ZoneMap wird mithilfe einer Registrierung gesteuert, die über MDM festgesetzt werden kann. Standardmäßig [http://finance](#) sind Namen mit einzelnen Bezeichnungen wie etwa bereits in der Intranetzone vorhanden. Bei Namen mit mehreren Bezeichnungen, beispielsweise [http://finance.net](#), muss die ZoneMap aktualisiert werden.

MDM-Richtlinie

Oma-URI-Beispiel:

./Vendor/MSFT/Registry/HKU/S-1-5-21-2702878673-795188819-444038987-2781/Software/Microsoft/Windows/CurrentVersion/Internet%20Settings/ZoneMap/Domains/<domain name>/*
als ganzzahliger Wert von 1 für jede Domäne, von der aus Sie SSO durchsetzen möchten auf Ihrem Gerät.
Dadurch werden die angegebenen Domänen der Intranetzone des Edge-Browsers hinzugefügt.

Anmelde Informationsanforderungen

Bei VPN werden die folgenden Typen von Anmeldeinformationen nach der Authentifizierung dem Anmelde Informationsmanager hinzugefügt:

- Benutzername und Kennwort
- Zertifikatbasierte Authentifizierung:
 - TPM-KSP-Zertifikat
 - Software KSP-Zertifikate
 - Smartcard-Zertifikat
 - Windows Hello for Business-Zertifikat

Der Benutzername sollte auch eine Domäne enthalten, die über die Verbindung erreicht werden kann (VPN oder WLAN).

Benutzerzertifikat Vorlagen

Wenn die Anmeldeinformationen Zertifikat basiert sind, müssen die Elemente in der folgenden Tabelle für die Zertifikatvorlagen konfiguriert werden, um sicherzustellen, dass Sie auch für die Kerberos-Clientauthentifizierung verwendet werden können.

TEMPLATE-ELEMENT	KONFIGURATION
SubjectName	<p>Der Distinguished Name (DN) des Benutzers, in dem die Domänen Komponenten des Distinguished Name den internen DNS-Namespace widerspiegeln, wenn der SubjectAlternativeName nicht über den vollqualifizierten UPN verfügt, der zum Auffinden des Domänencontrollers erforderlich ist.</p> <p>Diese Anforderung ist besonders in Umgebungen mit mehreren Gesamtstrukturen relevant, da dadurch sichergestellt wird, dass ein Domänencontroller gefunden werden kann.</p>
SubjectAlternativeName	<p>Der vollqualifizierte UPN des Benutzers, bei dem eine domänennamenkomponente des UPN des Benutzers dem DNS-Namespace der organisationsinternen Domäne entspricht.</p> <p>Diese Anforderung ist besonders in Umgebungen mit mehreren Gesamtstrukturen relevant, da sichergestellt wird, dass ein Domänencontroller gefunden werden kann, wenn der Betreffname nicht über den DN verfügt, der zum Auffinden des Domänencontrollers erforderlich ist.</p>
Schlüsselspeicheranbieter (KSP)	<p>Wenn das Gerät mit Azure AD verbunden ist, wird ein diskretes SSO-Zertifikat verwendet.</p>

TEMPLATE-ELEMENT	KONFIGURATION
EnhancedKeyUsage	<p>Mindestens eine der folgenden EKUs ist erforderlich:</p> <ul style="list-style-type: none"> - Client Authentifizierung (für das VPN) - EAP-Filter-OID (für Windows Hello for Business) - SmartCardLogon (für Azure AD-verbundene Geräte) <p>Wenn für die Domänencontroller eine Smart Card-EKU erforderlich ist:</p> <ul style="list-style-type: none"> - SmartCardLogon - ID-PKINIT-KPClientAuth (1.3.6.1.5.2.3.4) <p>Andernfalls:</p> <ul style="list-style-type: none"> - TLS/SSL-Client Authentifizierung (1.3.6.1.5.5.7.3.2)

NDES-Serverkonfiguration

Der NDES-Server muss so konfiguriert werden, dass eingehende SCEP-Anforderungen der richtigen zu verwendenden Vorlage zugeordnet werden können. Weitere Informationen finden Sie unter [Konfigurieren der Zertifikatinfrastruktur für SCEP](#).

Active Directory-Anforderungen

Sie benötigen eine IP-Konnektivität zu einem DNS-Server und Domänencontroller über die Netzwerkschnittstelle, damit die Authentifizierung auch erfolgreich ausgeführt werden kann.

Die Domänencontroller müssen über geeignete KDC-Zertifikate verfügen, damit der Client Ihnen als Domänencontroller vertraut, und da Telefone nicht mit der Domäne verbunden sind, muss sich die Stammzertifizierungsstelle des KDC-Zertifikats in der Stammzertifizierungsstelle des Drittanbieters oder im vertrauenswürdigen Roots-Speicher der Smartcard befinden.

Die Domänencontroller müssen Zertifikate verwenden, die auf der aktualisierten KDC-Zertifikatvorlage Kerberos-Authentifizierung basieren. Dies liegt daran, dass für Windows 10 Mobile die strenge KDC-Validierung aktiviert werden muss. Dies setzt voraus, dass alle authentifizierenden Domänencontroller Windows Server 2016 ausführen, oder Sie müssen die strenge KDC-Validierung auf Domänencontrollern aktivieren, auf denen frühere Versionen von Windows Server ausgeführt werden. Weitere Informationen finden Sie unter [Aktivieren der strikten KDC-Validierung in Windows Kerberos](#).