

Vista Neuerungen

Christian Zahler

Live-Symbole

Über die neue Live-Symbol-Funktion können Sie Dateien schneller finden und ihren Inhalt erkennen, ohne sie öffnen zu müssen.

Die Hauptelemente der Explorer unter Windows Vista sind so gestaltet, dass Sie die benötigten Informationen zum gewünschten Zeitpunkt finden. Die Schnellsuche steht stets bereit, damit Sie Dateien unmittelbar finden können. Der Navigationsbereich enthält die neue Windows Vista-Suchordnerfunktion sowie herkömmliche Ordner, die Sie auf dem Computer erstellt haben. Auf Befehlsleisten werden nur die Aufgaben angezeigt, die für die angezeigten Dateien am geeignetsten sind. Mit Hilfe der neuen Live-Symbole (skalierbare Miniaturansichten) in Windows Vista können Sie die erste Seite von Dokumenten, den Inhalt eines Fotos oder das "Cover" einzelner Songs in Ihrer Musiksammlung anzeigen, sodass Sie das gesuchte Element einfacher finden können.



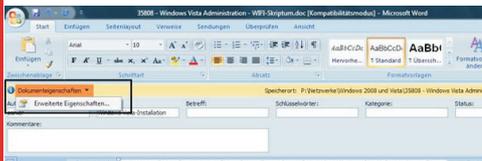
windows_vista_bri...

Voraussetzung für die Verfügbarkeit der Live-Symbole ist, dass beim Abspeichern einer Datei ein Abbild der ersten Seite erstellt wird. Dieses Abbild wird in der versteckten

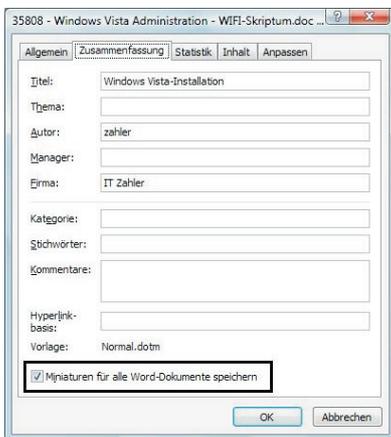
Datei `Thumbnail1s.db` hinterlegt. Dies kann bei Office 2007 folgendermaßen erreicht werden: Klicken Sie auf die Office-Schaltfläche und wählen **[Vorbereiten] – [Eigenschaften]**:



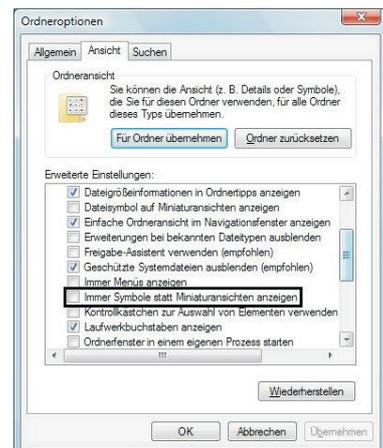
In der nun eingblendeten Eigenschaftsleiste wählen Sie aus dem Menü **[Dokumenteigenschaften] – [Erweiterte Eigenschaften]**:



Im nun eingblendeten Dialogfeld wählen Sie die Karteikarte **„Zusammenfassung“** und überprüfen, ob am unteren Rand dieser Karteikarte der Eintrag **„Miniaturen für alle Word-Dokumente speichern“** aktiviert ist.



Die Miniaturansichten werden allerdings nur angezeigt, wenn der Ordneroptions-Eintrag **„Immer Symbole statt Miniaturansichten anzeigen“** deaktiviert ist.



Linkfavoriten im Explorer definieren

Navigieren Sie in der Ordnerstruktur zu einem gewünschten Ordner. Ziehen Sie dann das Ordnersymbol in der Adresszeile in den Linkfavoriten-Bereich, so wird der Ordner zu den Linkfavoriten hinzugefügt. Damit lässt sich der Zugriff auf Ordner mit langen Pfadangaben, die häufig benötigt werden, massiv beschleunigen.

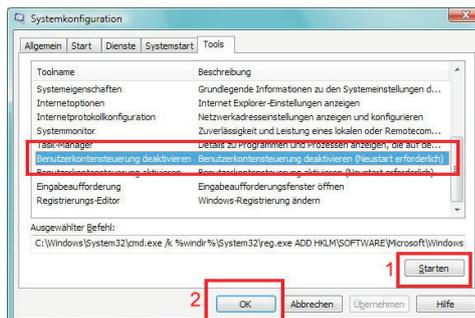


Abschalten der User Account Control

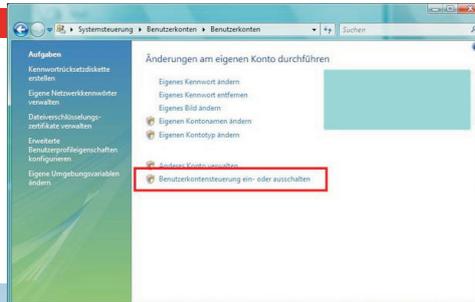
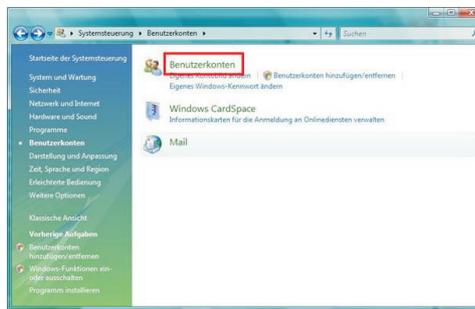
Es wird darauf hingewiesen, dass das Abschalten der UAC ausdrücklich nicht empfohlen wird!

Die UAC kann auf zwei Arten abgeschaltet werden:

Methode 1: Mittels **Ausführen (Start -> Ausführen -> msconfig (alternativ Windows-Taste (R) -> msconfig))** dem Ablauf **Tools -> Benutzerkontensteuerung deaktivieren -> Starten** folgen



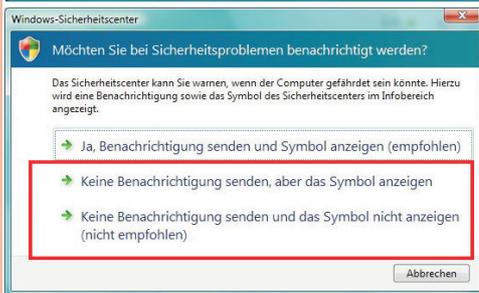
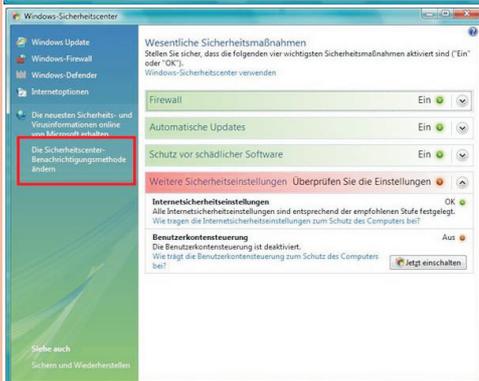
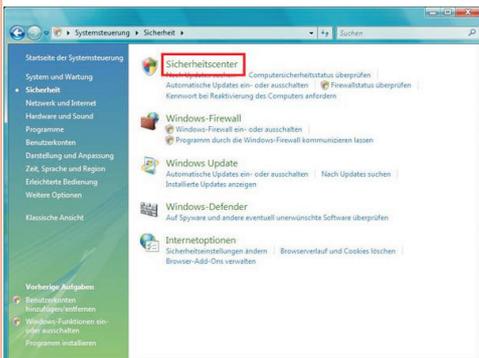
Methode 2: Wählen Sie den Systemsteuerungs-Menüpunkt **„Benutzerkonten“ (Systemsteuerung – Benutzerkonten – Benutzerkonten – Benutzerkontensteuerung ein- oder ausschalten)** und deaktivieren Sie die Einstellung **Benutzerkontensteuerung verwenden**, um zum Schutz des Computers beizutragen. Anschließend mit **OK** bestätigen.



Sicherheitswarnung abschalten

Jedoch hat dies einen kleinen Nachteil: Es erscheint fortwährend eine Sicherheitswarnung, dass die Benutzerkontensteuerung deaktiviert sei. Möchte man nicht oder nicht direkt darauf hingewiesen werden, so kann man diese (und andere Meldungen des Sicherheitscenters) deaktivieren. Hierzu ist folgendes zu tun:

Im Sicherheitscenter (Systemsteuerung – Sicherheit – Sicherheitscenter) im Linken Bereich auf Die Sicherheitscenter-Benachrichtigungsmethode ändern klicken. Im darauf folgenden Fenster wahlweise auf Keine Benachrichtigung senden, aber das Symbol anzeigen oder auf Keine Benachrichtigung senden und das Symbol nicht anzeigen (nicht empfohlen) auswählen (Ablauf siehe folgende Bilder)



Abschalten der UAC nur für die Administrator-Gruppe (Registry-Einstellung):

Ein weiterer Weg, die Benutzerkontensteuerung zu beeinflussen, ist, diese nur für die Benutzer der Gruppe *Administratoren* zu deaktivieren.

Hierfür muss man sich dem Registry-Editor zu Hilfe nehmen (*Start -> Ausführen -> registry(regedit)*)

Hier gibt es im Pfad

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System` einen Eintrag `ConsentPromptBehaviorAdmin` vom Typ `REG_DWORD`. Dieser muss ggf. noch angelegt werden. Dieser kann folgende Werte annehmen:

- 0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - alle Programme werden mit höheren Rechten ausgeführt
- 1 Bestätigung für höhere Rechte erforderlich. Weiterhin muss das Kennwort des Benutzers eingegeben werden.
- 2 Einfache Zustimmung über die Anforderung von höheren Rechten. Ein Kennwort ist nicht erforderlich (**Standard-Einstellung**)

Achtung: Aus Sicherheitsgründen sollte auch für die Administrator-Gruppe davon abgesehen werden, die Benutzerkontensteuerung auszuschalten.

Abschalten der UAC nur für die Standard-Benutzer-Gruppe (Registry-Einstellung)

Wenn die Benutzerkontensteuerung nur für Standard-Benutzer eingestellt werden, benötigt man den Registry-Editor.

Hier gibt es einen Eintrag `ConsentPromptBehaviorUser` (ggf. muss dieser noch angelegt werden) im Pfad

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System` Dieser ist vom Typ `REG_DWORD` und kann die folgenden Werte annehmen:

- 0 Keine Aufforderungen mehr seitens der Benutzerkontensteuerung - sollte jedoch ein Programm erhöhte Rechte benötigen, so werden diese **verweigert** und das Programm könnte eventuell nicht mehr oder nicht richtig ausgeführt werden.
- 1 Bestätigung für höhere Rechte erforderlich. Weiterhin muss das Konto eines Administrators mit dessen Kennwort eingegeben werden (**Standard-Einstellung**).

Achtung: Aus Sicherheitsgründen sollte davon abgesehen werden, die Benutzerkontensteuerung zu beeinflussen.

Security Principals

Unter diesem Begriff werden Objekte zusammengefasst, denen Berechtigungen zugewiesen werden können.

Zu den wichtigsten *Security Principals* zählen:

- Benutzerkonten
- Computerkonten
- Gruppenkonten

Benutzer-, Computer- und Gruppenkonten werden nicht über ihren Namen, sondern über einen internen Primärschlüssel, den sogenannten *Security Identifier (SID)*, verwaltet. Alle Berechtigungen für Benutzer-, Computer- und Gruppenkonten werden intern mit dieser SID gespeichert.

Aufbau einer SID



• **Domänen-SID:** Im Fall von lokalen Benutzerkonten spezifiziert diese Nummer den PC, bei Domänen-Benutzerkonten die Domäne. Alle lokalen Benutzerkonten auf demselben PC haben dieselbe Domänen-SID; alle AD-Benutzer derselben Domäne haben ebenfalls dieselbe Domänen-SID.

• **RID (Relative ID):** Diese oft vierstellige Nummer ist spezifisch für jedes Benutzer-, Computer- oder Gruppenkonto. Dabei hat das vordefinierte Administrator-Konto immer die

RID 500. So hätte das Administrator-Konto des obigen PCs folgende SID:

`S-1-5-21-1812011286-570857186-3424489074-500`
 SIDs können beispielsweise mit dem Tool `PsGetSID` angezeigt werden (Download unter <http://www.microsoft.com/technet/sysinternals/utilities/psgetsid.mspx>).

Well-Known SIDs

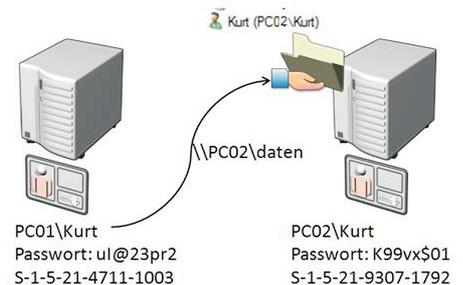
Einige *Security Principals* haben SIDs, die nicht wie oben beschrieben aufgebaut sind. Es handelt sich dabei um **Spezialidentitäten**, die vom System her vorgesehen sind und sich in vielen Fällen ähnlich wie Gruppenkonten verhalten. Die wichtigste Gemeinsamkeit dieser speziellen Objekte ist die immer gleiche SID – egal auf welchem PC oder in welcher Domäne. Die Mitgliedschaft wird vom Betriebssystem gesteuert und kann nicht geändert werden.

Beispiele (siehe nächste Seite):

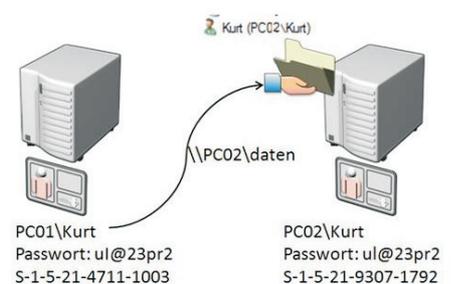
Fernanmeldung, automatische Fernanmeldung

Beispiel: Wir nehmen an, dass auf einem Rechner mit dem Namen `PC02` ein freigegebener Ordner mit dem Freigabennamen `daten` existiert. Auf beiden Rechnern wurde ein lokaler Benutzer mit dem Anmeldenamen `Kurt` erzeugt. Die beiden Benutzer haben unterschiedliche Kennwörter und natürlich auch unterschiedliche SIDs.

Die Sicherheitsberechtigungen für den Ordner `daten` wurden so eingerichtet, dass nur der Benutzer `Kurt` Zugriffsrechte (zum Beispiel „Ändern“) auf diesen Ordner hat.



Wir nehmen nun an, dass sich `PC01\Kurt` mit dem UNC-Pfad `\\PC02\daten` zum freigegebenen Ordner verbinden will. Die LSA (*Local Security Authority*) auf `PC02` überprüft Benutzernamen, Kennwort und SID. Nur eine von diesen drei Eigenschaften stimmt überein (der Benutzernamen), daher wird `PC01\Kurt` nicht ohne weiteres der Zugriff auf den Ordner gewährt; es erscheint ein **Dialogfeld für die Fernanmeldung**:



Modifizieren wir nun das Beispiel so, dass die Kennwörter der beiden Benutzerkonten übereinstimmen. Wieder überprüft die LSA auf `PC02` Benutzernamen, Kennwort und SID – zwei dieser drei Eigenschaften stimmen überein (Benutzernamen und Kennwort). Nun erscheint kein Dialogfeld; es erfolgt eine automatische Fernanmeldung. Die Zugriffsberechtigungen für `PC01\Kurt` sind so, als hätte er sich als `PC02\Kurt` angemeldet.

Beispiele für SIDs

SID	Name	Beschreibung
S-1-1-0	<i>Everyone (Jeder)</i>	Gruppe, die alle Benutzer einschließlich der anonymen Benutzer und Gäste enthält. Die Mitgliedschaft wird vom Betriebssystem gesteuert. Hinweis: Seit Windows XP Service Pack 2 (SP2) sind anonyme Benutzer standardmäßig nicht mehr Mitglied der Gruppe "Everyone".
S-1-3-0	<i>Ersteller-Besitzer</i>	Platzhalter in einem vererbaren ACE-Eintrag. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Objekterstellers.
S-1-5-1	<i>Dialup (DFÜ)</i>	Gruppe, die alle Benutzer enthält, die sich über eine DFÜ-Verbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-2	<i>Netzwerk</i>	Gruppe, die alle Benutzer enthält, die sich über eine Netzwerkverbindung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-3	<i>Batch (Batch)</i>	Gruppe, die alle Benutzer enthält, die sich über eine Batch-Warteschlangeneinrichtung angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-4	<i>Interactive (Interaktiv)</i>	Gruppe, die alle Benutzer enthält, die sich interaktiv angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-6	<i>Service (Dienst)</i>	Gruppe, die alle Sicherheitsprinzipale enthält, die sich als Dienst angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-7	<i>Anonymous (Anonym)</i>	Gruppe, die alle Benutzer enthält, die sich anonym angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-9	<i>Enterprise Domain Controllers (Domänencontroller der Organisation)</i>	Gruppe, die alle Domänencontroller in einer Gesamtstruktur enthält, die einen Verzeichnisdienst des Active Directory verwenden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-10	<i>Principal Self (Selbstprinzipal)</i>	Platzhalter in einem vererbaren ACE-Eintrag für ein Konto- oder Gruppenobjekt im Active Directory. Wenn der ACE-Eintrag geerbt wird, ersetzt das System diesen SID durch den SID des Sicherheitsprinzipals, dem das Konto gehört.
S-1-5-11	<i>Authenticated Users (Authentifizierte Benutzer)</i>	Gruppe, die alle Benutzer enthält, deren Identitäten bei der Anmeldung authentifiziert wurden. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-13	<i>Terminal Server Users (Terminalserverbenutzer)</i>	Gruppe, die alle Benutzer enthält, die sich bei einem Terminaldiensteserver angemeldet haben. Die Mitgliedschaft wird vom Betriebssystem gesteuert.
S-1-5-18	<i>Lokales System</i>	Dienstkonto, das vom Betriebssystem genutzt wird.
S-1-5-19	<i>NT Authority (NT-Autorität)</i>	Lokaler Dienst
S-1-5-20	<i>NT-Autorität</i>	Netzwerkdienst
S-1-5-32-544	<i>Administratoren</i>	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist das Administratorkonto einziges Mitglied der Gruppe. Wenn ein Computer einer Domäne beitrifft, wird die Gruppe "Domänen-Admins" der Administratorengruppe hinzugefügt. Wenn ein Server zum Domänencontroller wird, wird die Gruppe "Organisations-Admins" ebenfalls zur Administratorengruppe hinzugefügt.
S-1-5-32-545	<i>Benutzer</i>	Vordefinierte Gruppe. Nach der Erstinstallation des Betriebssystems ist die Gruppe der authentifizierten Benutzer einziges Mitglied dieser Gruppe. Wenn ein Computer einer Domäne beitrifft, wird die Gruppe der Domänenbenutzer zur Benutzergruppe auf dem Computer hinzugefügt.
S-1-5-32-546	<i>Gäste</i>	Vordefinierte Gruppe. Standardmäßig ist das Gastkonto einziges Mitglied dieser Gruppe. Die Gästegruppe ermöglicht es Gelegenheitsbenutzern oder einmaligen Benutzern, sich mit eingeschränkten Berechtigungen über das vordefinierte Gastkonto auf einem Computer anzumelden.
S-1-5-32-547	<i>Hauptbenutzer</i>	Vordefinierte Gruppe. Standardmäßig hat diese Gruppe keine Mitglieder. Hauptbenutzer können lokale Benutzer und Gruppen erstellen, von ihnen selbst erstellte Konten ändern und löschen und Benutzer aus den Hauptbenutzer-, Benutzer- und Gästegruppen löschen. Hauptbesucher können außerdem Programme installieren, lokale Drucker erstellen, verwalten und löschen sowie Dateifreigaben erstellen und löschen.