

Einschränken von Windows Server 2003-Terminalserversitzungen

(Engl. Originaltitel: [Locking Down Windows Server 2003 Terminal Server Sessions](#))

Veröffentlicht: Juli 2003

Zusammenfassung

Administratoren, die Microsoft® Windows Server™ 2003-Terminalserversitzungen auf bestimmte Funktionen beschränken möchten, bietet Active Directory® hierfür verschiedene Möglichkeiten an. Der vorliegende Artikel beschreibt diese und erläutert, worauf Sie – abhängig davon, wie Sie Terminalserver einsetzen – achten sollten, wenn Sie die Benutzerinteraktionen mit dem Betriebssystem konfigurieren. Eine besondere Rolle spielt in diesem Zusammenhang die Verwendung von Gruppenrichtlinien.

Einführung

Mit Hilfe von Terminalserver in Windows Server 2003 können auf nahezu jedem beliebigen Client-System 32-Bit-Anwendungen wie Microsoft Word und Microsoft Excel ausgeführt werden – an jedem Ort und zu jeder Zeit. Terminalserver stellt die Plattform zur Verfügung, um diese Anwendungen zentral zu verarbeiten, zu verwalten und zu warten. Mit seiner hohen Flexibilität kann Terminalserver für eine Vielzahl von Anwendungen und in einer Vielzahl von Umgebungen verwendet werden.

Ein Terminal kann sich in einem Büro, in einem Kiosk, in einem Schulungsraum, in einem Labor, in einer Fertigungsstätte oder, verbunden über das Internet, in einem anderen Land befinden, während der Server selbst in einem sicheren zentralen Serverraum steht. Zu den möglichen Nutzern von Terminalserver zählen beispielsweise Anbieter von Anwendungsdiensten, die über das Internet Kunden den Zugriff auf Applikationen ermöglichen. Allerdings ist es im Rahmen derartiger Implementierungen unter Umständen erforderlich, die Benutzeraktivitäten auf vordefinierte Anwendungen oder Funktionen des Windows-Betriebssystems zu beschränken. Das Active Directory von Windows Server 2003 bietet hierfür verschiedene Möglichkeiten an.

Wie kann dies umgesetzt werden?

Dieses Whitepaper richtet sich an Administratoren, die bereits mit Terminalserver und Active Directory vertraut sind. Es wird erläutert, wie Benutzersitzungen in Terminalserver mit den Features von Active Directory auf die Anwendungen und Desktopfunktionen beschränkt werden können, die der Administrator als notwendig erachtet. In diesem Dokument werden bestimmte Gruppenrichtlinien besonders hervorgehoben und deren Vorteile kurz erläutert. Nicht alle Einstellungen sind erforderlich, da sie eine stark eingeschränkte Benutzeroberfläche schaffen können. Verwenden Sie dieses Dokument als Leitfaden, um Terminalserver für die jeweilige Umgebung zu konfigurieren. Ausführliche Erklärungen zu den einzelnen erwähnten Richtlinien finden Sie auf der Registerkarte **Erklärung** im Gruppenrichtlinienobjekt-Editor.

Falls Active Directory nicht verfügbar ist, können Administratoren NTFS-Berechtigungen oder die lokale Richtlinie verwenden, um den Zugriff auf Anwendungen zu beschränken. Obwohl viele Richtlinien mit Hilfe der lokalen Richtlinie auch ohne Active Directory angewendet werden können, wird diese Methode nicht empfohlen. Wenn diese Richtlinien in der lokalen Richtlinie aktiviert werden, werden alle Konten im Terminalserver, einschließlich des Administratorkontos, eingeschränkt. Die Verwendung der lokalen Richtlinie kann umständlich sein, und liegt daher außerhalb des Themenbereichs dieses Dokuments. Zum Einschränken der Funktionen in Terminalserverversionen unter Windows Server 2003 wird die Verwendung von Active Directory empfohlen.

Anmerkung: Dieser Artikel enthält keine Maßnahmen zum Schutz vor Hackern, kreativen Benutzer, Anwendungen oder Treibern, die die in diesem Dokument beschriebenen Beschränkungen umgehen. Weitere Informationen zum Sichern der Terminaldienste unter Microsoft® Windows® 2000 finden Sie im Dokument *Securing Windows 2000 Terminal Services* (englischsprachig) unter <http://go.microsoft.com/fwlink/?LinkId=18404>.

Planung

Bei den in diesem Artikel beschriebenen Richtlinien handelt es sich um grundlegende Beschränkungen für die Benutzeroberfläche des Betriebssystems. Nicht alle Richtlinien sind erforderlich. Einige sind möglicherweise in bestimmten Umgebungen ungeeignet. Überprüfen Sie die Implementierung vor einer Bereitstellung. Darüber hinaus sollten Sie nicht nur die für die Umgebung geeigneten Beschränkungen ermitteln, sondern auch festlegen, wie diese Richtlinien implementiert werden.

Die in diesem Artikel behandelten Richtlinien können die Funktionalität für alle Benutzer, sogar für das Administratorkonto, erheblich einschränken. Es wird daher empfohlen, eine neue Organisationseinheit und ein neues Gruppenrichtlinienobjekt zu erstellen.

Wenn systemweite Beschränkungen auf den Terminalserver angewendet werden müssen, verschieben Sie das Terminalserver-Computerobjekt in die eingeschränkte Organisationseinheit. Dadurch werden computerbasierte Beschränkungen im Terminalserver erzwungen. Administratoren haben die Möglichkeit, für alle Benutzer einschließlich der Administratoren, die sich am Terminalserver anmelden, benutzerbasierte Beschränkungen anzuwenden. Diese Beschränkungen können zusätzlich zu oder anstelle von Richtlinien verwendet werden, die normalerweise für den Benutzer beim Anmelden an der Domäne gelten. Weitere Informationen finden Sie unter dem Thema *Loopbackrichtlinie*.

Wenn für einzelne Benutzer Beschränkungen angewendet werden müssen, verschieben Sie das Benutzerkontoobjekt in die eingeschränkte Organisationseinheit. In diesem Fall werden jedoch die benutzerbasierten Beschränkungen unabhängig von dem Computer, an dem sich der Benutzer an der Domäne anmeldet, erzwungen.

Nachstehend finden Sie zwei Empfehlungen für die Implementierung von Gruppenrichtlinien:

1. **Die Benutzerkonten werden in die eingeschränkte Organisationseinheit verschoben.** Erstellen Sie Benutzerkonten, die nur für Terminalserver gelten, und verschieben Sie diese in die eingeschränkte Organisationseinheit. Lassen Sie mit dem MMC-Snap-In für die Terminalserverkonfiguration Anmeldungen dieser Benutzer nur am Terminalserver zu. Weisen Sie die Benutzer an, für den Terminalserver nur diese Konten zu verwenden. Wenn Computerbeschränkungen erforderlich sein sollten, deaktivieren Sie die Loopbackverarbeitung und verschieben Sie das Terminalserver-Computerobjekt in die Organisationseinheit. Neben den beschränkenden Computerrichtlinien können für Benutzer unterschiedliche Beschränkungsebenen auf dem gleichen Terminalserver gelten. Diese Implementierung ermöglicht es Administratoren, einige Vorgänge auf dem Terminalserver durchzuführen, während Benutzer aktiv sind.

2. Nur das Terminalserver-Computerobjekt wird in die eingeschränkte Organisationseinheit verschoben.

Verschieben Sie nach dem Installieren und Konfigurieren aller Anwendungen auf dem Terminalserver das Terminalserver-Computerobjekt in die eingeschränkte Organisationseinheit. Aktivieren Sie die Loopbackverarbeitung. Alle Benutzer, die sich am Terminalserver anmelden, werden dann durch benutzerbasierte Richtlinien beschränkt, die durch das eingeschränkte Gruppenrichtlinienobjekt definiert werden, und zwar unabhängig von der Organisationseinheit, in der sich der Benutzer befindet. Das kann dazu führen, dass viele lokale Änderungen nicht auf den Terminalserver angewendet werden können. Der Server kann jedoch weiterhin remote verwaltet werden. Falls Administratoren auf den Terminalserver zugreifen müssen, können alle Benutzer abgemeldet und deren Anmeldung kann beim Terminalserver vorübergehend beschränkt werden. Verschieben Sie dazu das Terminalserver-Computerobjekt aus der eingeschränkten Organisationseinheit, und melden Sie sich an. Nach Abschluss der Wartung verschieben Sie das Terminalserver-Computerobjekt wieder in die eingeschränkte Organisationseinheit und aktivieren die Benutzeranmeldungen erneut. Bei dieser Implementierung müssen die Benutzer nicht über mehrere Benutzerkonten verfügen. Damit können auch Konfigurationsänderungen des Terminalservers in einer Produktionsumgebung verhindert werden.

Weitere Informationen zum Konfigurieren der Sicherheitseinstellungen finden Sie im Dokument *To edit a security setting on a Group Policy object* (englischsprachig) unter <http://go.microsoft.com/fwlink/?linkid=18541>.

Installieren von Terminalserver

Beim Installieren von Terminalserver auf einem Computer unter Windows Server 2003 werden Sie aufgefordert, als Kompatibilitätseinstellung für Berechtigungen **Vollständige Sicherheit** oder **Niedrige Sicherheit** auszuwählen. Diese Einstellung kann später mit dem MMC-Snap-In für die Terminalserverkonfiguration geändert werden.

Es wird empfohlen, die Option **Vollständige Sicherheit** auszuwählen. Dadurch werden die Berechtigungen für Terminalserverbenutzer auf die Gruppe **Benutzer** beschränkt. Bei der Einstellung **Vollständige Sicherheit** kann es jedoch zu Kompatibilitätsproblemen mit einigen älteren Anwendungen kommen. In einem solchen Fall sollten Sie die Einstellung **Niedrige Sicherheit** auswählen. Die Einstellung **Niedrige Sicherheit** ermöglicht den Terminalserverbenutzern nahezu Hauptbenutzerzugriff auf bestimmte Systemordner und Registrierungsschlüssel. Bei Auswahl der Einstellung **Niedrige Sicherheit** sollten Sie Richtlinien aktivieren, die den Zugriff auf Registrierungs-Editoren und Dateibrowser beschränken.

Beschränkende Computerrichtlinien

Diese Richtlinien werden nur auf Computerobjekte angewendet, die sich in der eingeschränkten Organisationseinheit befinden. Die Einstellungen gelten systemweit und betreffen alle Benutzer.

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

- Geräte: Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie erlaubt nur Benutzern, die sich an der Konsole des Terminalservers anmelden, auf das CD-ROM-Laufwerk zuzugreifen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer und Administratoren nicht remote auf Programme oder Daten auf einer CD-ROM zugreifen können.

- Geräte: Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie erlaubt nur Benutzern, die sich an der Konsole des Terminalservers anmelden, auf das Diskettenlaufwerk zuzugreifen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer und Administratoren nicht remote auf Programme oder Daten auf einer Diskette zugreifen können.

- Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen

Diese Richtlinie sorgt dafür, dass das zuletzt angemeldete Benutzerkonto nicht in der Windows-Anmeldeaufforderung der Konsole des Terminalservers angezeigt wird. Diese Richtlinie hat keine Auswirkung auf Terminalserverclients, die den Namen des angemeldeten Benutzers lokal zwischenspeichern.

[Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Systemdienste]

- Hilfe und Support

Empfohlene Einstellung: **Deaktiviert**

Diese Richtlinie deaktiviert den Hilfe- und Supportcenter-Dienst. Mit Hilfe dieser Einstellung wird verhindert, dass Benutzer die neue Hilfe- und Supportcenter-Anwendung von Windows starten. Durch diese Richtlinie werden nicht die alten Hilfedateien (wie z. B. CHM-Dateien) oder die Hilfe in anderen Anwendungen deaktiviert. Falls dieser Dienst deaktiviert wird, kann es zu Problemen bei anderen Programmen und Diensten kommen, die von diesem Dienst abhängen. Es wird empfohlen, diesen Dienst zu deaktivieren, damit die Benutzer keine anderen Anwendungen starten oder Systeminformationen über den Terminalserver anzeigen können.

[Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Terminaldienste]

- Terminaldienstebenutzer auf eine Remotesitzung beschränken

Diese Richtlinie verhindert, dass ein einzelner Benutzer mit einem einzelnen Benutzerkonto mehrere Terminalserver Sitzungen erstellt.

- Element „Trennen“ aus dem Dialog „Herunterfahren“ entfernen

Durch diese Richtlinie wird die Option **Trennen** aus dem Dialogfeld **Windows beenden** entfernt. Sie verhindert nicht, dass Benutzer die Sitzung zum Terminalserver trennen. Verwenden Sie diese Richtlinie, wenn Benutzer nicht ohne weiteres in der Lage sein sollen, ihre Sitzungen zu trennen, und das Dialogfeld **Windows beenden** nicht entfernt wurde.

[Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Terminaldienste\Client/Server-Datenumleitung]

- Laufwerkumleitung nicht zulassen

Empfohlene Einstellung: **Aktiviert**

Standardmäßig verbindet Terminalserver Clientlaufwerke beim Herstellen der Verbindung automatisch. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf Anwendungen auf ihrem lokalen Computer zugreifen können.

[Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Terminaldienste\Sitzungen]

- Zeitlimit für getrennte Sitzungen festlegen

Standardmäßig lässt Terminalserver zu, dass Benutzer eine Sitzung trennen und alle Anwendungen für einen unbegrenzten Zeitraum aktiv lassen. Diese Richtlinie definiert ein Zeitlimit, für dessen Dauer getrennte Terminalserver Sitzungen aktiv bleiben. Verwenden Sie diese Richtlinie, wenn getrennte Sitzungen auf dem Terminalserver nicht für längere Zeit aktiv bleiben sollen.

[Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Installer]

- Windows Installer deaktivieren

Empfohlene Einstellung: **Aktiviert – Immer**

Wenn diese Richtlinie nur für nicht verwaltete Anwendungen festgelegt wird, funktioniert Windows Installer weiterhin für Anwendungen, die veröffentlicht oder durch Gruppenrichtlinien zugewiesen wurden. Wenn diese Richtlinie auf **Immer** festgelegt wird, ist Windows Installer vollständig deaktiviert. Dies kann vorteilhaft sein, wenn einige veröffentlichte oder zugewiesene Anwendungen auf dem Terminalserver unerwünscht sind. Durch das Deaktivieren von Windows Installer wird nicht die Installation von Anwendungen durch andere Setupprogramme oder verfahren verhindert. Es wird empfohlen, Anwendungen zu installieren und zu konfigurieren, bevor diese Richtlinie aktiviert wird. Nachdem die Richtlinie aktiviert wurde, können Administratoren keine Anwendungen installieren, die Windows Installer verwenden.

[Computerkonfiguration\Administrative Vorlagen\System\Gruppenrichtlinie]

- Loopbackverarbeitungsmodus für Benutzergruppenrichtlinie

Wenn das Terminalserver-Computerobjekt in die eingeschränkte Organisationseinheit verschoben wird, das Benutzerkonto aber nicht, werden die beschränkenden Benutzerkonfigurationsrichtlinien durch die Loopbackverarbeitung auf alle Benutzer des Terminalservers angewendet. Wenn diese Richtlinie aktiviert wird, gelten die beschränkenden Benutzerkonfigurationsrichtlinien für alle Benutzer, einschließlich der Administratoren, die sich am Terminalserver anmelden, unabhängig davon, wo sich das Benutzerkonto befindet. Dabei stehen zwei Modi zur Verfügung. Im Zusammenführungsmodus wird zuerst das Gruppenrichtlinienobjekt des Benutzers, dann die einschränkende Richtlinie angewendet. Die einschränkende Richtlinie hat Vorrang vor dem Gruppenrichtlinienobjekt des Benutzers. Im Ersetzungsmodus wird lediglich die einschränkende Richtlinie, und nicht das Gruppenrichtlinienobjekt des Benutzers angewendet. Diese Richtlinie ist für Beschränkungen vorgesehen, die auf Computern anstatt auf dem Benutzerkonto basieren.

Wenn diese Richtlinie deaktiviert ist und das Terminalserver-Computerobjekt in die eingeschränkte Organisationseinheit verschoben wird, werden auf den Terminalserver nur die Computerkonfigurationsrichtlinien angewendet. Damit für einen Benutzer Benutzerkonfigurationsbeschränkungen angewendet werden, müssen die Benutzerkonten in die Organisationseinheit verschoben werden.

Beschränkende Benutzerrichtlinien

Diese Richtlinien werden auf Benutzerkonten angewendet, die sich in der eingeschränkten Organisationseinheit befinden. Wenn die Loopbackverarbeitung verwendet wird, werden diese Beschränkungen auf alle Benutzerkonten angewendet, die sich an Computern in der eingeschränkten Organisationseinheit anmelden.

[Benutzerkonfiguration\Windows-Einstellungen\Ordnerumleitung]

- Anwendungsdaten

Empfohlene Einstellung: Standardumleitung und **Einen Ordner für jeden Benutzer im Stammpfad erstellen**. Aktivieren Sie auf der Registerkarte **Einstellungen** die Option **Dem Benutzer exklusive Zugriffsrechte für erteilen**. Aktivieren Sie **Den Inhalt von an den neuen Ort verschieben**. Setzen Sie die Richtlinienentfernung auf **Ordner nach Entfernen der Richtlinie zurück an den Ort des lokalen Benutzerprofils umleiten** fest.

- Desktop

Empfohlene Einstellung: Standardumleitung und einen Ordner für jeden Benutzer im Stammpfad erstellen. Aktivieren Sie auf der Registerkarte Einstellungen die Option **Dem Benutzer exklusive Zugriffsrechte für erteilen**. Aktivieren Sie **Den Inhalt von Desktop an den neuen Ort verschieben**. Setzen Sie die Richtlinienentfernung auf **Ordner nach Entfernen der Richtlinie zurück an den Ort des lokalen Benutzerprofils umleiten** fest.

- Eigene Dateien

Empfohlene Einstellung: Standardumleitung und **Einen Ordner für jeden Benutzer im Stammpfad erstellen**. Aktivieren Sie auf der Registerkarte **Einstellungen** die Option **Dem Benutzer exklusive Zugriffsrechte für erteilen**. Aktivieren Sie **Den Inhalt von an den neuen Ort verschieben**. Setzen Sie die Richtlinienentfernung auf **Ordner nach Entfernen der Richtlinie zurück an den Ort des lokalen Benutzerprofils umleiten** fest.

- Startmenü

Empfohlene Einstellung: **Standardumleitung** und **An folgenden Pfad umleiten**.

Setzen Sie die Richtlinienentfernung auf der Registerkarte Einstellungen auf **Ordner nach Entfernen der Richtlinie zurück an den Ort des lokalen Benutzerprofils umleiten** fest. Erstellen Sie in diesem freigegebenen Ordner einen Ordner \Programme\Autostart. Durch Aktivieren dieser Richtlinien steht ein zentraler Punkt zum Sichern von Benutzerdaten zur Verfügung. Wenn die Richtlinie zum Beschränken des Zugriffs auf lokale Laufwerke (siehe unten) aktiviert wird, benötigen die Benutzer außerdem die Ordnerumleitung, damit keine Meldungen angezeigt werden, die auf den eingeschränkten Zugriff hinweisen. Wenn kein Server für servergespeicherte Profile zur Verfügung steht, können lokale Freigaben verwendet werden. Erstellen Sie einen Hauptordner für alle Benutzerdaten (wie z. B. **C:\Benutzerdaten**). Erstellen Sie vier Unterordner, jeweils einen für die einzelnen Ordnerarten (wie z. B. **Anwendungsdaten**, **Desktop**, **Eigene Dateien** und **Start**). Geben Sie die Unterordner frei, und legen Sie die Freigabeberechtigungen für die Gruppe **Jeder** auf **Ändern** fest. Setzen Sie die einzelnen Pfade auf die entsprechenden Freigaben fest. Das Startmenü kann anders konfiguriert werden. Es kann von allen Benutzern gemeinsam genutzt werden. Fügen Sie dort die Verknüpfungen zu den Anwendungen ein. Ändern Sie die Freigabeberechtigungen für die Gruppe **Jeder** in **Lesen**. Sie müssen den Ordner **Programme\Autostart** manuell im freigegebenen Ordner **Start** erstellen (**C:\Benutzerdaten\Start\Programme\Autostart**).

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer]

- Suchen: Suche nach Dateien über F3-Taste im Browser deaktivieren

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie deaktiviert die Verwendung der F3-Taste für Suchvorgänge in Microsoft® Internet Explorer und im Windows-Explorer. Die Benutzer können dann nicht durch Drücken von F3 das Internet (in Internet Explorer) bzw. die Festplatte (im Windows-Explorer) durchsuchen. Wenn der Benutzer F3 drückt, wird eine Meldung angezeigt, die ihn darüber informiert, dass dieses Feature deaktiviert wurde. Diese Richtlinie verhindert, dass ein Benutzer ohne weiteres nach Anwendungen auf der Festplatte suchen kann. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht nach Anwendungen auf dem Festplattenlaufwerk suchen bzw. das Internet durchsuchen können.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer\Browser-Menüs]

- Kontextmenü deaktivieren

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie deaktiviert die Anzeige des Kontextmenü, wenn Benutzer während der Verwendung des Browsers mit der rechten Maustaste klicken. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht das Kontextmenü als alternative Methode verwenden können, um Befehle auszuführen.

- Menü „Favoriten“ ausblenden

Diese Richtlinie verhindert, dass Benutzer Einträge in der Liste der Favoritenlinks hinzufügen, entfernen oder bearbeiten können. Wenn Sie diese Richtlinie aktivieren, wird das Menü **Favoriten** von der Benutzeroberfläche entfernt und die Schaltfläche **Favoriten** wird auf der Browsersymbolleiste abgeblendet dargestellt. Verwenden Sie diese Richtlinie, wenn das Menü **Favoriten** aus Windows-Explorer entfernt werden soll und die Benutzer nicht ohne weiteres auf Internet Explorer zugreifen können sollen.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Anwendungskompatibilität]

- Zugriff auf 16-Bit-Anwendungen verhindern

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass das MS-DOS-Subsystem (**ntvdm.exe**) für den Benutzer ausgeführt werden kann. Diese Einstellung wirkt sich auf das Starten aller 16-Bit-Anwendungen im Betriebssystem aus. Standardmäßig wird das MS-DOS-Subsystem für alle Benutzer ausgeführt. Viele MS-DOS-Anwendungen sind nicht für Terminalserver geeignet und können aufgrund der ständigen Abfrage der Tastatur zu einer hohen CPU-Auslastung führen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht den 16-Bit-Befehlsinterpreter, **Command.com**, ausführen können.

Anmerkung: Die Richtlinie **Zugriff auf 16-Bit-Anwendungen verhindern** kann in der Computerkonfiguration (systemweit) und in der Benutzerkonfiguration (benutzerspezifisch) konfiguriert werden.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows-Explorer]

- Menüeintrag „Ordneroptionen“ aus dem Menü „Extras“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt den Menüeintrag **Ordneroptionen** aus allen Windows-Explorer-Menüs sowie den Eintrag **Ordneroptionen** aus der Systemsteuerung. Die Benutzer können somit nicht das Dialogfeld **Ordneroptionen** verwenden. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer viele Eigenschaften vom Windows-Explorer nicht ändern können, wie z. B. Active Desktop, Webansicht, Offlinedateien, verborgene Systemdateien und Dateitypen.

- Menü „Datei“ aus Windows-Explorer entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt das Menü **Datei** aus **Arbeitsplatz** und Windows-Explorer. Durch diese Einstellung wird nicht verhindert, dass Benutzer andere Verfahren verwenden, um Aufgaben durchzuführen, die im Menü **Datei** verfügbar sind. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf Aufgaben wie **Neu** und **Öffnen** sowie Shellerweiterungen einiger Anwendungen zugreifen können. Durch das Aktivieren

dieser Richtlinie wird auch das Erstellen von Verknüpfungen zu ausführbaren Dateien erschwert.

- Optionen „Netzlaufwerk verbinden“ und „Netzlaufwerk trennen“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass Benutzer mit Windows-Explorer Verbindungen zu Freigaben herstellen oder trennen. Durch diese Einstellung wird nicht das Verbinden und Trennen von Laufwerken in anderen Anwendungen oder über den Befehl **Ausführen** verhindert. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer im Windows-Explorer die Domäne nicht ohne weiteres durchsuchen können. Wenn Netzlaufwerke erforderlich sind, können sie in einem Anmeldeskript verbunden werden.

- Schaltfläche „Suchen“ aus Windows-Explorer entfernen

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer im Windows-Explorer nicht nach Anwendungen suchen können. Diese Richtlinie verhindert keine Suchroutinen in anderen Anwendungen bzw. im Startmenü.

- Registerkarte „Sicherheit“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Registerkarte **Sicherheit** aus Windows-Explorer. Wenn Benutzer das Dialogfeld **Eigenschaften** für Dateisystemobjekte öffnen können, wie z. B. Ordner, Dateien, Verknüpfungen und Laufwerke, können sie nicht auf die Registerkarte **Sicherheit** zugreifen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht die Sicherheitseinstellungen ändern oder eine Liste aller Benutzer mit Zugriffsrechten für das Objekt anzeigen können.

- Standardkontextmenü aus Windows-Explorer entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Einstellung entfernt das Kontextmenü aus Windows-Explorer. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf Anwendungen zugreifen können, die Einträge in das Kontextmenü einfügen. Diese Richtlinie verhindert nicht den Zugriff auf Anwendungen im Kontextmenü mit anderen Methoden, wie z. B. durch Abkürzungstasten.

- Den Menüeintrag „Verwalten“ im Windows-Explorer-Kontextmenü ausblenden

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Option **Verwalten** aus Windows-Explorer und **Arbeitsplatz**. Die Option **Verwalten** öffnet das Computerverwaltungs-Snap-In (**compmgmt.msc**). In der Computerverwaltung ist ein Zugriff auf die Ereignisanzeige, Systeminformationen und Datenträgerverwaltung möglich. Durch diese Richtlinie wird nicht der Zugriff auf diese Tasks durch andere Methoden, wie z. B. über die Systemsteuerung oder den Befehl **Ausführen** verhindert. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf die Systeminformationen zu Terminalserver zugreifen können.

- Diese angegebenen Datenträger im Fenster „Arbeitsplatz“ ausblenden

Empfohlene Einstellung: **Aktiviert – Nur Laufwerke A, B, C und D beschränken**

Diese Richtlinie entfernt nur die Symbole aus **Arbeitsplatz**, Windows-Explorer und dem Standard-Dateialogfeld. Durch diese Einstellung wird nicht der Zugriff von Benutzern auf diese Laufwerke durch andere Methoden verhindert, z. B. über die Eingabeaufforderung. Mit dieser Richtlinie können nur die Laufwerke **A:** bis **D:** ausgeblendet werden. Es wird empfohlen, diese Richtlinie zu aktivieren, um das Diskettenlaufwerk, das CD-ROM-Laufwerk

und die Betriebssystempartition auszublenden. Als einziges Laufwerk, das für Benutzer sichtbar ist, kann eine Partition für öffentliche Daten konfiguriert werden. Bei Bedarf kann der Zugriff auf diese Partition mit NTFS-Berechtigungen beschränkt werden.

- Zugriff auf Laufwerke vom Arbeitsplatz nicht zulassen

Empfohlene Einstellung: **Aktiviert – Nur Laufwerke A, B, C und D beschränken**

Diese Richtlinie verhindert den Zugriff auf die Laufwerke **A:** bis **D:** über **Arbeitsplatz**, Windows-Explorer und dem Standard-Dateidialogfeld. Diese Richtlinie verhindert nicht den Zugriff über Programme, die nicht die Standarddialogfelder verwenden. Die Benutzer können weiterhin Anwendungen starten, die sich auf den eingeschränkten Laufwerken befinden. Es wird empfohlen, diese Richtlinie zu aktivieren, um das Suchen von Dateien in Systempartitionen zu beschränken.

- Registerkarte „Hardware“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Registerkarte **Hardware** für die Systemsteuerungsobjekte **Maus**, **Tastatur** und **Sounds und Audiogeräte**. Zusätzlich wird die Registerkarte **Hardware** aus dem Eigenschaftendialogfeld aller lokalen Laufwerke entfernt, wie z. B. Festplattenlaufwerke, Diskettenlaufwerke und CD-ROM-Laufwerke. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer mit der Registerkarte **Hardware** nicht die Geräteliste bzw. die Geräteeigenschaften anzeigen können.

- „Abzüge online bestellen“ von „Bildaufgaben“ löschen

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, um die Verknüpfung **„Abzüge online bestellen“ von „Bildaufgaben“** im Ordner **Eigene Bilder** zu entfernen.

- „Im Web veröffentlichen“ aus den Datei- und Ordneraufgaben entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinieneinstellung entfernt die Aufgaben **Im Web veröffentlichen**, **Diesen Ordner im Web veröffentlichen** und **Ausgewählte Elemente im Web veröffentlichen** im Windows-Explorer. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine Dateien oder Ordner auf einer Webseite veröffentlichen können.

- „Benachbarte Computer“ nicht unter Netzwerkumgebung anzeigen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Computer in der Domäne des Benutzers aus den Listen der Netzwerkressourcen im Windows-Explorer und **Netzwerkumgebung**. Durch diese Einstellung wird nicht verhindert, dass Benutzer mit Hilfe anderer Methoden Verbindungen zu diesen Computern herstellen, z. B. über die Eingabeaufforderung oder im Dialogfeld **Netzlaufwerk verbinden**. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer die Domäne nicht ohne weiteres durchsuchen können.

- Symbol „Gesamtes Netzwerk“ nicht in „Netzwerkumgebung“ anzeigen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Computer außerhalb der lokalen Domäne des Benutzers aus den Listen der Netzwerkressourcen im Windows-Explorer und **Netzwerkumgebung**. Durch diese Einstellung wird nicht verhindert, dass Benutzer durch andere Methoden Verbindungen zu diesen Computern herstellen, z. B. über die Eingabeaufforderung oder im Dialogfeld **Netzlaufwerk verbinden**. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer das Netzwerk nicht ohne weiteres durchsuchen können.

- Windows+X-Abkürzungstasten deaktivieren

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie deaktiviert die Windows -Tastenkürzel. Tastaturen mit einer Windows-Logotaste stellen Benutzern Tastenkombinationen für gebräuchliche Shellfeatures zur Verfügung. Durch Drücken der Tastenkombination Windows+R wird beispielsweise das Dialogfeld **Ausführen** geöffnet; durch Drücken von Windows+E wird Windows-Explorer gestartet. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer mit der Windows-Logotaste keine Anwendungen starten können.

- Klassische Shell aktivieren

Empfohlene Einstellung: **Aktiviert**

Mit dieser Richtlinie können die Features Active Desktop und Webansicht entfernt werden. Wenn diese Richtlinie aktiviert wird, werden Active Desktop und Webansicht deaktiviert. Darüber hinaus können Benutzer ihr System nicht so konfigurieren, dass Elemente mit einem einzigen Klick geöffnet werden können (z. B. unter **Maus** in der Systemsteuerung). Demzufolge ähnelt die Benutzeroberfläche der Benutzeroberfläche von Windows NT 4.0 und funktioniert auch wie diese, und Benutzer können die neuen Features nicht wiederherstellen. Es wird empfohlen, diese Richtlinie zu aktivieren, um Ordneraufgaben zu entfernen. Mit einigen Ordneraufgaben, wie z. B. über den Ordner **Eigene Musik**, kann Internet Explorer gestartet werden.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows-Explorer\Standarddialog "Datei öffnen"]

- Ortsleiste in Standarddialogen ausblenden

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Symbolleiste aus dem Standarddialogfeld **Datei öffnen**. Dieses Feature wurde zuerst in Windows 2000 hinzugefügt. Wenn es deaktiviert wird, sieht das Standarddialogfeld genauso aus wie in Windows NT 4.0 oder früher. Diese Richtlinien gelten nur für Programme, die das Standarddialogfeld verwenden. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres das Netzwerk oder den lokalen Computer durchsuchen können.

- Elemente, die in der Ortsleiste angezeigt werden

Diese Richtlinie ermöglicht es, Elemente in der Ortsleiste des Standarddialogfelds **Datei öffnen** durch vordefinierte Elemente zu ersetzen. Zum Anzeigen dieser Leiste starten Sie Editor, und wählen Sie **Datei** und dann **Öffnen** aus.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Taskplaner]

- Eigenschaftenseiten ausblenden

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht die Eigenschaften vorhandener Tasks anzeigen und ändern können.

- Löschen von Tasks nicht zulassen

Diese Richtlinie verhindert, dass Administratoren Tasks aus dem Ordner **Geplante Tasks** löschen. Durch diese Einstellung wird nicht verhindert, dass Administratoren Tasks mit dem Befehl **AT** oder von einem Remotecomputer aus löschen.

- Ausführen oder Beenden von einem Task verhindern

Diese Richtlinie verhindert, dass Administratoren Tasks starten oder beenden.

- Erstellen von neuen Tasks nicht zulassen

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine neuen geplanten Tasks erstellen oder Anwendungen suchen können. Durch diese Einstellung wird nicht verhindert, dass Administratoren Tasks mit dem Befehl **AT** oder von einem Remotecomputer aus erstellen.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Messenger]

- Ausführung von Windows Messenger nicht zulassen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie deaktiviert Windows Messenger für den Benutzer. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine Links oder Dateien von anderen Windows Messenger-Benutzern erhalten können.

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows Update]

- Zugriff auf alle Windows Update-Funktionen entfernen

Diese Richtlinie entfernt den Zugriff auf Windows Update. Wenn diese Einstellung aktiviert wird, werden alle Windows Update-Features entfernt. Diese Richtlinie sperrt den Zugriff auf die Microsoft Windows Update-Website unter <http://go.microsoft.com/fwlink/?LinkId=18539>, über den Windows Update-Hyperlink im Startmenü sowie im Menü **Extras** in Internet Explorer. Darüber hinaus wird die automatische Aktualisierung von Windows deaktiviert. Sie erhalten weder eine Benachrichtigung über wichtige Updates noch wichtige Updates selbst von Windows Update. Diese Einstellung verhindert auch, dass der Geräte-Manager automatisch Treiberupdates von der Windows Update-Website installiert. Mit dieser Richtlinie können auch Änderungen des Terminalservers in einer Produktionsumgebung verhindert werden. Wenn Sie Windows Update deaktivieren, sollten Sie regelmäßige Überprüfungen planen, damit sichergestellt wird, dass die neuesten wichtigen Windows-Updates vorhanden sind.

[Benutzerkonfiguration\Administrative Vorlagen\System\Taskleiste und Startmenü]

- Verknüpfungen und Zugriff auf Windows Update entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt Verknüpfungen zur und den Zugriff auf die Windows Update-Website. Die Windows Update-Website ist nur für Administratoren verfügbar. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf Internet Explorer zugreifen können.

- Standardprogrammgruppen aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt aus den Profilen aller Benutzer die Verknüpfungen zu Programmen. Es steht lediglich das Startmenü im Benutzerprofil bzw. das umgeleitete Startmenü zur Verfügung. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres auf integrierte Anwendungen wie Spiele, Rechner und Media Player zugreifen können.

- Liste angehefteter Programme aus dem Startmenü entfernen

Diese Richtlinie entfernt die Liste angehefteter Programme aus dem Startmenü. Darüber hinaus werden die Standardlinks zu Internet Explorer und Outlook Express entfernt (sofern sie angeheftet sind) sowie verhindert, dass Benutzer neue Programme an das Startmenü anheften. Die Liste häufig verwendeter Programme wird nicht beeinflusst.

- Programme im Menü „Einstellungen“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt **Systemsteuerung, Drucker und Netzwerkverbindungen** aus **Einstellungen** im klassischen Startmenü, **Arbeitsplatz** und Windows-Explorer. Darüber hinaus wird das Ausführen von Programmen verhindert, die durch diese Ordner dargestellt werden (wie z. B. **Control.exe**). Die Benutzer können jedoch weiterhin Objekte der Systemsteuerung mit anderen Methoden starten, wie z. B. durch Klicken mit der rechten Maustaste auf den Desktop, um **Anzeigeeigenschaften** zu öffnen, oder durch Klicken mit der rechten Maustaste auf **Arbeitsplatz**, um **Systemeigenschaften** zu öffnen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres Systemeinstellungen anzeigen oder darauf zugreifen können.

- Menüeintrag „Netzwerkverbindungen“ aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass der Ordner **Netzwerkverbindungen** geöffnet wird. Diese Richtlinie entfernt außerdem den Menüeintrag **Netzwerkverbindungen** aus **Einstellungen** im Startmenü. In der Systemsteuerung und im Windows-Explorer wird **Netzwerkverbindungen** weiterhin angezeigt. Wenn Benutzer versuchen, **Netzwerkverbindungen** zu starten, wird eine Meldung mit dem Hinweis angezeigt, dass eine Einstellung diese Aktion verhindert. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine neuen Verbindungen, wie z. B. VPN- oder DFÜ-Verbindungen, erstellen können.

- Menüeintrag „Suchen“ aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Suchfunktion aus dem Startmenü. Diese Einstellung entfernt **Suchen** aus dem Startmenü sowie aus dem Kontextmenü, das beim Klicken mit der rechten Maustaste auf das Startmenü angezeigt wird. Weiterhin zeigt das System keine Reaktion, wenn Benutzer Windows+F oder F3 drücken. Im Windows-Explorer wird weiterhin die Option **Suchen** auf der Symbolleiste für Standardschaltflächen angezeigt. Das System zeigt jedoch keine Reaktion, wenn der Benutzer STRG+F drückt. Wenn Sie mit der rechten Maustaste auf ein Symbol klicken, das ein Laufwerk oder einen Ordner darstellt, wird im Kontextmenü der Eintrag **Suchen** ebenfalls nicht angezeigt. Diese Einstellung beeinflusst lediglich die angegebenen Elemente der Benutzeroberfläche. Sie wirkt sich nicht auf Internet Explorer aus und verhindert nicht, dass Benutzer andere Suchverfahren verwenden. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres nach Anwendungen suchen können, die ihnen nicht zugewiesen wurden.

- Drag & Drop-Kontextmenüs aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass Benutzer mittels Drag & Drop Menüeinträge im Startmenü neu anordnen oder entfernen. Diese Einstellung verhindert nicht, dass Benutzer andere Verfahren verwenden, um das Startmenü anzupassen, oder Aufgaben ausführen, die in den Kontextmenüs verfügbar sind. Es wird empfohlen, diese Richtlinie zu aktivieren, um Kontextmenüs einschließlich Aufgaben, wie z. B. das Erstellen einer neuen Verknüpfung, aus dem Startmenü zu entfernen.

- Menüeintrag „Favoriten“ aus dem Startmenü entfernen

Diese Richtlinie verhindert, dass Benutzer das Menü **Favoriten** dem Startmenü oder dem klassischen Startmenü hinzufügen. Verwenden Sie diese Richtlinie, wenn Benutzer nicht in der Lage sein sollen, Internet Explorer auszuführen.

Anmerkung: Das Menü **Favoriten** wird standardmäßig nicht im Startmenü angezeigt. Diese Richtlinie deaktiviert jedoch den Link **Favoriten**. Diese Einstellung wirkt sich nur auf das Startmenü aus. Das Menü **Favoriten** ist im Windows-Explorer und Internet Explorer weiterhin vorhanden.

- Menüeintrag „Hilfe“ aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt den Link **Hilfe** aus dem Startmenü. Diese Einstellung wirkt sich nur auf das Startmenü aus. Zum Deaktivieren der neuen Hilfe- und Supportanwendung müssen Sie den Dienst in der Computerkonfiguration deaktivieren (siehe „Beschränkende Computerrichtlinien“). Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht ohne weiteres Systeminformationen zu Terminalserver anzeigen können.

- Menüeintrag „Ausführen“ aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht versuchen können, Anwendungen auszuführen. Diese Einstellung ist entscheidend, um Terminalserver einzuschränken. Wenn diese Richtlinie aktiviert wird, werden der Befehl **Ausführen** aus dem Startmenü und **Neuer Task** aus dem Task-Manager entfernt. Außerdem können die Benutzer in der Adressleiste von Internet Explorer keine UNC-Pfade, lokalen Laufwerke und lokalen Ordner eingeben. Benutzer, die erweiterte Tastaturen verwenden, können darüber hinaus nicht mehr das Dialogfeld **Ausführen** anzeigen, indem sie Windows+R drücken.

Anmerkung: Die Einstellung **Menüeintrag „Ausführen“ aus dem Startmenü entfernen** wirkt sich nur auf die angegebene Benutzeroberfläche aus. Sie verhindert nicht, dass Benutzer andere Methoden verwenden, um Programme auszuführen.

- Symbol „Netzwerkumgebung“ aus dem Startmenü entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt das Symbol **Netzwerkumgebung** aus dem Startmenü. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer das Netzwerk nicht ohne weiteres durchsuchen können.

- Option „Abmelden“ dem Startmenü hinzufügen

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer sich leicht von Terminalserversitzungen abmelden können. Diese Richtlinie fügt den Menüeintrag „<Benutzername>“ **abmelden** zum Startmenü hinzu und verhindert, dass Benutzer diesen Eintrag entfernen. Diese Einstellung wirkt sich nur auf das Startmenü aus. Sie hat keine Auswirkung auf den Menüeintrag **Abmelden** im Dialogfeld **Windows-Sicherheit**, das angezeigt wird, wenn auf einem Terminalserverclient STRG+ALT+ENTF oder STRG+ALT+ENDE gedrückt wird.

- Befehl „Herunterfahren“ entfernen und Zugriff darauf verweigern

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie macht es Benutzern unmöglich, im Startmenü und im Dialogfeld **Windows-Sicherheit** (STRG+ALT+ENTF) das Dialogfeld **Herunterfahren** zu öffnen. Diese Richtlinie verhindert nicht, dass Benutzer Programme ausführen, um Windows zu beenden. Es wird empfohlen, diese Richtlinie zu aktivieren, um eine Verwirrung der Benutzer zu vermeiden und Administratoren zu hindern, ein produktives System herunterzufahren.

- Ändern der Einstellungen für die Taskleiste und das Startmenü verhindern

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert eine Anpassung der Taskleiste und des Startmenüs. Durch diese Einstellung kann der Desktop übersichtlicher gestaltet werden, da die vom Administrator festgelegte Konfiguration eingehalten wird. Es wird empfohlen, diese Richtlinie zu aktivieren, um die Möglichkeit zu beschränken, durch Suchen oder Angeben des Pfades einer Anwendung weitere Anwendungen zum Startmenü hinzuzufügen.

- Zugriff auf Kontextmenüs für die Taskleiste deaktivieren

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt das Kontextmenü in der Taskleiste. Diese Einstellung verhindert nicht, dass Benutzer andere Verfahren verwenden, um Befehle auszuführen, die in diesem Menü verfügbar sind. Es wird empfohlen, diese Richtlinie zu aktivieren, um den Zugriff auf Dateien und Anwendungen durch Starten von Windows-Explorer oder Klicken auf **Suchen** zu verhindern.

- Klassisches Startmenü erzwingen

Diese Richtlinie hat Einfluss auf die Darstellung des Startmenüs. Das klassische Startmenü in Windows 2000 ermöglicht es Benutzern, Standardaufgaben auszuführen, während das neue Startmenü herkömmliche Menüeinträge in einem Menü zusammenfasst. Wenn das klassische Startmenü verwendet wird, werden die folgenden Symbole auf dem Desktop angeordnet: **Eigene Dateien**, **Eigene Bilder**, **Eigene Musik**, **Arbeitsplatz** und **Netzwerkumgebung**. Im neuen Startmenü werden diese Elemente direkt gestartet. Wenn das neue Startmenü deaktiviert wird, wird **Drucker und Faxgeräte** entfernt. Über **Drucker und Faxgeräte** können die Benutzer die Servereigenschaften anzeigen und feststellen, wo der Spoolordner installiert ist.

[Benutzerkonfiguration\Administrative Vorlagen\Desktop]

- Eintrag „Eigenschaften“ aus dem Kontextmenü von „Eigene Dateien“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Einstellung blendet die Option **Eigenschaften** im Kontextmenü von **Eigene Dateien** aus. Es wird empfohlen, diese Richtlinie zu aktivieren, wenn Kontextmenüs nicht deaktiviert sind und die Benutzer nicht ohne weiteres in der Lage sein sollen, den Pfad zum Ordner **Eigene Dateien** anzuzeigen oder zu bearbeiten.

- Eintrag „Eigenschaften“ aus dem Kontextmenü von „Arbeitsplatz“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Einstellung blendet die Option **Eigenschaften** im Kontextmenü von **Arbeitsplatz** aus. Es wird empfohlen, diese Richtlinie zu aktivieren, wenn Kontextmenüs nicht deaktiviert sind und die Benutzer nicht ohne weiteres in der Lage sein sollen, die Konfigurationsinformationen zu Terminalserver anzuzeigen.

- Eintrag „Eigenschaften“ aus dem Kontextmenü des Papierkorbs entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Option **Eigenschaften** aus dem Kontextmenü des Papierkorbs. Es wird empfohlen, diese Richtlinie zu aktivieren, wenn Kontextmenüs nicht deaktiviert sind und die Benutzer nicht ohne weiteres in der Lage sein sollen, die Einstellungen für den Papierkorb anzuzeigen oder zu ändern.

- Desktopsymbol „Netzwerkumgebung“ ausblenden

Empfohlene Einstellung: **Aktiviert**

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer das Netzwerk nicht ohne weiteres nach Anwendungen durchsuchen können. Diese Einstellung wirkt sich nur auf das Desktopsymbol aus. Durch diese Einstellung wird nicht verhindert, dass Benutzer Verbindungen zum Netzwerk herstellen oder mit anderen Methoden nach freigegebenen Computern im Netzwerk suchen.

- Internet Explorer-Symbol auf dem Desktop ausblenden

Diese Richtlinie entfernt das Symbol **Internet Explorer** vom Desktop. Durch diese Einstellung wird nicht verhindert, dass Benutzer Internet Explorer mit anderen Methoden starten können.

- Pfadänderung für den Ordner „Meine Dateien“ nicht zulassen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie beschränkt den Pfad von **Eigene Dateien** auf den angegebenen Pfad. Es wird empfohlen, diese Richtlinie zu aktivieren, um das Suchen nach Anwendungen zu verhindern.

- Alle Desktopsymbole ausblenden und deaktivieren

Diese Richtlinie entfernt Symbole, Verknüpfungen, und andere Standard- und benutzerdefinierte Elemente vom Desktop, wie z. B. **Aktenkoffer**, **Papierkorb**, **Arbeitsplatz** und **Netzwerkumgebung**. Durch das Entfernen der Symbole und Verknüpfungen wird nicht verhindert, dass der Benutzer mit anderen Methoden die Programme startet oder die jeweils dargestellten Elemente öffnet. Der Benutzer kann mit dem Standarddialogfeld **Datei** oder Windows-Explorer weiterhin Elemente auf dem Desktop speichern und öffnen. Die Elemente werden jedoch nicht auf dem Desktop angezeigt.

- Symbol „Eigene Dateien“ vom Desktop entfernen

Diese Richtlinie entfernt die meisten Vorkommen des Symbols **Eigene Dateien**. Durch diese Einstellung wird nicht verhindert, dass der Benutzer andere Verfahren verwendet, um auf den Inhalt des Ordners **Eigene Dateien** zuzugreifen.

- Symbol „Arbeitsplatz“ vom Desktop entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie blendet **Arbeitsplatz** auf dem Desktop und im neuen Startmenü aus. Darüber hinaus werden die Links zu **Arbeitsplatz** in der Webansicht aller Explorer-Fenster sowie **Arbeitsplatz** im Explorer-Fensterbereich mit der Ordnerstruktur ausgeblendet. Wenn der Benutzer mit dem Symbol **Nach oben zu Arbeitsplatz** navigiert, während diese Einstellung aktiviert ist, wird ein leerer Ordner **Arbeitsplatz** angezeigt. Es wird empfohlen, diese Richtlinie zu aktivieren, um die Desktopumgebung der Benutzer übersichtlicher zu gestalten und zu verhindern, dass Benutzer ohne weiteres auf **Computerverwaltung** und **Systemeigenschaften** zugreifen können, da das Klicken mit der rechten Maustaste auf das Symbol nicht mehr möglich ist.

Anmerkung: Durch Ausblenden von **Arbeitsplatz** und dessen Inhalt wird der Inhalt der untergeordneten Ordner von **Arbeitsplatz** nicht ausgeblendet. Wenn die Benutzer beispielsweise zu einem Festplattenlaufwerk navigieren, werden alle Ordner und Dateien angezeigt, auch wenn diese Einstellung aktiviert ist.

[Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung]

- Zugriff auf die Systemsteuerung nicht zulassen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt den Zugriff auf die Systemsteuerung und deaktiviert alle Programme der Systemsteuerung. Darüber hinaus wird das Starten von **Control.exe**, der Programmdatei für die Systemsteuerung, verhindert. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine Konfigurationsinformationen zu Terminalserver anzeigen können.

[Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung\Software]

- Systemsteuerungsoption „Software“ entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie entfernt die Option **Software** aus der Systemsteuerung sowie den Menüeintrag **Software** aus Menüs. Wenn der Zugriff auf die Systemsteuerung nicht zugelassen werden soll, können mit dieser Richtlinie die Links zu **Software** entfernt werden, wie z. B. in **Arbeitsplatz**. Beim Klicken auf einen solchen Link wird eine Meldung angezeigt, dass der Zugriff verweigert wird. Diese Einstellung verhindert nicht, dass Benutzer andere Werkzeuge und Methoden verwenden, um Programme zu installieren und zu deinstallieren. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine Konfigurationsinformationen zu Terminalserver anzeigen können.

[Benutzerkonfiguration\Administrative Vorlagen\Systemsteuerung\Drucker]

- Hinzufügen von Druckern verhindern

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass Benutzer mit den üblichen Methoden lokale Drucker und Netzwerkdrucker hinzufügen. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer das Netzwerk oder Active Directory nicht nach Druckern durchsuchen können. Diese Richtlinie verhindert nicht die automatische Erstellung von umgeleiteten Terminalserverdruckern, und sie verhindert auch nicht, dass Benutzer andere Programme ausführen, um Drucker hinzuzufügen.

[Benutzerkonfiguration\Administrative Vorlagen\System]

- Zugriff auf Eingabeaufforderung verhindern

Empfohlene Einstellung: **Aktiviert** – Setzen Sie **Soll die Skriptverarbeitung der Eingabeaufforderung auch deaktiviert werden?** auf **Nein** fest.

Diese Richtlinie verhindert, dass Benutzer die interaktive Eingabeaufforderung **Cmd.exe** ausführen. An der Eingabeaufforderung können Benutzer Anwendungen starten. Diese Einstellung legt außerdem fest, ob Batchdateien (CMD- und BAT-Dateien) auf dem Computer ausgeführt werden können.

Anmerkung: Sie sollten das Ausführen von Terminalserver-Batchdateien auf dem Computer nicht deaktivieren. Diese Richtlinie verhindert nicht den Zugriff auf **Command.com** (den 16-Bit-Befehlsinterpreter). Wenn Sie **Command.com** deaktivieren möchten, können Sie den Zugriff mit NTFS-Berechtigungen beschränken oder mit der Richtlinie **Zugriff auf 16-Bit-Anwendungen verhindern** alle 16-Bit-Anwendungen deaktivieren.

Es wird empfohlen, die Richtlinie **Zugriff auf Eingabeaufforderung verhindern** zu aktivieren, damit Benutzer andere Richtlinien nicht über die Eingabeaufforderung als Ersatz für Windows-Explorer als Shell umgehen können.

- Zugriff auf Programme zum Bearbeiten der Registrierung verhindern

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie hindert Benutzer daran, Registrierungseinträge zu ändern, da **Regedit.exe** deaktiviert wird. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nicht die Eingabeaufforderung als Shell verwenden oder andere Richtlinien umgehen können. Diese Richtlinie verhindert nicht, dass die Registrierung mit anderen Anwendungen bearbeitet wird.

- Nur zugelassene Windows-Anwendungen ausführen

Empfohlene Einstellung: **Aktiviert** – Definieren Sie die Liste der zugelassenen Anwendungen

Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer nur Programme ausführen können, die der Liste der zugelassenen Anwendungen hinzugefügt wurden. Diese Richtlinie verhindert lediglich, dass Benutzer Programme ausführen, die von Windows-Explorer gestartet werden. Sie verhindert nicht, dass Benutzer Programme, wie z. B. Task-Manager ausführen, der durch einen Systemprozess gestartet werden kann. Wenn die Benutzer auf die Eingabeaufforderung (**Cmd.exe**) zugreifen können, verhindert diese Einstellungen ebenfalls nicht, dass Benutzer Programme an der Eingabeaufforderung ausführen können, die sie mit Windows-Explorer nicht starten dürfen.

[Benutzerkonfiguration\Administrative Vorlagen\System\Strg+Alt+Entf-Optionen]

- Task-Manager entfernen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verhindert, dass Benutzer den Task-Manager starten. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer mit dem Task-Manager keine Programme starten oder beenden, die Leistung des Terminalservers überwachen und die Namen der ausführbaren Dateien von Anwendungen suchen können.

- Sperren des Computers entfernen

Diese Richtlinie verhindert, dass Benutzer ihre Sitzungen sperren. Die Benutzer können weiterhin Sitzungen trennen und sich abmelden. Im gesperrten Zustand kann der Desktop nicht verwendet werden. Nur der Benutzer, von dem das System gesperrt wurde, oder der Systemadministrator kann die Sperrung aufheben.

[Benutzerkonfiguration\Administrative Vorlagen\System\Skripts]

- Legacy-Anmeldeskripts im Hintergrund ausführen

Empfohlene Einstellung: **Aktiviert**

Diese Richtlinie verbirgt die Anweisungen in Anmeldeskripts, die für Windows NT 4.0 und früher geschrieben wurden. Es wird empfohlen, diese Richtlinie zu aktivieren, damit Benutzer keine Anmeldeskripts, die für Windows NT 4.0 und früher geschrieben wurden, anzeigen oder unterbrechen können.

Andere Konfigurationsoptionen (ohne Richtlinien)

Deaktivieren des Such-Assistenten von Internet Explorer

Benutzer können auf den Such-Assistenten von Internet Explorer zugreifen, indem sie auf der Symbolleiste auf **Suchen** klicken bzw. in Internet Explorer STRG+E drücken. Mit dem Such-Assistenten von Internet Explorer können Benutzer nach Dateien und Ordnern suchen. Es gibt keine Richtlinie, um den Such-Assistenten von Internet Explorer zu deaktivieren. Dieser Vorgang muss manuell durchgeführt werden.

1. Erstellen Sie eine Textdatei in der lokalen Partition (**c:\windows\nosearch.txt**).
2. Die Datei kann den Text „Suche ist deaktiviert.“ enthalten.
3. Setzen Sie die NTFS-Berechtigungen der Datei für die Gruppe **Jeder** auf **Lesen und Ausführen** fest.
4. Ändern Sie anschließend die folgenden Registrierungswerte:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search
"SearchAssistant" = REG_SZ: c:\windows\nosearch.txt
"CustomizeSearch" = REG_SZ: c:\windows\nosearch.txt

Wenn die Benutzer den Such-Assistenten öffnen, wird der Inhalt der Textdatei angezeigt. Anstelle einer Textdatei kann eine Hypertextdatei (HTML) verwendet werden.

Entfernen von „Drucker und Faxgeräte“ aus dem neuen Startmenü

Das neue Startmenü enthält einen Link auf den Ordner **Drucker und Faxgeräte**. In diesem Ordner können Benutzer die Servereigenschaften des Druckspoolers anzeigen. Auf der Registerkarte **Erweitert** können Benutzer den Pfad des Spoolordners anzeigen, aber nicht bearbeiten. Führen Sie einen der folgenden Schritte aus, um den einfachen Zugriff auf das Dialogfeld **Servereigenschaften** zu deaktivieren:

1. Aktivieren Sie die Richtlinien **Klassische Shell aktivieren** und **Menü „Datei“ aus Windows-Explorer entfernen**.
2. Legen Sie den folgenden Registrierungswert fest:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"Start_ShowPrinters" = REG_DWORD: 0x00000000
3. Aktivieren Sie die Richtlinie **Ändern der Einstellungen für die Taskleiste und das Startmenü verhindern**. (Die Registrierungseinstellung kann durch Anmeldeskripts (Ausführen von **regedit /s hideprinters.reg**) oder durch eine benutzerdefinierte ADM-Datei bereitgestellt werden.)
4. Klicken Sie mit der rechten Maustaste auf die Schaltfläche **Start**, wählen Sie **Eigenschaften** aus, und klicken Sie dann auf der Registerkarte **Startmenü** auf **Anpassen**.
5. Deaktivieren Sie auf der Registerkarte **Erweitert** das Kontrollkästchen **Drucker und Faxgeräte**, und aktivieren Sie dann die Richtlinie **Ändern der Einstellungen für die Taskleiste und das Startmenü verhindern**. (Es wird empfohlen, die Kontextmenüs im Startmenü zu entfernen und dann den Zugriff auf die Systemsteuerung zu deaktivieren.)
6. Deaktivieren Sie das neue Startmenü, indem Sie die Richtlinie **Klassisches Startmenü erzwingen** und anschließend **Menü „Datei“ aus Windows-Explorer entfernen** aktivieren.

Deaktivieren des vollständigen Pfades im Windows-Explorer

Im Windows-Explorer wird standardmäßig der vollständige Pfad zum aktuellen Ordner angezeigt. Wenn die Benutzer bei aktivierter Ordnerumleitung über den Ordner **Eigene Dateien** hinaus navigieren, wird der vollständige Pfad des Ordners in der Adressleiste angezeigt. Hierbei handelt es

sich um eine konfigurierbare Ordneroption, die nicht durch Gruppenrichtlinien festgelegt werden kann. Führen Sie einen der folgenden Schritte aus, um den vollständigen Pfad zu deaktivieren:

1. Klicken Sie im **Windows-Explorer** auf der **Symbolleiste** auf **Extras**, und wählen Sie dann **Ordneroptionen** aus.
2. Klicken Sie auf die Registerkarte **Ansicht**, und deaktivieren Sie dann die Kontrollkästchen **Vollständigen Pfad in Adressleiste anzeigen** und **Vollständigen Pfad in der Titelleiste anzeigen**.
3. Aktivieren Sie die Richtlinie **Menüeintrag „Ordneroptionen“ aus dem Menü „Extras“ entfernen**.
4. Legen Sie die folgenden Registrierungswerte fest:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Cabinet State]
"FullPathAddress" = REG_DWORD: 0x00000000
"FullPath" = REG_DWORD: 0x00000000

Die Registrierungseinstellung kann durch Anmeldeskripts (Ausführen von **regedit /s addressbar.reg**) oder durch eine benutzerdefinierte ADM-Datei bereitgestellt werden.

Entfernen von Internet Explorer und Windows-Explorer von der Schnellstartleiste

Standardmäßig werden Links zu Internet Explorer und Windows-Explorer zur Schnellstartleiste hinzugefügt. Diese Links können in einem Anmeldeskript durch Hinzufügen der folgenden Zeilen entfernt werden:

```
del "%userprofile%\Anwendungsdaten\Microsoft\Internet Explorer\Quick Launch\explorer.exe.lnk"
```

```
del "%userprofile%\Anwendungsdaten\Microsoft\Internet Explorer\Quick Launch\Internet Explorer Browser starten.lnk"
```

Deaktivieren der Hilfe

In vielen Anwendungen können durch Drücken von F1 Hilfedateien geöffnet werden. Viele dieser Hilfedateien können Links zu anderen Anwendungen und Websites enthalten, auf die Benutzer normalerweise nicht zugreifen können. Es gibt keine Gruppenrichtlinie, um in Anwendungen den Zugriff auf die Hilfe zu beschränken. Dazu muss der Zugriff auf CHM- und HLP-Dateien mit NTFS-Berechtigungen beschränkt werden. Die Mehrzahl der Windows-Hilfedateien befindet sich im Ordner **%SystemRoot%\Help**, normalerweise **c:\windows\help**. Entfernen Sie einfach die Benutzergruppen aus der Zugriffskontrollliste für den Ordner. Aktivieren Sie dann die entsprechende Option, sodass die Berechtigungseinträge aller untergeordneten Objekte ersetzt werden. Dadurch wird verhindert, dass Benutzer Hilfedateien öffnen können.

Durchsuchen des Netzwerks mit den Standarddialogfeldern zum Öffnen/Speichern von Dateien

Das Standarddialogfeld **Datei öffnen/speichern** wird von vielen Anwendungen zum Öffnen oder Speichern von Dateien verwendet. Das Dialogfeld wird angezeigt, wenn in Anwendungen wie Editor im Menü **Datei** die Option **Öffnen** oder die Option **Speichern** ausgewählt wird. Vom Eingabefeld für den Pfad aus können Benutzer das Netzwerk durchsuchen. Im Dialogfeld **Datei öffnen/speichern** können die Benutzer UNC-Pfade eingeben, wie z. B. **\\localhost**, und dann die Freigaben des lokalen Servers durchsuchen. Über das Symbol **Eine Ebene nach oben** gelangen Benutzer zum übergeordneten Objekt, sodass sie die Domäne oder das Netzwerk durchsuchen können. Obwohl die Namen von Servern und Freigaben angezeigt werden, gelten für die Benutzer weiterhin die Beschränkungen aufgrund der Berechtigungen auf Freigabe- oder NTFS-Ebene. Wenn verhindert werden muss, dass Benutzern die Namen von Servern oder Freigaben angezeigt werden, stehen die folgenden Optionen zur Verfügung:

1. Verwenden Sie den Registrierungsschlüssel **RestrictAnonymous** zusammen mit Freigabe- und NTFS-Berechtigungen, um den Zugriff zu beschränken. Weitere Informationen finden Sie im Knowledge Base-Artikel 246261 *Verwenden des Registrierungswertes restrictanonymous in Windows 2000* unter <http://support.microsoft.com/default.aspx?scid=kb;de;246261>.
2. Verbergen Sie einen Freigabennamen, indem Sie am Ende des Freigabennamens „\$“ hinzufügen. Weitere Informationen finden Sie im Knowledge Base-Artikel 90929 *Freigabennamen mit „\$“-Zeichen am Ende werden nicht angezeigt* unter <http://support.microsoft.com/default.aspx?scid=kb;de;90929>.
3. Konfigurieren Sie die Computer so, dass keine Ankündigungen an Browser in der Domäne gesendet werden. Dies kann durch Hinzufügen des folgenden Registrierungswertes oder Ausführen des folgenden Befehls erreicht werden:

In der Registrierung:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
Wertname: Hidden
Datentyp: REG_DWORD
Datenwerte: 1

Die Registrierungseinstellung kann durch Anmeldeskripts (Ausführen von **regedit /s addressbar.reg**) oder durch eine benutzerdefinierte ADM-Datei bereitgestellt werden.

In der Eingabeaufforderung:

```
net config server /hidden:yes
```

Weitere Informationen finden Sie im Knowledge Base-Artikel 321710 *HOW TO: Hide a Windows 2000 -Based Computer from the Browser List* (englischsprachig) unter <http://go.microsoft.com/fwlink/?LinkId=18397>.

Weitere Beschränkungen

Richtlinien für Softwareeinschränkung

Die Richtlinien für Softwareeinschränkung sind ein neues Feature in Microsoft Windows XP und Windows Server 2003. Dieses wichtige Feature bietet Administratoren einen richtliniengesteuerten Mechanismus, um Programme, die auf den Computern in einer Domäne ausgeführt werden, zu ermitteln. Es steuert zudem, ob diese Programme ausgeführt werden können. Die Richtlinien können zerstörerische Skripts blockieren, unterstützen das Einschränken von Computern oder verhindern das Ausführen von unerwünschten Anwendungen.

Weitere Informationen zu Richtlinien für Softwareeinschränkung finden Sie im Whitepaper *Using Software Restriction Policies to Protect Against Unauthorized Software* (englischsprachig) unter <http://go.microsoft.com/fwlink/?LinkId=17299> und im Knowledge Base-Artikel 324036, *SO WIRD'S GEMACHT: Verwendung von Richtlinien für Softwareeinschränkung in Windows Server 2003* unter <http://support.microsoft.com/default.aspx?scid=kb;de;324036>.

Internet Explorer im Kioskmodus

Administratoren können die Standardbenutzeroberfläche von Windows-Explorer durch Internet Explorer im Kioskmodus ersetzen. Wenn Internet Explorer im Kioskmodus ausgeführt wird, werden die Titelleiste, die Menüs, die Symbolleisten und die Statusleiste von Internet Explorer nicht angezeigt und Internet Explorer wird im Vollbildmodus ausgeführt. Es werden nur Webseiten angezeigt. Internet Explorer im Kioskmodus kann durch Aktivieren der folgenden Richtlinie aktiviert werden:

[Benutzerkonfiguration\Administrative Vorlagen\System]

- Benutzerdefinierte Benutzerschnittstelle

Empfohlene Einstellung: **Aktiviert**

Dateiname der Schnittstelle: "%ProgramFiles%\Internet Explorer\IExplore.exe" –K

Wenn Internet Explorer im Kioskmodus als Benutzeroberfläche verwendet wird, sollten unbedingt die beschränkenden Richtlinien für Internet Explorer in den folgenden Abschnitten überprüft und aktiviert werden:

[Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer]

[Benutzerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Internet Explorer]

Zusammenfassung

Bei Windows Server 2003 handelt es sich um eine leistungsfähige Plattform, die die Funktionen von Terminalserver in einer Vielzahl von Umgebungen bereitstellen kann. Diese Bereitstellungen weisen unterschiedliche Anforderungen hinsichtlich Kontrolle und Verwaltbarkeit auf. Mit Hilfe von Active Directory können Sie die Integration von Terminalserver in unterschiedliche Umgebungen schnell und einfach konfigurieren und kontrollierte Desktopfunktionen und verwalteten Zugriff auf Anwendungen bereitstellen.

Verwandte Hyperlinks

In den folgenden Dokumenten finden Sie weitere Informationen:

- [„Microsoft Windows Server 2003 Terminal Server Overview“](#) (englischsprachig)
- [„Microsoft Windows Server 2003 Active Directory – technische Übersicht“](#)
- [„Securing Windows 2000 Terminal Services“](#) (englischsprachig)
- <http://support.microsoft.com/default.aspx?scid=kb;de;90929>.
- Knowledge Base-Artikel 321710, *HOW TO: Hide a Windows 2000 -Based Computer from the Browser List* (englischsprachig) unter <http://go.microsoft.com/fwlink/?LinkId=18397>.
- *Using Software Restriction Policies to Protect Against Unauthorized Software* (englischsprachig) unter <http://go.microsoft.com/fwlink/?LinkId=17299>.
- Knowledge Base-Artikel 324036 *SO WIRD'S GEMACHT: Verwendung von Richtlinien für Softwareeinschränkung in Windows Server 2003* unter <http://support.microsoft.com/default.aspx?scid=kb;de;324036>.
- *Windows 2003 Server-Website* unter <http://www.microsoft.com/germany/ms/windowsserver2003/>.

Bei diesem Dokument handelt es sich um ein vorläufiges Dokument, das bis zur endgültigen Handelsausgabe der hier beschriebenen Software wesentlichen Änderungen unterliegen kann.

Die in diesem Dokument enthaltenen Informationen stellen die behandelten Themen aus der Sicht der Microsoft Corporation zum Zeitpunkt der Veröffentlichung dar. Da Microsoft auf sich ändernde Marktanforderungen reagieren muss, stellt dies keine Verpflichtung seitens Microsoft dar, und Microsoft kann die Richtigkeit der hier dargelegten Informationen nach dem Zeitpunkt der Veröffentlichung nicht garantieren.

Dieses Dokument dient nur zu Informationszwecken. MICROSOFT SCHLIESST FÜR DIE INFORMATIONEN IN DIESEM DOKUMENT JEDE GEWÄHRLEISTUNG AUS, SEI SIE AUSDRÜCKLICH ODER KONKLUDENT.

Die Benutzer/innen sind verpflichtet, sich an alle anwendbaren Urheberrechtsgesetze zu halten. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den fachlichen Inhalt dieses Dokuments beziehen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Personen und Ereignissen sind frei erfunden. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Personen oder Ereignissen ist rein zufällig.

© 2003 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, Windows, das Windows-Logo und Windows Server sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Die in diesem Dokument aufgeführten Produkt- und Firmennamen können geschützte Marken ihrer jeweiligen Inhaber sein.