



Windows Server® 2008 R2

Workshop - Oliver Ryf MCITP

Active Directory
Security
Networking
Management

AGENDA

AD Administrative Center

Powershell

Recycle Bin Feature

Group Policy Management

Managed Service Accounts

Offline Domain Join

Authentication Mechanism

Assurance

ACTIVE DIRECTORY



Administrative Center

Click to add nodes to the navigation pane or to connect to other domains

Navigation Pane

The screenshot shows the Active Directory Administrative Center interface for the 'proseware (local)' domain. The interface is divided into several panes:

- Navigation Pane:** Located on the left, it shows a tree view of the domain structure including 'Users', 'Domain Controllers', and 'proseware-Users'. A red box highlights the 'Add Navigation Nodes...' button at the top.
- Breadcrumb Bar:** Located at the top, it shows the current path: 'Active Directory Domain Services > proseware (local)'. A red box highlights this bar.
- Management List:** The central pane displays a table of objects in the domain. A red box highlights this list.
- Tasks Pane:** Located on the right, it shows a list of actions available for the selected object, such as 'New', 'Move...', 'Delete', and 'Properties'. A red box highlights this pane.
- Preview Pane:** Located at the bottom, it shows details for the selected object, including 'Object class: builtinDomain' and 'Modified: 2/23/2009 4:25 PM'. A red box highlights this pane.

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgra...
Domain Controllers	Organizational Unit	Default container for domain...
ForeignSecurityPrincipals	Container	Default container for securit...
Infrastructure	infrastructureUpdate	
LostAndFound	lostAndFound	Default container for orphar...
Managed Service Accounts	Container	Default container for manag...
NTDS Quotas	msDS-QuotaContainer	Quota specifications contain...
Program Data	Container	Default location for storage...
System	Container	Builtin system settings
test1	Organizational Unit	
Users	Container	Default container for upgra...

Preview Pane

Management List

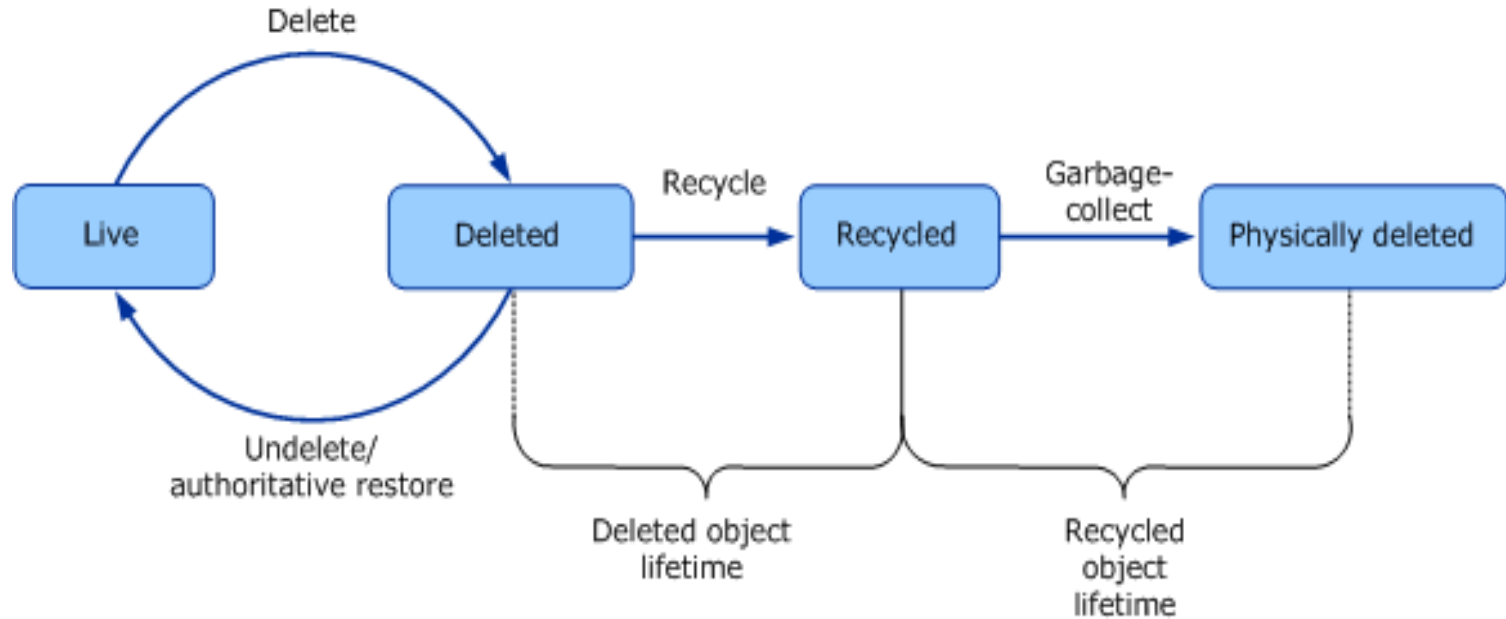
Tasks Pane

- Command-line scripting für
 - Administration
 - Konfiguration
 - Diagnostic
- Active Directory module provider mounted
 - Active Directory domains
 - AD LDS instances
 - Active Directory Database Mounting Tool instances

- Import-Module ActiveDirectory
- Get-Module
- Get-Command *ad*
- cd AD:
- cd "dc=whatever,dc=local"
- dir |format-table -auto
- New-AD.....

- Vorher:
 - DeletedObjects werden mit einem Tombstone versehen
 - Restore über Tombstone Reanimating beschränkt (SID)
- Neu:
 - DeletedObjects bleiben während 180 erhalten
 - Vollständiger Restore inklusive Backlinks möglich

Active Directory Object Life Cycle in Windows Server 2008 R2 with Active Directory Recycle Bin Enabled





Recycle Bin aktivieren

- `Get-ADOptionalFeature -filter 'name -like "*"'`
- `Enable-ADOptionalfeature 'recycle bin feature' -Scope ForestOrConfigurationSet -Target "whatever.local"`



Restore UserObject (ParentOU noch vorhanden)

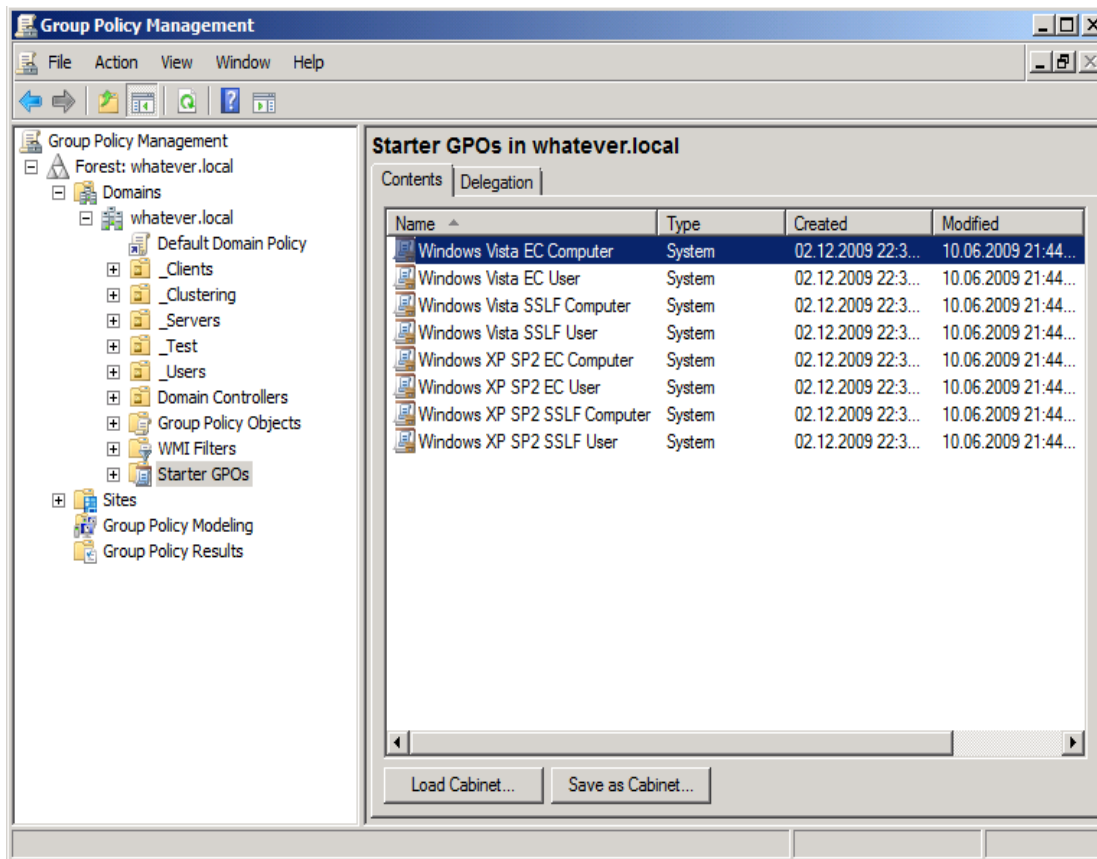
- `Get-ADObject -SearchBase "cn=deleted objects,dc=whatever,dc=local" -ldapfilter "(objectclass=*)" -includedeletedobjects`
- `Get-ADObject -filter {displayName -eq "Mary"} -includedeletedobjects | Restore-ADObject`

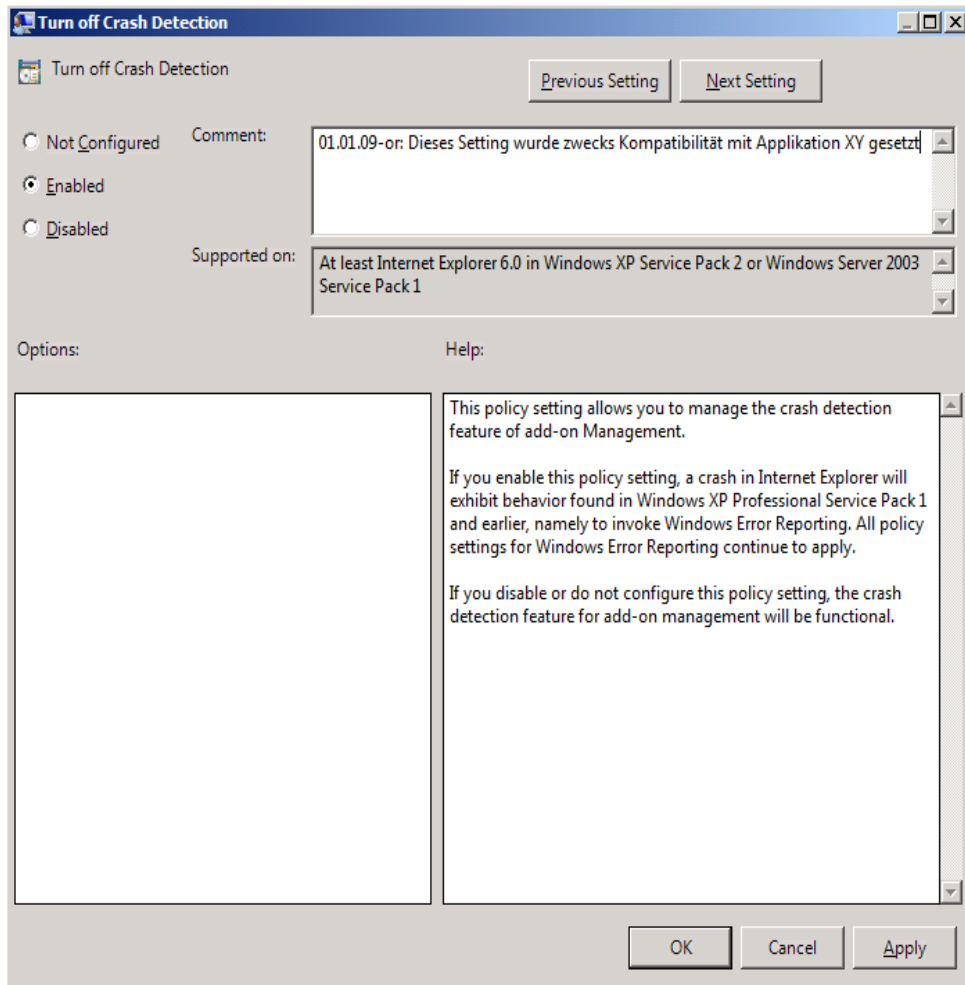
Restore OrganizationalUnit

- `Get-ADObject -filter 'name -like "oliver*"' -searchscope subtree -includedeletedobjects -properties lastknownparent`
- `Restore-ADObject -identity 'GUID'`
- `Get-ADObject -ldapfilter "(lastknownparent=OU=Benutzer,dc=whatever,dc=local)" -includedeletedobjects | Restore-ADObject`



- StarterGPOs bereits vorhanden
- Verbesserte Oberfläche zum Bearbeiten der GPOs
 - Search (endlich!)
 - Comments (an der richtigen Stelle)
- PowerShell Support





- Provision New Computer Account
 - DJOIN /provision /domain whatever.local /machine Client999 /savefile Client999.djoin
- Check File
 - Type Client999.djoin
- Offline Join
 - DJOIN /requestodj /loadfile Client999.djoin /windowspath \mount\windows

- Problem: Passwörter von Service Accounts werden praktisch nie gewechselt
- Lösung: Managed Service Accounts
 - Managed Service Accounts
 - Managed Virtual Accounts
- Nur mit PowerShell konfigurierbar
 - **New-ADServiceAccount -Name MOSS-Service -Path "CN=Managed Service Accounts,DC=whatever,DC=local"**

- Zugriff basierend auf Logonmethode bestimmen.
- Unterschiedliche Berechtigungen, abhängig davon, ob mit oder ohne Smartcard angemeldet wird.
- Voraussetzungen:
 - R2 Domain Functional Level
 - Certificate Infrastructure
 - AD Federation Services

Auditing
Multiple Active Firewall Profiles
Network Policy Server
Network Access Protection

SECURITY

- Advanced audit policy settings
 - 53 new settings
- "Reason for access" reporting
- Global Object Access Auditing



The screenshot shows the Group Policy Management Editor window. The left pane displays a tree view of policy categories, with 'Advanced Audit Policy Configuration' expanded to show 'Audit Policies'. The right pane displays the configuration page for 'Advanced Audit Policy Configuration', including a 'Getting Started' section with a warning icon and a table summarizing the status of various audit categories.

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

[More about Advanced Audit Configuration](#)

[Which editions of windows support Advanced Audit Configuration?](#)

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

- NPS templates and Templates Management
- RADIUS accounting improvements
- Full support for international, non-English character sets using UTF-8 encoding



- Multi-configuration SHV
- NAP client user interface improvements

DNS

DirectAccess

VPN Reconnect

BranchCache

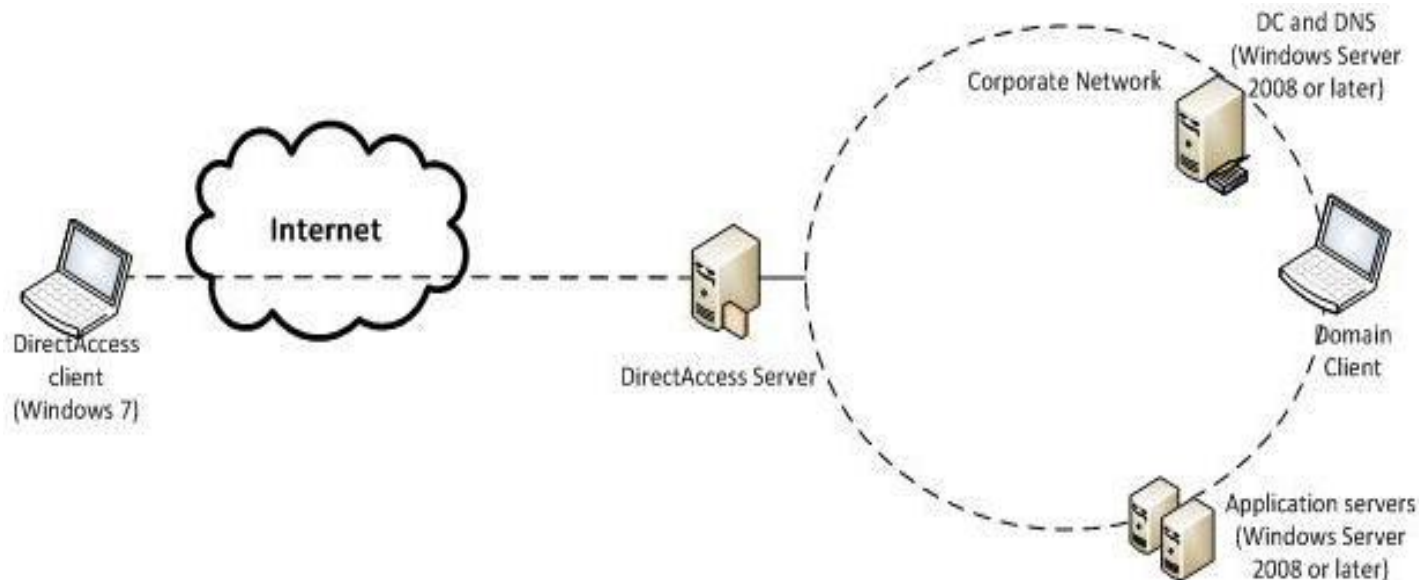
NETWORKING

- Support der DNS Security Extensions (DNSSEC)
 - Digitale Signierung der Zone und aller Records
 - Support der DNSKEY, RRSIG, NSEC, und DS Resource Records.
- DNS Devolution
 - Der Devolution-Level definiert, bis zu welcher Ebene Namensauflösung erfolgt

- Massnahmen gegen Cache-Poisoning
 - DNS Cache Locking
 - DNS Socket Pool



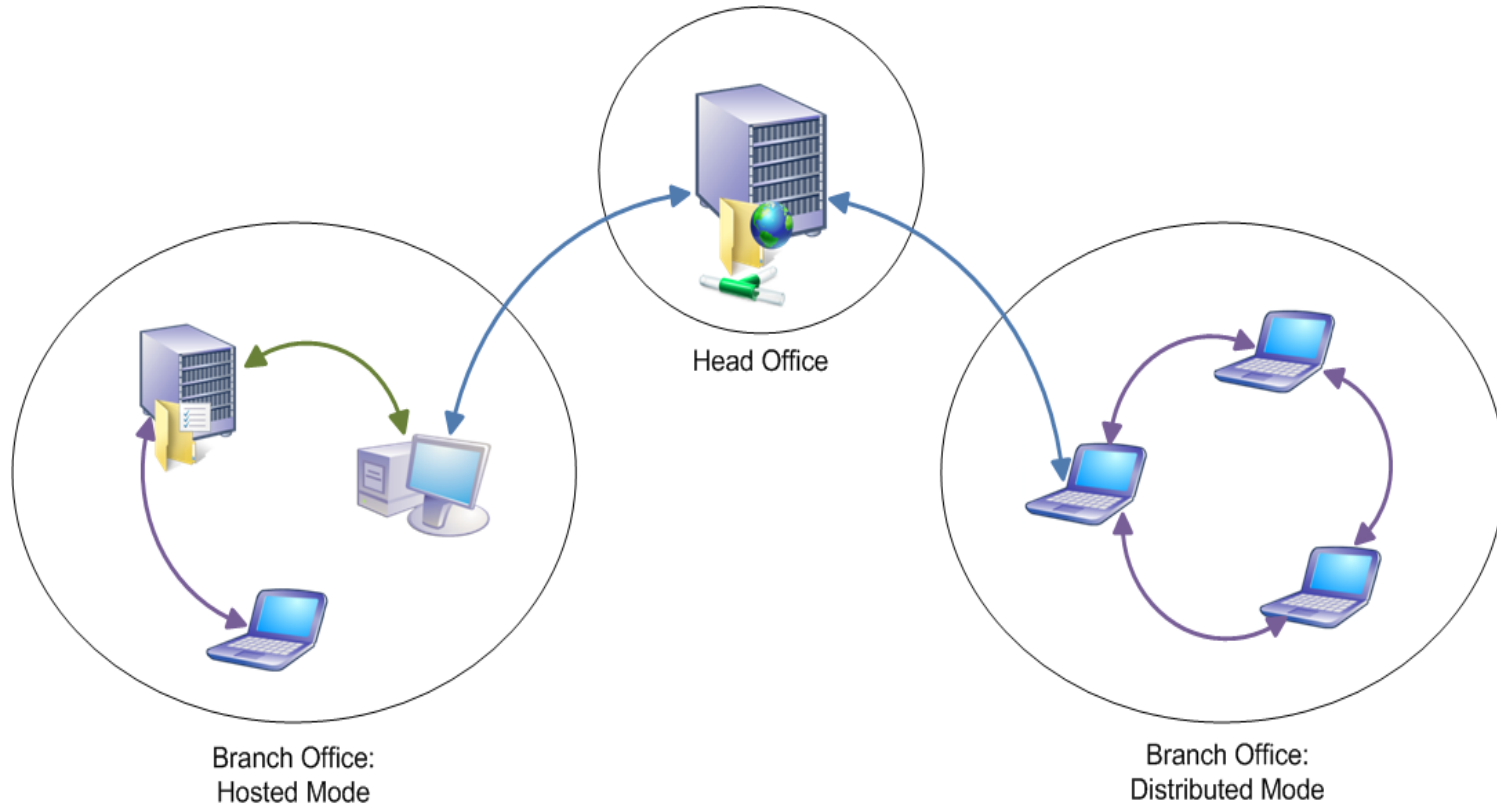
- Bietet Benutzern transparenten Zugriff auf interne Netzwerk-Ressourcen bei Verbindung via Internet
- IT-Verantwortliche können entfernte Verwaltung betreiben
- Aktualisierung von Richtlinien und Updates
- Benötigt keine VPN-Verbindung
- Verwendet IPv6!



- Nahtlose und konsistente VPN-Konnektivität
- Verwaltung entfernter Computer
- Automatische Wiederherstellung der VPN-Verbindung
- Für Benutzer transparent



- Verbessert die Verfügbarkeit von Netzwerk-
anwendungen und den Dateitransfer
- Reduziert Verwendung des WAN-Links
- Optimiert Datenfluss zwischen Clients und Servern
- Unterstützt allgemeine Netzwerkprotokolle





Server Core

Print and Document Services

Failover Clustering

Backup (!?!)

Server Management

Remote Management

ROLES/FEATURES/MANAGEMENT

- Remote Management via Server Manager
- Neue Rollen
 - Active Directory® Certificate Services (AD CS)
 - File Server Resource Manager component der File Services
 - Ein Subset von ASP.NET des Web Servers

- Neue Features
 - NET Framework
 - A subset of .NET Framework 2.0
 - A subset of .NET Framework 3.0, including Windows Communication Foundation (WCF) and Windows Workflow Foundation (WF)
 - A subset of .NET Framework 3.5, including WF additions from .NET Framework 3.5 and .NET Language-Integrated Query (LINQ)
 - Windows PowerShell
 - Windows-on-Windows 64-bit (WoW64)

- Print migration enhancements
 - Selektives Backup
- Printer driver isolation
 - Fehlerhafte Druckertreiber haben keinen Impact auf den Spooler-Prozess
- Print administrator delegation
- Location-aware printing
 - Verschiedene "Default-"Printer für verschiedene Netzwerke

- Bessere Validierung des Clusters
- Clustering des Remote Desktop Connection Broker
- Cluster Shared Volumes (CSV)
 - Single, consistent file namespace - c:\ClusterStorage
 - Mehrere Virtual Machines teilen sich ein LUN
 - Live Migration für Hyper-V
- Powershell Unterstützung

- Let's change topic . . .

- Best Practise Analyzer
- Server Manager Remote Management
 - WinRM Service
 - Rollen konfigurieren aber nicht hinzufügen
 - Auch für Server Core

- **Core Parking**

- Core Parking ist eine Funktion, welche den Stromverbrauch reduziert, indem Prozessorkerne basierend auf ihrer Auslastung heruntergefahren werden
- Windows 7 and Windows Server 2008 R2 unterstützen die Advanced Configuration and Power Interface (ACPI) 4.0 Spezifikation vom Juni 2009.

oliver.ryf@fonstone.com

FRAGEN?



Workshop - Oliver Ryf MCITP

Benutzeroberfläche
Management
Security
Windows XP Modus

Boot from VHD
Deployment

AGENDA



Taskbar

Fenster

Tastenkombinationen

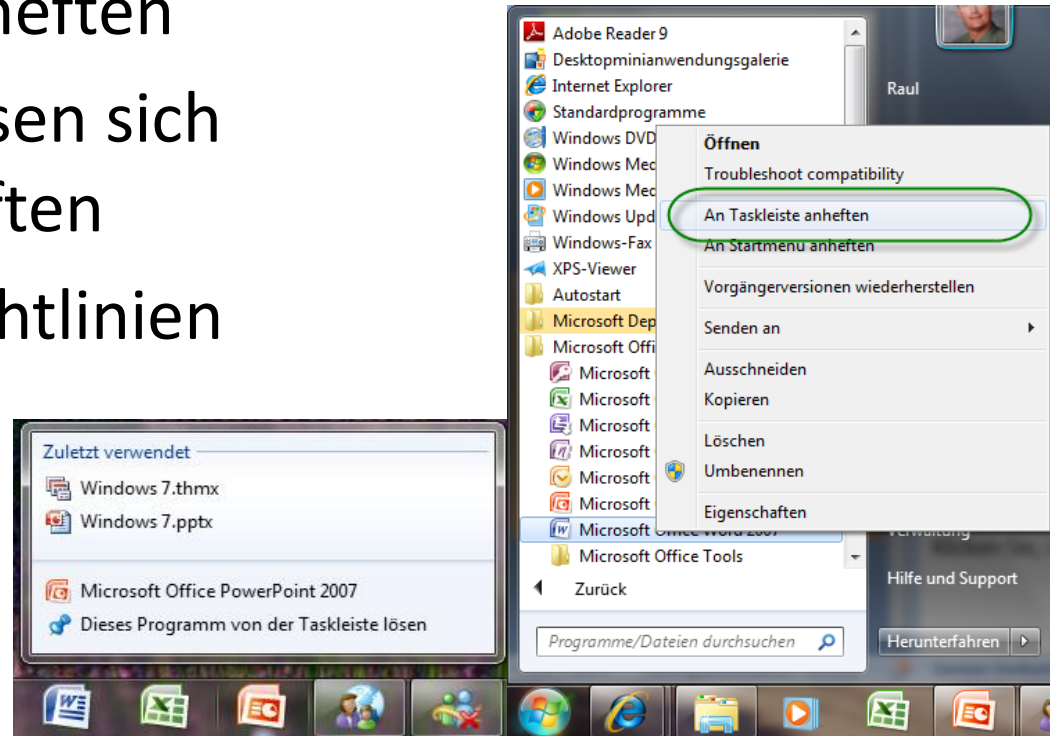
Bibliotheken

Search

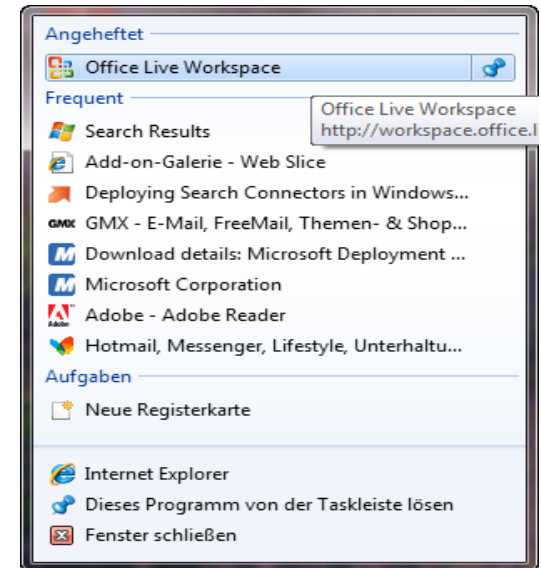
Action Center

BENUTZEROBERFLÄCHE

- Ersetzt die Schnellstartleiste
- Dokumente anheften
- Dokumente lassen sich gruppiert anheften
- Mit Gruppenrichtlinien steuerbar



- Links zu Webseiten können ebenfalls angeheftet werden
- Dadurch entfällt das Suchen in den Favoriten
- Lokale und Netzwerkordner anheften

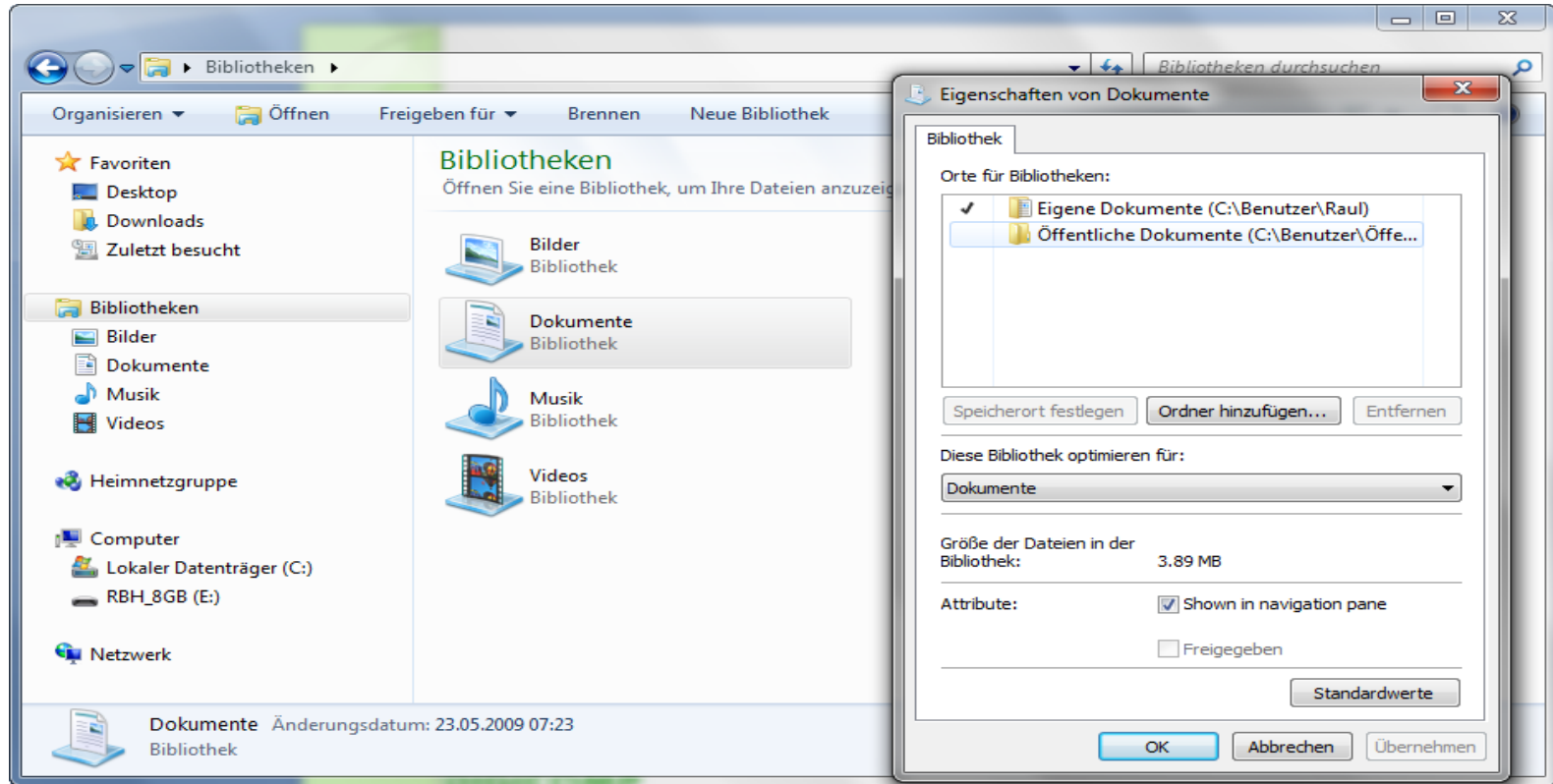


- Zieht man ein Fenster an den Bildschirmrand, wird es horizontal oder vertikal skaliert
- Im Center für erleichterte Bedienung kann diese Funktion ein- oder ausgeschaltet werden
- Zum Fenster schnell maximieren oder minimieren, auf dessen Icon in der Taskleiste geklickt wird
- "Schütteln" eines Fensters minimiert alle anderen

Tastenkombination	Zweck
Windows-Logo-Taste + Zahl	Starten des Programms, das an der durch die Zahl angegebenen Position an die Taskleiste angeheftet ist. Sollte das Programm bereits ausgeführt werden, wird zu diesem Programm gewechselt.
UMSCHALT+Windows-Logo-Taste + Zahl	Starten einer neuen Instanz des Programms, das an der durch die Zahl angegebenen Position an die Taskleiste angeheftet ist
STRG+Windows-Logo-Taste + B	Wechseln zu dem Programm, von dem im Infobereich eine Meldung angezeigt wurde
Windows-Logo-Taste + LEERTASTE	Anzeigen einer Desktopvorschau
Windows-Logo-Taste + NACH-OBEN	Maximieren des Fensters
Windows-Logo-Taste + NACH-LINKS	Maximieren des Fensters auf der linken Seite des Bildschirms
Windows-Logo-Taste + NACH-RECHTS	Maximieren des Fensters auf der rechten Seite des Bildschirms
Windows-Logo-Taste + NACH-UNTEN	Minimieren des Fensters
Windows-Logo-Taste + POS1	Minimieren aller Fenster mit Ausnahme des aktiven Fensters
Windows-Logo-Taste + UMSCHALT+NACH-OBEN	Vergrößern des Fensters bis zum oberen und unteren Rand des Bildschirms
Windows-Logo-Taste + UMSCHALT+NACH-LINKS oder NACH-RECHTS	Verschieben eines Fensters von einem Monitor an einen anderen Monitor
Windows-Logo-Taste + P	Auswählen eines Anzeigemodus für Präsentationen
Windows-Logo-Taste + G	Umschalten zwischen Minianwendungen

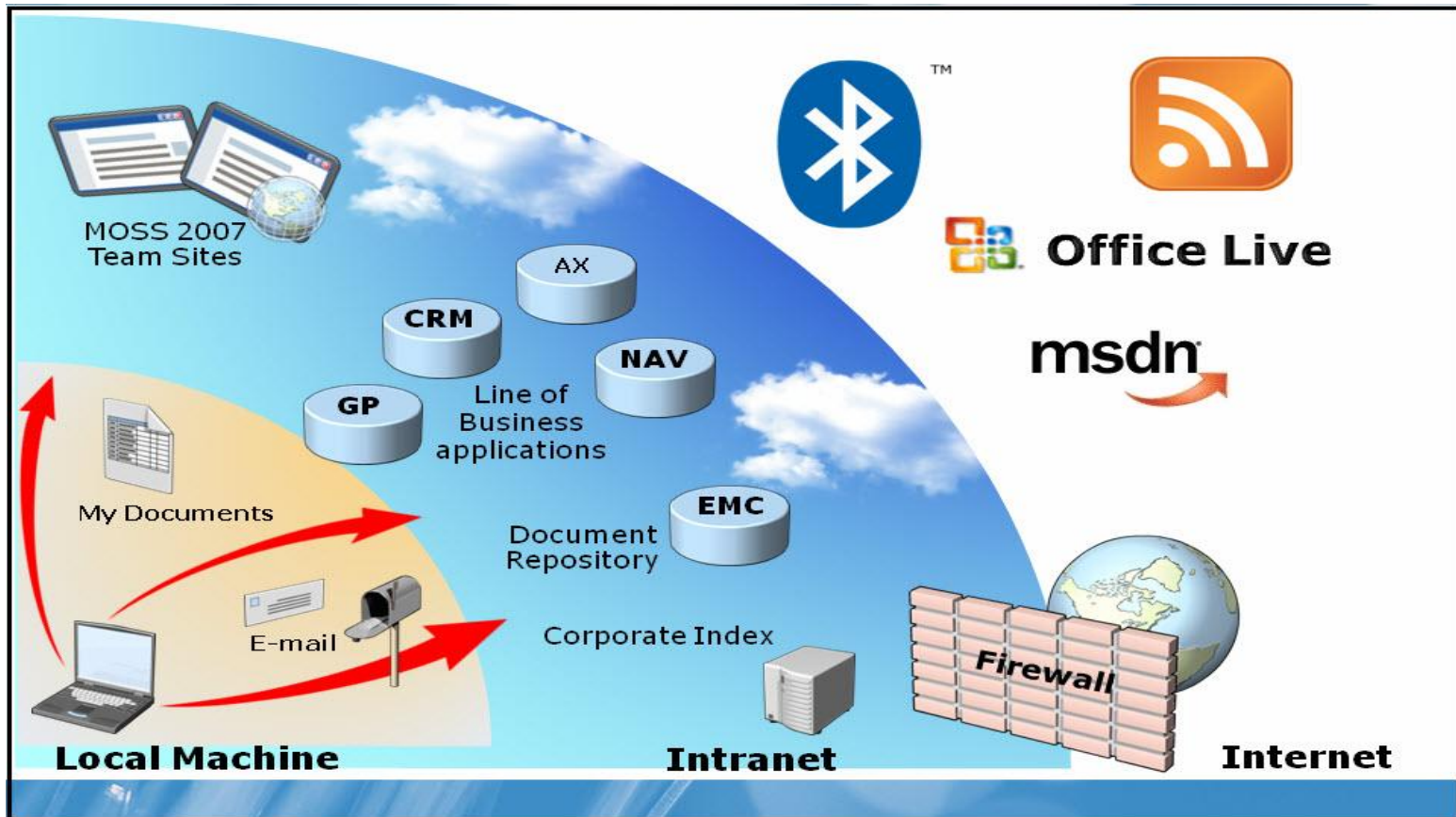


- Mit Bibliotheken können lokale und Netzwerkdateien organisieren und angezeigt werden
- Windows 7 bietet einen Satz an Standard-Bibliotheken an
- Neue Bibliotheken können definiert werden
- Bibliotheken werden automatisch indiziert
- Bibliotheken können für andere Benutzer freigegeben werden





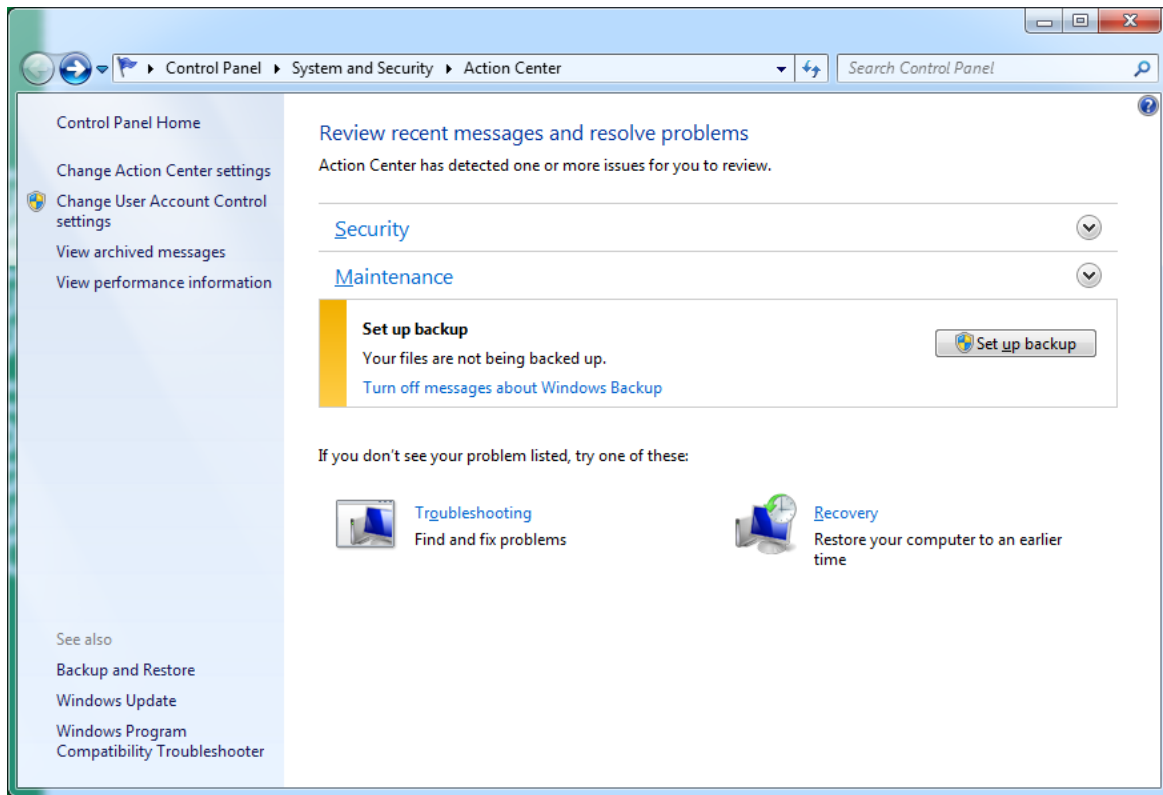
- Eine Suche betrifft alle Daten in bestehenden Bibliotheken
- Die Resultate erscheinen als normale Dateien
- In der Systemsteuerung kann nach Verwaltungsaufgaben gesucht werden
- Während der Eingabe des Suchbegriffs werden bereits Vorschläge angezeigt
- Suchergebnisse in Bibliotheken werden nach Relevanz sortiert
- Die Suche kann über Gruppenrichtlinien gesteuert werden





- Connector installieren
- Connector zu Gruppenrichtlinie hinzufügen

- Zentrales Tool für alle Hinweise an den Benutzer:
 - Sicherheitsupdates
 - Backups
 - Problemreporting
 - Lösungshinweise
 - Troubleshooting
 - Recovery



Gruppenrichtlinien
Device Management and Installation
Problem Steps Recorder
Troubleshooting
Location aware Printing

MANAGEMENT



- Powershell-Support
- Gruppenrichtlinienerweiterungen (Preferences)
 - Power Plan (Windows Vista and later) preference items
 - Scheduled Task (Windows Vista and later) preference items
 - Immediate Task (Windows Vista and later) preference items
 - Internet Explorer 8 preference items



- >3'000 Gruppenrichtlinien für Windows 7
- Remoteverwaltung mittels RSAT (Remote Server Administration Tool)

- Mit Hilfe von Device Management können die erlaubten, resp. zertifizierten Treiber zentral bereitgestellt werden.
- Windows 7 prüft zuerst Windows Update (WSUS) für aktualisierte Treiber.

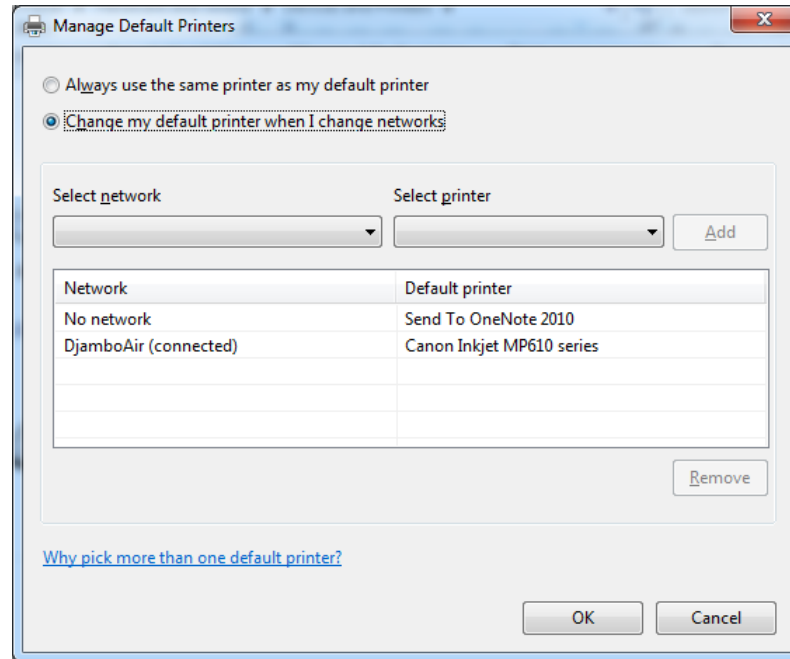
📁 Einschränkungen bei der Geräteinstallation

- ☑️ Prioritize all digitally signed drivers equally during the driver ranking and selection process
- ☑️ Sprechblasen mit der Meldung "Neue Hardware gefunden" während der Geräteinstallation deaktivieren
- ☑️ Do not send a Windows error report when a generic driver is installed on a device
- ☑️ Configure device installation time-out
- ☑️ Prevent Windows from sending an error report when a device driver requests additional software during installati...
- ☑️ Prevent creation of a system restore point during device activity that would normally prompt creation of a restore...
- ☑️ Allow remote access to the Plug and Play interface
- ☑️ Prevent device metadata retrieval from the Internet
- ☑️ Specify search order for device driver source locations

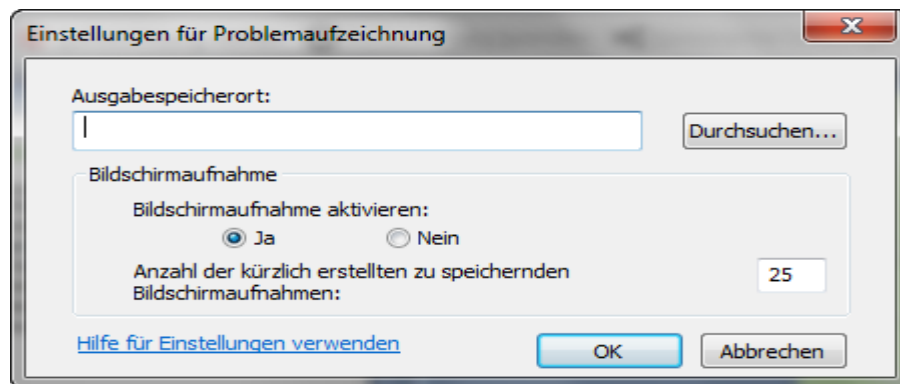
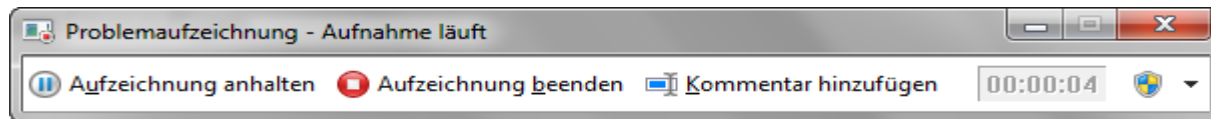
Einstellung

- ☑️ Administratoren das Außerkraftsetzen der Richtlinien unter "Einschränkungen bei der Geräteinstallation" erlauben
- ☑️ Installation von Geräten mit Treibern zulassen, die diesen Gerätesetupklassen entsprechen
- ☑️ Installation von Geräten mit Treibern verhindern, die diesen Gerätesetupklassen entsprechen
- ☑️ Display a custom message when installation is prevented by a policy setting
- ☑️ Display a custom message title when device installation is prevented by a policy setting
- ☑️ Installation von Geräten mit diesen Geräte-IDs zulassen
- ☑️ Installation von Geräten mit diesen Geräte-IDs verhindern
- ☑️ Time (in seconds) to force reboot when required for policy changes to take effect
- ☑️ Installation von Wechselgeräten verhindern
- ☑️ Installation von Geräten verhindern, die nicht in anderen Richtlinien beschrieben sind

- Für jedes Netzwerk kann neu ein Standarddrucker festgelegt werden



- Probleme aufzeichnen



- Ereignisanzeige
- NetMon 3.2
- Leistungsüberwachung
- Ressourcenmonitor
- Speicherdiagnose
- Troubleshooting

Windows Biometric Framework

User Account Control

BitLocker/-ToGo

ActiveX Installer

SECURITY



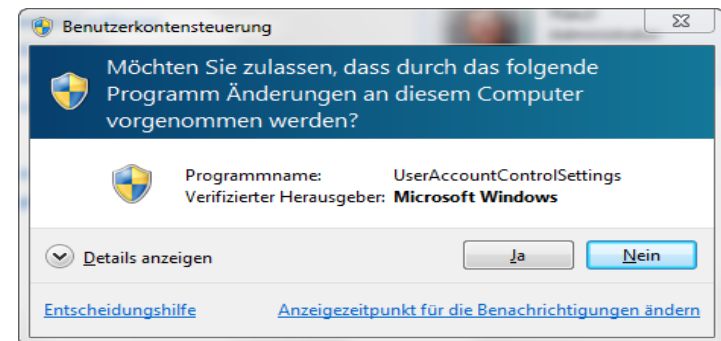
- Standardunterstützung für Biometrische Devices
- Biometric Devices Applet in der Systemsteuerung
- Device Manager Unterstützung
- Neue Group Policy Einstellungen
- Entsprechende Treiber via Windows Update verfügbar

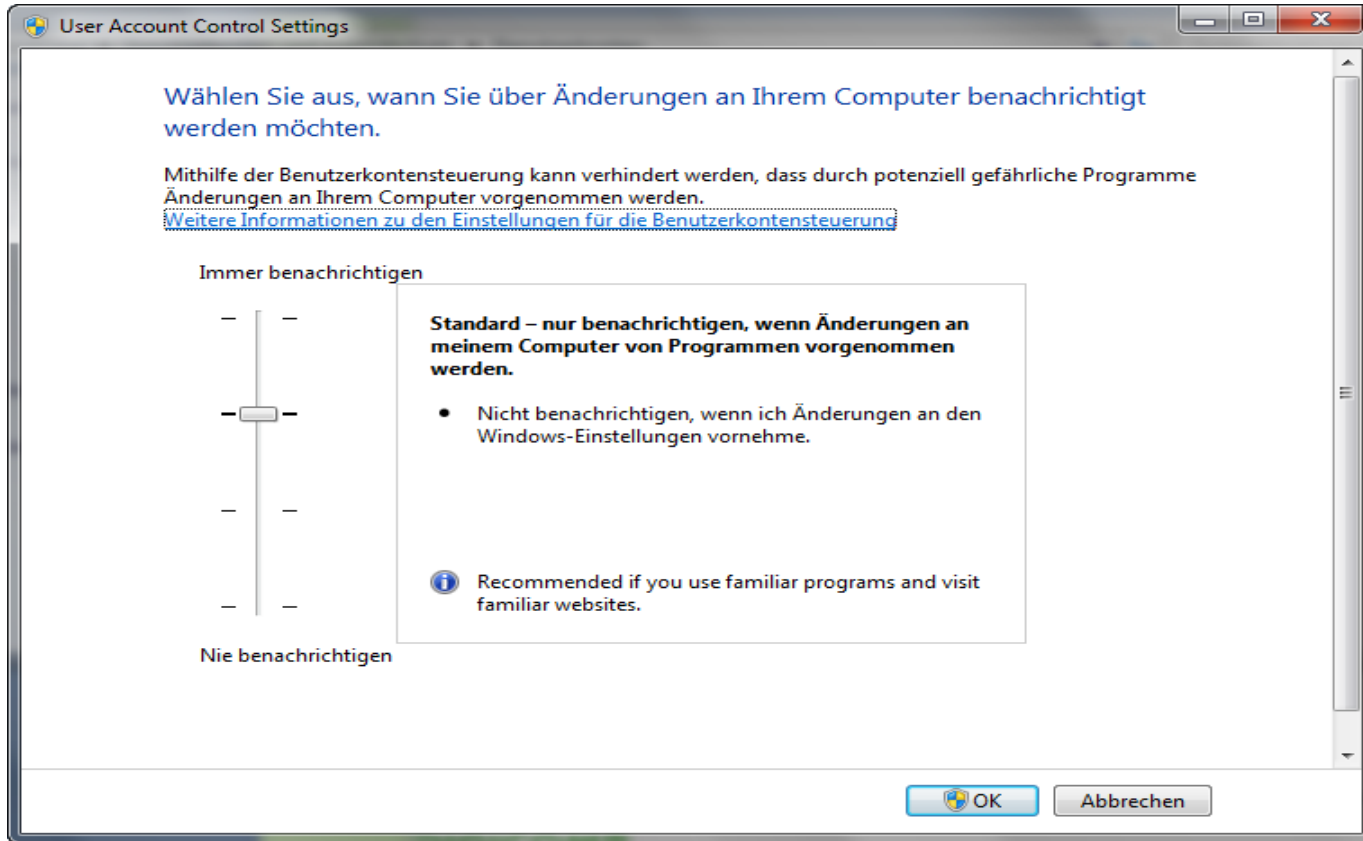


- Alle Benutzer arbeiten mit Standard-Benutzerberechtigungen
- Malware kann sich nicht lautlos installieren
- Installationen müssen explizit bestätigt werden

Standard Users	Administrators
Establish a Local Area Network connection	Install and uninstall applications
Establish and configure a wireless connection	Install a driver for a device, such as a digital camera driver
Modify Display Settings	Install Windows updates
Users cannot defragment the hard drive, but a service does this on their behalf	Configure Parental Controls
Play CD/DVD media (configurable with Group Policy)	Install an ActiveX control
Burn CD/DVD media (configurable with Group Policy)	Open the Windows Firewall Control Panel
Change the desktop background for the current user	Change a user's account type
Open the Date and Time Control Panel and change the time zone	Modify UAC settings in the Security Policy Editor snap-in (secpol.msc)
Use Remote Desktop to connect to another computer	Configure Remote Desktop access
Change user's own account password	Add or remove a user account
Configure battery power options	Copy or move files into the Program Files or Windows directory
Configure Accessibility options	Schedule Automated Tasks
Restore user's backed-up files	Restore system backed-up files
Set-up computer synchronization with a mobile device (smart phone, laptop, or PDA)	Configure Automatic Updates
Connect and configure a Bluetooth device	Browse to another user's directory

- Verbesserte Feineinstellungen
 - Vermeidung zu vieler Bestätigungsauf-forderungen
 - **Standardbenutzer** müssen Anmeldeinformationen eingeben, damit administrative Aufgaben ausgeführt werden können
 - **Administratoren** müssen die Aufforderung lediglich bestätigen

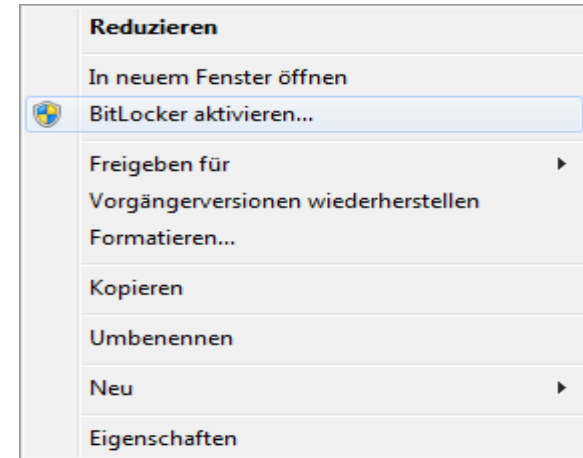






- Verschlüsselt das gesamte Betriebssystem
- Bietet Offline-Datensicherheit
- Schützt alle Anwendungen
- Überprüfung der Systemintegrität
- Überprüfung der Boot-Integrität zum frühest möglichen Zeitpunkt
- Sichert die Integrität des Startprozesses

- Rechtsklick auf Laufwerk
- Automatische Erstellung der Zusatzpartition bei Installation von Windows 7
- BitLocker To Go für USB-Flash-Laufwerke
- Data Recovery Agent für alle geschützten Dateien



- Computer mit TPM 1.2 oder besser
- Externes USB-Laufwerk
- TPM-kompatibles BIOS
- Unterstützung der USB-Schnittstelle während des Starts

Einstellung

- 📁 Fixed Data Drives
- 📁 Operating System Drives
- 📁 Removable Data Drives
- 📄 Store BitLocker recovery information in Active Directory Domain Services(Windows Server 2008 and Windows Vista)
- 📄 Choose default folder for recovery password
- 📄 Choose how users can recover BitLocker-protected drives (Windows Server 2008 and Windows Vista)
- 📄 Choose drive encryption method and cipher strength
- 📄 Provide the unique identifiers for your organization
- 📄 Überschreiben des Arbeitsspeichers beim Neustart verhindern
- 📄 Validate smart card certificate usage rule compliance



- Unterstützung von USB-Laufwerken
- Granulare Steuerung über Gruppen-richtlinien
- Benutzer entscheiden über Verschlüsselung externer Laufwerke
- Rechtsklick schaltet Verschlüsselung um
- Zugriff auf verschlüsselte externe Laufwerke über nicht verschlüsselte Computer
- Aufhebung der Verschlüsselung mit:
 - Wiederherstellungskennwort
 - Smart Card oder Auto-Unlock



- Neues Feature von Windows 7
- Exakte Festlegung welche Anwendungen ausgeführt werden dürfen
- Zusätzlicher Gruppenrichtlinien-Mechanismus



- AppLocker ersetzt die früheren Richtlinien zur Softwareeinschränkung
 - SRP wegen Kompatibilitätsgründen vorhanden
- AppLocker-Regeln sind von SRP getrennt
- AppLocker-Regeln haben Priorität vor SRP

Create Executable Rules

Publisher

Before You Begin
Permissions
Conditions
Publisher
Exceptions
Name

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:
C:\Program Files\Microsoft Games\Chess\Chess.exe

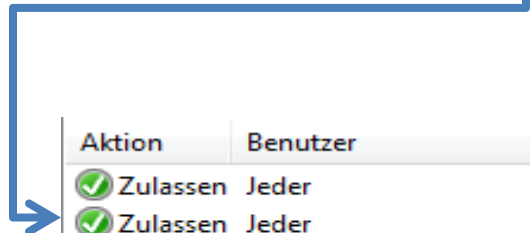
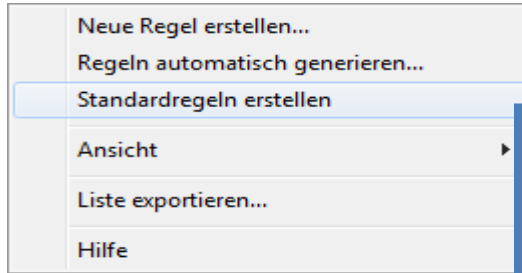
Any publisher
 Publisher: O=MICROSOFT CORPORATION, L=REDMOND, S=\
 Product name: MICROSOFT® WINDOWS® OPERATING SYSTEM
 File name: CHESS.EXE
 File version: * And above

Use custom values
Rule scope:
Applies to all files signed by the specified publisher with this product name and with this file

[More about publisher rules](#)



- Kerndateien des Betriebssystems dürfen immer ausgeführt werden
- Benutzer können keine Programme aus-führen, die in ihrem Profil installiert sind
- Alle Programme im Programmverzeichnis dürfen ausgeführt werden
- Alle Benutzer dürfen signierte Programme ausführen
- Administratoren dürfen alle Programme ausführen



Aktion	Benutzer	Name	Condition
<input checked="" type="checkbox"/> Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner "Programme"	Pfad
<input checked="" type="checkbox"/> Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner "Windows"	Pfad
<input checked="" type="checkbox"/> Zulassen	VORDEFINIERT\Administrators	(Standardregel) Alle Dateien	Pfad



- AppLocker ermöglicht keine explizit autorisierten Programme
- Helpdesk wird anfänglich öfter kontaktiert
- Leichter Rückgang der Leistungsfähigkeit
- Sind nur auf Windows 7 anwendbar
- Regeln in Gruppenrichtlinien haben Vorrang
- Nur-überwachen-Modus wendet Regel nicht an
- Mindestens ein Windows Server 2008 R2 Domänencontroller ist erforderlich



- Unter Windows 7 standardmässig installiert
- Subdomänen in der TrustedSites Liste können mit Wildcards angegeben werden
 - Per-site ActiveX
 - Per-user ActiveX
 - Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service



WINDOWS XP MODE



- Problem: "Alte" Applikationen waren und Vista nicht oder nur mit grossem Aufwand lauffähig
- Lösung: Eine "virtuelle" Umgebung auf Basis von Windows XP
 - Virtual PC
 - Windows XP Mode
 - Shortcuts von Applikationen werden via Integration Feature in den Windows 7 Desktop integriert.



BOOT FROM VHD



- Windows 7 und Windows Server 2008 R2 unterstützen das Booten über eine VHD-Datei
- Ideal für Multiboot-Umgebungen
- Einfachste Sicherung

- Installation starten
- Bei der Auswahl der Installationslaufwerks
Shift+F10 drücken
- Diskpart starten
 - CREATE VDISK FILE=c:\vhd\win7.vhd MAXIMUM=100000
 - SELECT VDISK FILE=c:\vhd\win7.vhd
 - ATTACH DISK

DISM

DEPLOYMENT

MDT 2010

WAIK

MAP 5.0 Beta

ACT 5.5

- Deployment Image Servicing and Management
DISM
 - Management von WIM-Dateien
 - Management von VHD-Dateien

- Change Features
 - Dism /Get-WIMInfo /WimFile:C:\test\images\install.wim
 - Dism /Mount-WIM
/WimFile:C:\wim\Windows7\install.wim
/Name:"Windows 7 HomeBasic" /MountDir:C:\wim
 - Dism /Image:C:\test\offline /Get-Features
 - Dism /Image:C:\test\offline /Enable-Feature
/FeatureName:Hearts
 - Dism /Unmount-WIM /MountDir:C:\test\offline /Commit

- Change Drivers
 - Dism /Get-WimInfo /WimFile:C:\test\images\install.wim
 - Dism /Mount-Wim /WimFile:C:\test\images\install.wim /Name:"Windows 7 HomeBasic" /MountDir:C:\test\offline
 - Dism /Image:C:\test\offline /Add-D
 - Dism /Image:C:\test\offline /Add-Driver /Driver:C:\drivers\mydriver.INF river /Driver:C:\drivers\mydriver.INF
 - Dism /Unmount-Wim /MountDir:C:\test\offline /Commit



oliver.ryf@fonstone.com

FRAGEN?