

## Windows 2000/2003

# Musterlösung 1.1 / 1.5 für schulische Netzwerke

WSUS-Server / Bedienungsanleitung und Hinweise  
09.03.2006



## **Impressum**

### **Herausgeber**

Landesmedienzentrum Baden-Württemberg (LMZ)  
Projekt „Support-Netz“  
Rosensteinstraße 24  
70191 Stuttgart

### **Autoren**

der Zentralen Expertengruppe Netze (ZEN),  
Projekt „Support-Netz“, LMZ  
Martin Resch

### **Endredaktion**

Ulrike Boscher

### **Weitere Informationen**

[www.support-netz.de](http://www.support-netz.de)  
[www.lmz-bw.de](http://www.lmz-bw.de)  
[www.medienoffensive-schule-bw.de](http://www.medienoffensive-schule-bw.de)

Veröffentlicht: **2006**

© Landesmedienzentrum Baden-Württemberg

# Inhaltsverzeichnis

<b>1.</b>	<b>WSUS – Automatische Updateverteilung</b>	<b>2</b>
1.1.	Einführung	2
1.2.	Überblick in Screenshots	3
1.3.	Voraussetzungen	6
1.4.	Installation auf einem Windows 2000-Server	6
1.4.1.	Aktualisieren per Windows-Update	6
1.4.2.	Installation der MSDE	7
1.4.3.	Installation des WSUS	8
1.5.	Installation auf einem Windows 2003-Server	8
1.6.	Serverseitige Konfiguration	8
1.7.	Clientseitige Konfiguration über Gruppenrichtlinien	8
1.7.1.	Eigenschaften automatische Updates	11
1.7.2.	Interner Pfad ... angeben	11
1.7.3.	Clientseitige Zielzuordnung	11
1.7.4.	Zeitplan für geplante Installation neu erstellen	11
1.7.5.	Keinen Neustart für geplante Installationen	12
1.7.6.	Suchhäufigkeit für automatische Updates	12
1.7.7.	Automatische Updates sofort installieren	12
1.7.8.	Erneut zu einem Neustart auffordern	13
1.8.	Updates für die Domänencontroller	13
1.9.	Sonstige Einstellungen	14
1.10.	Ein Blick auf die Reports	14
<b>2.</b>	<b>Der WSUS und die Musterlösung</b>	<b>15</b>
2.1.	Konfiguration des Proxy	15
2.2.	Notwendige Anpassung der Raumkonsole bis Version 1.1	16
<b>3.</b>	<b>Verschiedenes zum WSUS</b>	<b>17</b>
3.1.	Mögliche Probleme und Lösungen	17
3.1.1.	Der Server synchronisiert nicht	17
3.1.2.	Das Synchronisieren funktioniert, aber der Dateidownload nicht	17
3.1.3.	Die Updates kommen nicht bei den Clients an	18
3.1.4.	Weitere Maßnahmen	18
3.2.	Sofortiges Update eines Clients	19
3.3.	Update eines bestehenden SUS-Servers	19
3.4.	Übernahme der Dateien von einem anderen WSUS	20
3.5.	Weiterführende Informationen, Quellenangaben und Links	20
<b>4.</b>	<b>Anhang: Konfiguration bei Verwendung des IIS-Lockdown-Tools</b>	<b>21</b>

# 1. WSUS – Automatische Updateverteilung

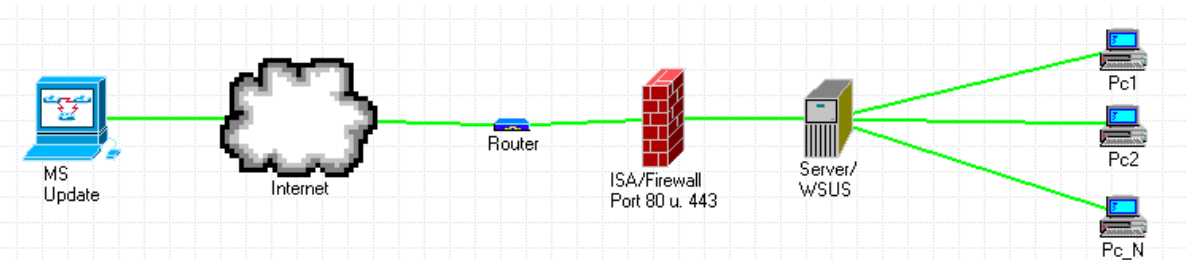
## 1.1. Einführung

Diese Dokumentation liefert Ergänzungen und einen Überblick zu den am Ende des Dokuments genannten Anleitungen. Die Verweise im Text sind in eckigen Klammern angegeben und beziehen sich auf den Anhang (s. Abschnitt 3.5). Die vorliegende Beschreibung kann diese nicht ersetzen, sondern geht vielmehr auf die im Zusammenspiel mit der Musterlösung notwendigen Konfigurationen ein.

Wer ein Windows-Netzwerk betreut, sollte regelmäßig aktuelle Sicherheitsupdates auf allen Rechnern einspielen.

Inzwischen ist davon auszugehen, dass schwere Sicherheitslücken bereits wenige Tage nach ihrer Bekanntgabe entsprechende Schadsoftware nach sich ziehen (vergleiche z.B. <http://www.heise.de/newsticker/meldung/62874>). Auch wenn in der Musterlösung der ISA-Server einen guten Schutz gegen Angriffe aus dem Internet bietet, sollte man sich keinesfalls ausschließlich darauf verlassen, denn Würmer können auch über Notebooks in das lokale Netz eingeschleust werden.

Bei der anfallenden Menge von Sicherheitsupdates ist es ohne ein geeignetes Hilfsmittel sehr aufwändig, diese Updates zu verteilen. Seit Windows XP und Windows 2000 ab SP3 gibt es den Dienst **Automatische Updates**, der automatisch auf Microsoft Internetservern nach neuen Updates sucht, und diese anschließend auf Wunsch installiert. In lokalen Netzen ist diese Lösung aber weniger geeignet, da jeder Rechner sich die Updates über das Internet holt. Besser wäre es, wenn nur *ein* Rechner die Updates von den Microsoft Internetservern herunterlädt und anschließend diese den anderen Rechnern im LAN zur Verfügung stellt.



Für diese Problematik bot Microsoft seit einiger Zeit den kostenlosen Dienst **Software Update Service (SUS)** an, mit dem ein lokaler Server zum Update-Server umfunktioniert werden kann. Der **Windows Server Update Services (WSUS)** ist der Nachfolger von SUS. Er arbeitet datenbankbasiert und bietet deutlich erweiterte Funktionalitäten/Konfigurationsmöglichkeiten und Updates zu anderen Microsoft-Produkten.

Der WSUS-Server kann folgende Updates bereitstellen:

- Service Packs und Service Rollups
- Sicherheitsupdates für die Betriebssysteme Windows 2000, Windows XP und Windows 2003
- Sicherheitsupdates für systemnahe Software, z.B. für den Internet-Explorer
- Sicherheitsupdates zu MS-Office und Visio
- Sicherheitsupdates zu MS-Exchange

Weitere Microsoftprodukte (z.B. MS-ISA-Server) sollen in naher Zukunft eingebunden werden.

**Wichtiger Hinweis:** Der IE6 wird auf Windows-2000-Maschinen *nicht* verteilt, das müssen Sie weiterhin über Gruppenrichtlinien vornehmen (S. z.B. [5]).

Der Administrator kann jederzeit frei entscheiden, welche Updates heruntergeladen werden sollen und welche davon wiederum auf den Computern installiert werden. Es lassen sich sogar Computergruppen mit unterschiedlichem Updateverhalten konfigurieren, so dass ein Testen der Updates möglich wird. Sämtliche Konfiguration erfolgt über eine Webschnittstelle, kann also per IE von jedem Client im Netz aus vorgenommen werden.

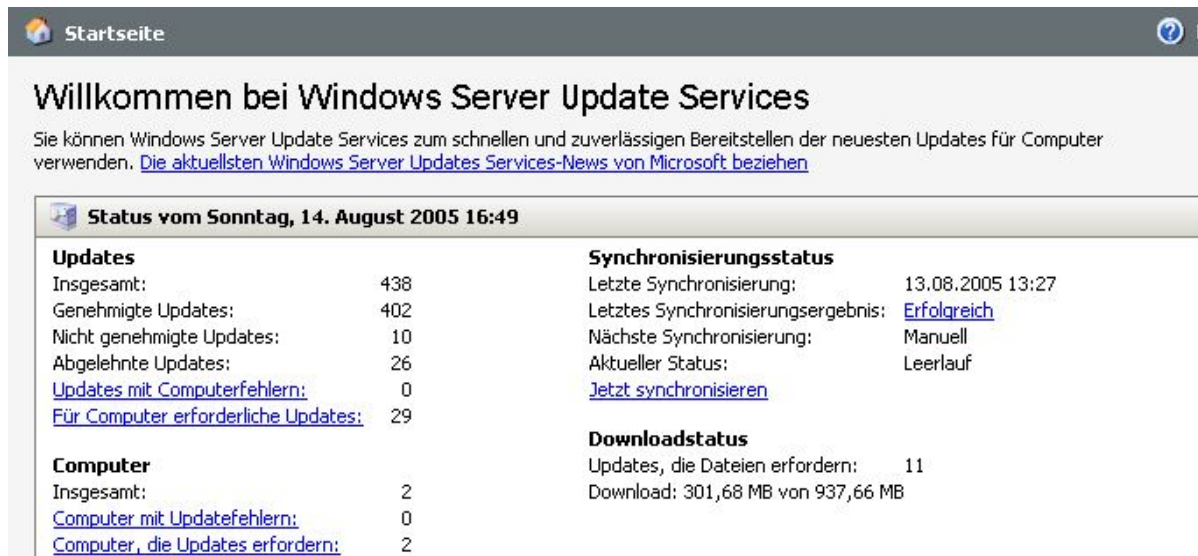
## 1.2.

### Überblick in Screenshots

Einen guten Eindruck zur Funktionsvielfalt des WSUS kann man sich durch die folgenden kommentierten Screenshots verschaffen.



Der WSUS ist auf Deutsch verfügbar. Über eine Menüleiste im Browser kann direkt auf die wichtigsten Funktionen zugegriffen werden.



**Startseite**

## Willkommen bei Windows Server Update Services

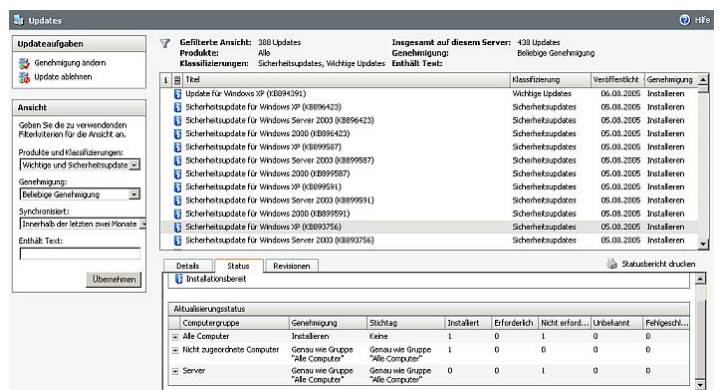
Sie können Windows Server Update Services zum schnellen und zuverlässigen Bereitstellen der neuesten Updates für Computer verwenden. [Die aktuellsten Windows Server Updates Services-News von Microsoft beziehen](#)

**Status vom Sonntag, 14. August 2005 16:49**

Updates		Synchronisierungsstatus	
Insgesamt:	438	Letzte Synchronisierung:	13.08.2005 13:27
Genehmigte Updates:	402	Letztes Synchronisierungsergebnis:	<a href="#">Erfolgreich</a>
Nicht genehmigte Updates:	10	Nächste Synchronisierung:	Manuell
Abgelehnte Updates:	26	Aktueller Status:	Leerlauf
<a href="#">Updates mit Computerfehlern:</a>	0	<a href="#">Jetzt synchronisieren</a>	
<a href="#">Für Computer erforderliche Updates:</a>	29		
Computer		Downloadstatus	
Insgesamt:	2	Updates, die Dateien erfordern:	11
<a href="#">Computer mit Updatefehlern:</a>	0	Download:	301,68 MB von 937,66 MB
<a href="#">Computer, die Updates erfordern:</a>	2		

Die Startseite liefert die wichtigsten Informationen über verfügbare Updates, deren Genehmigungszustand und Downloadstatus, aber auch Informationen über die lokalen Clients.

Unter *Updates* wird eine Liste sämtlicher bekannter Updates dargestellt. Zu jedem Patch kann man weitergehende Informationen abrufen, feststellen auf welchem Client dieses Update installiert wurde oder noch installiert werden soll oder die Verteilung des Updates für alle oder auch nur für bestimmte Computer anstoßen.



The screenshot shows the WSUS Updates console. On the left, there are navigation options like 'Updateaufgaben', 'Anzeige', and 'Synchronisiert'. The main area displays a list of updates with columns for 'Titel', 'Klassifizierung', 'Veröffentlicht', and 'Genehmigung'. Below the list, there is a 'Details' tab showing the 'Aktualisierungszustand' for different computer groups.

Computergruppe	Genehmigung	Stichtag	Installiert	Erforderlich	Nicht erforderl...	Unbekannt	Fehlgeschl...
Alle Computer	Installieren	Keine	1	0	1	0	0
Nicht zugeordnete Computer	Genau wie Gruppe 'Alle Computer'	Genau wie Gruppe 'Alle Computer'	1	0	0	0	0
Server	Genau wie Gruppe 'Alle Computer'	Genau wie Gruppe 'Alle Computer'	0	0	1	0	0

Details	Status	Statusbericht drucken	
<a href="#">Sicherheitupdate für Windows XP (KB890077)</a>	Installieren	<a href="#">Anforderungen</a>	<a href="#">Anforderungen</a>
<a href="#">Sicherheitupdate für Windows XP (KB891781)</a>	Installieren	<a href="#">Erforderlich</a>	<a href="#">Erforderlich</a>
<a href="#">Sicherheitupdate für Windows XP (KB893086)</a>	Installieren	<a href="#">Erforderlich</a>	<a href="#">Erforderlich</a>
<a href="#">Update für Windows XP (KB887742)</a>	Installieren	<a href="#">Erforderlich</a>	<a href="#">Erforderlich</a>
<a href="#">Wichtiges Update für Windows XP (KB886185)</a>	Installieren	<a href="#">Erforderlich</a>	<a href="#">Erforderlich</a>
<a href="#">Kumulatives Sicherheitupdate für Internet Explorer unter Windows XP (KB896727)</a>	Installieren	<a href="#">Neustart erforderlich</a>	<a href="#">Neustart erforderlich</a>
<a href="#">Sicherheitupdate für Windows XP (KB885835)</a>	Installieren	<a href="#">Neustart erforderlich</a>	<a href="#">Neustart erforderlich</a>
<a href="#">Sicherheitupdate für Windows XP (KB890046)</a>	Installieren	<a href="#">Neustart erforderlich</a>	<a href="#">Neustart erforderlich</a>
<a href="#">Sicherheitupdate für Windows XP (KB890859)</a>	Installieren	<a href="#">Neustart erforderlich</a>	<a href="#">Neustart erforderlich</a>

Umgekehrt kann man auch bei den Clients zu jedem einzelnen Rechner, der für den WSUS konfiguriert ist, den Patch-Stand abrufen. Dabei werden sowohl der Soll- als auch der Ist-Zustand angezeigt. Es kann allerdings eine Weile dauern, bis diese Informationen aktuell sind.

In dieser Gruppe enthaltene Computer: 2      Von diesem Server verwaltete Computer: 2  
**Computergruppe:** Alle Computer

Computername	Betriebssystem	Letzter Statusbericht	Computergruppe
pc1.schule.local	Windows XP	11.08.2005 17:28	Nicht zugeordnete Computer
31.schule.local	Windows Server 2003	14.08.2005 16:47	Server

Über das Datum des Statusberichts lassen sich Rückschlüsse ziehen, wenn der PC das letzte Mal (innerhalb des Netzes) im Betrieb war. So können auch insbesondere Laptops gezielt zum Betanken mit Updates (und dann auch am besten Antiviren-Softwareupdates) ins Netz gestellt werden.

Die Computer lassen sich gruppieren, ihnen kann man dann ein unterschiedliches Updateverhalten, (zusätzlich zu den Vorgaben über Gruppenrichtlinien) vorgeben.

### Produkte und Klassifizierungen

Sie können die Produkte festlegen, für die Updates gedownloadet werden sollen, und die Updatetypen auswählen.

#### Produkte:

Alle Exchange Produkte  
 Alle Office Produkte  
 Alle SQL Produkte  
 Windows 2000  
 Windows Server 2003  
 Windows XP

Ändern...

#### Updateklassifizierungen:

Definitionsupdates  
 Service Packs  
 Sicherheitsupdates  
 Update-Rollups  
 Updates  
 Wichtige Updates

Ändern...

### Proxyserver

Diese Proxyservereinstellungen gelten nur, wenn dieser Server mit einem Upstreamserver oder Microsoft Update synchronisiert wird.

Proxyserver für die Synchronisierung verwenden

Servername:

Portnummer:

Benutzeranmeldedaten für die Verbindungsherstellung mit dem Proxyserver verwenden

Benutzername:

Domäne:

Kennwort:

Standardauthentifizierung zulassen (Kennwort wird in Klartext gesendet)

Bei den Basiseinstellungen werden das Synchronisationsverhalten und die Proxyeinstellungen festgelegt. Die Pakete werden allerdings erst nach dem Freischalten heruntergeladen.

### Updates

Sie können festlegen, ob und wie die automatische Installation und Ermittlung für Updates genehmigt werden sollen. Die Genehmigung erfolgt, wenn ein Update oder dessen Metadaten auf den Windows Server Update Services-Server gedownloadet werden.  
 Hinweis: Die Installationsregel wird verwendet, falls die Installations- und Ermittlungsregeln in Konflikt stehen.

**Für die Ermittlung genehmigt**

Das Ermitteln von Updates unter Anwendung folgender Regel automatisch genehmigen:  
**Klassifizierungen:** Sicherheitsupdates, Wichtige Updates Klassifizierungen hinzufügen/entfernen...  
**Computergruppen:** Alle Computer Computergruppen hinzufügen/entfernen...

**Zum Installieren genehmigen**

Updates für die Installation unter Anwendung folgender Regel automatisch genehmigen:  
**Klassifizierungen:** Sicherheitsupdates, Wichtige Updates Klassifizierungen hinzufügen/entfernen...  
**Computergruppen:** Alle Computer Computergruppen hinzufügen/entfernen...

Auch ein automatisches Freigeben lässt sich konfigurieren. Dabei kann nach Klassifizierungen der Updates differenziert werden.

Insgesamt erscheint der WSUS als deutlich ausgereifteres Produkt als der SUS. Er liefert dem Administrator viele sicherheitsrelevante Informationen und erleichtert die Arbeitsstationen auf dem aktuellen Stand zu halten deutlich.

### 1.3. Voraussetzungen

#### Server:

- Windows 2003 (empfohlen) oder Windows 2000 Server ab SP4
- IIS ab 5.0
- IE6
- BITS 2.0
- MS-SQL-Server bzw. (W)MSDE

#### Hardwareempfehlung bei ca. 500 Clients:

- 2 GHz Taktfrequenz, mindestens 1GB RAM
- 2 GB auf der Systempartition, weitere 10 GB auf einer weiteren Partition (empfohlen sind 30 GB)

#### Clients:

- Windows 2000 mit SP3, Windows XP mit SP 1 oder Windows 2003
- Automatisches Update aktiviert und über Gruppenrichtlinien konfiguriert

Weitere Informationen finden Sie unter [2].

### 1.4. Installation auf einem Windows 2000-Server

Die folgenden Informationen sind eine kommentierte Zusammenfassung von [3].

Folgende Voraussetzungen sollten in der Musterlösung 1.1 bereits erfüllt sein:

- Installiertes SP4 auf dem Server
- IE 6 SP1
- IIS 5

Bevor die Installation des WSUS beginnen kann, benötigen Sie weitere Software, die im Gegensatz zum WSUS auf Windows 2003 per Hand installiert werden muss (vgl. [3, S. 8f]).

#### 1.4.1. Aktualisieren per Windows-Update

Bringen Sie zunächst das Serverbetriebssystem per Windows-Update auf den neuesten Stand. Achten Sie darauf, dass unbedingt die erforderlichen Komponenten BITS2.0 und .Net Framework1.1 SP1 enthalten sind oder laden Sie dieses über das Microsoft Download Center. Nur per Windows-Update erhalten Sie dann garantiert die aktuellen Komponenten.



Der Updatevorgang kann einige Zeit dauern und mehrere Neustarts, sowie mehrmaliges Aufrufen der Windows-Update-Seite (-bei Net Framework 1.1 wird das SP1 erst nach Installation von Framework 1.1 angezeigt-) erfordern. Die Aktualisierung ist deshalb nach Möglichkeit außerhalb der Unterrichtszeit auszuführen.

#### 1.4.2.

#### Installation der MSDE

Bei der Musterlösung Windows 2000 ist standardmäßig kein SQL-Server vorhanden (der eigene Lizenzen benötigen würde). Microsoft bietet daher als kostenlose Alternative die Datenbank MSDE an.

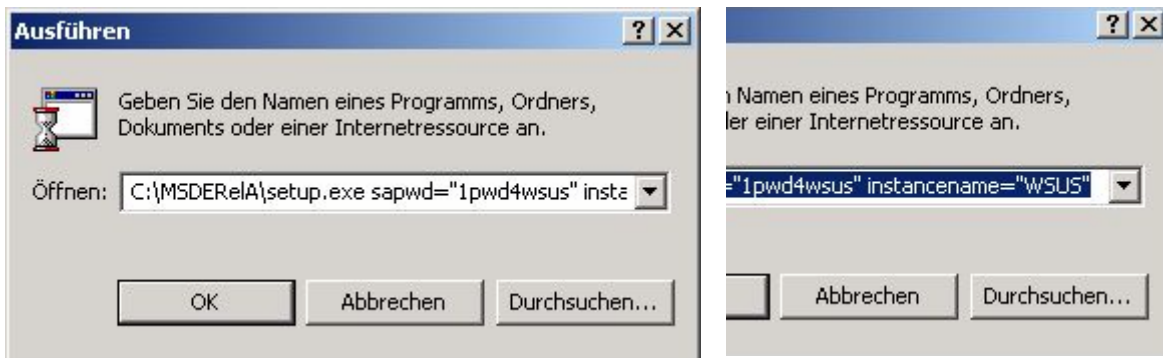
Sie können diese als deutsche Version unter

<http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=413744D1-A0BC-479F-BAFA-E4B278EB9147> herunterladen ([GER\\_MSDE2000A.exe](#), ca. 45 MB).

Weitere Details zur Installation der MSDE finden Sie unter [3, S. 10ff.] und [1, S. 93ff].

Bestätigen Sie zunächst den Installationsordner (es handelt sich nur um den Ort, an den die gepackten Dateien entpackt werden).

**Wichtig:** Sie müssen nun das Setup-Programm aus diesem Ordner mit Optionen starten, um ein sicheres Passwort und den Namen der Instanz festzulegen. Einfaches Doppelklicken ist nicht möglich!



Hier heißt das Passwort „1pwd4wsus“. Wählen Sie hierfür unbedingt ein sehr sicheres Passwort mit mehr als zehn Zeichen. Anschließend ist ein Server-Neustart notwendig.

**Hinweis:** Nachdem Sie den Server durchgestartet haben, erscheint die Meldung, dass ein Dienst nicht gestartet wurde. Es handelt sich um den Dienst MSSQL\$WSUS. Dieser kann manuell oder durch einen erneuten Neustart gestartet werden. Es sollten aber danach keine weiteren Dienstfehler mehr auftreten.

Beachten Sie unbedingt die in der Anleitung von Microsoft gemachten Hinweise zur Installation des SQL-Hotfixes und des IIS-Lockdown-Tools. SQL-Server ohne aktuellen Patchstand sind ein beliebtes Einfalltor für Angriffe. Schüler könnten auf diese Weise Administratorenrechte erlangen!

Die Konfiguration des Lockdown-Tools im Kontext der Musterlösung entnehmen Sie bitte dem Anhang, Kapitel 4.

### 1.4.3.

## Installation des WSUS

Starten Sie anschließend die Installation des WSUS. Sie können jeweils die Standardvorgaben übernehmen.

### 1.5.

## Installation auf einem Windows 2003-Server

Es ist deutlich erkennbar, dass bei der Entwicklung von WSUS in erster Linie an eine Installation auf einem Windows 2003-Server gedacht wurde. In diesem Fall ist nämlich die erforderliche Datenbank WMSDE (die auf Windows 2000 nicht einsetzbar ist) bereits im Setup des WSUS enthalten.

Eine ausführliche, deutschsprachige Anleitung finden Sie unter [4, S. 10ff]. Sie sollten jeweils die Standardeinstellungen übernehmen. Eine gute Installationsanleitung gibt es auch unter [11, Installation].

### 1.6.

## Serverseitige Konfiguration

Die Webseite zur Konfiguration rufen Sie über **http://[IhrServer]/wsusadmin** von einem beliebigen Rechner im Netz aus auf.

Konfigurieren Sie zunächst den Proxy (s. Abschnitt 2.1). Sollten Sie ohne Proxy arbeiten wollen, müssen Sie beim ISA eine entsprechende anonyme Zugriffsregel anlegen, das ist aber komplizierter (vgl. [4, S. 16] und <http://www.msisafaq.de/Anleitungen/2000/Client/WUV52k.htm>).

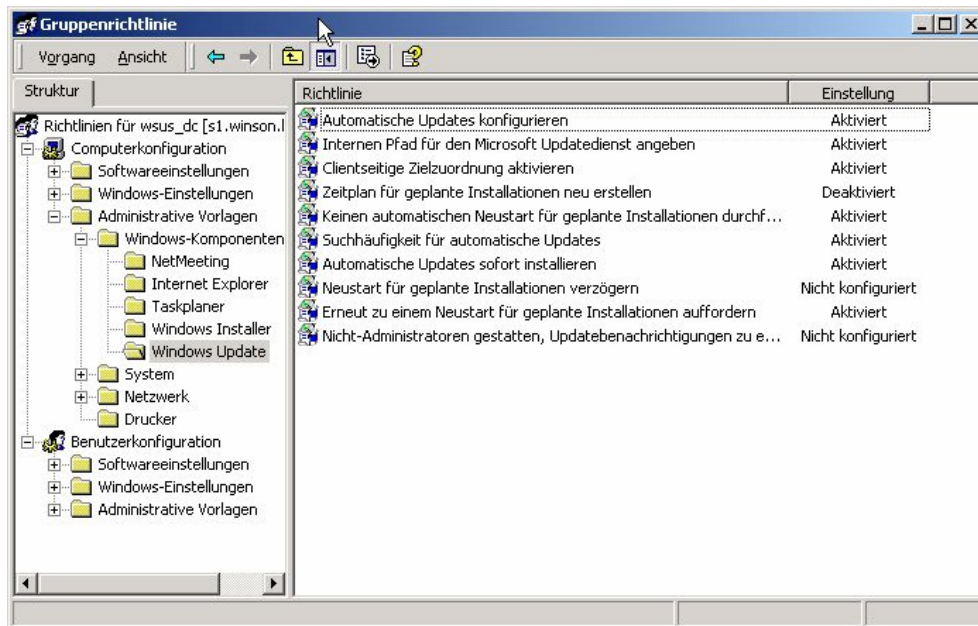
Anschließend können Sie den WSUS manuell synchronisieren (s. [4, S. 18]). Dieser Vorgang kann über eine Stunde und mehr in Anspruch nehmen, da jetzt die Updatedatenbank aufgebaut wird. Ein Herunterladen von Dateien findet noch nicht statt.

### 1.7.

## Clientseitige Konfiguration über Gruppenrichtlinien

Damit die Clients in Zukunft ihre Updates auf dem lokalen WSUS abholen können, müssen sie entsprechend konfiguriert werden (Eintrag des Servers, automatisches Update...). Diese Einstellungen werden in der Registry gespeichert und lassen sich am bequemsten über Gruppenrichtlinien verteilen.

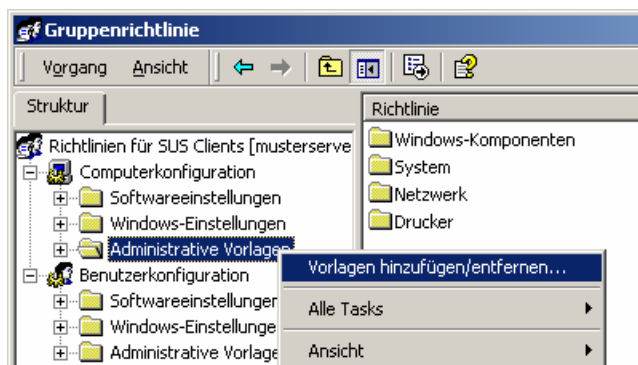
Ein konkretes Konfigurationsbeispiel finden Sie im Folgenden abgebildet. Die angezeigten Einstellungen sind im Beispiel zwar für die OU der Domänencontroller abgebildet, die Beschreibung im Text steht aber für Clients.



Für die Konfiguration erstellen Sie eine neue Gruppenrichtlinie mit der Bezeichnung *Musterlösung\_WSUSClient*, die den Workstations zugeordnet wird. In den *Administrativen Vorlagen* für Computer gibt es einen Abschnitt *Windows-Komponenten* mit dem Unterabschnitt *Windows Update*. Wie abgebildet sind nur einige der möglichen Einstellungen zu konfigurieren („Aktiviert“).

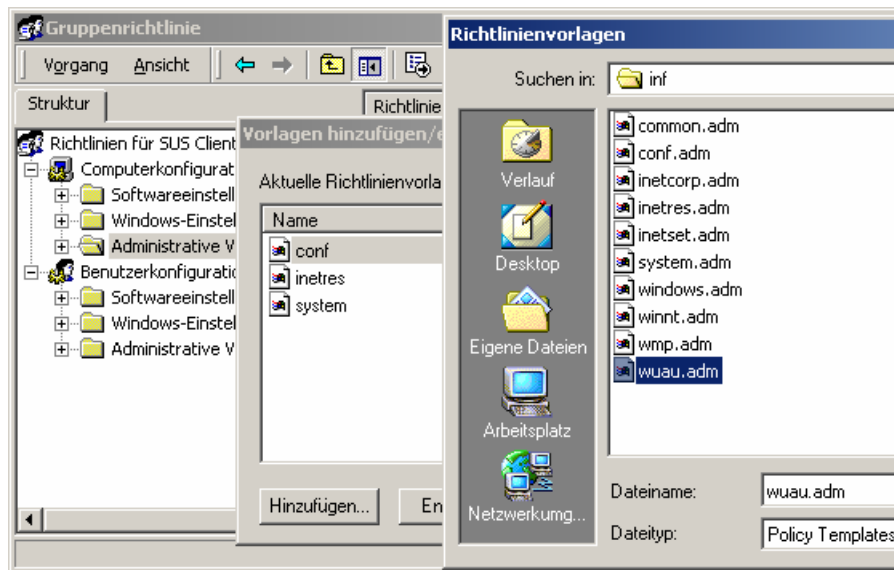
Wahrscheinlich müssen Sie vor der Konfiguration der Einstellung erst die aktuelle Windows-Update-ADM-Datei importieren. Diese wird zwar automatisch bei der Konfiguration als C:\WINNT\inf\wuau.adm zur Verfügung gestellt, muss aber erst in die Gruppenrichtlinie eingebunden werden.<sup>1</sup>

1. Klicken Sie in der Struktur mit der rechten Maustaste auf *Computerkonfiguration | Administrative Vorlagen* und wählen Sie im Kontextmenü *Vorlagen hinzufügen/entfernen...* aus.



<sup>1</sup> Fehlt die Datei, so können Sie sie auf einem CAB-Archiv auf dem Server extrahieren. Microsoft schreibt dazu: "Nach der WSUS-Installation ist im Verzeichnis c:\Programme\Update\Services\Selfupdate\au\{x86}\xp die Datei wucltui.cab in verschiedenen Sprachordnern. In der wucltui.cab befindet sich die aktuellste wuau.adm mit den neusten WSUS-Optionen."

2. Klicken Sie auf *Hinzufügen...* und wählen Sie die *wuau.adm* aus.



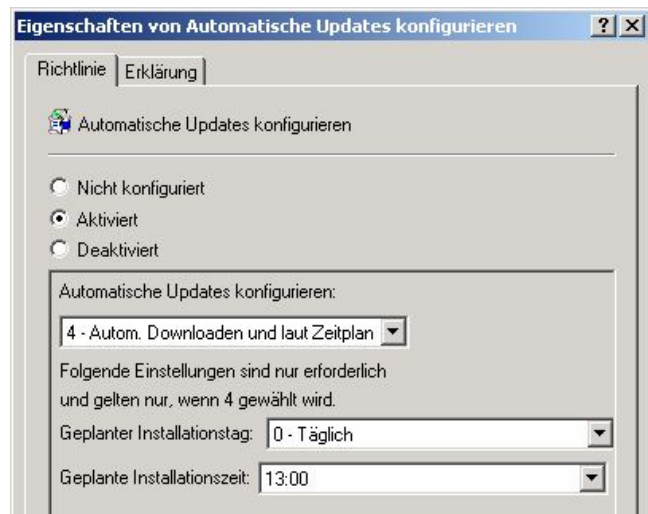
Sollten Sie gefragt werden, ob eine bereits vorhandene Datei überschrieben werden soll, können Sie mit *Ja* bestätigen.

3. Sie sehen nun unter *Computerkonfiguration | Administrative Vorlagen | Windows-Komponenten* einen neuen Eintrag *Windows Update*. Wählen Sie diesen aus. Auf der rechten Seite stehen die auf der vorigen Seite abgebildeten zehn Punkte zur Konfiguration des Updateverhaltens zur Verfügung.

## 1.7.1.

## Eigenschaften automatische Updates

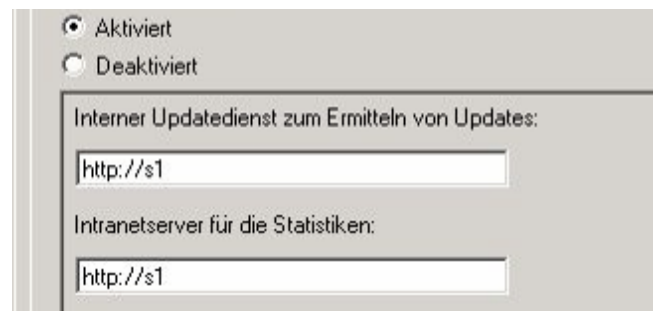
Hier legen Sie die Grundeinstellungen wie abgebildet fest. Updates werden automatisch vom WSUS geladen und hier ab ca. 13 h, also in der Mittagspause, installiert. Sie sollten hier eine Zeit wählen, zu der Ihre Clients zwar eingeschaltet sind, aber nicht zu Unterrichtszwecken genutzt werden.



## 1.7.2.

## Interner Pfad ... angeben

Diese Einstellung müssen Sie aktivieren und zweimal den Pfad zu Ihrem WSUS angeben (s. Abbildung).



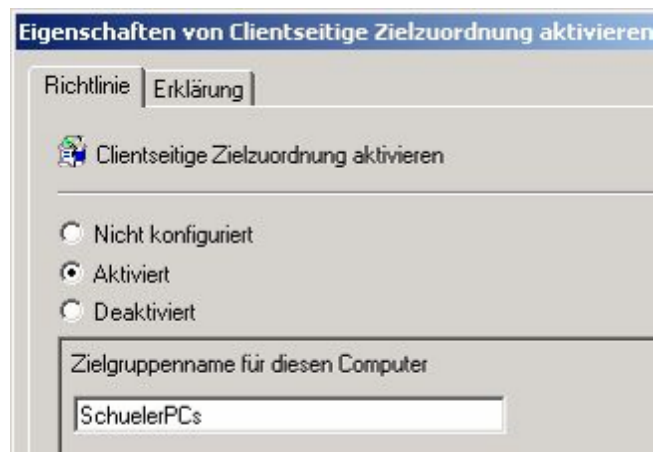
## 1.7.3.

## Clientseitige Zielzuordnung

Diese Konfiguration müssen Sie zunächst *nicht* vornehmen. Über diese Einstellung ist es später möglich, die Workstations automatisch zu Gruppen einzuordnen. Genaueres dazu entnehmen Sie bitte der Erklärung zu dieser Richtlinie.

**Hinweis:** Diese Regel funktioniert nur, wenn auf dem WSUS-Server unter *Optionen / Computeroptionen* die Option

„Gruppenrichtlinien- oder Registrierungseinstellungen auf den Computern verwenden“ aktiviert wurde.



## 1.7.4.

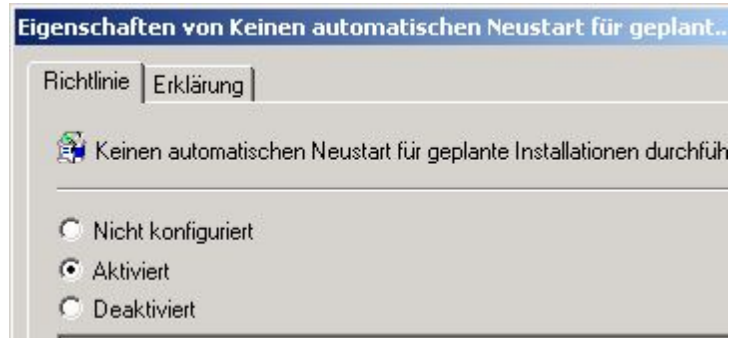
## Zeitplan für geplante Installation neu erstellen

Diese Richtlinie greift, wenn der unter 1.7.1 genannte Zeitpunkt „verpasst“ wurde, weil der Computer ausgeschaltet war. Es gibt hier die Möglichkeit, die Updates eine Minute nach dem Hochfahren vorzunehmen

(„Nicht konfiguriert“), selbst eine Zeitspanne einzutragen („Aktiviert“) oder zu warten, bis der oben angegebene Zeitpunkt das nächste Mal erreicht wird („Deaktiviert“). Haben Sie unter 1.7.1 eine Zeit in der Nacht angegeben, so dürfen Sie hier sinnvollerweise nur dann „Deaktiviert“ vorgeben, wenn Sie den Rechner geplant über Nacht laufen lassen wollen.

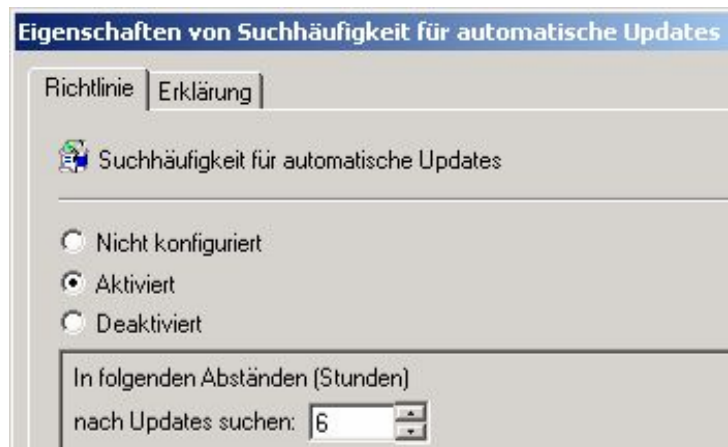
#### 1.7.5. Keinen Neustart für geplante Installationen

Will man erzwungene Neustarts verhindern, kann man die Richtlinie aktivieren. Das Update wird dann eben beim planmäßigen Abschalten zu Ende geführt.



#### 1.7.6. Suchhäufigkeit für automatische Updates

Hier wird eingestellt, in welchen Zeitabständen ein Client (in etwa) nach neuen Updates auf dem WSUS schaut. Der Defaultwert von 22 Stunden kann auch belassen werden.



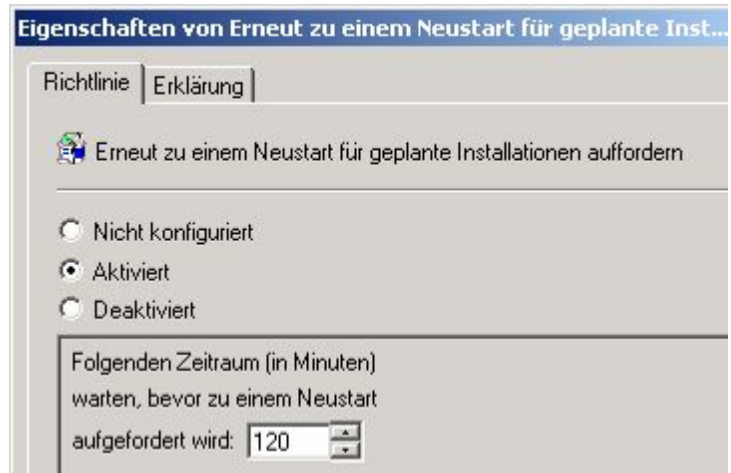
#### 1.7.7. Automatische Updates sofort installieren

Gemäß der Erklärung sind hiervon nur Updates betroffen, die weder den PC noch den Systemdienst neu starten. Es wird empfohlen, die Richtlinie zu aktivieren.

## 1.7.8.

Erneut zu einem Neustart  
auffordern

Fünf Minuten nach Abschluss der Installation (das bestimmt die vorherige Richtlinie, die nicht aktiviert werden muss) fordert der Rechner einen Neustart an. Diese Frage wird standardmäßig alle 10 Minuten wiederholt. Wenn Sie das als störend empfinden, können Sie das Intervall über diese Richtlinie verlängern. Die letzte Richtlinie, Nicht-Administratoren betreffend, bleibt unkonfiguriert.



## 1.8.

## Updates für die Domänencontroller

Auch für den oder die Server sollte man eine entsprechende Gruppenrichtlinie anlegen, so dass diese(r) automatisch upgedatet wird. Hierbei sind folgende Überlegungen sinnvoll:

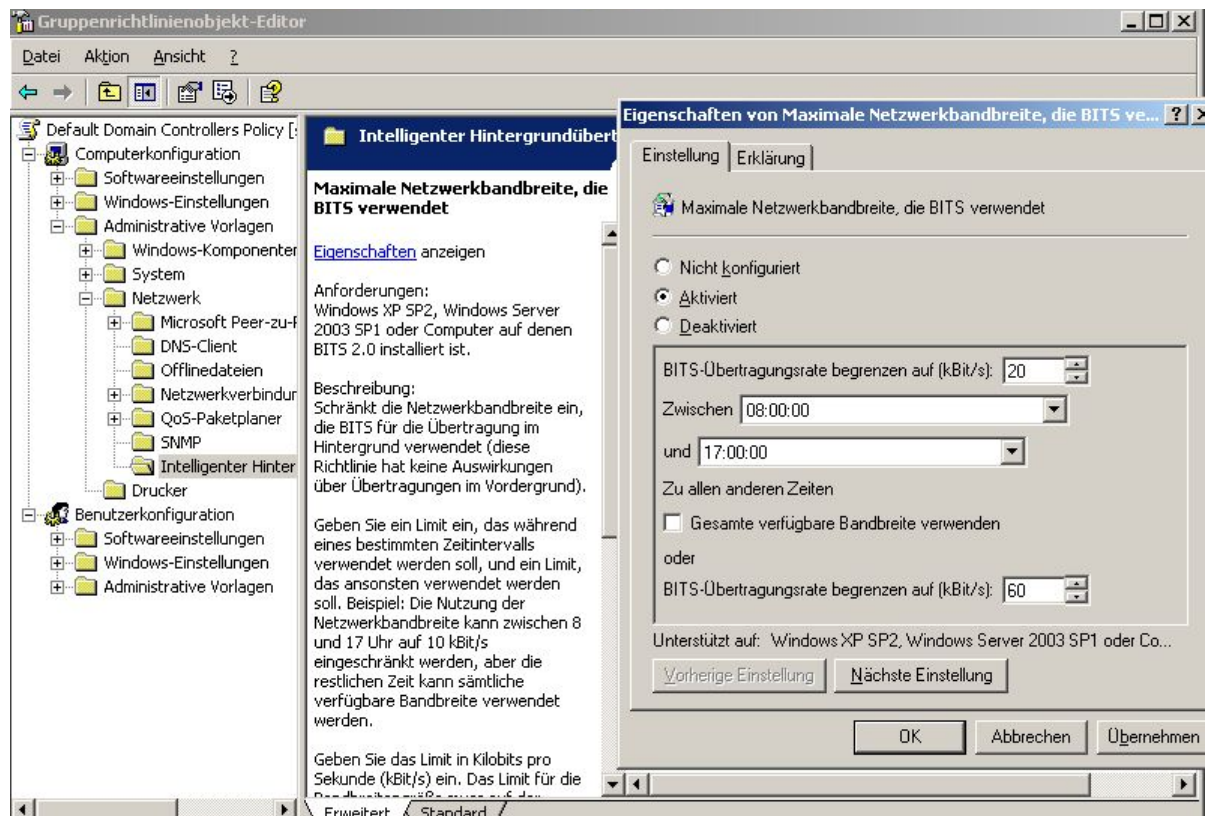
- Der Server läuft rund um die Uhr. Updates sollten daher in der Nacht stattfinden.
- Die Updates sollten vor denen der Clients vorgenommen werden
- Der Neustart sollte anschließend gleich automatisch vorgenommen werden, so dass die Systemicherheit sofort gewährleistet ist. (Dieser Punkt ist allerdings umstritten. Manche Systemadministratoren halten einen unbeaufsichtigten Neustart auch für kritisch und daher nicht wünschenswert).

Es empfiehlt sich ferner, für die Server im WSUS eine eigene Computergruppe anzulegen. Ob es sinnvoll ist, alle Updates auch den Servern sofort zuzuweisen kann nicht eindeutig beantwortet werden. Schließlich wurden immer wieder Updates ausgeliefert, die noch nachgebessert werden mussten. Insbesondere bei Servicepacks sollte erst abgewartet werden, ob mit diesen Probleme auftreten.

Informationen, welche Servicepacks für die Musterlösung empfohlen sind, finden Sie regelmäßig unter [www.support-netz.de](http://www.support-netz.de). Für einzelne Patches kann das natürlich nicht geleistet werden.

## 1.9. Sonstige Einstellungen

Es kann sich als sinnvoll erweisen, die Bandbreite für die Downloads zu beschränken. Dadurch steht weiterhin während der Schulzeiten ein Großteil der Bandbreite für das „normale Arbeiten“ mit dem Internet zur Verfügung. Für die Nacht kann ein abweichender Wert eingestellt werden.



Sie können diese Konfiguration über eine Gruppenrichtlinie vornehmen, die sich auf den WSUS auswirkt. Die entsprechende Einstellung finden Sie unter *Computerkonfiguration | Administrative Vorlagen | Netzwerk | Intelligenter Hintergrundübertragungsdienst | Maximale Netzwerkbandbreite, die BITS verwendet*: Man könnte diese Einstellung auch für die Clients verwenden, um die Bandbreite beim Updaten zu beschränken, das macht aber in der Regel wenig Sinn.

Nähere Informationen siehe <http://www.microsoft.com/germany/technet/datenbank/articles/600527.mspx#ECAA>.

**Hinweis:** Die an diese Stelle beschriebenen Regeln sind erst ab einem Windows 2003-Server verfügbar.

## 1.10. Ein Blick auf die Reports

Die Möglichkeit, Reports zu erstellen ist zwar etwas spartanisch und performancelastig, bietet aber dennoch gegenüber dem SUS die Möglichkeit nachzuverfolgen, wie der Patch-Stand im lokalen Netzwerk ist.

- Reports werden grundsätzlich aus der Datenbank erstellt.
- Die Clients werden nicht abgefragt, sondern melden ihren Ist-Zustand an die Datenbank. Das kann einige Zeit dauern.
- Abfragen z.B. nach dem Client-Betriebssystem sind nur dann möglich, wenn man die Rechner von Hand in entsprechende Gruppen einsortiert.

Am besten nutzt man die Reportfunktion ein bis zwei Tage nach angestoßenem Verteilen der Updates.

Über die Reportfunktion ist es z.B. sehr gut möglich nachzuverfolgen, welche Rechner schon lange nicht mehr aktualisiert wurden. Das kann insbesondere bei mobilen Stationen daran liegen, dass sie schon längere Zeit nicht mehr an das Netz der Musterlösung angeschlossen waren.

## 2.

### Der WSUS und die Musterlösung

Im Zusammenhang mit WSUS – Musterlösung konnten bislang keine größeren Probleme festgestellt werden. Sie sollten lediglich die nachfolgenden Punkte beachten. Falls Ihnen weitere Probleme auffallen, bitten wir um Rückmeldung an die Hotline ([www.support-netz.de](http://www.support-netz.de)).

#### 2.1.

#### Konfiguration des Proxy

Konfigurieren Sie den Proxy des WSUS wie in der Abbildung angegeben.

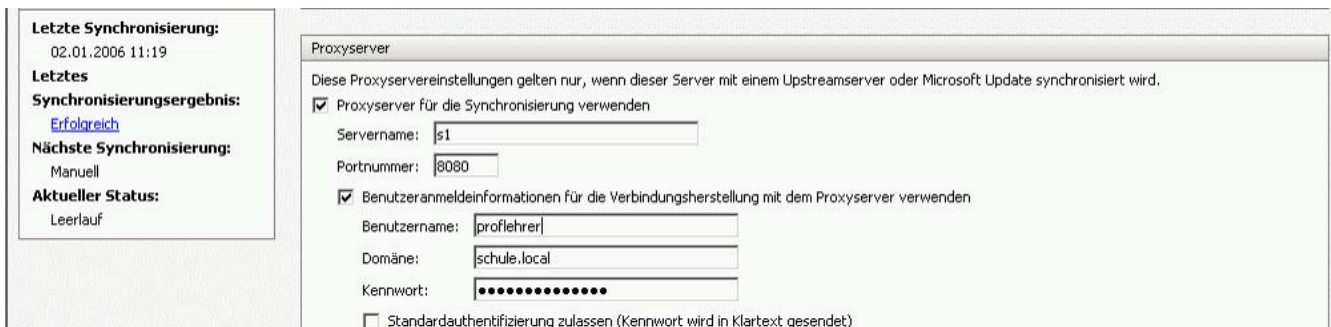
Servername: **s1 (Mehrserver: S2 oder S3)**

Portnummer: **8080**

Benutzername: **proflehrer**

Domäne: **schule.local**

Kennwort: **siehe proflehrer**



**Hinweise:** Wie in der Abbildung sollten Sie dabei *nicht* den Administrator als Benutzer eintragen. Es genügt ein beliebiger Benutzer, dem der ISA-Server den Zugriff auf das Internet gestattet. Aus Sicherheitsgründen empfiehlt es sich nämlich, administrative Accounts wirklich nur dort zu verwenden, wo sie absolut notwendig sind. An dieser Stelle genügt auch z.B. „proflehrer“. In der Mehrserverlösung müssen Sie den

Servename des ISA-Servers eintragen. Ohne Angabe eines Benutzers geht die Verbindung in dem Fall schief, wo Sie (wie in der Anleitung zur Raumkonsole beschrieben) eine globale Authentifizierung gegenüber dem ISA-Server verlangen. Siehe auch [4, S. 18].

## 2.2.

### Notwendige Anpassung der Raumkonsole bis Version 1.1

Nachdem der WSUS installiert wurde, bringt die Raumkonsole folgende Fehlermeldungen:

```
Fehler asp 0159:80004005
Pufferung deaktiviert
/raumkonsole/status_start_asp line 35
Die Pufferung muss aktiviert sein
```

Ursache ist ein undokumentiertes Umkonfigurieren des IIS bei der Installation, denn es wird dadurch die Pufferung global abgeschaltet. Diese lässt sich (nur für die Raumkonsole) wieder aktivieren, indem man in `c:\inetpub\Raumkonsole\common.asp` in Zeile 41 einfügt:

```
response.buffer = true
```

Danach funktioniert alles wieder. Empfohlen ist aber ein Update auf die Raumkonsole 1.5, die Sie auf [www.support-netz.de](http://www.support-netz.de) herunterladen können.

### 3. Verschiedenes zum WSUS

#### 3.1. Mögliche Probleme und Lösungen

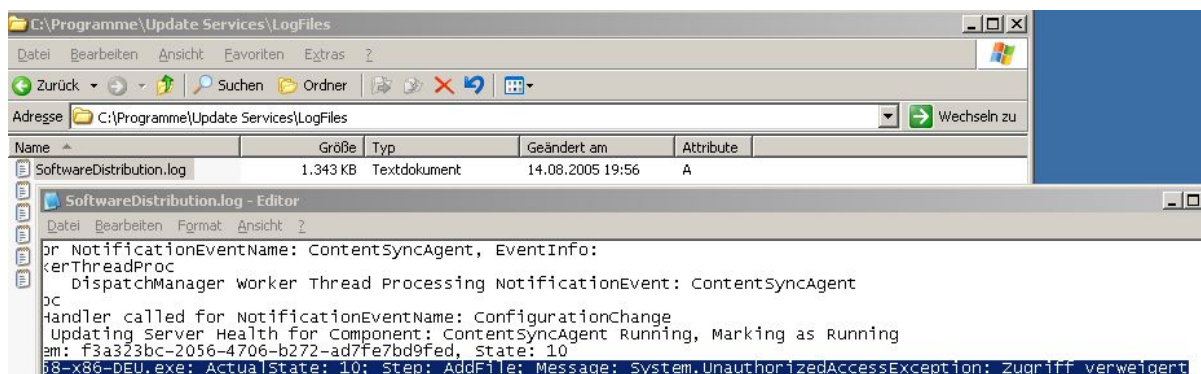
Nicht immer funktionieren die installierten Dienste des WSUS auf Anhieb. Bei einer Suche mit Google oder in einschlägigen Newsgroups findet man viele Probleme und entsprechend manche Lösungen werden aufgeführt. Deren Aufzählung sprengt jedoch den Rahmen dieses Papiers, so dass hier nur die wichtigsten genannt werden.

##### 3.1.1. Der Server synchronisiert nicht

- Erlaubt der ISA-Server dem WSUS Zugriff auf das Internet? Existiert also eine entsprechende Zugriffsregel?
- Stimmen die Proxy-Einstellungen? Ist hier ein expliziter Benutzer mit konkretem Passwort eingetragen?

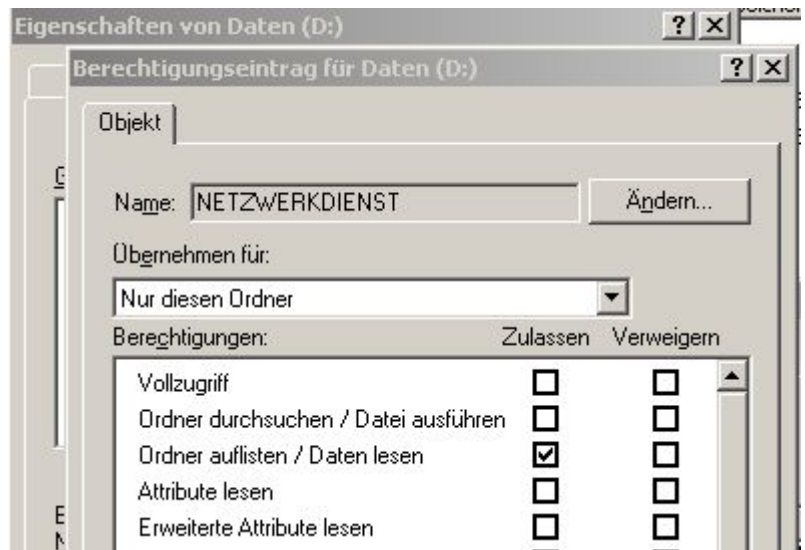
##### 3.1.2. Das Synchronisieren funktioniert, aber der Dateidownload nicht

Es kann sein, dass der Datei-Download an einem Berechtigungsproblem scheitert. Kontrollieren Sie bitte, ob das Rootverzeichnis der Partition, auf der die WSUS-Daten liegen, für den Benutzer „Netzwerkdienst“ Leserechte besitzt.



Sie können diesen Fehler durch einen Blick in die Log-Datei *SoftwareDistribution.log* im Verzeichnis *c:\Programme\Update Services\logFile* ausfindig machen (siehe Abbildung).

Um den Fehler abzustellen, müssen Sie die Berechtigungen im Root-Verzeichnis der Festplattenpartition mit den Update-Daten anpassen (in der Abbildung: D:\). Es genügt das abgebildete Recht für den Netzwerkdienst. Dieser sollte außerdem Vollzugriff auf das Verzeichnis mit den Update-Dateien (D:\WSUS\WSUSContent\) haben.



### 3.1.3.

Die Updates kommen nicht bei den Clients an

- Stellen Sie sicher, dass die Konfiguration über die Gruppenrichtlinie richtig vorgenommen ist und auch bei den Clients ankommt. Sie können die Einstellungen über die Systemsteuerung abrufen.
- Kontrollieren Sie die Datei *WindowsUpdate.log*. Sie finden diese bei Windows 2000 unter c:\winnt und bei Windows 2003 unter c:\windows. Sollten Sie in der Logdatei Error-Meldungen finden, können Sie auf der Fehlerübersichtsseite [6] nachschauen, was schief gelaufen ist.

### 3.1.4.

Weitere Maßnahmen

Bei Microsoft sind unter

<http://www.microsoft.com/windowsserversystem/updateservices/downloads/default.msp> je ein Diagnose-Tool für den Server und die Clients herunterzuladen. Vielleicht können Sie damit den Fehler eingrenzen.

Mit dem WSUSDebugTool können Sie auch weitere Maßnahmen durchführen, z.B. die nicht benötigten (und damit von Ihnen als abgelehnt gekennzeichneten) Updates physikalisch von der Platte löschen, um Festplattenplatz zu sparen. Das geht mit der Option

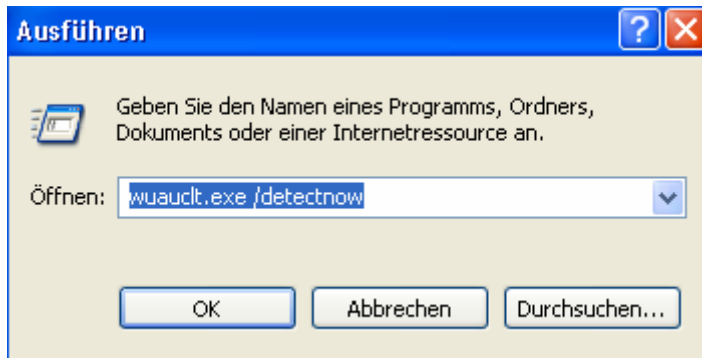
```
WsusDebugTool.exe /Tool:PurgeUnneededFiles
```

In der zugehörigen readme-Datei finden Sie alle Optionen beschrieben.

## 3.2.

## Sofortiges Update eines Clients

Es ist leider nicht möglich, mit einem einfachen Mausklick seinen Rechner sofort zu aktualisieren. Sie können aber über *Start | Ausführen* mit dem Kommando `wuauclt.exe /detectnow` einen Update-Zyklus erzwingen. Es dauert dann allerdings 5-10 Minuten bis die Updates heruntergeladen und zur Installation angeboten werden.



Ein Anstoßen des Updates vom Server aus ist nicht möglich.

## 3.3.

## Update eines bestehenden SUS-Servers

Ein direktes Update ist von Microsoft nicht vorgesehen. Der Microsoft Windows Update Services Deployment Guide [1] beschreibt ab S. 79 Möglichkeiten, bestehende Einstellungen zu übernehmen.

Leider ist es nicht möglich, die heruntergeladenen Updates einfach zu kopieren, da diese in einer anderen Filestruktur vorliegen. Microsoft bietet jedoch ein Migrationstool an. Die Beschreibung im Deployment-Guide [1] geht auf mehrere Szenarien ein. Weitere Informationen finden Sie auch unter [8].

Dieses Tool kann jedoch auch dazu verwendet werden, z.B. auf DVD gesicherte SUS-Patch-Sammlungen in den WSUS einzulesen.

**Wichtig:** Kopieren Sie dazu zunächst den kompletten Ordner *CABS* aus dem Verzeichnis *CONTENT* auf eine lokale Platte und entfernen Sie über die Dateieigenschaften den Schreibschutz (vgl. [7]).

Beispiel: der Ordner *CABS* wurde nach `d:\downloads` kopiert. Geben Sie dann unter *Start | Ausführen*

```
"C:\Programme\Update Services\Tools\wsusutil.exe" migratesus /content
d:\Downloads\cabs /log c:\wsuslog.txt
```

ein. Nach einiger Zeit ist die Integration abgeschlossen und das Kommandozeilenfenster schließt sich. In der Datei `C:\wsuslog.txt` können Sie überprüfen, ob die Dateien erfolgreich übernommen wurden. Dieses Verfahren wurde von uns mit Erfolg getestet. Nach dem Einspielen der alten Updates kann es jedoch sein, dass die Datenbank zunächst nicht ansprechbar ist. Bitte warten Sie einige Zeit ab und führen Sie gegebenenfalls einen Neustart des Servers durch.

## 3.4.

## Übernahme der Dateien von einem anderen WSUS

Hierzu kann man die in [1, S. 74ff] beschriebene Methode verwenden, die zeigt, wie man auch einen nicht mit dem Internet verbundenen WSUS mit Updates versorgt. Letztendlich muss nur das Verzeichnis `D:\WSUS\WSUSContent\` kopiert werden (der Laufwerksbuchstabe kann abweichen). Auch die Datenbank kann gesichert und übertragen werden, das ist jedoch ein aufwändiges Verfahren.

## 3.5.

## Weiterführende Informationen, Quellenangaben und Links

[1] Microsoft Windows Update Services Deployment Guide (engl., 1,4MB, 149S.)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=e99c9d13-63e0-41ce-a646-eb36f1d3e987&DisplayLang=en>

[2] WSUSOverview.doc (engl., 214kB, 21S.)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=2478d594-a29c-483c-9dc1-9740bf3081a5&displaylang=en>

[3] WSUSWin2k.doc (engl., 324kB, 24S.)

<http://go.microsoft.com/fwlink/?LinkId=49071>.

[4] WSUSStepbyStep.doc (dt., 366kB, 26 S.)

<http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=3BA03939-A5A9-407B-A4B0-1290BA5182F8>

[5] Installation des IE6Sp1 auf den Clients per Gruppenrichtlinie

<http://www.ml-tipps.de/cms/Software/detail.php?nr=32&kategorie=Software>

[6] Einige Fehlernummern in WindowsUpdate.log und ihre Bedeutungen

<http://docxp.mvps.org/WU5-ERR.htm>

[7] [http://www.administrator.de/WSUS\\_migration\\_Error:\\_Der\\_Zugriff\\_auf\\_den\\_Pfad....html](http://www.administrator.de/WSUS_migration_Error:_Der_Zugriff_auf_den_Pfad....html)

[8] SUSToWSUS.doc (engl., 287kB)

<http://www.microsoft.com/downloads/details.aspx?FamilyId=150E795E-AE32-4D47-A6B8-E01F918AAE93&displaylang=en>

[9] Technet-Artikel: [Windows Server Update Services aktualisieren Software zuverlässig](#)

[10] WSUS-Übersichtsseite auf Deutsch:

<http://www.microsoft.com/germany/windowsserver2003/technologien/updateservices/default.msp>

[11] <http://www.wsus-praxis.de/>

[12] Deutsche WSUS-Seite mit empfehlenswerter FAQ:

<http://www.wsus.de/faq.htm>

Die Links verstehen sich Stand 03/06. Leider werden die Dateien von Microsoft in kurzen Zeitabständen umorganisiert.

## 4.

## Anhang: Konfiguration bei Verwendung des IIS-Lockdown-Tools

Im Zusammenhang mit der Installation des WSUS-Servers wird auch die Anwendung des IIS-Lockdown-Tools empfohlen. Beim SUS erfolgte dies noch automatisch, führte aber mit den verwendeten Defaulteinstellungen zu Problemen mit Exchange und der Raumkonsole.

Das Lockdown-Tool ist nur auf einem Windows 2000-Server notwendig! Windows 2003 verwendet den IIS 6, der von Haus aus sicherer konfiguriert ist.

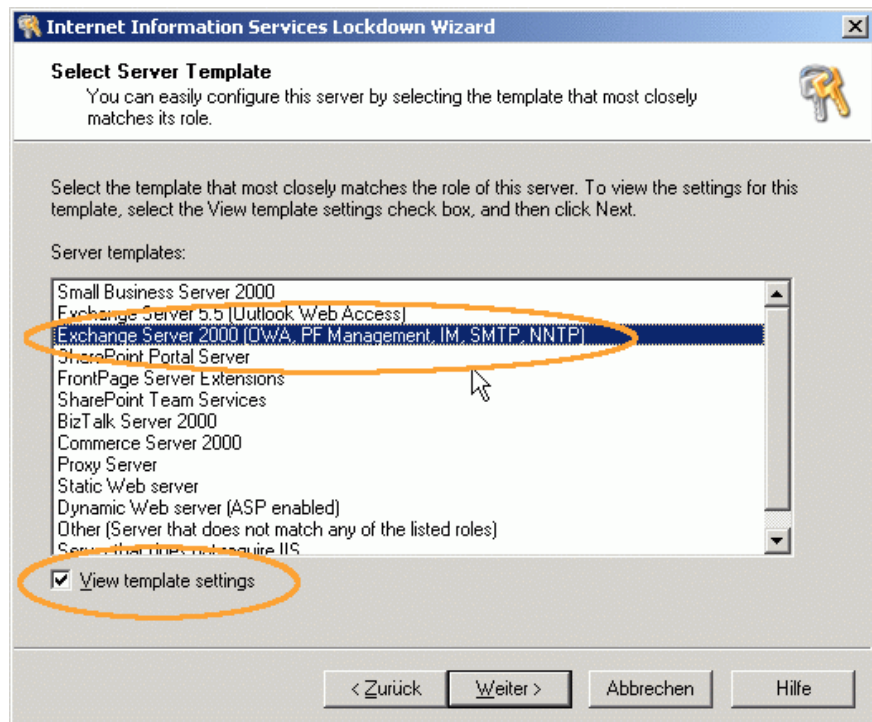
**Wichtiger Hinweis:** Das Lockdown-Tool speichert die IIS Konfiguration vor der Installation ab und setzt bei der Deinstallation den IIS wieder zurück. Somit werden die Einträge der Raumkonsole (wenn diese nach dem Verwenden des Lockdown-Tools installiert wurde) gelöscht und die Raumkonsole kann nicht mehr aufgerufen werden.

Sollte dieser Fall eingetreten sein, können Sie über *Start | Programme | Systemsteuerung | Software* die Raumkonsole 1.5 entfernen und danach wieder neu installieren.

Gehen Sie wie folgt vor:

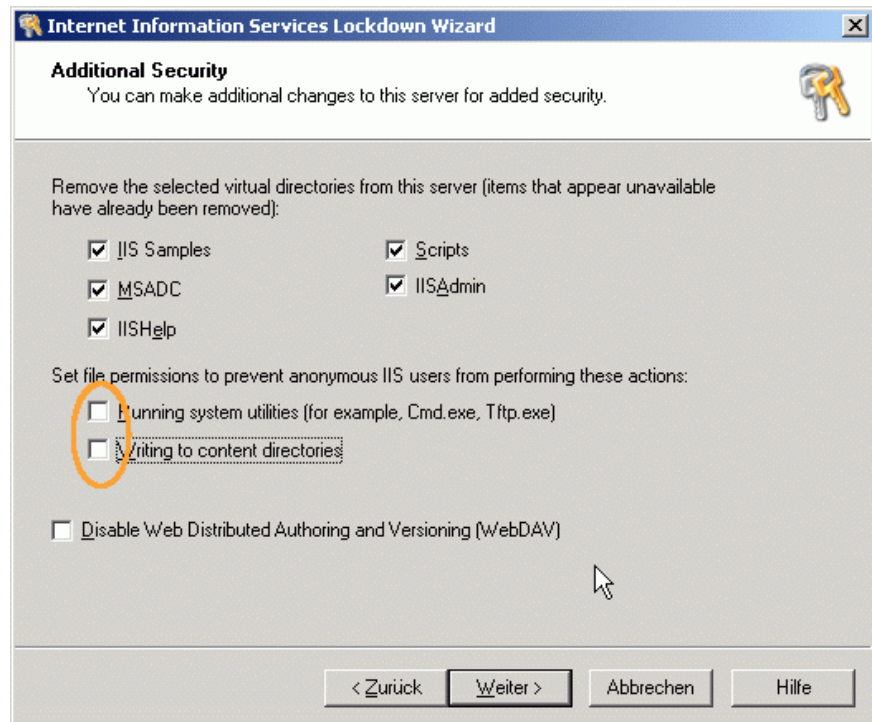
1. Das IIS Lockdown-Tool 2.1 (*iislockd.exe*, 285 KB, 10/10/2002) von der Microsoft-Seite herunterladen (Die Linkadresse ändert sich ständig, suchen Sie bei Microsoft Downloads).
2. Doppelklick auf *iislockd.exe* und akzeptieren Sie die Lizenzbestimmungen

Im nächsten Fenster nehmen Sie folgende Änderungen vor:



In den nächsten beiden Fenstern klicken Sie auf *Weiter*.

Im folgenden Fenster entfernen Sie zwei Haken.



Nun können Sie in den folgenden Fenstern immer die Voreinstellung übernehmen und die Installation abschließen.

Folgende Probleme sind mitunter noch aufgetreten:

Wenn auf den Clients keine Updates installiert werden, kann die Datei Windows Update.log im Verzeichnis C:\WINNT der Clients bei der Fehlersuche helfen: Suchen Sie in dieser Datei nach Fehlermeldungen (Error)

Im Zusammenhang mit der Musterlösung trat vor allem folgender Fehler auf:

```
[05-05-2004 - 01:03:07] Client at 10.0.2.83: URL contains extension '.exe',
which is disallowed. Request will be rejected. Site Instance='1', Raw
URL= '/content/WindowsXP-KB824105-x86-ENU_92192cc7a15f27eda4f0e6a932db355.exe'
```

Abhilfe: Öffnen Sie auf dem Server die Datei C:\WINNT\system32\inetrv\urlscan\urlscan.ini und suchen Sie den Abschnitt:

```
; Deny executables that could run on the server
; .exe
.bat
.cmd
.com
```

Hier muss vor exe unbedingt ein Semikolon stehen, sonst werden die Updates nicht installiert.