



## Erweiterte Sicherheit beim Anmeldeprozess

In diesem Dokument gehe ich auf die Umstellung der WSUS-Kommunikation ein. Das Ziel ist die HTTP Verbindung auf HTTPS umzustellen. Also von dem Standard Port 8530 auf 8531.

Im Moment ist der Service noch immer unter http zu erreichen.

The screenshot shows the WSUS Update Services console for server SRV00. The 'Aufgaben' section indicates 7 computers have not reported their status for over 30 days. The 'Übersicht' section provides a summary of computer and update statuses. The 'Verbindung' (Connection) details are highlighted in a red box: Type: Lokal/SSL, Port: 8530, User role: Administrator, Server version: 10.0.14393.2848. The 'Ressourcen' section lists links to WSUS homepage, community, and Microsoft Update Catalog.

Über die interne CA besorgen wir uns ein SSL-Zertifikat. Bitte denkt an eventuelle Subject Alternative Namens (SAN).

Starten den IIS und durchlaufen folgende Zahlen, um der WSUS-Verwaltung ein Zertifikat zuzuweisen und daran zu binden.

The screenshot shows the IIS Manager for server SRV00. The 'WSUS-Verwaltung' site is selected. In the 'Site Bindings' section, a new binding for port 8531 is being configured. The 'Sitebindung bearbeiten' dialog is open, showing the following settings: Type: https, IP-Adresse: Keine zugewiesen, Port: 8531, Hostname: (empty), SNI erforderlich: unchecked, SSL-Zertifikat: SRV00.ndsedv.de. Step numbers 1 through 7 are overlaid on the interface to guide the configuration process.



## Erweiterte Sicherheit beim Anmeldeprozess

Danach stellen wir die einzelnen Services wie gezeigt auf SSL um. Der Ablauf ist immer derselbe 1-4.

- APIremoting30
- ClientWebService
- DSSAuthWebService
- ServerSyncWebService
- SimpleAuthWebService

### APIremoting30

The screenshot shows the IIS Manager interface for the 'WSUS-Verwaltung' application on 'SRV00'. The 'APIremoting30' site is selected. In the center pane, under the 'IIS' category, the 'SSL-Einstellungen' icon (labeled 2) is highlighted. A red circle with the number 1 is placed over the 'Apiremoting30' site node in the left navigation tree. The right pane contains various management actions like 'Feature öffnen', 'Anwendung durchsuchen', and 'Hilfe'.

The screenshot shows the 'SSL-Einstellungen' configuration page for the 'APIremoting30' site. The 'SSL erfordern' checkbox is checked (labeled 3). A red circle with the number 4 is in the top right corner of the action bar. The left navigation tree shows the 'Apiremoting30' site selected. The bottom status bar indicates 'Konfiguration: "localhost" applicationHost.config, <location path="WSUS-Verwaltung/APIremoting30">'.



## Erweiterte Sicherheit beim Anmeldeprozess

### ClientWebService

The screenshot shows the IIS Manager interface for a site named 'ClientWebService'. In the left navigation pane, under 'Verbindungen', the path is: Startseite > SRV00 (NDSEDVNDS) > Anwendungspools > Sites > ClientWebService. The main content area is titled 'SSL-Einstellungen' and contains the following text: 'Auf dieser Seite können Sie die SSL-Einstellungen für den Inhalt einer Website oder Anwendung ändern.' A checkbox labeled 'SSL erforderlich' is checked. Below it, there's a section for 'Clientzertifikate' with three radio button options: 'Ignorieren' (selected), 'Akzeptieren', and 'Erforderlich'. The right side of the screen includes a 'Warnungen' panel with a message: 'Die Änderungen wurden erfolgreich gespeichert.', and an 'Aktionen' panel with buttons for 'Übernehmen', 'Abbrechen', and 'Hilfe'. At the bottom, there are links for 'Ansicht "Features"' and 'Ansicht "Inhalt"'. The status bar at the bottom indicates: 'Konfiguration: "localhost" applicationHost.config, <location path="WSUS-Verwaltung/ClientWebService">'.

### DSSAuthWebService

The screenshot shows the IIS Manager interface for a site named 'DssAuthWebService'. The left navigation pane follows the same structure as the previous screenshot. The main content area is titled 'SSL-Einstellungen' and contains the same configuration options: 'SSL erforderlich' checked, 'Clientzertifikate' with 'Ignorieren' selected, and a message indicating successful save in the 'Warnungen' panel. The right side includes an 'Aktionen' panel with 'Übernehmen', 'Abbrechen', and 'Hilfe' buttons. The status bar at the bottom indicates: 'Konfiguration: "localhost" applicationHost.config, <location path="WSUS-Verwaltung/DssAuthWebService">'.



## Erweiterte Sicherheit beim Anmeldeprozess

### ServerSyncWebService

The screenshot shows the IIS Manager interface for a Windows Server 2008 R2 system. The left navigation pane shows the server structure: Startseite, SRV00 (NDSEDVNDS), Anwendungspools, and Sites. Under Sites, several websites are listed: Default Web Site, WSUS-Verwaltung, ApiRemoting30, ClientWebService, Content, DssAuthWebService, Inventory, ReportingWebService, Selfupdate, ServerSyncWebService, and SimpleAuthWebService. The 'ServerSyncWebService' node is selected. The main content area displays the 'SSL-Einstellungen' (SSL Settings) page. It includes a warning message: 'Auf dieser Seite können Sie die SSL-Einstellungen für den Inhalt einer Website oder Anwendung ändern.' (You can change the SSL settings for the content of a website or application.) A checkbox labeled 'SSL erforderlich' (SSL required) is checked. Below it, there's a section for 'Clientzertifikate' (Client certificates) with three radio button options: 'Ignorieren' (Ignore), 'Akzeptieren' (Accept), and 'Erforderlich' (Required). The right sidebar contains a 'Warnungen' (Warnings) section with a message: 'Die Änderungen wurden erfolgreich gespeichert.' (The changes were successfully saved.) and an 'Aktionen' (Actions) section with buttons for 'Übernehmen' (Accept) and 'Abbrechen' (Cancel). At the bottom, there are links for 'Ansicht "Features"' and 'Ansicht "Inhalt"'.

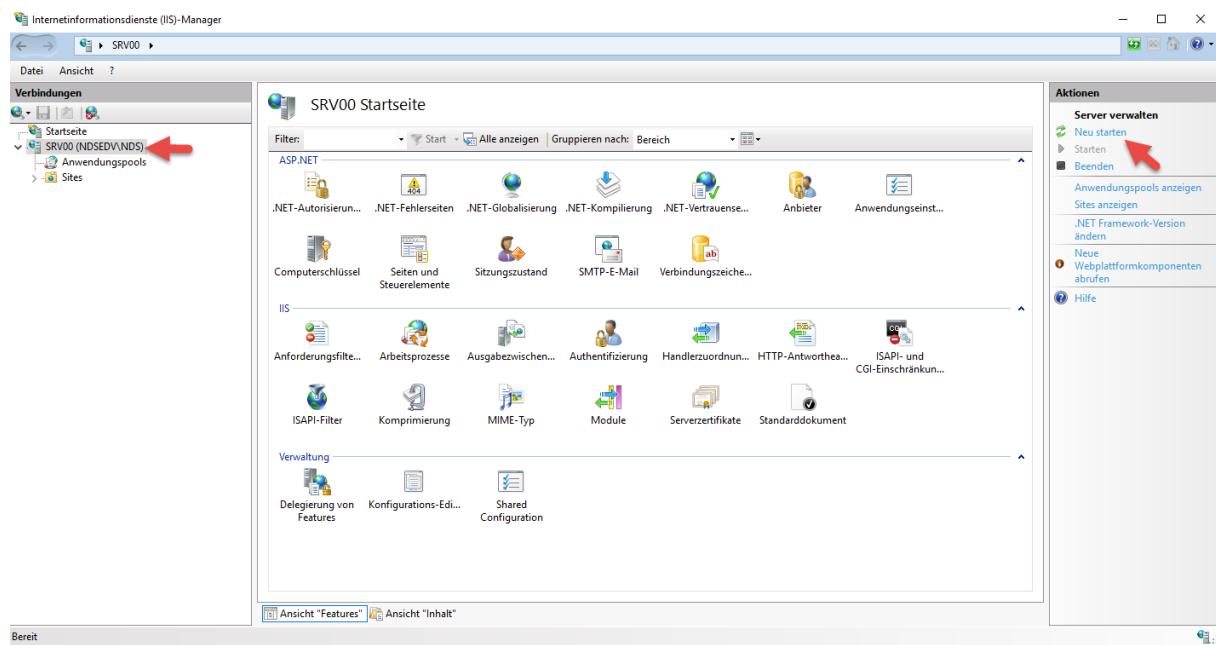
### SimpleAuthWebService

This screenshot is identical to the one above, showing the IIS Manager interface for the 'SimpleAuthWebService'. The left navigation pane, main content area, and right sidebar all reflect the same configuration and state as the 'ServerSyncWebService' screenshot, specifically regarding the 'SSL-Einstellungen' (SSL Settings) page for the 'SimpleAuthWebService' site.

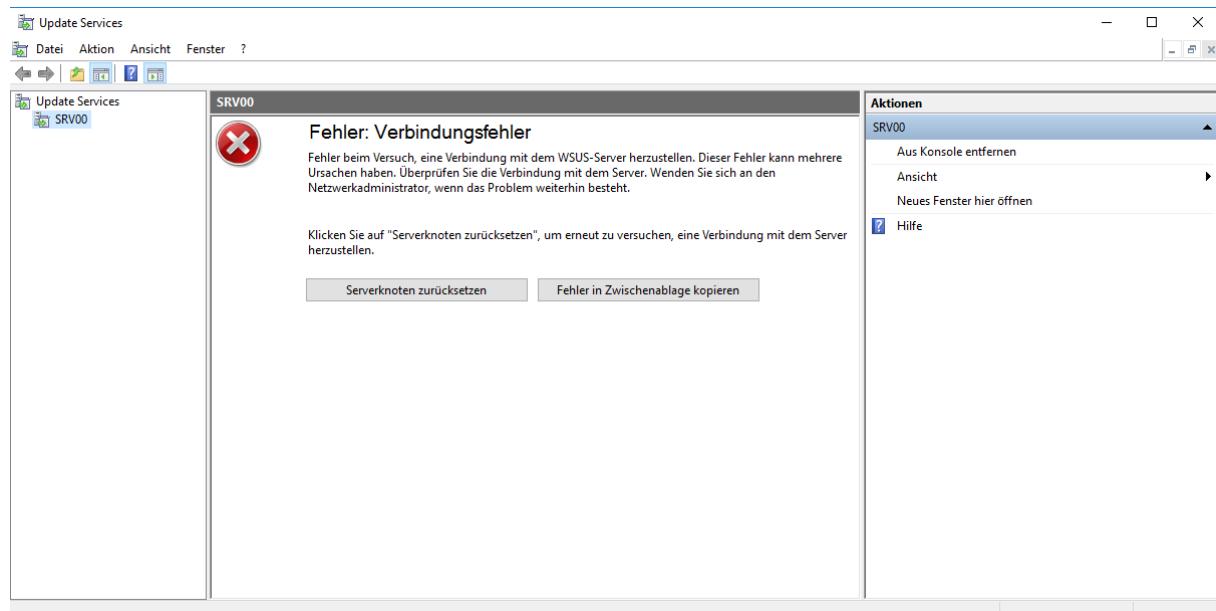


## Erweiterte Sicherheit beim Anmeldeprozess

Jetzt starten wir den IIS einmal durch.



Würde man jetzt versuchen die WSUS-Konsole zu öffnen, würde ein Verbindungsfehler angezeigt werden. Die Konsole muss auch noch auf SSL umgestellt werden



Dazu öffne wir die CMD mit administrativen Rechten und setzen folgenden Befehl ab:

**wsusutil.exe configuressl srv00.ndsedv.de**

```
Administrator: Eingabeaufforderung
C:\Program Files\Update Services\Tools>wsusutil.exe configuressl srv00.ndsedv.de
URL: https://srv00.ndsedv.de:8531
C:\Program Files\Update Services\Tools>
```



## Erweiterte Sicherheit beim Anmeldeprozess

Die Konsole lässt sich nun wieder öffnen und die Kommunikation ist auf SSL umgestellt.

Sollte sich die Konsole nicht öffnen lassen, einfach den IIS noch einmal durchstarten und die Bindung des Zertifikats kontrollieren.

The screenshot shows the Windows Update Services console for server SRV00. The 'Aufgaben' (Tasks) section indicates 5 computers have not reported their status for 30 days. The 'Übersicht' (Overview) section shows computer and update statistics. The 'Verbindungen' (Connections) section is highlighted with a red box, showing a connection to 'Lokal/SSL' port 8531 by the administrator. The 'Ressourcen' (Resources) section lists various WSUS links. The 'Aktionen' (Actions) sidebar on the right includes options like 'Suchen...', 'Aus Konsole entfernen', and 'Updates importieren...'.

Jetzt prüfen wir ob die Client-Verbindung steht.

<https://srv00.ndsedv.de:8531/selfupdate/wuident.cab>

The screenshot shows an Internet Explorer window displaying a download dialog. The message reads: 'Wie möchten Sie mit „wuident.cab“ verfahren?'. It provides file details: Größe: 26,8 KB and Von: srv00.ndsedv.de. Three options are listed: 'Öffnen' (Open), 'Speichern' (Save), and 'Speichern unter' (Save As). A note below 'Öffnen' states: 'Die Datei wird nicht automatisch gespeichert.' (The file will not be automatically saved.) At the bottom is a 'Abbrechen' (Cancel) button.



## Erweiterte Sicherheit beim Anmeldeprozess

Um das Ganze schlussendlich fertig zu stellen, passen wir noch die Gruppenrichtlinie an, um die ganzen Clients und Server über die Umstellung zu informieren.

The screenshot shows the Group Policy Management console. On the left, the navigation pane shows a tree structure under 'Gruppenrichtlinienverwaltung' for 'Gesamtstruktur: ndsev.de'. Under 'Domainen', there is a 'WSUS' node under 'Server'. The main pane displays the 'WSUS' policy settings. It includes three tables of rules:

Richtlinie	Einstellung	Kommentar
De Standardoption "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anpassen	Aktiviert	
Erneut zu einem Neustart für geplante Installationen auffordern	Aktiviert	
Folgenden Zeitraum (in Minuten) warten, bevor zu einem Neustart aufgefordert wird:	1440	

Richtlinie	Einstellung	Kommentar
Internen Pfad für den Microsoft Updatedienst angeben	Aktiviert	
Intranetserver zum Ermitteln von Updates:	<a href="http://sv00.ndsev.de:8530">http://sv00.ndsev.de:8530</a>	
Intranetserver für die Statistik:	<a href="http://sv00.ndsev.de:8530">http://sv00.ndsev.de:8530</a>	
Alternativen Downloadserver festlegen: (Beispiel: http://IntranetUpd01)		
Dateien ohne URL in den Metadaten herunterladen, wenn ein alternativer Downloadserver festgelegt ist	Deaktiviert	

Richtlinie	Einstellung	Kommentar
Keinen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind	Aktiviert	
Neustart für geplante Installationen verzögern	Aktiviert	
Folgenden Zeitraum (in Minuten) warten, bevor ein geplanter Neustart aufgefordert wird:	30	

The screenshot shows the 'Gruppenrichtlinienverwaltung' console again. A red arrow points to the 'WSUS' node under 'Server'. Another red arrow points to the 'Internen Pfad für den Microsoft Updatedienst angeben' dialog window. This dialog is used to specify the internal path for the Microsoft Update service. The 'Aktiviert' (Enabled) radio button is selected. The 'Internen Pfad' field contains the URL <https://sv00.ndsev.de:8531>. The 'Intranetserver für die Statistik' field also contains the same URL. The 'OK' button at the bottom right is highlighted.



## Erweiterte Sicherheit beim Anmeldeprozess

Nach einem **gpupdate** sollte die neue Verbindung in der Registry an dieser Stelle gefunden werden.

The screenshot shows the Windows Registry Editor window. The left pane displays a tree structure of registry keys under 'Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate'. The right pane is a table with columns 'Name', 'Typ', and 'Daten'. The 'WUStatusServer' entry is highlighted with a red arrow. Its 'Name' is 'WUStatusServer', 'Typ' is 'REG\_SZ', and 'Daten' is 'https://srv00.ndsedv.de:8531'.

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
ElevateNonAd...	REG_DWORD	0x00000001 (1)
TargetGroup	REG_SZ	Server
TargetGroupEna...	REG_DWORD	0x00000001 (1)
UpdateServiceU...	REG_SZ	
<b>WUStatusServer</b>	<b>REG_SZ</b>	<b>https://srv00.ndsedv.de:8531</b>
WUStatusServer	REG_SZ	https://srv00.ndsedv.de:8531