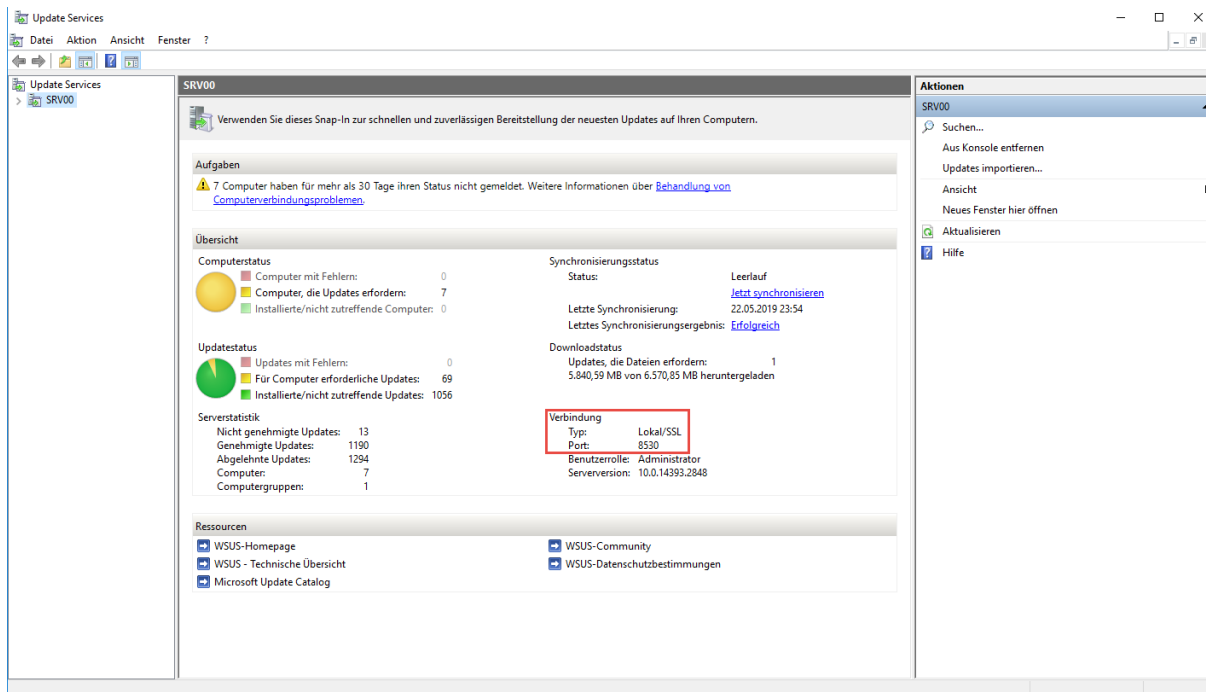




Erweiterte Sicherheit beim Anmeldeprozess

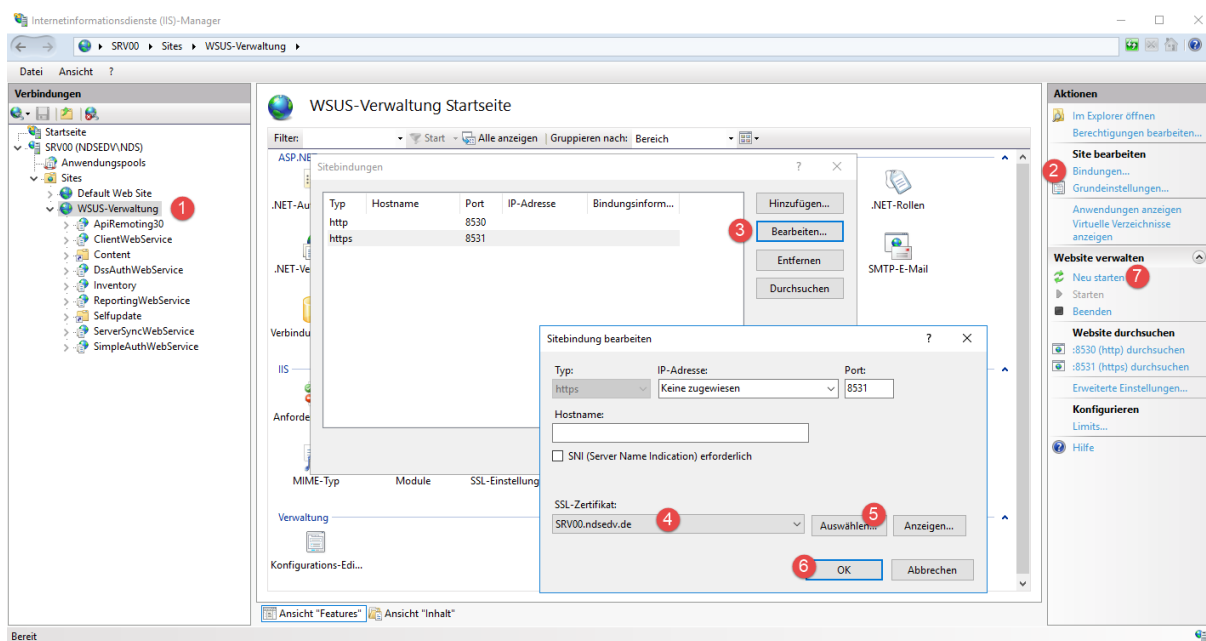
In diesem Dokument gehe ich auf die Umstellung der WSUS-Kommunikation ein. Das Ziel ist die HTTP Verbindung auf HTTPS umzustellen. Also von dem Standard Port 8530 auf 8531.

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



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.



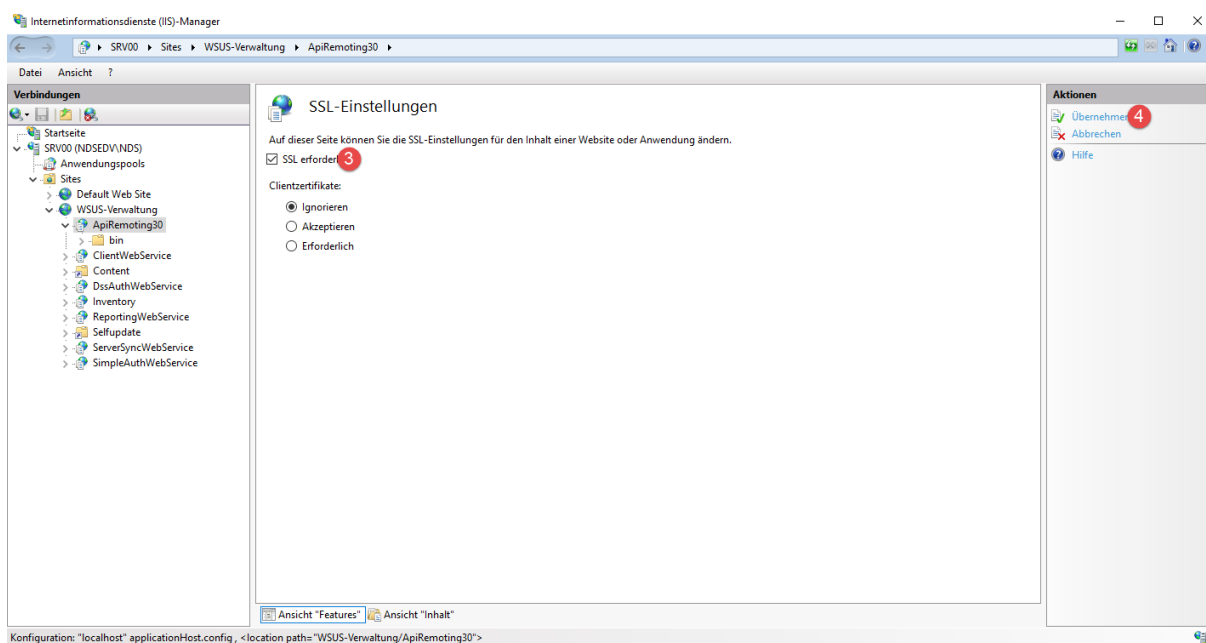
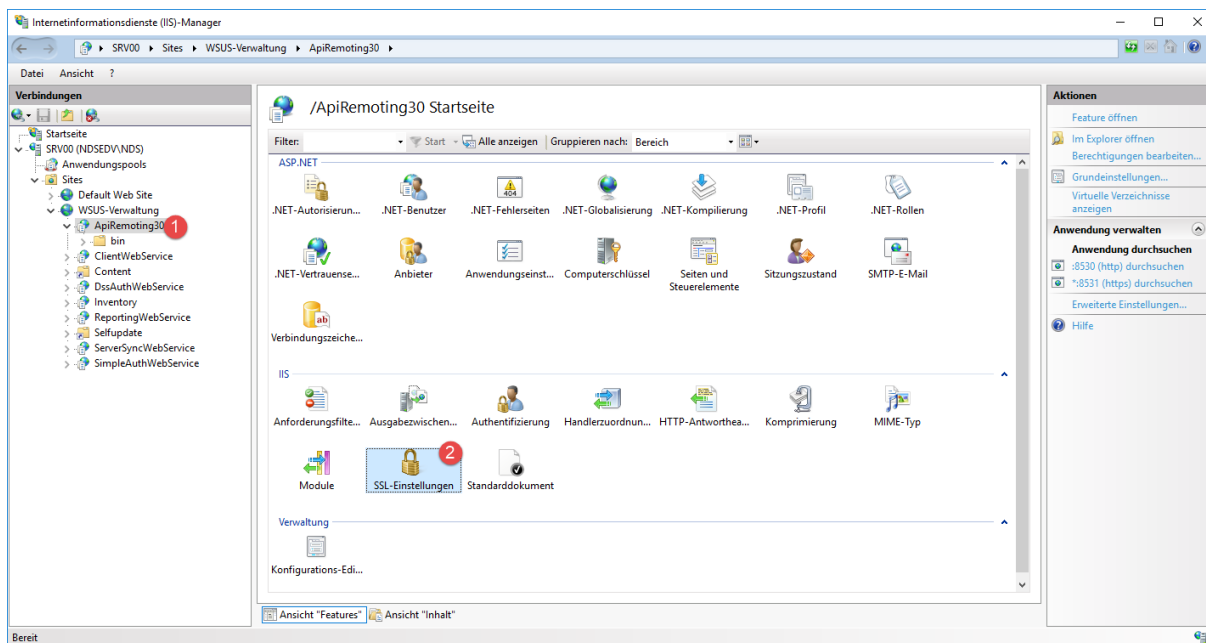


Erweiterte Sicherheit beim Anmeldeprozess

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

- APIremoting30
- ClientWebService
- DSSAuthWebService
- ServerSyncWebService
- SimpleAuthWebService

APIremoting30





Erweiterte Sicherheit beim Anmeldeprozess

ClientWebService

The screenshot shows the IIS Manager interface for the 'ClientWebService' site. The left-hand 'Verbindungen' (Connections) pane shows a tree view with 'WSUS-Verwaltung' expanded to 'ClientWebService'. The main pane displays the 'SSL-Einstellungen' (SSL Settings) for this site. The 'SSL erforderlich' (SSL required) checkbox is checked. Under 'Clientzertifikate' (Client certificates), the 'Ignorieren' (Ignore) radio button is selected. A warning message at the top right states: 'Die Änderungen wurden erfolgreich gespeichert.' (Changes were successfully saved). The bottom status bar shows the configuration path: 'Konfiguration: "localhost" applicationHost.config, <location path="WSUS-Verwaltung/ClientWebService">'.

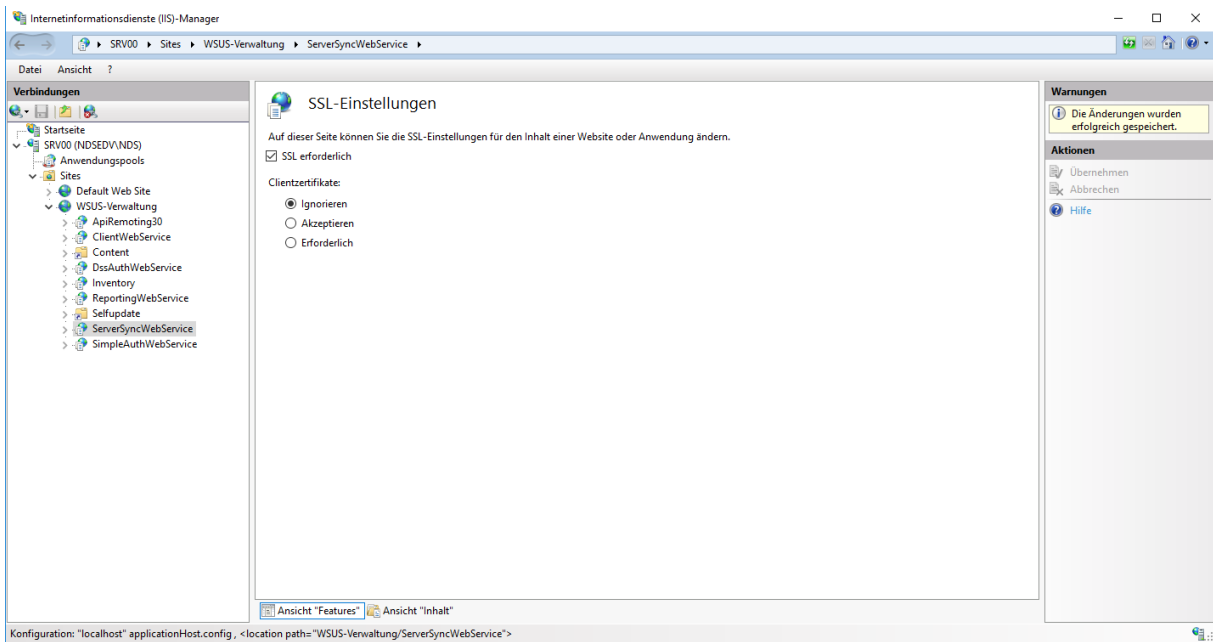
DSSAuthWebService

The screenshot shows the IIS Manager interface for the 'DSSAuthWebService' site. The left-hand 'Verbindungen' (Connections) pane shows a tree view with 'WSUS-Verwaltung' expanded to 'DSSAuthWebService'. The main pane displays the 'SSL-Einstellungen' (SSL Settings) for this site. The 'SSL erforderlich' (SSL required) checkbox is checked. Under 'Clientzertifikate' (Client certificates), the 'Ignorieren' (Ignore) radio button is selected. A warning message at the top right states: 'Die Änderungen wurden erfolgreich gespeichert.' (Changes were successfully saved). The bottom status bar shows the configuration path: 'Konfiguration: "localhost" applicationHost.config, <location path="WSUS-Verwaltung/DSSAuthWebService">'.

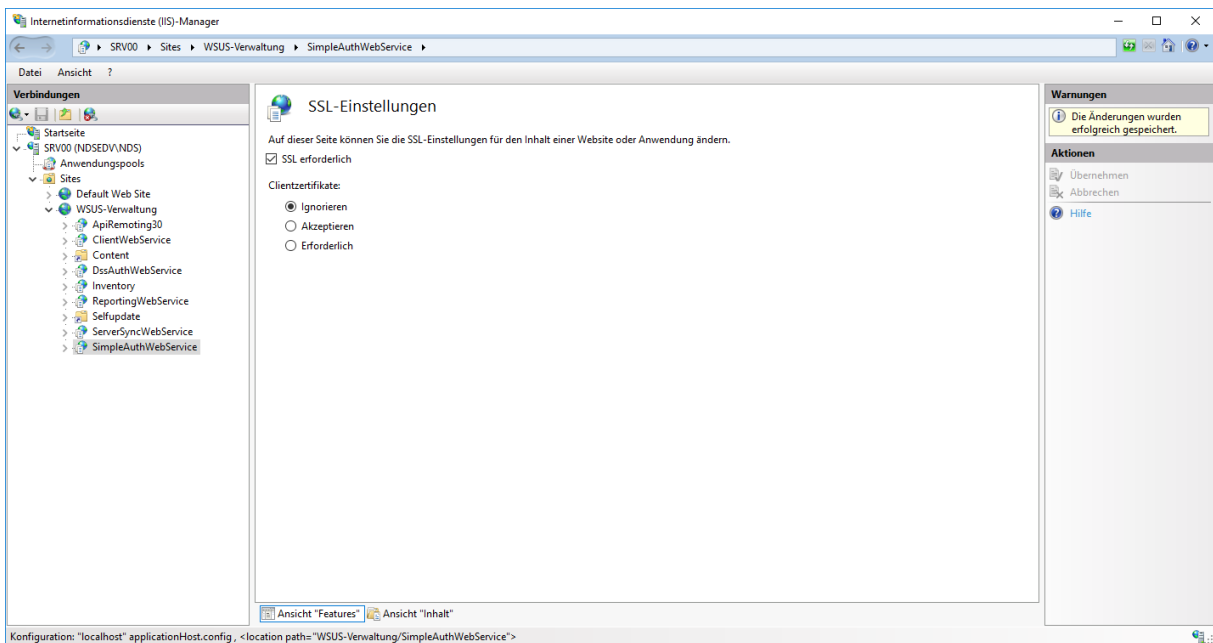


Erweiterte Sicherheit beim Anmeldeprozess

ServerSyncWebService



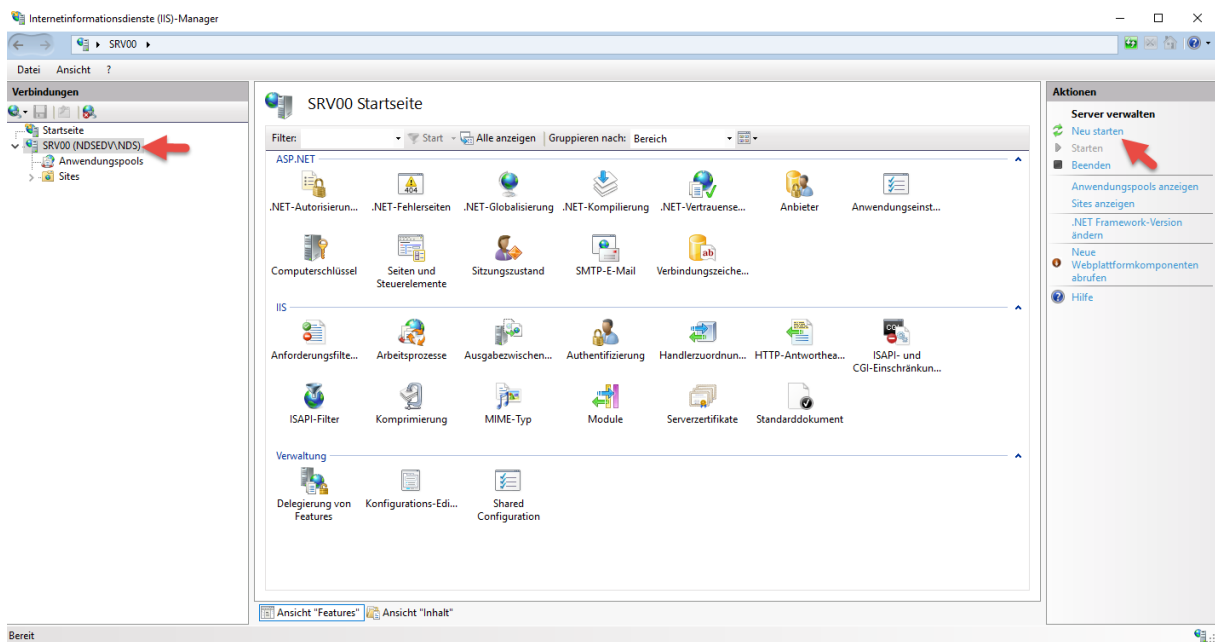
SimpleAuthWebService



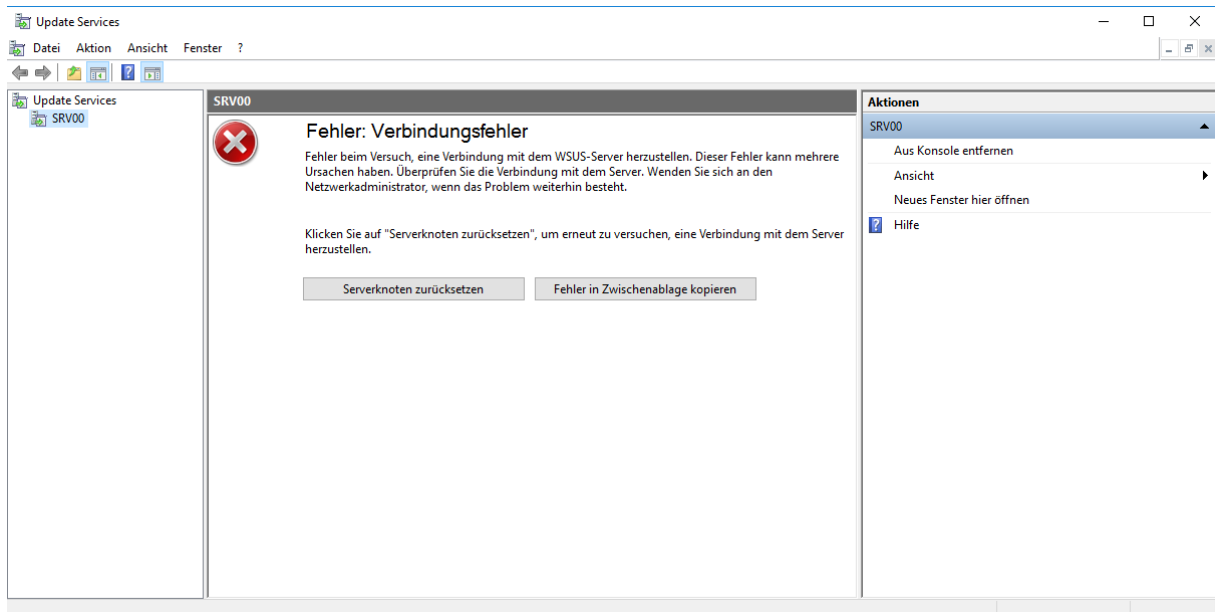


Erweiterte Sicherheit beim Anmeldeprozess

Jetzt starten wir den IIS einmal durch.

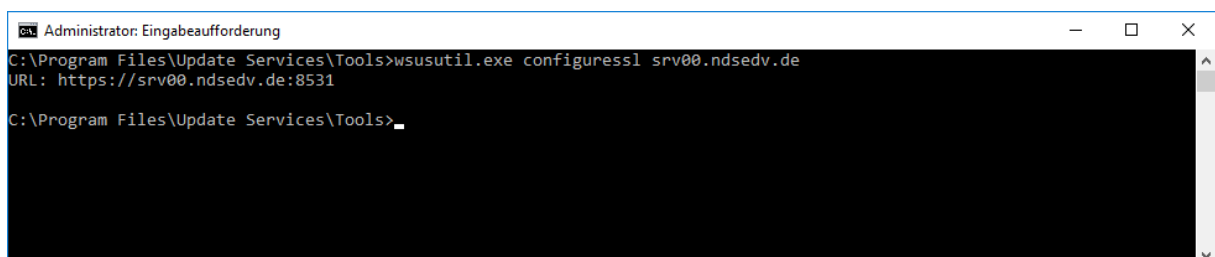


Würde man jetzt versuchen die WSUS-Konsole zu öffnen, würde ein Verbindungsfehler angezeigt werden. Die Konsole muss auch noch auf SSL umgestellt werden



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

wsutil.exe configuresssl srv00.ndsedv.de





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.

Computerstatus		Synchronisierungsstatus	
Computer mit Fehlern:	0	Status:	Leerlauf
Computer, die Updates erfordern:	7	Letzte Synchronisierung:	22.05.2019 23:54
Installierte/nicht zutreffende Computer:	0	Letztes Synchronisierungsergebnis:	Erfolgreich

Updatestatus		Downloadstatus	
Updates mit Fehlern:	0	Updates, die Dateien erfordern:	0
Für Computer erforderliche Updates:	72		
Installierte/nicht zutreffende Updates:	1056		

Verbindung	
Typ:	Lokal/SSL
Port:	8531
Benutzerrolle:	Administrator
Serverversion:	10.0.14393.2848

Jetzt prüfen wir ob die Client-Verbindung steht.

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

Internet Explorer

Wie möchten Sie mit „wuident.cab“ verfahren?

Größe: 26,8 KB
Von: srv00.ndsedv.de

→ Öffnen
Die Datei wird nicht automatisch gespeichert.

→ Speichern

→ Speichern unter

Abbrechen



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 for the 'ndsebv.de' domain. The 'WSUS' policy is expanded, showing the following settings:

Richtlinie	Einstellung	Kommentar
Die Standardoption "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anpassen	Aktiviert	
Erneut zu einem Neustart für geplante Installationen aufrufen	Aktiviert	
Folgendes Zeitraum (in Minuten) warten, bevor zu einem Neustart aufgefordert wird:		
		1440
Internen Pfad für den Microsoft Updatedienst angeben	Aktiviert	
Interner Updatedienst zum Ermitteln von Updates:		
Intranetserver für die Statistik:		http://sv00.ndsebv.de:8530
Alternativen Downloadserver festlegen:		http://sv00.ndsebv.de:8530
Daten ohne URL in den Metadaten herunterladen, wenn ein alternativer Downloadserver festgelegt ist	Deaktiviert	
Kenen automatischen Neustart für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind	Aktiviert	
Neustart für geplante Installationen verzögern	Aktiviert	
Folgendes Zeitraum (in Minuten) warten, bevor ein geplanter Neustart aufgefordert wird:		
		30
Nichtadministratoren gestatten, Updatebenachrichtigungen zu erhalten	Aktiviert	
Option "Updates installieren und herunterfahren" im Dialogfeld "Windows herunterfahren" nicht anzeigen	Aktiviert	

The screenshot shows the Group Policy Management console for the 'ndsebv.de' domain. The 'WSUS' policy is expanded, and the 'Internen Pfad für den Microsoft Updatedienst angeben' policy is selected. The configuration window for this policy is open, showing the following settings:

Internen Pfad für den Microsoft Updatedienst angeben

Nicht konfiguriert Kommentar:

Aktiviert

Deaktiviert

Unterstützt auf: Mindestens Windows XP Professional Service Pack 1 oder Windows 2000 Service Pack 3, Windows RT ausgenommen

Optionen:

Interner Updatedienst zum Ermitteln von Updates:

https://sv00.ndsebv.de:8531

Intranetserver für die Statistik:

https://sv00.ndsebv.de:8531

Alternativen Downloadserver festlegen:

(Beispiel: http://IntranetUpd01)

Dateien ohne URL in den Metadaten herunterladen, wenn ein alternativer Downloadserver festgelegt ist

Hilfe:

Gibt einen Intranetserver an, der als Host für Updates von Microsoft Update fungiert. Mit diesem Updatedienst können Sie dann die Computer in Ihrem Netzwerk automatisch aktualisieren.

Mit dieser Einstellung können Sie einen Server im Netzwerk als Host für einen internen Updatedienst bestimmen. Der Client für automatische Updates durchsucht diesen Dienst nach Updates, die auf die Computer in Ihrem Netzwerk angewendet werden können.

Wenn Sie diese Einstellung verwenden möchten, müssen Sie zwei Werte für Servernamen festlegen: den Server, auf dem der Client für automatische Updates die Updates sucht und von dem er sie herunterlädt, und den Server, auf den die aktualisierten Arbeitsstationen Statistiken hochladen. Sie können für beide Werte den gleichen Server festlegen. Außerdem können Sie einen optionalen Servernamenwert angeben, um den Windows Update-Agent so zu konfigurieren, dass er Updates von einem alternativen Downloadserver anstatt vom Updatedienst im Intranet herunterlädt.

OK Abbrechen Übernehmen



Erweiterte Sicherheit beim Anmeldeprozess

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

