



Es werden keine Vorlagen angezeigt

Wer die Webregistrierung einsetzt, um ein Zertifikat anzufordern, was recht selten ist, der stößt unter Umständen eventuell auf ein Problem.

The screenshot shows the Microsoft Active Directory Certificate Services website. The browser address bar displays `https://trustcenter.dwp.local/certsrv/`. The page title is "Microsoft-Active Directory-Zertifikatdienste - SRVSUBCA". The main heading is "Willkommen". The text explains that users can request certificates for web browsers, email clients, or other programs. It also mentions that users can download certificates or check the status of pending requests. A red arrow points to the link "Ein Zertifikat anfordern" under the heading "Wählen Sie eine Aufgabe:". Other links include "Status ausstehender Zertifikate anzeigen" and "Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste".

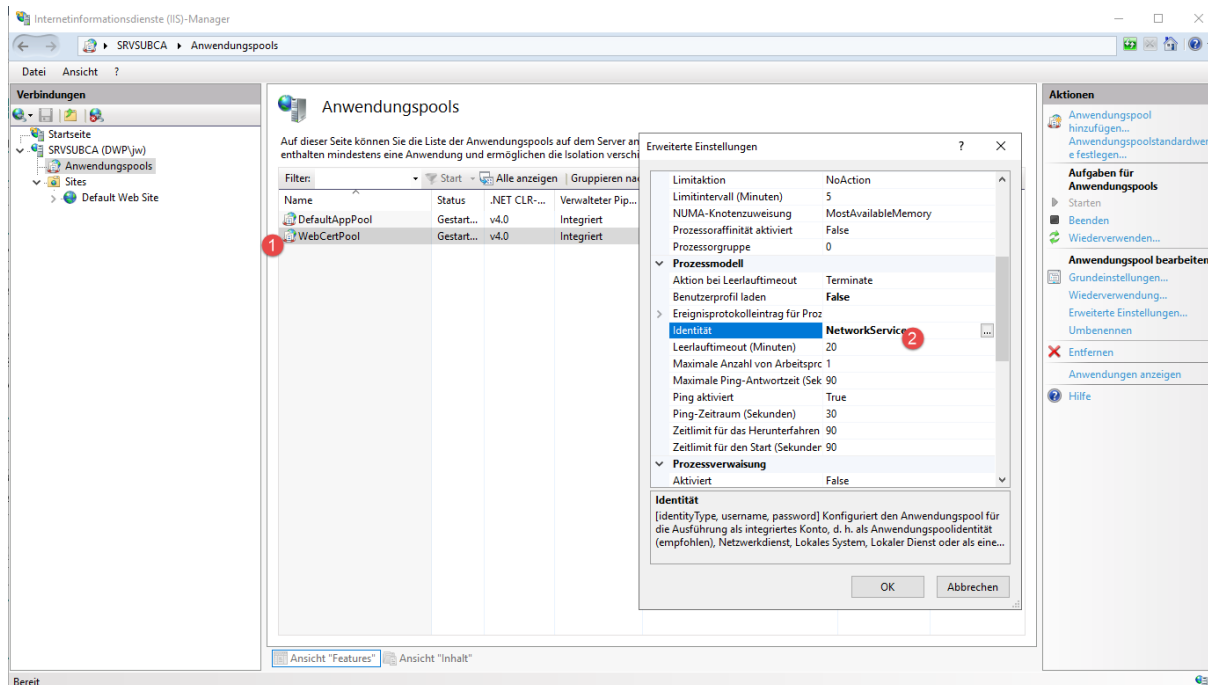
Es wurden keine Vorlagen gefunden, lautet die Meldung. Das kann richtig sein. Zertifikatsvorlagen ab der Version 3 werden nicht mehr unterstützt. Das bedeutet, dass nur noch Vorlagen bis v2 angezeigt werden.

The screenshot shows the "Erweiterte Zertifikatanforderung" page. The browser address bar displays `https://trustcenter.dwp.local/certsrv/certrqma.asp`. The page title is "Microsoft-Active Directory-Zertifikatdienste - SRVSUBCA". The main heading is "Erweiterte Zertifikatanforderung". The "Zertifikatvorlage:" dropdown menu shows "(Es wurden keine Vorlagen gefunden)". The "Schlüsseloptionen:" section includes radio buttons for "Neuen Schlüsselsatz erstellen" (selected) and "Bestehenden Schlüsselsatz verwenden". The "Kryptografiediensteanbieter:" dropdown shows "Wird geladen...". The "Schlüsselverwendung:" section has radio buttons for "Austausch" (selected), "Signatur", and "Beide". The "Schlüsselgröße:" input field is set to 0. The "Zusätzliche Optionen:" section includes radio buttons for "CMC" (selected) and "PKCS10", a "Hashalgorithmus:" dropdown, and a checkbox for "Anforderung speichern". The "Attribute:" field is empty, and the "Anzeigenname:" field is also empty. An "Einsenden" button is at the bottom right.

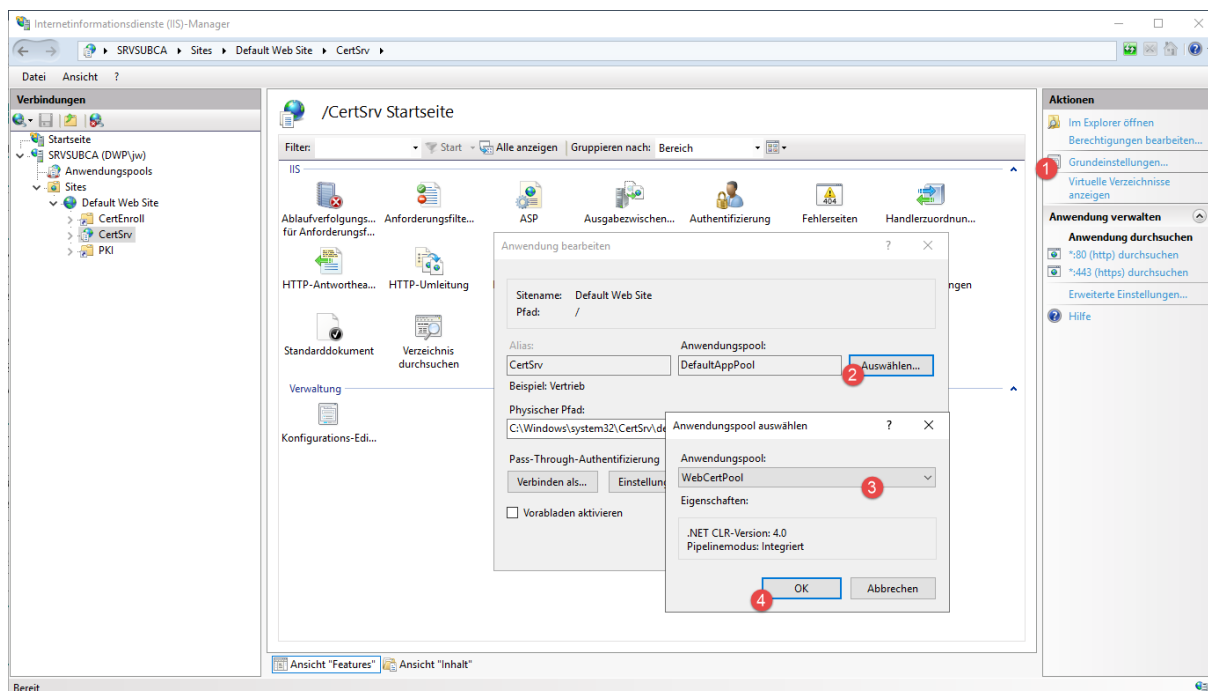


Es werden keine Vorlagen angezeigt

Nichtsdestotrotz sollten Fehler ausgeschlossen werden. Der häufigste Fehler ist, dass der ApplicationPool mit einer nicht korrekten Identitätseinstellung gestartet wurde. Bevor man den DefaultAppPool umkonfiguriert, legt man lieber schnell einen neuen an und nennt diesen z.B. WebCertPool. Die Identität stellen wir auf NetworkService.



Navigieren zu CertSrv sofern der Standard bei der Installation belassen wurde und ändert unter Grundeinstellungen den Anwendungspool. Stellt diesen auf den zuvor angelegten Pool um.

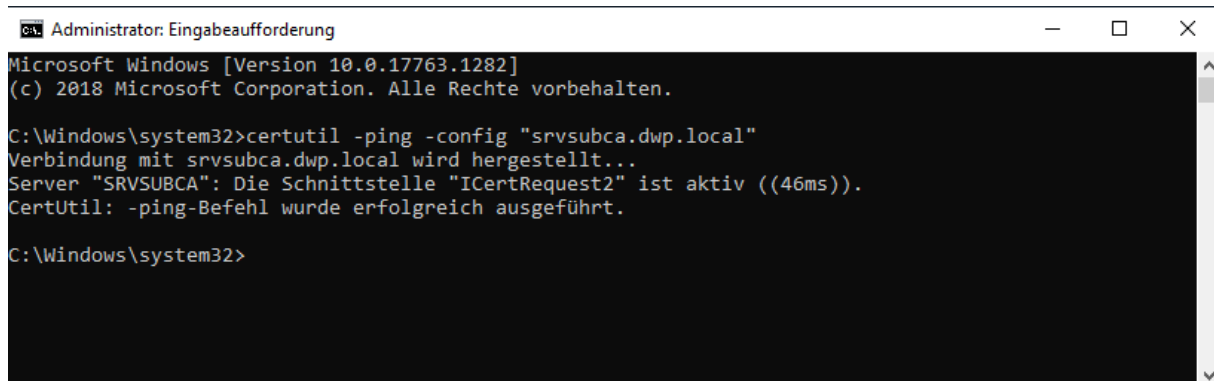




Es werden keine Vorlagen angezeigt

Dann prüft man, ob die Konfigurationseinstellungen (DNS) erreichbar sind.

Entweder ausgeführt über die CMD...

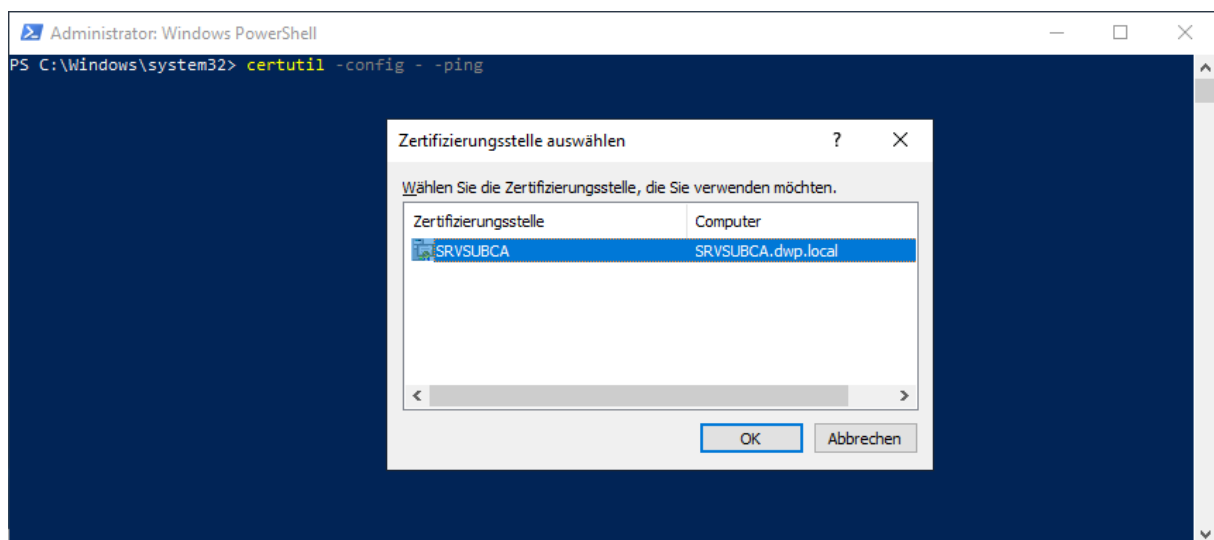


```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.1282]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>certutil -ping -config "srvsubca.dwp.local"
Verbindung mit srvsubca.dwp.local wird hergestellt...
Server "SRVSUBCA": Die Schnittstelle "ICertRequest2" ist aktiv ((46ms)).
CertUtil: -ping-Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>
```

...oder der Powershell



```
Administrator: Windows PowerShell
PS C:\Windows\system32> certutil -config - -ping
```

Zertifizierungsstelle auswählen

Wählen Sie die Zertifizierungsstelle, die Sie verwenden möchten.

Zertifizierungsstelle	Computer
SRVSUBCA	SRVSUBCA.dwp.local

OK Abbrechen



Es werden keine Vorlagen angezeigt

Der Name der ermittelten Zertifizierungsstelle sollte als FQDN wiedergegeben werden.
Der FQDN wiederum sollte ebenfalls in der certdat.inc wieder zu finden sein.

The screenshot shows a Windows PowerShell window running the command `certutil -config -ping` in the directory `C:\Windows\system32`. The output indicates that the connection to the local Certificate Enrollment Service (CES) is successful.

Below the PowerShell window, a File Explorer window shows the directory `C:\Windows\System32\certsrv`. The file `certdat.inc` is selected, and its contents are displayed in a text editor.

```
<% CODEPAGE=65001 'UTF-8%>
<% certdat.inc - (CERT)srv web - global (DAT)a
' Copyright (C) Microsoft Corporation, 1998 - 1999 %>
<%
    ' default values for the certificate request
    sDefaultCompany=""
    sDefaultOrgUnit=""
    sDefaultLocality=""
    sDefaultState=""
    sDefaultCountry=""

    ' global state
    sServerType="Enterprise" 'vs StandAlone
    sServerConfig="SRVSUBCA.dwp.local\SRVSUBCA"
    sServerDisplayName="SRVSUBCA"
    nPendingTimeoutDays=10
```



Es werden keine Vorlagen angezeigt

Der wiederrum sollte mit den Einstellungen in der Konfigurationspartition übereinstimmen.

Zu finden an dieser Stelle mittels ADSIEDIT.

CN=**Zertifikatsserver**, CN=Enrollment Services, CN=Public Key Services, CN=Services, CN=Configuration, DC=**DWP**,DC=local

Wenn nicht ist der Eintrag in der certdat.inc anzupassen.

The screenshot shows the ADSI-Editor interface. The left pane displays the directory tree for 'Konfiguration [DC1.dwp.local]'. The 'CN=Enrollment Services' folder is selected. The right pane shows the properties of the selected object, 'CN=SRVSUBCA'. The 'distinguishedName' attribute is highlighted, and its value is 'CN=SRVSUBCA,CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=DWP,DC=local'. A red arrow points to this attribute in the 'Eigenschaften von CN=SRVSUBCA' dialog box.

IISReset gefolgt von einem repadmin /syncall /AdePq

```
Administrator: Eingabeaufforderung
C:\Temp>repadmin /syncall /AdePq
Alle NCs auf DC1 werden synchronisiert.
Partition wird synchronisiert: DC=ForestDnsZones,DC=dwp,DC=local
SyncAll wurde ohne Fehler beendet.

Partition wird synchronisiert: DC=DomainDnsZones,DC=dwp,DC=local
SyncAll wurde ohne Fehler beendet.

Partition wird synchronisiert: CN=Schema,CN=Configuration,DC=dwp,DC=local
SyncAll wurde ohne Fehler beendet.

Partition wird synchronisiert: CN=Configuration,DC=dwp,DC=local
SyncAll wurde ohne Fehler beendet.

Partition wird synchronisiert: DC=dwp,DC=local
SyncAll wurde ohne Fehler beendet.

C:\Temp>_
```



Es werden keine Vorlagen angezeigt

Nun sollten die v2 Vorlagen wieder angezeigt werden.

Microsoft-Active Directory-Zertifikatdienste -- SRVSUBCA Startseite

Erweiterte Zertifikatanforderung

Zertifikatvorlage: Webserver-SSL

Schlüsseloptionen: Neuen Schlüsselsatz erstellen Bestehenden Schlüsselsatz verwenden

Kryptografiedienstanbieter: Wird geladen...

Schlüsselverwendung: Austausch Signatur Beide

Schlüsselgröße: Min.: (Allgemeine Schlüsselgrößen:) Max.:

Automatischer Schlüsselcontainername Vom Benutzer angegebener Containername

Schlüssel als "Exportierbar" markieren

Verstärkte Sicherheit für den privaten Schlüssel aktivieren

Zusätzliche Optionen:

Anforderungsformat: CMC PKCS10

Hashalgorithmus: Wird nur zum Signieren der Anforderung verwendet.

Anforderung speichern

Attribute: < >

Anzeigename:

Einsenden

Microsoft-Active Directory-Zertifikatdienste -- SRVSUBCA Startseite

Zertifikat- oder Erneuerungsanforderung einreichen

Fügen Sie eine Base-64-codierte CMC- oder PKCS #10-Zertifikatanforderung oder eine PKCS #7-Erneuerungsanforderung, die von einer externen Quelle (wie z. B. einem Webserver) generiert wurde, in das Feld "Gespeicherte Anforderung" ein, um eine gespeicherte Anforderung bei der Zertifizierungsstelle einzureichen.

Gespeicherte Anforderung:

Base-64-codierte Zertifikatanforderung (CMC oder PKCS #10 oder PKCS #7): < >

Zertifikatvorlage: Webserver-SSL

Zusätzliche Attribute:

Attribute: < >

Einsenden

