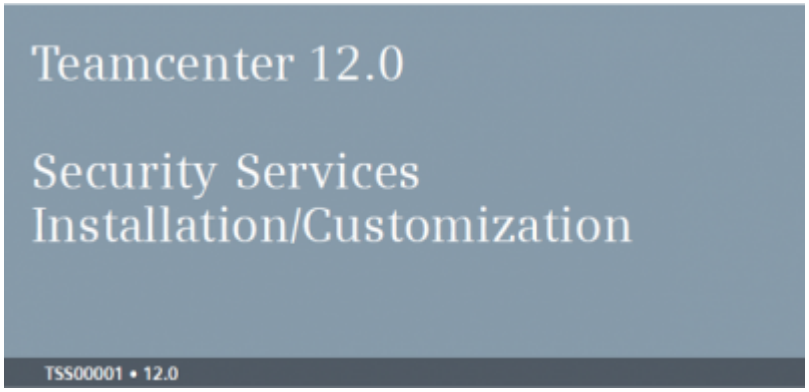
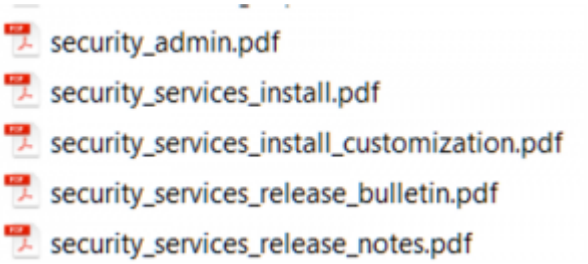
Table of Contents

Handbuch Tc 12 Security Services



Oktober 2020 Patrick Granwehr Christoph Bühler

Achtung:
Dies ist nur ein Leitfaden. Bitte zusätzlich noch die originalen Dokumente mit einbeziehen...



Impressum

avasis AG
Gemperenstrasse 26
CH-9442 Berneck
Tel.: +41 71 737 99 22

1. Vorbedingungen Clientinstallation

Wenn Umgebung schon so aufgesetzt ist muss nur noch die Anpassung für SSO gemacht werden.

Ist weiter unten beschrieben.

Dies kann auch später mit der SSO konfiguration nach der web_tier konfiguration gemacht werden.

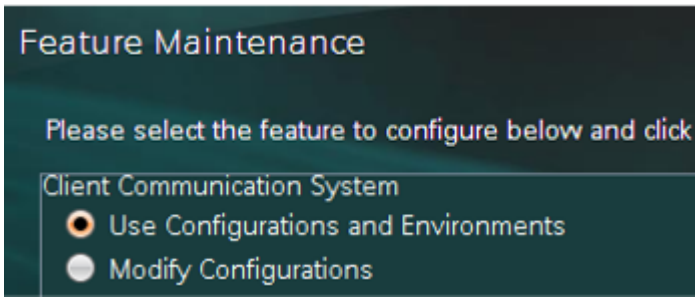
2. 4-tier Client installation auf tccs umstellen

Dieser Schritt ist nur notwendig, falls dieser nicht schon bei Grundinstallation des 4-tier RichClient gemacht wurde.

2.1 Feature Maintenance

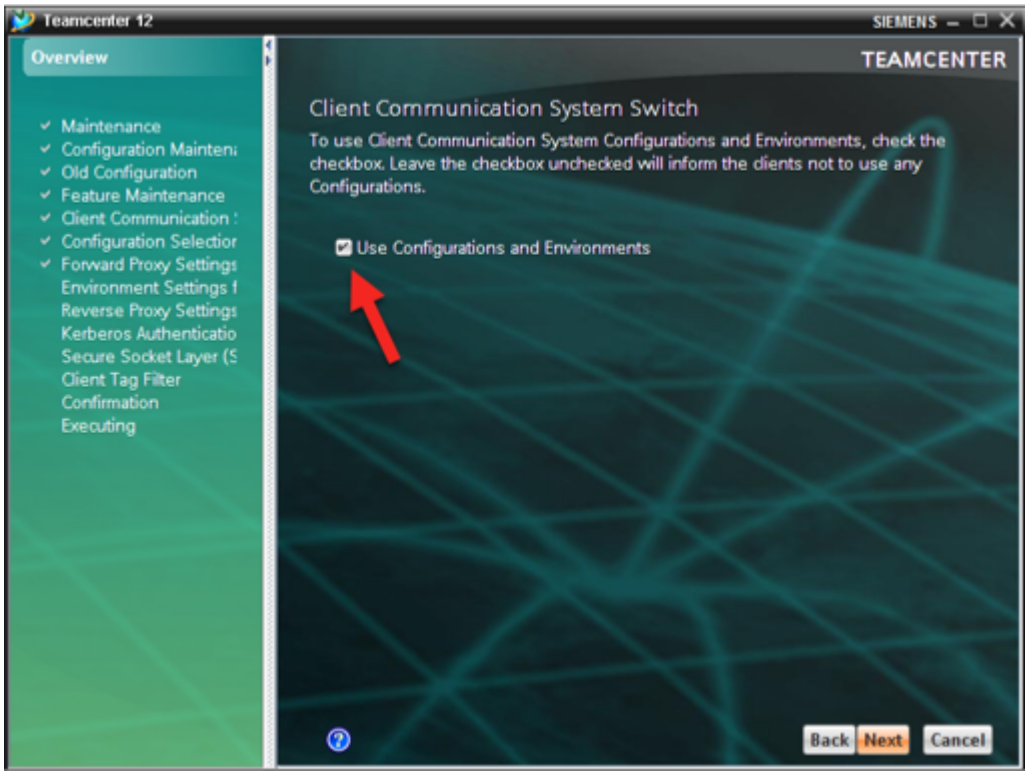
Client Communication System Use configurations and Environments

◉ Use configurations and Environments



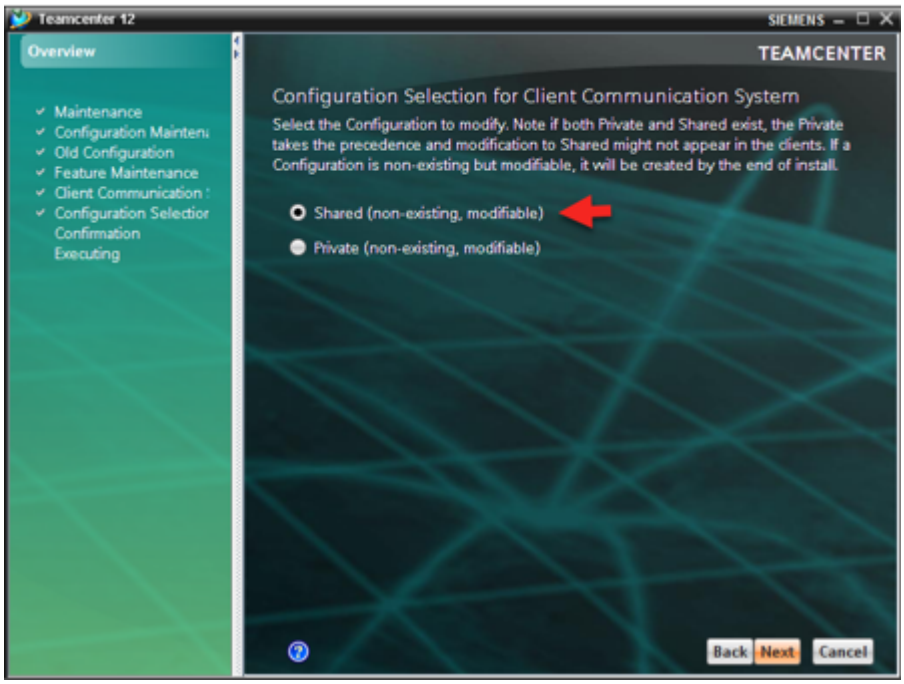
2.2 Client Communication System Switch

☑ Use Configuration and Environments



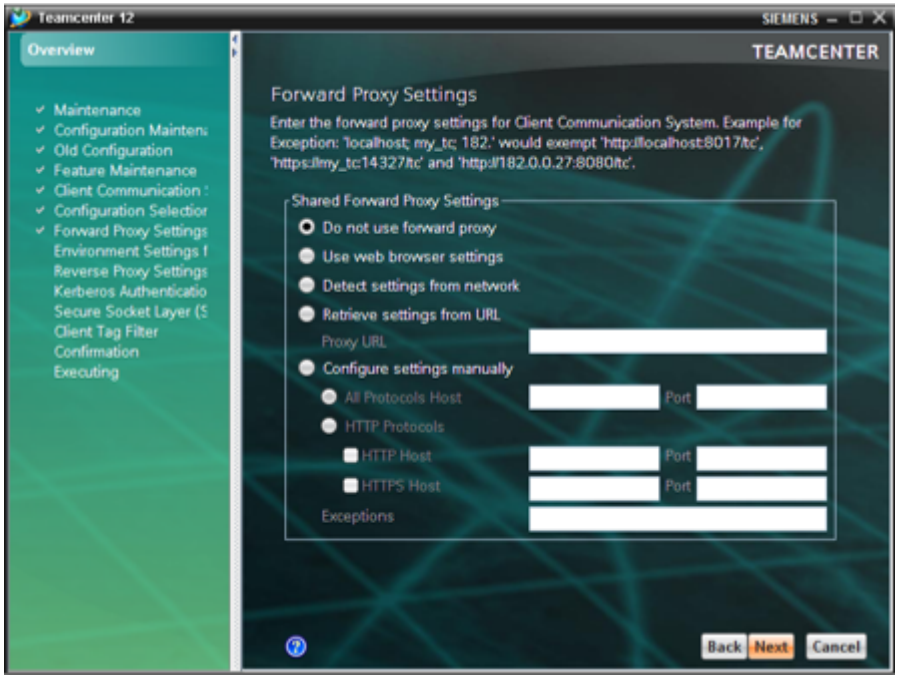
2.3 Configuration Selection for Client Communication System

◉ Shared (non-existing, modifiable)



2.4 Forward Proxy Settings

◉ Do not use forward proxy



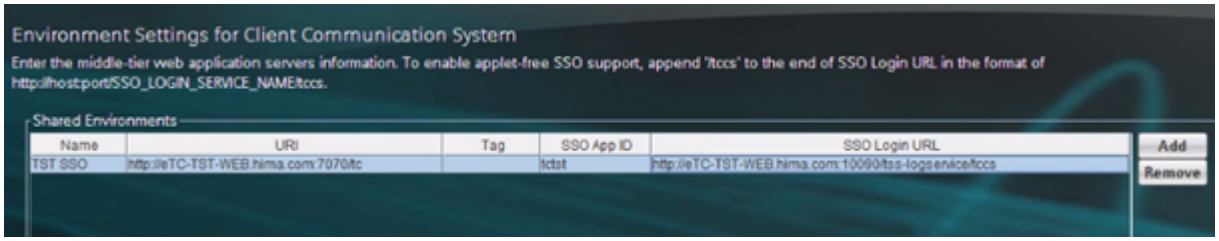
2.5 Environment Settings for Client Communication System

Add...

- Name: tcprod
- URI: http://avademo14:7070/tc
- Tag:
- SSO App ID:
- SSO Login URL:

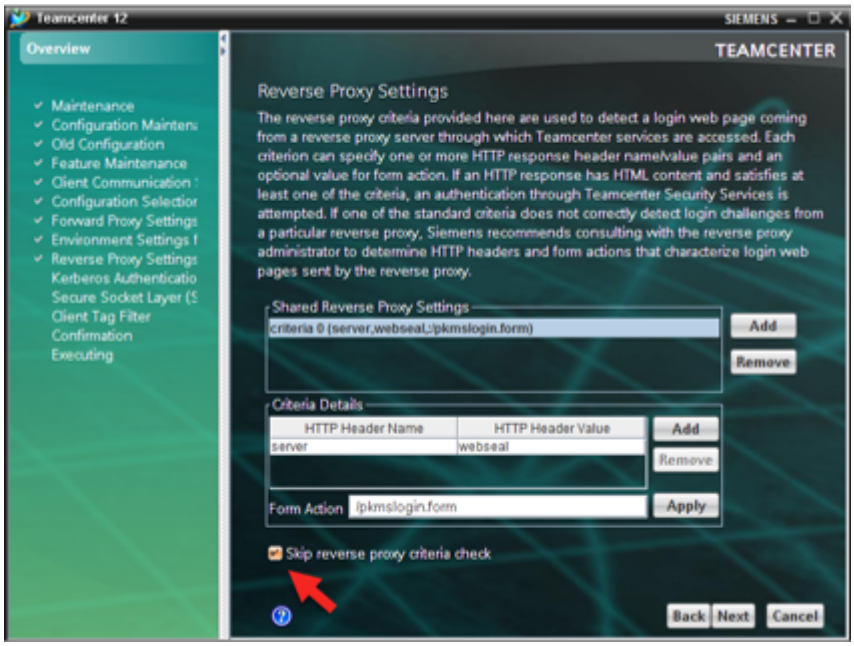
Add...

- Name: TST SSO
- URI: http://eTC-TST-WEB.hima.com:7070/tc
- Tag:
- SSO App ID: tctst
- SSO Login URL: http://eTC-TST-WEB.hima.com:10090/tss-logservice/tccs



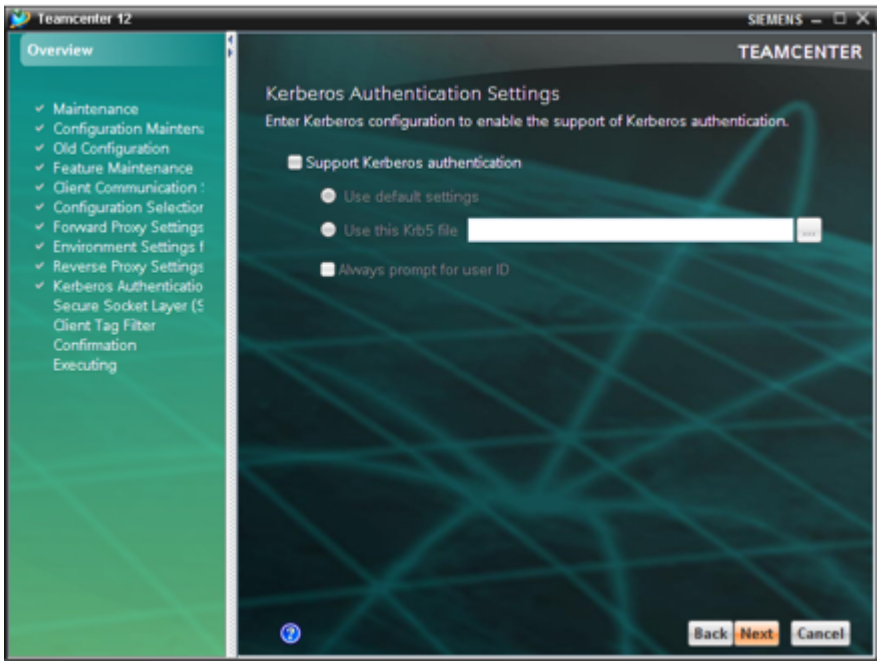
2.6 Reverse Proxy Settings

- ☑ Skip reverse proxy criteria check



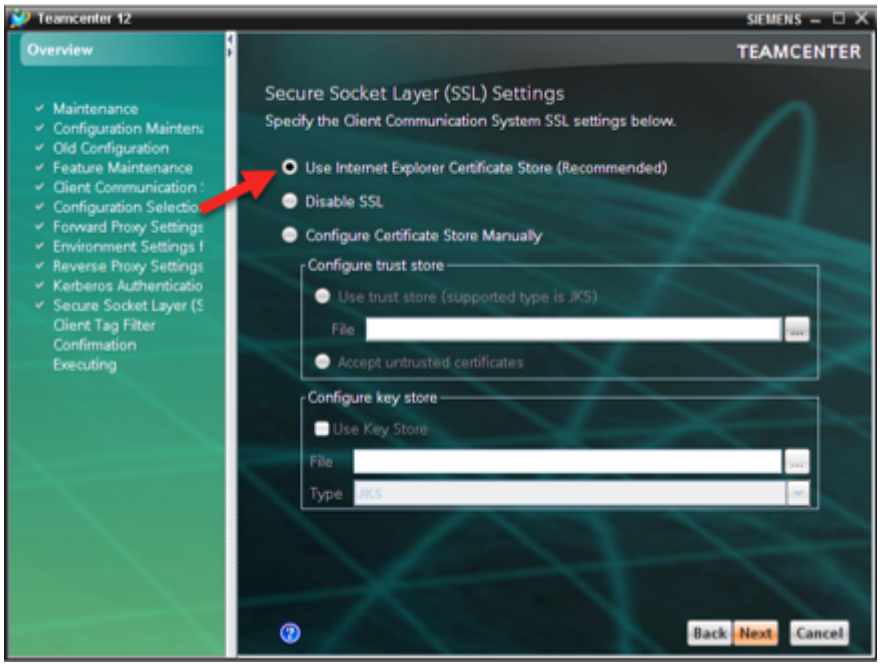
2.6 Kerberos Authentication Settings

Next...



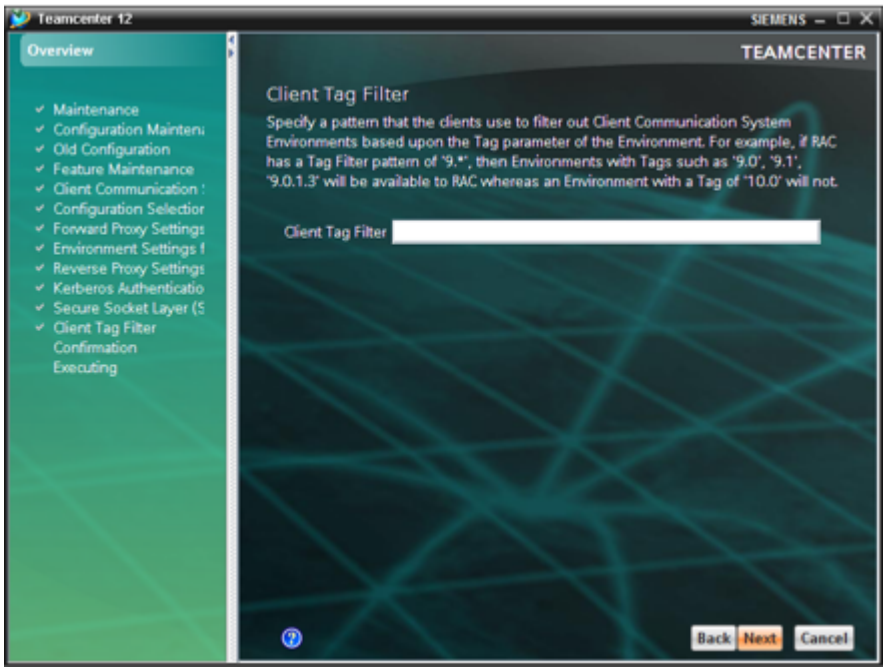
2.7 Secure Socket Layer (SSL) Settings

- ⦿ Use Internet Explorer Certificate Store (Recommended)

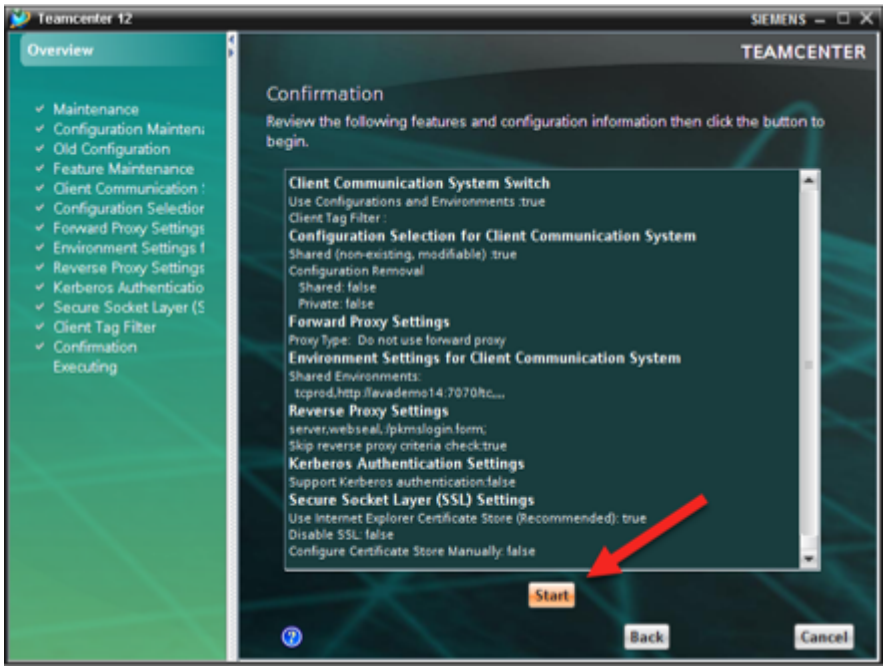


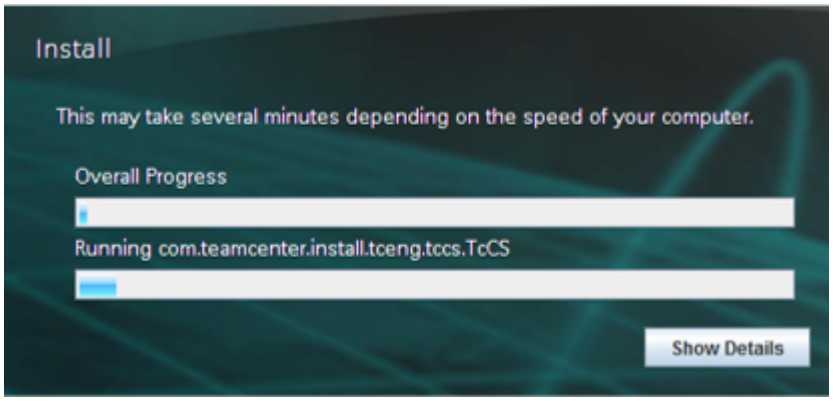
2.8 Client Tag Filter

Next...



Confirmation





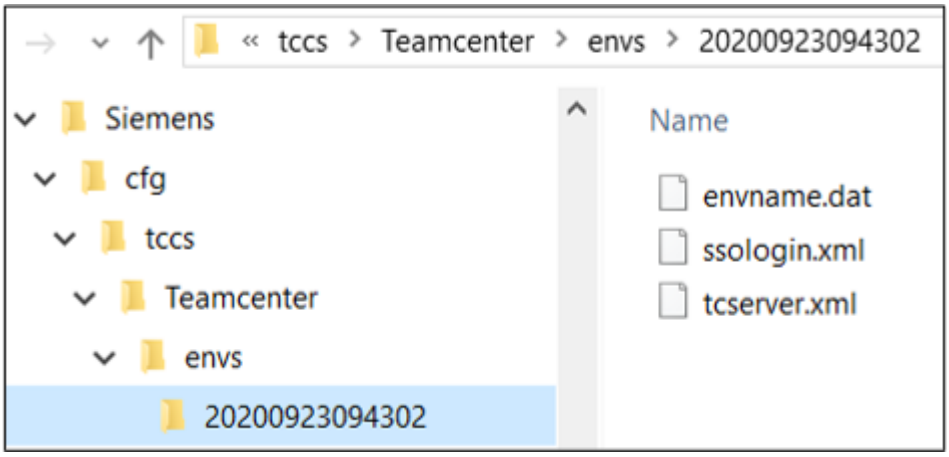
close

2.9 Ergebnis

In C:\plm\tc12\portal\plugins\configuration_12000.2.0\client_specific.properties

```
66  #
67  # Runtime and custom entries below this line
68  PortalViewer_Cache=C:/plm/tc12/portal/temp
69  PortalViewer_Optional_Licenses=Simplified_Rendering,ECAD,Concept
70  httpServerCount=1
71  portalCommunicationTransport=tccs
72  tccsVersionFilter=
73  jttoasciiCommand=C:/plm/tc12/jtutilities/bin/jttoascii
74  fileCacheEnabled=true
75  iiopServerCount=0
```

Siemens Ordner in C:\ProgramData\

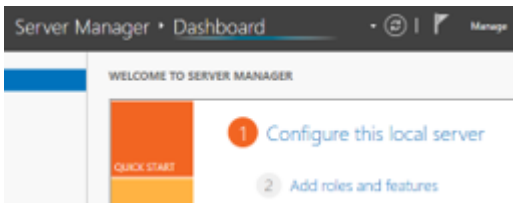


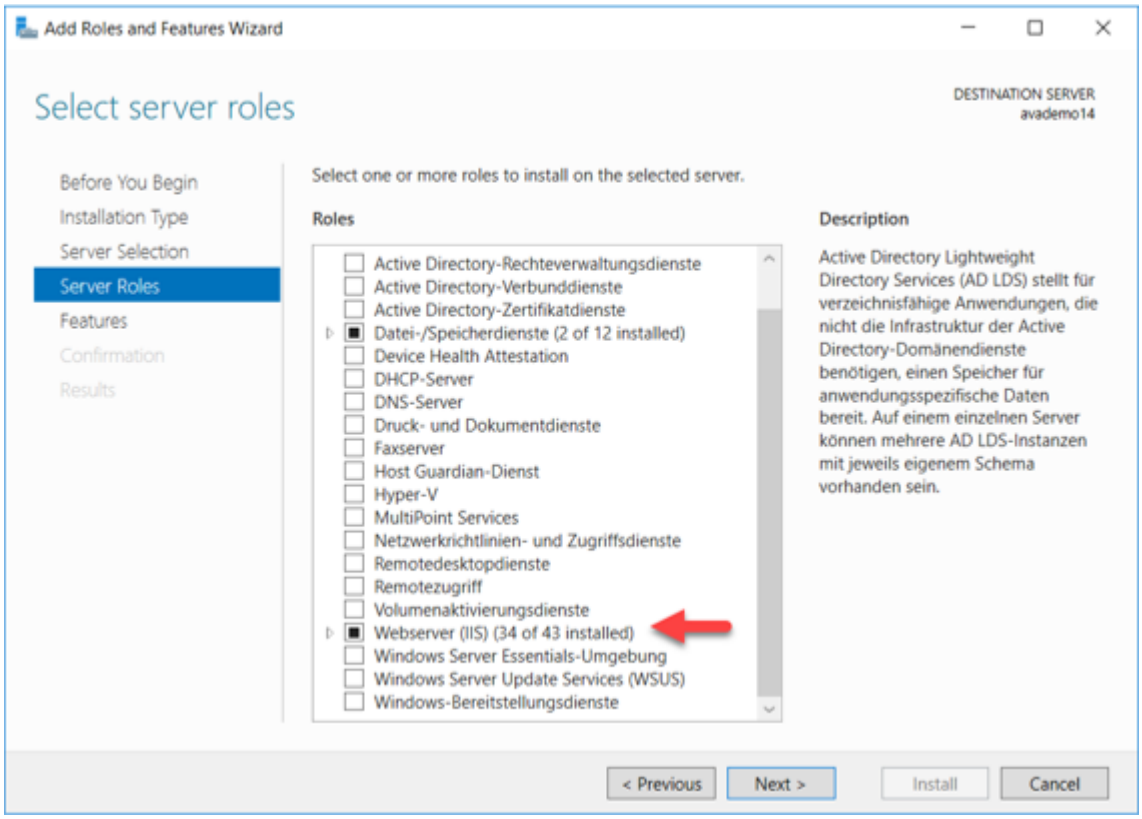
3. IIS auf Webserver konfigurieren

Die IIS Webserverkonfiguration wird wegen der Verifizierung Kerberos authentication benötigt.

3.1 IIS installieren

3.1.1 Configure Microsoft IIS





Common HTTP Features

- Default Document
- Directory Browsing
- HTTP Errors
- Static Content
- HTTP Redirection

Health and Diagnostics

- HTTP Logging
- Logging Tools
- Request Monitor
- Tracing

Performance

- Static Content Compression
- Dynamic Content Compression

Security

- Request Filtering
- Basic Authentication
- Client Certificate Mapping Authentication
- Digest Authentication
- IIS Client Certificate Mapping Authentication
- IP and Domain Restrictions
- URL Authorization
- Windows Authentication

Application Development

- .NET Extensibility 4.*x*
- ASP
- ASP.NET 4. *x*
- CGI
- ISAPI Extensions
- ISAPI Filters
- Server Side Includes

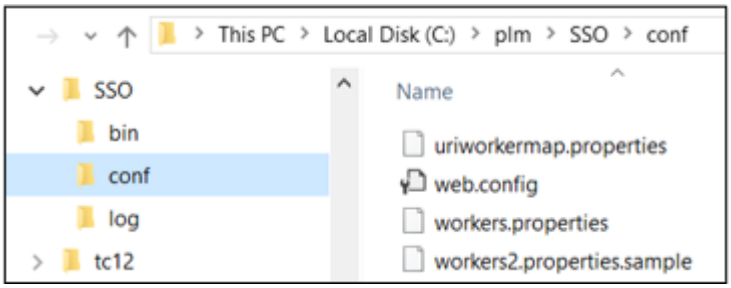
> Note
>
> Install only the available **ASP.NET 4.*x*** role services. Do not install ASP.NET 3.*x* role services.

Management Tools

- IIS Management Console

4. C:\plm\SSO einrichten

1. Ordner SSO von ... \avaCentralRepository\avaSSO\c\plm\SSO nach c:\plm kopieren



2. Pfade prüfen in: “C:\plm\SSO\bin\isapi_redirect.properties”

isapi_redirect.properties

```
# Configuration file for the Jakarta ISAPI Redirector

# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector
log_file=c:\plm\SSO\log\isapi_redirect.log

# Log level (debug, info, warn, error or trace)
log_level=error

# Full path to the workers.properties file
worker_file=c:\plm\SSO\conf\workers.properties

# Full path to the uriworkermap.properties file
worker_mount_file=c:\plm\SSO\conf\uriworkermap.properties
```

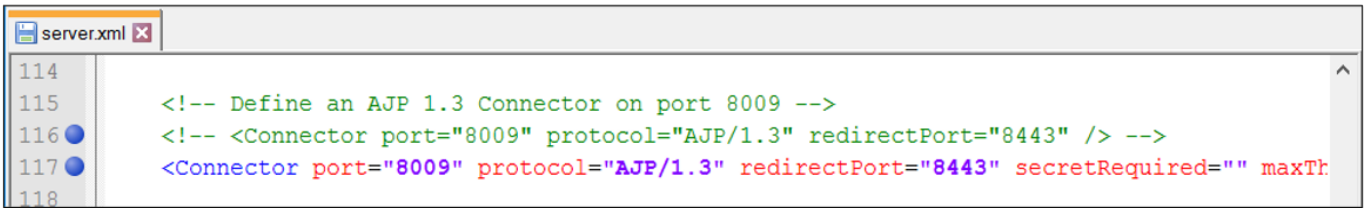
3. In “C:\plm\SSO\conf\workers.properties“ host anpassen

workers.properties

```
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to match.
#
worker.ajp13w.type=ajp13
worker.ajp13w.host=avademo14.hawaii.com
worker.ajp13w.port=8009
worker.ajp13w.max_packet_size=65536
```

5. Modify Tomcat server.xml

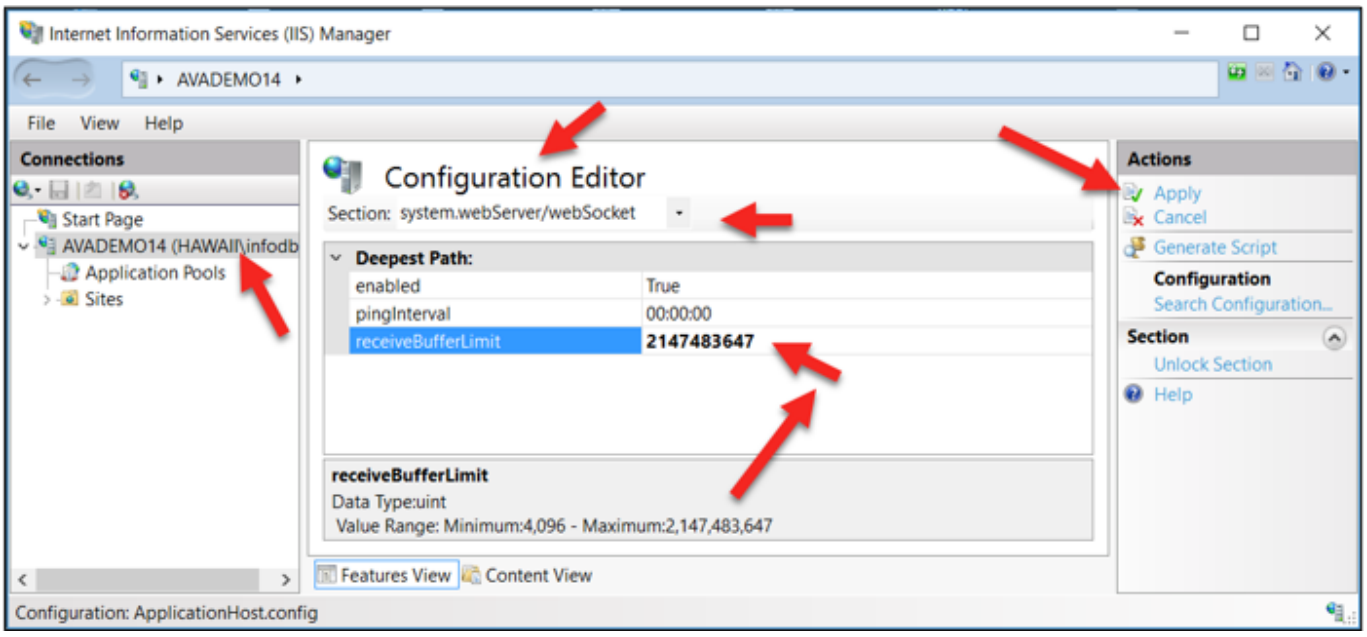
In “C:\plm\webapp\apache-tomcat-9.0.16\conf\server.xml“ anpassen:

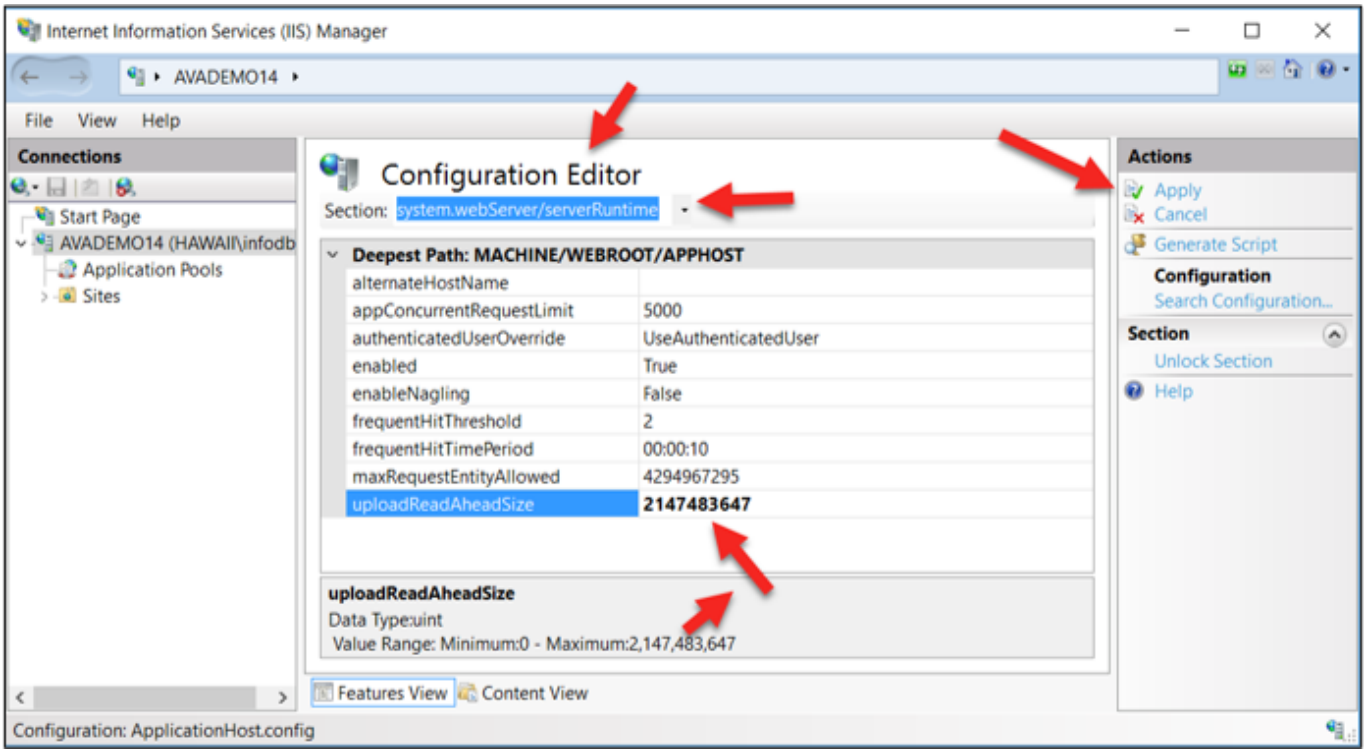



```
 <!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443"
secretRequired="" maxThreads="800" packetSize="65536" URIEncoding="UTF-8"
tomcatAuthentication="false"/>
```

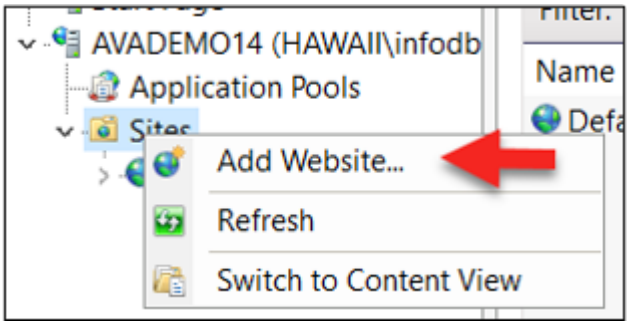
6. IIS konfigurieren

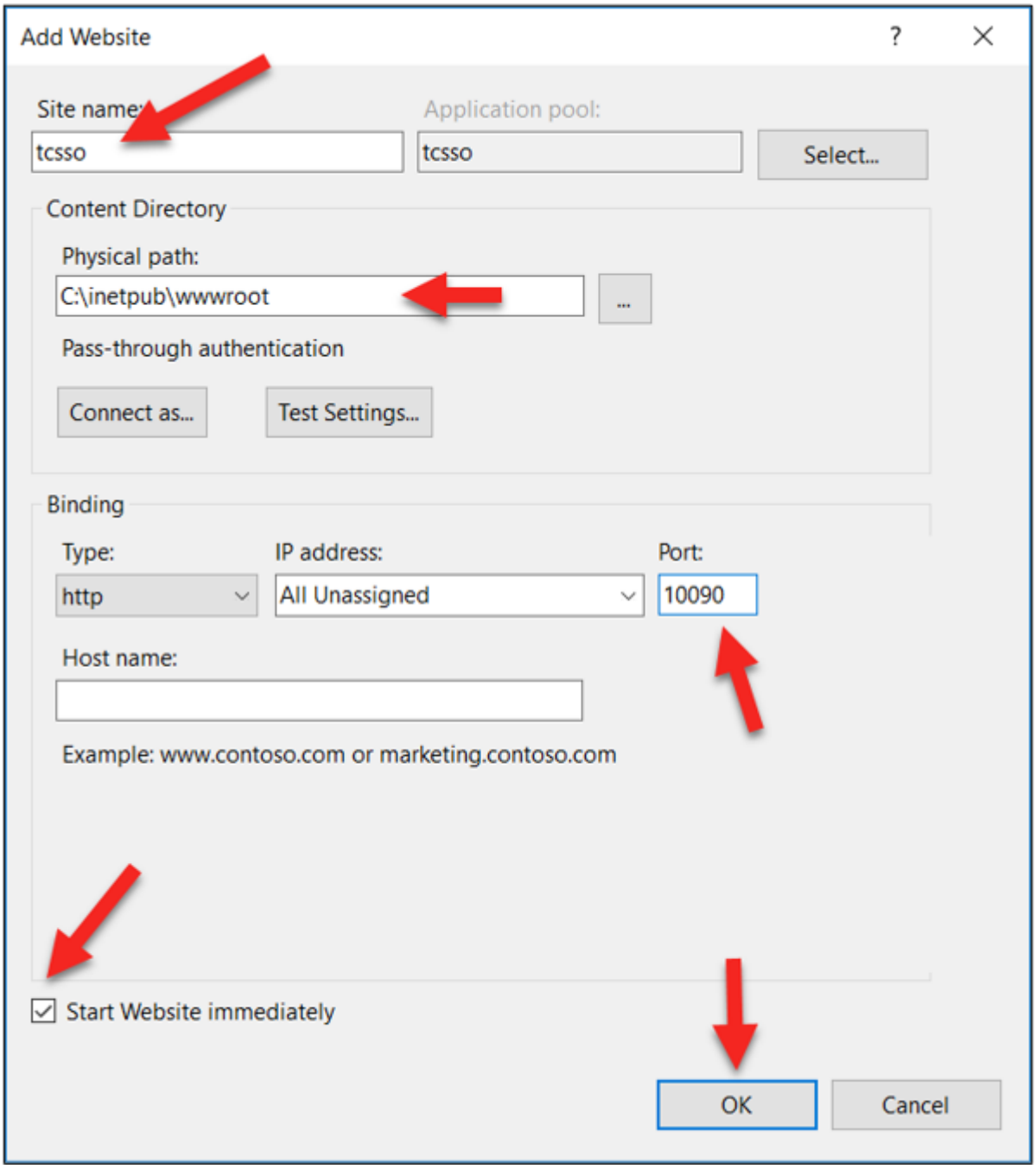
1. Configuration Editor



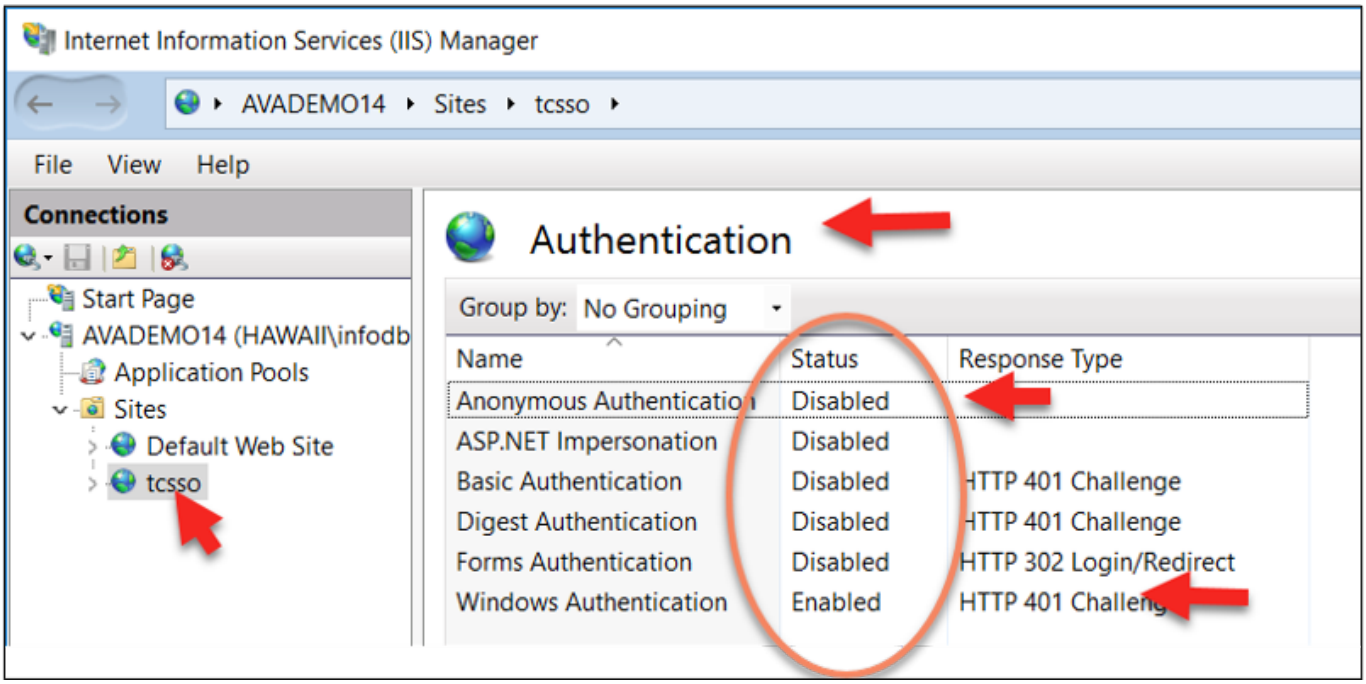


2. Website hinzufügen

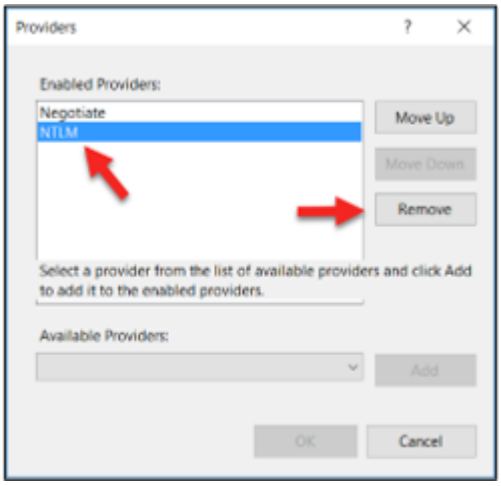




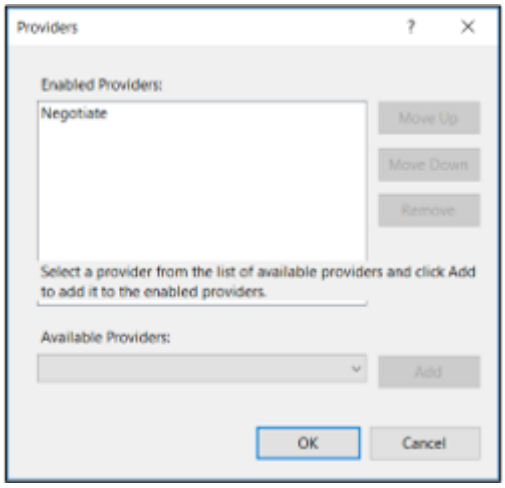
3. Remove NTLM



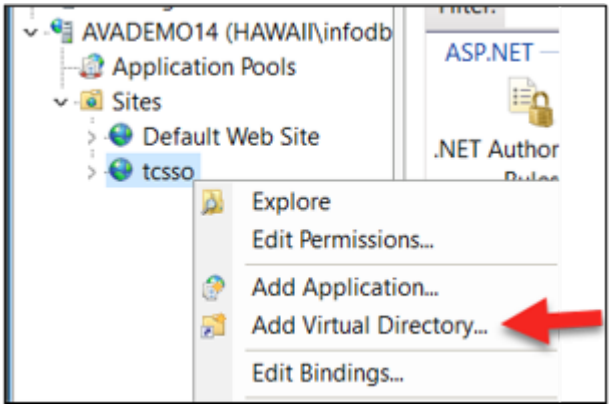
RMB Windows Authentication, Providers

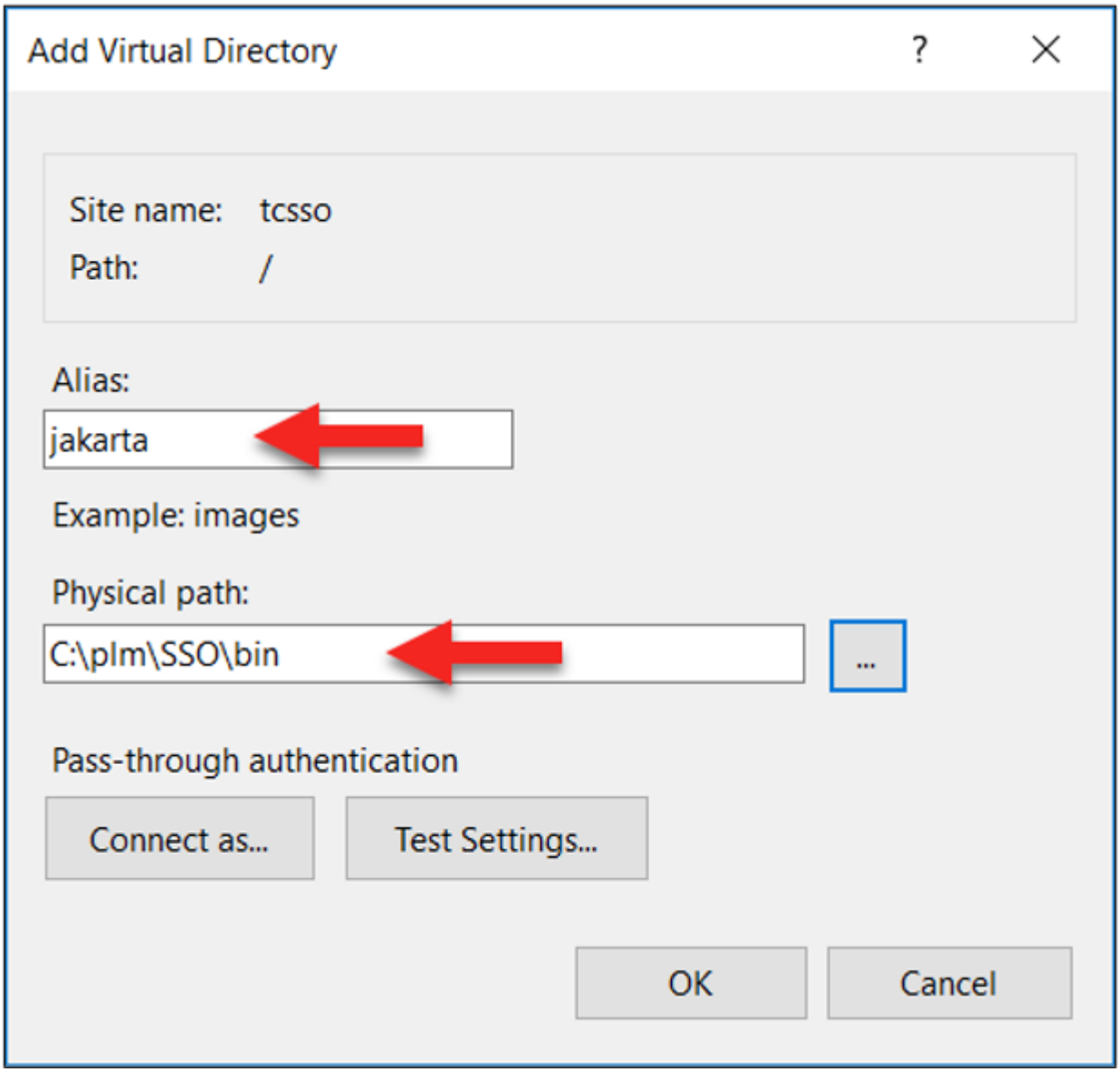


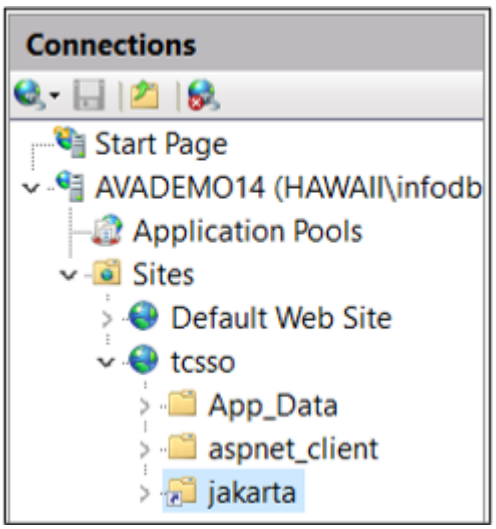
wird



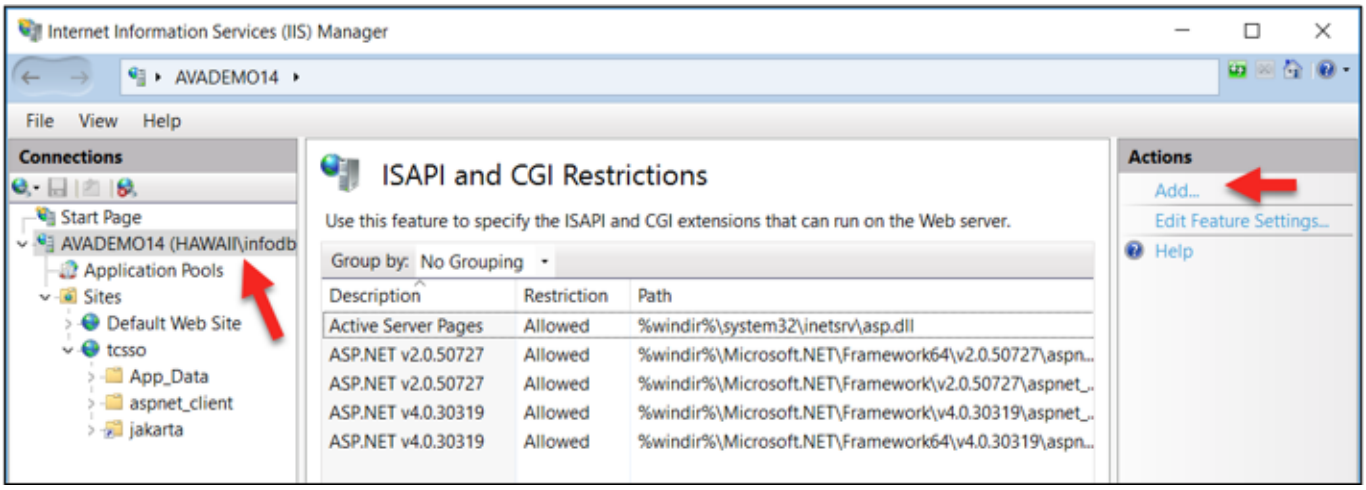
4. Virtuelle Verzeichnis hinzufügen

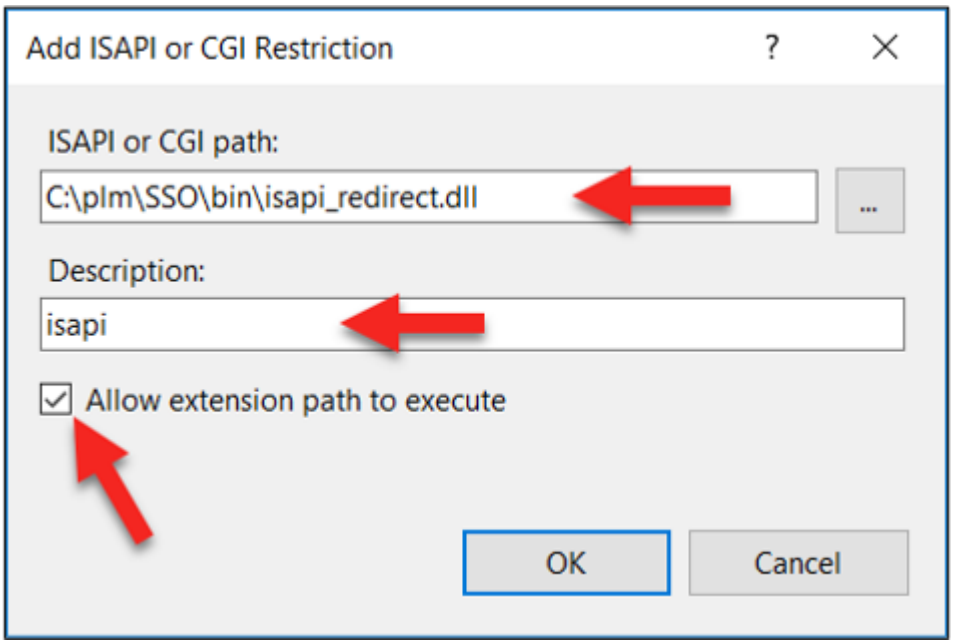


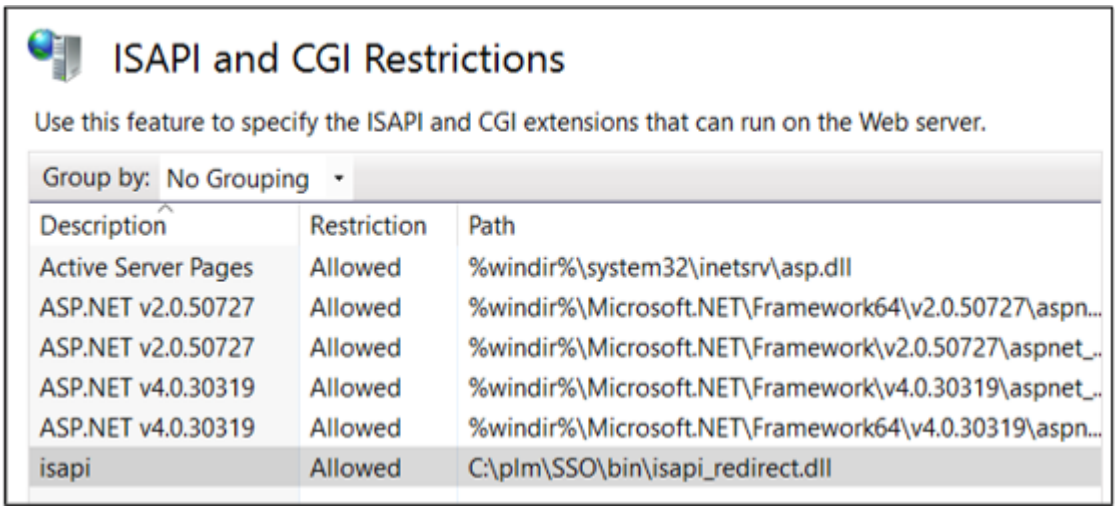




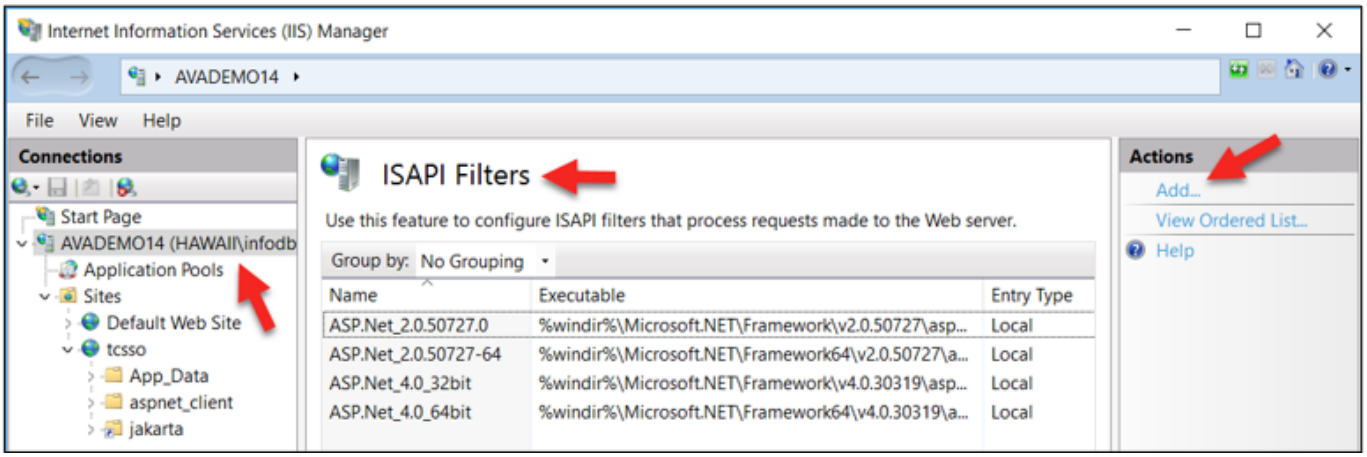
5. ISAPI and CGI Restrictions

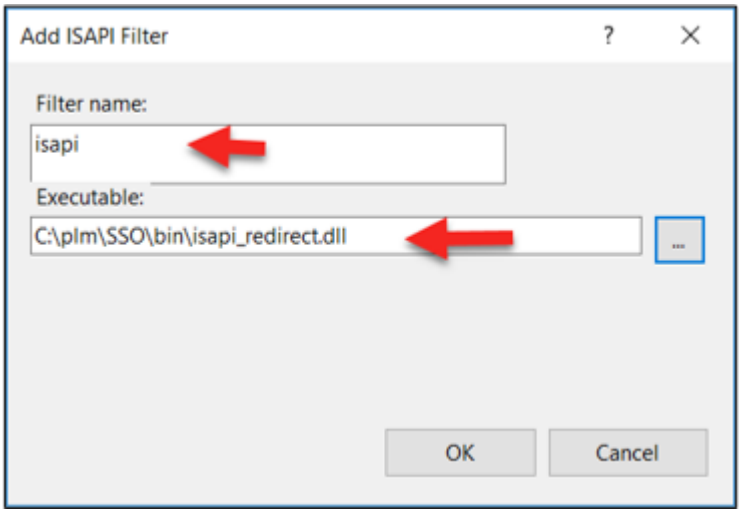


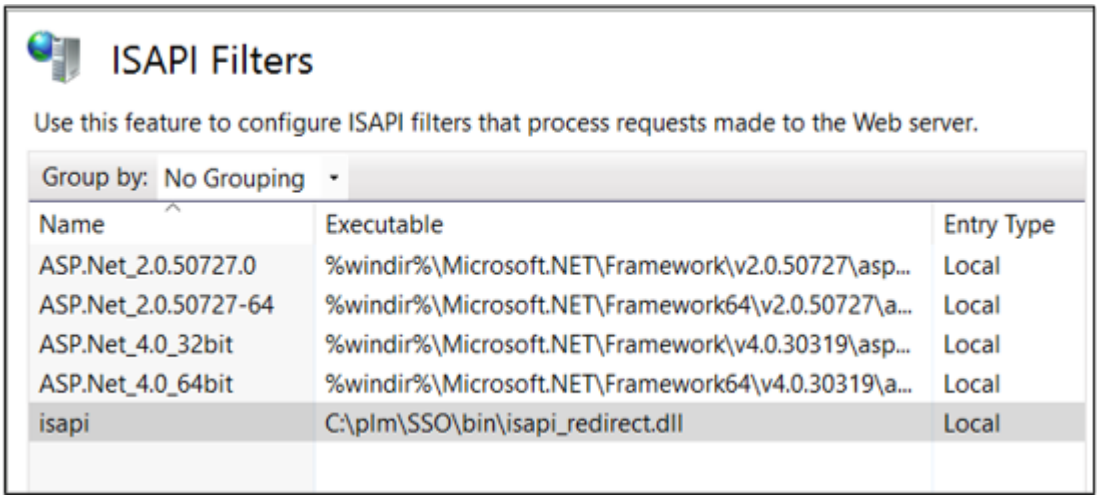


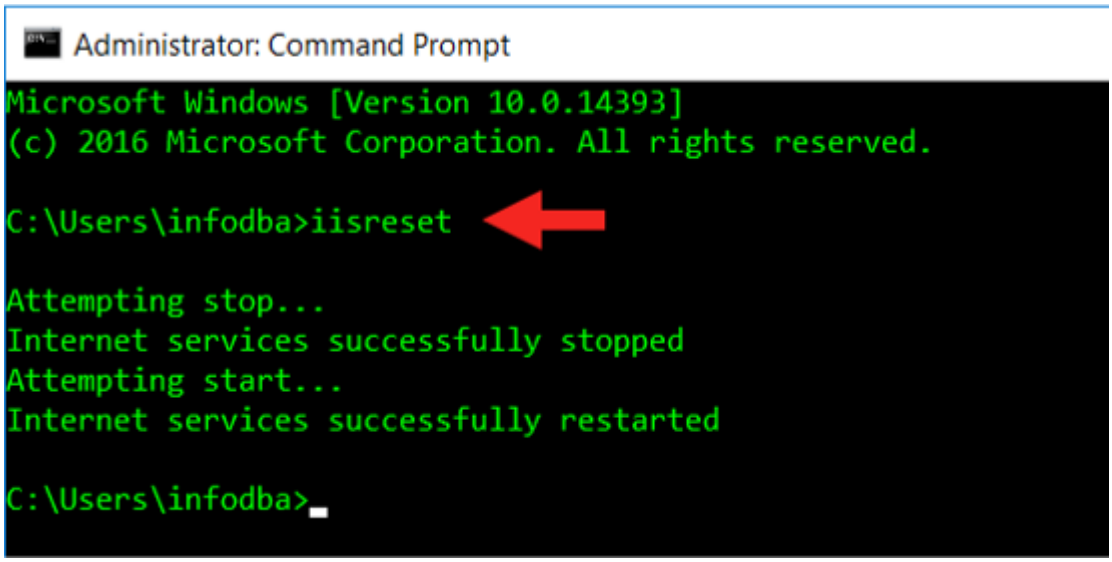


6. ISAPI-Filter


Internet Information Services (IIS) Manager
AVADEMO14
File View Help
Connections
Start Page
AVADEMO14 (HAWAII\infodb
Application Pools
Sites
Default Web Site
tcsso
App_Data
aspnet_client
jakarta
ISAPI Filters
Use this feature to configure ISAPI filters that process requests made to the Web server.
Group by: No Grouping
Name Executable Entry Type
ASP.Net_2.0.50727.0 %windir%\Microsoft.NET\Framework\v2.0.50727\asp... Local
ASP.Net_2.0.50727-64 %windir%\Microsoft.NET\Framework64\v2.0.50727\a... Local
ASP.Net_4.0_32bit %windir%\Microsoft.NET\Framework\v4.0.30319\asp... Local
ASP.Net_4.0_64bit %windir%\Microsoft.NET\Framework64\v4.0.30319\a... Local
Actions
Add...
View Ordered List...
Help

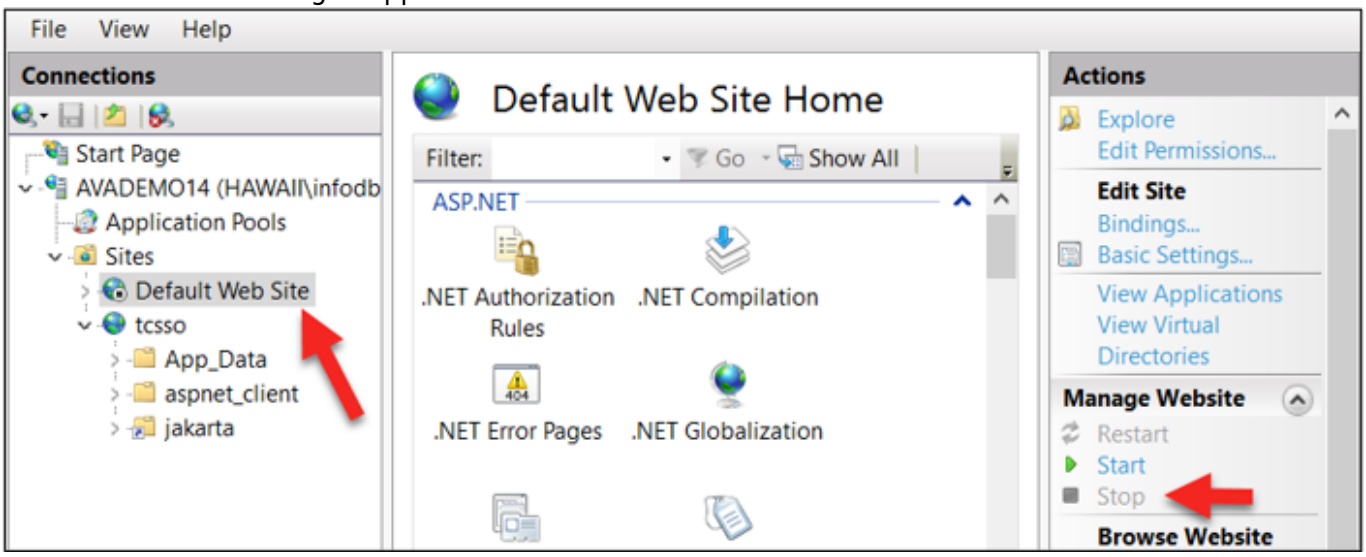

Add ISAPI Filter
Filter name:
isapi
Executable:
C:\plm\SSO\bin\isapi_redirect.dll
...
OK
Cancel


ISAPI Filters
Use this feature to configure ISAPI filters that process requests made to the Web server.
Group by: No Grouping
Name Executable Entry Type
ASP.Net_2.0.50727.0 %windir%\Microsoft.NET\Framework\v2.0.50727\asp... Local
ASP.Net_2.0.50727-64 %windir%\Microsoft.NET\Framework64\v2.0.50727\a... Local
ASP.Net_4.0_32bit %windir%\Microsoft.NET\Framework\v4.0.30319\asp... Local
ASP.Net_4.0_64bit %windir%\Microsoft.NET\Framework64\v4.0.30319\a... Local
isapi C:\plm\SSO\bin\isapi_redirect.dll Local

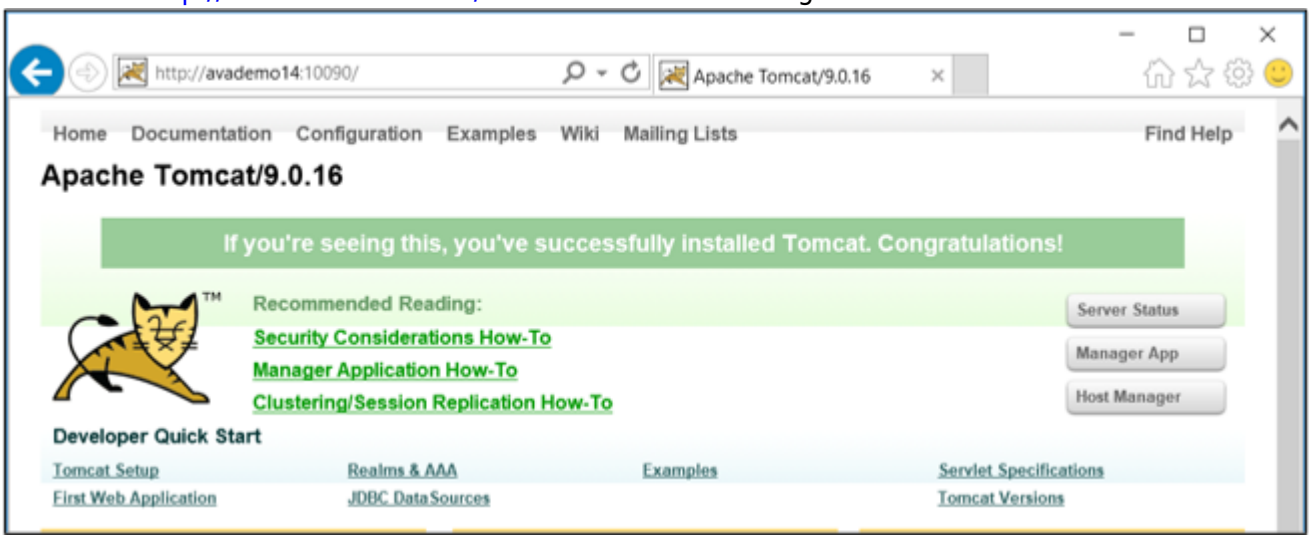


7. Default Web Site deaktivieren

Bleibt auch bei Reboot gestoppt...



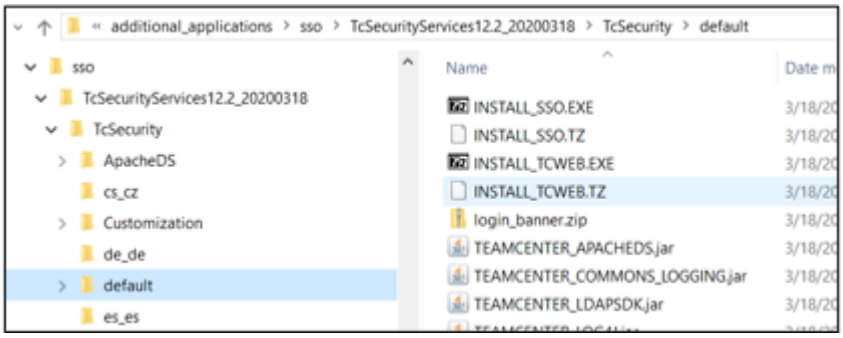
IIS testen: http://avademo14:10090/ IIS wird auf Tomcat umgeleitet



7. Installing Security Services

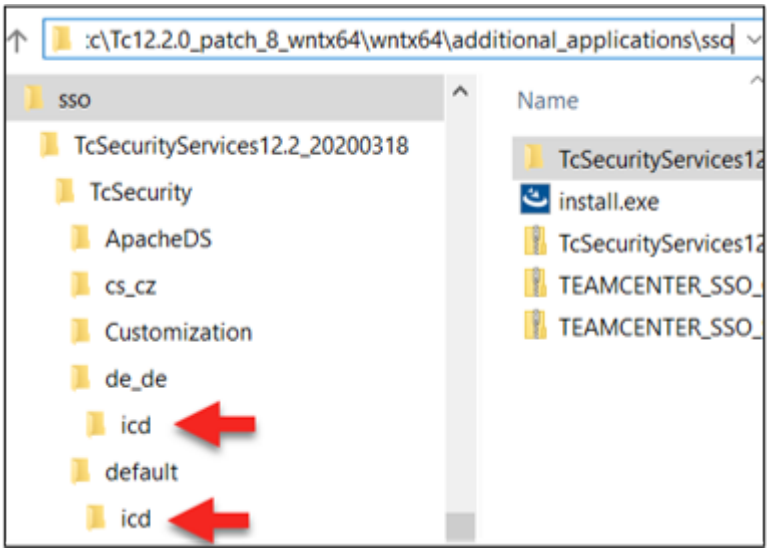
7.1 SSO Sources vorbereiten

In aktuell installiertem Patch, z.B.
...\Tc12.2.0_patch_8_wntx64\wntx64\additional_applications\sso\TcSecurityServices12.2_20200318.zip
entpacken:



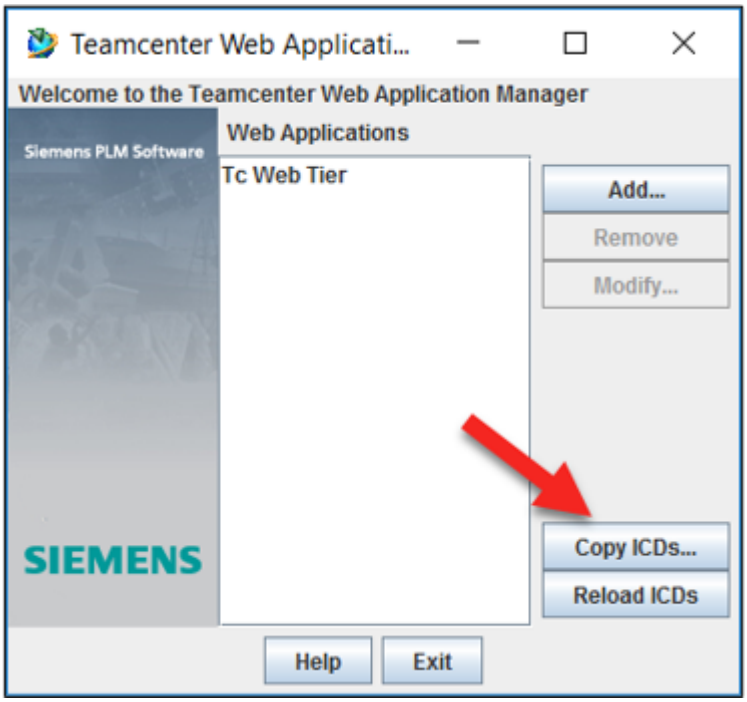
Folgendes ausführen:
...\wntx64\additional_applications\sso\TcSecurityServices12.2_xx\TcSecurity\default\INSTALL_SSO.EXE
...\wntx64\additional_applications\sso\TcSecurityServices12.2_xx\TcSecurity\de_de\INSTALL_SSO_DE_DE.EXE

Ergebnis: icd Folders

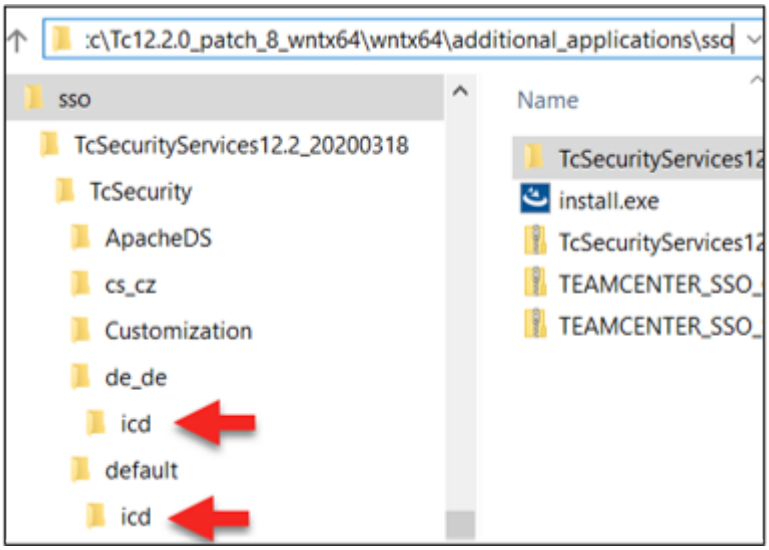


7.2 SSO ICD kopieren

Start “C:\plm\web_tier\insweb.bat«



Zuvor extrahierte ICD einlesen

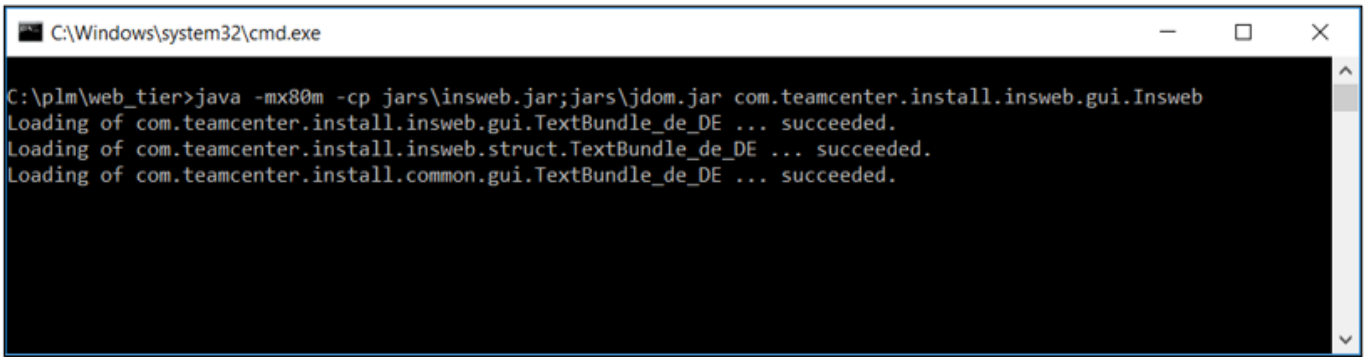


8. Tss-logiservice erstellen

8.1 Create the Login Service

1. Start the Web Application Manager

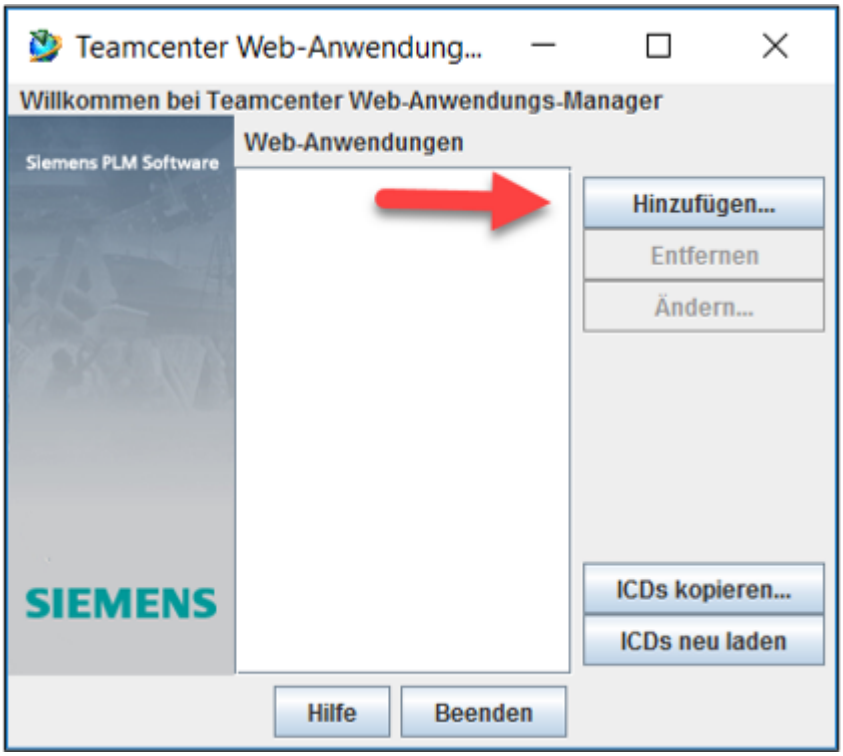
- c:\plm\web_tier\insweb.bat



Java must be installed...

Teamcenter Web-Anwendungs-Manager

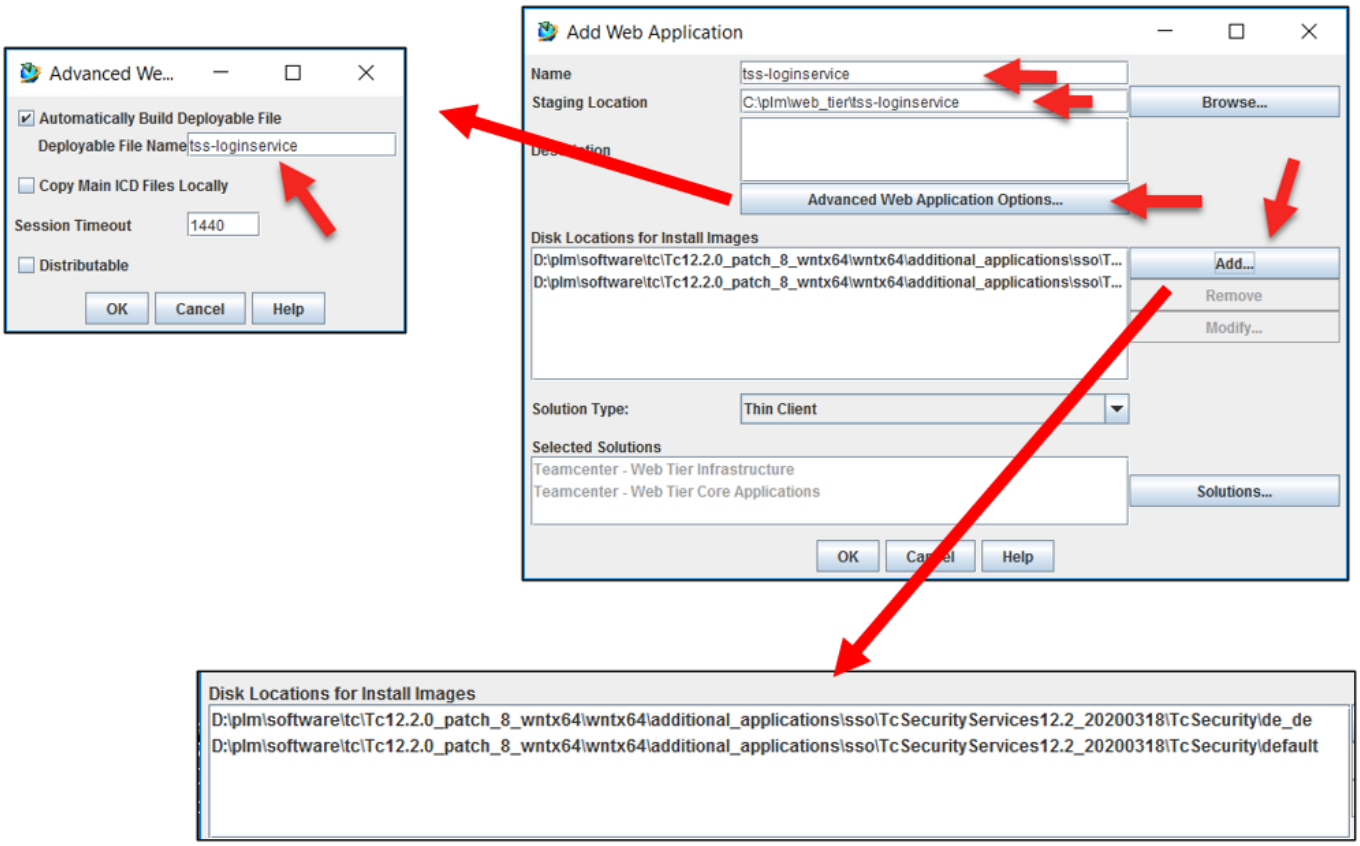
- Select: **Hinzufügen...**



2. Add Web Application

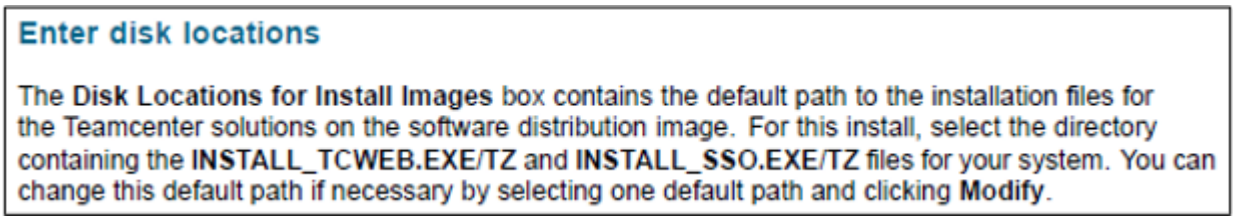
- Name: tss-loginservice
- Staging Location: c:\plm\web_tier\tss-loginservice
- Advanced Web Application Options...

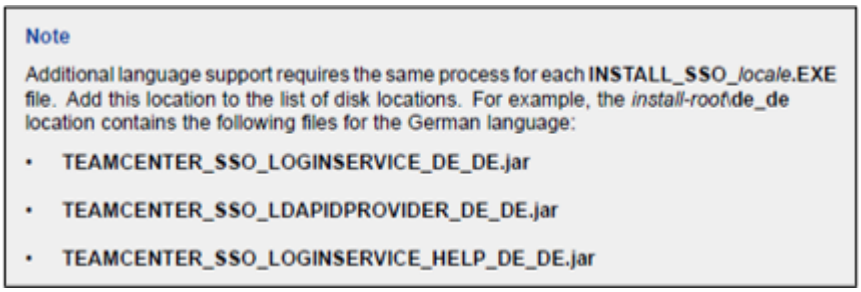
Zu verwendende Datei: tss-loginservice



3. Disk Locations for Install Images

- Add...

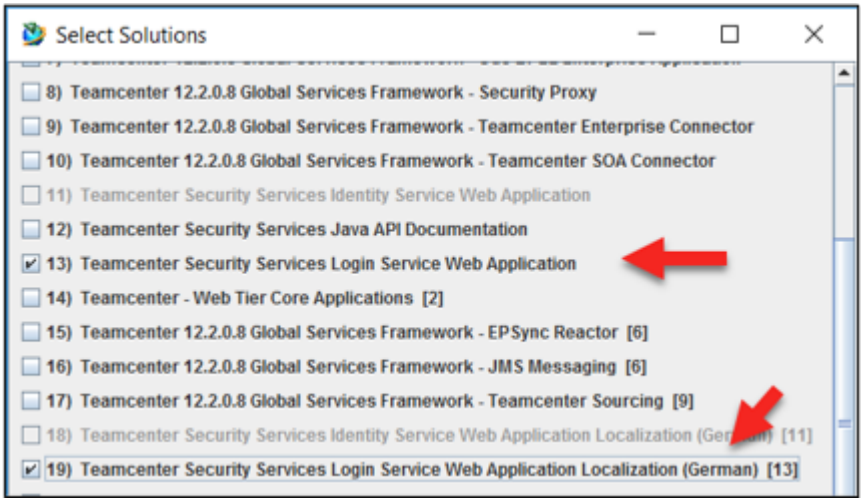




4. Solution Typ: → Thin Client

5. Selected Solutions

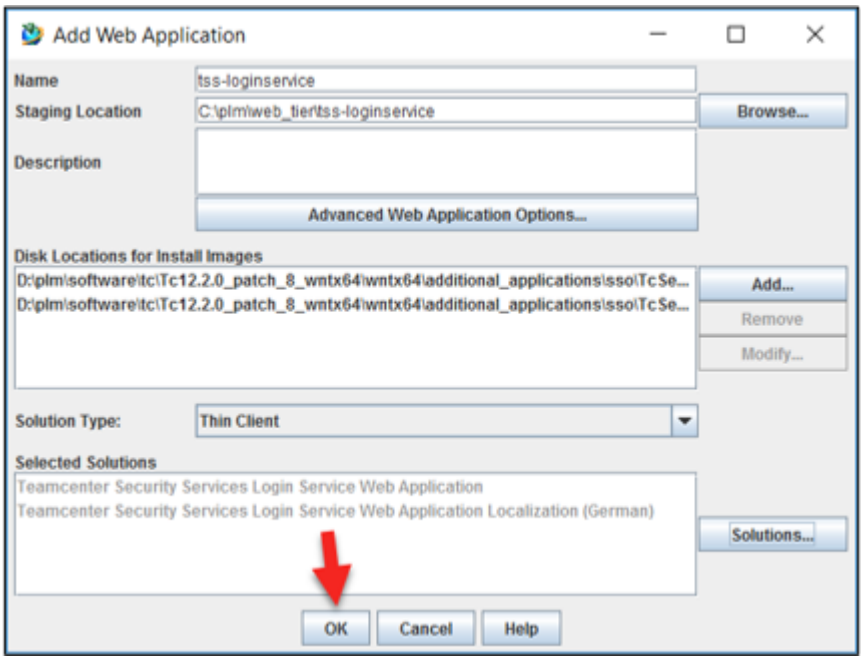
- Select the following:
  - **Security Services Login Service Web Application** (required)
  - **Language** (optional)



- Confirm with: OK

6. Terminate Add Web Application

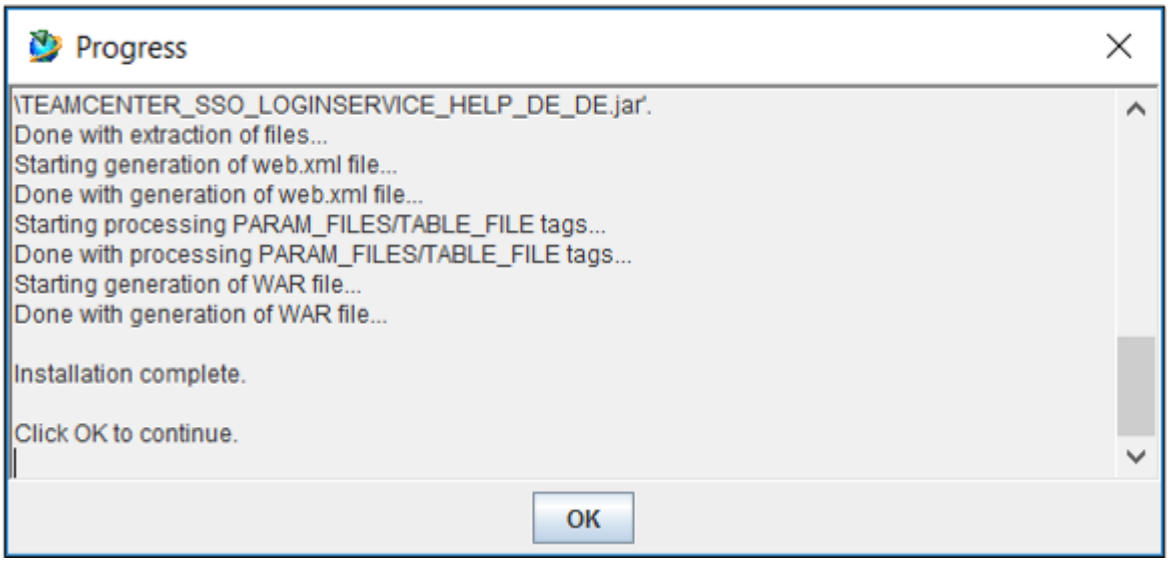
- Check entries...



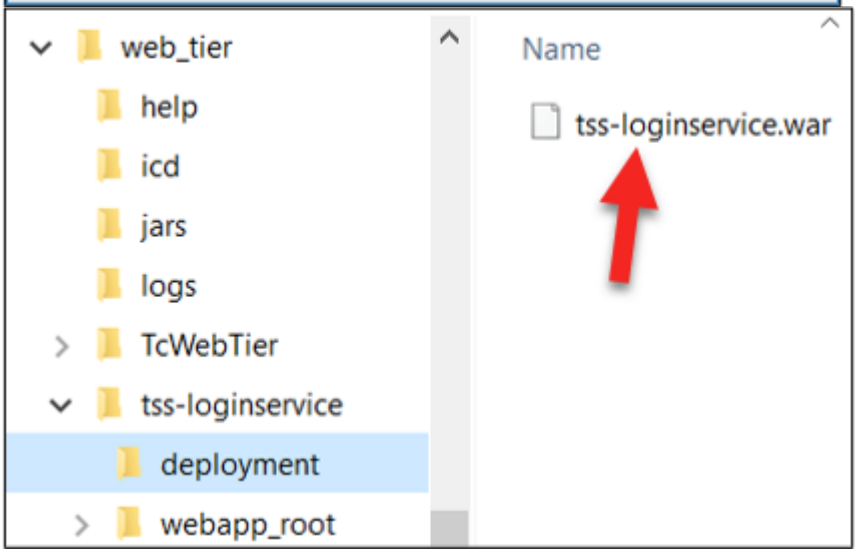
- Confirm with: OK

7. Progress:

- Confirm with: OK


Progress
\TEAMCENTER_SSO_LOGINSERVICE_HELP_DE_DE.jar'.
Done with extraction of files...
Starting generation of web.xml file...
Done with generation of web.xml file...
Starting processing PARAM_FILES/TABLE_FILE tags...
Done with processing PARAM_FILES/TABLE_FILE tags...
Starting generation of WAR file...
Done with generation of WAR file...
Installation complete.
Click OK to continue.
OK


Teamcenter Web-Anwendung...
Willkommen bei Teamcenter Web-Anwendungs-Manager
Siemens PLM Software
Web-Anwendungen
Tc Login Service
Hinzufügen...
Entfernen
Ändern...
ICDs kopieren...
ICDs neu laden
SIEMENS
Hilfe
Beenden

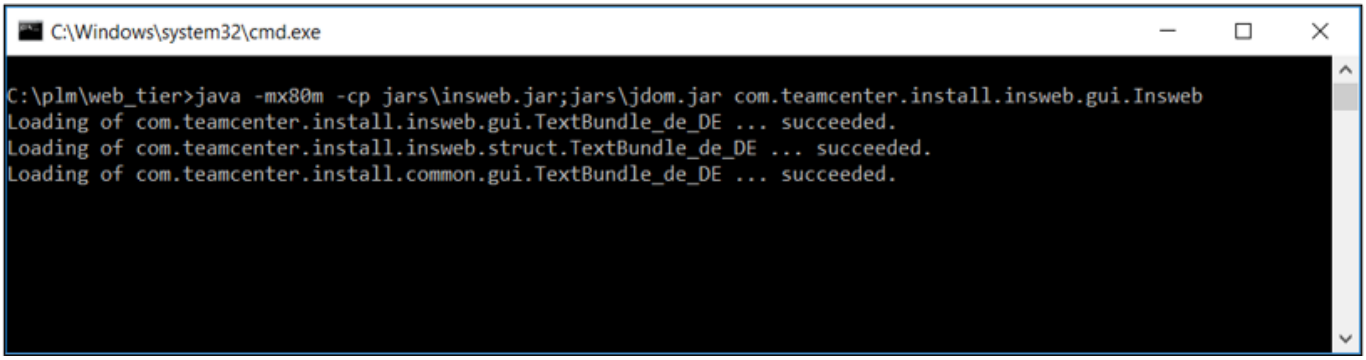

web_tier
help
icd
jars
logs
TcWebTier
tss-loginservice
deployment
webapp_root
Name
tss-loginservice.war

9. Tss-idservice erstellen

9.1 Create the Identity Service

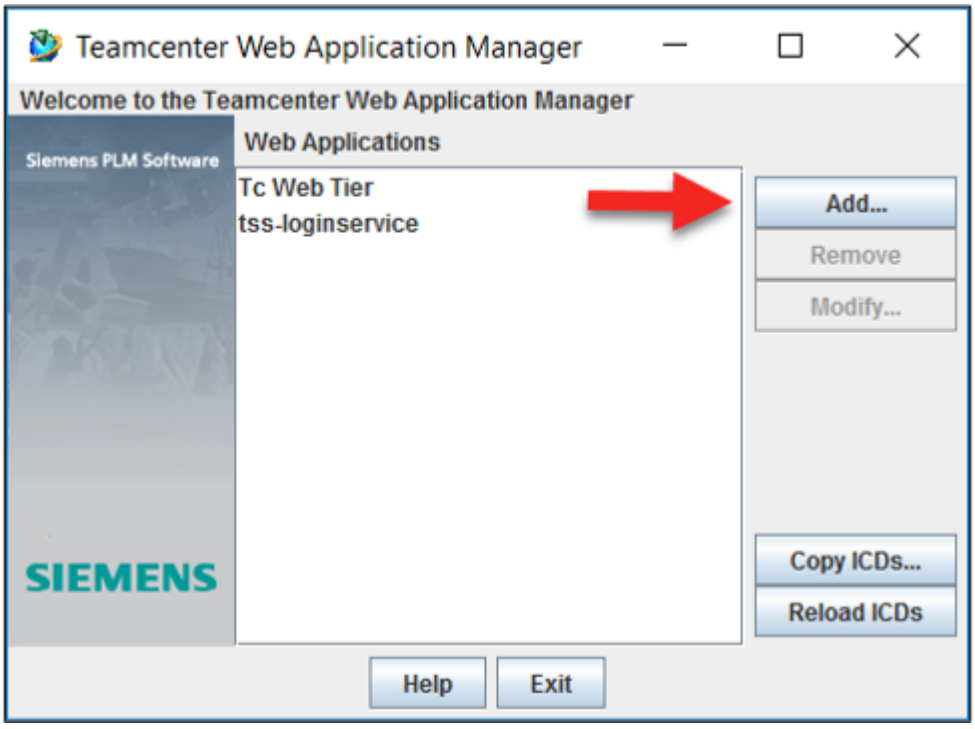
1. Start the Web Application Manager

- c:\plm\web_tier**insweb.bat**



Teamcenter Web-Anwendungs-Manager

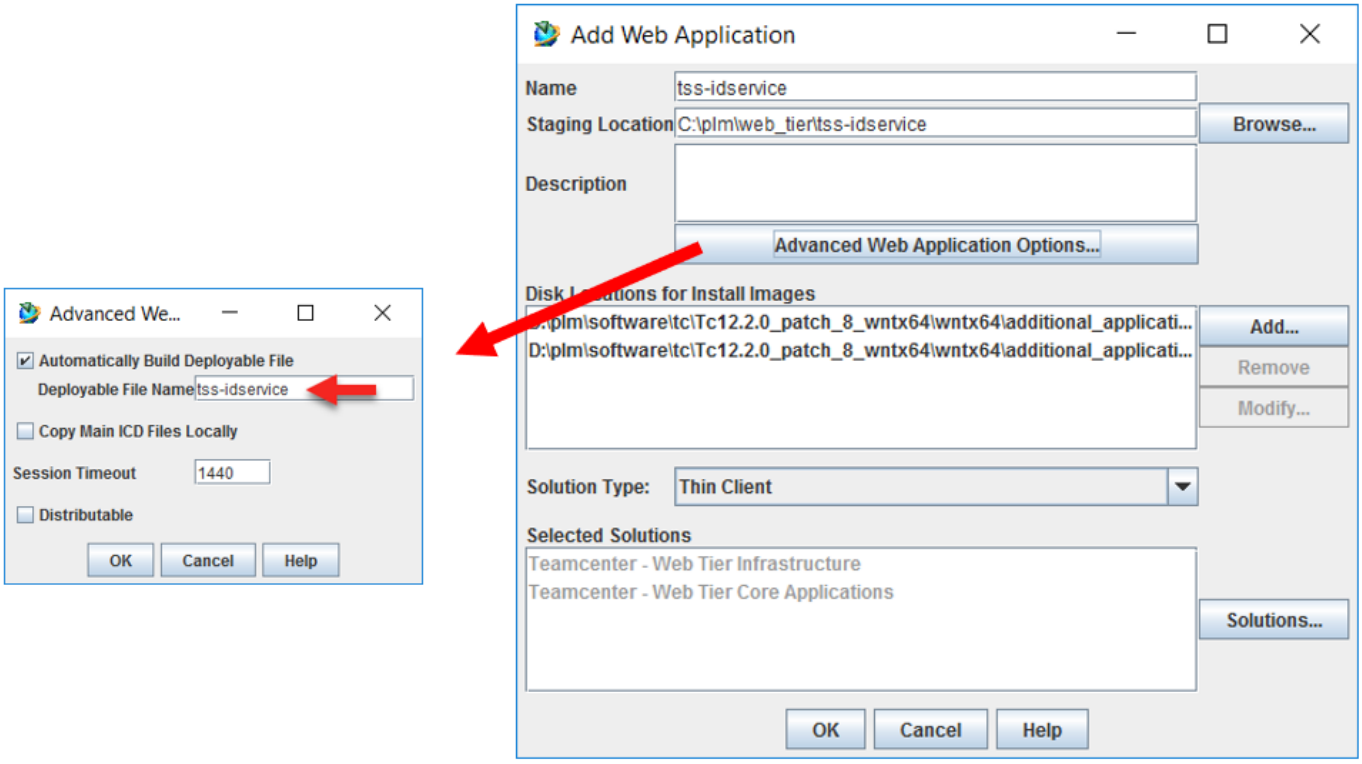
- Select: **Hinzufügen...**



Add Web Application

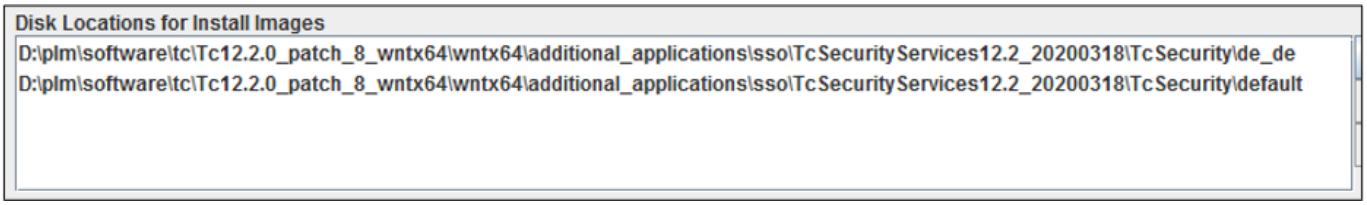
- Name: tss-idservice
- Staging Location: c:\plm\web_tier\tss-idservice
- Advanced Web Application Options...

Zu verwendende Datei: tss-idservice



2. Disk Locations for Install Images

- Add...

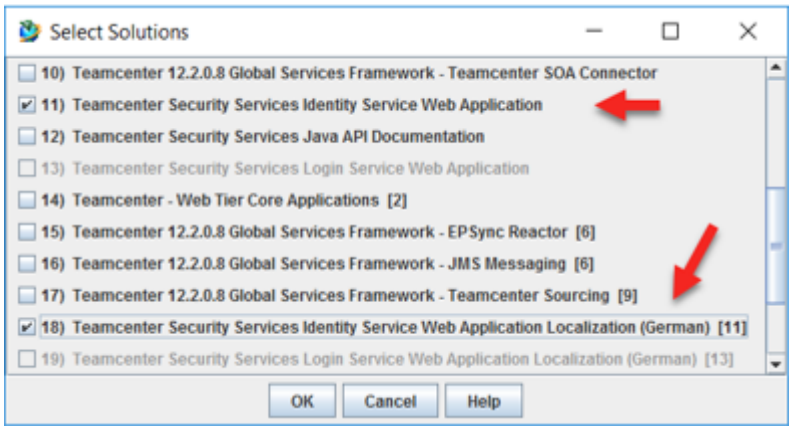


3. Solution Typ: → Thin Client

4. Selected Solutions

Select the following:

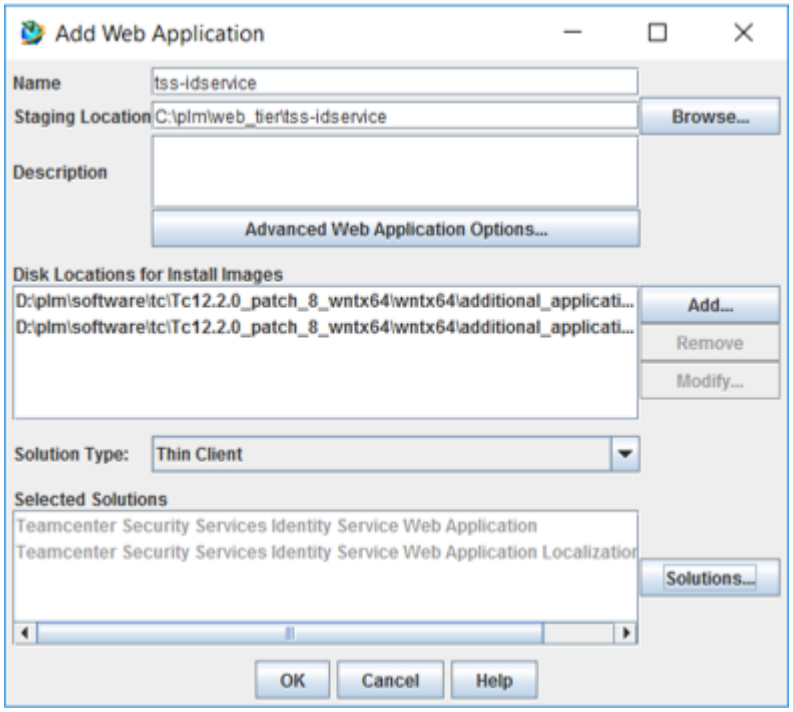
- **TC Security Services Identity Service Web Application** (requiered)
- **Language** (optional)



- Confirm with: OK

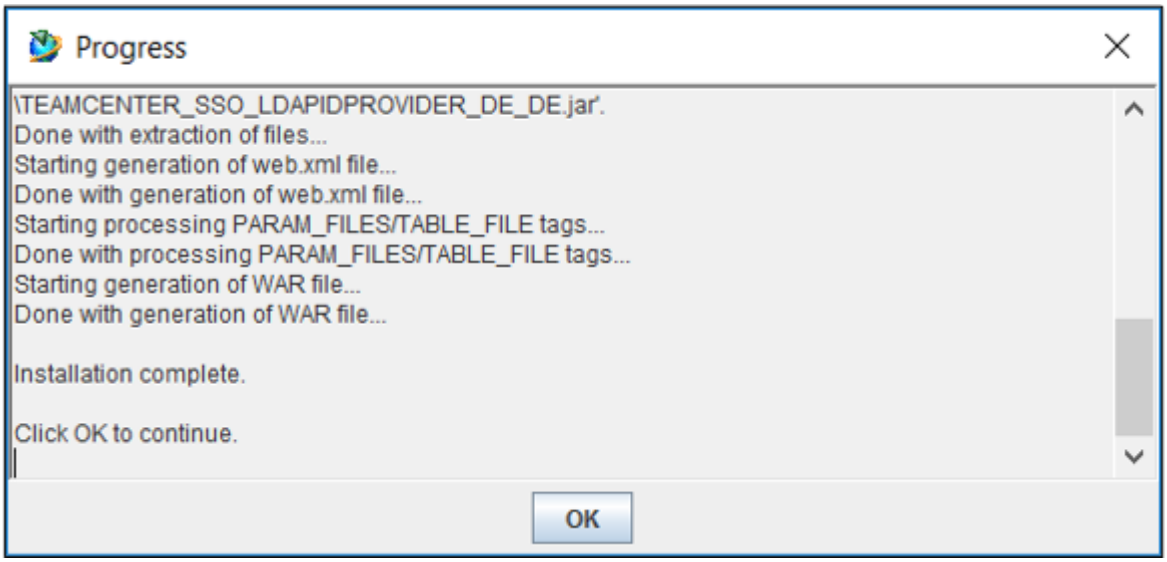
Terminate Add Web Application

- Check entries...

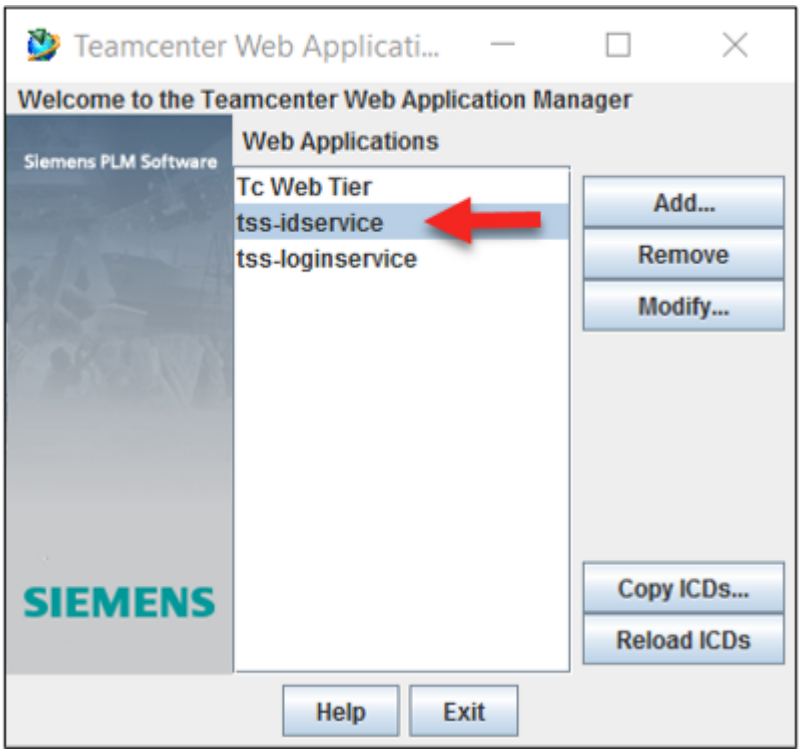


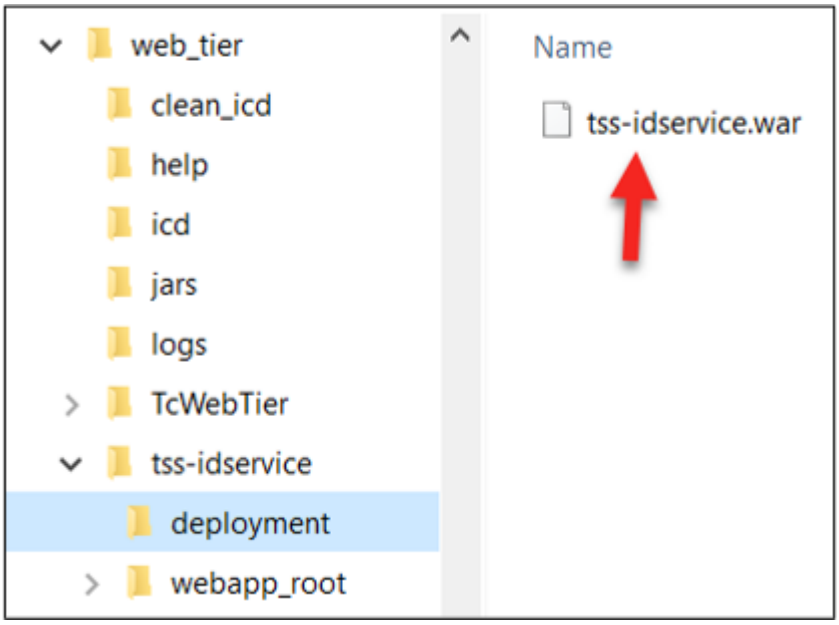
- Confirm with: OK

5. Progress:



- Confirm with: **OK**

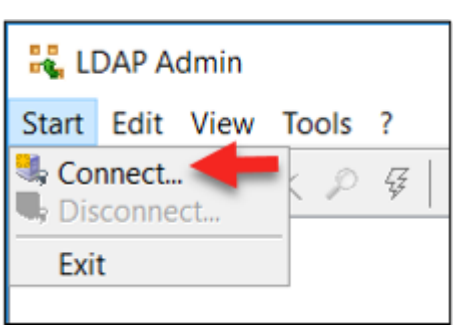


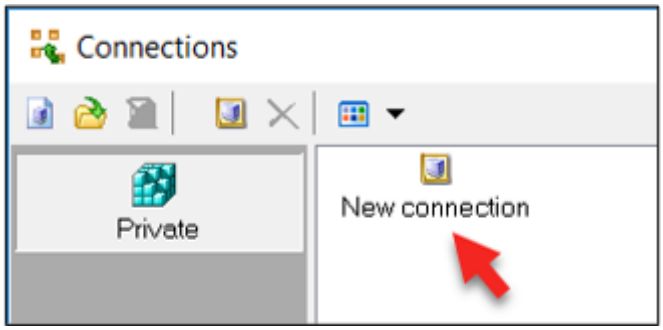


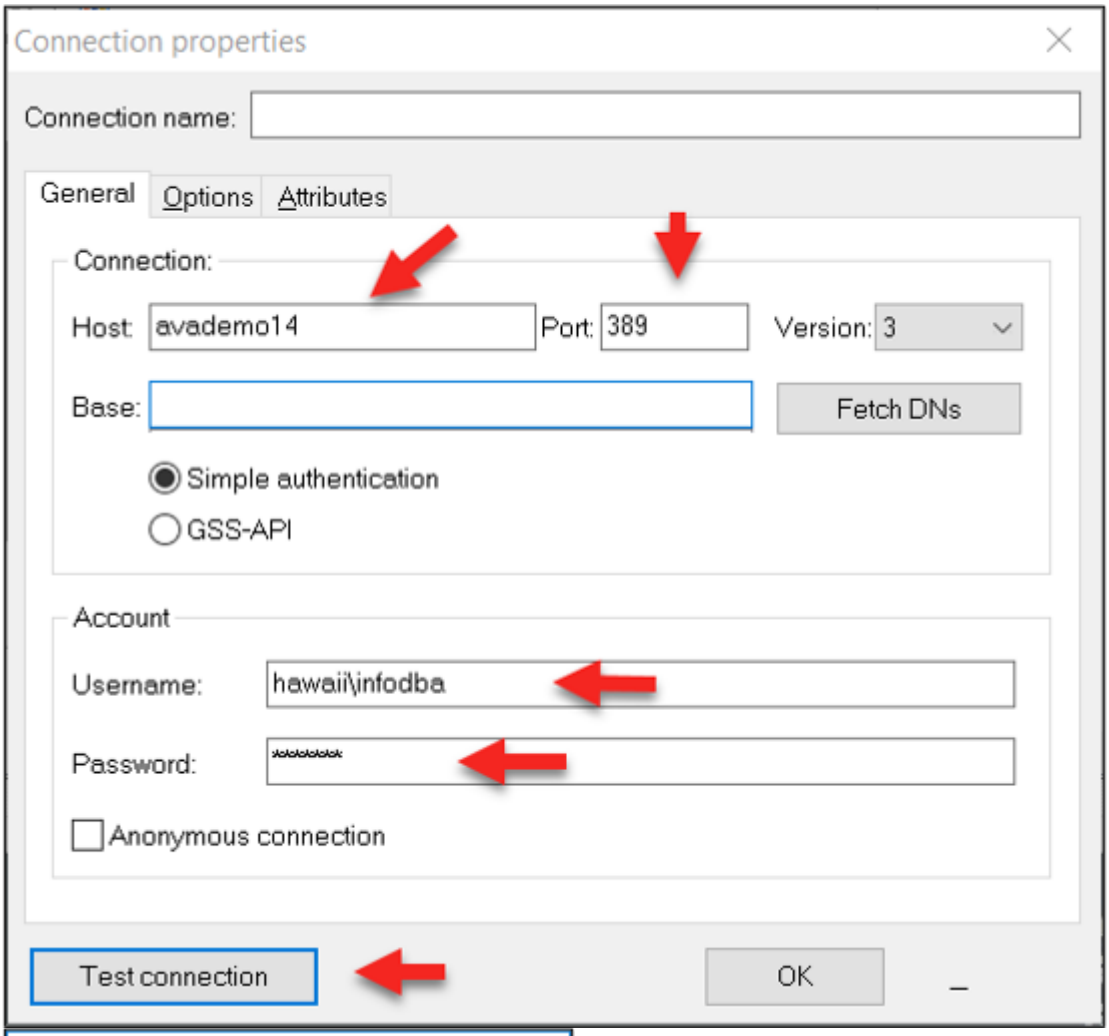
10. Tss-loginservices anpassen

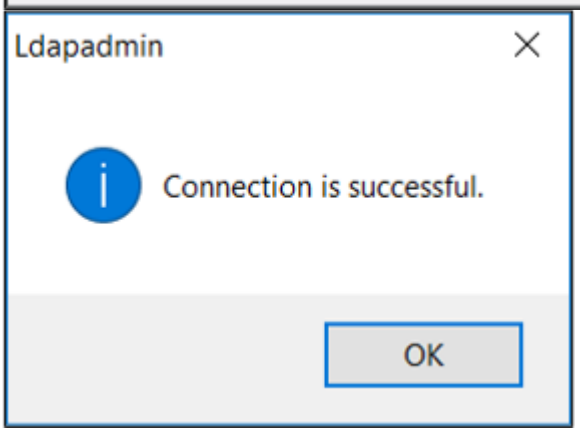
10.1 LdapAdmin

10.1.1 Mit LdapAdmin Loginuser überprüfen

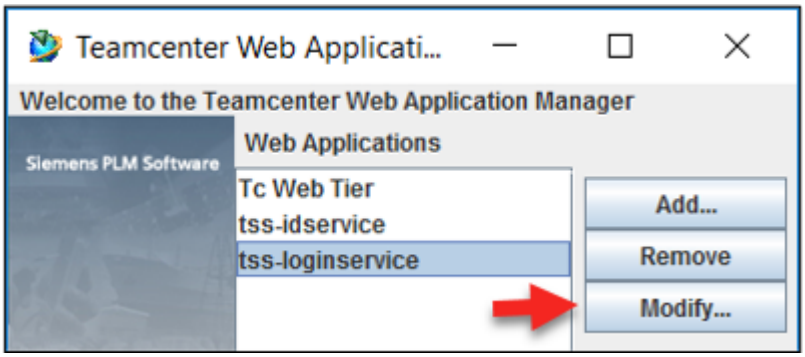


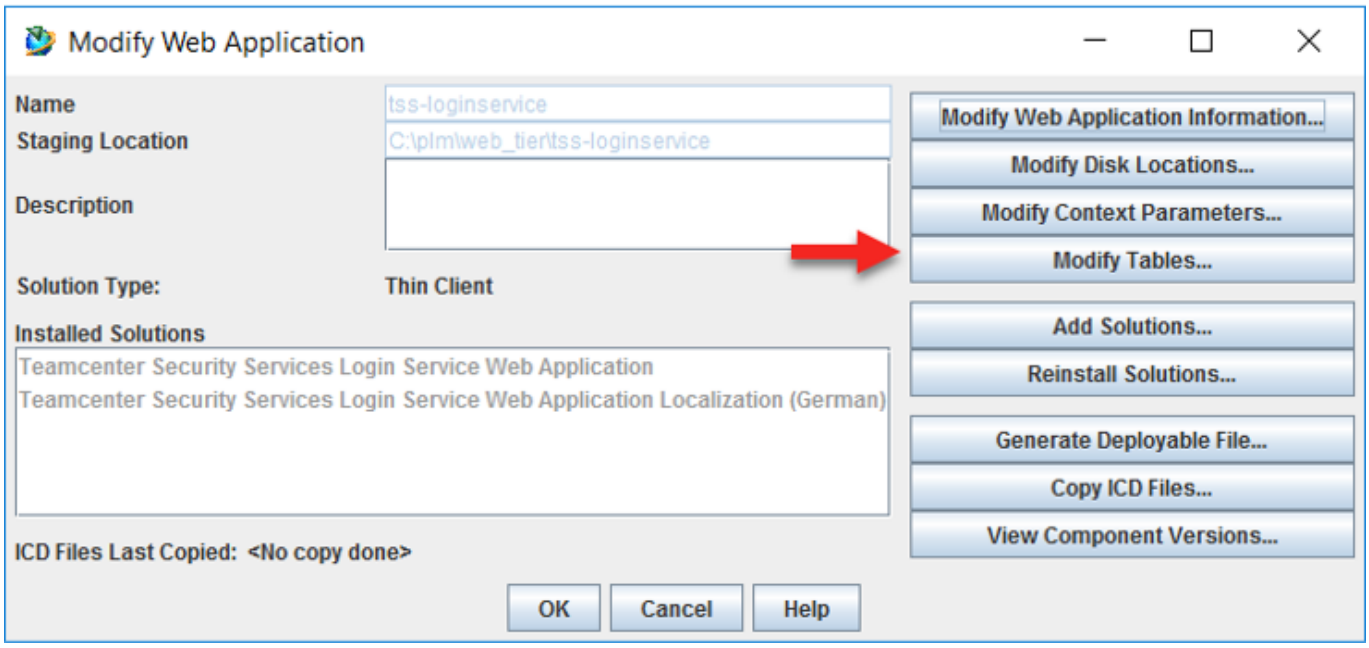


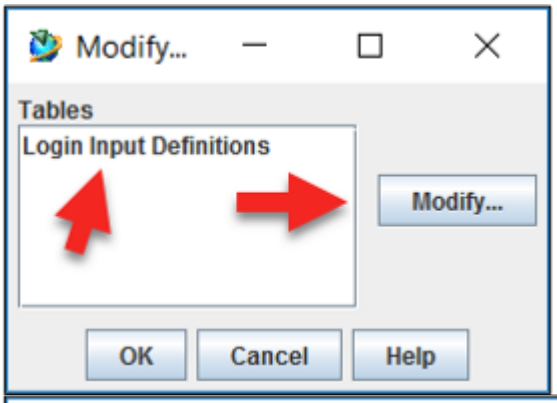


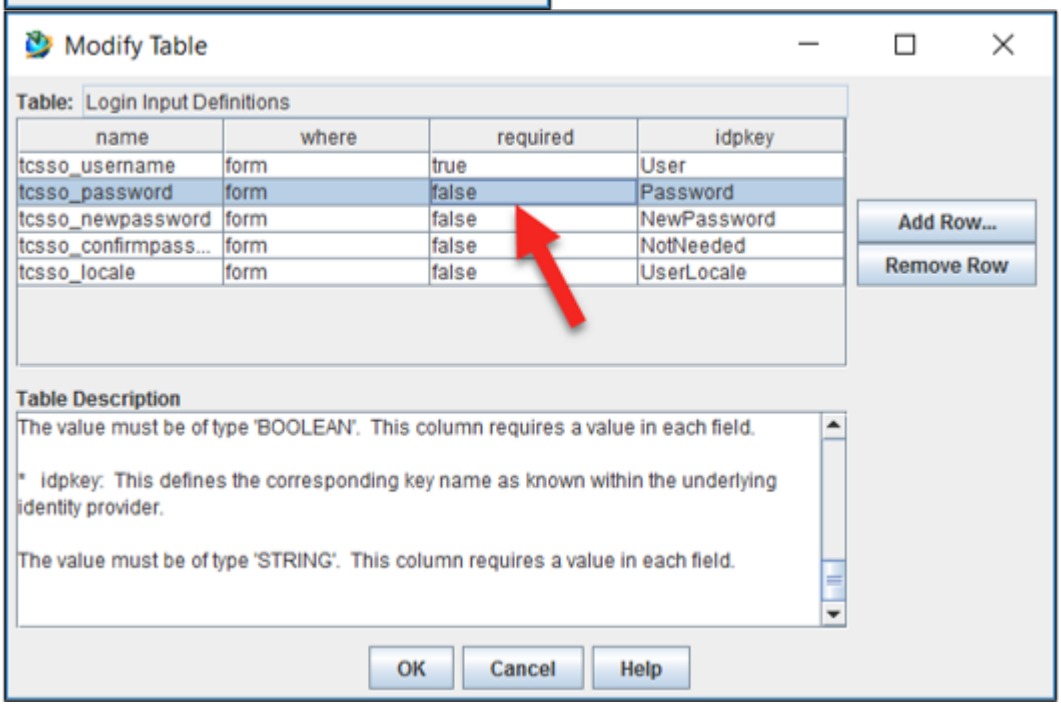


10.1.2 tss-loginservice anpassen, Modify Tables

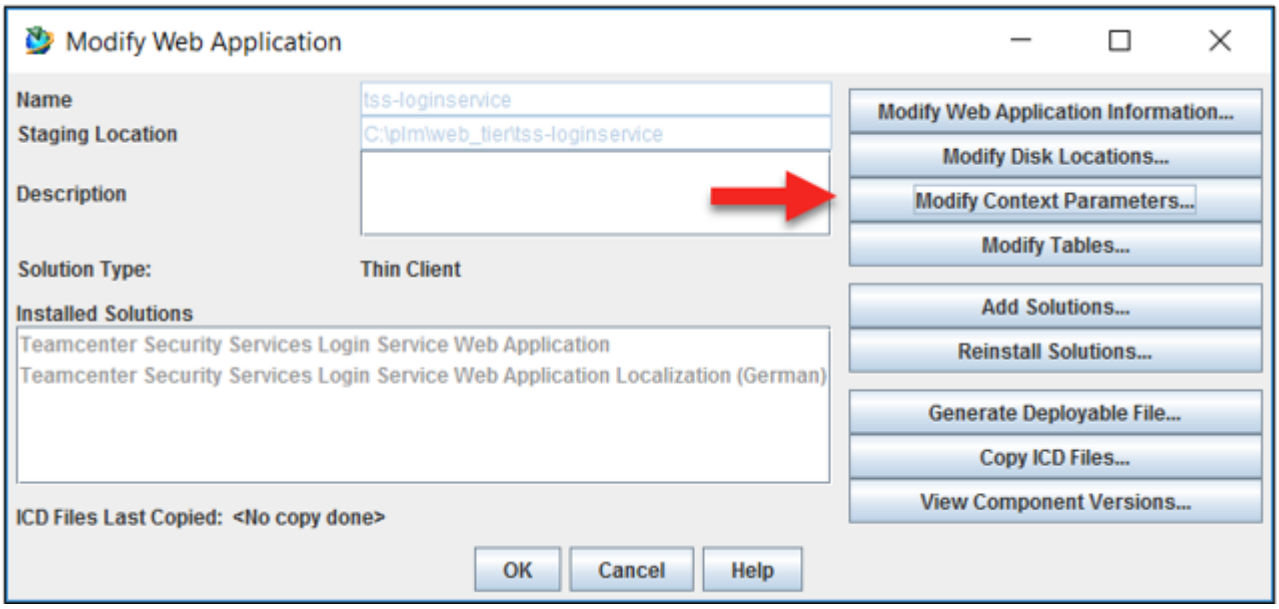




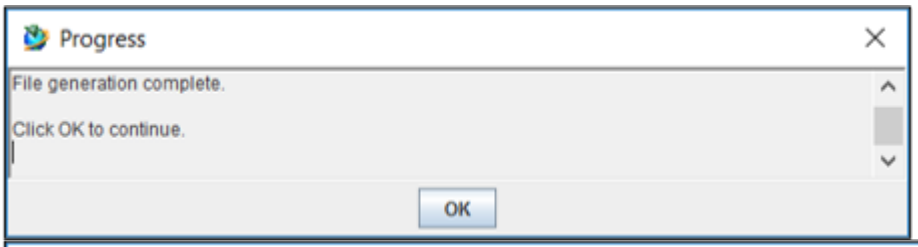


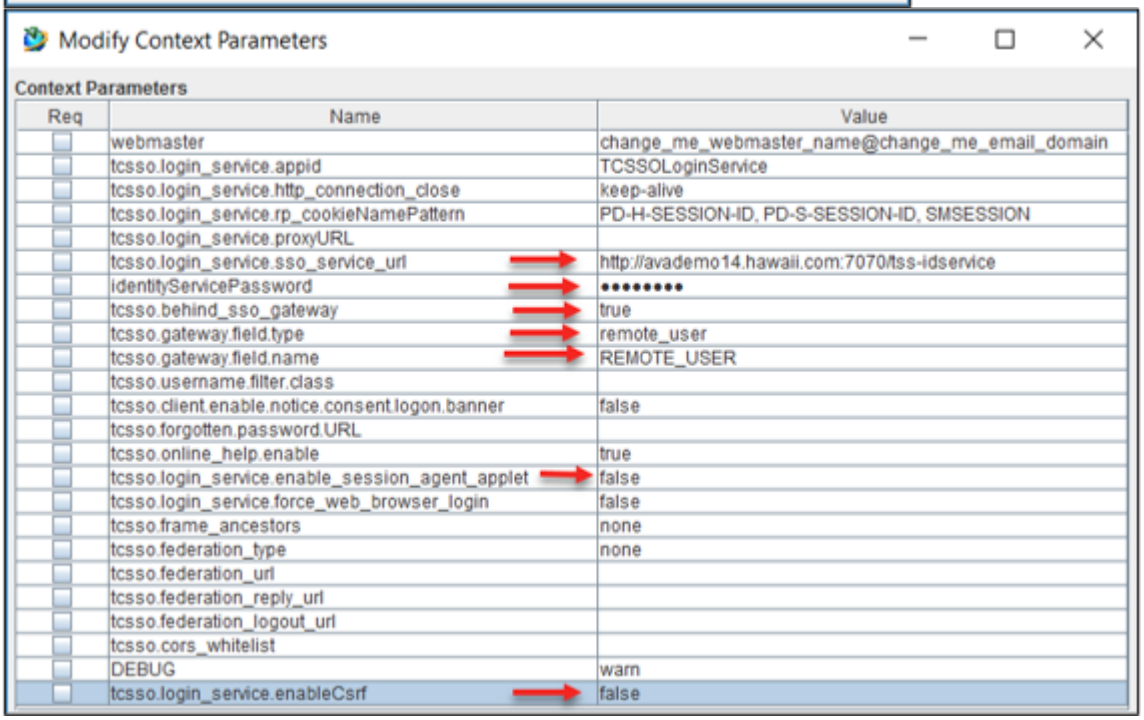


10.1.3 tss-loginservice anpassen, Modify Context Parameters



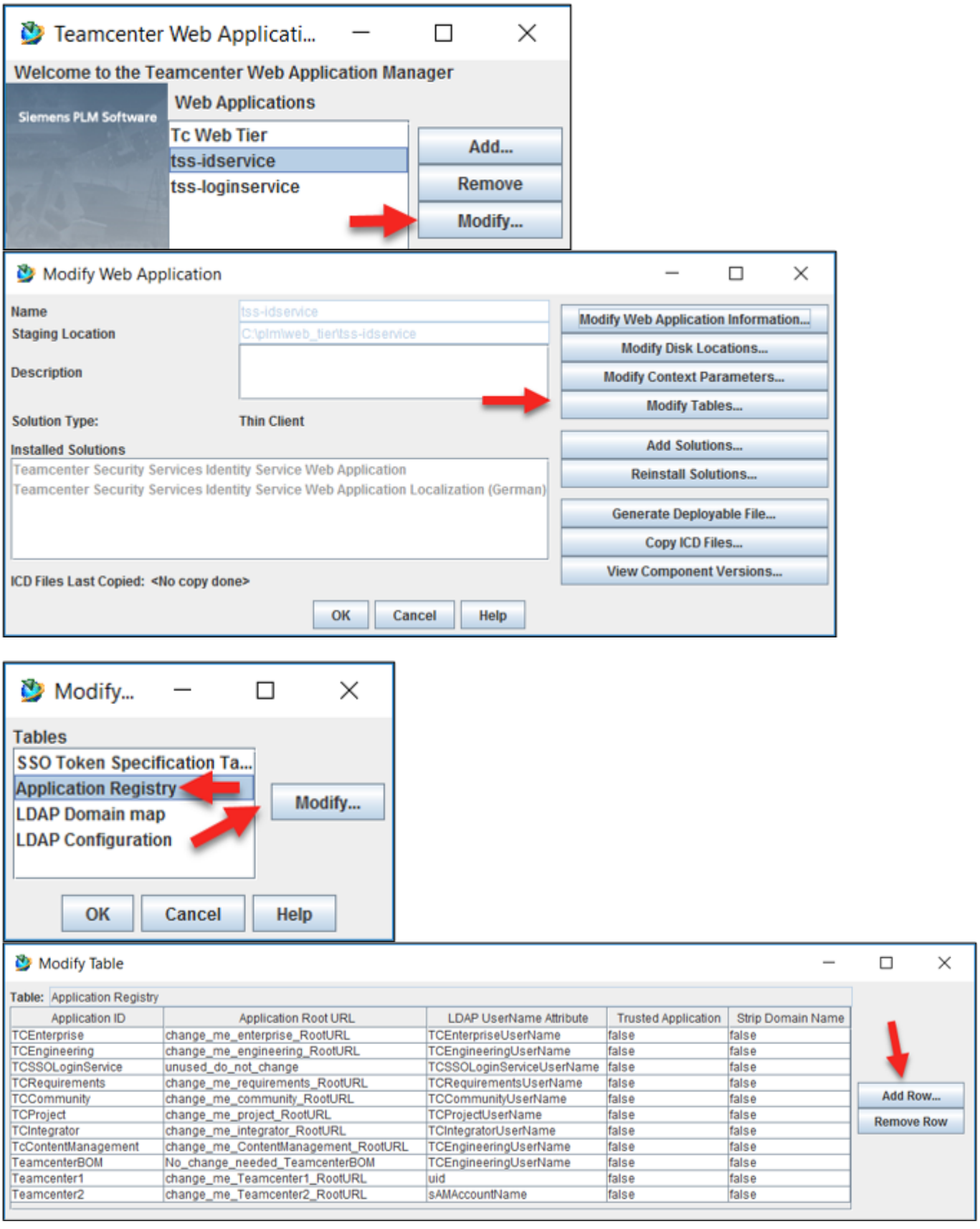
tcsso.login_service.sso_service_url:	http://avademo14.hawaii.com:7070/tss-idservice
identityServicePassword:	sicheres Passwort eingeben: 1nFodbAA
tcsso.behind_sso_gateway:	true
tcsso.gateway.field.type:	remote_user
tcsso.gateway.field.name:	REMOTE_USER
tcsso.login_service.enable_session_agent_applet:	false
tcsso.login_service.enableCsrf:	false





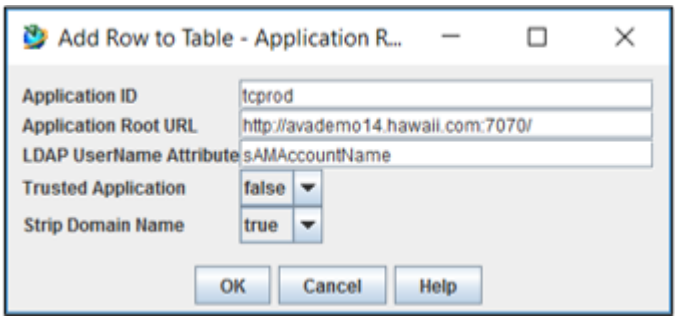
10.2 Tss-idservices anpassen

10.2.1 tss-idservice anpassen, Modify Tables

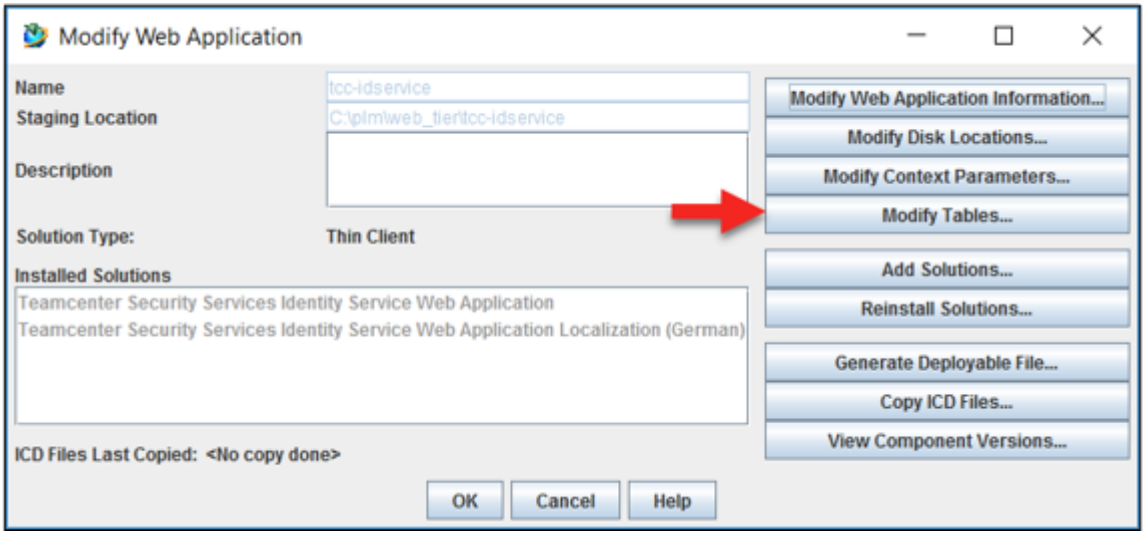


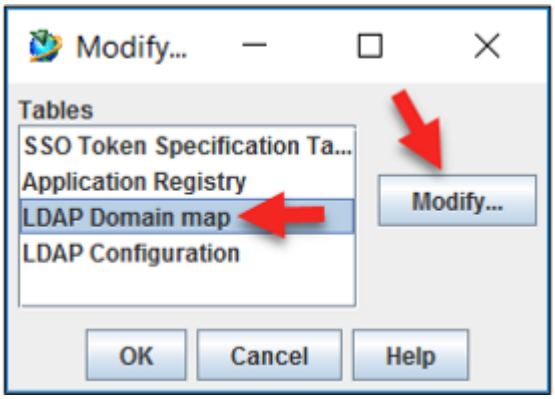
Application ID:	tcprod (SID...)
Application Root URL:	http://avademo14.hawaii.com:7070/

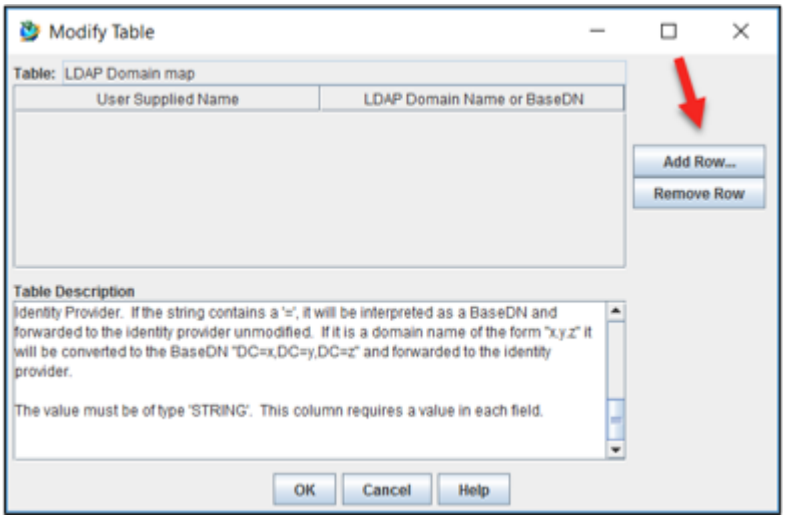
LDAP UserName Attribute:	sAMAccountName
Trusted Application:	false
Strip Domain Name:	true



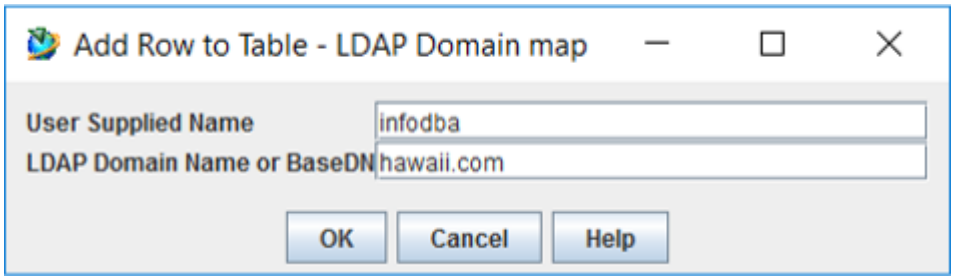
10.2.2 tss-idservice anpassen, Modify Tables



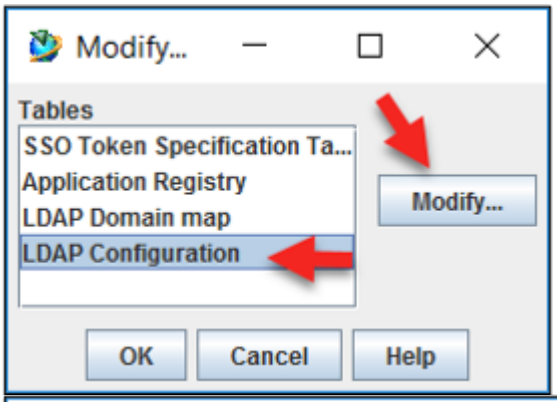


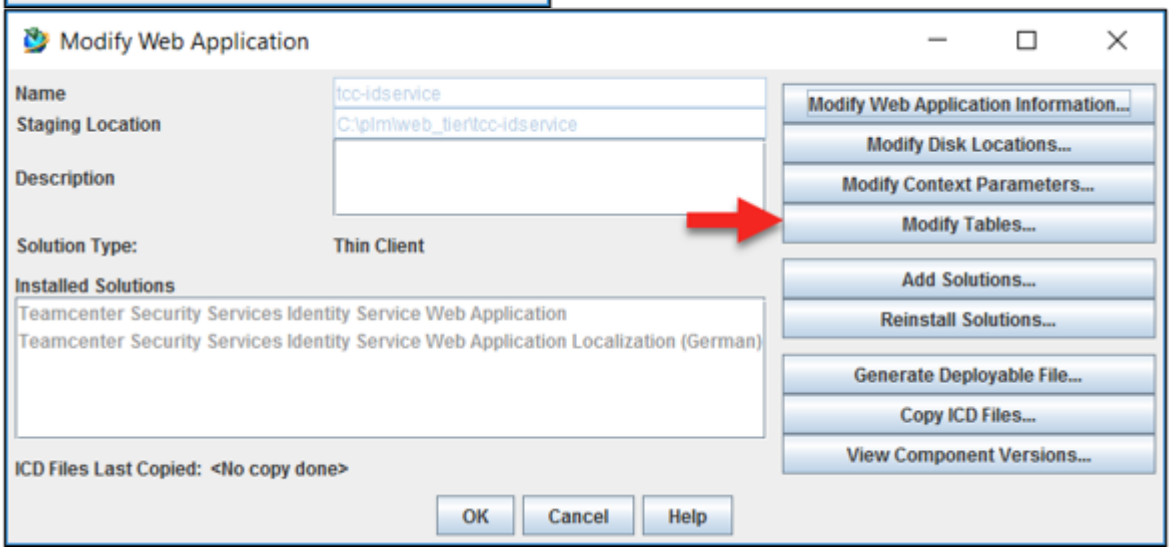


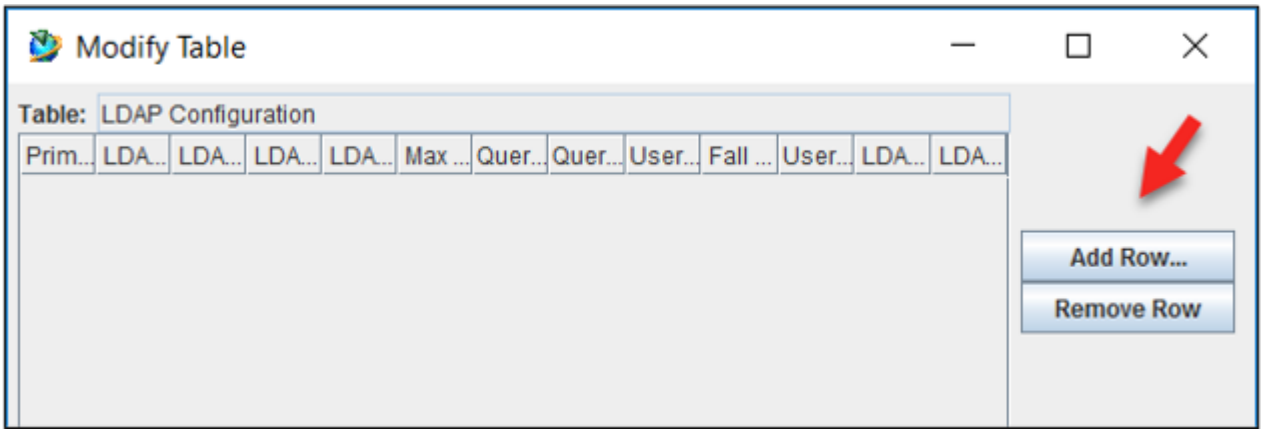
User Supplied Name:	infodba (Domänenbenutzer welcher abfragen darf ob TC-User Mitglied in Domäne ist)
LDAP Domain Name or BaseDN:	hawaii.com

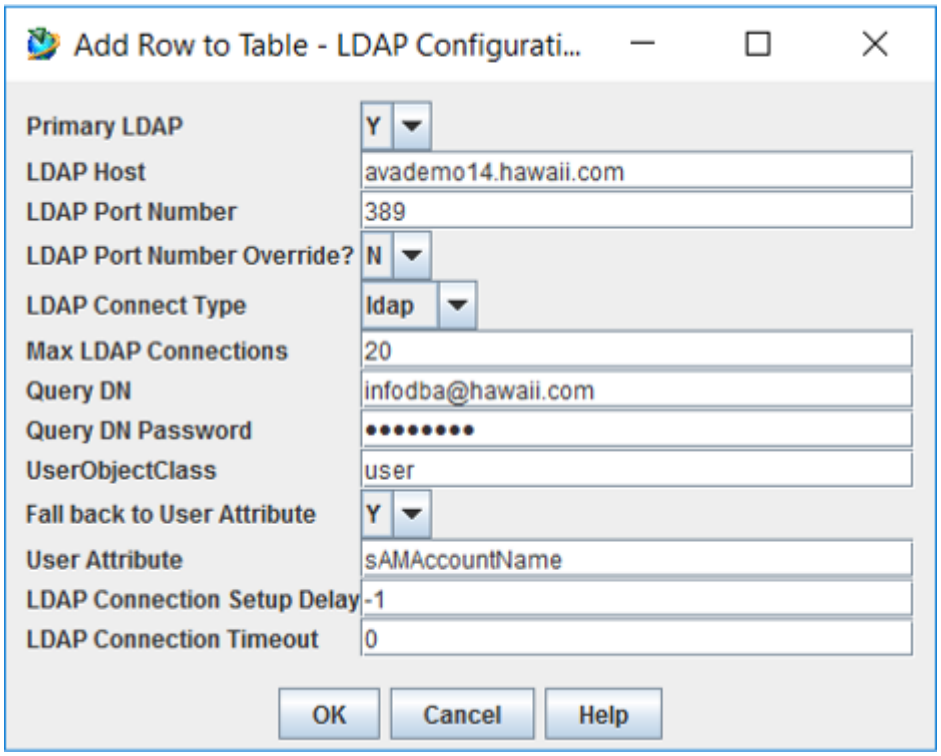


10.2.3 tss-idservice anpassen, Modify Tables



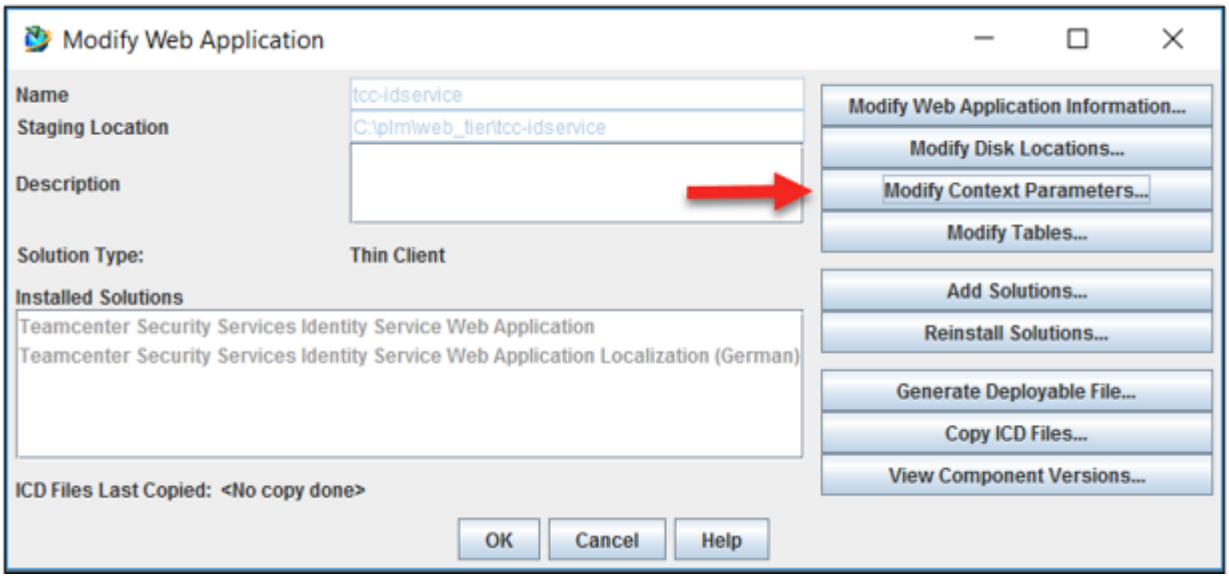




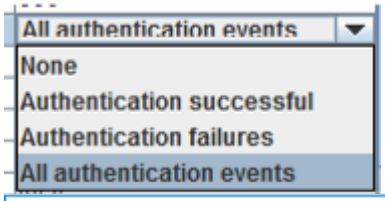


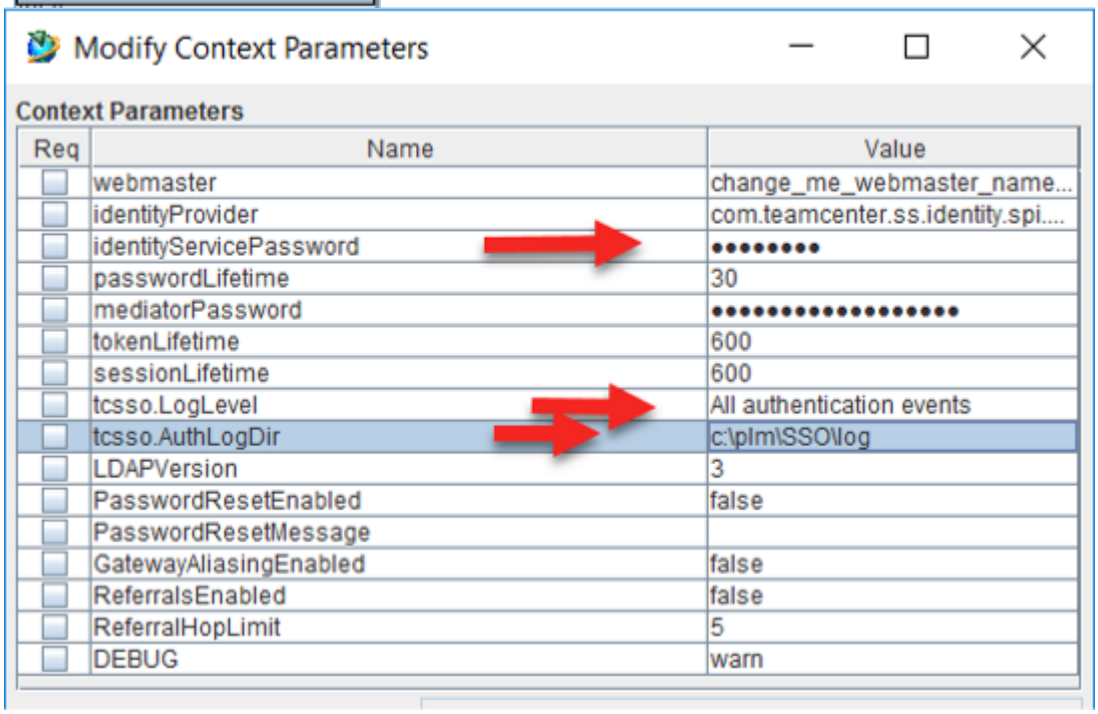
Primary LDAP:	Y
LDAP Host:	avademo14.hawaii.com
LDAP Port Number:	389
LDAP Port Number Override?:	N
LDAP Connect Type:	ldap
Max LDAP Connections:	20
Query DN:	infodba@hawaii.com
Query DN Password:	infodba (Passwort User)
UserObjectClass:	user
Fall back to User Attribute:	Y
User Attribute:	sAMAccountName
LDAP Connection Setup Delay:	-1
LDAP Connection Timeout:	0

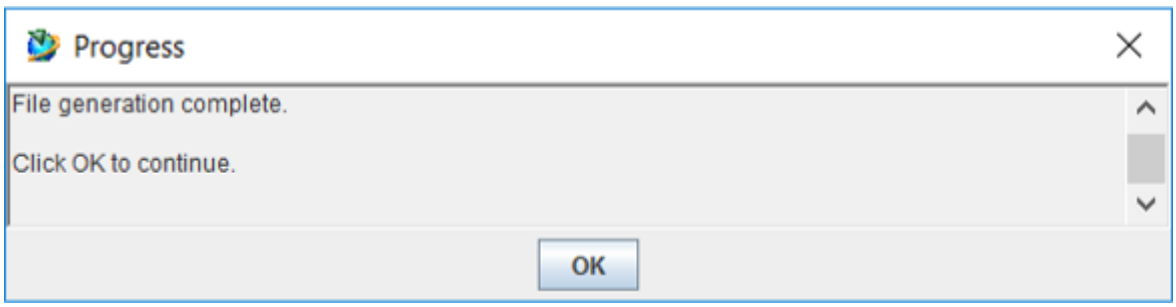
10.2.4 tss-idservice anpassen, Modify Context Parameters



identityServicePassword:	sicheres Passwort eingeben: 1nFodbAA (gleiches wie bei loginservice!!!)
tcsso.LogLevel	Authentication failures
tcsso.AuthLogDir	c:\plm\SSO\log

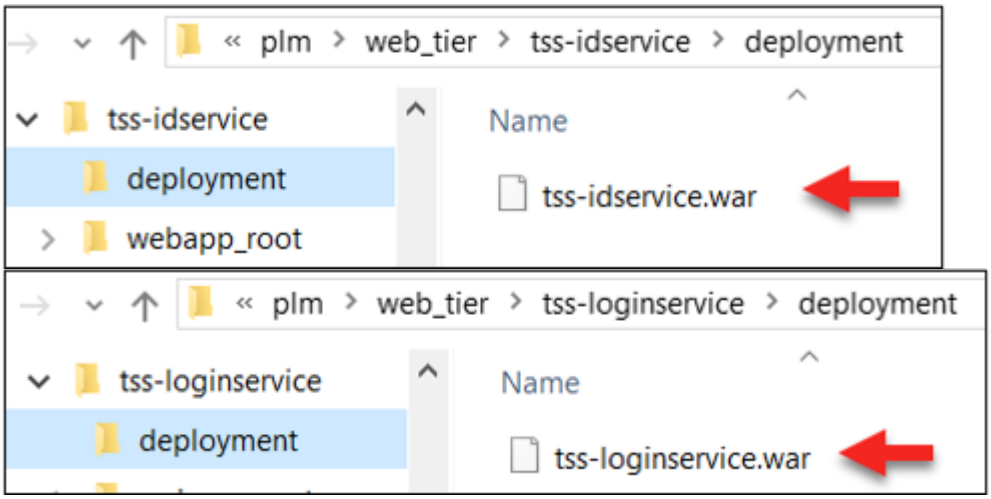




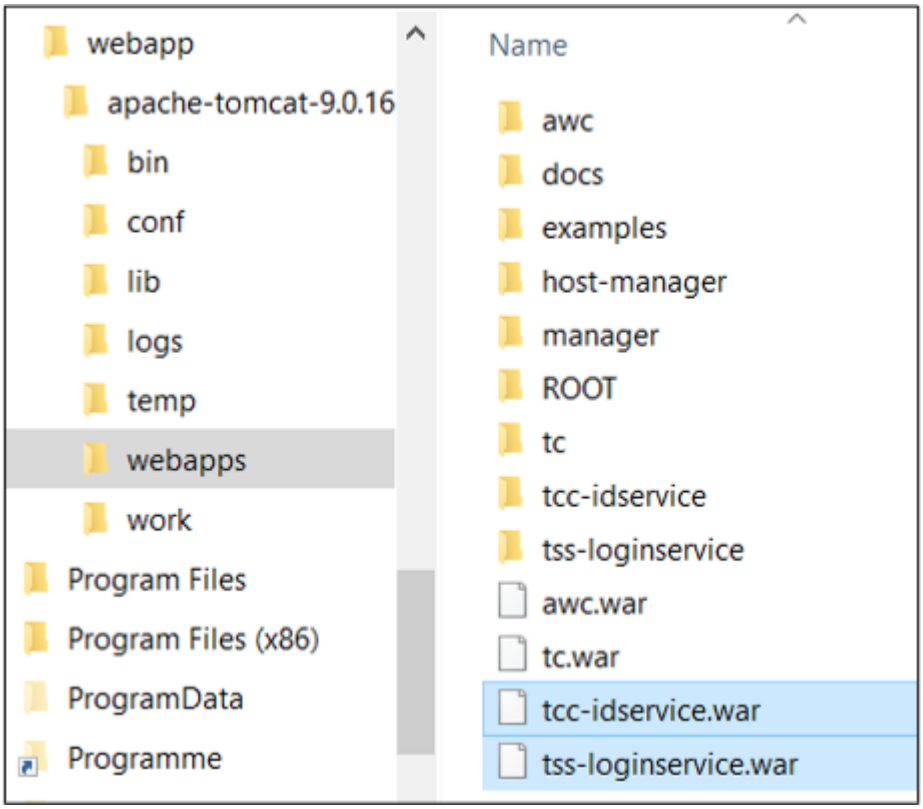


10.2.5 Deploy war-Files

Kopieren



nach



11. TCServer Manager changes

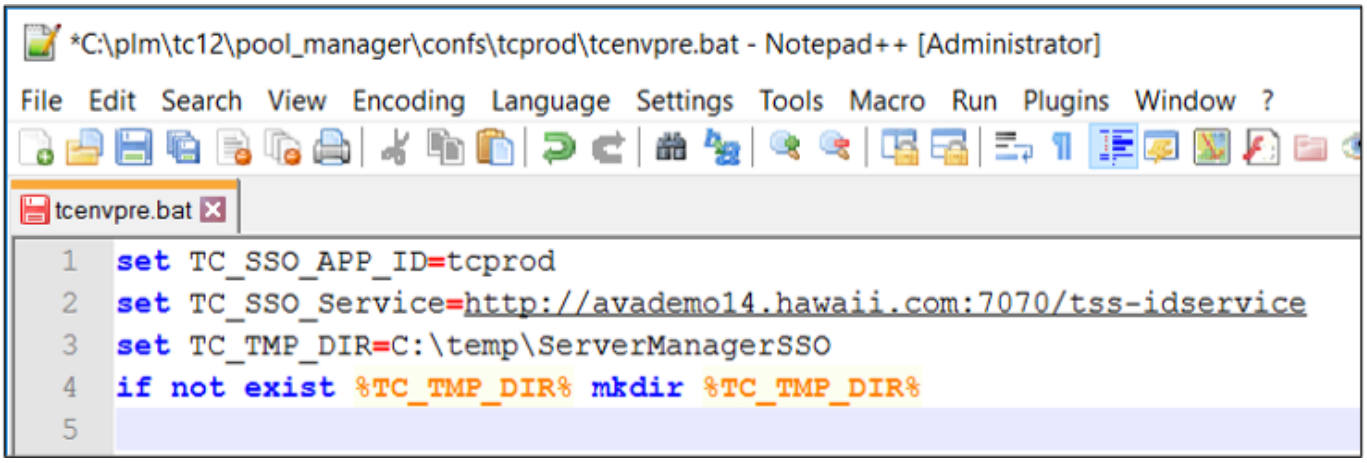
11.1 tcenvpre.bat

In Ordner C:\plm\tc12\pool_manager\confs\tcprod eine Datei mit folgendem Namen erstellen:

tcenvpre.bat

Inhalt:

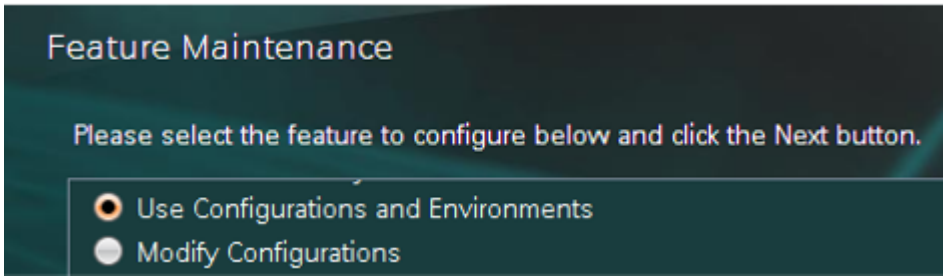
```
set TC_SSO_APP_ID=tcprod
set TC_SSO_Service=http://avademo14.hawaii.com:7070/tss-idservice
set TC_TMP_DIR=C:\temp\ServerManagerSSO
if not exist %TC_TMP_DIR% mkdir %TC_TMP_DIR%
```



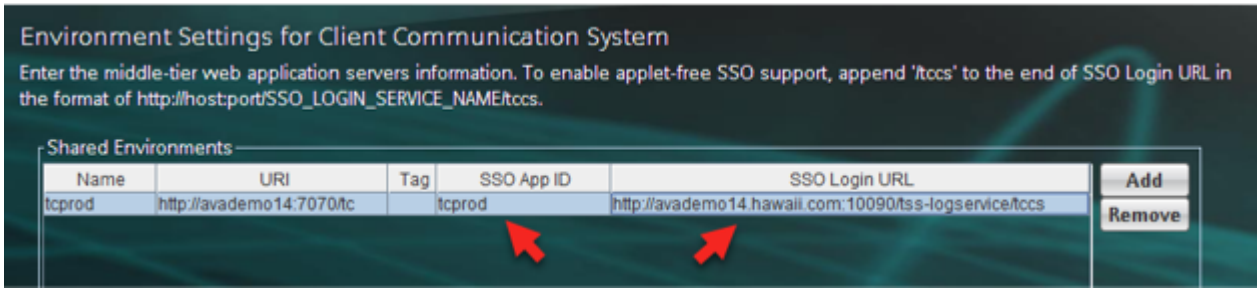
12. TCServer Manager changes

12.1 4-tier Client installation auf tccs umstellen

Feature Maintenance



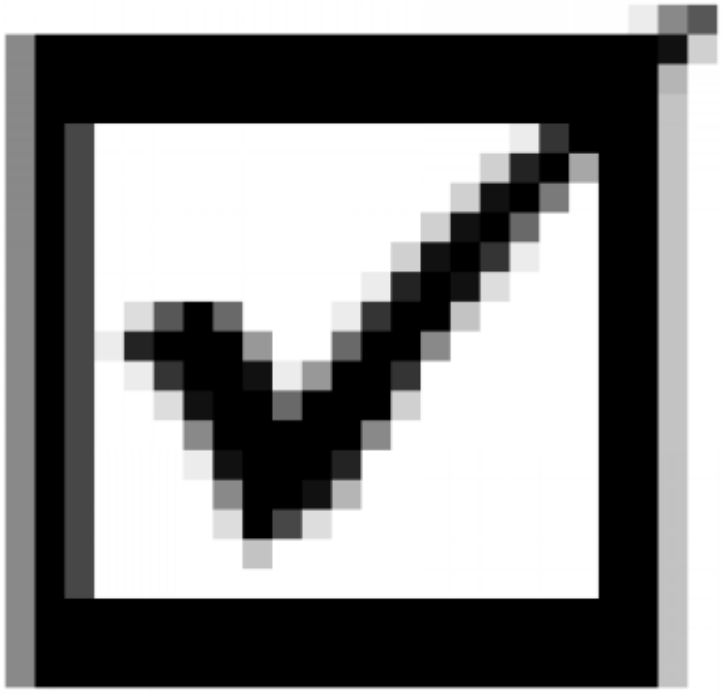
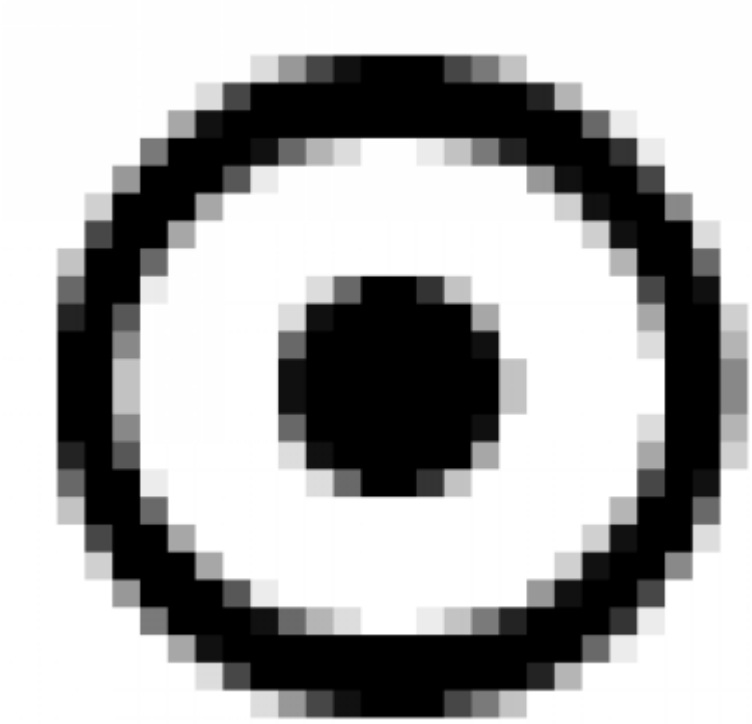
Environment Settings for Client Communication System

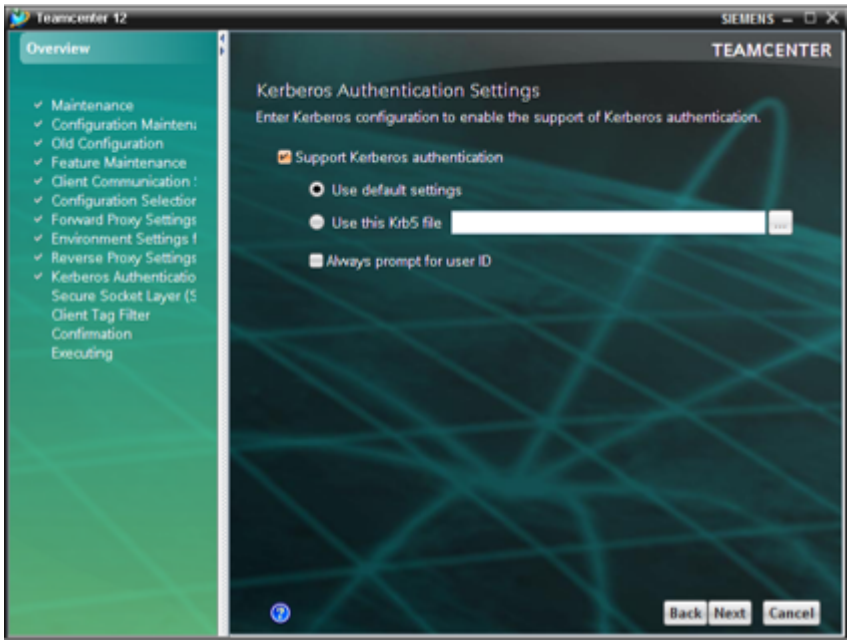


Anpassen:

Name:	tcprod
URI:	http://avademo14:7070/tc
Tag:	
SSO App ID:	tcprod
SSO Login URL:	http://avademo14.hawaii.com:10090/tss-loginservice/tccs

Kerberos Authentication Settings

-  Support Kerberos authentication
  -  Use default settings



12.2 Richclient 4-tier

Einmal anmelden:

Sollte nun ohne Passworteingabe funktionieren

13. AWC auf SSO umstellen