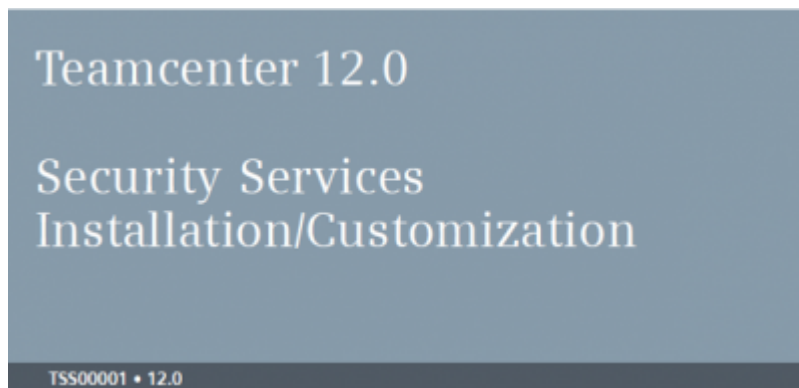


Inhaltsverzeichnis

Handbuch Tc 12 Security Services	3
Impressum	3
1. Vorbedingungen Clientinstallation	3
2. 4-tier Client installation auf tccs umstellen	4
2.1 Feature Maintenance	4
2.2 Client Communication System Switch	4
2.3 Configuration Selection for Client Communication System	4
2.4 Forward Proxy Settings	5
2.5 Environment Settings for Client Communication System	5
2.6 Reverse Proxy Settings	6
2.6 Kerberos Authentication Settings	7
2.7 Secure Socket Layer (SSL) Settings	7
2.8 Client Tag Filter	8
2.9 Ergebnis	9
3. IIS auf Webserver konfigurieren	10
3.1 IIS installieren	10
4. C:\plm\SSO einrichten	11
5. Modify Tomcat server.xml	12
6. IIS konfigurieren	13
7. Installing Security Services	21
7.1 SSO Sources vorbereiten	21
7.2 SSO ICD kopieren	21
8. Tss-logiservice erstellen	22
8.1 Create the Login Service	22
9. Tss-idservice erstellen	27
9.1 Create the Identity Service	27
10. Tss-loginservices anpassen	31
10.1 LdapAdmin	31
10.2 Tss-idservices anpassen	35
11. TCServer Manager changes	40
11.1 tcenvpre.bat	40

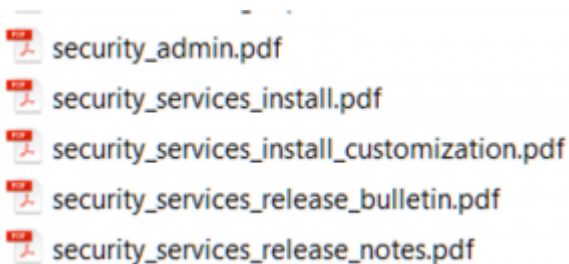
Handbuch Tc 12 Security Services



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



Diese Unterlagen sind urheberrechtlich geschützt. Alle Rechte, auch die der Übersetzung, des Nachdruckes und Vervielfältigung der Unterlagen oder Teilen daraus, vorbehalten. Kein Teil der Unterlagen darf ohne Genehmigung von avasis AG in irgendeiner Form (Fotokopien, Mikrofilm oder ein anderes Verfahren), auch nicht für Zwecke der Unterrichtsgestaltung, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet oder vervielfältigt oder Dritten zugänglich gemacht werden.

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

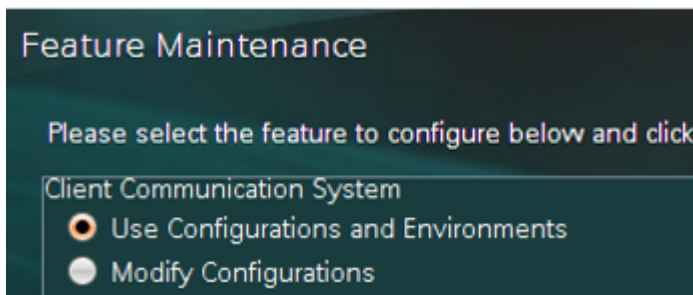
Dieser Schritt ist nur notwendig, falls dieser nicht schon bei Grundinstallation des 4-tier RichClient gemacht wurde.

2.1 Feature Maintenance

Client Communication System Use configurations and Environments



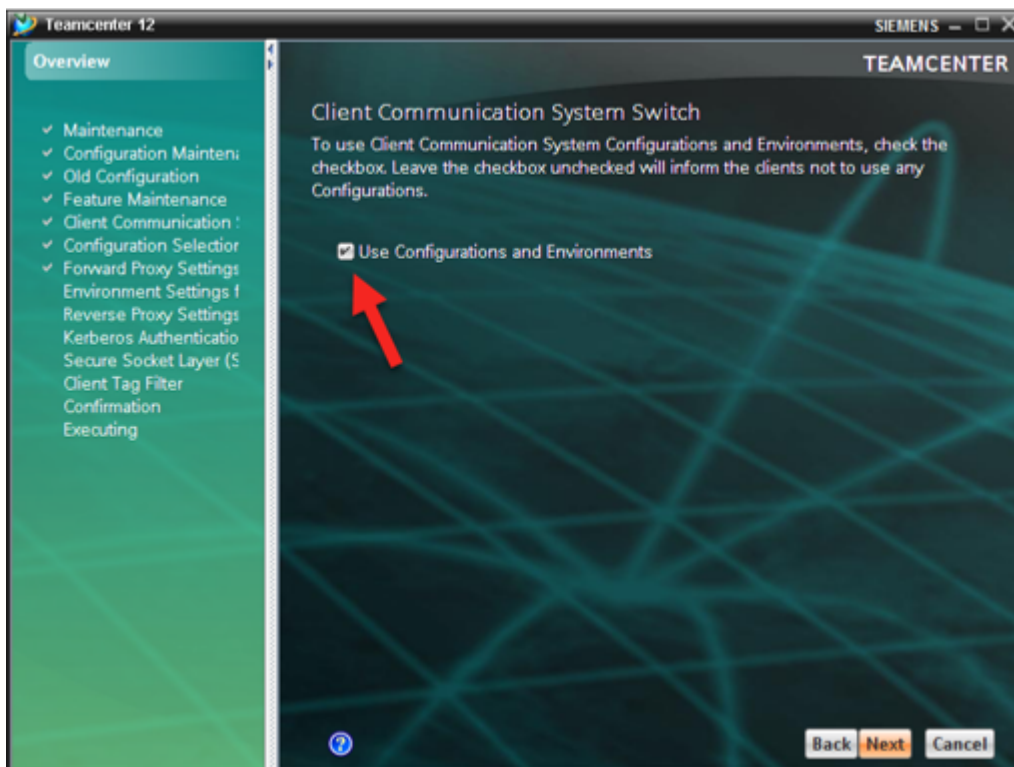
Use configurations and Environments



2.2 Client Communication System Switch



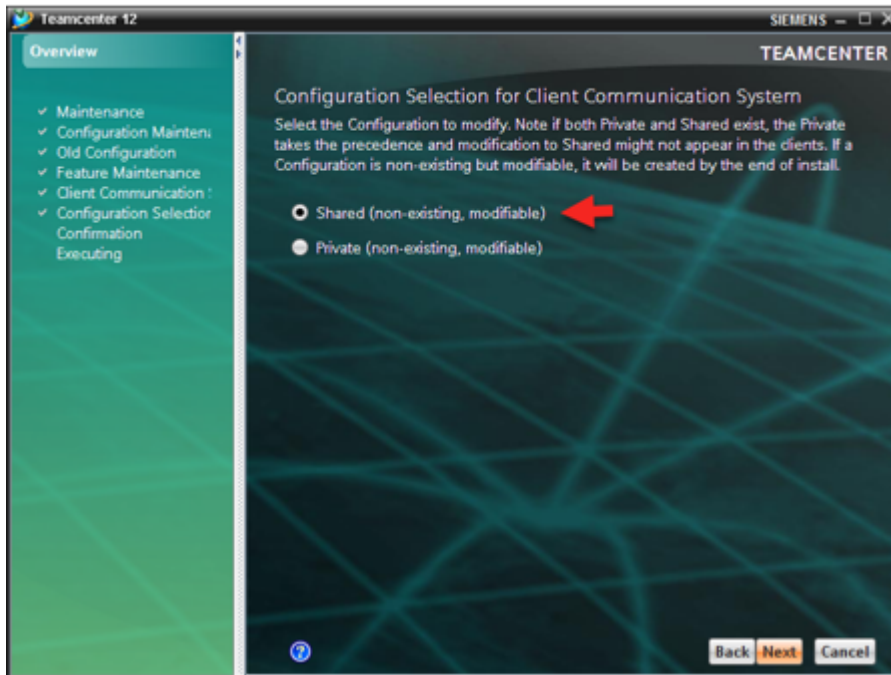
Use Configuration and Environments



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

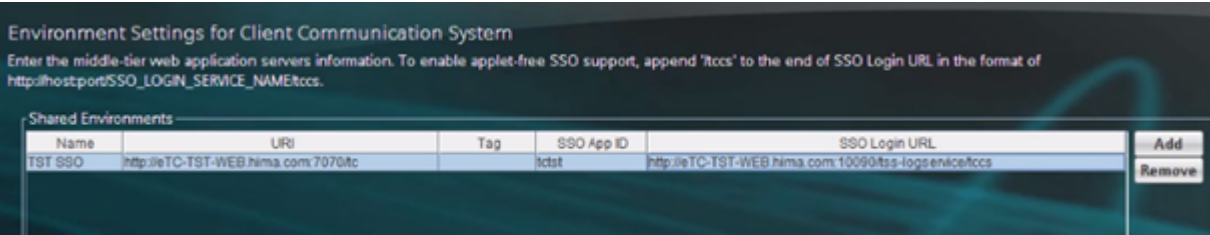
Add...

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



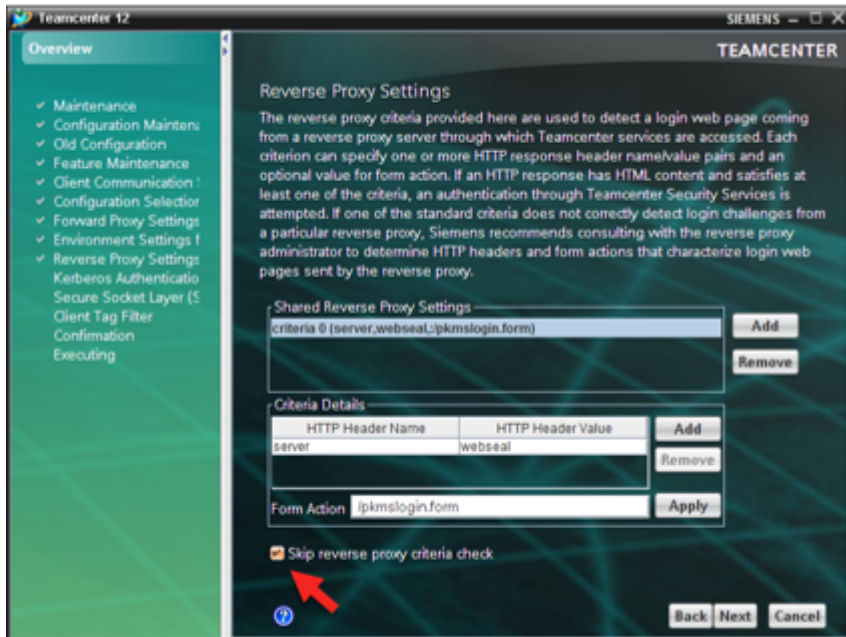
Add...

- 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>



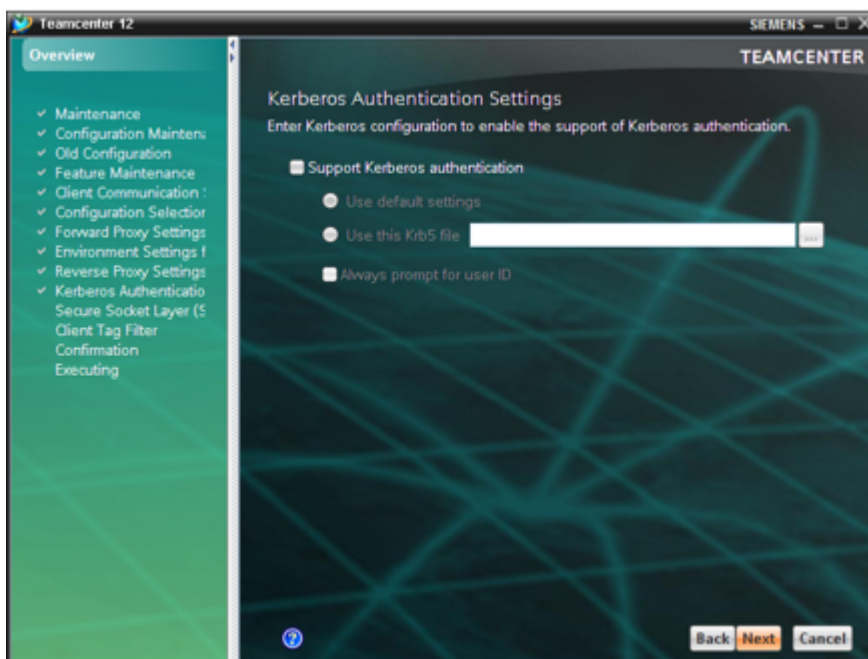
2.6 Reverse Proxy Settings

- ☒ Skip reverse proxy criteria check



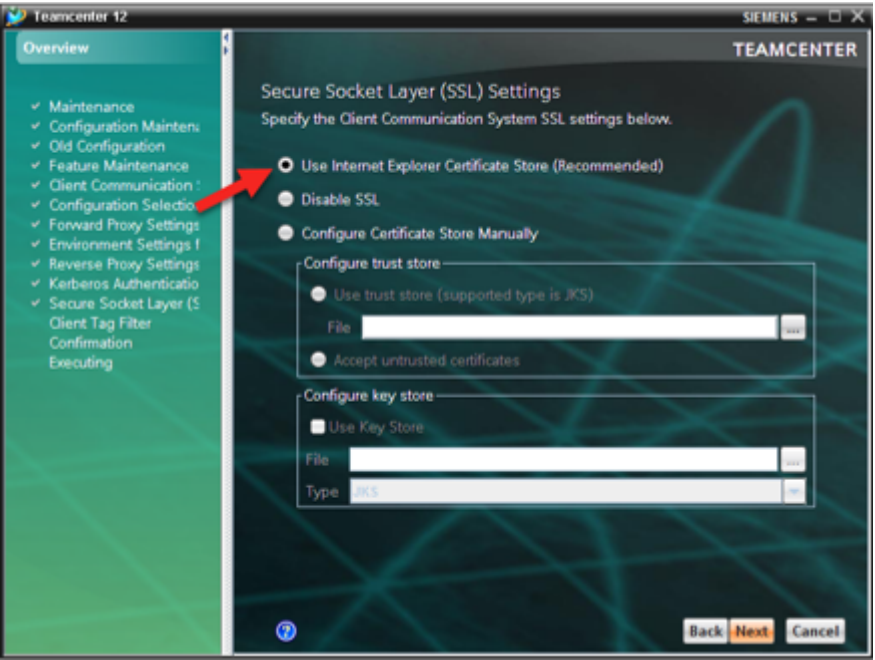
2.6 Kerberos Authentication Settings

Next...



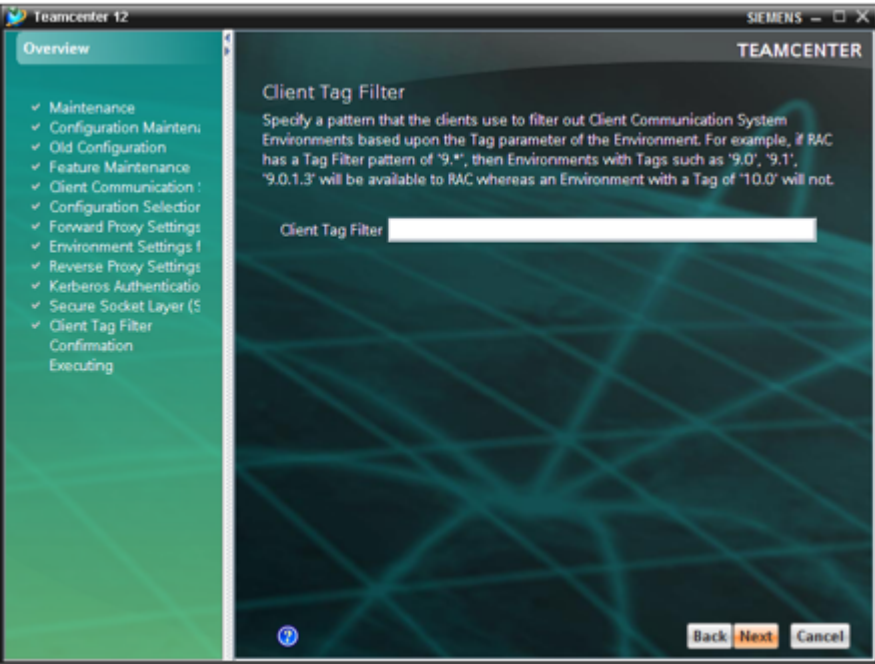
2.7 Secure Socket Layer (SSL) Settings

-  Use Internet Explorer Certificate Store (Recommended)

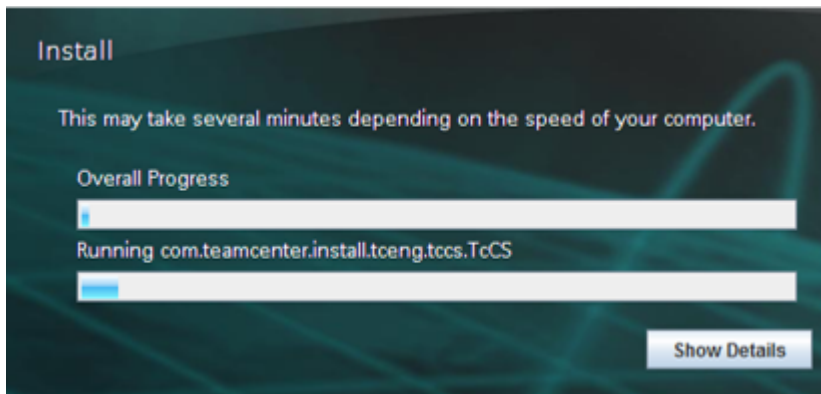
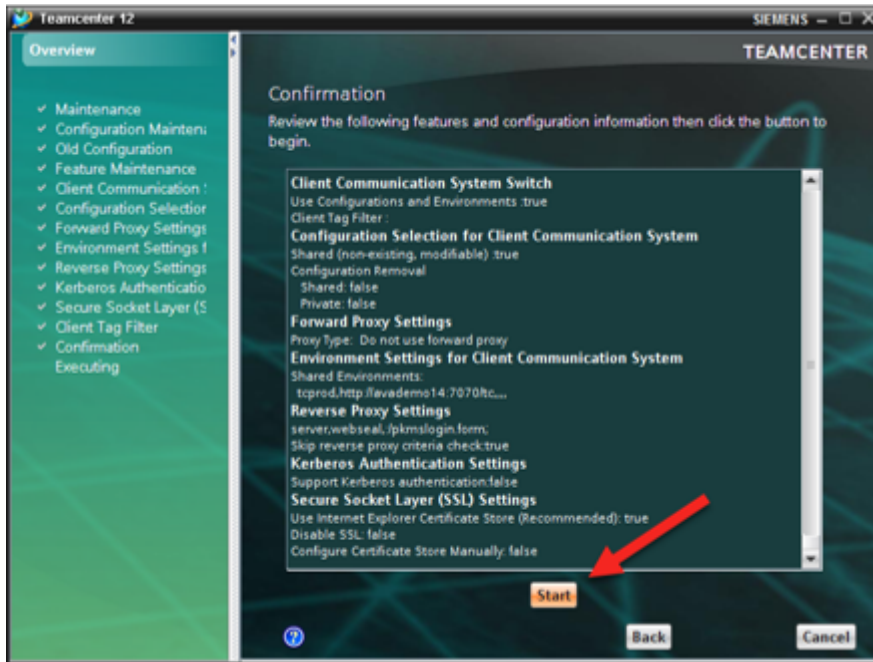


2.8 Client Tag Filter

Next...



Confirmation



close

2.9 Ergebnis

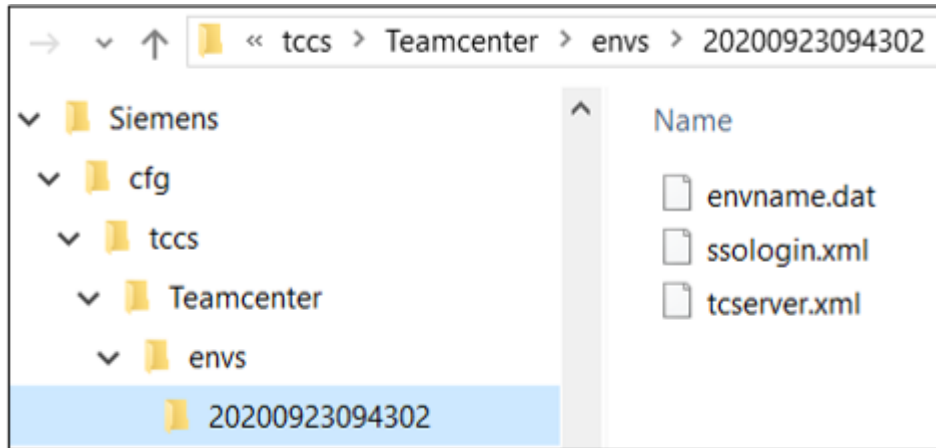
In C:\plm\tc12\portal\plugins\configuration_12000.2.0\client_specific.properties

```

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
76

```

Siemens Ordner in C:\ProgramData\

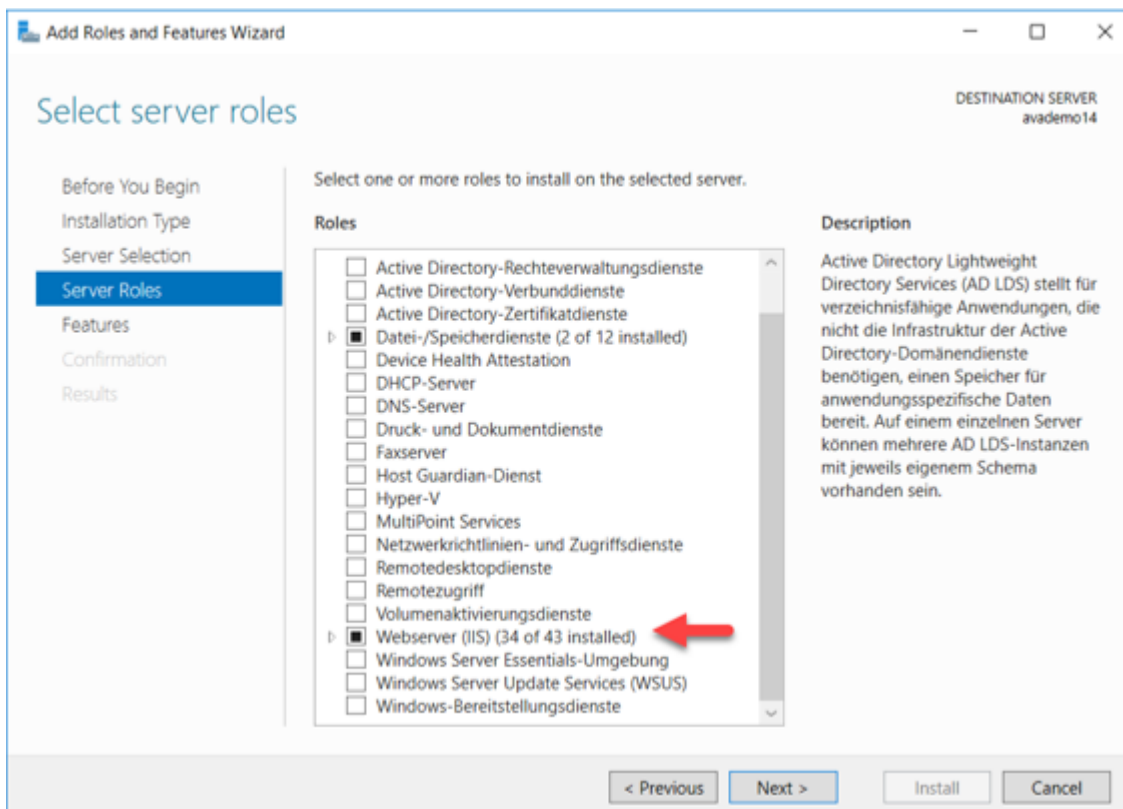
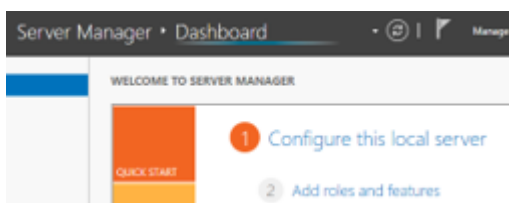


3. IIS auf Webserver konfigurieren

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

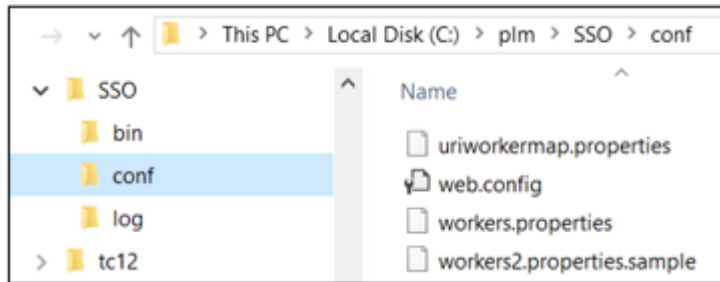
Install only the available **ASP.NET 4.x** role services. Do not install ASP.NET 3.x role services.

Management Tools

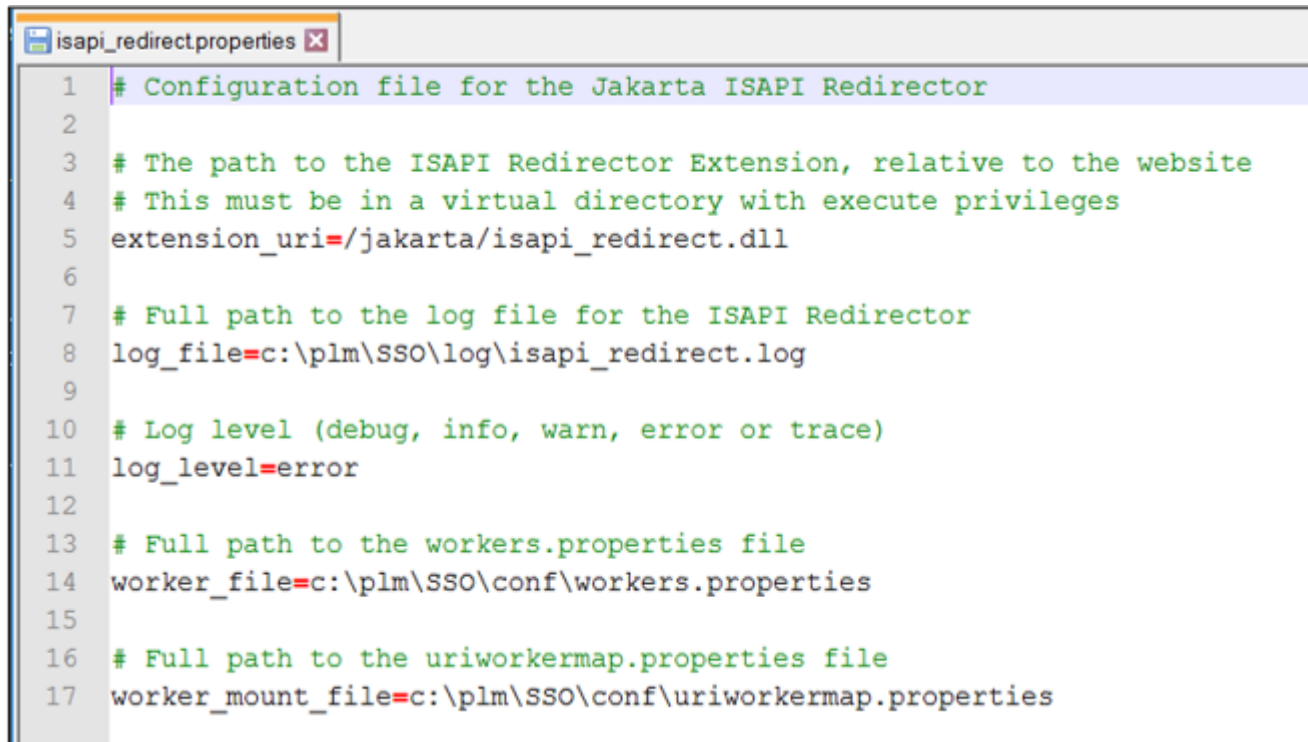
- IIS Management Console

4. C:\plm\SSO einrichten

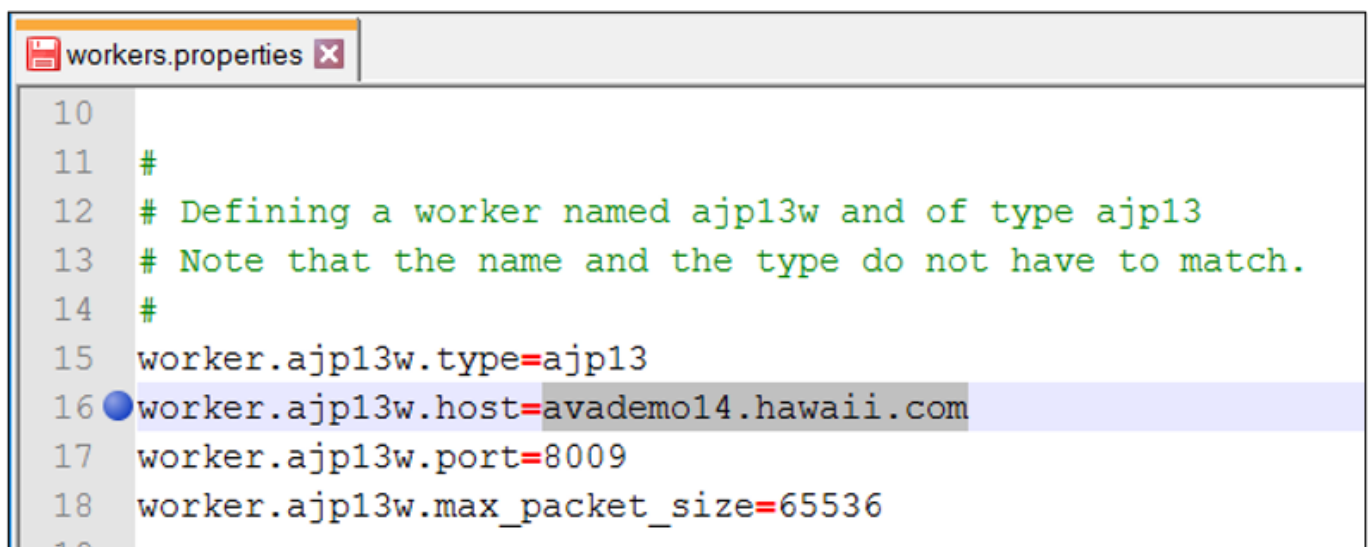
1. Ordner SSO von ... \avaCentralRepository\avaSSO\c\plm\SSO nach c:\plm kopieren



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



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



5. Modify Tomcat server.xml

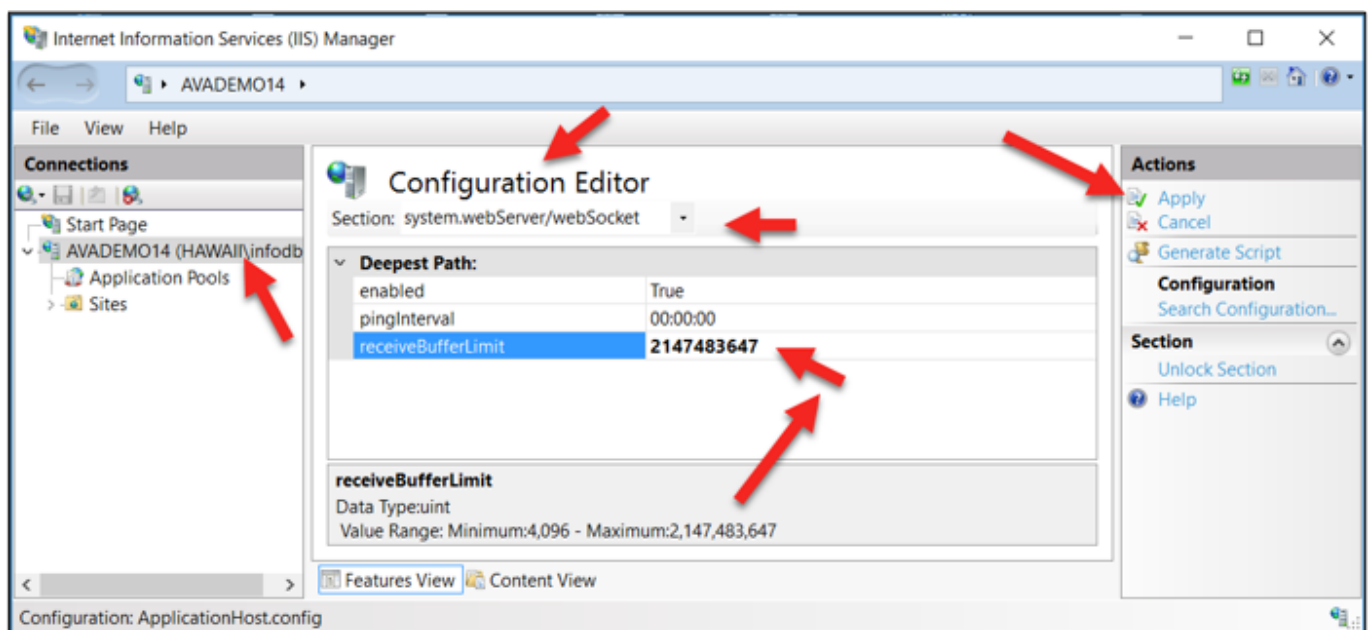
In „C:\plm\webapp\apache-tomcat-9.0.16\conf\server.xml“ anpassen:

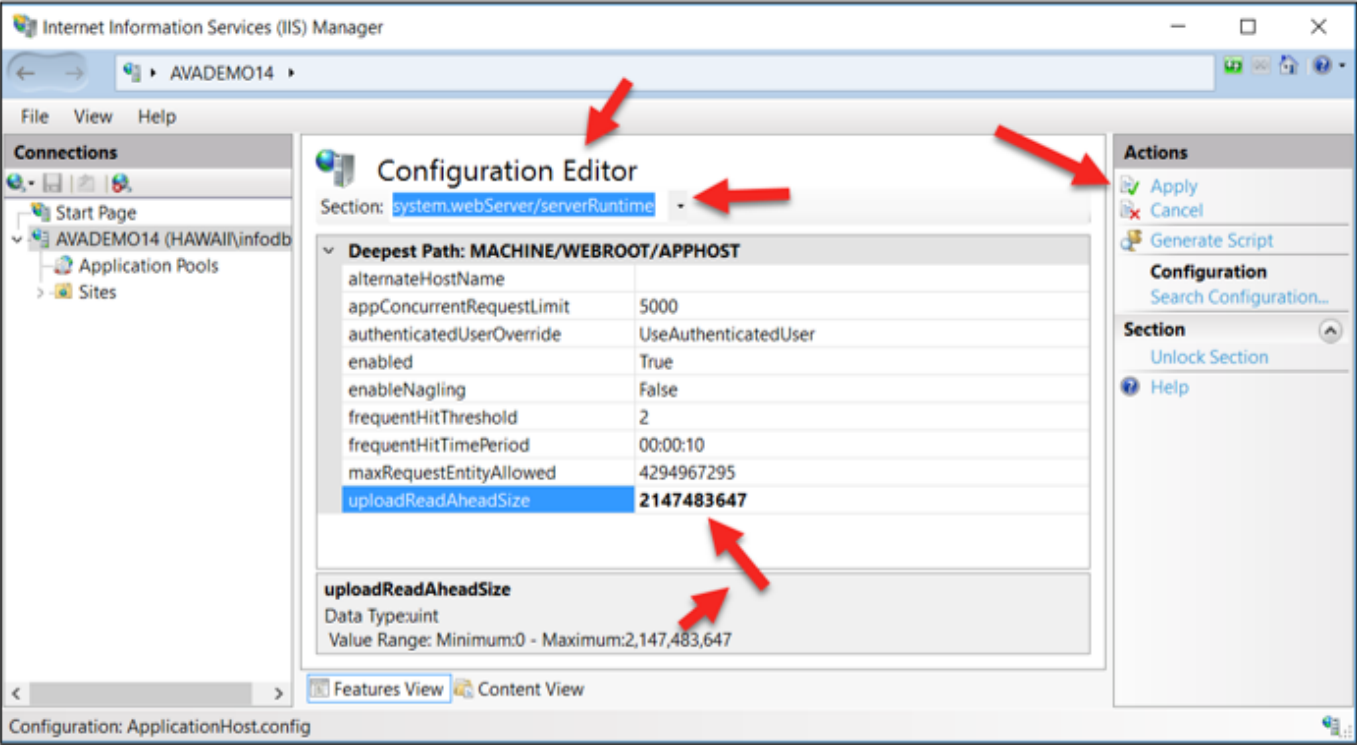
```
server.xml x
114
115      <!-- Define an AJP 1.3 Connector on port 8009 -->
116      <!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
117      <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" secretRequired="" maxTh
118
```

```
<!-- <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"/>
```

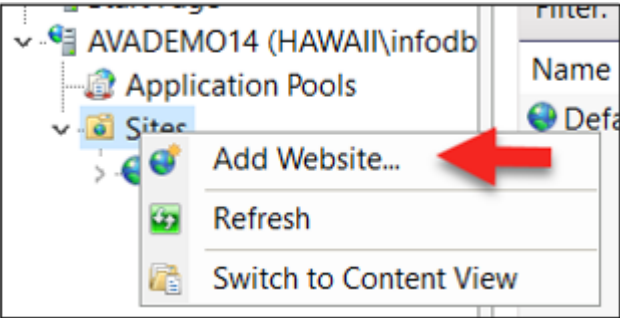
6. IIS konfigurieren

1. Configuration Editor





2. Website hinzufügen



Add Website

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

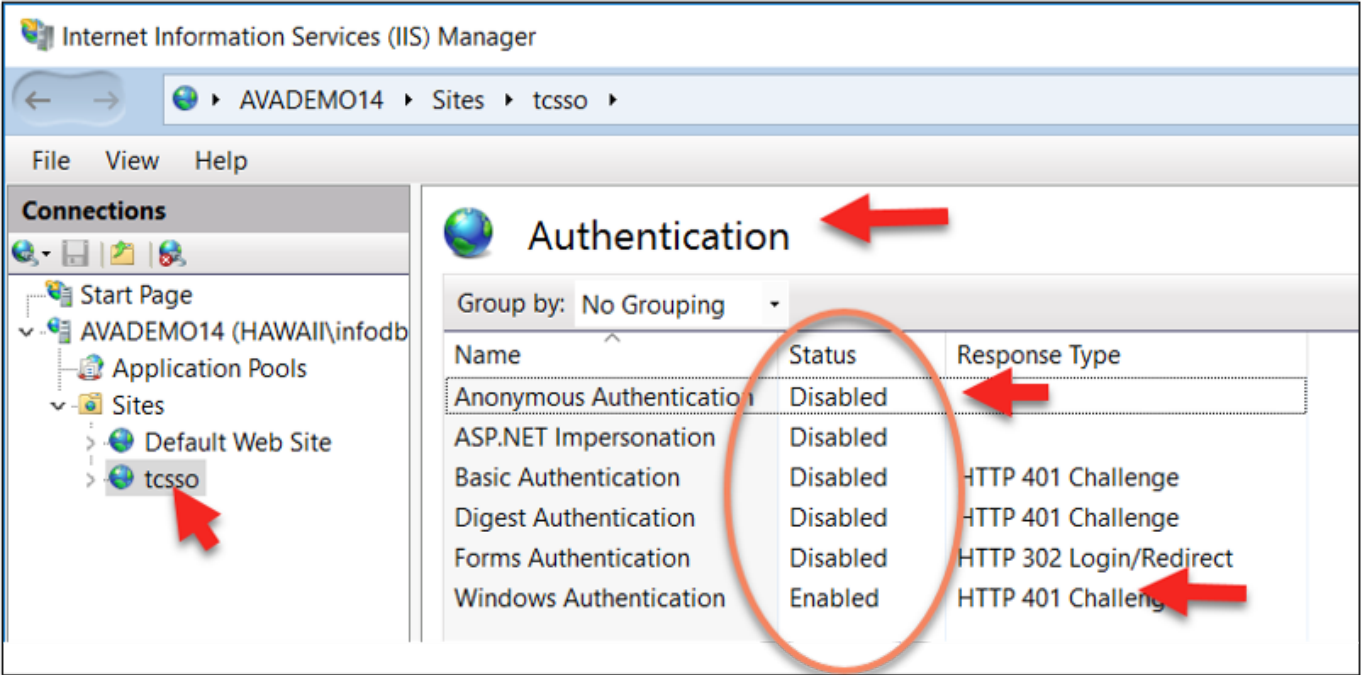
Type: IP address: Port:

Host name:

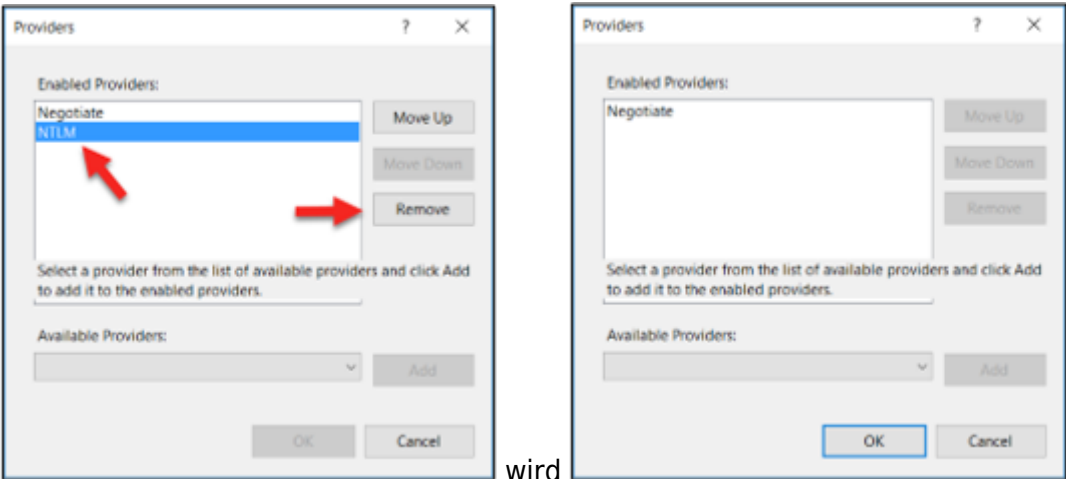
Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

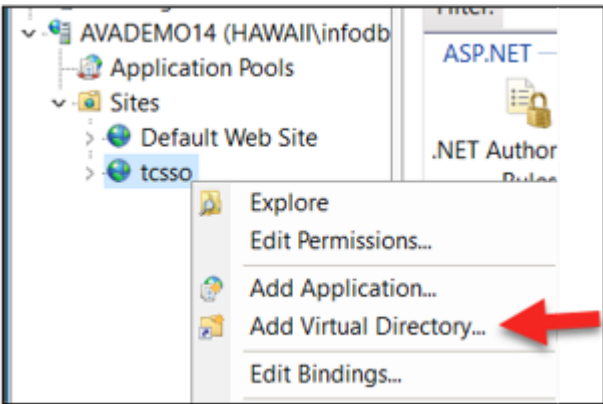
3. Remove NTLM



RMB Windows Authentication, Providers



4. Virtuelle Verzeichnis hinzufügen



Add Virtual Directory ? X

Site name: tcsso
Path: /

Alias:
jakarta

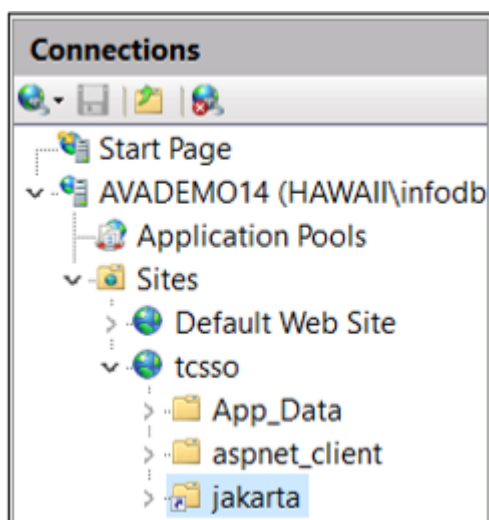
Example: images

Physical path:
C:\plm\SSO\bin

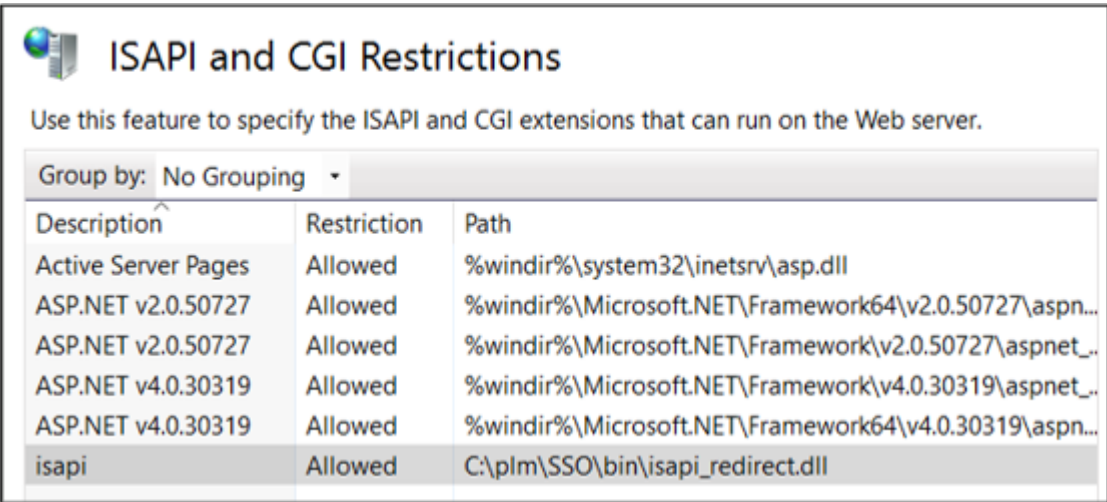
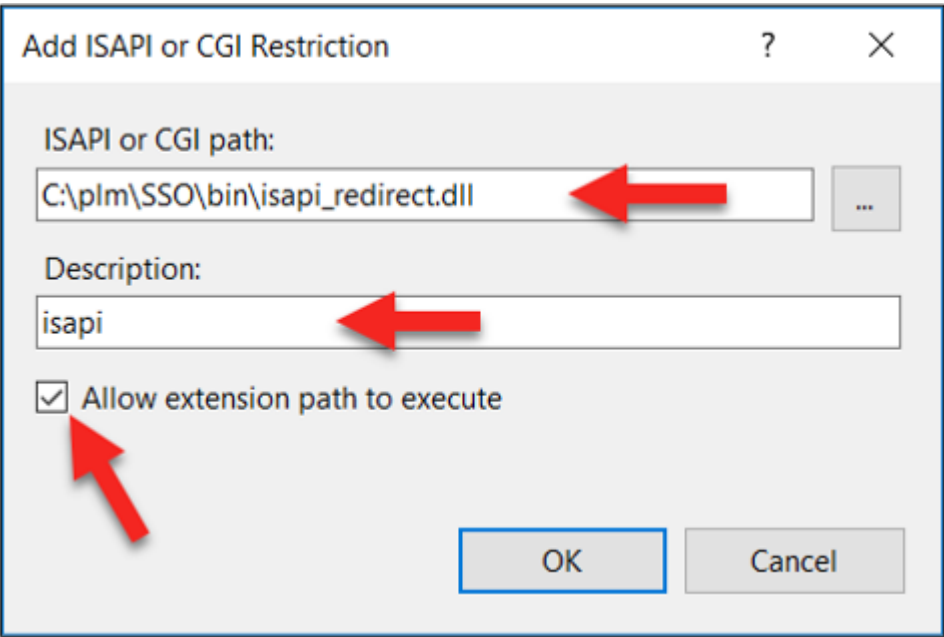
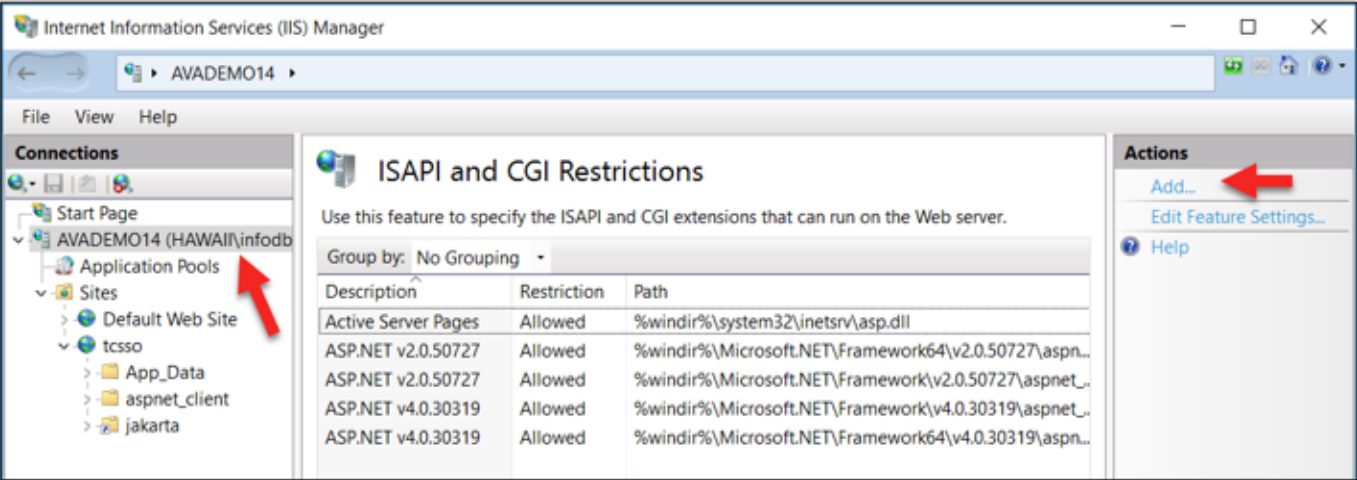
Pass-through authentication

Connect as... Test Settings...

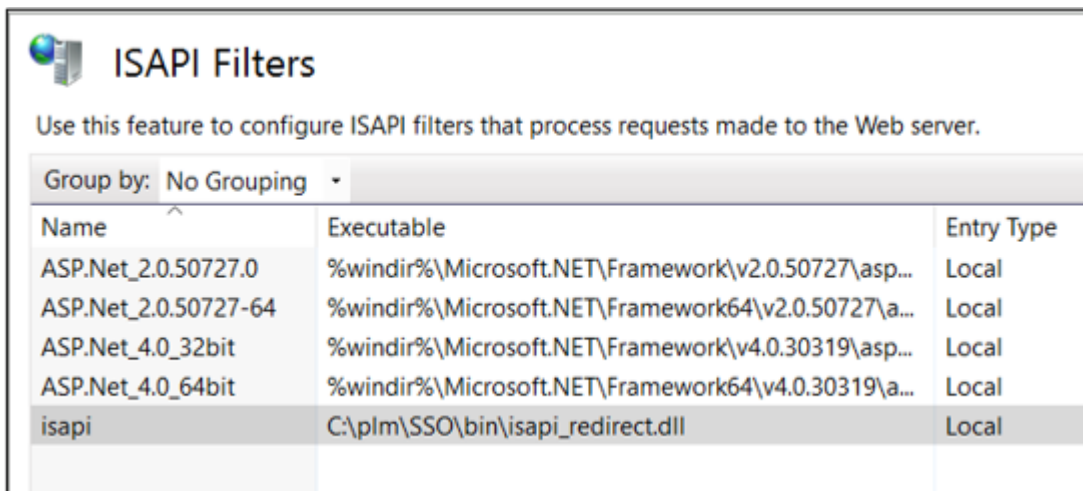
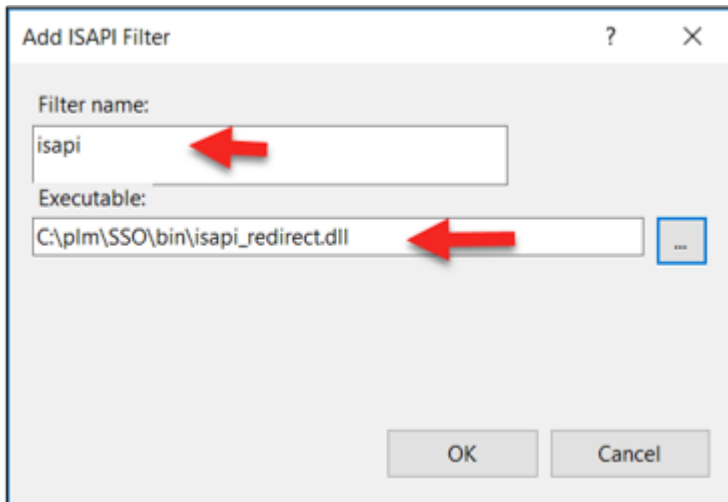
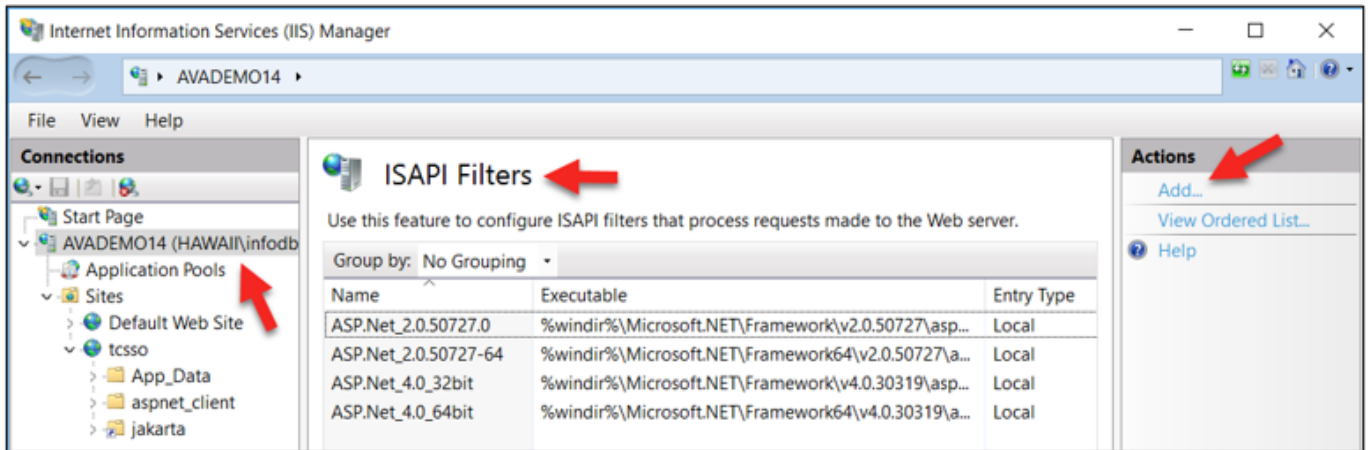
OK Cancel



5. ISAPI and CGI Restrictions



6. ISAPI-Filter



```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

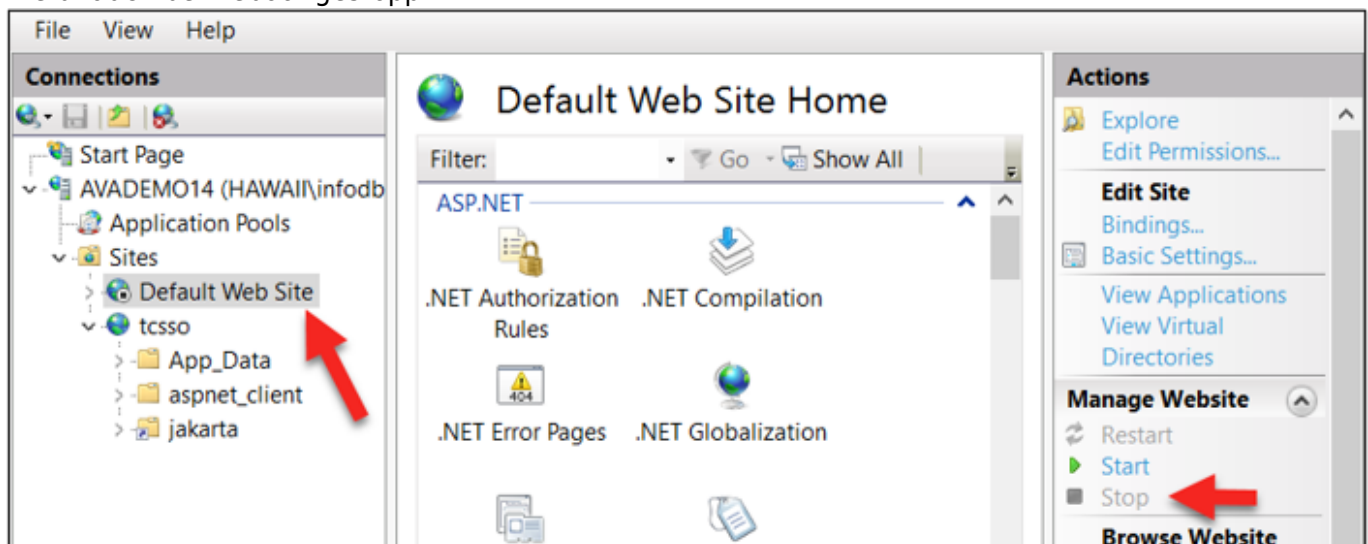
C:\Users\infodba>iisreset ←

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

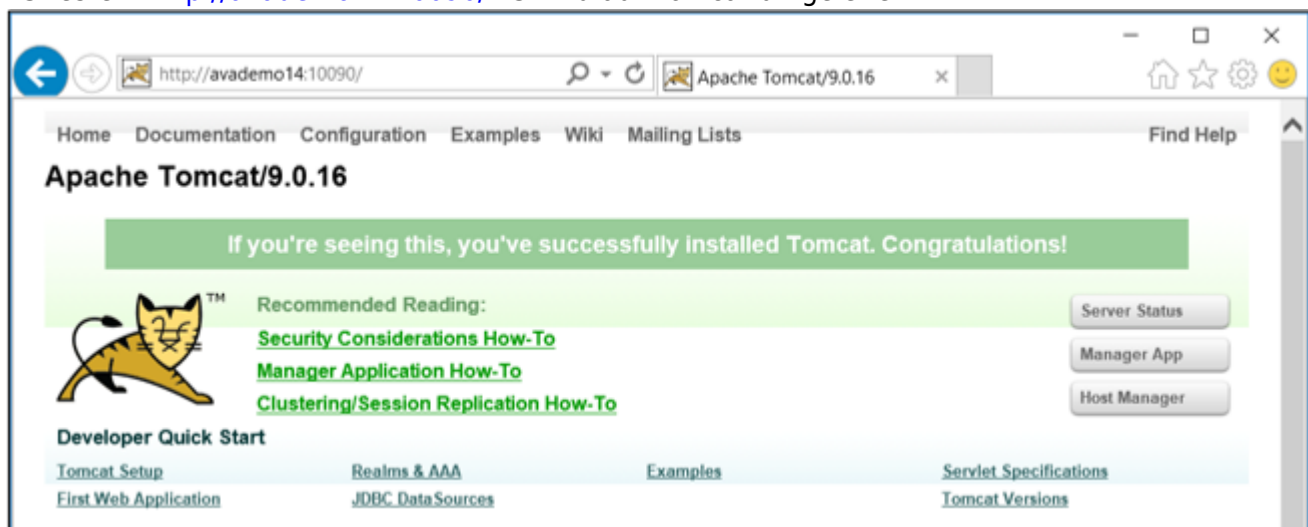
C:\Users\infodba>
```

7. Default Web Site deaktivieren

Bleibt auch bei Reboot gestoppt...



IIS testen: <http://avademol4:10090/> IIS wird auf Tomcat umgeleitet

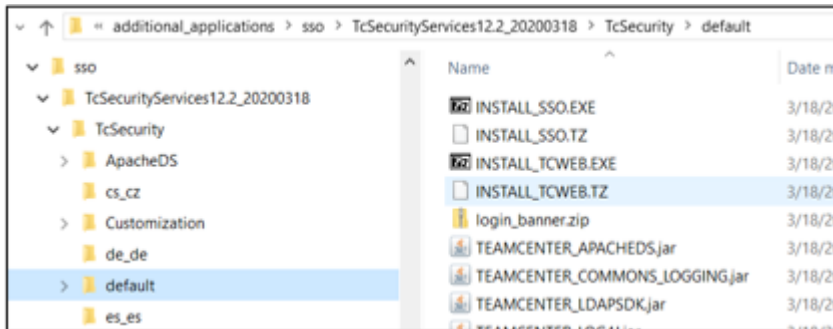


7. Installing Security Services

7.1 SSO Sources vorbereiten

In aktuell installiertem Patch, z.B.

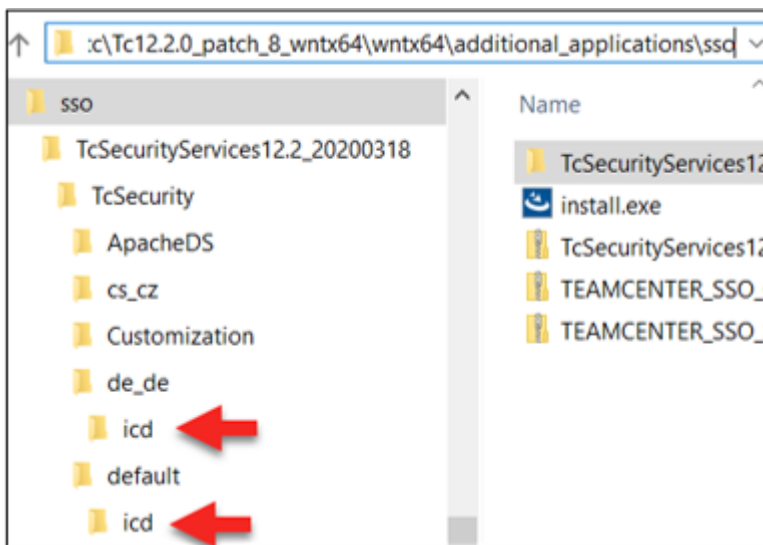
...\Tc12.2.0_patch_8_wntx64\wntx64\additional_applications\sso\TcSecurityServices12.2_20200318.zip
 ip
 entpacken:



Folgendes ausführen:

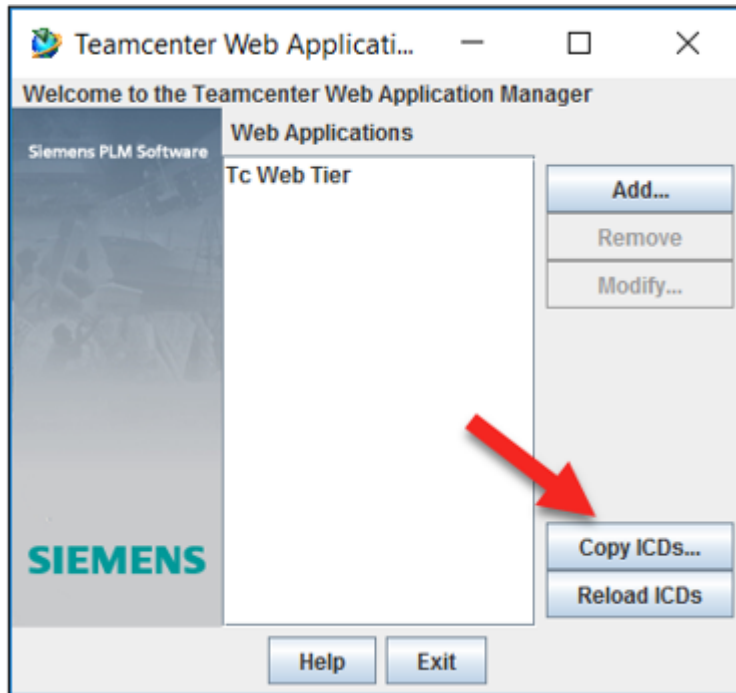
...\wntx64\additional_applications\sso\TcSecurityServices12.2_xx\TcSecurity\default\INSTALL_SSO.EXE
 ...\\wntx64\additional_applications\sso\TcSecurityServices12.2_xx\TcSecurity\de_de\INSTALL_SSO_DE_DE.EXE

Ergebnis: icd Folders

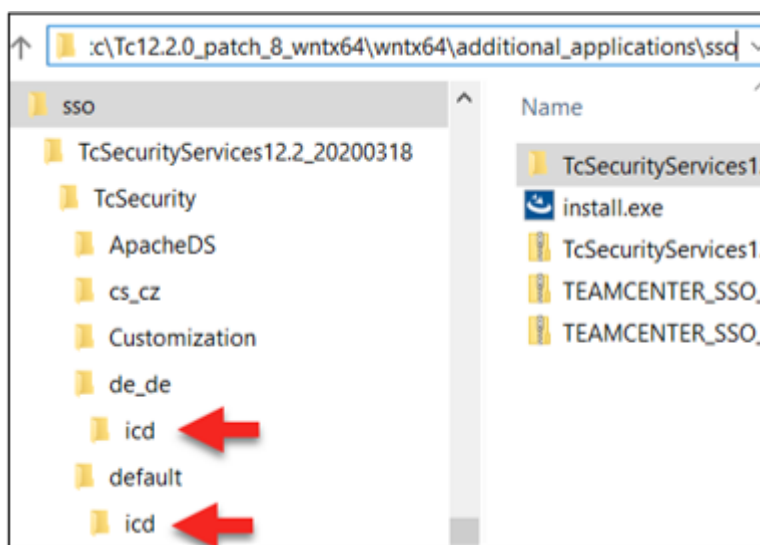


7.2 SSO ICD kopieren

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

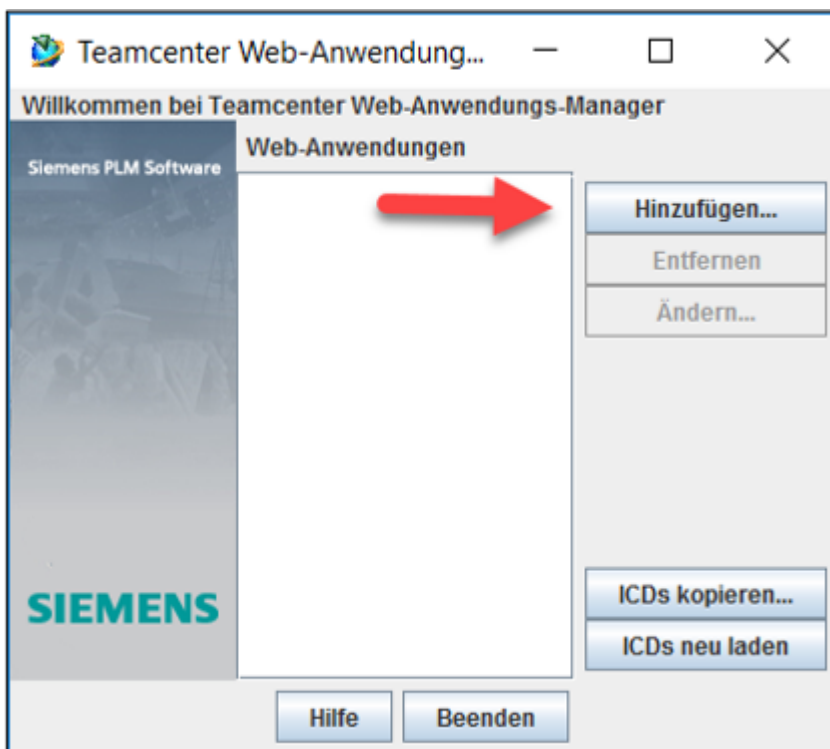
```
C:\Windows\system32\cmd.exe

C:\plm\web_tier>java -mx80m -cp jars\insweb.jar;jars\jdom.jar com.teamcenter.install.insweb.gui.Insweb
Loading of com.teamcenter.install.insweb.gui.TextBundle_de_DE ... succeeded.
Loading of com.teamcenter.install.insweb.struct.TextBundle_de_DE ... succeeded.
Loading of com.teamcenter.install.common.gui.TextBundle_de_DE ... succeeded.
```

Java must be installed...

Teamcenter Web-Anwendungs-Manager

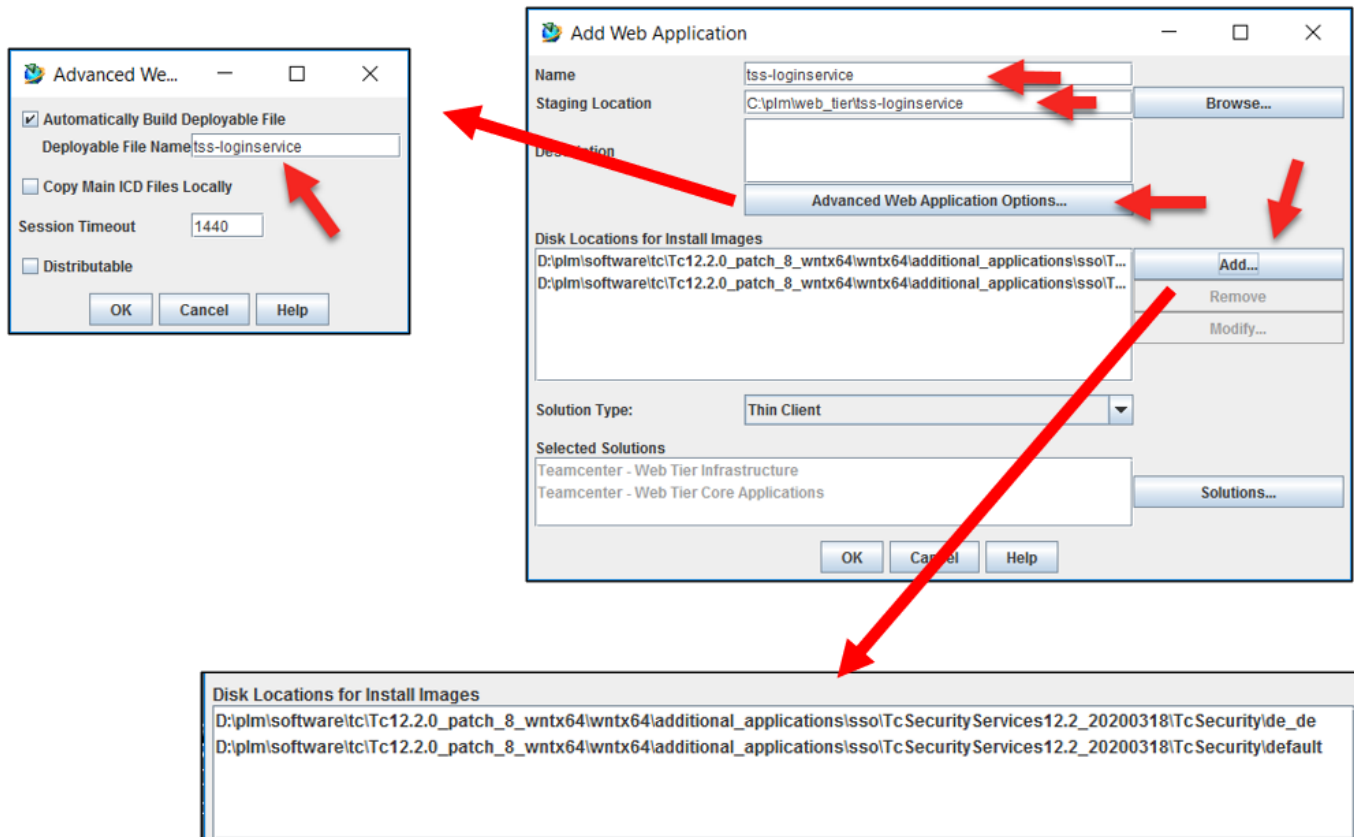
- Select: **Hinzufügen...**



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...

Enter disk locations

The Disk Locations for Install Images box contains the default path to the installation files for the Teamcenter solutions on the software distribution image. For this install, select the directory containing the **INSTALL_TCWEB.EXE/TZ** and **INSTALL_SSO.EXE/TZ** files for your system. You can change this default path if necessary by selecting one default path and clicking **Modify**.

Note

Additional language support requires the same process for each **INSTALL_SSO_locale.EXE** file. Add this location to the list of disk locations. For example, the *install-root\de_de* location contains the following files for the German language:

- TEAMCENTER_SSO_LOGINSERVICE_DE_DE.jar
- TEAMCENTER_SSO_LDAPIDPROVIDER_DE_DE.jar
- TEAMCENTER_SSO_LOGINSERVICE_HELP_DE_DE.jar

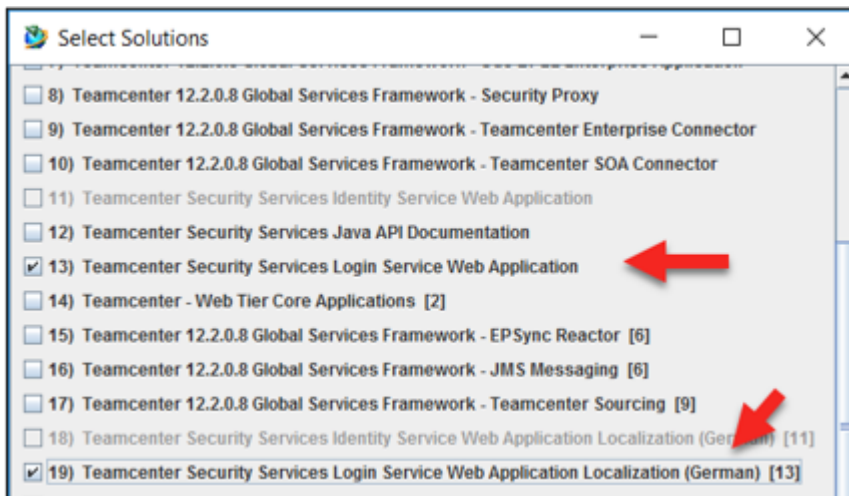
4. Solution Typ: → Thin Client

Lösungstyp: Thin Client

5. Selected Solutions

Solutions...

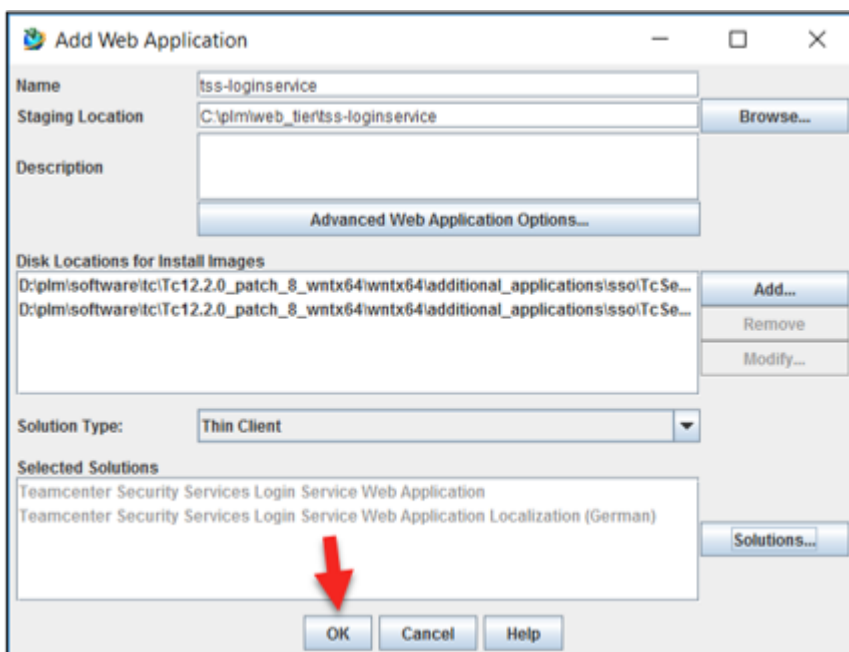
- Select the following:
 - **Security Services Login Service Web Application** (required)
 - **Language** (optional)



- Confirm with: OK

6. Terminate Add Web Application

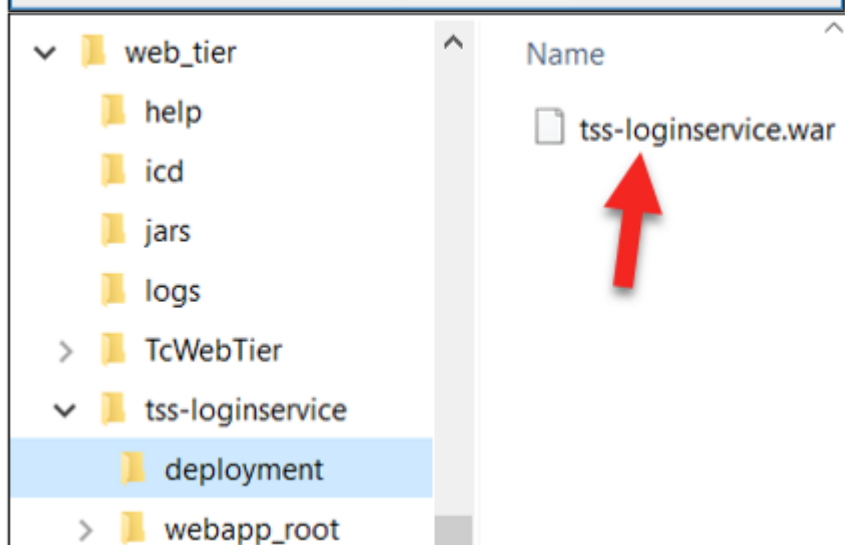
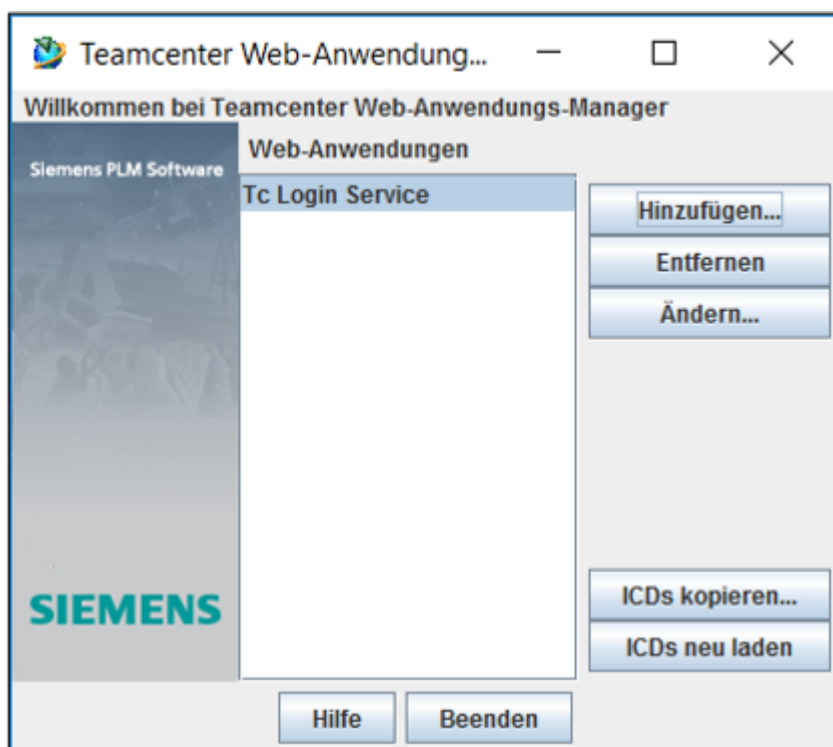
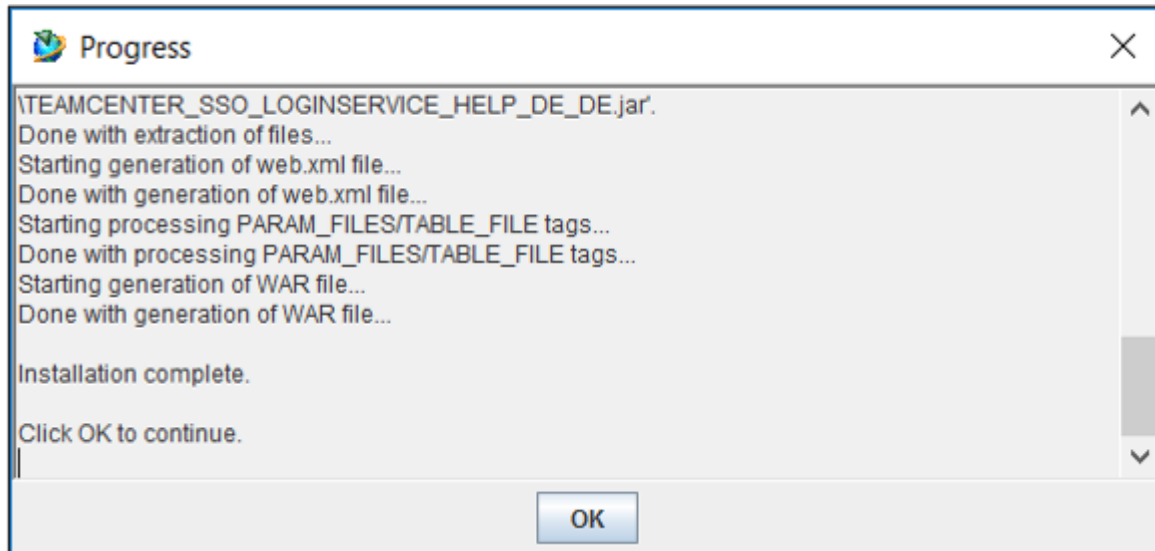
- Check entries...



- Confirm with: OK

7. Progress:

- Confirm with: OK

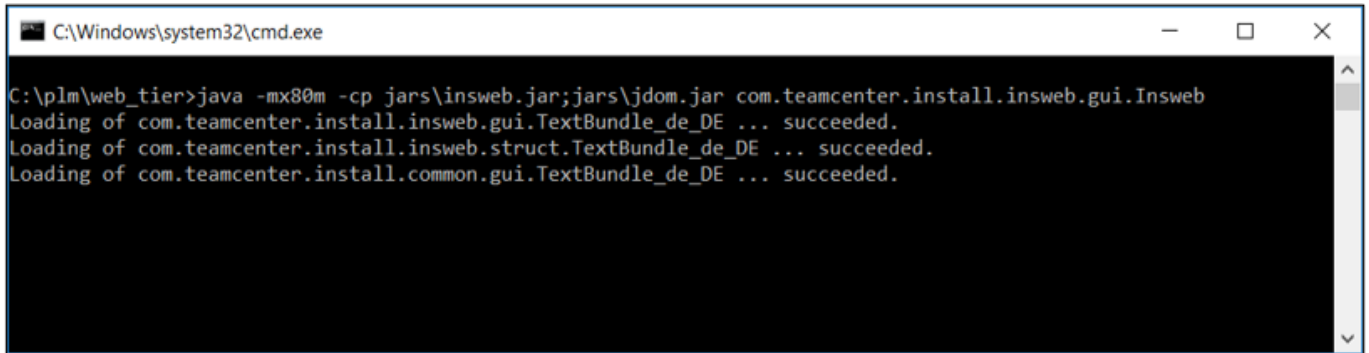


9. Tss-idservice erstellen

9.1 Create the Identity Service

1. Start the Web Application Manager

- c:\plm\web_tier\insweb.bat

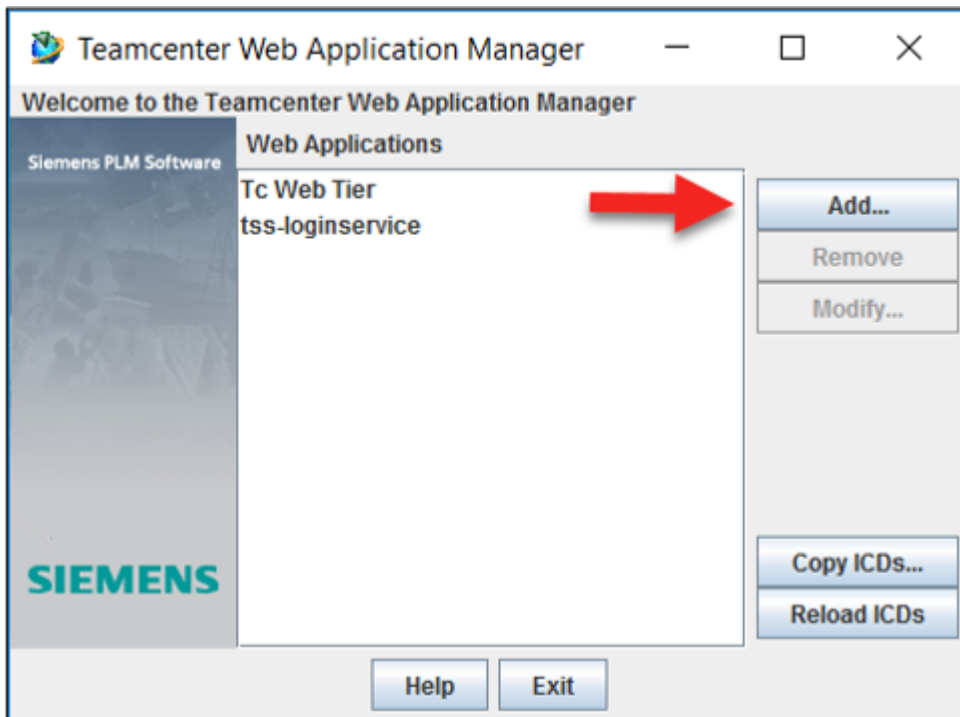


```
C:\Windows\system32\cmd.exe

C:\plm\web_tier>java -mx80m -cp jars\insweb.jar;jars\jdom.jar com.teamcenter.install.insweb.gui.Insweb
Loading of com.teamcenter.install.insweb.gui.TextBundle_de_DE ... succeeded.
Loading of com.teamcenter.install.insweb.struct.TextBundle_de_DE ... succeeded.
Loading of com.teamcenter.install.common.gui.TextBundle_de_DE ... succeeded.
```

Teamcenter Web-Anwendungs-Manager

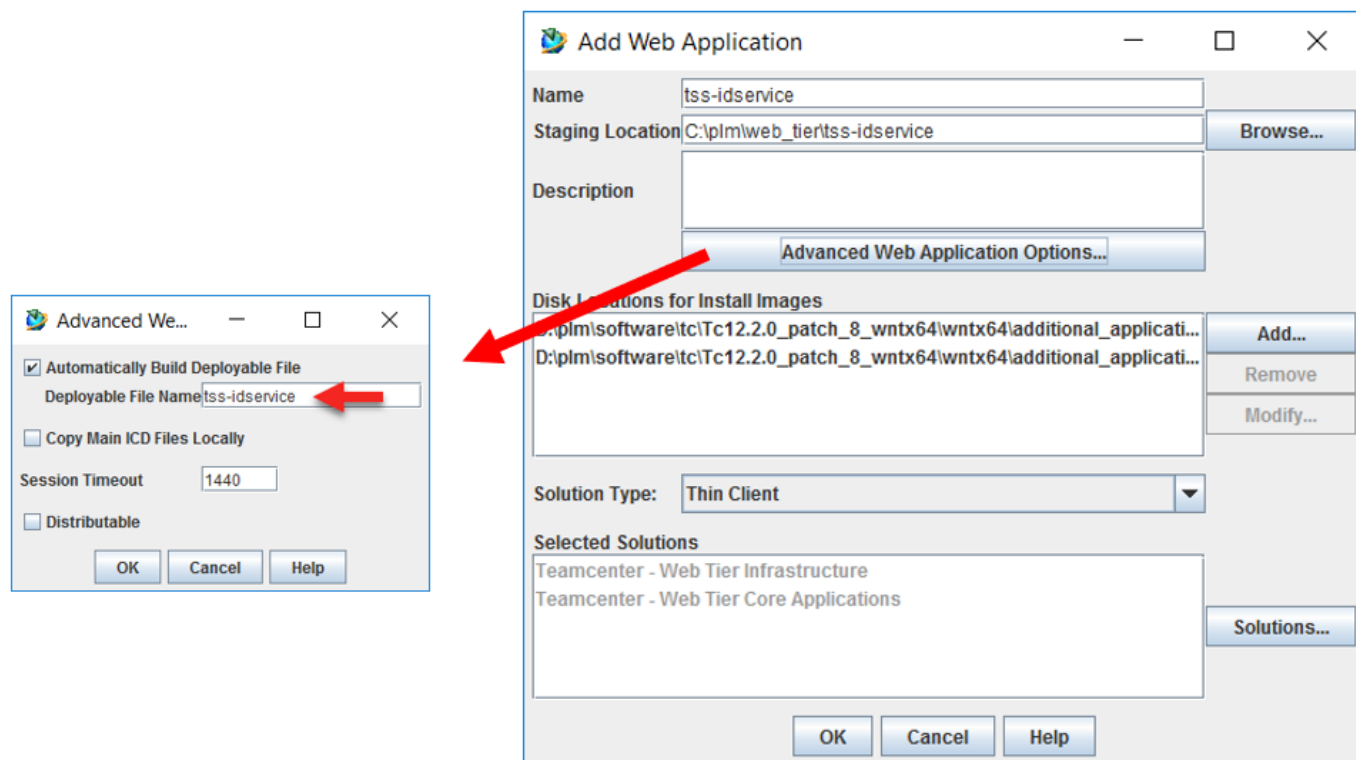
- Select: **Hinzufügen...**



Add Web Application

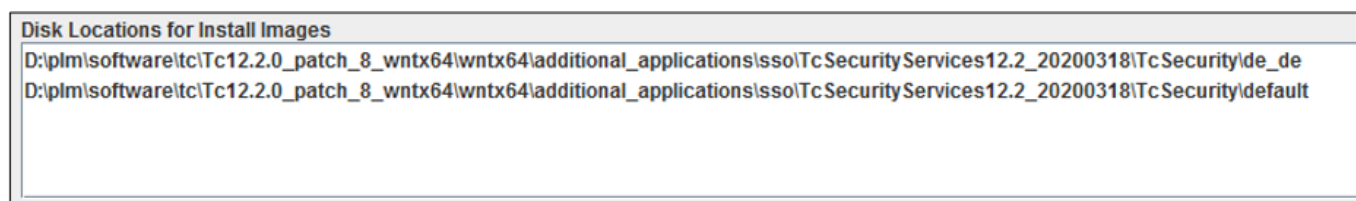
- Name: tss-idservice
- Staging Location: c:\plm\web_tier\tss-idservice
- Advanced Web Application Options...

Zu verwendende Datei: tss-idservice

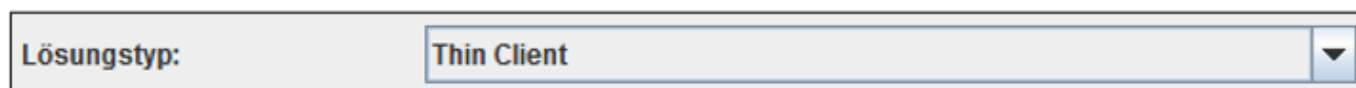


2. Disk Locations for Install Images

- Add...



3. Solution Typ: → Thin Client

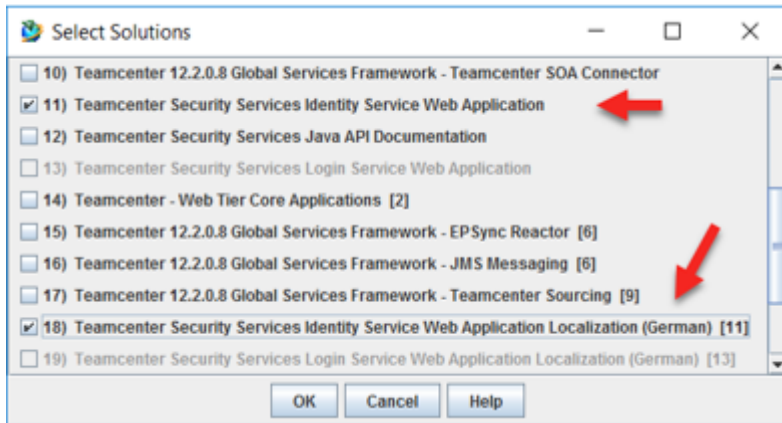


4. Selected Solutions



Select the following:

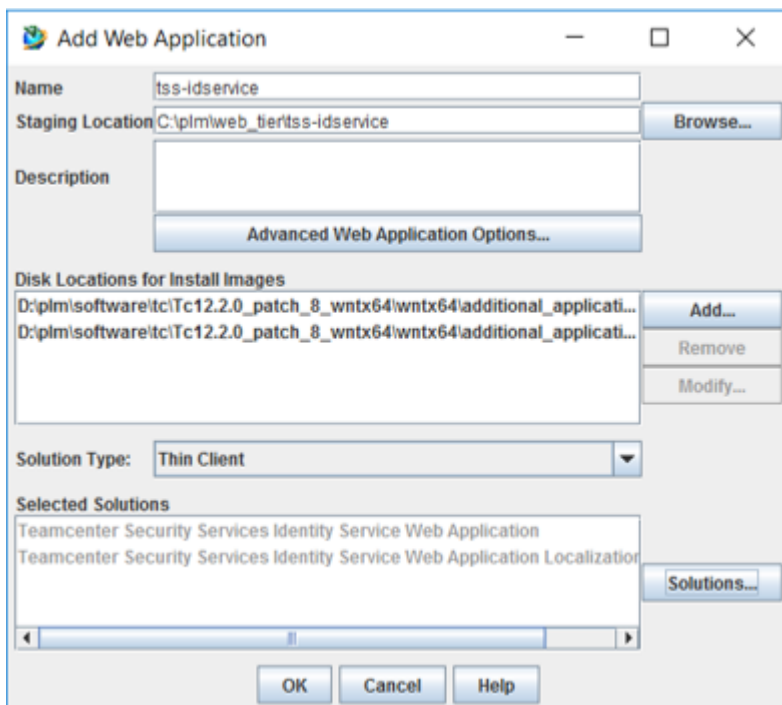
- **TC Security Services Identity Service Web Application** (required)
- **Language** (optional)



- Confirm with: OK

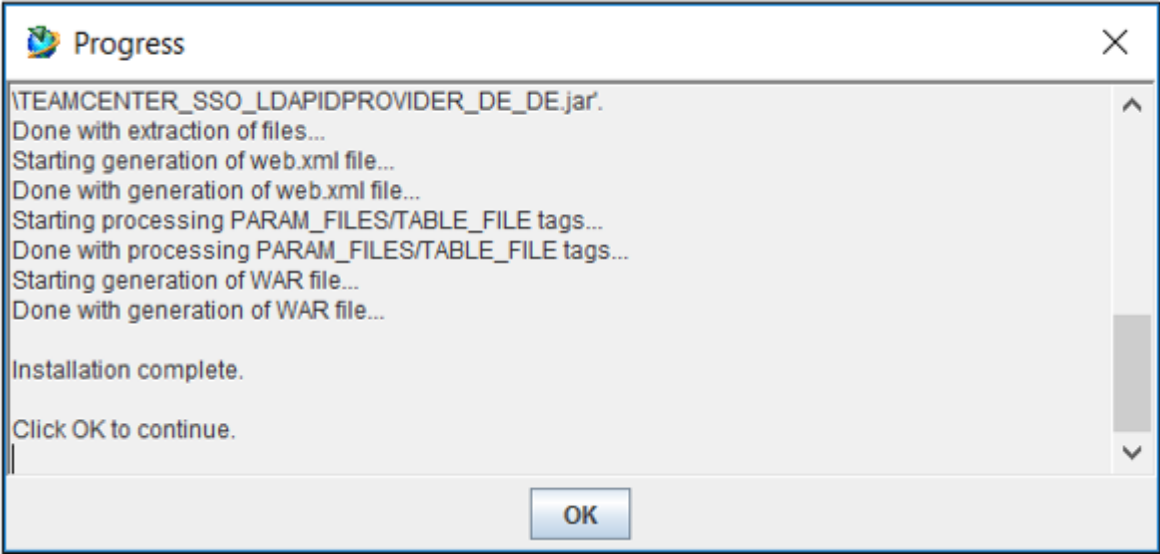
Terminate Add Web Application

- Check entries...

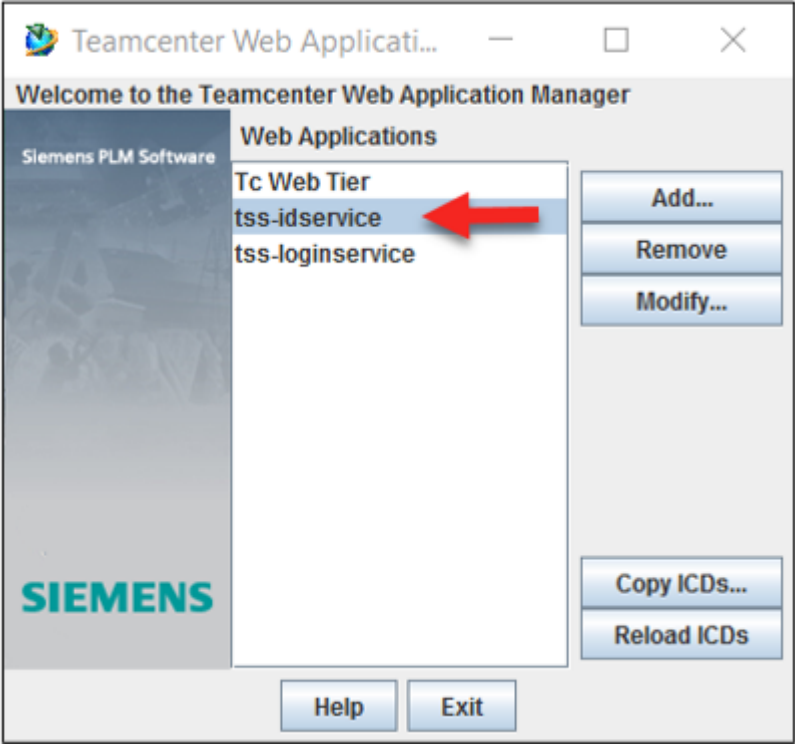


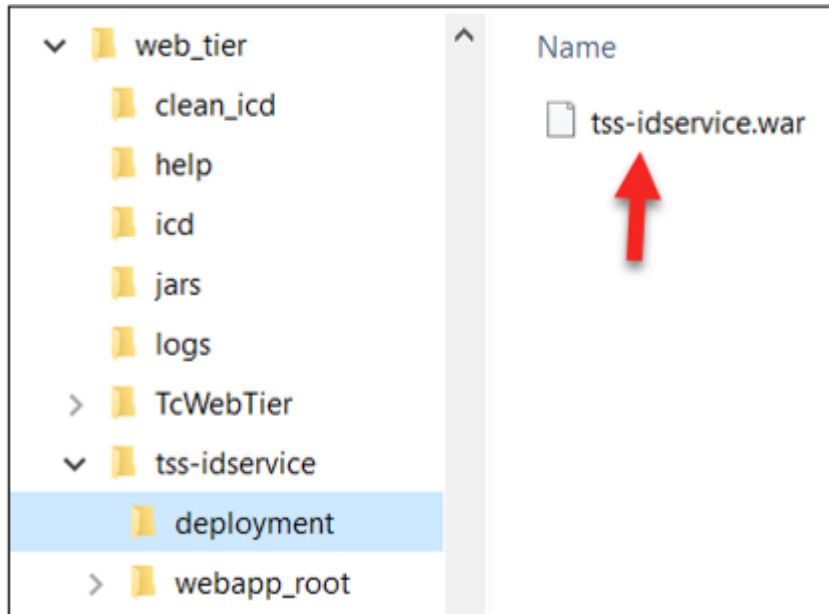
- Confirm with: OK

5. Progress:



- Confirm with: **OK**

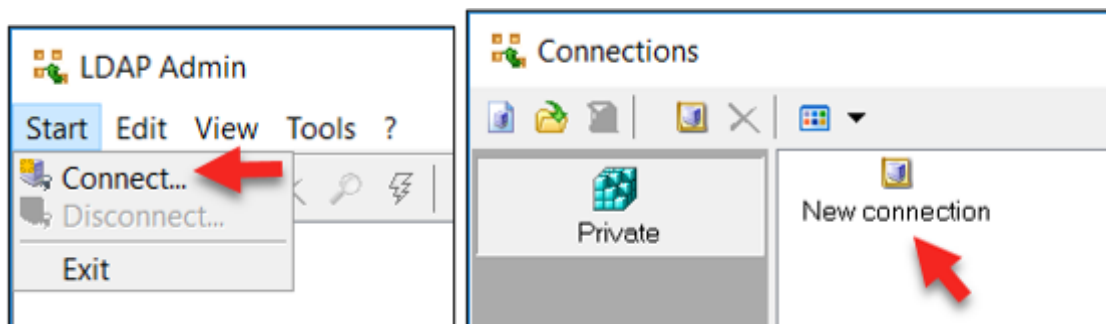




10. Tss-loginservices anpassen

10.1 LdapAdmin

10.1.1 Mit LdapAdmin Loginuser überprüfen



Connection properties

Connection name:

General Options Attributes

Connection:

Host: Port: Version:

Base:

☒ Simple authentication
☐ GSS-API

Account

Username:

Password:

☐ Anonymous connection

Ldapadmin

Connection is successful.

10.1.2 tss-loginservice anpassen, Modify Tables

Teamcenter Web Applicati...

Welcome to the Teamcenter Web Application Manager

Web Applications

Siemens PLM Software

Tc Web Tier

tss-idservice

tss-loginservice

Modify Web Application

Name:

Staging Location:

Description:

Solution Type: **Thin Client**

Installed Solutions:

- Teamcenter Security Services Login Service Web Application
- Teamcenter Security Services Login Service Web Application Localization (German)

ICD Files Last Copied: <No copy done>

Buttons: OK, Cancel, Help

Right Panel Buttons:

- Modify Web Application Information...
- Modify Disk Locations...
- Modify Context Parameters...
- Modify Tables...
- Add Solutions...
- Reinstall Solutions...
- Generate Deployable File...
- Copy ICD Files...
- View Component Versions...



Modify...

Tables

Login Input Definitions

Buttons: OK, Cancel, Help

Modify...



Modify Table

Table: Login Input Definitions

name	where	required	idpkey
tcsso_username	form	true	User
tcsso_password	form	false	Password
tcsso_newpassword	form	false	NewPassword
tcsso_confirmpass...	form	false	NotNeeded
tcsso_locale	form	false	UserLocale

Buttons: Add Row..., Remove Row

Table Description

The value must be of type 'BOOLEAN'. This column requires a value in each field.

* idpkey: This defines the corresponding key name as known within the underlying identity provider.

The value must be of type 'STRING'. This column requires a value in each field.

Buttons: OK, Cancel, Help



10.1.3 tss-loginservice anpassen, Modify Context Parameters

Modify Web Application

Name: tss-loginservice

Staging Location: C:\plm\web_tier\tss-loginservice

Description:

Solution Type: Thin Client

Installed Solutions

- Teamcenter Security Services Login Service Web Application
- Teamcenter Security Services Login Service Web Application Localization (German)

ICD Files Last Copied: <No copy done>

Buttons on the right:

- Modify Web Application Information...
- Modify Disk Locations...
- Modify Context Parameters...
- Modify Tables...
- Add Solutions...
- Reinstall Solutions...
- Generate Deployable File...
- Copy ICD Files...
- View Component Versions...

Buttons at the bottom:

- OK
- Cancel
- Help

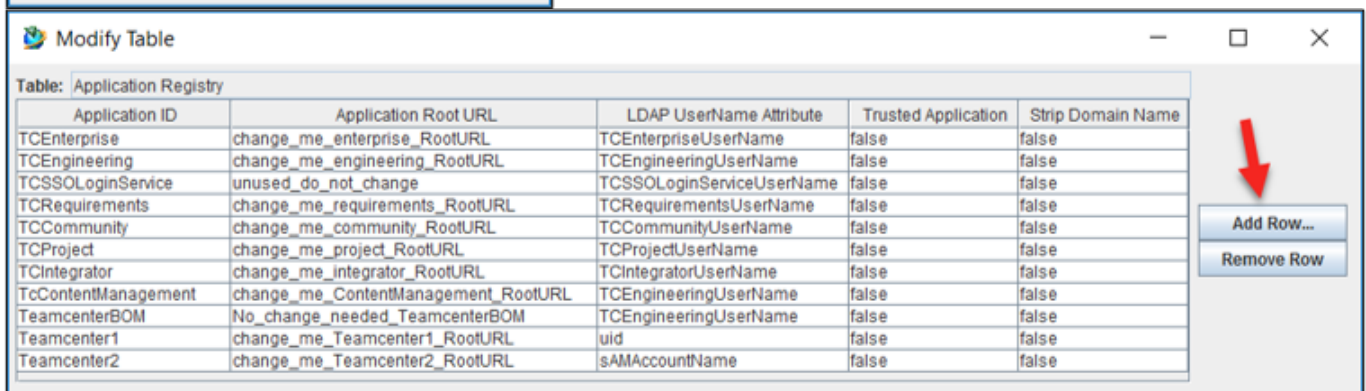
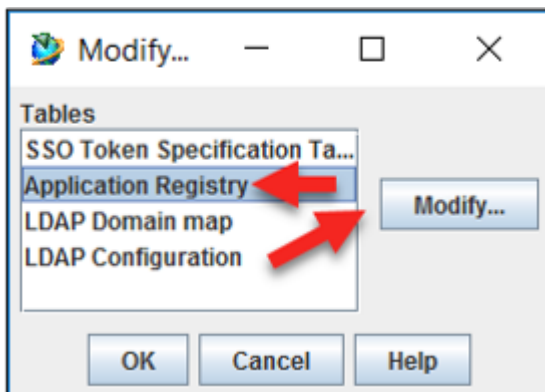
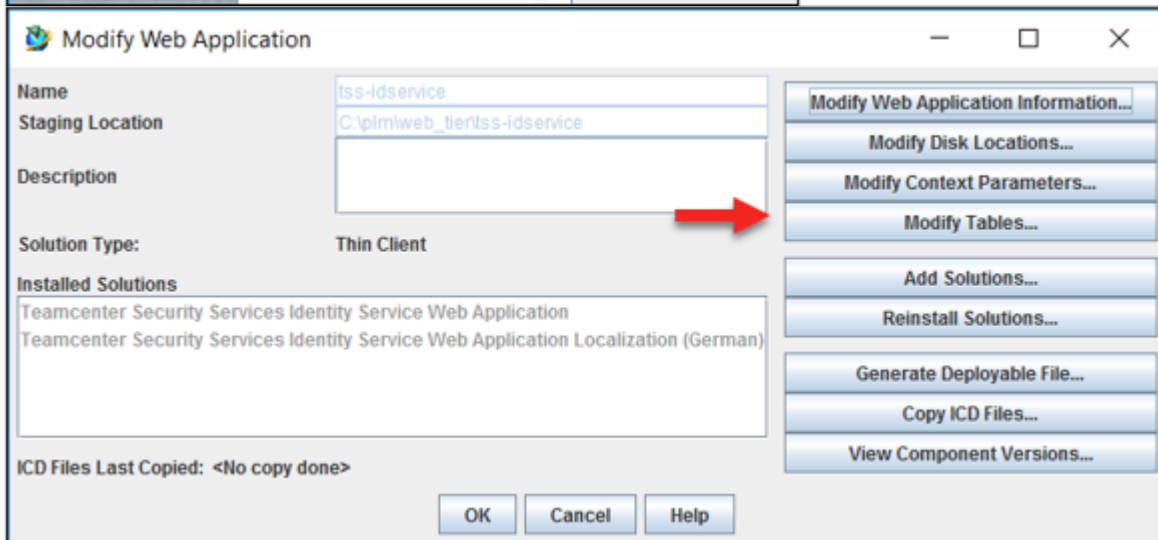
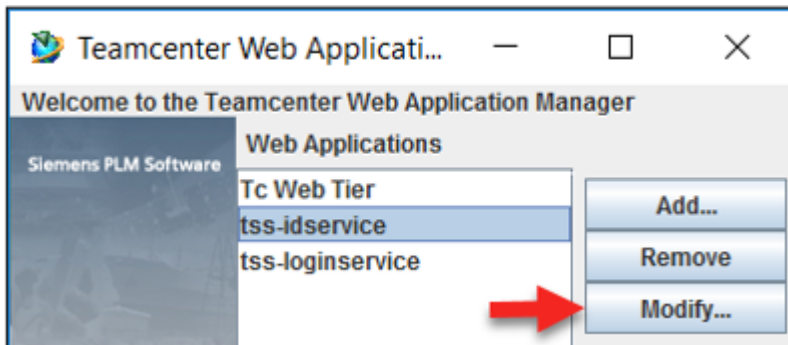
tcsso.login_service.sso_service_url:	http://avademo14.hawaii.com:7070/tss-idservice
identityServicePassword:	sicheres Passwort eingeben: 1nFodbAA
tcsso.behind_sso_gateway:	true
tcsso.gateway.field.type:	remote_user
tcsso.gateway.field.name:	REMOTE_USER
tcsso.login_service.enable_session_agent_applet: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



Context Parameters		
Req	Name	Value
☐	webmaster	change_me_webmaster_name@change_me_email_domain
☐	tcsso.login_service.appid	TCSSOLoginService
☐	tcsso.login_service.http_connection_close	keep-alive
☐	tcsso.login_service.rp_cookieNamePattern	PD-H-SESSION-ID, PD-S-SESSION-ID, SMSESSION
☐	tcsso.login_service.proxyURL	
☐	tcsso.login_service.sso_service_url	http://avademio14.hawaii.com:7070/tss-idservice
☐	identityServicePassword	*****
☐	tcsso.behind_sso_gateway	true
☐	tcsso.gateway.field.type	remote_user
☐	tcsso.gateway.field.name	REMOTE_USER
☐	tcsso.username.filter.class	
☐	tcsso.client.enable.notice.consent.logon.banner	false
☐	tcsso.forgotten.password.URL	
☐	tcsso.online_help.enable	true
☐	tcsso.login_service.enable_session_agent_applet	false
☐	tcsso.login_service.force_web_browser_login	false
☐	tcsso.frame_ancestors	none
☐	tcsso.federation_type	none
☐	tcsso.federation_url	
☐	tcsso.federation_reply_url	
☐	tcsso.federation_logout_url	
☐	tcsso.cors_whitelist	
☐	DEBUG	warn
☐	tcsso.login_service.enableCsrf	false

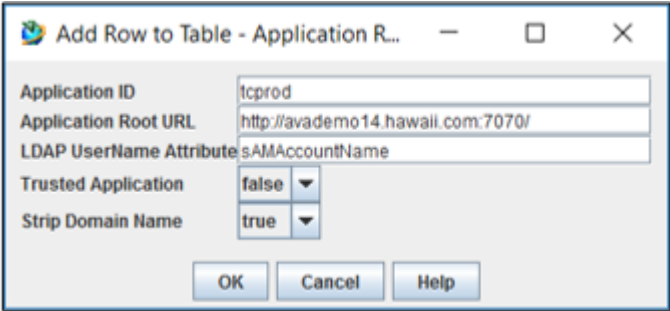
10.2 Tss-idservices anpassen

10.2.1 tss-idservice anpassen, Modify Tables

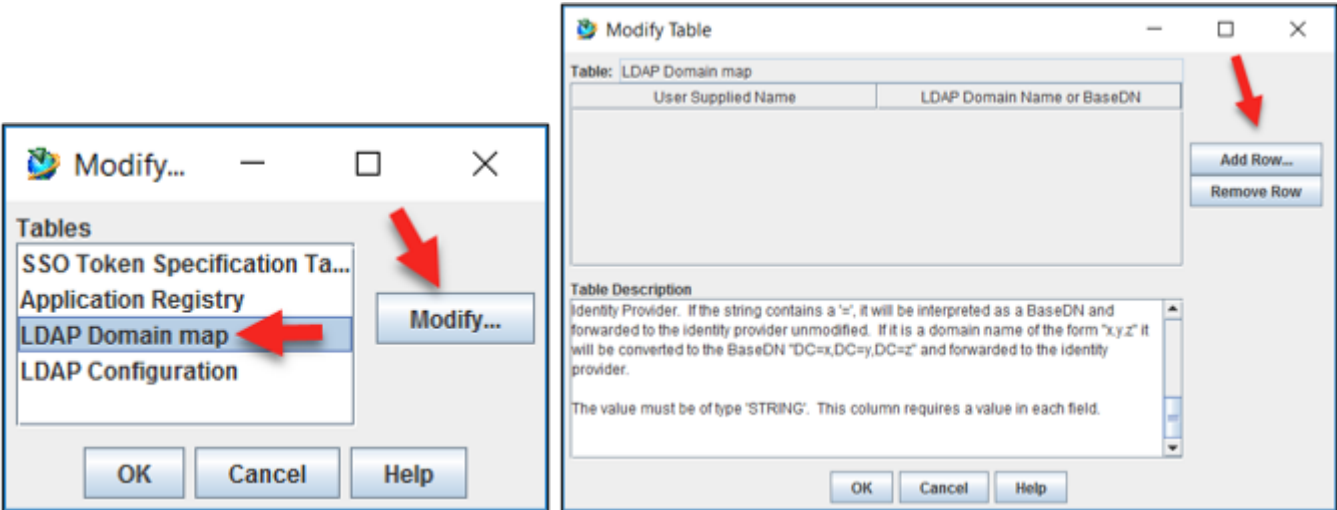
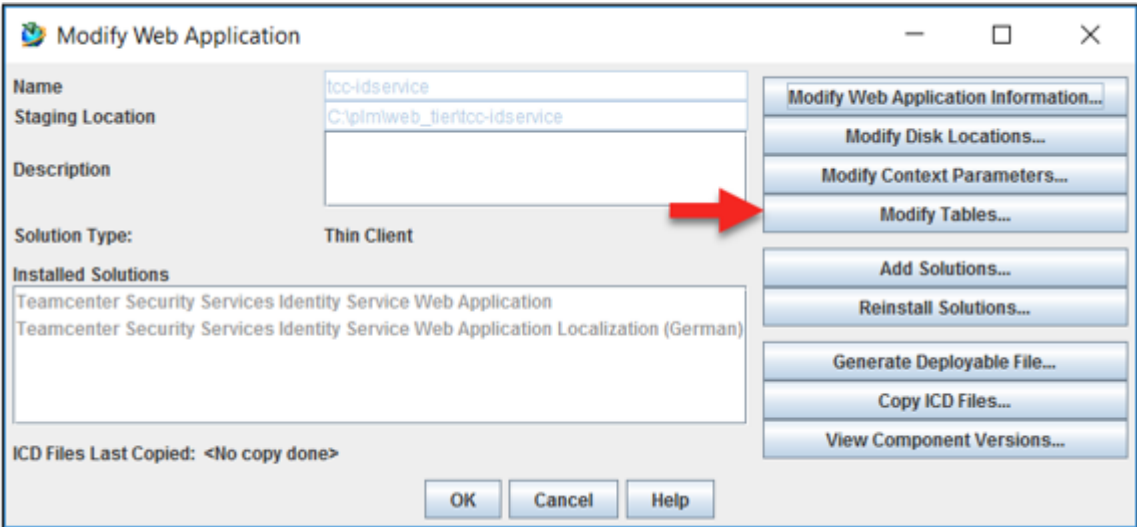


Application ID:	tcprod (SID...)
Application Root URL:	http://avademo14.hawaii.com:7070/

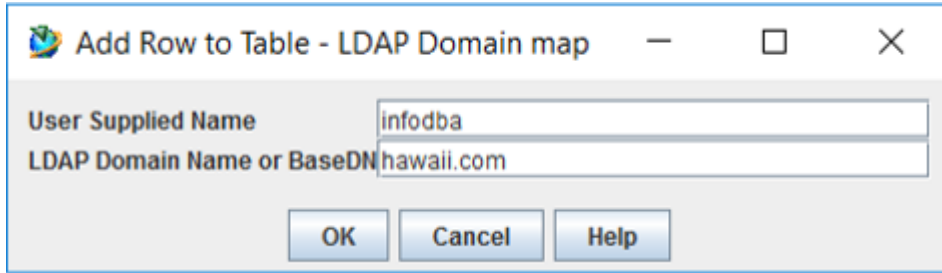
LDAP UserName Attribute:	sAMAccountName
Trusted Application:	false
Strip Domain Name:	true



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



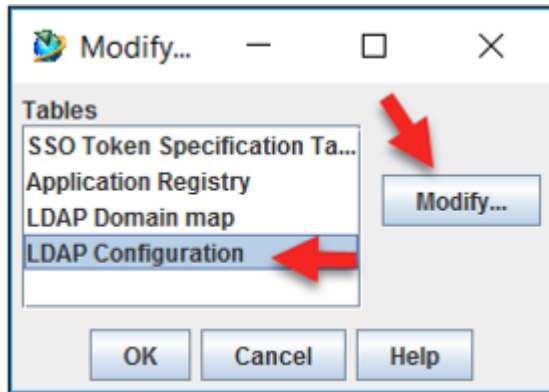
Add Row to Table - LDAP Domain map

User Supplied Name: infodba

LDAP Domain Name or BaseDN: hawaii.com

OK Cancel Help

10.2.3 tss-idservice anpassen, Modify Tables



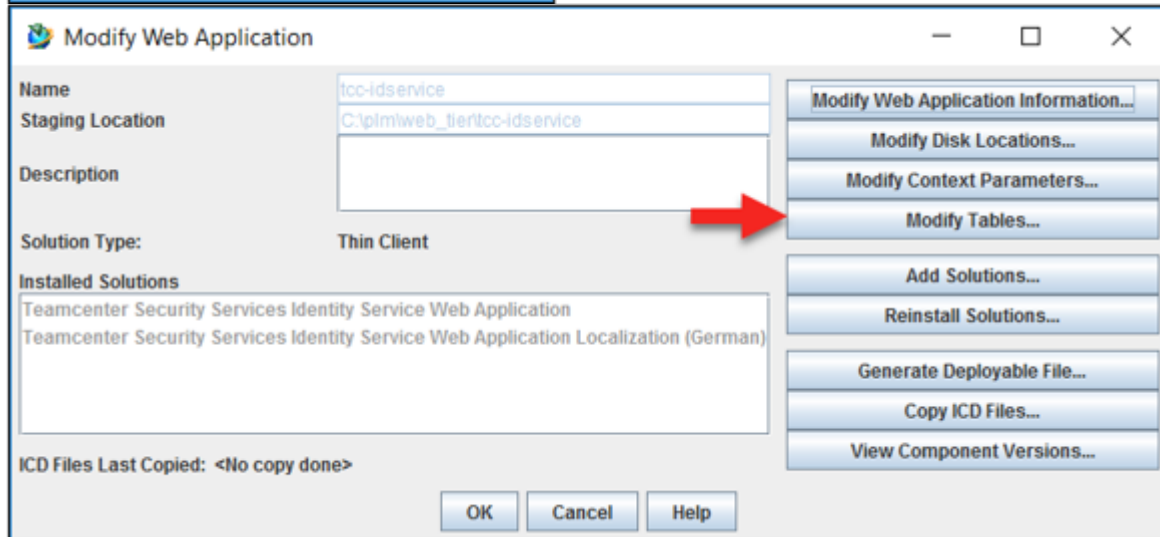
Modify...

Tables

- SSO Token Specification Ta...
- Application Registry
- LDAP Domain map
- LDAP Configuration**

Modify...

OK Cancel Help



Modify Web Application

Name: tcc-idservice

Staging Location: C:\pim\web_tier\tcc-idservice

Description:

Solution Type: Thin Client

Installed Solutions:

- Teamcenter Security Services Identity Service Web Application
- Teamcenter Security Services Identity Service Web Application Localization (German)

ICD Files Last Copied: <No copy done>

Modify Web Application Information...

Modify Disk Locations...

Modify Context Parameters...

Modify Tables...

Add Solutions...

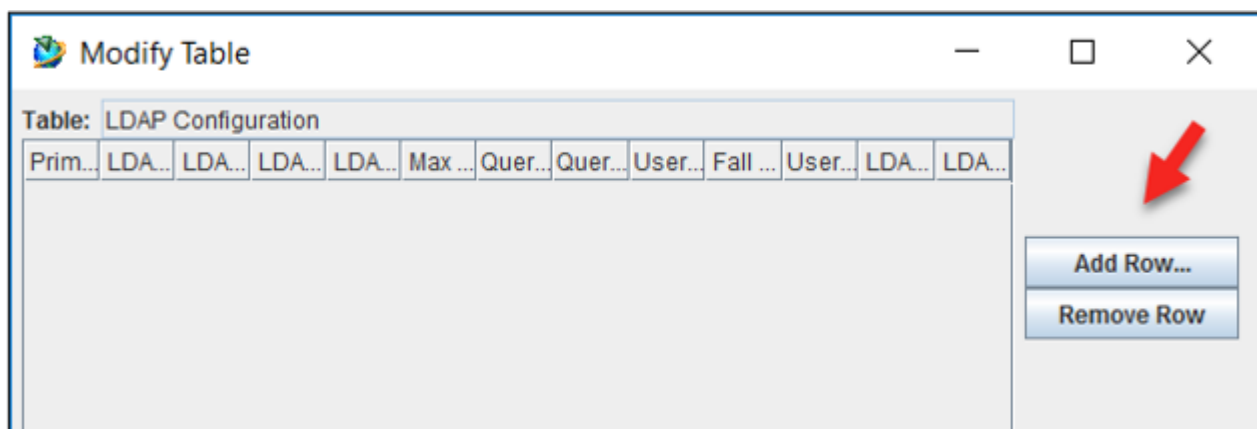
Reinstall Solutions...

Generate Deployable File...

Copy ICD Files...

View Component Versions...

OK Cancel Help



Modify Table

Table: LDAP Configuration

Prim...	LDA...	LDA...	LDA...	LDA...	Max ...	Quer...	Quer...	User...	Fall ...	User...	LDA...	LDA...

Add Row...

Remove Row

Add Row to Table - LDAP Configurati...

Primary LDAP

LDAP Host

LDAP Port Number

LDAP Port Number Override?

LDAP Connect Type

Max LDAP Connections

Query DN

Query DN Password

UserObjectClass

Fall back to User Attribute

User Attribute

LDAP Connection Setup Delay

LDAP Connection Timeout

OK

Cancel

Help

Y

avademo14.hawaii.com

389

N

ldap

20

infodba@hawaii.com

user

Y

sAMAccountName

-1

0

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

Modify Web Application

Name: tcc-id-service
 Staging Location: C:\plm\web_tier\tcc-id-service
 Description:
 Solution Type: Thin Client
 Installed Solutions:
 Teamcenter Security Services Identity Service Web Application
 Teamcenter Security Services Identity Service Web Application Localization (German)
 ICD Files Last Copied: <No copy done>

Buttons on the right:
 Modify Web Application Information...
 Modify Disk Locations...
 Modify Context Parameters...
 Modify Tables...
 Add Solutions...
 Reinstall Solutions...
 Generate Deployable File...
 Copy ICD Files...
 View Component Versions...

Buttons at the bottom: OK, Cancel, Help

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

Authentication events dropdown menu:

- None
- Authentication successful
- Authentication failures
- All authentication events (selected)

Modify Context Parameters

Req	Name	Value
☐	webmaster	change_me_webmaster_name...
☐	identityProvider	com.teamcenter.ss.identity.spi...
☐	identityServicePassword	
☐	passwordLifetime	30
☐	mediatorPassword	
☐	tokenLifetime	600
☐	sessionLifetime	600
☐	tcsso.LogLevel	All authentication events
☐	tcsso.AuthLogDir	c:\plm\SSO\log
☐	LDAPVersion	3
☐	PasswordResetEnabled	false
☐	PasswordResetMessage	
☐	GatewayAliasingEnabled	false
☐	ReferralsEnabled	false
☐	ReferralHopLimit	5
☐	DEBUG	warn

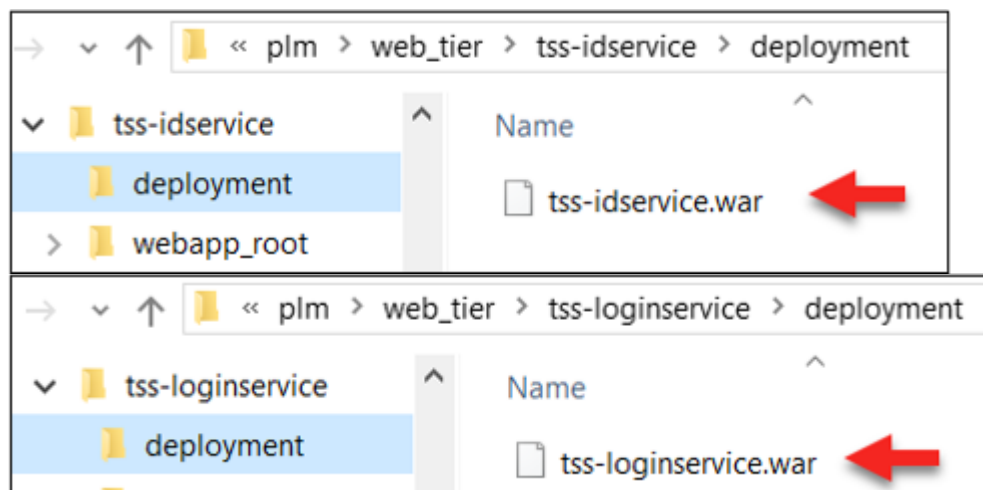
Progress

File generation complete.
 Click OK to continue.

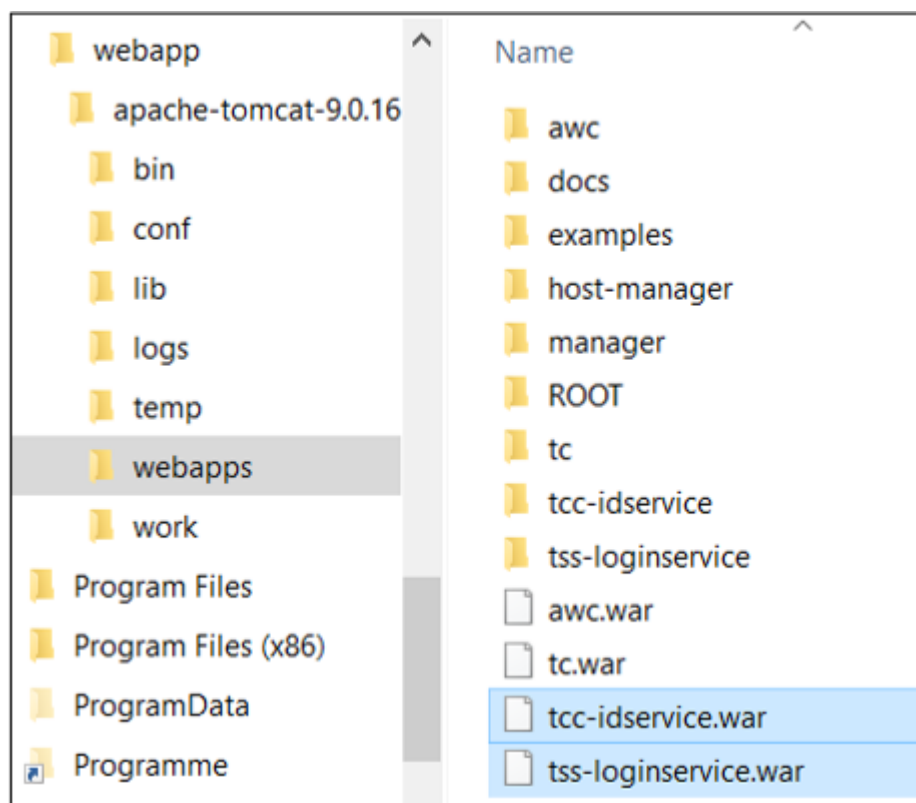
OK

10.2.5 Deploy war-Files

Kopieren



nach



11. TCServer Manager changes

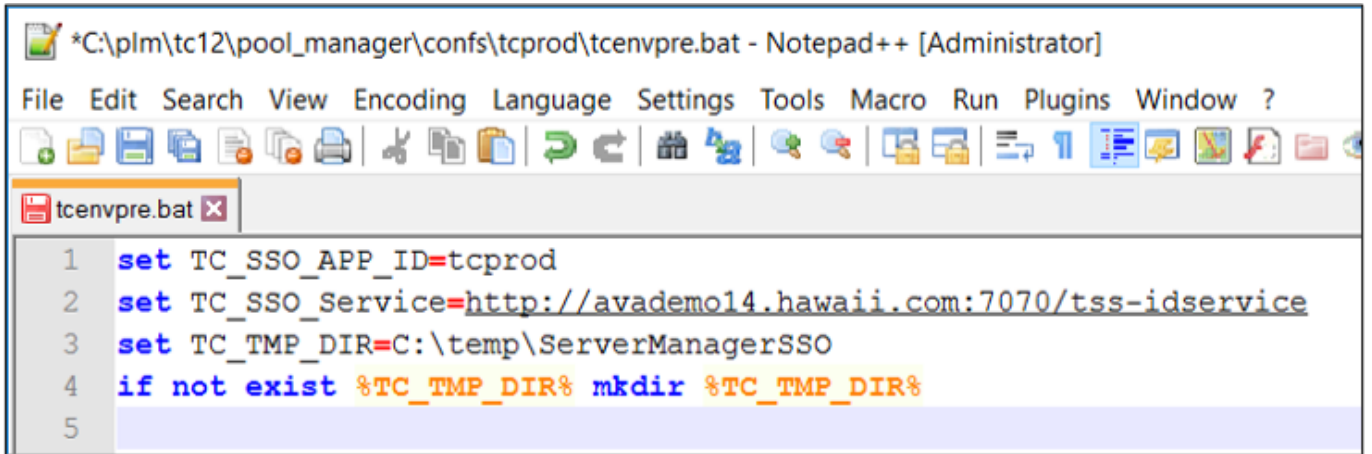
11.1 tcenvpre.bat

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://avademol4.hawaii.com:7070/tss-idservice
set TC_TMP_DIR=C:\temp\ServerManagerSSO
if not exist %TC_TMP_DIR% mkdir %TC_TMP_DIR%
```



```
*C:\plm\tc12\pool_manager\confs\tcprod\tcenvpre.bat - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
tcenvpre.bat
1 set TC_SSO_APP_ID=tcprod
2 set TC_SSO_Service=http://avademol4.hawaii.com:7070/tss-idservice
3 set TC_TMP_DIR=C:\temp\ServerManagerSSO
4 if not exist %TC_TMP_DIR% mkdir %TC_TMP_DIR%
5
```