Titel: E-ConsentPro Single Sign On
Version 1.5 vom 30.05.2025
Satz: Dr. Ira Zauner
Geprüft: Daniel Pfeil

Thieme Compliance

E-ConsentPro Single Sign On

Ab ECP 7.0

Inhalt

Thieme Compliance

1. ECP SSO Übersicht

Die Implementierung von ECP SSO basiert auf SPNEGO und Kerberos v5.

In Abbildung 1.1 sind die am SSO-Betrieb beteiligten Akteure und Interaktionen dargestellt.

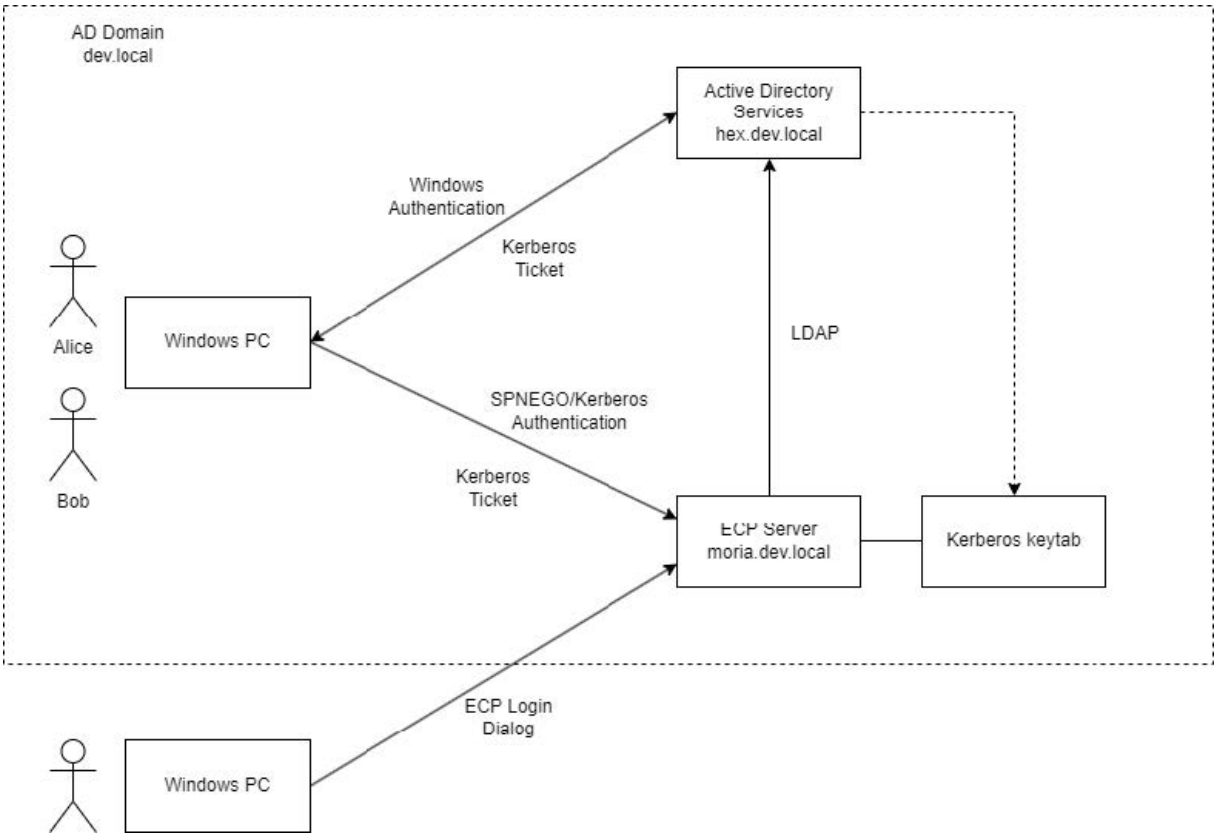


Abbildung 1.1: ECP SSO in einer Windows AD-Domain.

In den folgenden Beispielen gehen wir davon aus, dass:

- die Windows-Domain „dev.local“ heißt
- der Domänencontroller „hex.dev.local“ ist
- ECP auf dem Host „moria.dev.local“ installiert wird
- der ECP-Dienst als Benutzer „dev\ecpsvc“ läuft
- Alice ein Konto in der Domain „dev.local“ hat

Die SSO-Einrichtung umfasst die Konfiguration des ECP-Servers und die Vorbereitung der Benutzerkonten. Die folgende Abbildung enthält eine Liste der erforderlichen Maßnahmen, während Abschnitt 2 dieses Dokuments detaillierte Anweisungen enthält.

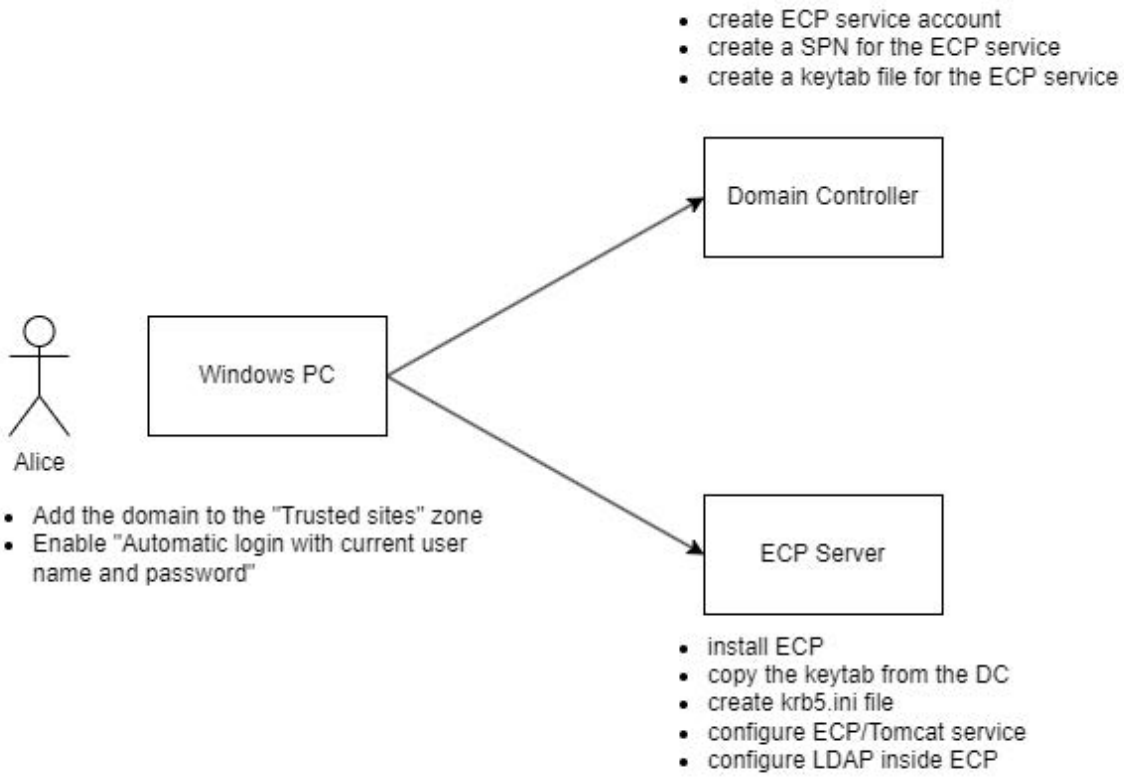


Abbildung 1.2: ECP SSO Konfiguration

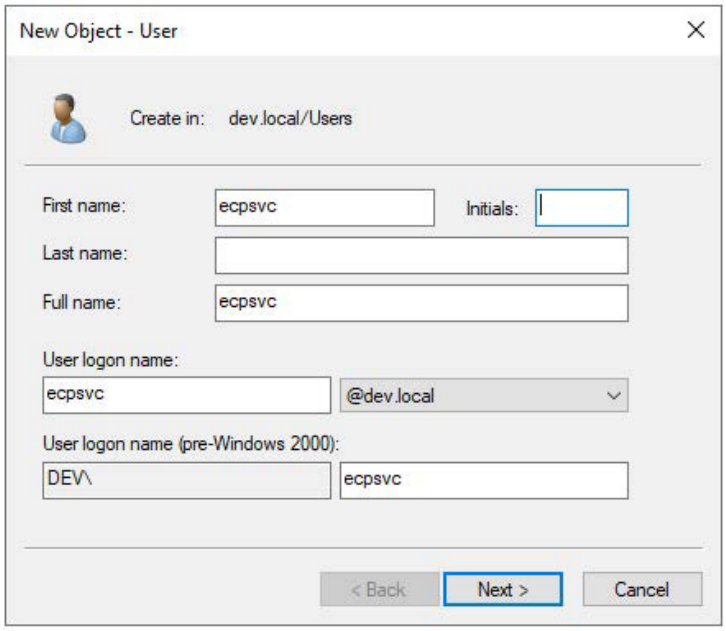
2. ECP SSO konfigurieren

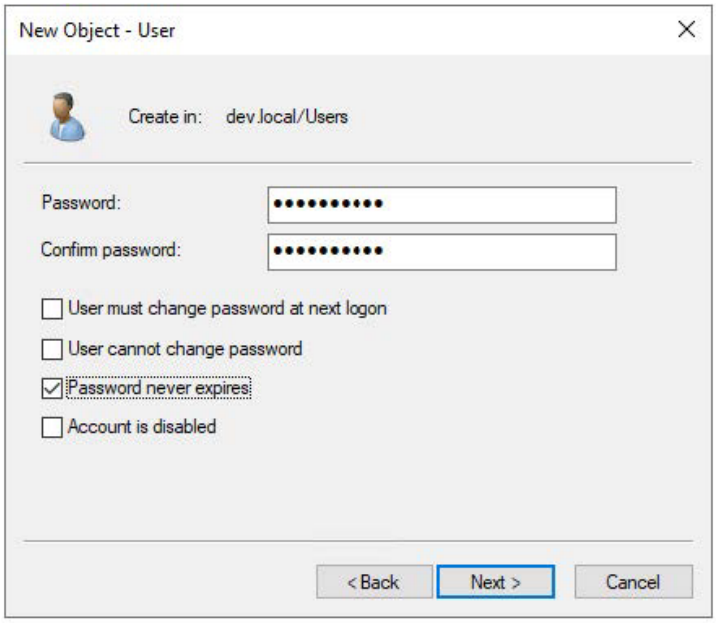
2.1. Active Directory

2.1.1. ECP-Dienstkonto erstellen

Erstellen Sie auf hex.dev.local ein Konto, das zur Ausführung des ECP-Dienstes auf dem Host ecp.dev.local verwendet werden soll.

Stellen Sie sicher, dass das Konto Kerberos AES128bit und AES256bit Verschlüsselung unterstützt (siehe Abbildung 2.1).





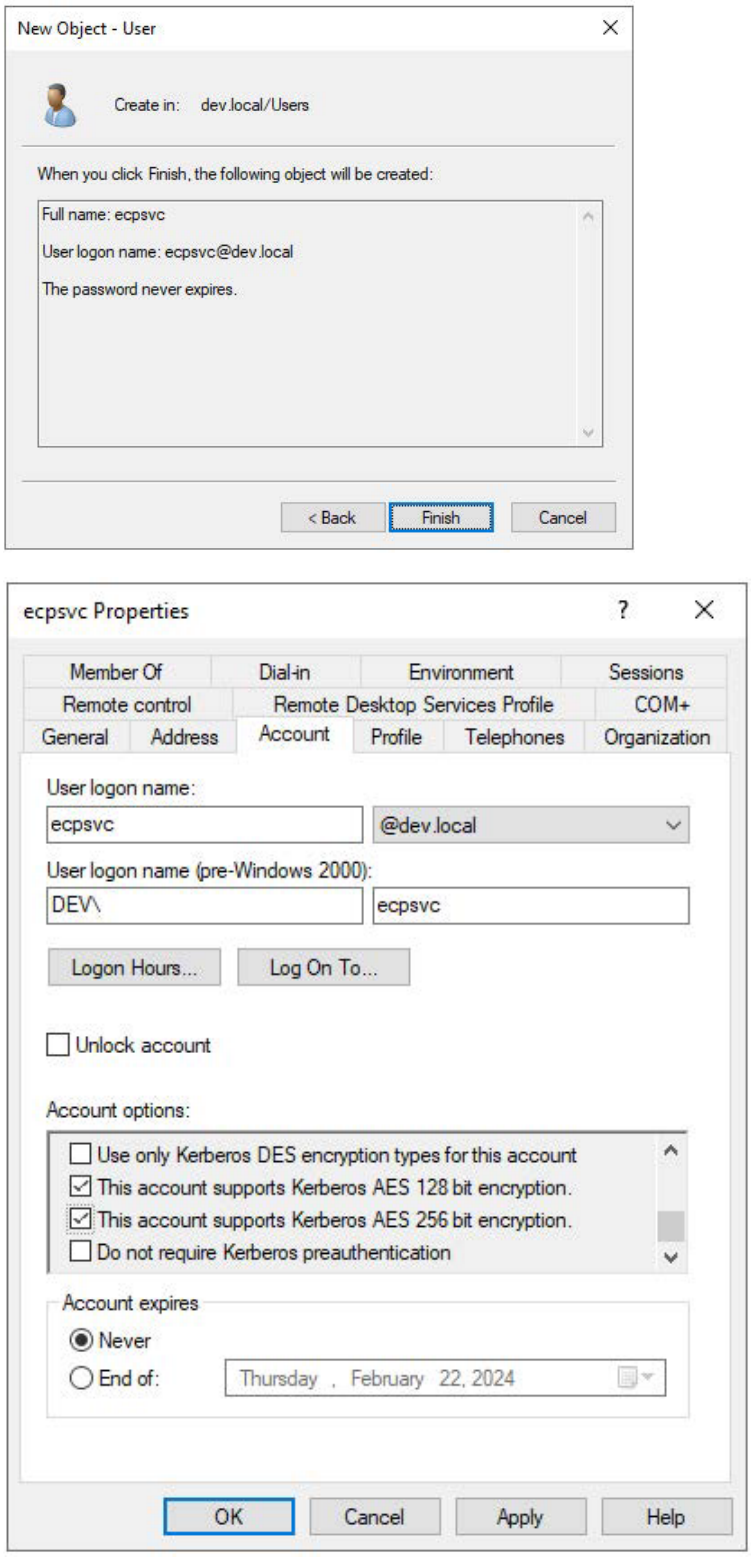


Abbildung 2.1: Erstellung eines ECP-Dienstkontos.

Hier sind die Anmeldedaten des von uns erstellten Dienstkontos:

`Logon-Benutzername: ecpsvc@dev.local`

`Passwort: xxxxxxxxxx`

2.1.2. Dienstprincipalname (SPN) für ECP-Dienst erstellen

Öffnen Sie auf hex.dev.local ein Powershell-Fenster und geben Sie ein:

`setspn -S **HTTP/moria.dev.local** dev\ecpsvc`

```
PS C:\Users\Administrator> setspn -S HTTP/moria.dev.local dev\ecpsvc
Checking domain DC=dev,DC=local

Registering ServicePrincipalNames for CN=ecpsvc,CN=Users,DC=dev,DC=local
        HTTP/moria.dev.local
Updated object
```

Bitte beachten Sie, dass das http im obigen Befehl eine Dienstklasse und kein Protokoll ist. Sowohl http- als auch HTTPS-Protokolle verwenden die http-Dienstklasse.

Prüfen Sie den soeben erstellten SPN:

`setspn -L ecpsvc`

```
PS C:\Users\Administrator> setspn -L ecpsvc
Registered ServicePrincipalNames for CN=ecpsvc,CN=Users,DC=dev,DC=local:
        HTTP/moria.dev.local
```

2.1.3. Keytab-Datei für ECP-Dienst erstellen

Öffnen Sie auf hex.dev.local ein Powershell-Fenster und geben Sie ein:

`ktpass /princ **HTTP/moria.dev.local**@DEV.LOCAL /mapuser ecpsvc@DEV.LOCAL /pass Secret 123+ /out ecp.keytab /crypto all ptype KRB5_NT_PRINCIPAL /kvno 0`

ACHTUNG! Bei den Namen der Auftraggeber wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass der SPN, den Sie im vorherigen Schritt erstellt haben, mit dem übereinstimmt, der zur Erstellung der Keytab verwendet wurde (siehe den fettgedruckten Text in den Beispielen).

```
PS C:\Users\Administrator> ktpass /princ HTTP/moria.dev.local@DEV.LOCAL /mapuser ecpsvc@DEV.LOCAL /
all /ptype KRB5_NT_PRINCIPAL /kvno 0
Targeting domain controller: HEX.dev.local
Successfully mapped HTTP/moria.dev.local to ecpsvc.
Password successfully set!
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to ecp.keytab:
Keytab version: 0x502
keysize 57 HTTP/moria.dev.local@DEV.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x1 (DES-CBC-CRC)
keysize 57 HTTP/moria.dev.local@DEV.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x3 (DES-CBC-MD5)
keysize 65 HTTP/moria.dev.local@DEV.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x17 (RC4-HMAC) k
627db7f)
keysize 81 HTTP/moria.dev.local@DEV.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x12 (AES256-SHA1
b15c00196b111a70584d2a125ca5c8b0a7194e26dc)
keysize 65 HTTP/moria.dev.local@DEV.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 0 etype 0x11 (AES128-SHA1
5227f1fdf3)
```

```
PS C:\Users\Administrator> dir ecp.keytab


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/23/2024   7:25 AM            347 ecp.keytab
```

Kopieren Sie die Datei ecp.keytab nach moria.dev.local. Nach der Installation von ECP verschieben wir die Keytab-Datei an ihren endgültigen Speicherort im Tomcat-Konfigurationsverzeichnis (z. B. C:\E-ConsentPro\tomcat\conf\ecp.keytab).

2.2. ECP-Server

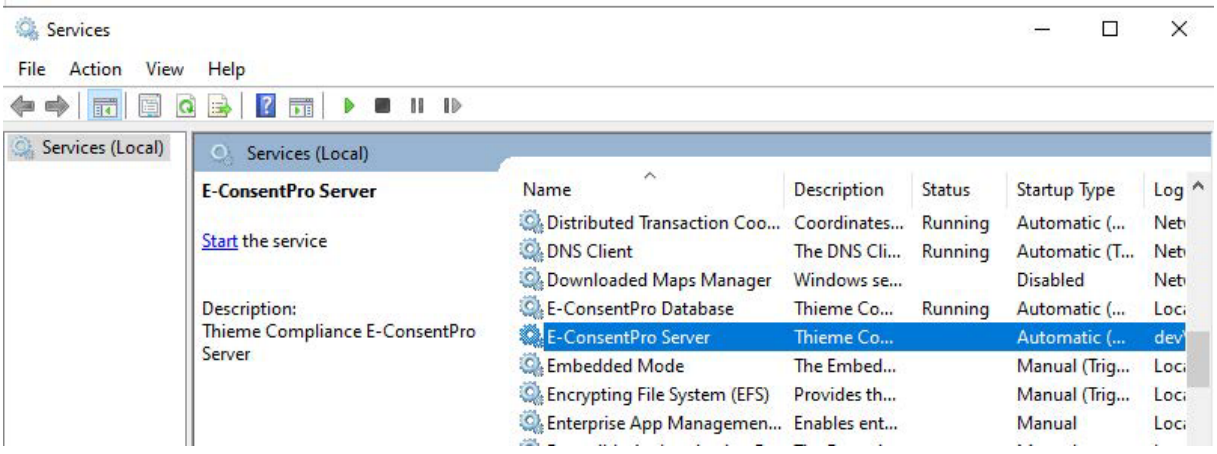
Der Server moria.dev.local ist der Server, auf dem wir ECP ausführen.

2.2.1. ECP installieren

Installieren Sie E-ConsentPro (Version 7 oder höher) und konfigurieren Sie es so, dass es auf die Ports 80 (http) und 443 (https) hört.

Stellen Sie sicher, dass die Ports in der Windows-Firewall geöffnet sind.

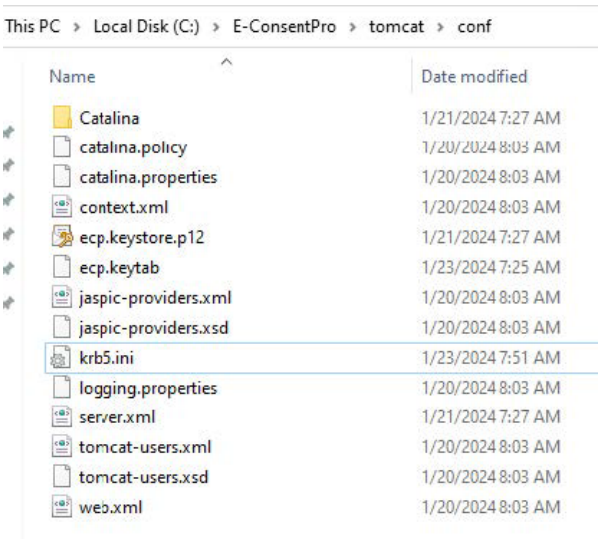
Stoppen Sie den E-ConsentPro-Dienst, bevor Sie die folgenden Schritte durchführen.



2.2.2. Keytab und Kerberos config Dateien

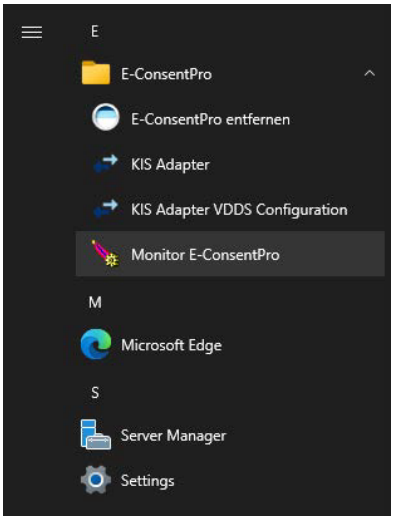
- Kopieren Sie `ecp.keytab` in `C:\E-ConsentPro\tomcat\conf\ecp.keytab`
- Erstellen Sie die Kerberos-Konfigurationsdatei `C:\E-ConsentPro\tomcat\conf\krb5.ini`

```
[libdefaults]

default_realm=DEV.LOCAL

default_keytab_name=FILE:C:\E-ConsentPro\tomcat\conf\ecp.keytab
```



2.2.3. Dienstkonfiguration – VM-Parameter

Starten Sie den E-ConsentPro-Monitor, damit wir die notwendigen Java VM-Parameter definieren können.

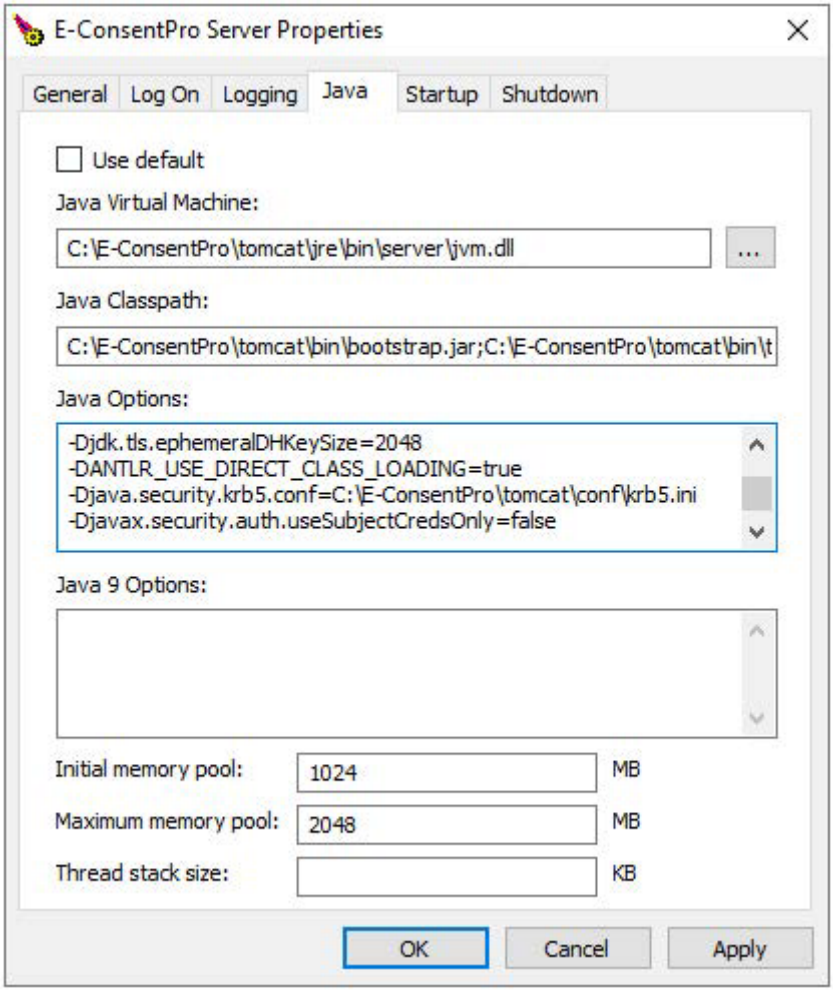


Thieme Compliance

Fügen Sie am Ende der „Java-Optionen“ auf der Registerkarte „Java“ hinzu:

- `Djava.security.krb5.conf=C:\E-ConsentPro\tomcat\conf\krb5.ini`
- `Djavax.security.auth.useSubjectCredsOnly=false`

ACHTUNG! Achten Sie darauf, dass nach dem Wert „false“ keine Leerzeichen stehen!

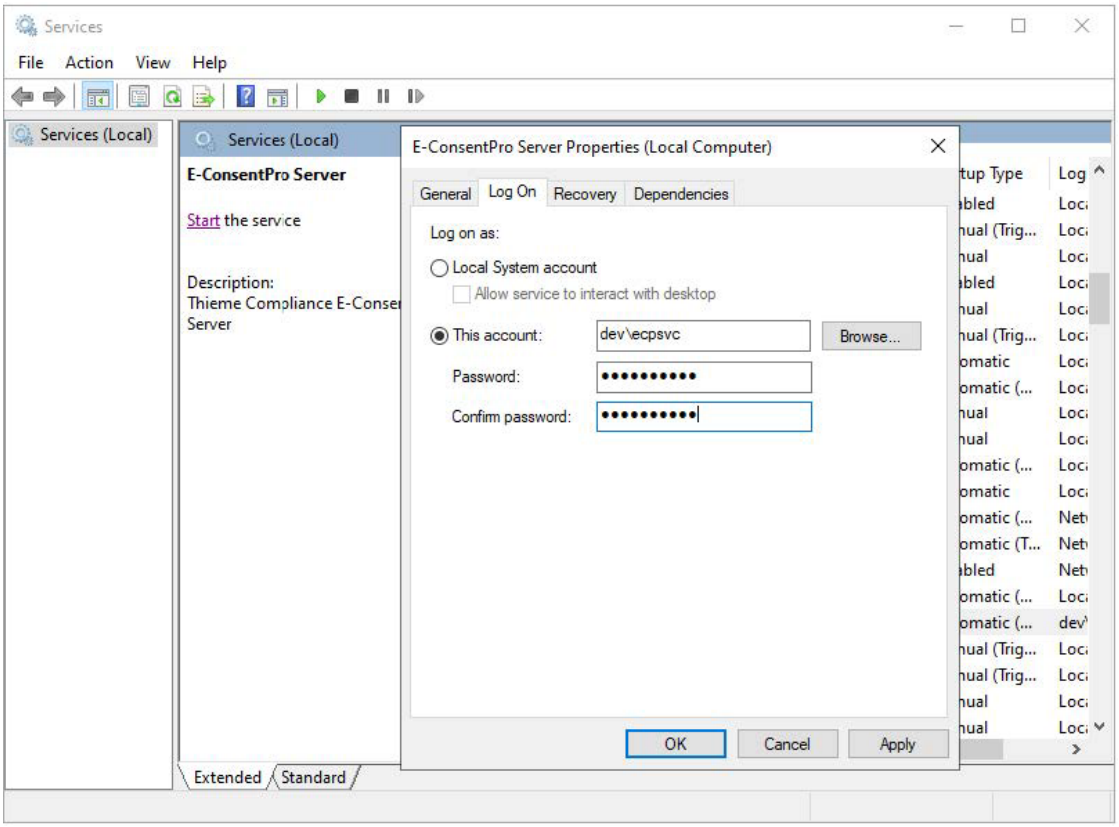


Klicken Sie auf OK, um den E-ConsentPro-Monitor zu schließen. Starten Sie den Dienst noch nicht!

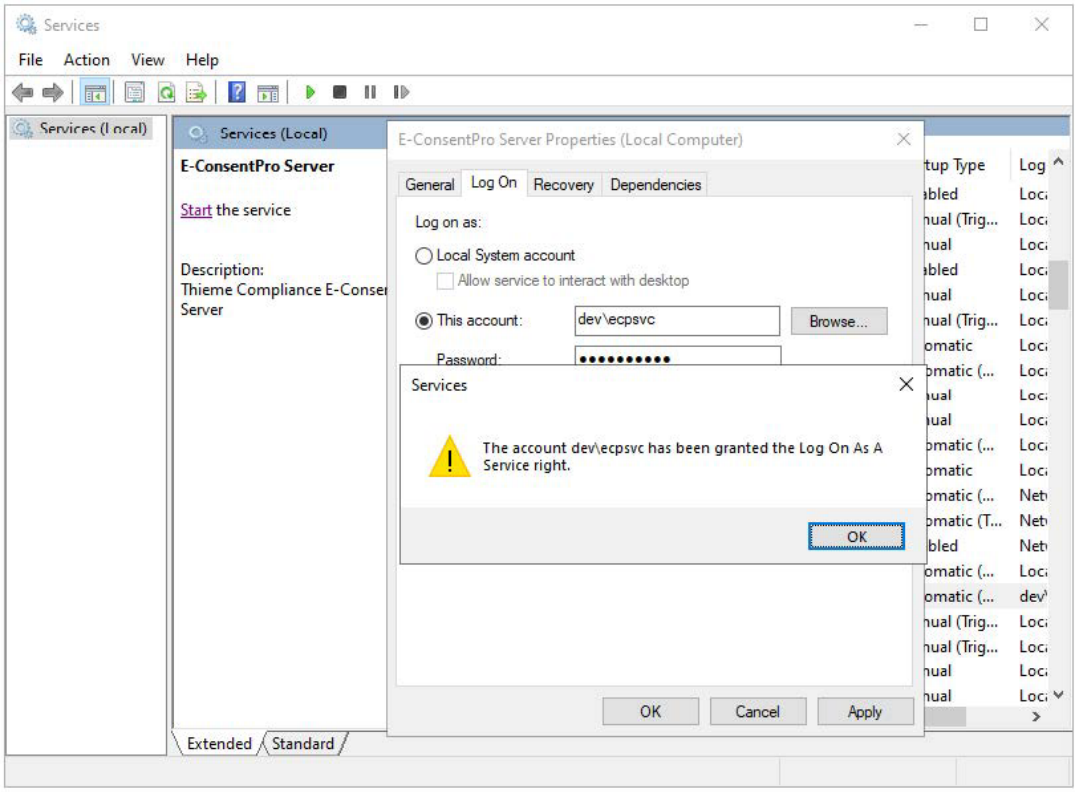
2.2.4. Dienstkonfiguration – Dienstkonto

Verwenden Sie den Windows Services Manager (services.msc), um das ECP-Dienstkonto anzugeben, das wir in Abschnitt 2.1.1 erstellt haben.

ACHTUNG! Verwenden Sie nicht den E-ConsentPro-Monitor, um den Benutzer für den ECP-Dienst zu konfigurieren! Sie müssen den Windows Services Manager für diese Aufgabe verwenden.



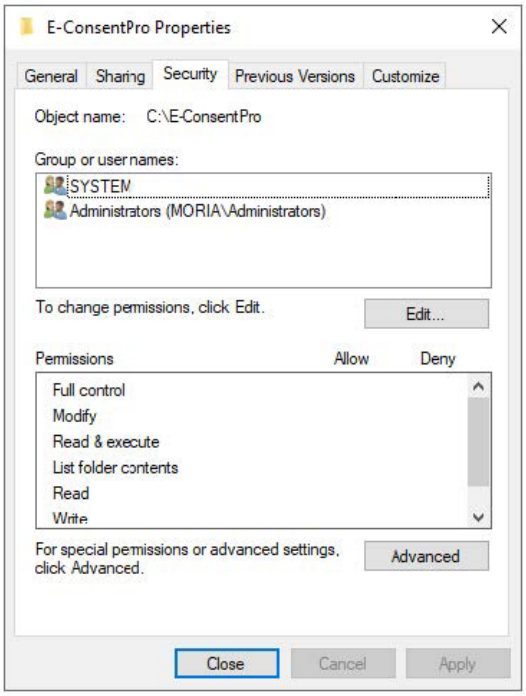
Klicken Sie auf „Apply“ (Anwenden).



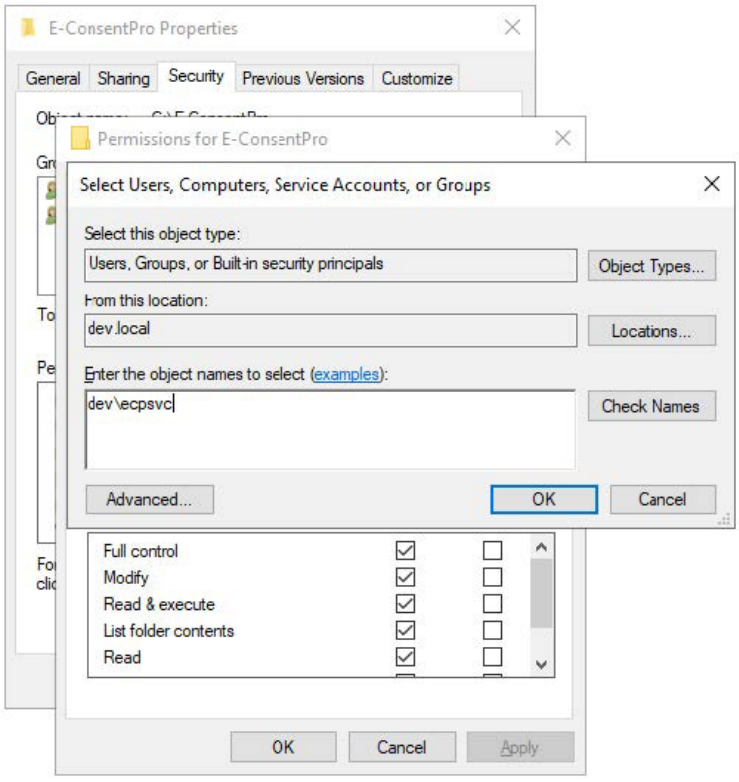
Lassen Sie das Fenster geöffnet und **starten Sie den Dienst noch nicht!**

2.2.5. Reparieren der Dateiberechtigungen

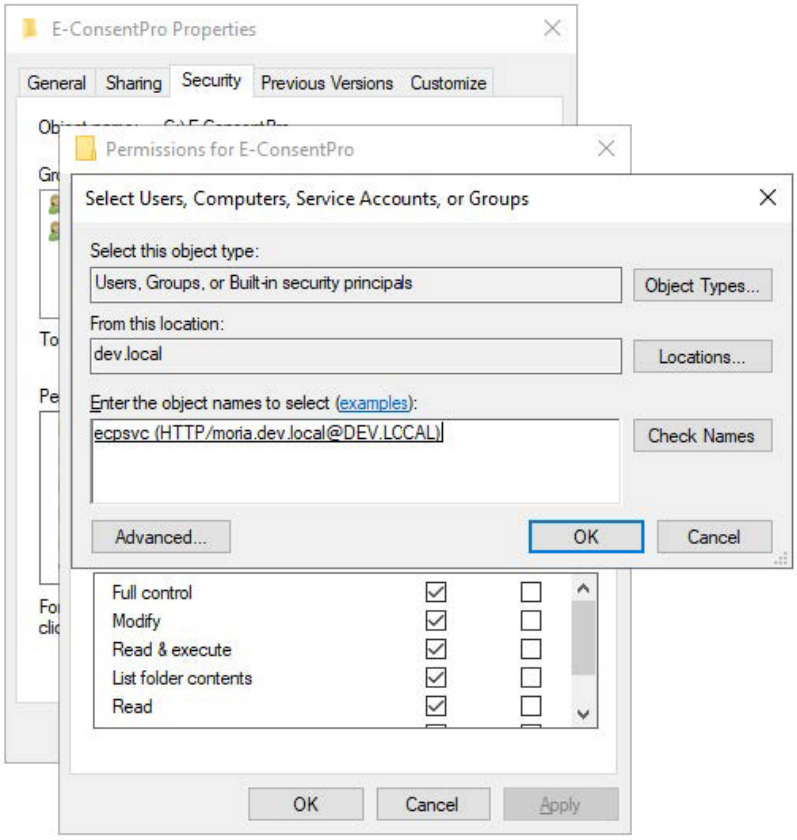
Der Benutzer dev\ecpsvc muss volle Kontrolle über das Installationsverzeichnis und seine Unterverzeichnisse haben.



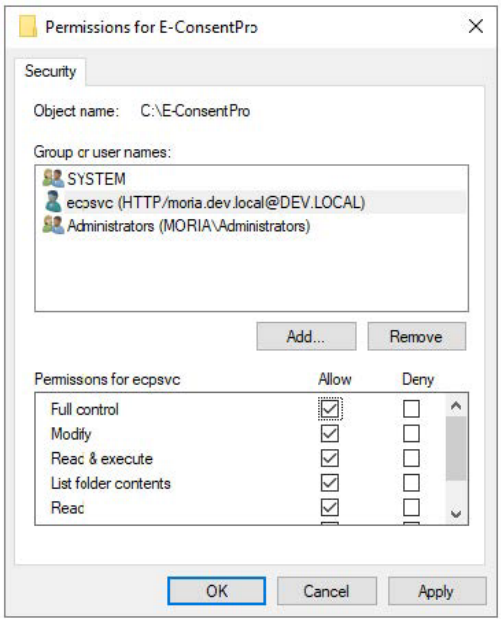
Klicken Sie auf „Edit“ > „Add“ (Bearbeiten > Hinzufügen)



Klicken Sie auf „ Namen überprüfen“ (Check Names)



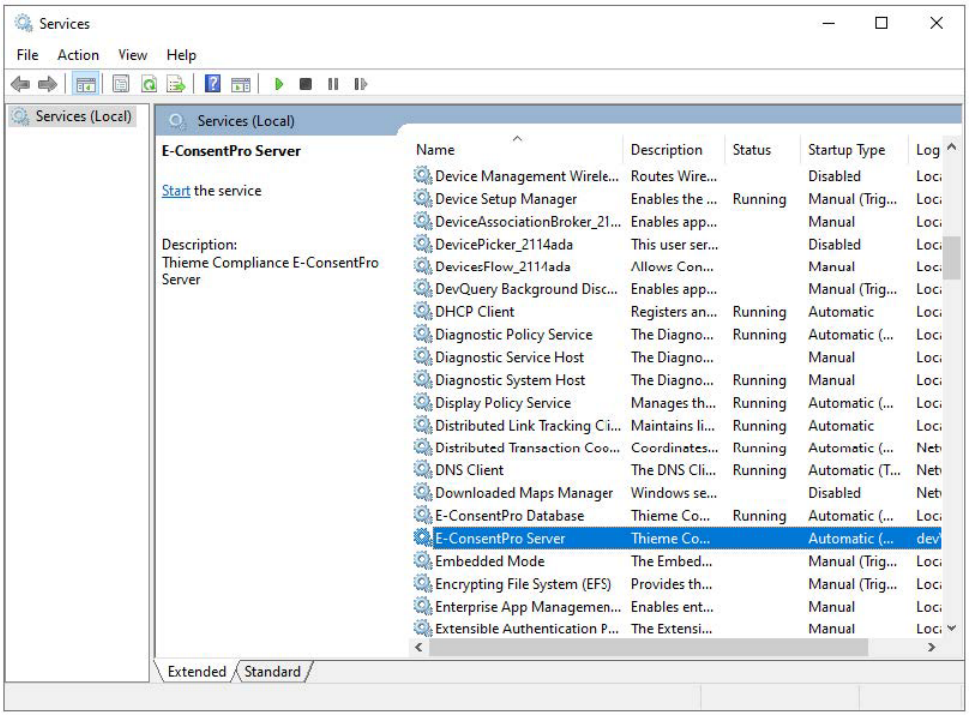
Klicken Sie auf „OK“



Und wieder auf „OK“ klicken

2.2.6. Starten des ECP-Dienstes

Wechseln Sie zum Fenster „Dienste“ (Services) und starten Sie den E-ConsentPro-Dienst

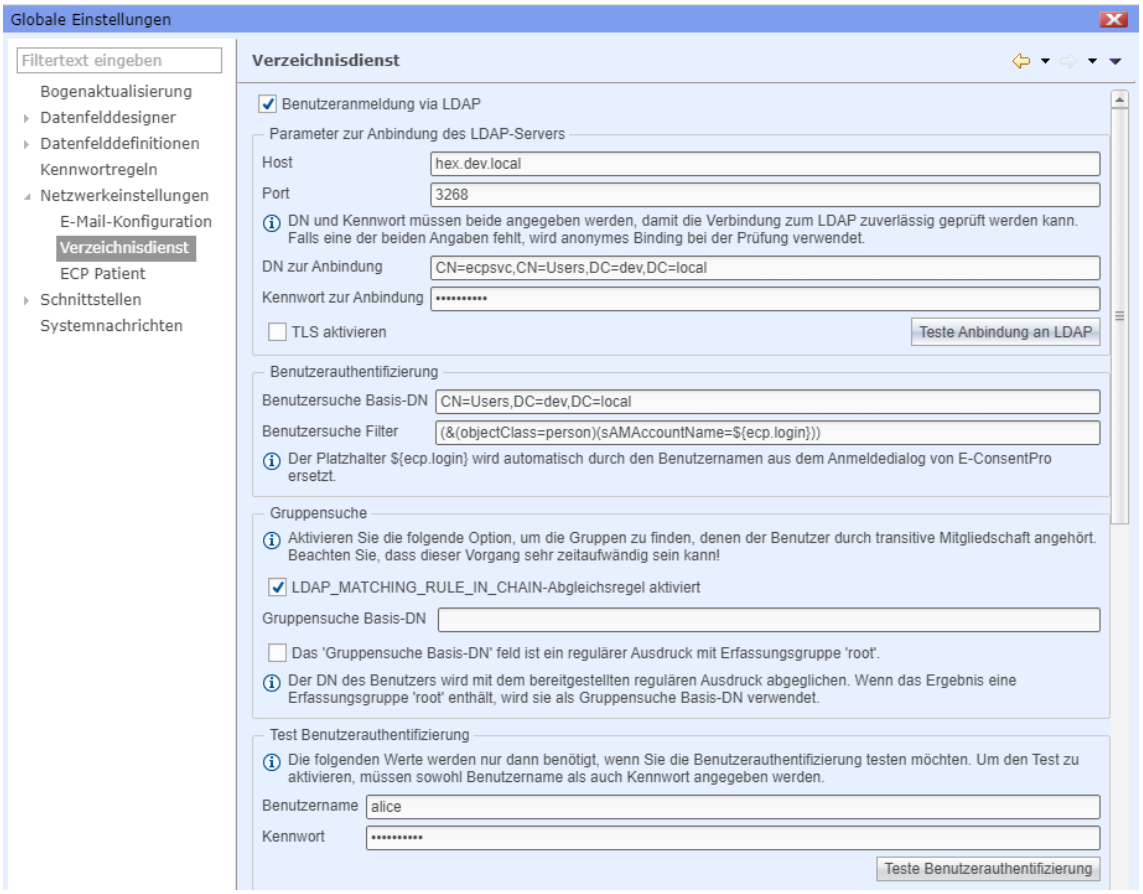


2.2.7. ECP LDAP konfigurieren

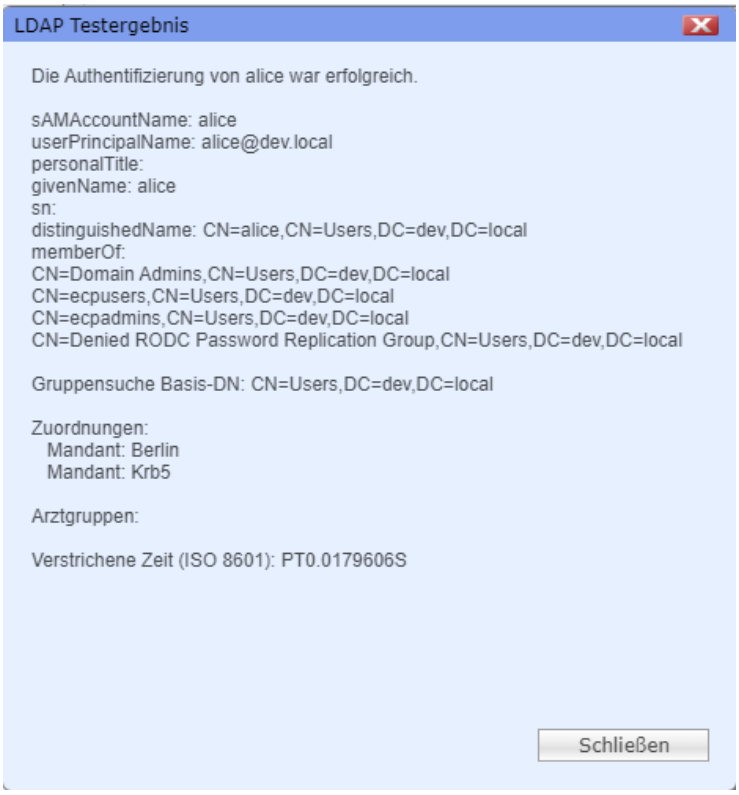
Anmeldung bei ECP als Administrator.

Konfigurieren Sie die Zuordnung von Mandant zu LDAP-Gruppen.

Konfigurieren Sie die LDAP-Verbindung: Globale Einstellungen > Netzwerkeinstellungen > Verzeichnisdienst



Testen Sie die Konfiguration mit den Anmeldedaten eines Domänenbenutzers – in unserem Beispiel ist dies „Alice“.



2.3. Vorbereiten der Benutzer-Workstations

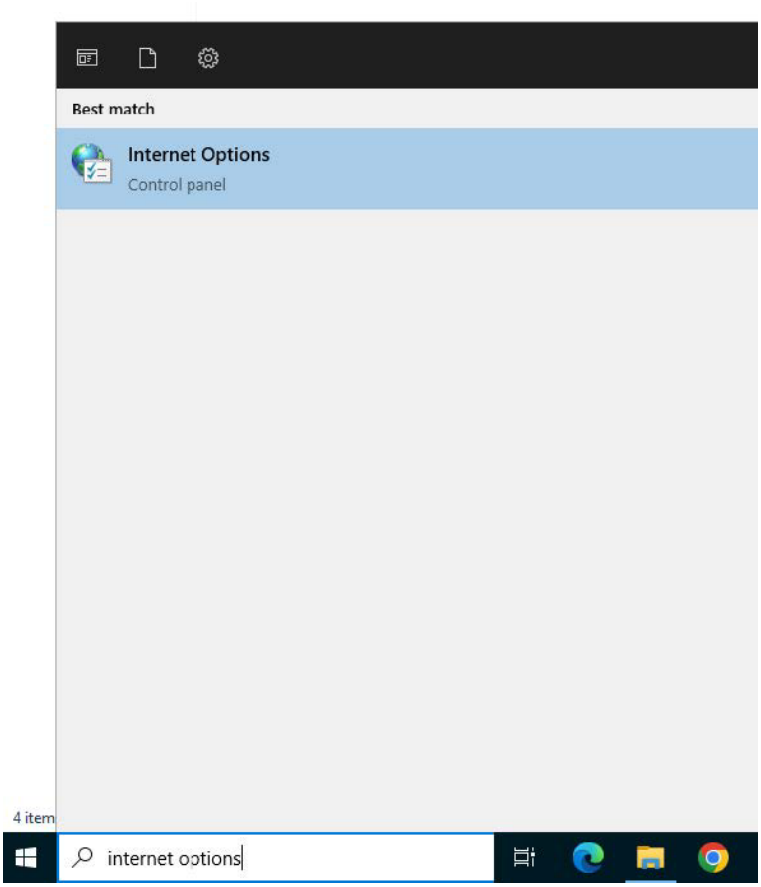
Jede Arbeitsstation muss bereits der Active Directory-Domäne beigetreten sein (in unserem Beispiel dev.local).

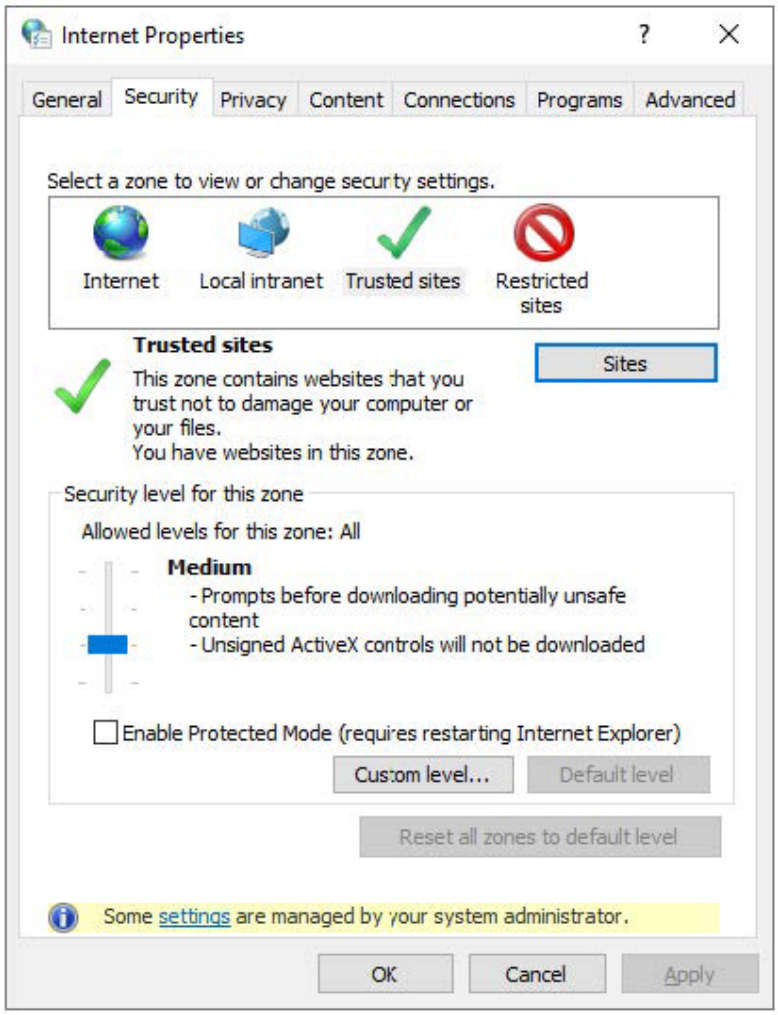
Für jedes Benutzerkonto muss die Domäne zur Zone „Vertrauenswürdiger Bereich“ (Trusted Sites) hinzugefügt und „Automatiscshe Anmeldung mit aktuellem Benutzernamen“ (Automatic login with current user name and password") aktiviert werden. Die Abschnitte 2.3.1 - 2.3.3 zeigen, wie die Einstellungen über die „Systemsteuerung > Internetoptionen“ (Control panel > Internet Options) an den Arbeitsplätzen der Benutzer vorgenommen werden können.
Für mehrere Konten ist es jedoch am einfachsten, Gruppenrichtlinien-Objekte zu verwenden - siehe Abschnitt 2.3.4.

2.3.1. Internet-Optionen

Melden Sie sich als Domänenbenutzer an (in unserem Beispiel wird dies dev\alice sein).

Öffnen Sie die Internetoptionen.

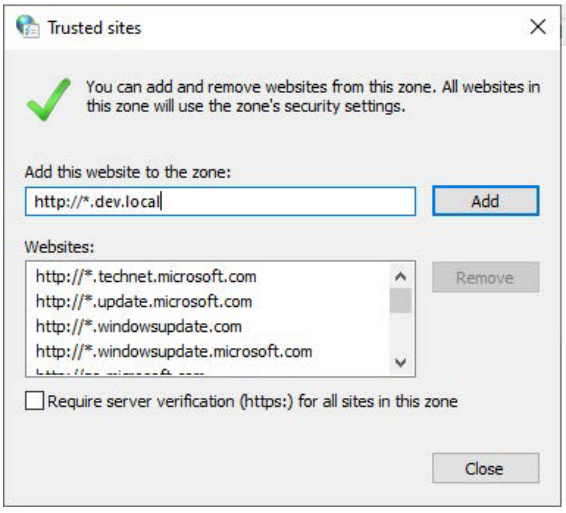




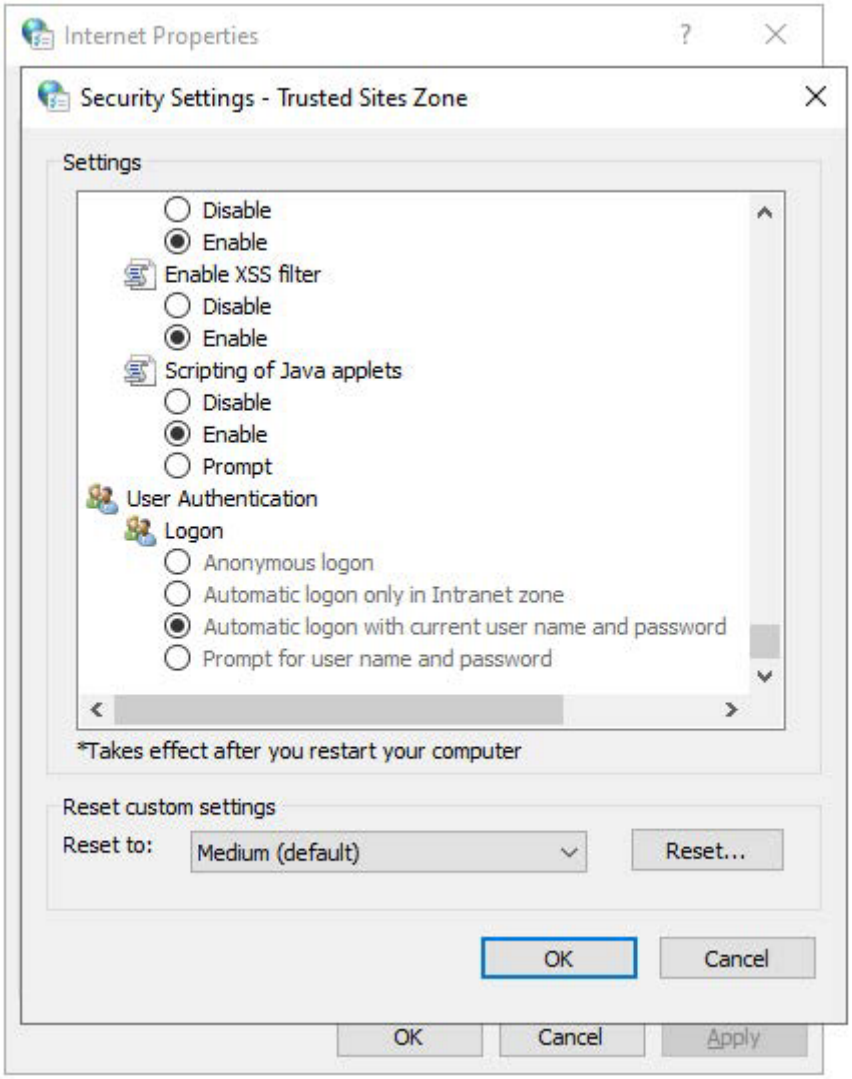
2.3.2. Hinzufügen der Domain zur Zone „Vertrauenswürdige Sites“

http://*.dev.local

https://*.dev.local



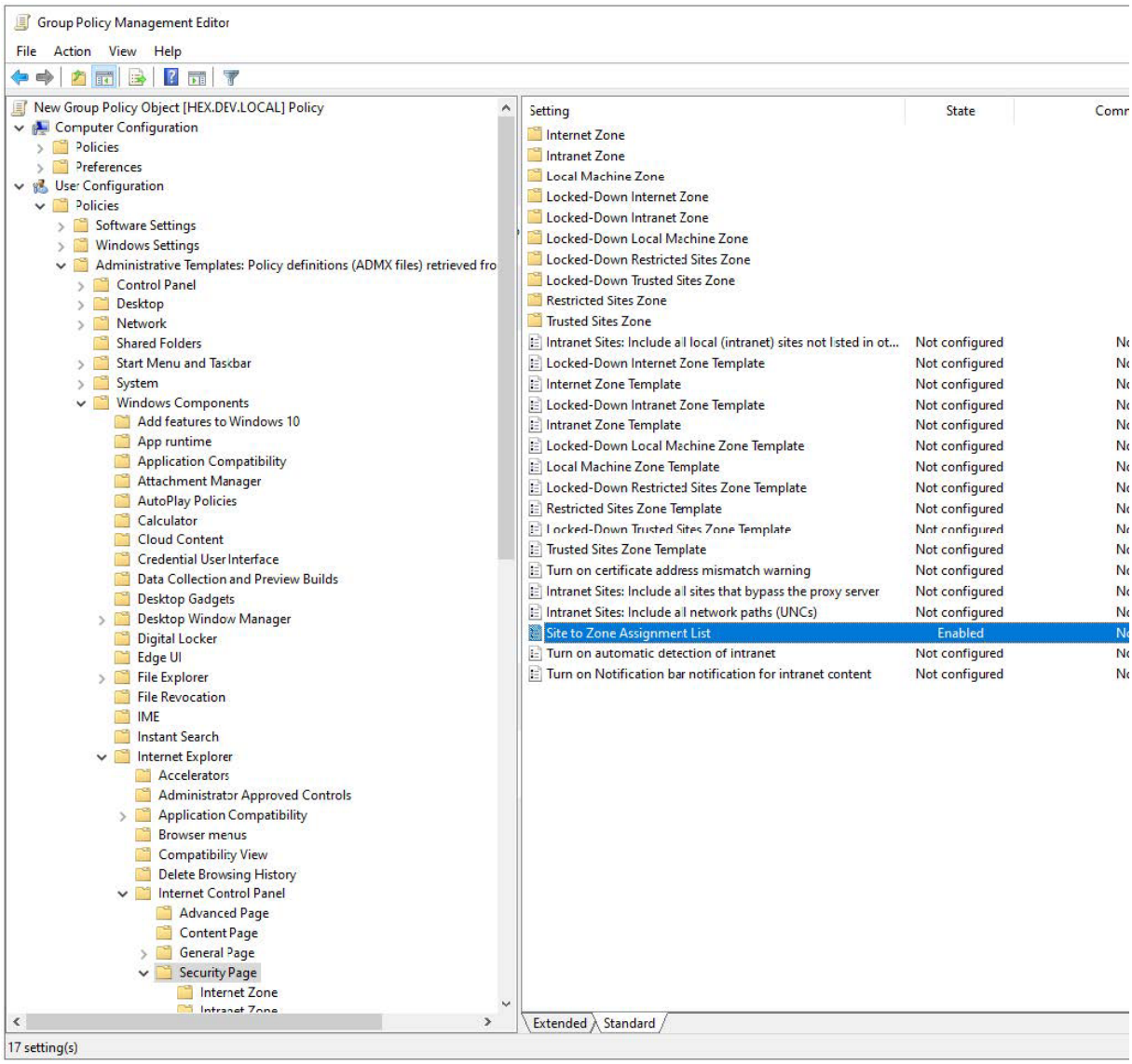
2.3.3. Aktivierung von „Automatische Anmeldung mit aktuellem Benutzernamen und Passwort“

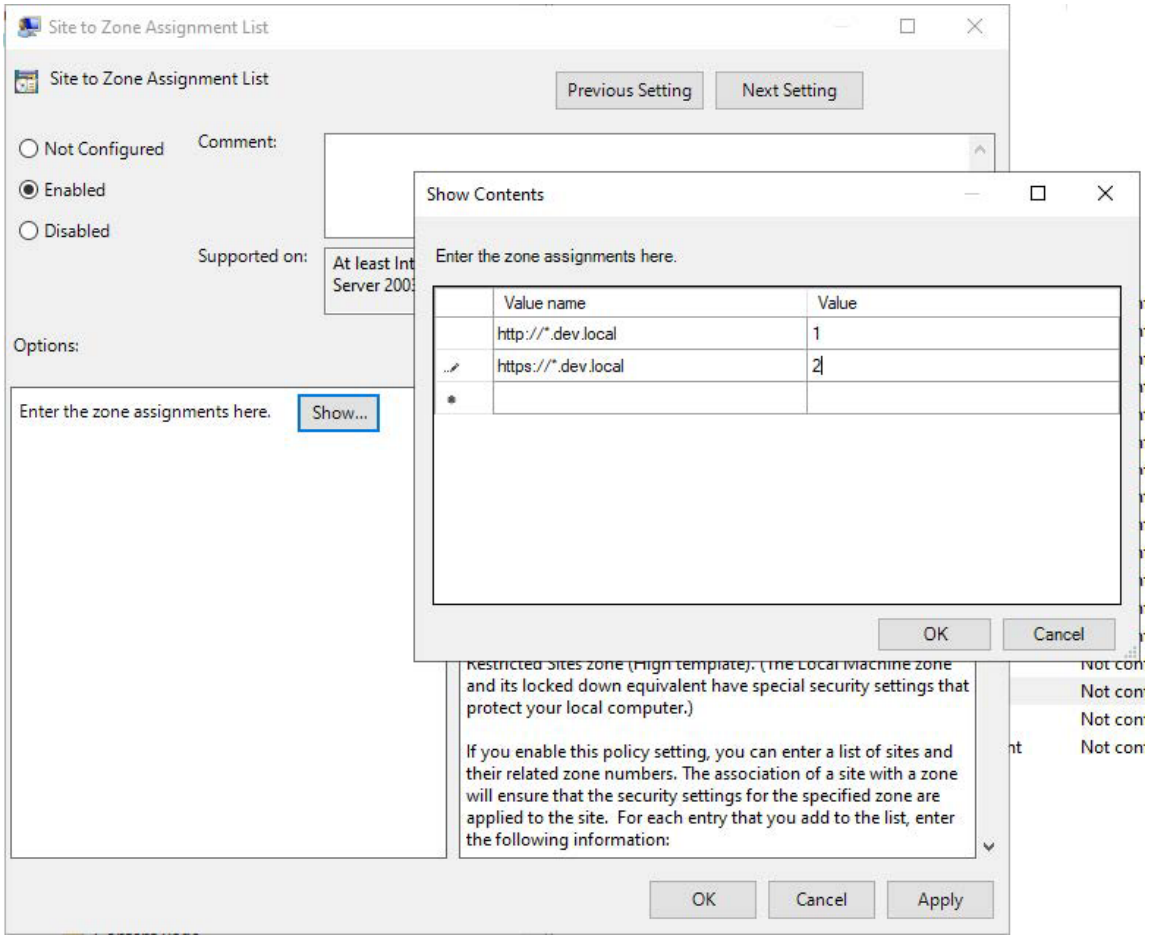


2.3.4. Konfigurieren von Benutzerkonten mit GPOs

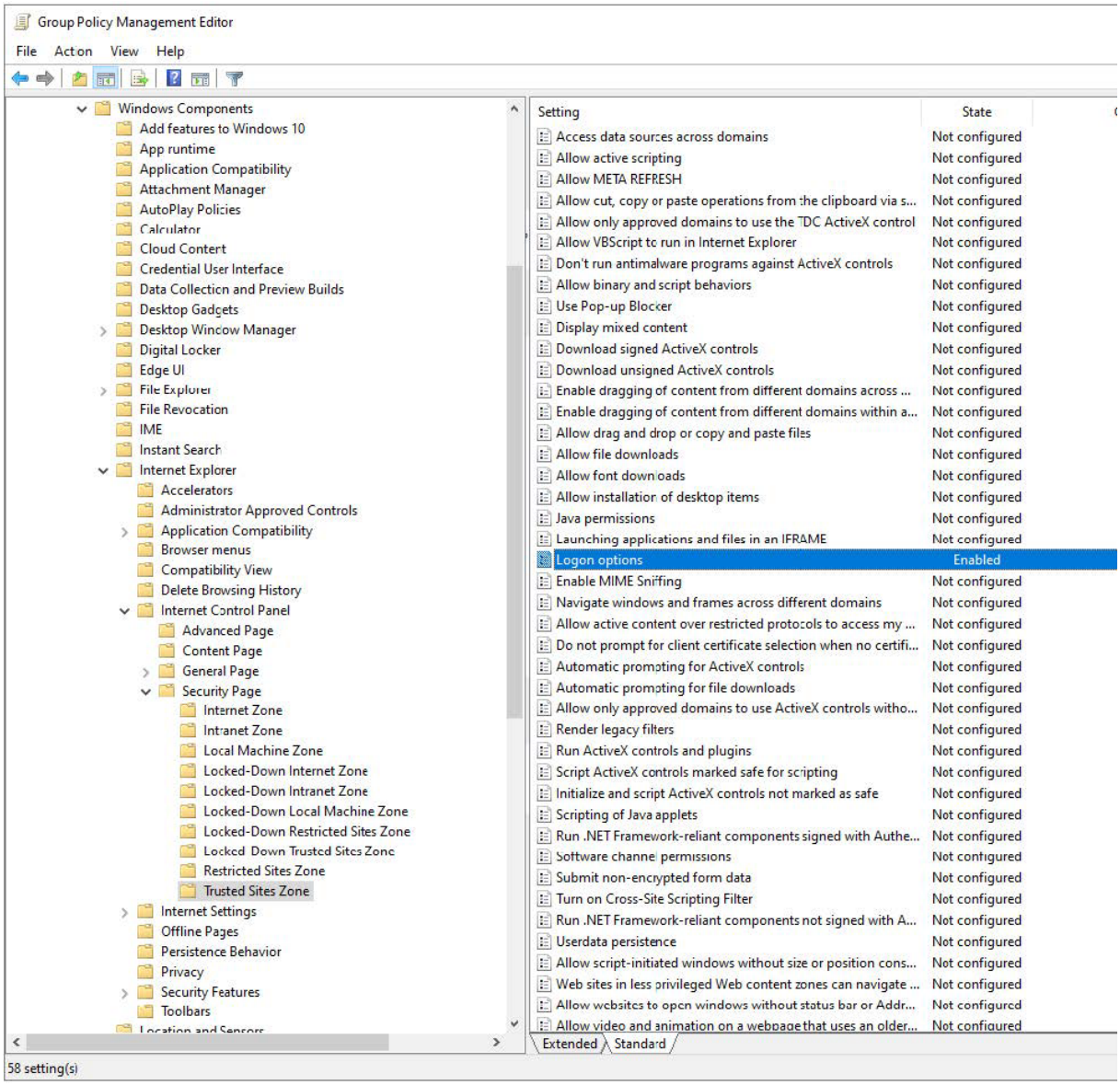
Dieser Abschnitt ist für erfahrene Windows AD-Administratoren gedacht, daher werden wir die detaillierten Erklärungen auslassen.

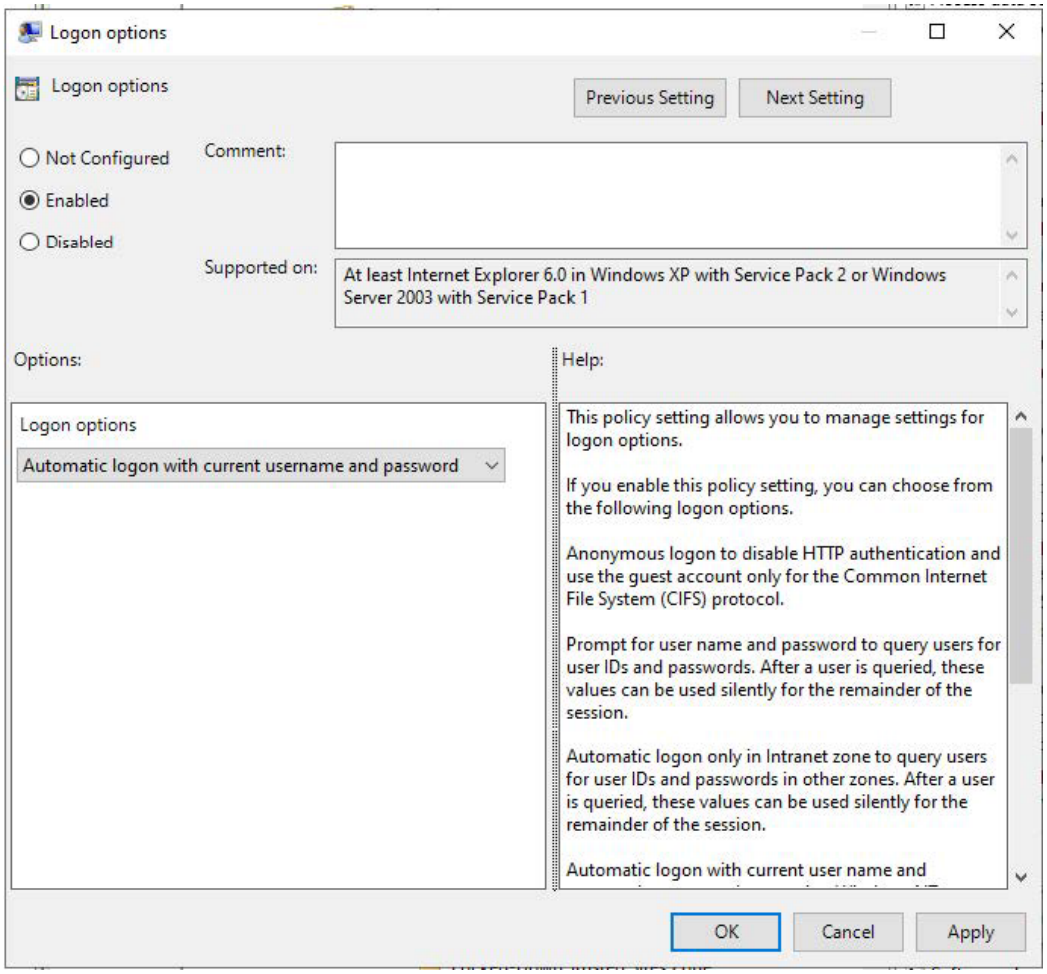
Fügen Sie die Domäne zur Zone "Vertrauenswürdige Sites“ (Trusted Sites Zone“ (Vertrauenswürdige Sites) hinzu.

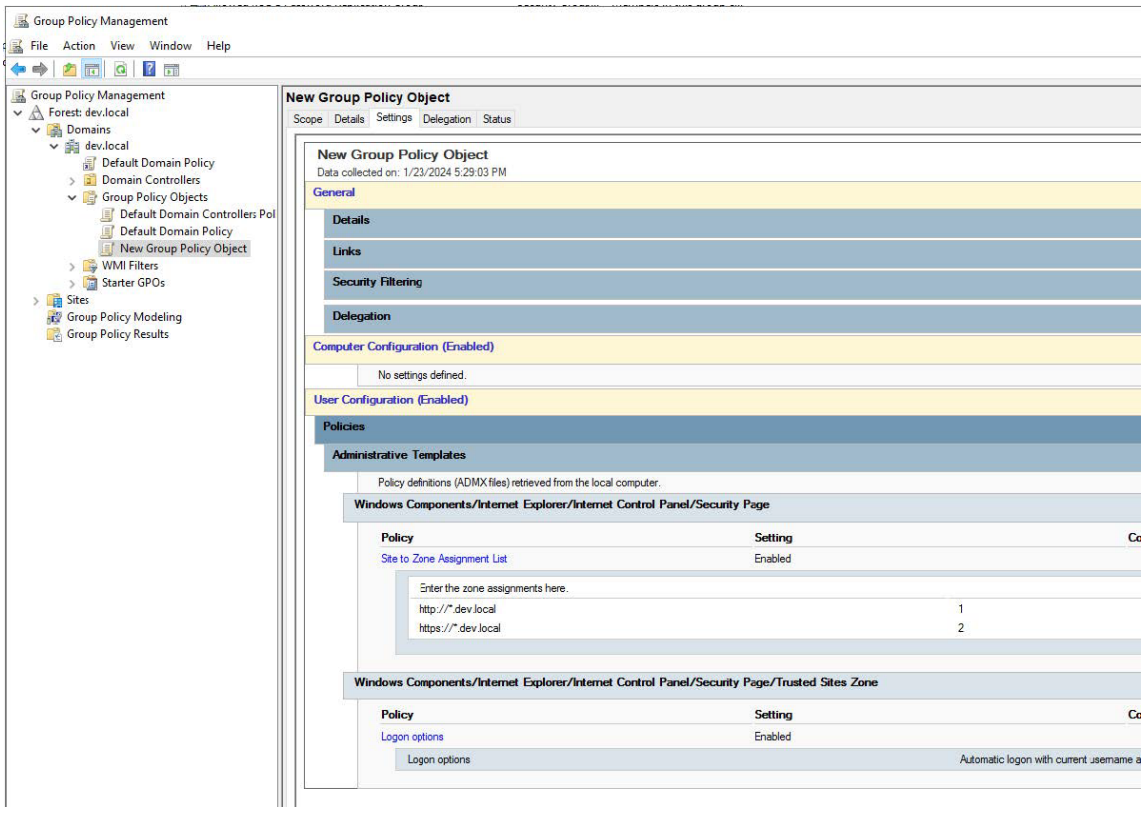

Group Policy Management Editor
File Action View Help
New Group Policy Object [HEX.DEV.LOCAL] Policy
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) retrieved fro
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
Add features to Windows 10
App runtime
Application Compatibility
Attachment Manager
AutoPlay Policies
Calculator
Cloud Content
Credential User Interface
Data Collection and Preview Builds
Desktop Gadgets
Desktop Window Manager
Digital Locker
Edge UI
File Explorer
File Revocation
IME
Instant Search
Internet Explorer
Accelerators
Administrator Approved Controls
Application Compatibility
Browser menus
Compatibility View
Delete Browsing History
Internet Control Panel
Advanced Page
Content Page
General Page
Security Page
Internet Zone
Setting
State
Internet Zone
Intranet Zone
Local Machine Zone
Locked-Down Internet Zone
Locked-Down Intranet Zone
Locked-Down Local Machine Zone
Locked-Down Restricted Sites Zone
Locked-Down Trusted Sites Zone
Restricted Sites Zone
Trusted Sites Zone
Intranet Sites: Include all local (intranet) sites not listed in ot... Not configured
Locked-Down Internet Zone Template Not configured
Internet Zone Template Not configured
Locked-Down Intranet Zone Template Not configured
Intranet Zone Template Not configured
Locked-Down Local Machine Zone Template Not configured
Local Machine Zone Template Not configured
Locked-Down Restricted Sites Zone Template Not configured
Restricted Sites Zone Template Not configured
Trusted Sites Zone Template Not configured
Turn on certificate address mismatch warning Not configured
Intranet Sites: Include all sites that bypass the proxy server Not configured
Intranet Sites: Include all network paths (UNCs) Not configured
Site to Zone Assignment List Enabled
Turn on automatic detection of intranet Not configured
Turn on Notification bar notification for intranet content Not configured
Extended Standard
17 setting(s)

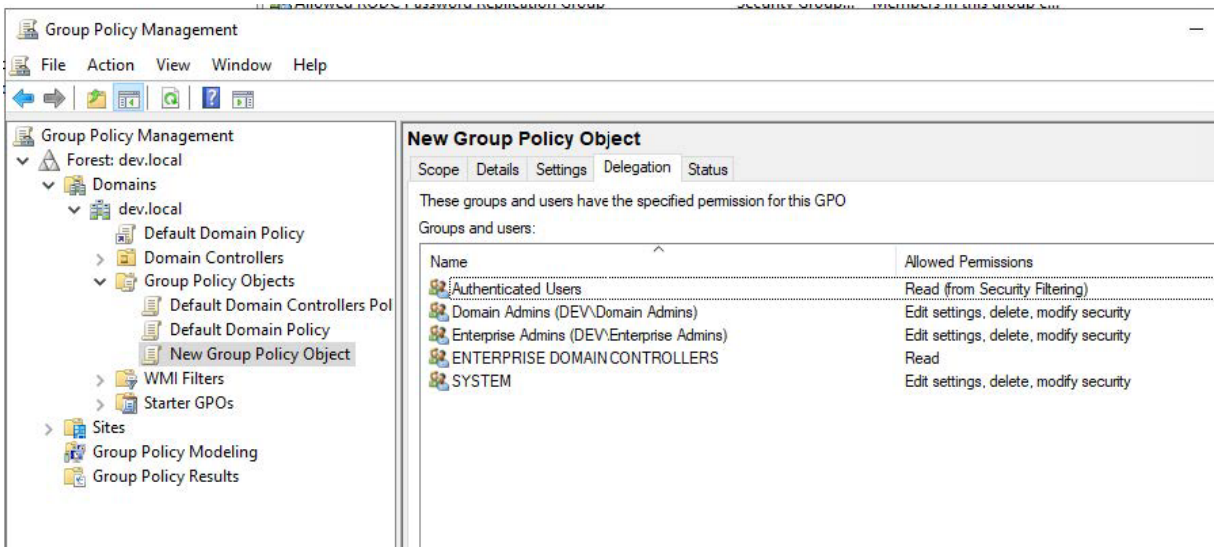


Aktivieren Sie "Automatische Anmeldung mit aktuellem Benutzernamen und Passwort" (Automatic login with current user name and password).


Group Policy Management Editor
File Action View Help
Windows Components
Add features to Windows 10
App runtime
Application Compatibility
Attachment Manager
AutoPlay Policies
Calculator
Cloud Content
Credential User Interface
Data Collection and Preview Builds
Desktop Gadgets
Desktop Window Manager
Digital Locker
Edge UI
File Explorer
File Revocation
IME
Instant Search
Internet Explorer
Accelerators
Administrator Approved Controls
Application Compatibility
Browser menus
Compatibility View
Delete Browsing History
Internet Control Panel
Advanced Page
Content Page
General Page
Security Page
Internet Zone
Intranet Zone
Local Machine Zone
Locked-Down Internet Zone
Locked-Down Intranet Zone
Locked-Down Local Machine Zone
Locked-Down Restricted Sites Zone
Locked-Down Trusted Sites Zone
Restricted Sites Zone
Trusted Sites Zone
Internet Settings
Offline Pages
Persistence Behavior
Privacy
Security Features
Toolbars
Setting
State
Access data sources across domains Not configured
Allow active scripting Not configured
Allow META REFRESH Not configured
Allow cut, copy or paste operations from the clipboard via s... Not configured
Allow only approved domains to use the TDC ActiveX control Not configured
Allow VBScript to run in Internet Explorer Not configured
Don't run antimalware programs against ActiveX controls Not configured
Allow binary and script behaviors Not configured
Use Pop-up Blocker Not configured
Display mixed content Not configured
Download signed ActiveX controls Not configured
Download unsigned ActiveX controls Not configured
Enable dragging of content from different domains across ... Not configured
Enable dragging of content from different domains within a... Not configured
Allow drag and drop or copy and paste files Not configured
Allow file downloads Not configured
Allow font downloads Not configured
Allow installation of desktop items Not configured
Java permissions Not configured
Launching applications and files in an IFRAME Not configured
Logon options Enabled
Enable MIME Sniffing Not configured
Navigate windows and frames across different domains Not configured
Allow active content over restricted protocols to access my ... Not configured
Do not prompt for client certificate selection when no certifi... Not configured
Automatic prompting for ActiveX controls Not configured
Automatic prompting for file downloads Not configured
Allow only approved domains to use ActiveX controls witho... Not configured
Render legacy filters Not configured
Run ActiveX controls and plugins Not configured
Script ActiveX controls marked safe for scripting Not configured
Initialize and script ActiveX controls not marked as safe Not configured
Scripting of Java applets Not configured
Run .NET Framework-reliant components signed with Authe... Not configured
Software channel permissions Not configured
Submit non-encrypted form data Not configured
Turn on Cross-Site Scripting Filter Not configured
Run .NET Framework-reliant components not signed with A... Not configured
Userdata persistence Not configured
Allow script-initiated windows without size or position cons... Not configured
Web sites in less privileged Web content zones can navigate ... Not configured
Allow websites to open windows without status bar or Addr... Not configured
Allow video and animation on a webpage that uses an older... Not configured
Extended Standard
58 setting(s)


Logon options
Logon options
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Internet Explorer 6.0 in Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1
Options:
Help:
Logon options
Automatic logon with current username and password
This policy setting allows you to manage settings for logon options.
If you enable this policy setting, you can choose from the following logon options.
Anonymous logon to disable HTTP authentication and use the guest account only for the Common Internet File System (CIFS) protocol.
Prompt for user name and password to query users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session.
Automatic logon only in Intranet zone to query users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session.
Automatic logon with current user name and
OK
Cancel
Apply


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dev.local
Domains
dev.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Pol
Default Domain Policy
New Group Policy Object
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
New Group Policy Object
Scope Details Settings Delegation Status
New Group Policy Object
Data collected on: 1/23/2024 5:29:03 PM
General
Details
Links
Security Filtering
Delegation
Computer Configuration (Enabled)
No settings defined.
User Configuration (Enabled)
Policies
Administrative Templates
Policy definitions (ADMX files) retrieved from the local computer.
Windows Components/Internet Explorer/Internet Control Panel/Security Page
Policy
Setting
Site to Zone Assignment List
Enabled
Enter the zone assignments here.
http://*.dev.local
1
https://*.dev.local
2
Windows Components/Internet Explorer/Internet Control Panel/Security Page/Trusted Sites Zone
Policy
Setting
Logon options
Enabled
Logon options
Automatic logon with current username a

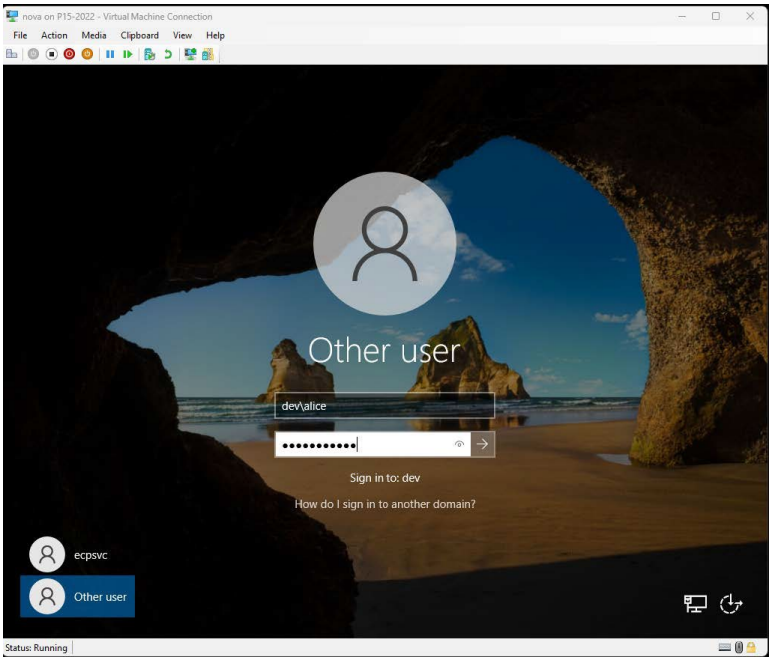

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: dev.local
Domains
dev.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Pol
Default Domain Policy
New Group Policy Object
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
New Group Policy Object
Scope Details Settings Delegation Status
These groups and users have the specified permission for this GPO
Groups and users:
Name
Allowed Permissions
Authenticated Users
Read (from Security Filtering)
Domain Admins (DEV\Domain Admins)
Edit settings, delete, modify security
Enterprise Admins (DEV\Enterprise Admins)
Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS
Read
SYSTEM
Edit settings, delete, modify security

3. Testen

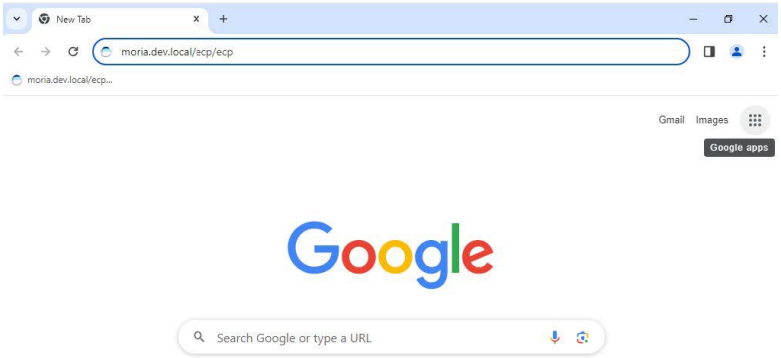
ACHTUNG! Das SSO funktioniert nicht, wenn Sie sich auf dem Host anmelden, auf dem ECP installiert ist. Bei den folgenden Tests wird davon ausgegangen, dass die Arbeitsstation des Benutzers und der ECP-Server unterschiedliche Hosts sind.

3.1. Der Windows-Benutzer und der ECP-Benutzer sind identisch

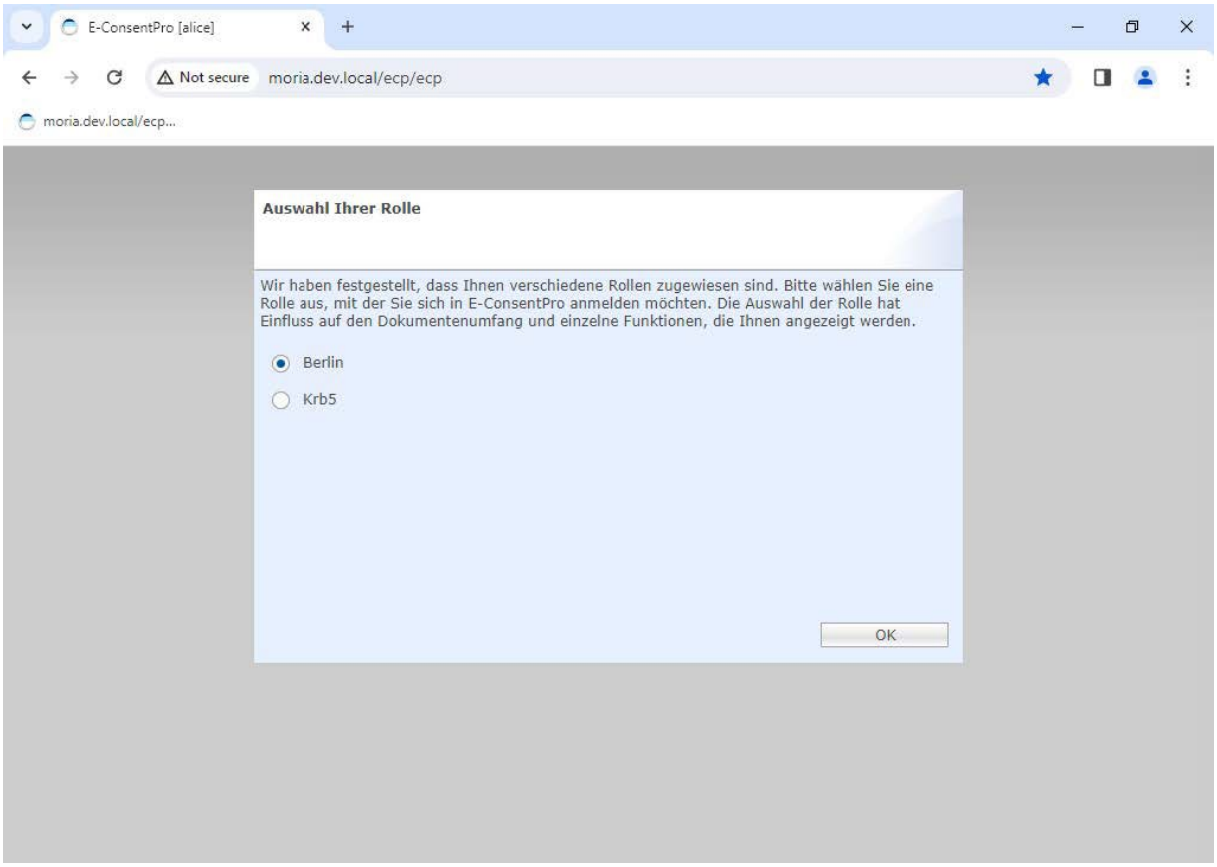
Die Domänenbenutzerin Alice meldet sich an einer Windows-Arbeitsstation an, die Teil der Domäne dev.local ist.



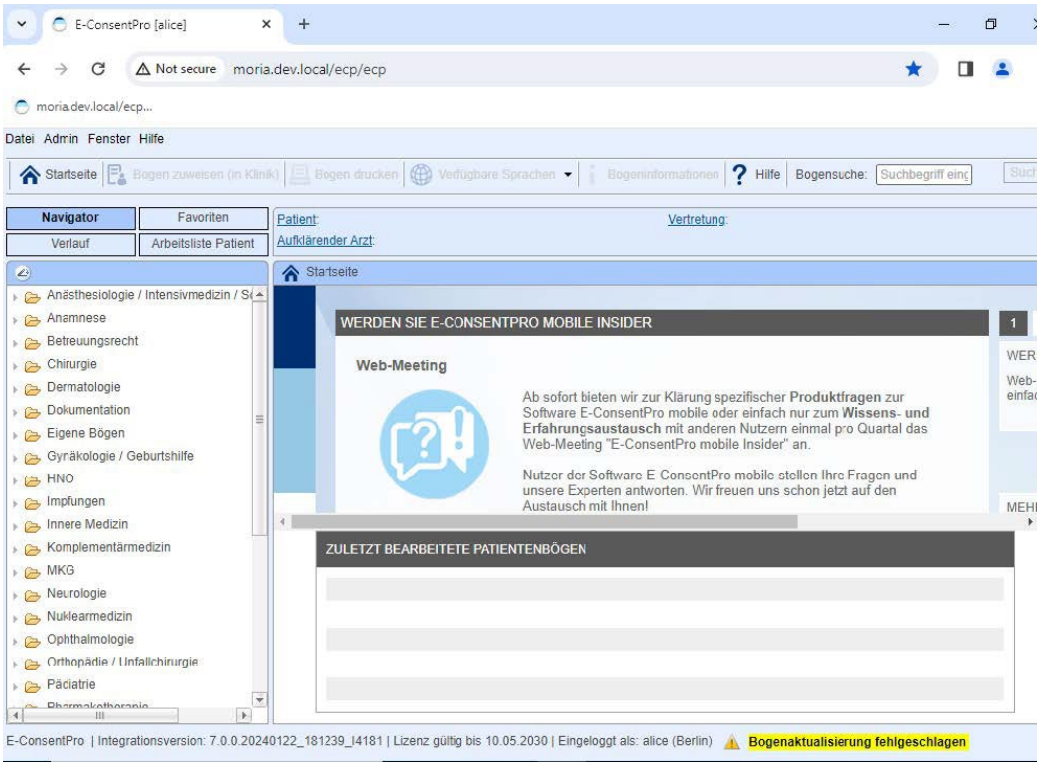
Öffnen Sie einen Browser und geben Sie die ECP-URL ein.



Es wird kein Anmeldedialog angezeigt.

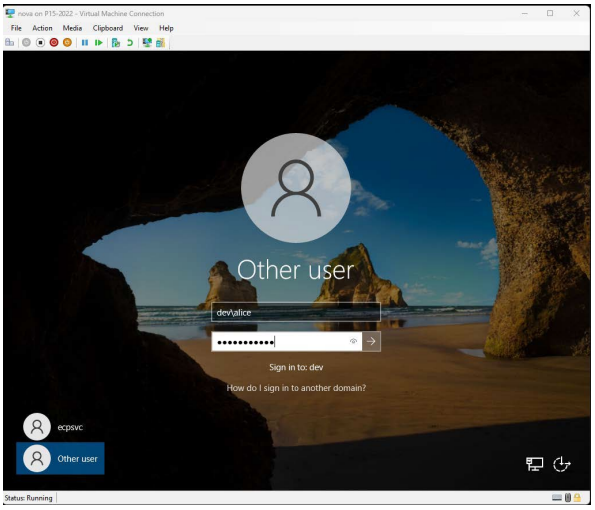


Alice ist über SSO bei ECP angemeldet. Beachten Sie den Benutzernamen und den Mandanten in der Statusleiste am unteren Rand.



3.2. Der ECP-Benutzer ist ein anderer als der Windows-Benutzer

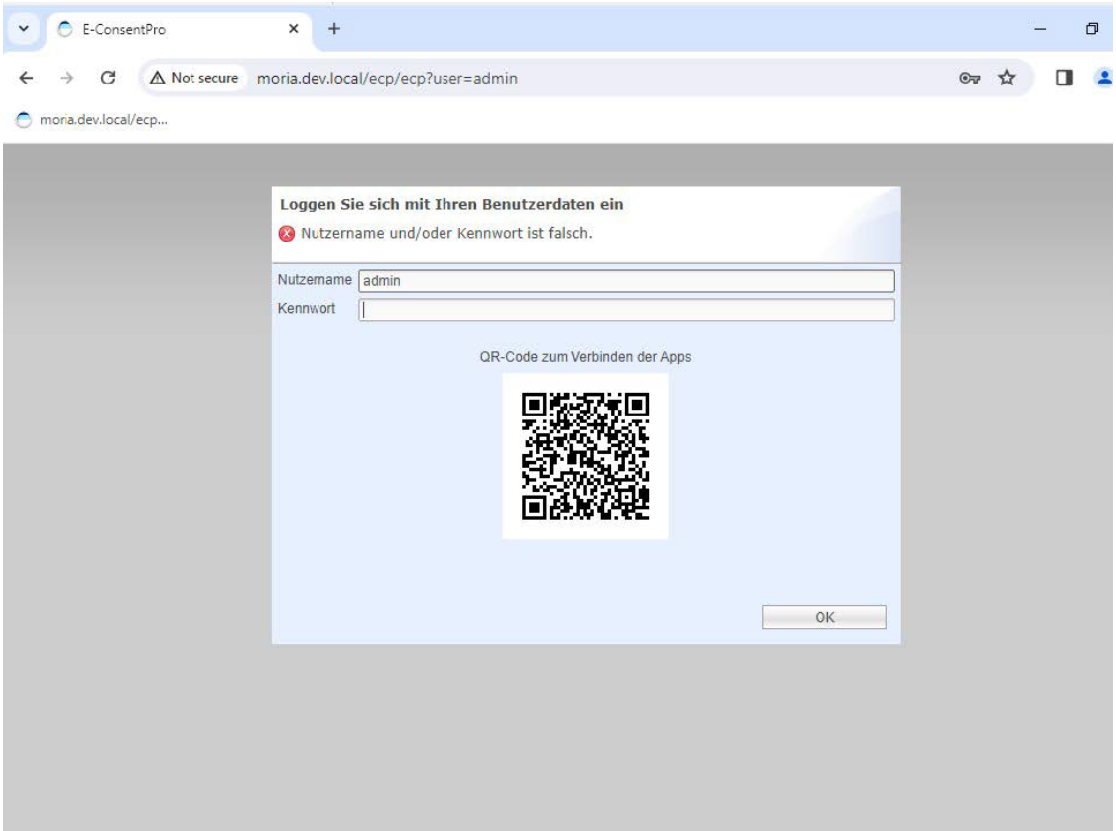
Die Domänebenutzerin „Alice“ meldet sich an einer Windows-Arbeitsstation an, die Teil der Domäne dev.local ist.



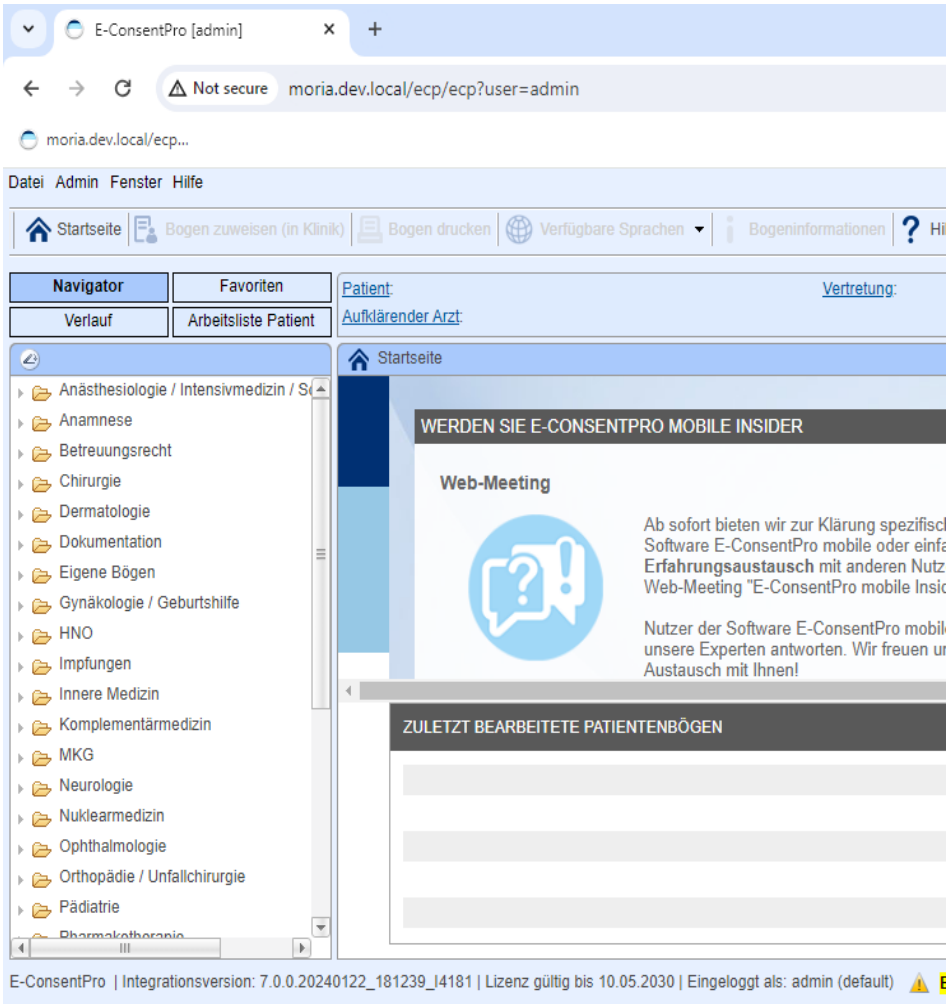
Alice möchte sich bei ECP als Benutzer "admin" anmelden.

Sie öffnet einen Browser und gibt die ECP-URL mit einem zusätzlichen Parameter ein: admin:

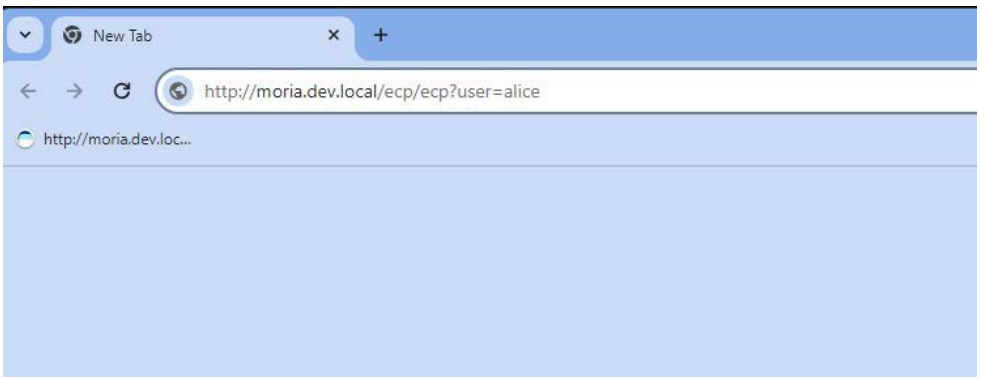
http://moria.dev.local/ecp/ecp?**user=admin**



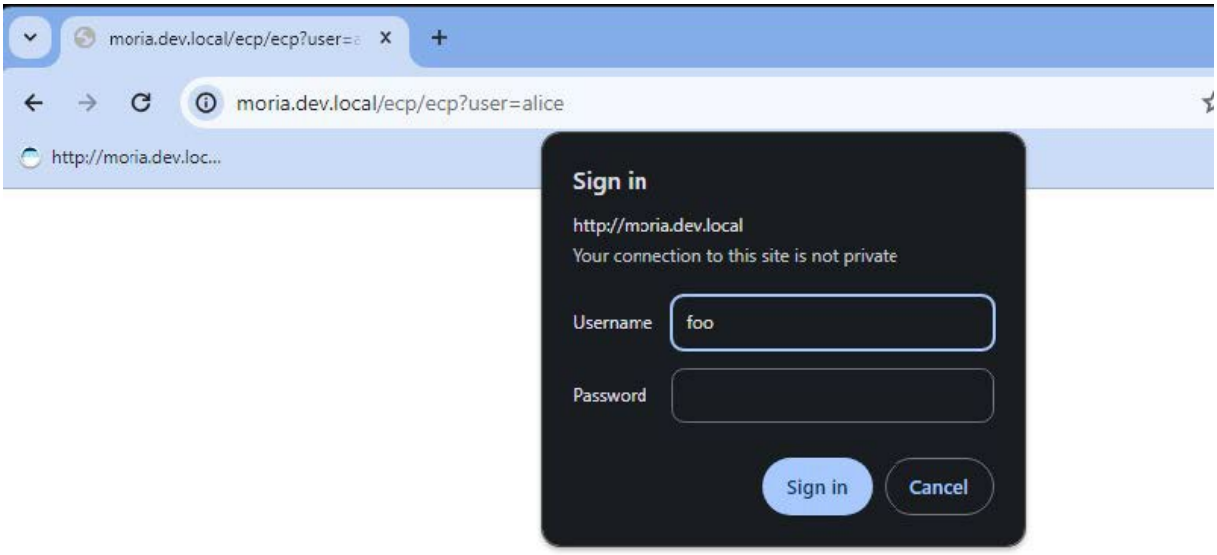
Beachten Sie den Benutzernamen in der Statusleiste am unteren Rand.



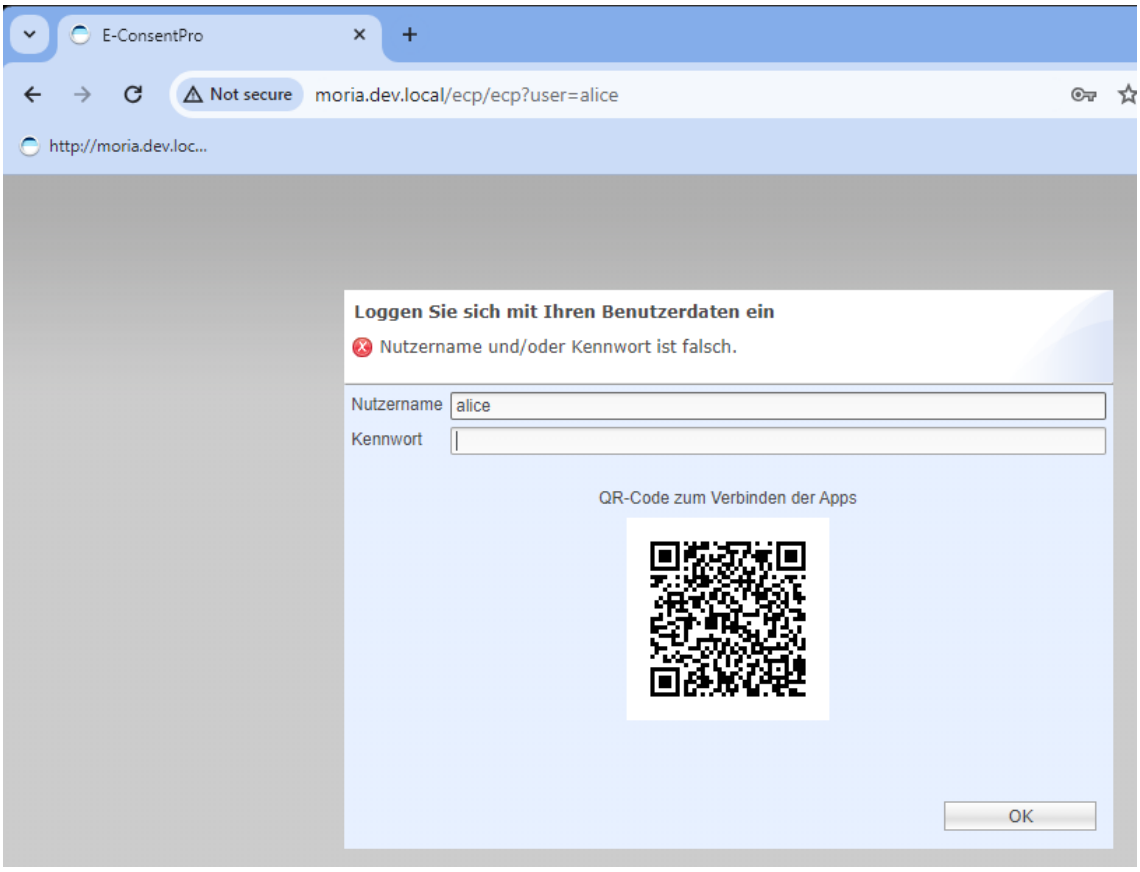
3.3. Verbindung zu ECP von einer Arbeitsstation außerhalb der AD-Domain



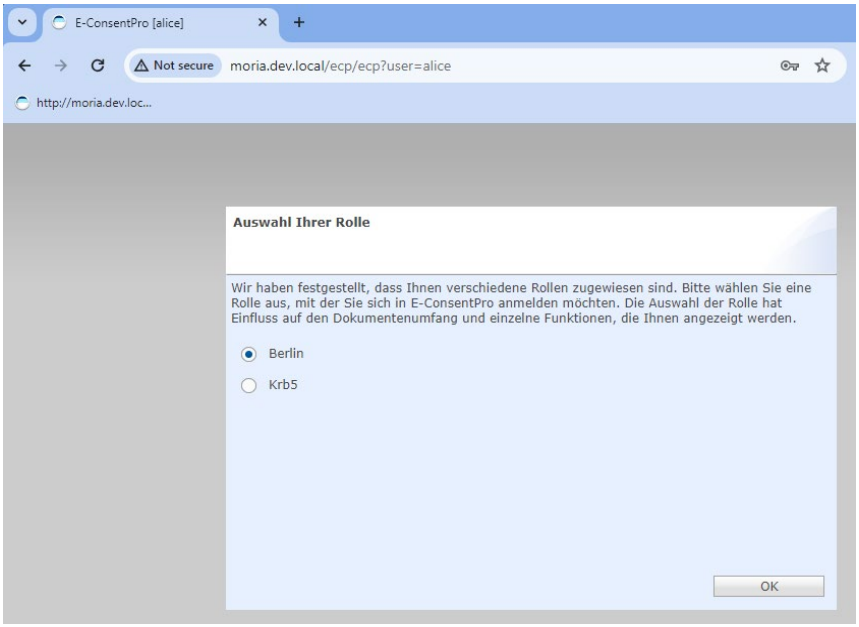
ACHTUNG! Geben Sie hier nicht Ihre echten Anmeldedaten ein – geben Sie einfach einige Buchstaben in das Feld Benutzername ein und klicken Sie auf „Anmelden“.

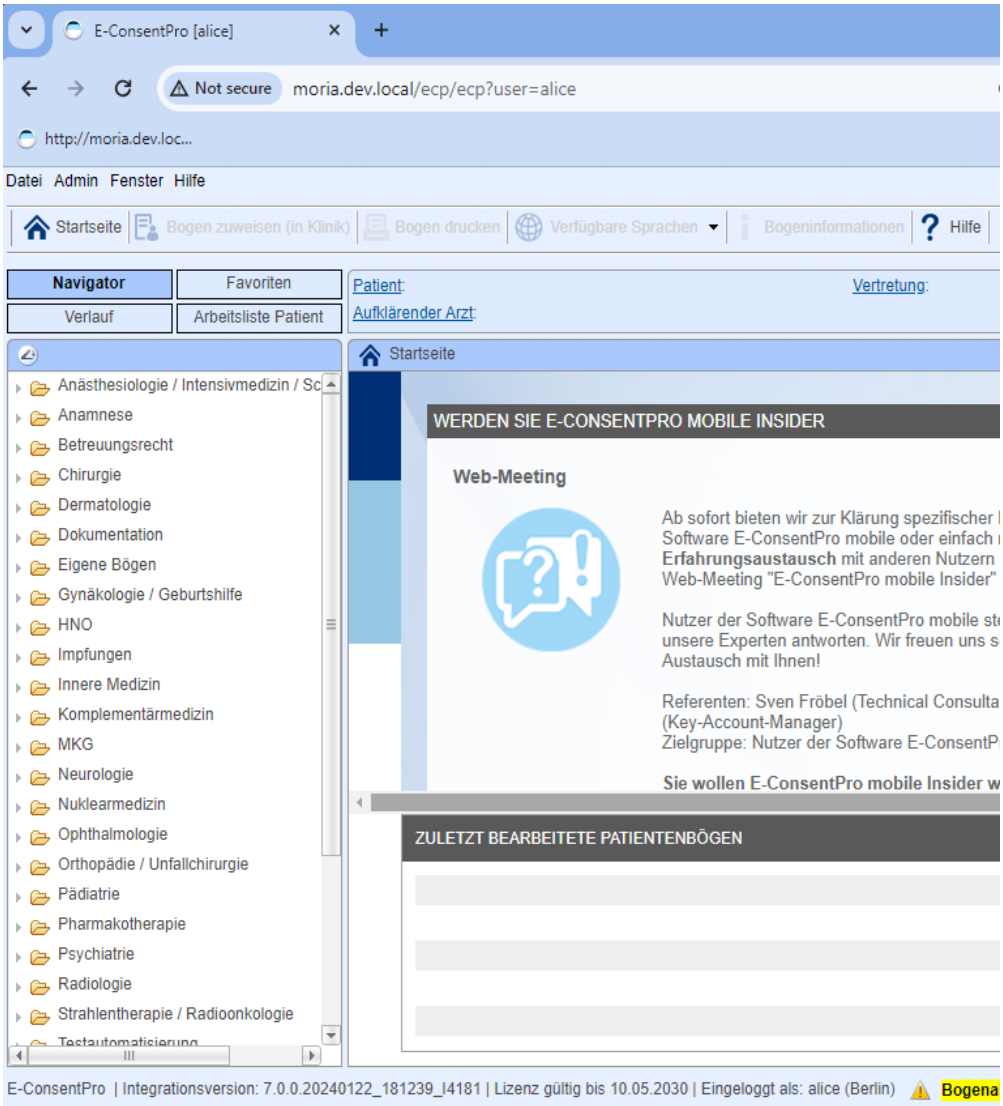


Die ECP-Anmeldeseite wird angezeigt.



Geben Sie nun das richtige Passwort ein und fahren Sie mit der ECP-Anmeldung fort.


E-ConsentPro [alice]
Not secure
moria.dev.local/ecp/ecp?user=alice
http://moria.dev.loc...
Auswahl Ihrer Rolle
Wir haben festgestellt, dass Ihnen verschiedene Rollen zugewiesen sind. Bitte wählen Sie eine Rolle aus, mit der Sie sich in E-ConsentPro anmelden möchten. Die Auswahl der Rolle hat Einfluss auf den Dokumentenumfang und einzelne Funktionen, die Ihnen angezeigt werden.
Berlin
Krb5
OK

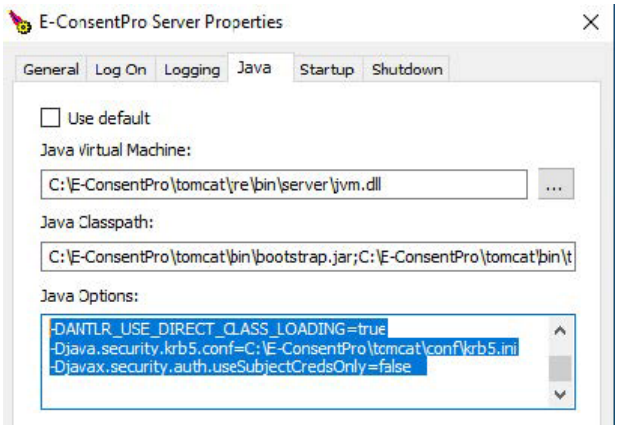

E-ConsentPro [alice]
Not secure
moria.dev.local/ecp/ecp?user=alice
http://moria.dev.loc...
Datei Admin Fenster Hilfe
Startseite
Bogen zuweisen (in Klinik)
Bogen drucken
Verfügbare Sprachen
Bogeninformationen
Hilfe
Navigator
Favoriten
Verlauf
Arbeitsliste Patient
Patient:
Vertretung:
Aufklärender Arzt:
Anästhesiologie / Intensivmedizin / Sc
Anamnese
Betreuungsrecht
Chirurgie
Dermatologie
Dokumentation
Eigene Bögen
Gynäkologie / Geburtshilfe
HNO
Impfungen
Innere Medizin
Komplementärmedizin
MKG
Neurologie
Nuklearmedizin
Ophthalmologie
Orthopädie / Unfallchirurgie
Pädiatrie
Pharmakotherapie
Psychiatrie
Radiologie
Strahlentherapie / Radioonkologie
Startseite
WERDEN SIE E-CONSENTPRO MOBILE INSIDER
Web-Meeting
Ab sofort bieten wir zur Klärung spezifischer
Software E-ConsentPro mobile oder einfach
Erfahrungsaustausch mit anderen Nutzern
Web-Meeting "E-ConsentPro mobile Insider"
Nutzer der Software E-ConsentPro mobile st
unsere Experten antworten. Wir freuen uns s
Austausch mit Ihnen!
Referenten: Sven Fröbel (Technical Consulta
(Key-Account-Manager)
Zielgruppe: Nutzer der Software E-ConsentP
Sie wollen E-ConsentPro mobile Insider w
ZULETZT BEARBEITETE PATIENTENBÖGEN
E-ConsentPro | Integrationsversion: 7.0.0.20240122_181239_I4181 | Lizenz gültig bis 10.05.2030 | Eingeloggt als: alice (Berlin)
Bogena

4. Fehlersuche

4.1. Leerzeichen in VM-Parametern – “false“ != “false “

Manifestation: SSO funktioniert nicht.

Überprüfen: Stellen Sie sicher, dass nach "false" und "true" keine Leerzeichen stehen. Oft werden sie beim Kopieren/Einfügen der VM-Parameter angehängt.



4.2. GSSException: Failure unspecified at GSS-API level (Mechanism level: Checksum failed)

Manifestation: SSO funktioniert nicht, die ECP-Protokolle enthalten eine Ausnahme:

```
2024-01-21 23:19:11.272 [http-nio-80-exec-2] ERROR c.t.e.c.a.a.sso.SpnegoFilter -

org.ietf.jgss.GSSException: Failure unspecified at GSS-API level (Mechanism level: Checksum
failed)

at java.security.jgss/sun.security.jgss.krb5.Krb5Context.acceptSecContext(Unknown Source)

at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

at java.security.jgss/sun.security.jgss.spnego.SpNegoContext.GSS_acceptSecContext(Unknown
Source)

at java.security.jgss/sun.security.jgss.spnego.SpNegoContext.acceptSecContext(Unknown Source)

at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

at
com.thieme.ecp.client.accesscontrol.authentication.sso.SpnegoFilter.authenticate(SpnegoFilter.
java:82)

at
com.thieme.ecp.client.accesscontrol.authentication.sso.SpnegoFilter.doFilter(SpnegoFilter.java
:61)
```

Wahrscheinliche Ursache: Der Name des Auftraggebers im SPN stimmt nicht mit dem Namen in der Schlüsseltabelle überein.

Bei den Principal-Namen wird zwischen Groß- und Kleinschreibung unterschieden. Vergewissern Sie sich, dass der SPN, den Sie erstellt haben, mit dem übereinstimmt, der zur Erstellung der Keytab verwendet wurde (siehe Abschnitte 2.1.2 und 2.1.3)

Abhilfe: Erstellen Sie eine neue Keytab-Datei, deren Principal-Namen mit dem SPN übereinstimmen. Kopieren Sie die neue Keytab-Datei auf den ECP-Server. Starten Sie ECP neu.

4.3. GSSException: Failure unspecified at GSS-API level (Mechanism level: Encryption type RC4 with HMAC is not supported/enabled)

Manifestation: SSO funktioniert nicht, die ECP-Protokolle enthalten eine Ausnahme:

```
org.ietf.jgss.GSSException: Failure unspecified at GSS-API level (Mechanism level: Encryption
type RC4 with HMAC is not supported/enabled)

    at java.security.jgss/sun.security.jgss.krb5.Krb5Context.acceptSecContext(Unknown Source)

    at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

    at java.security.jgss/sun.security.jgss.GSSContextImpl.acceptSecContext(Unknown Source)

    at java.security.jgss/sun.security.jgss.spnego.SpNegoContext.GSS_acceptSecContext(Unknown
Source)
```

Wahrscheinliche Ursache: Das ECP-Dienstkonto ist nicht richtig konfiguriert.

Abhilfe: Aktivieren Sie die Kerberos AES128bit und AES256bit Verschlüsselung für das Dienstkonto.