gemdat

Vorbereitung Installation «gemdat bau» für Silverlight-Installationen

Rollenverzeichnis

Rolle	Mitarbeiter
Dokumentenverantwortlicher	Gemdat
Reviewzirkel	Gemdat
Zielgruppe	Systemverantwortlicher Kunde, Integration Gemdat

Änderungsverzeichnis

Datum	Änderungen	Version	Person
04.04.2025	Aufteilung Dokument nur Silverlight	8.7	Tanja Muñoz
19.12.2024	Redirect Url für Clients angepasst (Kap. 5.1.2 und 5.2.2)	8.6	Daniel Wolf
05.11.2024	Token Claims ergänzt	8.5	Daniel Wolf
27.08.2024	Azure Konfiguration für WebDav	8.4	Marco Sutter
14.08.2024	Valid Issuer braucht ein / am Schluss	8.3	Daniel Wolf
18.07.2024	Ergänzung email für Token Konfiguration + Kapitel 8 (ME-Kompatibilität)	8.2	Raphael Gubler
19.06.2024	Aktualisierung für Version 7.2	8.1	Silvio Fuchs
10.04.2024	Benutzer Authentifizierung mit Entra ID und AD FS	8.0	Marco Sutter

Zweck des Dokuments

Dieses Dokument beschreibt die Vorbereitungsarbeiten für die Installation von «gemdat bau». Diese sind durch den Systemverantwortlichen kundenseitig auszuführen.

Inhalt

1 Allgemeines

1.1 Ziele

Der Administrator muss die Infrastruktur so weit vorbereiten, dass eine Installation von «gemdat bau» durch Gemdat AG ohne Neustart des Systems vorgenommen werden kann.

1.2 Informationen

Datenbankserver, Applikationsserver (Webserver) und Dateiablage können zusammen auf einem oder auch getrennt auf mehreren Servern betrieben werden.
Dieses Dokument beschreibt die minimal notwendigen Anforderungen an Datenbank und Webserver. Optional können weitere Features installiert werden.

1.3 Anhang

— Checkliste Vorbereitung
— Infoblatt (Server Informationen)
— Update von früheren Versionen

2 Installation Webserver-Rolle

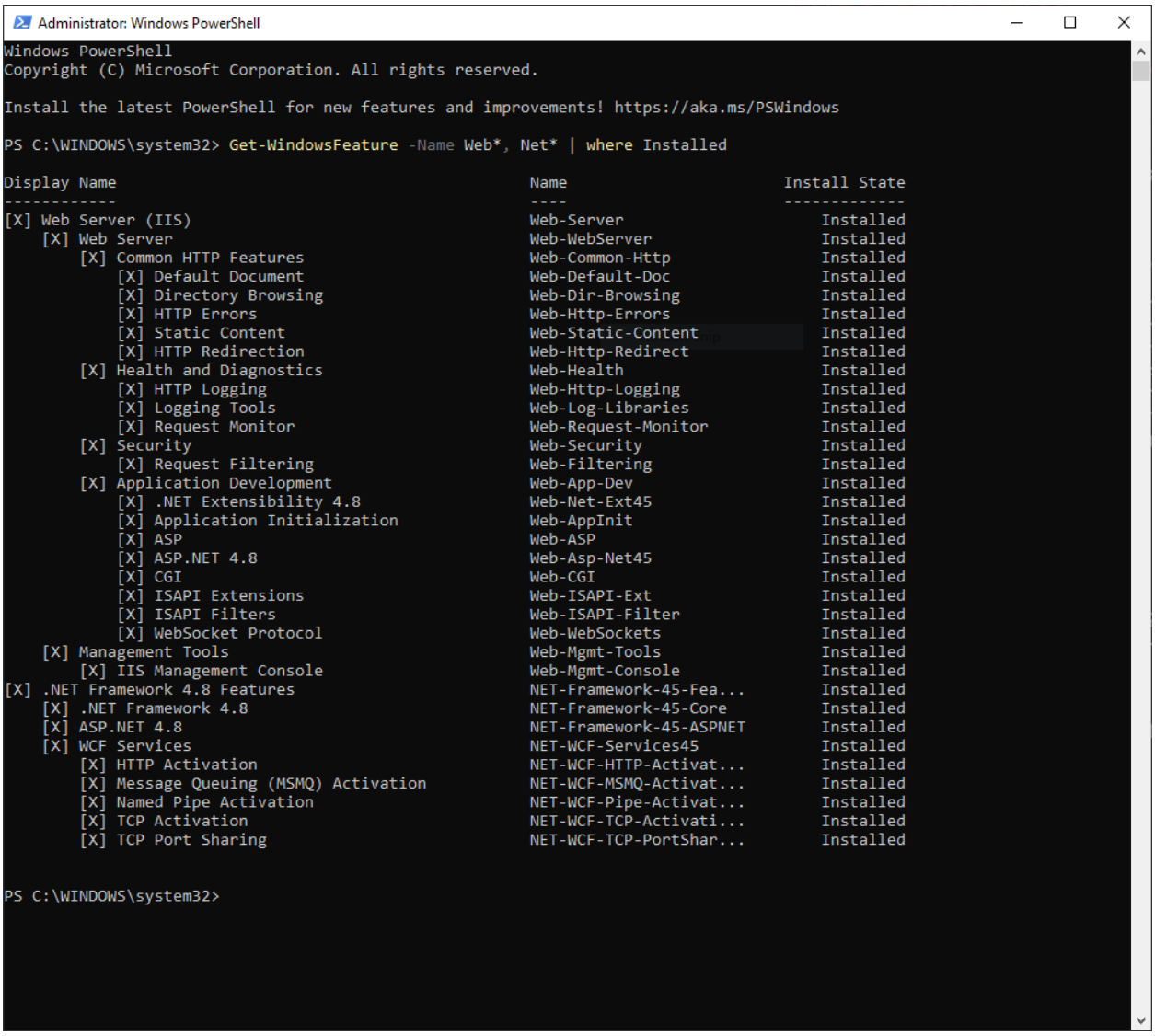
2.1 Beschreibung

Auf dem Applikationsserver muss die Webserver-Rolle IIS installiert werden. Die für «gemdat bau» erforderlichen Rollendienste und Features sind in diesem Abschnitt beschrieben. Falls die IIS Rolle bereits installiert ist, muss kontrolliert werden, ob alle erforderlichen Features installiert sind.

2.2 Installation .NET

.NET muss gemäss dem Dokument «Technische Voraussetzungen» installiert sein.

2.3 IIS Rollen



Wichtig: Nachfolgende Hinweise beachten!

```
Import-Module ServerManager
Get-WindowsFeature -Name Web*, Net* | where Installed
```

Einstellungen:

- IIS Feature: Urlrewrite 2.1 muss installiert sein
- IIS Performance Feature «dynamic content compression» muss deaktiviert oder deinstalliert sein
- IIS Performance Feature «static content compression» muss deaktiviert oder deinstalliert sein

Hinweis:
Name des Applikationsservers auf Infoblatt vermerken!

2.4 Betrieb über HTTPS

Damit «gemdat bau» über HTTPS betrieben werden kann, ist der Kunde für ein passendes Zertifikat verantwortlich. Dieses muss auf dem Applikationsserver installiert sein.

Hinweis:
Weitere Infos unter Kapitel 6 DNS Konfiguration

2.5 Bei Verwendung «gemdat archiv»: Verteiltes Transaction-Handling aktivieren

Bei Kunden, die das Produkt «gemdat archiv» lizenziert haben, muss die 'MS Transaction Manager Communication' aktiviert werden:

- Via Aufruf 'dcomcnfg' → Component Services → Computers → MyComputer → Distibuted Transaction Coordinator → Local DTC → Properties → Security → Enable (Allow Inbound & Allow Outbound)

Grund: Der Token wird in einem verteilten Cache gespeichert, welcher allen Worker-Prozessen des IIS sowie der Job-Engine zur Verfügung steht. Daher muss auf dem Applikations- und Datenbankserver das verteilte Transaktions-Handling eingeschaltet sein.

3 Einrichtung SQL-Server

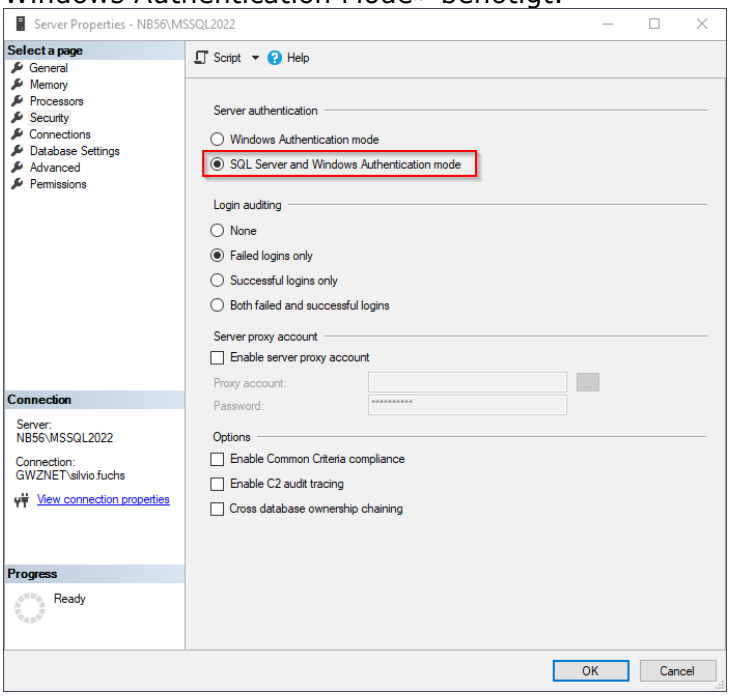
3.1 Beschreibung

Als Datenbank-Server wird Microsoft SQL in englischer Standardsprache vorausgesetzt. Gemdat empfiehlt die Installation einer Test- und Produktiv-Datenbank. Die beiden Datenbanken können wahlweise auf unterschiedlichen Instanzen oder Servern betrieben werden.

Hinweis:
Datenbank-Server Host Name, SQL Server Instanz Name und Datenbank Name im Infoblatt ergänzen.

3.2 Kompatibilität zu Gemdat/5

Falls «GemDat/5» und «gemdat bau» parallel betrieben werden, wird «SQL Server and Windows Authentication Mode» benötigt.



Für «gemdat bau» allein genügt «Windows Authentication Mode».

4 Einrichten ActiveDirectory

4.1 Beschreibung

Um die JobEngine und den Anwendungspool von «gemdat bau» auszuführen, wird ein Domänen-Benutzer (Dienstbenutzer) benötigt. Dieser Benutzer wird später als Dienstbenutzer für den GemDatJobEngine-Dienst (Windows Service) und den IIS-Anwendungspool benötigt.

Hinweis:
Benutzernamen auf Infoblatt im Anhang vermerken!

4.2 Anmeldeberechtigungen für den Dienstbenutzer vergeben

Der «gemdat bau»-Dienstbenutzer benötigt auf dem Applikationsserver Anmeldeberechtigung als Dienst und Stapelverarbeitungsauftrag.

4.3 E-Mail-Feld bei Benutzern mit «gemdat archiv» oder «gemdat sign»

Damit sich ein «gemdat archiv» Benutzer auch erfolgreich bei «gemdat archiv» oder «gemdat sign» authentifizieren kann muss im entsprechenden Verzeichnisdienst (z.B. Active Directory oder Entra-ID) auf dem Benutzerobjekt das E-Mail-Feld abgefüllt sein. Falls der/die Benutzer/in keine E-Mail besitzt kann auch eine nicht funktionierende oder erfundene E-Mail-Adresse verwendet werden.

5 Konfiguration der Autorisierungs-Instanzen

«gemdat bau» unterstützt ab Version 7.2 «Microsoft Entra ID» und «Active Directory Federation Service» (AD FS) als Benutzer Autorisierungs- Instanzen. «Microsoft Active Directory» ist hingegen nicht mehr unterstützt. Für die Verwendung von EntraID ist die Einrichtung der Installation auf HTTPS unter Punkt 2.4 zwingend.

5.1 Konfiguration «Microsoft Entra ID»

Für «gemdat bau» müssen in Microsoft Entra ID zwei App Registrationen vorgenommen werden, je eine Registration für die Frontend- und Backend- App:

- gemdat bau [name]-frontend
- gemdat bau [name]-backend

(Die Namensgebung muss nicht zwingend dem vorgeschlagenen Namensschema folgen, es gibt diesbezüglich keine Restriktionen)

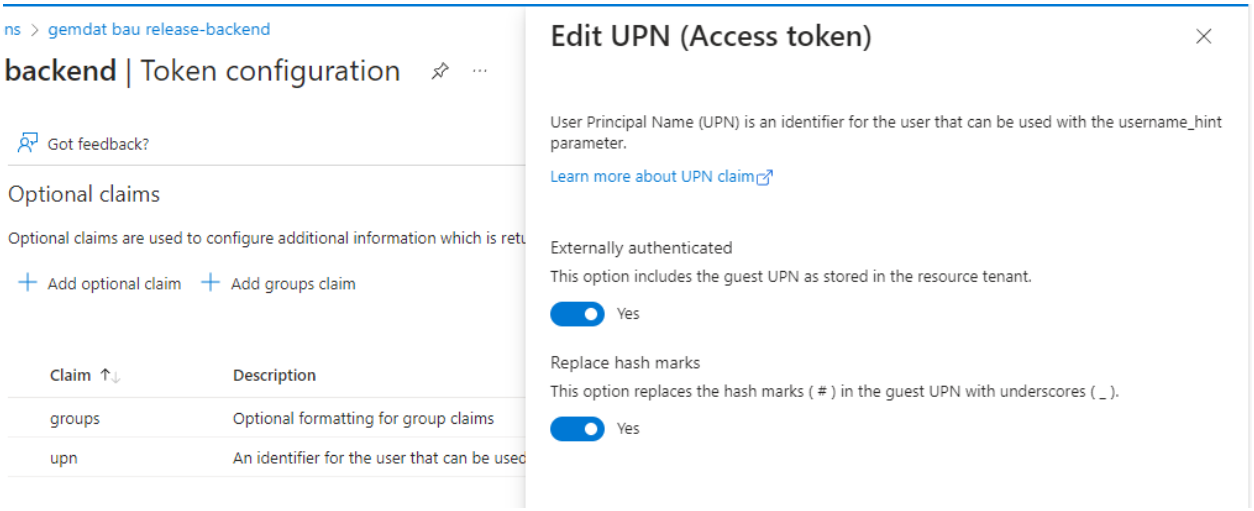
5.1.1 Konfiguration Backend App Registration

Tab «Tokenkonfiguration»

Es sind folgende optionale Ansprüche (Claim) hinzuzufügen. Diese Claims sind einerseits für die Aufnahme der Sicherheitsgruppen ins generierte «access_token» erforderlich. Andererseits wird der angemeldete Benutzer über den UPN (User Principal Name) identifiziert. Zwingend notwendig ist das «email» Claim als Token type «Access».

Claim ↑↓	Description	Token type ↑↓	Optional settings
email	The addressable email for this user, if the user has one	Access	-
groups	Optional formatting for group claims	ID, Access, SAML	Default
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and should not be used to key data	Access	Yes

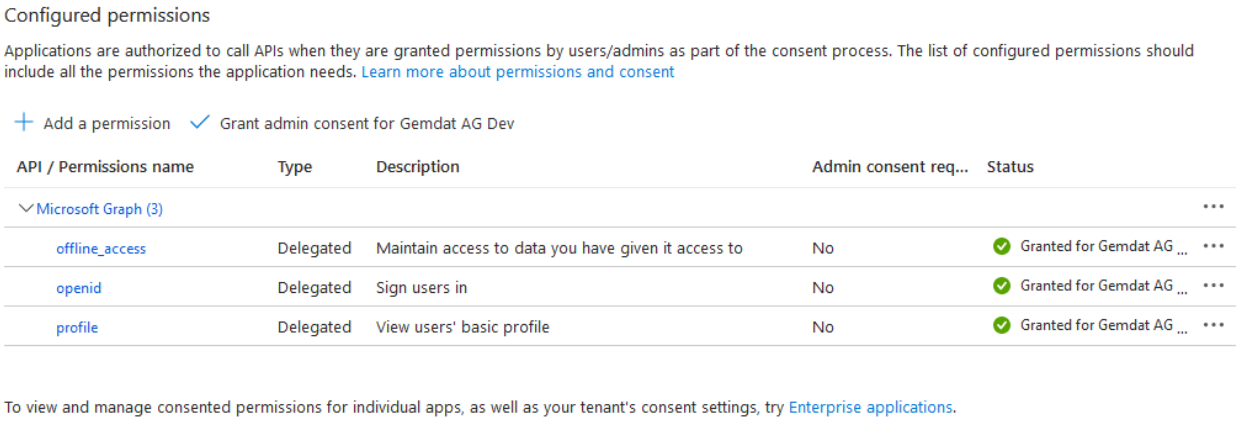
Beim UPN Access Token müssen die Optionen «Externally authenticated» und «Replace hash marks» aktiviert werden.



Tab «API-Berechtigungen»

Es wird bei Microsoft Graph die Berechtigungen für offline_access, openId und profile benötigt.

Nach der korrekten Zuweisung sieht das beispielsweise so aus:



Administratoreinwilligung muss gewährt werden.

Tab «Eine API verfügbar machen»

Ein neuer Bereich «Bau.All» muss gemäss folgendem Schema zugefügt werden:

- api://[clientId]/Bau.All

wobei [clientId] der Application (client) ID der Backend App Registration entsprechen soll.

Beispiel:

Hinweis:

Client ID und Bereich (Audience) auf Infoblatt im Anhang vermerken!

5.1.2 Konfiguration Frontend- App

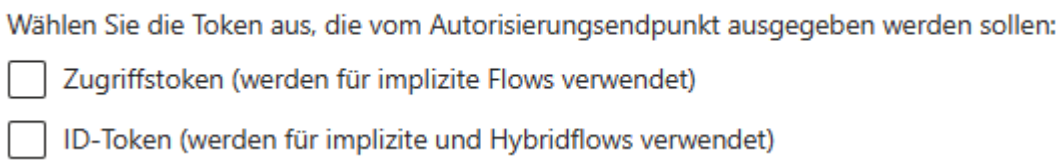
Tab «Authentifizierung»
Hier müssen die Redirect URLs für die «Single-Page-Webanwendung» erfasst werden. Konkret müssen 4 URLs registriert werden: Silverlight Bau/Admin und Html5 Bau/Admin. Dabei ist zu beachten, dass die URLs exakt der Installation vom «gemdat bau» entsprechen müssen (Registrierte Domain, Webseite im IIS, Relativer Pfad der Webanwendung):

- https://[domain]/[site]/[page]

Beispielkonfiguration:

Client	Client Typ	Beispiel Redirect Url
Admin Client	Html	https://gemdat.contoso.com/bau/bau-client-admin
Bau Client	Html	https://gemdat.contoso.com/bau/bau-client
Admin Client	Silverlight	https://gemdat.contoso.com/bau/App/GemDatAdmin.aspx
Bau Client	Silverlight	https://gemdat.contoso.com/bau/App/GemDatBau.aspx

Keine impliziten Genehmigungen:



Tab «Tokenkonfiguration»
Es sind folgende optionalen Ansprüche (Claims) hinzuzufügen. Diese werden im ID Token für die Identifizierung und Anzeige des Benutzers verwendet.

Folgende Claims müssen zwingend konfiguriert werden:

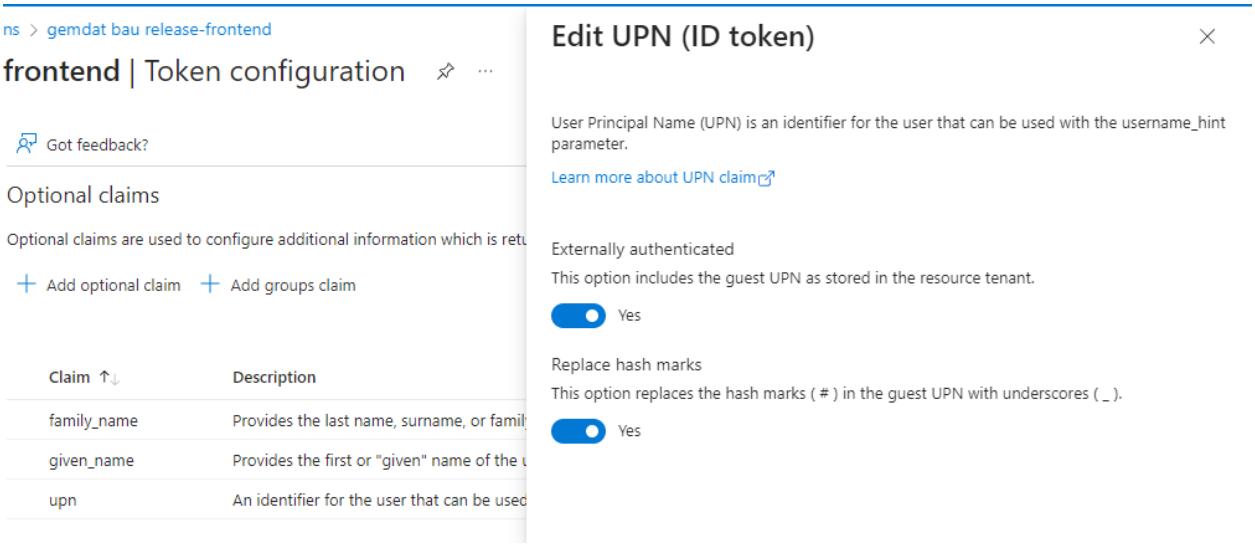
- User Principal Name/ upn
- email

Folgende Claims können optional als Good Practices konfiguriert werden:

- family_name
- given_name

Claim	Description	Token type	Optional settings
email	The addressable email for this user, if the user has one	Access	-
family_name	Provides the last name, surname, or family name of the user as defined in the user object	ID	-
given_name	Provides the first or "given" name of the user, as set on the user object	ID	-
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and should not be used to key data	ID	Yes

Beim UPN ID Token müssen die Optionen «Externally authenticated» und «Replace hash marks» aktiviert werden.

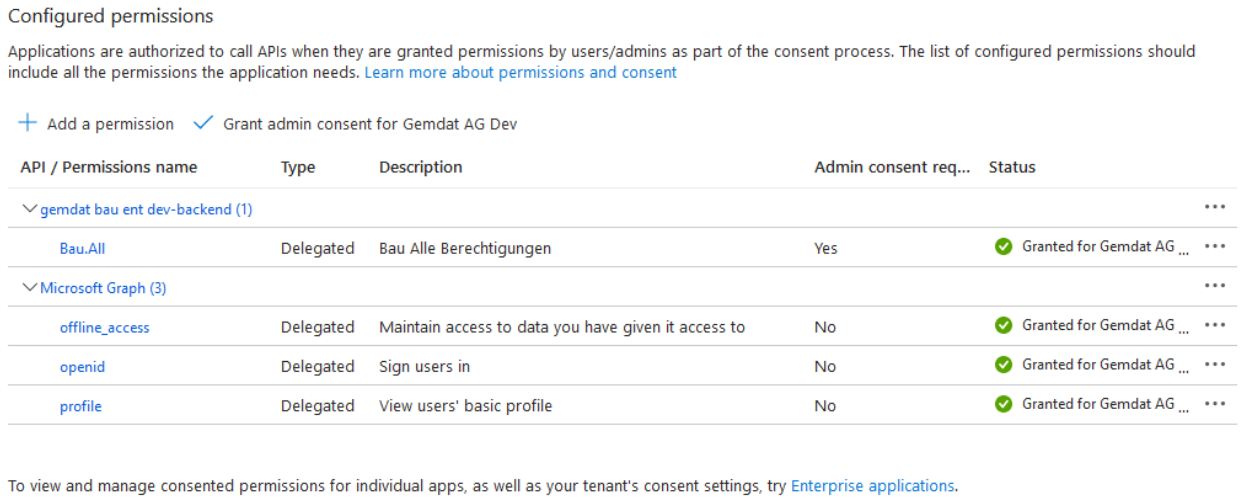


Tab «API-Berechtigungen»

Um die zuvor im Backend zur Verfügung gestellte API hinzuzufügen, kann über den Button «Berechtigung hinzufügen» zunächst ein Dialog geöffnet werden, wo im Tab «Von meiner Organisation verwendete API's» die API der Backend App Registration ausgewählt werden muss.

Es wird bei Microsoft Graph die Berechtigungen für offline_access, openId und profile benötigt.

Nach der korrekten Zuweisung sieht das beispielsweise so aus:



Administratoreinwilligung muss gewährt werden.

5.1.3 Einrichtung der Sicherheitsgruppen und Benutzer

Im gleichen Tenant, in dem die App- Registrationen vorgenommen worden sind, sind die gewünschten Sicherheitsgruppen anzulegen. Zudem müssen die Benutzer für «gemdat bau» angelegt und den entsprechenden Sicherheitsgruppen zugewiesen werden.

Typische Sicherheitsgruppen sind:

Folgende Benutzer und Sicherheitsgruppen sind empfohlen:

Bezeichnung	**AD Typ**	**Beschreibung**
Gemdat_TestUser	Benutzer	Testbenutzer für den Funktionstest nach der Installation. (Stellt einen Mitarbeiter dar, welcher mit «gemdat bau» arbeitet)
Gemdat_Administratoren	Gruppe	Gruppe für die Administration von «gemdat bau» **(zwingend erforderlich)**
Gemdat_Bauverwaltung	Gruppe	Sicherheitsgruppe für «gemdat bau» (Standard-) Anwender
Gemdat_Lesend	Gruppe	Sicherheitsgruppe für «gemdat bau» Anwender mit Leseberechtigung

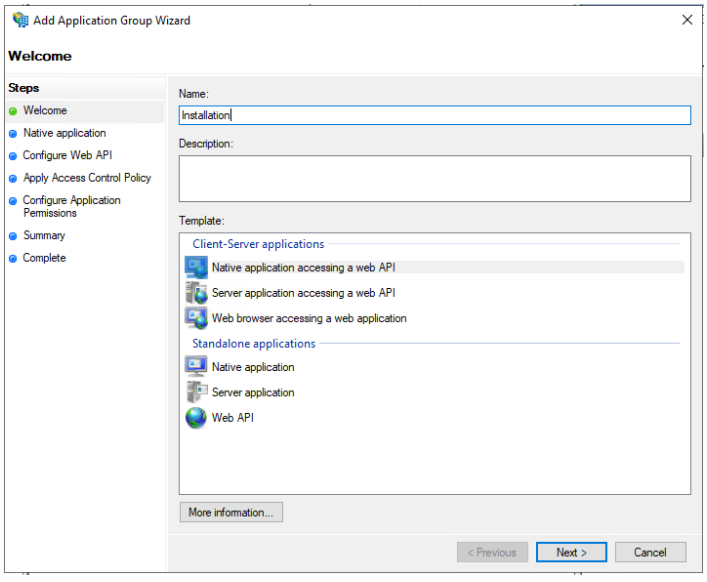
Die UUID’s (Universally Unique Identifier) dieser Entra ID Sicherheitsgruppen müssen in der Bau Anwendung den Bau Sicherheitsgruppen zugewiesen werden.

Hinweis:
Die Administratoren Sicherheitsgruppe ist zwingend erforderlich. Die UUID der Administratoren Sicherheitsgruppe auf Infoblatt im Anhang vermerken!

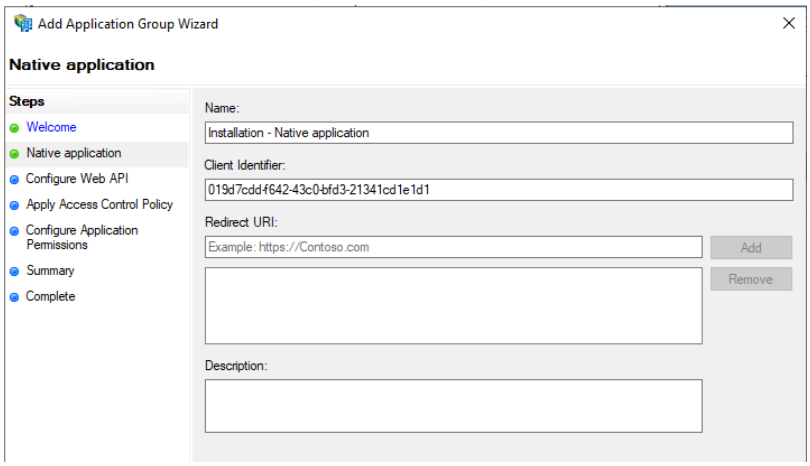
5.2 Konfiguration «AD FS»

5.2.1 Einrichten Applikation Gruppe

Für die Konfiguration des AD FS Service soll in der AD FS Adminkonsole eine neue Application Group erstellt werden. Dabei muss dieser einen sprechenden Namen geben werden. Aus Sicht «gemdat bau» kann dieser frei gewählt werden. Für die Applikation kann sowohl «Native application accessing a web API» oder «Web browser accessing a web application» gewählt werden. Diese haben beide dasselbe Resultat. In dieser Anleitung gehen wir auf erstes ein.



5.2.2 Native Application



Für die Native Application ist ebenfalls ein Name zu definieren, falls der generierte Standard nicht den Wünschen des Betriebsteam der Kunden IT entsprechen sollte. Anschliessend ist der Client Identifier zu kopieren und in den Anhängen zu vermerken. Dies ist die ClientID für «gemdat bau». Zum Schluss sind die Redirect URIs zu erfassen nach dem Schema aus dem folgenden Kapitel.

Erfassung der Redirect URLs:
Konkret müssen 4 Redirect URLs registriert werden: Silverlight Bau/Admin und Html5 Bau/Admin. Dabei ist zu beachten, dass die URLs exakt der Installation vom «gemdat bau» entsprechen müssen (Registrierte Domain, Webseite im IIS, Relativer Pfad der Webanwendung):

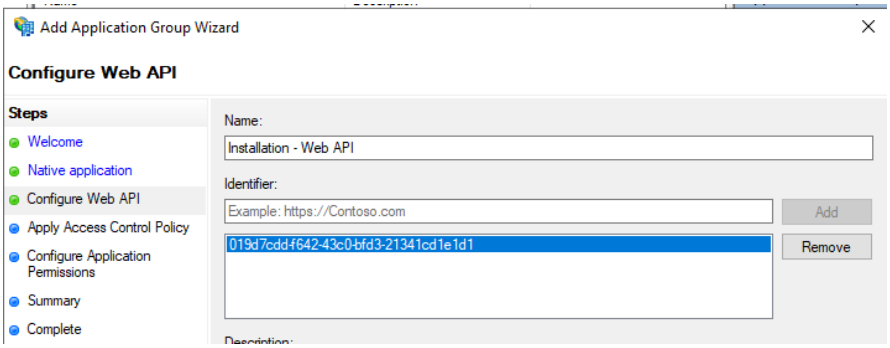
- https://[domain]/[site]/[page]

Beispielkonfiguration:

Client	Client Typ	Beispiel Redirect Url
Admin Client	Html	https://gemdat.contoso.com/bau/bau-client-admin
Bau Client	Html	https://gemdat.contoso.com/bau/bau-client
Admin Client	Silverlight	https://gemdat.contoso.com/bau/App/GemDatAdmin.aspx
Bau Client	Silverlight	https://gemdat.contoso.com/bau/App/GemDatBau.aspx

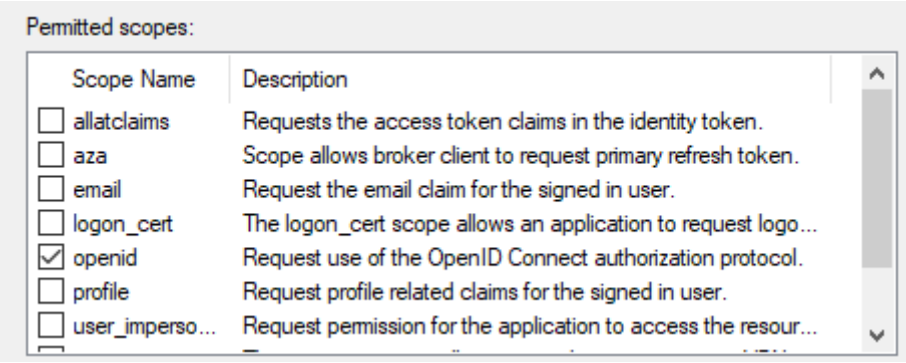
5.2.3 Konfiguration der WebAPI

Für die WebApi kann ebenfalls nach Wünschen des Betriebsteams der Namen definiert werden. Anschliessend muss der Identifier aus dem Punk 5.2.2 hinzugefügt werden.



5.2.4 Authentifizierungsberechtigungen

Im Anschluss an die Konfiguration der WebApi kann definiert werden, wer sich über diese Applikationsgruppe authentifizieren kann. Dies hat noch nicht explizit etwas mit «gemdat bau» zu tun, sondern ist eine AD FS Autorisierungsfunktion.
Wir empfehlen hier eine Gesamtgruppe zu erstellen, die die einzelnen Gemdat Berechtigungsgruppen enthält, und diese dann als «Permit Specific group» hinzuzufügen.
Anschliessend können für die «Native Application» die Scopes oder Anforderungsberechtigungen gesetzt werden. Hier ist relevant, dass für «gemdat bau» die «openid» Berechtigung gesetzt wird.

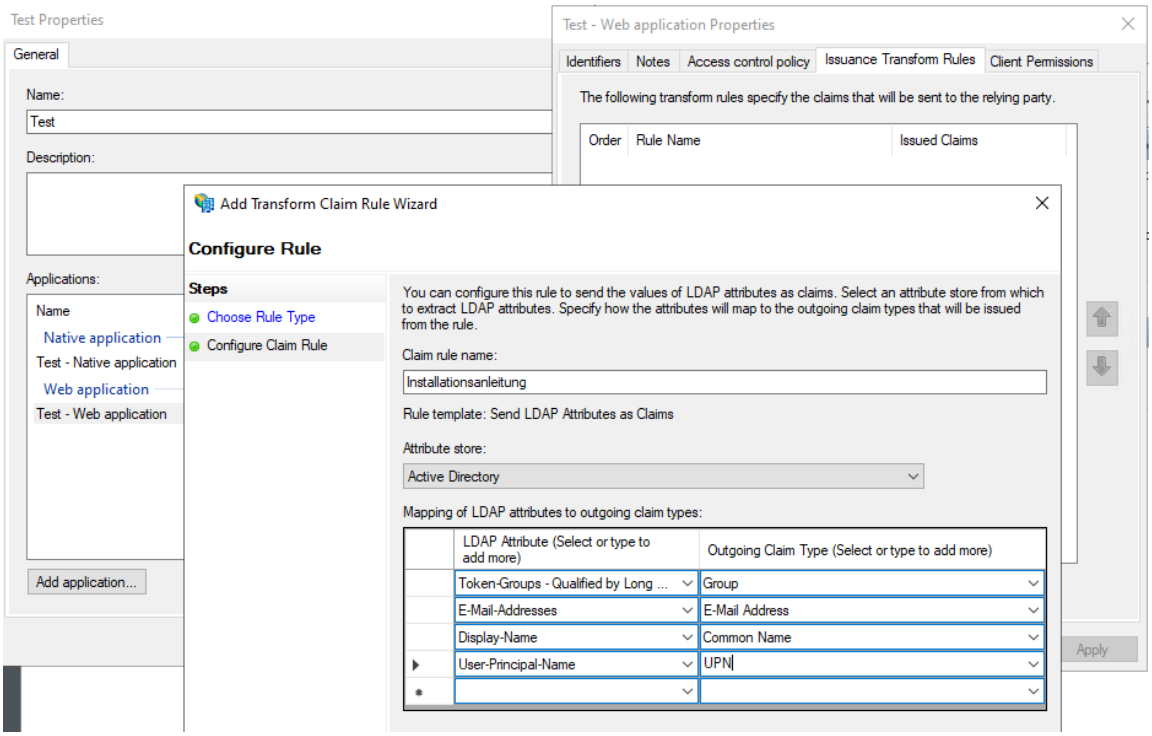


Nun kann die Applikationserstellung abgeschlossen werden. Es sind jedoch noch die Token Claims zu konfigurieren.

5.2.5 Token Claims

Die neu erstellte Applikationsgruppe soll nun erneut geöffnet werden. Anschliessend die Webapplication oder WebApi öffen. Im Reiter den Issuance Transform Rules auswählen. Hier muss nun eine neue Rule erstellt werden. In der neuen Rule kann ein Name definiert werden, der der Applikation zugeordnet werden kann. Als Attribute Store soll das darunterliegende Active Directory dienen, dieses muss entsprechend ausgewählt werden. Nun können die Attribute Übersetzungen zwischen den JWT Token Claims und den Active Directory vorgenommen werden. Es sind folgende:

Surname	Surname
Given-Name	Given Name
Token-Groups – Qualified by Long Domain Name	Group
E-Mail-Addresses	E-Mail Address
Display-Name	Common Name
User-Principal-Name	UPN



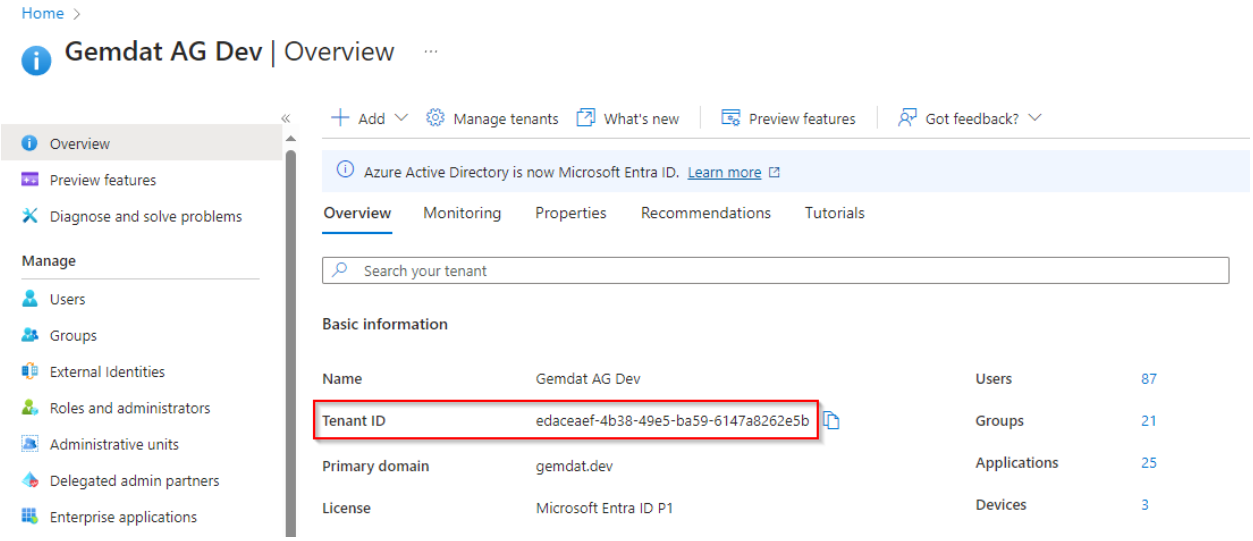
Mit der Konfiguration der Attribute Übersetzungstabelle ist die Konfiguration für «gemdat bau» abgeschlossen.

5.3 Konfiguration «gemdat bau»

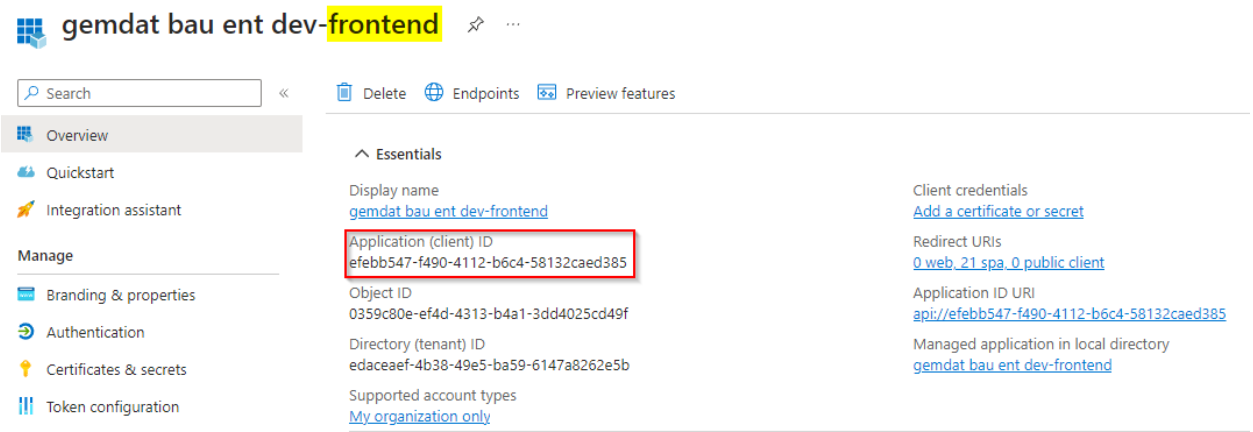
5.3.1 Microsoft Entra ID

Bei einer Neuinstallation oder einem Update ab Version 7.2 von «gemdat bau» müssen im Installationswizard folgende Parameter angegeben werden:

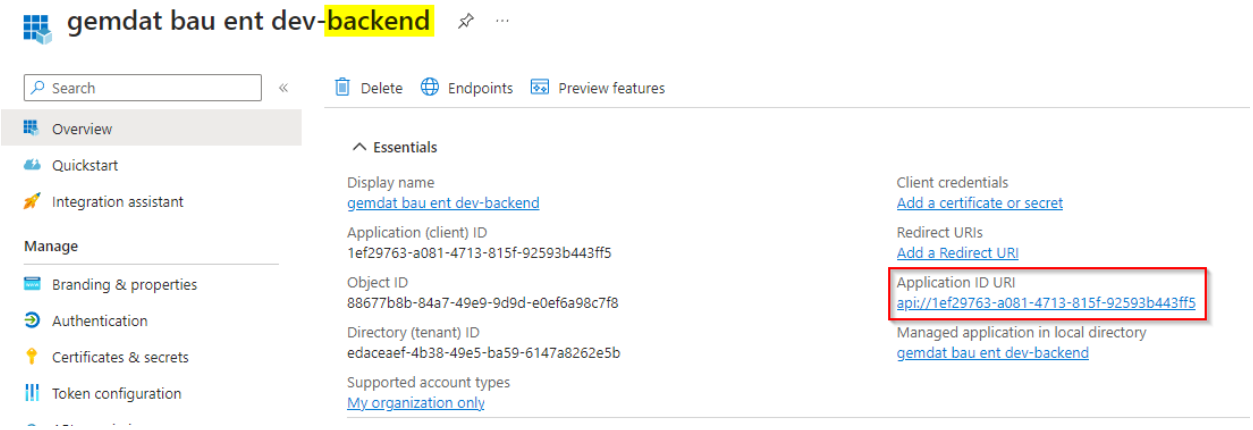
Tenant ID
UUID der Instanz von Microsoft Entra ID (Tab Overview)



Client ID
Application (client) ID der Frontend App Registration



Application ID/ Audience
Application ID URI (Audience) der Backend App Registration



Hinweis:
Für Access Token Format V2.0 wird die Audience ohne "api://" konfiguriert

Authority
Die Authority von Microsoft Entra ID.
Beispiel: `https://login.microsoftonline.com`

Open ID Config
Open ID Config von Microsoft Entra ID.
Beispiel: `https://login.microsoftonline.com/organizations/v2.0/.well-known/openid-configuration`

Valid Issuer
Access Token Format V1.0: https://sts.windows.net/<Tenant ID>/
Beispiel: https://sts.windows.net/edaceaef-4b38-49e5-ba59-6147a8262e5b/

Access Token Format V2.0: https://login.microsoftonline.com/<Tenant ID>/v2.0
Beispiel: https://login.microsoftonline.com/edaceaef-4b38-49e5-ba59-6147a8262e5b/v2.0

5.3.2 AD FS

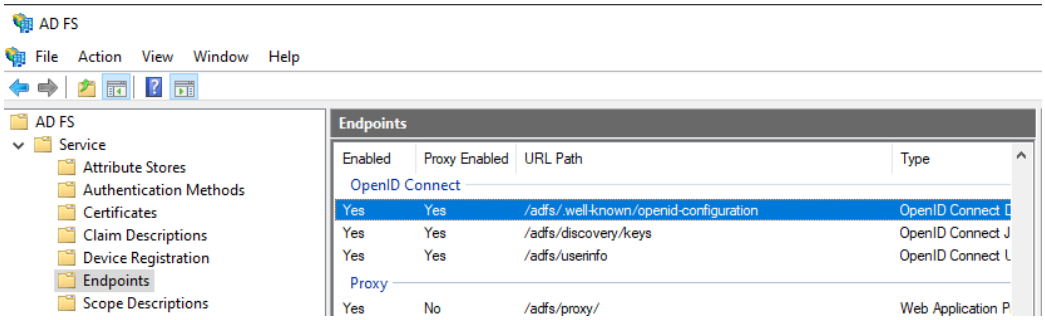
Bei einer Neuinstallation oder einem Update ab Version 7.2 von «gemdat bau» müssen im Installationswizard folgende Parameter angegeben werden:

Client ID
Die Client ID ist die ID die unter Schritt 5.2.2 gespeichert und ins Infoblatt vermerkt wurde.

Authority
Ist die URl unter welcher das AD FS bei der Grundinstallation installiert wurde. Dieser Parameter kann mittels Powershell ermittelt werden:
'Get-ADFSProperties' anschliessend ist dieser als «Hostname» Property aufgeführt.

Application ID/ Audience
Dieser Parameter kann mittels Powershell ermittelt werden:
'Get-ADFSProperties' anschliessend ist dieser als «IdTokenIssuer» Property aufgeführt.

Meta Data
URL zu dem Metadatenexport vom AD FS
Open ID Config
Dieser kann unter den Endpoints in der AD FS Admin Konsole auf dem Server nachgesehen werden. Er setzt sich aber aus dem «Hostname» und «/adfs/.well-known/openid-configuration» zusammen.



Valid Issuer
Dieser Parameter kann mittels Powershell ermittelt werden:
'Get-ADFSProperties' anschliessend ist dieser als «Identifier» Property aufgeführt.

```
PS C:\Windows\system32> Get-AdfsProperties | Select Hostname, Identifier, IdTokenIssuer | Format-List


HostName      : adfs.gemdat.ch
Identifier    : http://adfs.gemdat.ch/adfs/services/trust
IdTokenIssuer : https://adfs.gemdat.ch/adfs
```

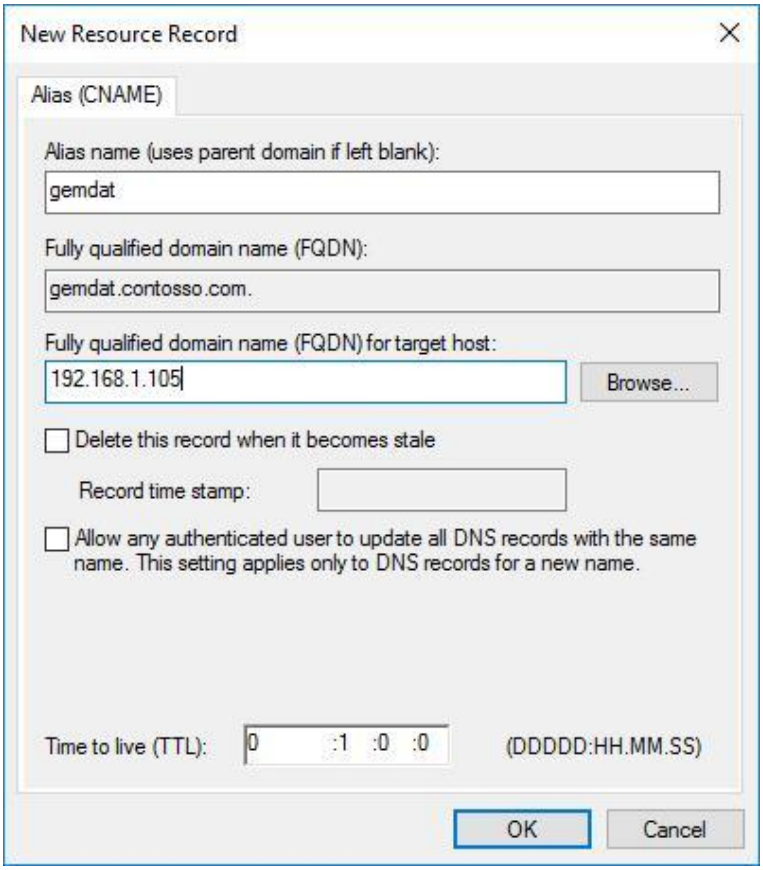
'Get-AdfsProperties | Select Hostname, Identifier, IdTokenIssuer | Format-List'

6 DNS Konfiguration

6.1 Beschreibung

«gemdat bau» bzw. «gemdat bau»-Test werden über definierte URLs aufgerufen. Hierzu muss für jede Anwendung ein entsprechender DNS Eintrag erstellt werden.

Beispiel:	Produktiv
Aufruf:	https://gemdat.contoso.com/bau
DNS Eintrag:	



Hinweis:
Bei der Verwendung von HTTPS muss der DNS-Eintrag mit dem verwendeten Zertifikat übereinstimmen!

7 Client Vorbereitung

7.1 Beschreibung

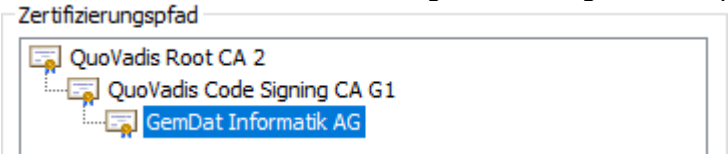
«gemdat bau» benötigt das Microsoft Silverlight Plugin Version 5. Im Zusammenhang mit dem Erstellen und Bearbeiten von Dokumenten direkt aus «gemdat bau» werden ausserdem ein Anwendungszertifikat und ein zusätzlicher Registrierungseintrag benötigt. Zusätzlich muss gewährleistet sein, dass die aufgerufene URL zur Zone der Vertrauenswürdigen Sites gehört.

7.2 Installation Silverlight

Auf der Website von Microsoft kann die aktuelle Silverlight-Version nicht mehr heruntergeladen werden. Diese kann neu über den Gemdat-Helpdesk bezogen und auf den Clients installiert werden.

7.3 Import Zertifikat

Das von Gemdat AG zur Verfügung gestellte Zertifikat muss auf allen «gemdat bau»-Clients zu den vertrauenswürdigen Herausgebern importiert werden.



https://fileservice.gemdat.ch/index.php/s/mxDbsAtrWepdY5G

7.4 Erstellung Registrierungseintrag

Direkt in der Registrierung des Clients oder mittels Gruppenrichtlinien folgende Registrierungseinträge erstellen:
Pfad:

- 32-Bit Betriebssystem:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Silverlight
- 64-Bit Betriebssystem:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Silverlight

Werte:

- DWORD-Eintrag: AllowElevatedTrustAppsInBrowser mit dem Wert 1
- DWORD-Eintrag: AllowLaunchOfElevatedTrustApps mit dem Wert 1

7.5 Sicherheitszone Vertrauenswürdige Sites

Mittels Gruppenrichtlinien oder direkt in den Internetoptionen auf dem Client Betriebssystem muss dafür gesorgt werden, dass die URL (für «gemdat cloud» Kunden: *.gemdat.cloud) zur Zone der Vertrauenswürdigen Sites gehört.

Zusätzlich zur Gemdat-URL muss auch die folgende Seite in die vertrauenswürdigen Sites des Internet Explorers aufgenommen werden:
https://login.microsoftonline.com. Dies damit die sichere Authentifizierung über OAuth2 gemacht werden kann.

Pfad für die Gruppenrichtlinienkonfiguration:
User Configuration/Policies/Windows Components/Internet Explorer/Internet Control Panel/Security Page/Trusted Sites Zone

Der "Geschützte Modus" in den Internetoptionen für die Zone "Trusted Sites" / "Vertrauenswürdige Sites" darf nicht aktiviert sein.

8 Microsoft Edge-Kompatibilität

8.1 Voraussetzungen

Voraussetzung ist, dass eine Version des Edge gemäss technischer Voraussetzung installiert ist. Ebenfalls müssen die in den obigen Kapiteln 7.1-7.5 beschriebenen Einrichtungen erledigt sein.

8.2 Download und Installation Policy Template

Unter folgendem Link kann mit der Angabe von Version, Build und Plattform das Policy Template heruntergeladen werden. Link: https://docs.microsoft.com/en-us/deployedge/edge-ie-mode-policies

Im extrahierten Verzeichnis wählt man unter Windows die beiden msedge.admx und msedgeupdate.admx Dateien und das entsprechende Sprachenverzeichnis aus. Diese werden dann in die Policy Definitions kopiert, welche sich meistens im Sysvol Verzeichnis des DC befinden.

8.3 Policy erstellen

Nun wird eine Policy erstellt unter Computer Configuration -> Policies -> Administrative Templates: Policy definitions (ADMX files) retrieved from the central store -> Microsoft Edge. Hier werden folgende beiden Settings eingeschalten:
— Configure Internet Explorer integration: Wert auf Internet Explorer mode (1) stellen
— Configure the Enterprise Mode Site List: UNC Pfad zur XML mit den URL's
— Specify how «in-page» navigations to unconfigured sites behave when started from Internet Explorer mode pages: enabled – Keep only automatic navigations in Interne Explorer mode

Die Policy auf die entsprechenden OU's anwenden.

8.4 Enterprise Sites XML einrichten oder ergänzen

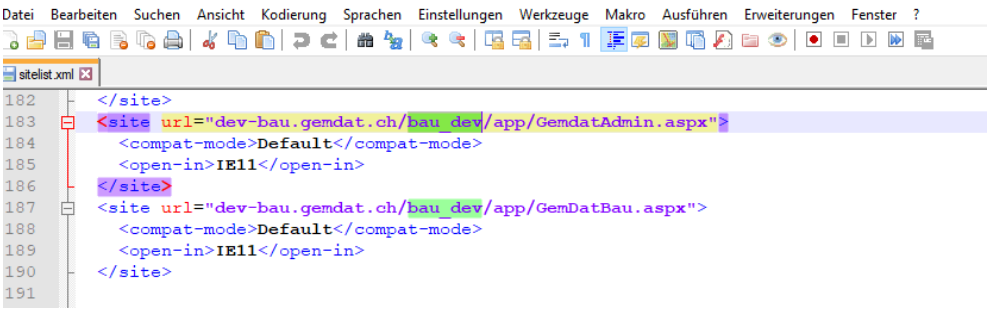
Damit ab v7.0.0 sowohl der neu entwickelte HTML5-, als auch die bisherigen Silverlight-Clients in MS Edge geöffnet werden können, muss die Konfiguration für die Ausführung im IE-Mode für die jeweilige Applikation angepasst werden. Nur die bisherigen Silverlight Clients müssen weiterhin im IE-Mode ausgeführt werden:

Im MS Edge aufrufen: edge://compat/enterprise

- Unternehmensmodus-Websitenliste und Standort zur sitelist.xml aufrufen

- Eintrag mit Url auf Root-Verzeichnis entfernen
  (z.B. Eintrag mit Url «dev.bau.gemdat.ch/bau-dev»)

- Separate Einträge für die alten Silverlight-Einträge erfassen (Beispiel für gemdat bau und gemdat admin):



Sollten Sie «gemdat bau» selbst betreiben, so muss im Tag die URL zu Ihrer «gemdat bau» Umgebung stehen. Ergänzungen dazu: https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/add-multiple-sites-to-enterprise-mode-site-list-using-the-version-2-schema-and-enterprise-mode-tool

Das XML File wird sodann in einem Share abgelegt, damit die Liste von den Browsern auf den Clients eingesehen werden kann. Der Pfad zu dieser Liste wird im Punkt 3 Policy erstellen als UNC Pfad bei dem Setting Configure the Enterprise Mode Site List eingetragen.

Eine umfassende Microsoft Anleitung zu diesem Thema ist unter folgendem Link zu finden: https://docs.microsoft.com/en-us/deployedge/edge-ie-mode-policies

8.5 Einstellung für Kunden mit Autorisierung «Microsoft Entra ID»

Damit die Authentifizierung funktioniert, muss die folgende Seite in die vertrauenswürdigen Sites des Internet Explorers aufgenommen werden, damit sowohl die «gemdat bau» Webseite wie auch das Loginverfahren die Token untereinander austauschen können:
https://login.microsoftonline.com/

9 Anhang A: Checkliste

- ☐ Server
  - ☐ IIS Rolle mit zugehörigen Rollendiensten und Features installiert
  - ☐ SQL-Server mit gewünschten Features installiert
  - ☐ Datenbank ist erstellt
- ☐ Active Directory
  - ☐ Anmeldeberechtigung des Dienstbenutzers konfiguriert
- ☐ Entra ID/AD FS Konfiguration
  - ☐ Sicherheitsgruppen erstellt
  - ☐ Testbenutzer erstellt
  - ☐ App Registrations erstellt
  - ☐ Token konfiguriert
  - ☐ Konfiguration WebDav erstellt
- ☐ DNS Konfiguration
  - ☐ DNS Einträge erstellt
- ☐ Clients
  - ☐ Silverlight installiert
  - ☐ Zertifikat importiert
  - ☐ Zonenkonfiguration in den Internetoptionen erstellt
  - ☐ Registrierungseinträge erstellt / kontrolliert

10 Anhang B: Infoblatt Entra ID

(Kopie an Gemdat AG)

Umgebung:

	Produktivsystem:	Testsystem:
Name:	……	……

SQL-Server Infos:

	Produktivsystem:	Testsystem:
SQL-Server Host Name:	……	……
SQL-Server Edition/Version:	……	……
SQL-Instanz Name:	……	……
SQL-Datenbank Name:	……	……

Applikationsserver (IIS) Infos:

	Produktivsystem:	Testsystem:
Servername:	……	……
Site-URL:	……	……
IIS-Webseiten HTTP/HTTPS (Port):	(80/443)……	(80/443)……
HTTPS Zertifikat vorhanden?	……	……

Active Directory

Benutzername Dienstbenutzer: ……

Microsoft Entra ID:

Tenant ID: ……

Client ID: ……

Audience: ……

Authority: ……

Open ID Config: ……

Valid Issuer: ……

Sicherheitsgruppe Administratoren UUID: ……

Benutzername Testuser (optional): ……

Dokumentenhandling:

Filesystem Verzeichnis: .....

Vorlagen Verzeichnis: .....

Temporäres Dokumentenverzeichnis: .....

11 Anhang C: Infoblatt AD FS

(Kopie an Gemdat AG)

Umgebung:

	Produktivsystem:	Testsystem:
Name:	……	……

SQL-Server Infos:

	Produktivsystem:	Testsystem:
SQL-Server Host Name:	……	……
SQL-Server Edition/Version:	……	……
SQL-Instanz Name:	……	……
SQL-Datenbank Name:	……	……

Applikationsserver (IIS) Infos:

	Produktivsystem:	Testsystem:
Servername:	……	……
Site-URL:	……	……
IIS-Webseiten HTTP/HTTPS (Port):	(80/443) ……	(80/443) ……
HTTPS Zertifikat vorhanden?	……	……

Active Directory

Benutzername Dienstbenutzer: ……

AD FS:

Client ID: ……

Audience: ……

Authority: ……

Open ID Config: ……

Valid Issuer: ……

Sicherheitsgruppe Administratoren Name: ……

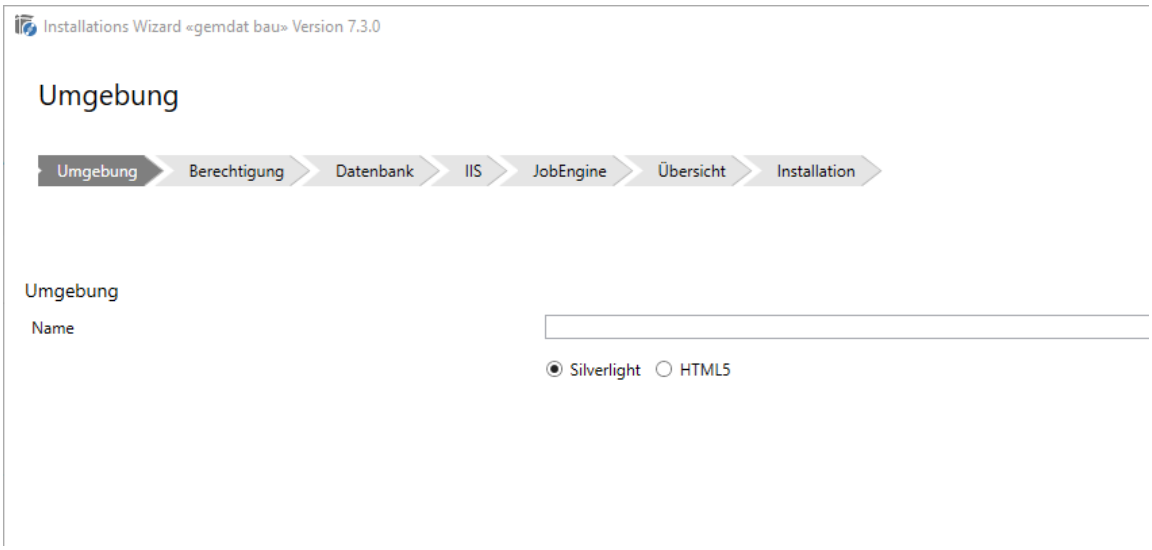
Benutzername Testuser (optional): ……

12 Anhang D: Update von früheren Versionen

Beim Update von älteren Versionen von «gemdat bau» muss folgendes beachtet werden.

12.1 Installations-Wizzard

Mit der Version 7.3.0 steht «gemdat bau» als HTML5 Version für Neuinstallationen zur Verfügung. **Für Updates von bestehenden Umgebungen muss im Installationswizard zwingend Silverlight ausgewählt werden.**



12.2 Technische Anpassungen

Ab Version 7.0:

- IIS Feature: Urlrewrite 2.1 muss installiert sein
- IIS Performance Feature «dynamic content compression» muss deaktiviert oder deinstalliert sein
- IIS Performance Feature «static content compression» muss deaktiviert oder deinstalliert sein

Ab Version 7.2:

- «Visual C++ 2013 Redistributable Package» wird nicht mehr benötigt und kann deinstalliert werden

12.3 Skript einspielen

Wird ein Update auf 7.3 von einer Version <7.2 ausgeführt und dabei das Login-Verfahren auf AD FS oder EntraID umgestellt, muss mit Gemdat geprüft werden, ob nach dem Update das Skript '115400_Change_Prefix_and_Suffix_In_UserName_Fields.sql' auf der Datenbank ausgeführt werden soll oder nicht. Damit können die alten Benutzernamen auf die neuen Benutzernamen umgestellt werden, damit userspezifische Einstellungen wie Verlauf, GWR-Login, persönliche Auswertungen nicht verloren gehen.

Zusätzlich muss ein Skript vor dem Update ausgeführt werden, damit das Update fehlerfrei durchläuft (Applicationhost URL).

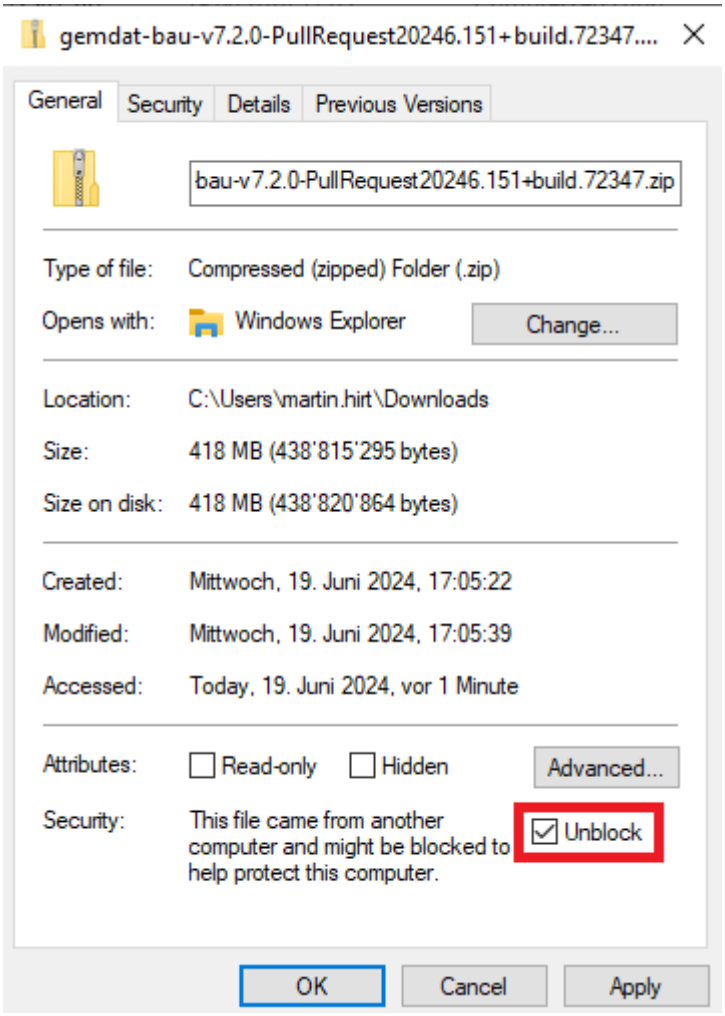
Bitte kontaktieren Sie den Gemdat-Support, damit die nötigen Abklärungen sowie Einstellungen im Skript korrekt vorgenommen werden können.

12.4 Lizenz 7.3 einspielen

Ab der Version 7.3 muss neu die neue Lizenz zwingend immer eingespielt werden bei einem Update.

13 Anhang E: Hinweis zum Setup ausführen

Die Setup-Dateien befinden sich in der Containerdatei (Beispiel: gemdat-bau-v7.2.0+30812.zip) und müssen zuerst entpackt werden. Beim Entpacken muss darauf geachtet werden, dass das Attribut 'Unblock' angekreuzt ist:



Anschliessend die Setup.exe ausführen und eine neue «gemdat bau»-Installation starten. Im Installationswizard müssen die Angaben gemäss diesem Dokument parametrisiert werden.

Beim Update ab 7.2 müssen die Angaben zu Entra ID oder ADFS im Installationswizzard gemäss diesem Dokument parametrisiert werden.