

Vorbereitung Installation «gemdat bau» für HTML5- Installationen

Rollenverzeichnis

Rolle	Mitarbeiter
Dokumentenverantwortlicher	Gemdat
Reviewzirkel	Gemdat
Zielgruppe	IT Gemdat

Änderungsverzeichnis

Datum	Änderungen	Version	Person
31.07.2025	Ergänzung Kap 7.2 bzgl. Popup	1.1	Tanja Muñoz
28.03.2025	Neuerstellung Dokument für HTML5	1.0	Tanja Muñoz

Zweck des Dokuments

Dieses Dokument beschreibt die Vorbereitungsarbeiten für die Installation von «gemdat bau» in der Cloud. **Die HTML5-Installation für die Version 7.3 ist nur für der Einsatz in der Gemdat-Cloud freigegeben.**

Inhalt

1	Allgemeines	4
1.1	Ziele	4
1.2	Informationen	4
1.3	Anhang	4
2	Installation Webserver-Rolle	5
2.1	Beschreibung	5
2.2	Installation .NET	5
2.3	IIS Rollen	6
2.4	Betrieb über HTTPS	7
2.5	Bei Verwendung «gemdat archiv»: Verteiltes Transaction-Handling aktivieren	7
3	Einrichtung SQL-Server	7
3.1	Beschreibung	7
3.2	Kompatibilität zu Gemdat/5	8
4	Einrichten ActiveDirectory	9
4.1	Beschreibung	9
4.2	Anmeldeberechtigungen für den Dienstbenutzer vergeben	9
4.3	E-Mail-Feld bei Benutzern mit «gemdat archiv» oder «gemdat sign»	9
5	Konfiguration der Autorisierungs-Instanzen	10
5.1	Konfiguration «Microsoft Entra ID»	10
5.1.1	Konfiguration Backend App Registration	10
5.1.2	Konfiguration Frontend- App	12
5.1.3	Einrichtung der Sicherheitsgruppen und Benutzer	13
5.2	Konfiguration «gemdat bau»	14
5.2.1	Microsoft Entra ID	14
6	DNS Konfiguration	15
6.1	Beschreibung	15
7	Client Vorbereitung	16
7.1	Sicherheitszone Vertrauenswürdige Sites	16

8	Anhang A: Checkliste	17
9	Anhang B: Infoblatt Entra ID	18
10	Anhang D: Update von früheren Versionen	20
11	Anhang E: Hinweis zum Setup ausführen	20

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.

Hinweis: Die HTML5-Installation für die Version 7.3 ist nur für der Einsatz in der Gemdat-Cloud freigegeben.

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

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-WindowsFeature -Name Web*, Net* | where Installed

Display Name                                         Name                                Install State
-----
[X] Web Server (IIS)                                Web-Server                         Installed
[X] Web Server                                       Web-WebServer                     Installed
[X] Web Server                                       Web-Common-Http                   Installed
[X] Common HTTP Features                            Web-Default-Doc                   Installed
[X] Default Document                                Web-Dir-Browsing                  Installed
[X] Directory Browsing                               Web-Http-Errors                   Installed
[X] HTTP Errors                                       Web-Static-Content                Installed
[X] Static Content                                   Web-Http-Redirect                 Installed
[X] HTTP Redirection                                 Web-Health                        Installed
[X] Health and Diagnostics                           Web-Http-Logging                  Installed
[X] HTTP Logging                                       Web-Log-Libraries                 Installed
[X] Logging Tools                                     Web-Request-Monitor              Installed
[X] Request Monitor                                  Web-Security                      Installed
[X] Security                                           Web-Filtering                    Installed
[X] Application Development                           Web-App-Dev                       Installed
[X] .NET Extensibility 4.8                             Web-Net-Ext45                    Installed
[X] Application Initialization                       Web-AppInit                      Installed
[X] ASP                                                Web-ASP                           Installed
[X] ASP.NET 4.8                                       Web-Asp-Net45                    Installed
[X] CGI                                                Web-CGI                           Installed
[X] ISAPI Extensions                                Web-ISAPI-Ext                    Installed
[X] ISAPI Filters                                    Web-ISAPI-Filter                 Installed
[X] WebSocket Protocol                               Web-WebSockets                   Installed
[X] Management Tools                                 Web-Mgmt-Tools                   Installed
[X] IIS Management Console                           Web-Mgmt-Console                 Installed
[X] .NET Framework 4.8 Features                       NET-Framework-45-Fea...          Installed
[X] .NET Framework 4.8                               NET-Framework-45-Core            Installed
[X] ASP.NET 4.8                                       NET-Framework-45-ASPNET          Installed
[X] WCF Services                                     NET-WCF-Services45              Installed
[X] HTTP Activation                                  NET-WCF-HTTP-Activat...          Installed
[X] Message Queuing (MSMQ) Activation                 NET-WCF-MSMQ-Activat...          Installed
[X] Named Pipe Activation                             NET-WCF-Pipe-Activat...          Installed
[X] TCP Activation                                    NET-WCF-TCP-Activati...          Installed
[X] TCP Port Sharing                                 NET-WCF-TCP-PortShar...          Installed

PS C:\WINDOWS\system32>
```

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 → Distributed 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

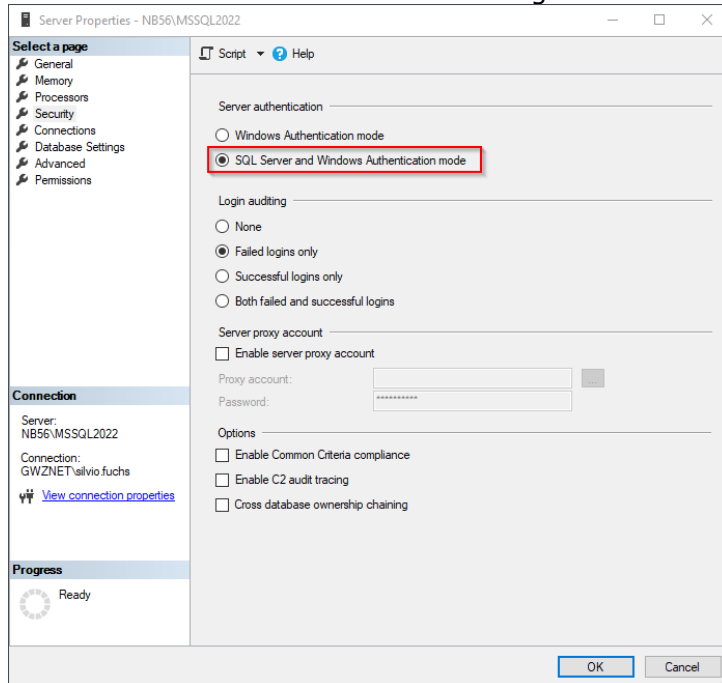
Als Datenbank-Server wird Microsoft SQL in englischer Standardsprache vorausgesetzt. Gemdat empfiehlt die Installation einer Test- und Produktiv-Datenbank. Die beiden Datenbanken können wahlweise auf unterschiedlichen Instanzen oder Servern betrieben werden.

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 für die HTML5 Installationen mit 7.3 «Microsoft Entra ID» 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.

Die Benutzer Authentifizierung erfolgt für die WebClients im Frontend nach dem «OAuth 2.0 authorization code grant» flow. Die Benutzer Authentifizierung innerhalb Office für die Dokumentenbearbeitung erfolgt nach dem «OAuth 2.0 client credentials flow».

5.1 Konfiguration «Microsoft Entra ID»

Für «gemdat bau» müssen in Microsoft Entra ID zwei App Registrations 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 «Authentifizierung»

Registration der Backend Als «Web Plattform» für den «OAuth 2.0 client credentials flow» mit folgenden Optionen:

Web-Plattform:

- Redirect Uri: <https://{site-name}/api/document-management/webdav/success>

Tokenausgabe (Implizite Genehmigungen):

- Zugriffstoken
- ID-Token

Unterstützte Kontotypen:

- Nur Konten in diesem Organisationsverzeichnis

Tab «Zertifikate & Geheimnisse»

Für die Dokumentenbearbeitung via WebDav ist das Bau Backend als «ConfidentialClient» registriert, welches für die Authentifizierung einen «Clientschlüssel» benötigt.

«Clientschlüssel» haben zwingend ein Ablaufdatum. Die maximale Gültigkeit ist entsprechend der vorhandenen IT-Richtlinien zu wählen. **Zudem muss das Ablaufdatum aktiv überwacht werden**, um den «Clientschlüssel» vor Ablauf der Frist rechtzeitig zu

erneuern. Nach Ablauf des Clientschlüssels funktioniert die Dokumentenbearbeitung in gemdat-bau nicht mehr.

Im Bereich „Zertifikate und Geheimnisse“ muss ein geheimer «Clientschlüssel» hinzugefügt werden:

✖ Diagnose und Problembehandlung

Verwalten

- Branding und Eigenschaften
- Authentifizierung
- Zertifikate & Geheimnisse**
- Tokenkonfiguration
- API-Berechtigungen
- Eine API verfügbar machen
- App-Rollen

Anwendungsregistrierungszertifikate, Geheimnisse und Verbundanmeldeinformationen finden Sie auf den Registerkarten unten.

Zertifikate (0) **Geheime Clientschlüssel (1)** Verbundanmeldeinformationen (0)

Eine geheime Zeichenfolge, die von der Anwendung beim Anfordern eines Tokens als Identitätsnachweis verwendet wird. Wird auch als Anwendungskennwort bezeichnet.

+ Neuer geheimer Clientschlüssel

Beschreibung	Gültig bis	Wert	Geheime ID
WebDav	22.8.2026	u2Y*****	22bdcfe6-93eb-4705-b1fe-750305b401d3

Tab «Tokenkonfiguration»

Es sind folgende optionalen Ansprüche zu konfigurieren:

Anspruch	Beschreibung	Token typ	Optionale Einstellungen
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	ID	-
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	Zugriff	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	ID	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	Zugriff	-
groups	Optionale Formatierung für Gruppenansprüche	ID, Zugriff, SAML	Ja
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	ID	Ja
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	Zugriff	Ja

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:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Gemdat AG Dev

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (3)				...
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for Gemdat AG ...
openid	Delegated	Sign users in	No	✓ Granted for Gemdat AG ...
profile	Delegated	View users' basic profile	No	✓ Granted for Gemdat AG ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

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:

Bereiche	Zum Einwilligen ber...	Anzeigename der Admi...	Anzeigename der Benu...	Zustand
api://1ef29763-a081-4713-815f-92593b443ff5/Bau.All	 Nur Administratoren	Bau Alle Berechtigungen	Bau Alle Berechtigungen	Aktiviert

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» für den «OAuth 2.0 authorization code grant flow» 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:

Wählen Sie die Token aus, die vom Autorisierungsendpunkt ausgegeben werden sollen:

- ☐ Zugriffstoken (werden für implizite Flows verwendet)
- ☐ ID-Token (werden für implizite und Hybridflows verwendet)

Tab «Tokenkonfiguration»

Es sind folgende optionalen Ansprüche (Claims) hinzuzufügen.

Anspruch ↑	Beschreibung	Token typ ↑↓	Optionale Einstellungen
family_name	Gibt den Nachnamen oder Familiennamen des Benutzers gemäß Definition im Benutzerobjekt an.	ID	-
given_name	Gibt den Vornamen des Benutzers gemäß Festlegung im Benutzerobjekt an.	ID	-
upn	Ein Bezeichner für den Benutzer, der mit dem username_hint-Parameter verwendet werden kann. Es handelt sich nicht um einen dauerhaften...	ID	Ja

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:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Gemdat AG Dev

API / Permissions name	Type	Description	Admin consent req...	Status
▼ gemdat bau ent dev-backend (1) ...				
Bau.All	Delegated	Bau Alle Berechtigungen	Yes	✓ Granted for Gemdat AG ...
▼ Microsoft Graph (3) ...				
offline_access	Delegated	Maintain access to data you have given it access to	No	✓ Granted for Gemdat AG ...
openid	Delegated	Sign users in	No	✓ Granted for Gemdat AG ...
profile	Delegated	View users' basic profile	No	✓ Granted for Gemdat AG ...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

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 «gemdat bau»

5.2.1 Microsoft Entra ID

Benutzer Authentifizierung Web Client

Parameter	Wert
TenantId	TenantId von Microsoft Entra Id
ClientId	ClientId der Frontend App-Registrierung
Authority	https://login.microsoftonline.com
Audience	api://{clientId Backend}
OpenIdConfig	https://login.microsoftonline.com/organizations/v2.0/.well-known/openid-configuration
ValidIssuer	https://sts.windows.net/{tenantId}/

Benutzer Authentifizierung Dokumentenbearbeitung

Parameter	Wert
TenantId	TenantId von Microsoft Entra Id
ClientId	ClientId der Backend App-Registrierung
Authority	https://login.microsoftonline.com
Audience	ClientId der Backend App-Registrierung
OpenIdConfig	https://login.microsoftonline.com/organizations/v2.0/.well-known/openid-configuration
ValidIssuer	https://login.microsoftonline.com/{tenantId}/v2.0 https://sts.windows.net/{tenantId}/
RedirectUri	https://{bau-site}/api/document-management/webdav/success
ClientSecret	Client Secret aus Azure App Registrierung

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:

New Resource Record

Alias (CNAME)

Alias name (uses parent domain if left blank):
gemdat

Fully qualified domain name (FQDN):
gemdat.contoso.com.

Fully qualified domain name (FQDN) for target host:
192.168.1.105 Browse...

☐ Delete this record when it becomes stale

Record time stamp:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

OK Cancel

Hinweis:

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

7 Client Vorbereitung

7.1 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:

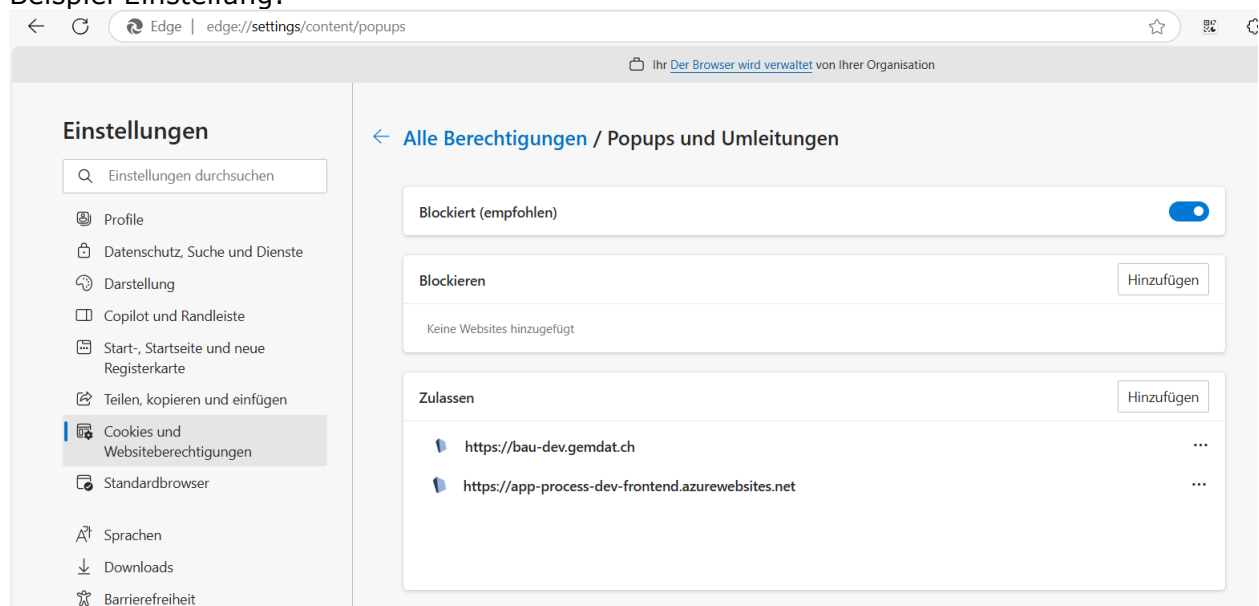
User Configuration/Policies/Windows Components/Internet Explorer/Internet Control Panel/Security Page/Trusted Sites Zone

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

7.2 Popup erlauben

Damit ein Re-Login in der Prozessablauf-App vorgenommen werden kann, müssen für die URL von «gemdat bau» und die Basis URL des Prozessablaufs Popups zugelassen werden.

Beispiel Einstellung:



8 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 Konfiguration
 - ☐ Sicherheitsgruppen erstellt
 - ☐ Testbenutzer erstellt
 - ☐ App Registrations erstellt
 - ☐ Token konfiguriert
 - ☐ Konfiguration WebDav erstellt
- ☐ DNS Konfiguration
 - ☐ DNS Einträge erstellt
- ☐ Clients
 - ☐ Zonenkonfiguration in den Internetoptionen erstellt

9 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 (frontend):
Audience:
Authority:
Open ID Config:
Valid Issuer:
Sicherheitsgruppe Administratoren UUID:
Benutzername Testuser (optional):

Dokumentenablage für Schnittstellen und Vorlagen:

Filesystem Verzeichnis:

Vorlagen Verzeichnis:

Temporäres Dokumentenverzeichnis:

Dokumentenhandling WebDav (HTML5):

Redirect Uri:

Tenant ID (wenn abweichend):

Client ID (Backend):

Audience (wenn abweichend):

Authority (wenn abweichend):

Open ID Config (wenn abweichend):

Valid Issuer (muss V1 und V2 hinterlegt werden):

Prozessablauf (HTML5):

Basis URL:

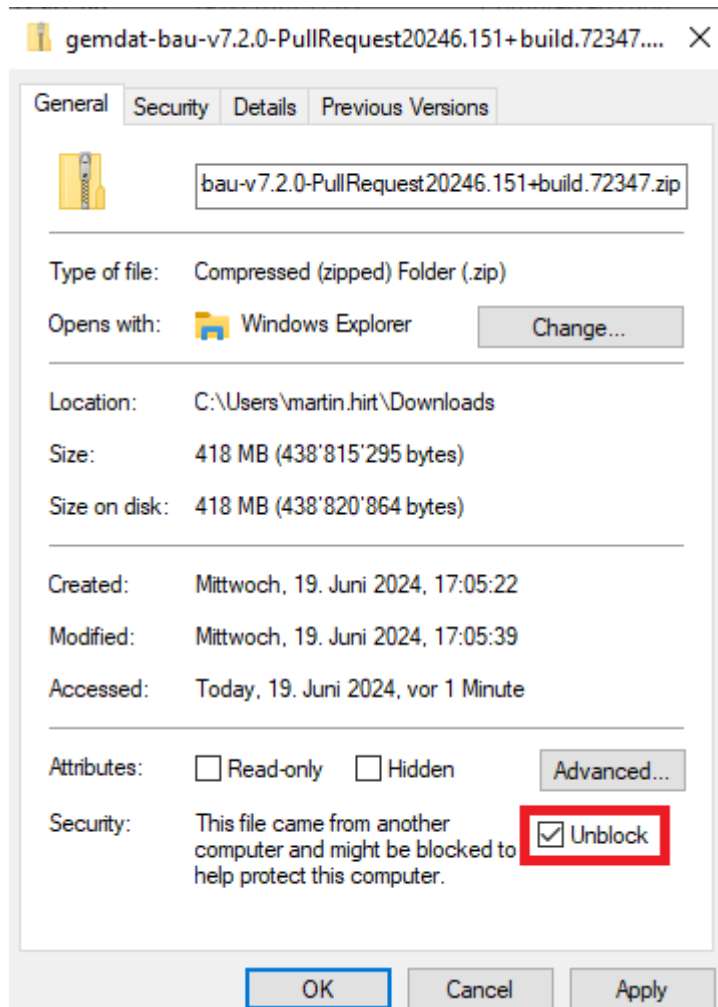
Kundeninstanz Identifikation:

10 Anhang D: Update von früheren Versionen

Mit der Version 7.3.0 steht «gemdat bau» als HTML5 Version für Neuinstallationen zur Verfügung. **Für Updates von bestehenden Umgebungen steht die Version in HTML5 noch nicht zur Verfügung.**

11 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.