GAPTEQ-FEATURES KURZ ERKLÄRT

Single-Sign-On für GAPTEQ-Applikationen im internen Netzwerk (Intranet) mit der Integrierten Windows-Authentifizierung für AD-User umsetzen

Ein Single-Sign-On (SSO) für interne Websites und Applikationen im Intranet erhöhen den Benutzerkomfort erheblich. Um das Anmelden an einer GAPTEQ-Applikation im internen Netzwerk ohne erneute Eingabe von Username und Passwort zu ermöglichen, unterstützt GAPTEQ in der BUSINESS-Version die Nutzung der Integrierten Windows-Authentifizierung.

VORTEILE & VORAUSSETZUNGEN

- Anmelden an der GAPTEQ-Applikation ohne Eingabe von Username und Passwort.
- GAPTEQ-Server für den Betrieb mit einem Active Directory User konfiguriert (siehe Feature Tipp zum Microsoft Active Directory).
- Betrieb im internen Netzwerk mit dem Microsoft Active Directory (AD).
- Anbindung eines Azure Active Directory mit Hilfe der Azure Active Directory Domain Services.
- Login nur noch für Active Directory User möglich (lokale GAPTEQ-User können sich in dieser Konfiguration nicht mehr anmelden).
- AD-User benötigt Leserechte für das Verzeichnis GAPTEQ Web

SO GEHT'S SCHRITT FÜR SCHRITT

Mit Hilfe der Integrierten Windows-Authentifizierung werden die Anmeldedaten des lokalen GAPTEQ-Benutzers an die internen Websites des IIS-Webservers weitergereicht. Während Internet Explorer, Edge, Chrome und Opera die Integrierte Windows-Authentifizierung automatisch per Voreinstellung unterstützen, muss die Funktionalität für den Firefox erst aktiviert werden.

So gehen Sie beim Anlegen des SSO mit Hilfe der Integrierten Windows-Authentifizierung vor:

1. Integrierte Windows-Authentifizierung im IIS Webserver aktivieren.
2. Integrierte Windows-Authentifizierung in GAPTEQ aktivieren.
3. Optional: Windows-Authentifizierung in Firefox aktivieren.

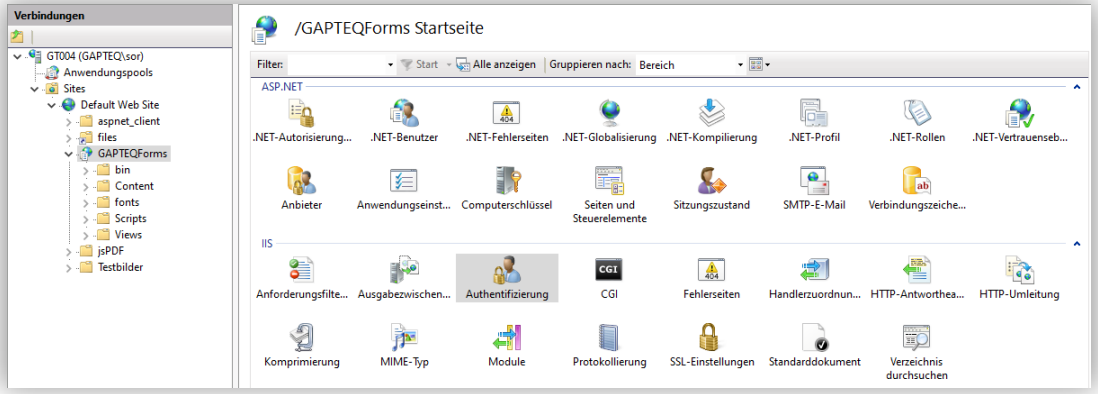
Die Anmeldung am Repository im GAPTEQ-Designer ist von der Anwendung der Integrierten Windows-Authentifizierung nicht betroffen und funktioniert weiterhin mit direkter Eingabe von Username und Passwort.

Dateirechte GAPTEQ Web

Nach der Installation von GAPTEQ Web müssen AD-User auf diesen Ordner lesend zugreifen können (C:\Program Files (x86)\GAPTEQ\GAPTEQ Web 3.x).
Bitte berechtigen Sie nach der Installation und nach einem Upgrade Ihre AD-User für lesenden Zugriff auf den GAPTEQ Web Ordner und enthaltene Dateien.

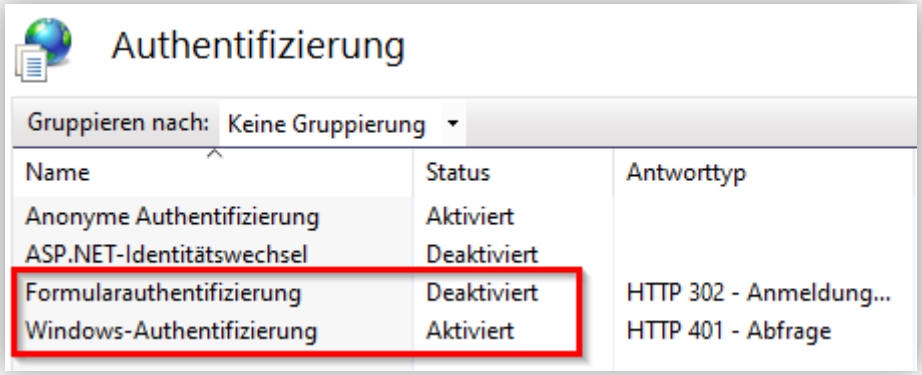
1. Windows-Authentifizierung im IIS Webserver aktivieren

Im IIS Manager bei Sites -> Default Web Site -> GAPTEQForms im Bereich IIS-Authentifizierung wählen.



Anonyme Authentifizierung muss aktiviert bleiben, um öffentliche Seiten, die keine Anmeldung erfordern, auszuliefern.

Windows-Authentifizierung wird aktiviert, alle **anderen Methoden** bis auf die Anonyme Authentifizierung müssen deaktiviert werden.



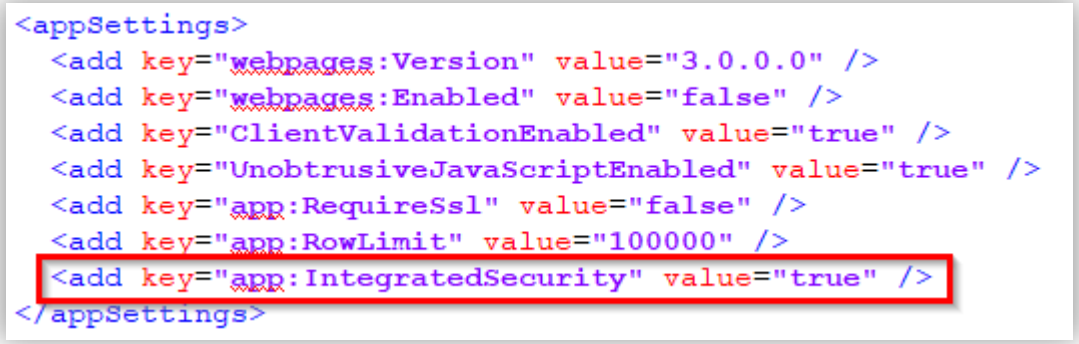
2. Windows-Authentifizierung in GAPTEQ aktivieren

Web.config Datei mit Texteditor zur Bearbeitung öffnen:

C:\Program Files (x86)\GAPTEQ\GAPTEQ Web 3.x\Web.config

Bei appSettings IntegratedSecurity von flase auf true ändern.

<add key="app:IntegratedSecurity" value="true" />



3. Windows-Authentifizierung im Firefox aktivieren

Ein pauschales Freischalten für SSO ist in Firefox nicht vorgesehen. Alle Hosts, die für SSO erlaubt werden sollen, müssen einzeln angegeben werden.

Dies lässt sich in der Browser-Konfiguration oder über Gruppenrichtlinien erledigen.
Für eine Konfiguration über Gruppenrichtlinie kontaktieren Sie bitte ihren System Administrator.

Feature aktivieren im Firefox Browser

In der Adresszeile des Firefox Browsers folgenden Befehl eingeben:

about:config

Nach Bestätigung des Risikohinweises öffnet sich die Konfigurationsseite. Hier suchen Sie nach network.automatic und wählen in der Trefferliste:

network.automatic-ntlm-auth.trusted-uris

In dem Eingabefeld werden die Host-Namen angegeben. Mehrere Hosts werden mit Komma getrennt.