



Version 5.10

FFAuth: Einheitliches Login für
FORCAM FORCE™
Handbuch

Dokument: **Handbuch - FFAuth.docx**

Erstellt: **02.05.19**

Letzte Änderung: **30.09.19**

Autor: **AEgilmez**



Inhaltsverzeichnis

1	Konzept	3
1.1	Hintergrund	4
1.2	Zeitüberschreitung (Timeout)	5
2	Wechsel zwischen Workbench und Office	6
2.1	URL in einer Kachel.....	7
2.2	URL in Systemkonfigurationen.....	7
3	Sicherheitszertifikat (HTTPS).....	8

1 Konzept

FFAuth ist die Single Sign-on-Lösung von FORCAM FORCE™. Dabei kann sich der Benutzer über eines der beiden Module Workbench oder Office anmelden und wird automatisch auf dem anderen Modul ebenfalls angemeldet, ohne die Benutzerdaten erneut angeben zu müssen. Die Anmeldung wird von FFAuth übernommen.

Ziel ist es, dem Benutzer das Gefühl zu geben, durch eine einzige Anwendung zu navigieren. Der Haupteinstiegspunkt ist die Workbench mit ihrer Kachel-Navigation. Durch eine Kachel gelangt der Benutzer direkt in das Office-Modul und per Umleitung (Redirect) wieder zurück in die Workbench.

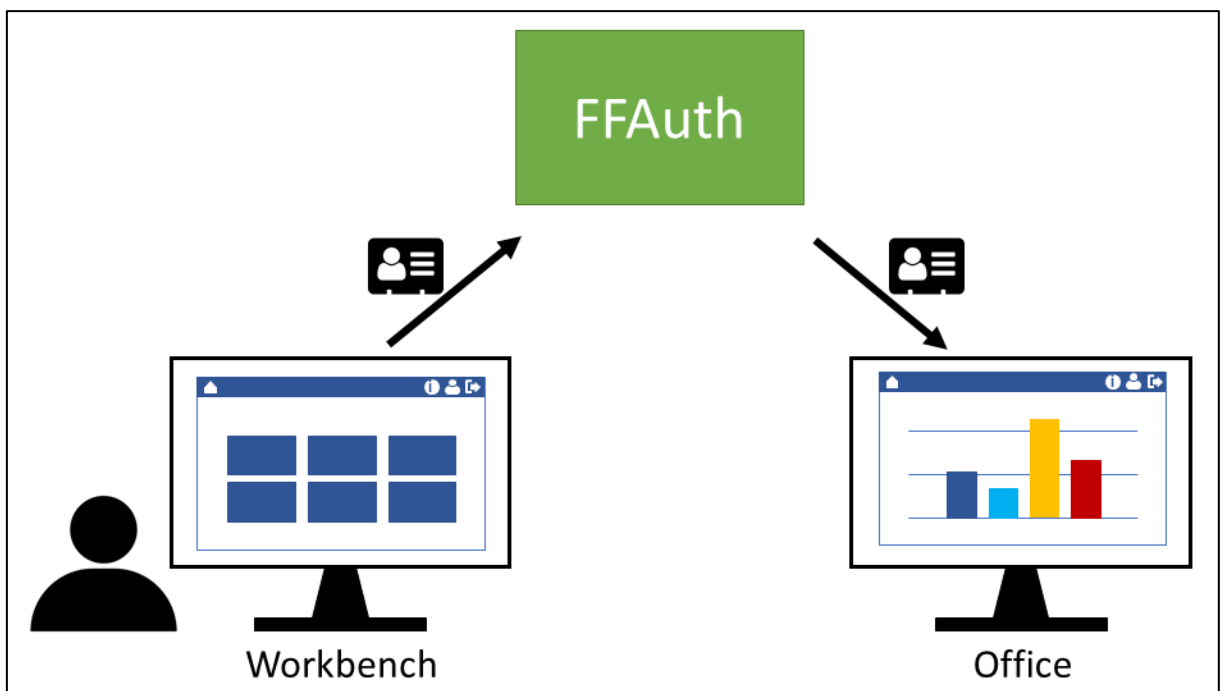


Bild 1: Übertragung von Anmeldeinformationen über FFAuth

FFAuth ist ein Service, der Anmeldeinformationen zentral verwaltet. Meldet sich der Benutzer beispielsweise über die Workbench an, wird er zunächst zentral bei FFAuth angemeldet. Die Informationen werden dann an die Workbench übertragen. Ruft der Benutzer dann das Office auf, werden die Informationen übertragen und der Benutzer wird automatisch angemeldet. Die Informationen umfassen Anmeldedaten- und Status des Benutzers. Die Spracheinstellungen werden ebenfalls übertragen, der Austausch findet jedoch zwischen den Modulen direkt statt. Meldet sich der Benutzer über eines der Module ab, wird er im anderen ebenfalls abgemeldet.

 Um FFAuth nutzen zu können, müssen Cookies im verwendeten Browser akzeptiert werden.

Konzept

Der Anmeldebildschirm der Module unterscheidet sich optisch geringfügig bei der Verwendung von FFAuth.

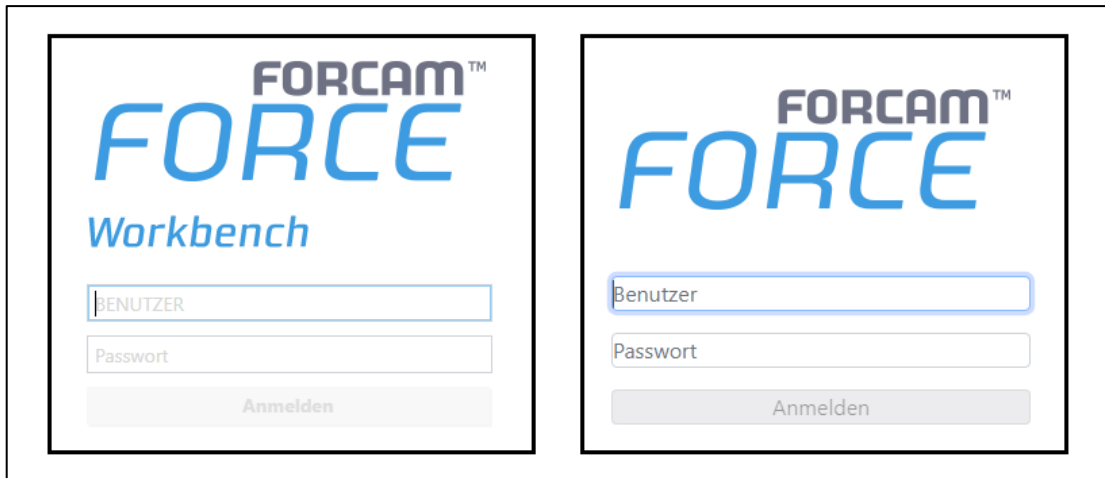



Bild 2: Workbench-Anmeldebildschirm ohne (links) und mit (rechts) FFAuth

 Der Anmeldebildschirm wird in der verwendeten Browsersprache angezeigt.

1.1 Hintergrund

Workbench, Office und FFAuth sind drei unabhängige Applikationen. Meldet sich ein Benutzer über die Workbench an, werden die Anmeldedaten zentral in FFAuth hinterlegt. Öffnet der Benutzer nun das Office, startet dies eine Anfrage bei FFAuth und fragt ab, ob der Benutzer bereits angemeldet ist. Bei einem positiven Ergebnis wird der Benutzer auch im Office automatisch angemeldet. Die Prüfung geschieht ohne nennenswerte Zeitverzögerung.

Meldet sich der Benutzer von einem Modul ab, wird die Abmeldeinformation ebenfalls an das andere Modul übertragen und der Benutzer wird auch dort abgemeldet.

Spracheinstellungen werden ebenfalls übertragen, jedoch nicht von FFAuth verwaltet. Der Austausch findet direkt über die Module statt: Wird in einem Modul eine Sprache ausgewählt, wird das andere Modul darüber informiert und ändert die Sprache ebenfalls. Ist ein Benutzer in der Workbench beispielsweise in der Sprache **English (US)** eingeloggt, wird diese Einstellung auf das Office übertragen und es startet ebenfalls auf Englisch.

Sind Workbench und Office gleichzeitig in einem Browser geöffnet, überträgt sich die Spracheinstellung von einem Modul in das andere erst nach einer Aktualisierung des zweiten Moduls. Im Beispiel oben muss der Benutzer den Office-Reiter neu laden. Meldet sich der Benutzer im Office ab, wird die vorherige Spracheinstellung wieder geladen.

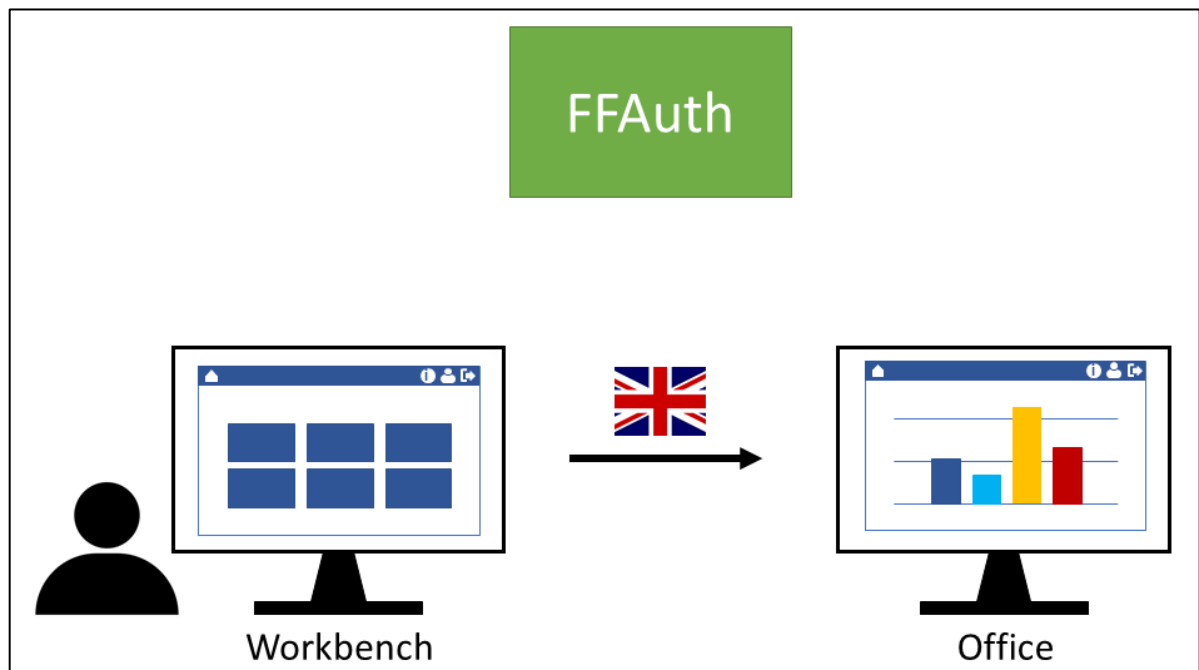


Bild 3: Übertragung von Spracheinstellungen direkt über Module

1.2 Zeitüberschreitung (Timeout)

Die zentrale Anmeldung bei FFAuth ist 24 Stunden lang gültig.

Meldet sich der Benutzer in der Workbench an, wird eine Sitzung gestartet, die 24 Stunden lang offen ist. Nach Ablauf wird der Benutzer automatisch abgemeldet.

Meldet er sich beispielsweise nach 20 Stunden wieder ab, endet die Sitzung. Meldet er sich erneut an, startet eine neue 24-stündige Sitzung. Ruft der Benutzer dann nach 20 Stunden das Office-Modul auf, wird eine neue, separate Sitzung gestartet. Die Sitzung im Office-Modul läuft allerdings bereits nach 30 Minuten ab.

2 Wechsel zwischen Workbench und Office

Durch FFAuth werden die Module Workbench und Office näher zusammengebracht. Die Navigation zwischen den Modulen ist fließend und benötigt keine erneute Anmeldung. Die Workbench dient als Einstiegspunkt. In der Kachel-Navigation kann eine URL so konfiguriert werden, dass durch sie das Office im selben Fenster aufgerufen wird. Klickt der Benutzer im Office auf das Home-Icon oder verwendet die Zurück-Funktion des Browsers, gelangt er wieder in die Workbench. Durch FFAuth wird dadurch das Gefühl vermittelt, eine einzige Anwendung zu verwenden.

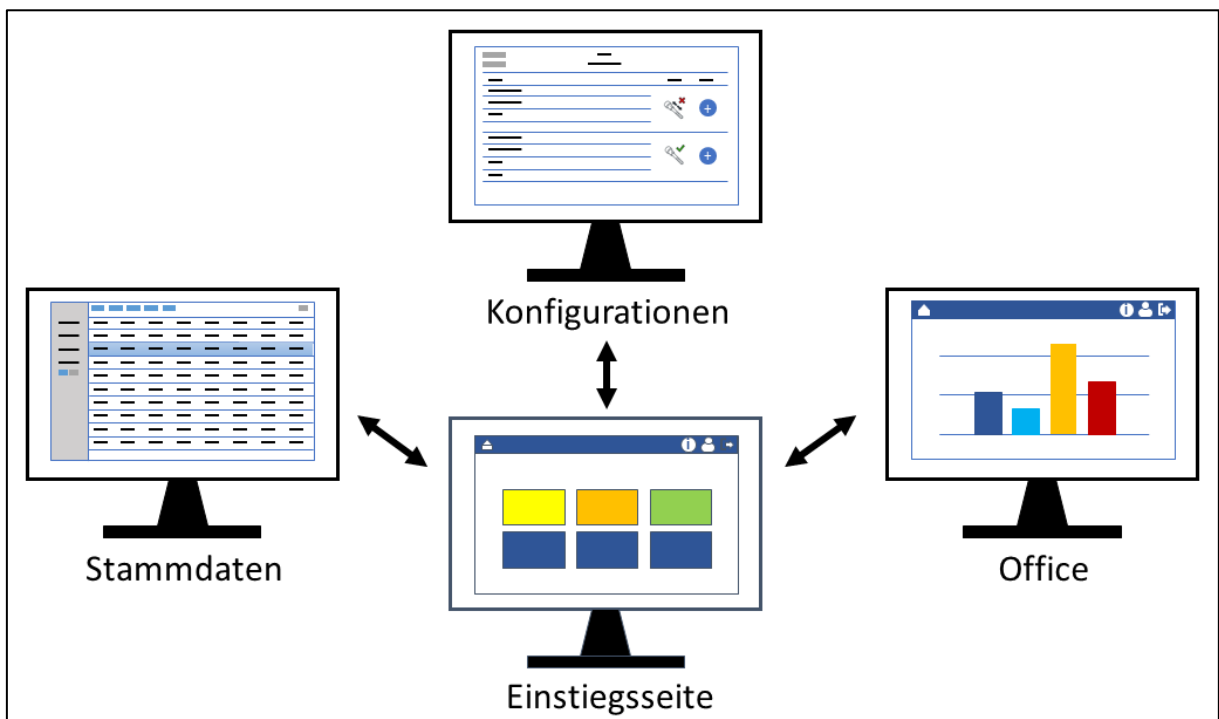


Bild 4: Flüssige Navigation über die Workbench

Für die Navigation zwischen Workbench und Office müssen URLs an zwei Stellen hinterlegt werden.

2.1 URL in einer Kachel

Die Kachelnavigation der Workbench ist flexibel anpassbar. Die Kacheln können frei konfiguriert werden. Für eine detaillierte Anleitung, siehe das Handbuch **Stammdaten und Systemkonfiguration**.

Um in das Office zu navigieren, muss die Adresse des Moduls in eine URL-Kachel eingetragen werden:

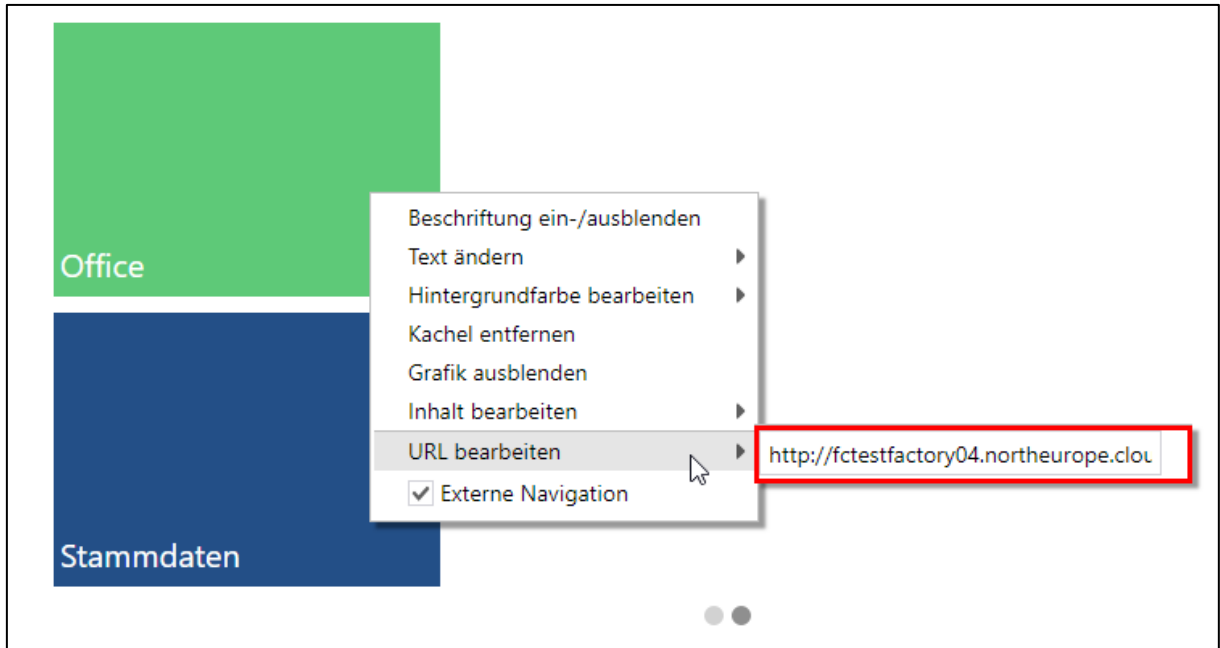


Bild 5: Office-Adresse in URL-Kachel eintragen

2.2 URL in Systemkonfigurationen

Um vom Office durch Klicken auf das Home-Icon oder die Zurück-Funktion des Browsers wieder in die Workbench zu gelangen, muss die Adresse der Workbench in den Systemeinstellungen eingetragen sein:

System	Bezeich	Wert
FORCAM FORCE™	Workbench Konfiguration	
<ul style="list-style-type: none"> ▼ Konfigurationen <ul style="list-style-type: none"> > Allgemein ▼ Module <ul style="list-style-type: none"> > Runtime ▼ Workbench <ul style="list-style-type: none"> Url Datenbankverbindungen 	Url	http://fctestfactory04.northeurope.cloudapp.azure.com:15080/ffworkbench

Bild 6: Workbench-Adresse in Systemkonfigurationen eintragen

3 Sicherheitszertifikat (HTTPS)

FFAuth verwendet die Transportverschlüsselung HTTPS. Es ist möglich, ein vorhandenes Zertifikat zu verwenden. Dies muss kundenseitig bereitgestellt werden. Es können auch eigene Zertifikate generiert werden. Diese werden vom Browser allerdings als unsicher eingestuft.

Bei Verwendung eines selbstgenerierten Zertifikats zeigt der Browser beim Aufruf eines Moduls eine „unsichere Verbindung“ an. Die Warnung vor Unsicherheit erscheint in jedem Fall nur beim ersten Aufruf des Moduls.



Bild 7: Sicherheitswarnung bei Google Chrome