

Lexware API Kochbuch “Onboarding”

Standard Partner Onboarding	1
Erster Kontakt	1
Anlegen eines API Clients auf der Lexware sandbox	1
Implementieren der Anbindung	3
Entwicklungs-Support	3
Die Lexware sandbox	4
Lexware Partner API	4
Autorisierung der Client-Anwendung	4
refresh_tokens	5
access_tokens	6
Lexware insights	7
Lexware Verträge und deren Lebenszyklus	7
Berechtigungen in Lexware	8
Firmen- und Steuer-Relevante Einstellungen	8
Testen der Anbindung auf der Lexware sandbox	8
Rollout der Anbindung	9
Legal	9
3rd Level Support & Ansprechpartner	9
Aufbau der Partner-Landingpage	9
Testbetrieb / Silent Launch	9
Pilotphase / Silent Launch	10
Veröffentlichung der Anbindung	11

Standard Partner Onboarding

Erster Kontakt

Bei einem ersten Videocall stehen Ihre Fragen zur Anbindung, der UseCase, die UserTouchpoints (Verbindungsaufbau, Buttons/ Trigger zur Datenübertragung ...), die Rahmenbedingungen zur Nutzung der API und ein Ausblick zur Vermarktung der Anbindung auf der Agenda. Offene Punkte werden zur Nachbearbeitung festgehalten.

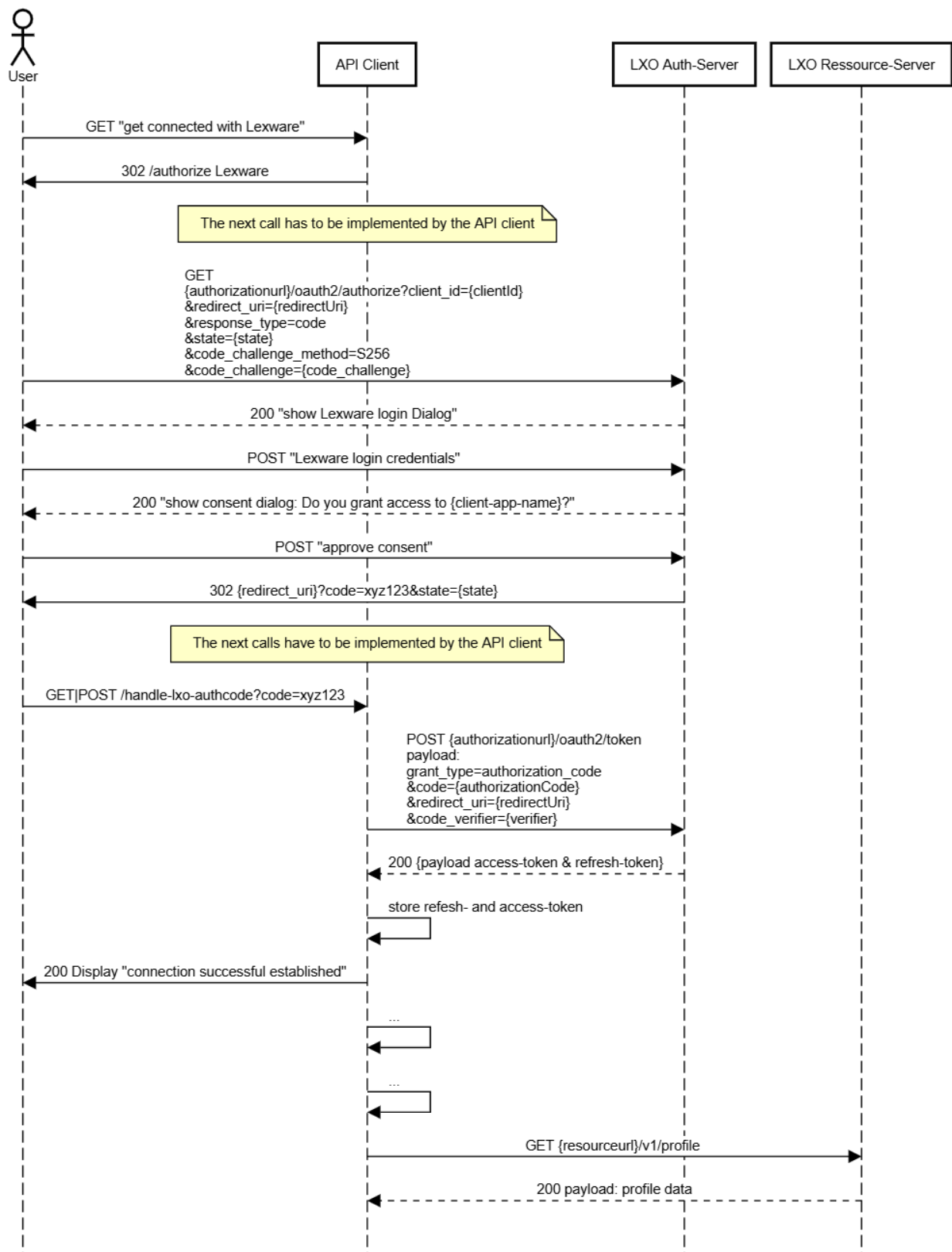
Damit Sie sich einen Überblick über den Funktionsumfang der Partner API machen können, stellen wir Ihnen den Zugang zur Lexware Partner API Dokumentation zur Verfügung.

Wenn Sie sich entschlossen haben, die Anbindung Ihrer Client-Anwendung mit Lexware zu beginnen, setzen wir einen permanenten API Client auf der Lexware sandbox auf.

Anlegen eines API Clients auf der Lexware sandbox

Für die Konfiguration des API Clients müssen die notwendigen API scopes sowie Rücksprung-URL (redirect_uri) für den OAuth2 Autorisierungs-Webflow bekannt sein.

OAuth2 Webflow



Vereinfachter Ablauf des OAuth2 Autorisierungs-Webflow

Vereinfacht beschrieben dient die `redirect_uri` dazu, den Browser des Anwenders nach dem Abschluss der Autorisierungs-Seite vom Lexware AuthServer zurück zur Client-Anwendung zu lenken und den `authorizationCode` sowie optional den `state` zu übermitteln.

Die `redirect_uri` muss gemäß OAuth2 Vorgabe im Lexware API Client hinterlegt sein und mit der beim Aufruf des Autorisierungs-Webflows verwendeten `redirect_uri` identisch sein. Es ist daher nicht möglich, die `redirect_uri` beliebig bzw. dynamisch zu setzen.

Für den Fall, dass keine statische `redirect_uri` zur Verfügung steht (z.B. jeder Anwender betreibt die anzubindende Client-Anwendung unter einer eigenen Domain oder die Client-Anwendung ist eine Desktop-Anwendung) kommt ein "Non SaaS" API Client zum Einsatz. "Non SaaS" API Clients haben eine von uns feste definierte `redirect_url`. Sie leitet den Browser des Anwenders nach dem Abschluss der Autorisierungs-Seite auf eine Lexware Seite die den `authorizationCode` anzeigt. Den angezeigten `authorizationCode` muss der Anwender innerhalb von fünfzehn Minuten per copy & paste in die Client-Anwendung übertragen, damit von dort aus der `authorizationCode` eingelöst werden kann.

Hinweis: In der Lexware sandbox Umgebung ist es zulässig, einem API Client mehrere `redirect_uri`'s zuzuweisen. In der Entwicklungsumgebung ist der Einsatz von HTTP und HTTPS `redirect_uris` möglich. Die Verwendung von `redirect_uri`'s zu Produktiv-Systemen ist für sandbox API clients nicht erlaubt. In der Produktivumgebung sind ausnahmslos HTTPS `redirect_uris` erlaubt.

Nachdem der API Client angelegt wurde, teilen wir Ihnen credentials (`client_id` & `client_secret`, `redirect_uri`'s) mit.

Implementieren der Anbindung

Entwicklungs-Support

Während der Implementierungszeit erhalten Sie Support von uns rund um die geplante Anbindung. Unser Support umfasst technische, fachliche und UX Fragestellungen und steht Ihnen kostenfrei per Email zur Verfügung.

Die Lexware sandbox

Für die Entwicklung von Partner-Anbindungen steht eine Lexware sandbox zur Verfügung.

URL: <https://app.lexware-sandbox.de/>

Die URL zur sandbox ist vertraulich zu behandeln.

Hinweis: Die Lexware sandbox ist nicht für Endanwender vorgesehen. Es muss unbedingt vermieden werden, dass Endanwender eine Verbindung mit der Lexware sandbox aufbauen oder sich dort Accounts anlegen. Lexware sandbox API Clients dürfen daher nicht in Ihrer Produktionsumgebung zum Einsatz kommen.

Sie können sich beliebig viele Accounts auf der Lexware sandbox anlegen. Halten Sie sich dazu an diese FAQ [Link](#).

In unregelmäßigen Abständen wird die Lexware sandbox deployed. Deployments der sandbox werden ca. 24 Stunden vor der Durchführung per Email an die subscribed User des Entwickler-Newsletters angekündigt. Der Newsletter kann [hier](#) abonniert werden.

Bitte beachten Sie, dass bei einem Deployment alle Accounts und Bewegungsdaten auf der sandbox verloren gehen, wenn die Datenbank neu aufgesetzt werden muss.

Lexware Partner API

Zugriff auf Lexware steht per JSON RESTful API zur Verfügung.

URL zur Entwicklerdokumentation: <https://developers.lexware.io/partner/>

Die URL zur Partner API Dokumentation ist vertraulich zu behandeln.

Autorisierung der Client-Anwendung

Die Autorisierung einer Client-Anwendung erfolgt durch den OAuth2

Autorisierungs-Webflow (s.o.). Der Anwender genehmigt damit den Zugriff der Client-Anwendung auf die im API Client fest definierten scopes.

Nach erfolgter Genehmigung der Autorisierungsanfrage erhält die Client-Anwendung refresh_tokens und access_tokens, mit deren Hilfe der Zugriff per REST API auf genau diesen Lexware Account möglich ist.

Aufrufe der REST API erfolgen immer im Kontext und mit den Berechtigungen des Lexware Anwenders, der die Autorisierungsanfrage durchgeführt und genehmigt hat.

Hinweis:

- Das im Zuge einer Autorisierung ausgestellte refresh_token und access_token bezieht sich auf den Lexware Account der die Autorisierung durchgeführt hat.
- Der Zugriff auf Daten des Lexware Accounts per REST API ist nur im Umfang der genehmigten scopes möglich. Aufrufe von Funktionen, deren scope nicht genehmigt wurde, werden mit HTTP 403 quittiert.

refresh_tokens

Seit Einsatz des token rotation Verfahrens haben refresh_tokens per Default eine Gültigkeitsdauer von 90 Tagen, gerechnet ab dem Zeitpunkt der Ausstellung des Tokens.

Hinweis: refresh_tokens müssen in der Client-Applikation sicher zum Client-Account der die API Verbindung autorisiert hat, gespeichert werden. Jeder, der im Besitz von refresh_token und den API credentials ist, hat per REST API Zugriff auf alle autorisierten Funktionen und Daten des zum refresh_token gehörigen Lexware Accounts. Bitte informieren Sie uns unverzüglich, wenn refresh_tokens von Lexware Anwendern gestohlen wurden oder der Verdacht eines Datendiebstahls besteht.

Mit gültigen refresh_tokens können jederzeit access_tokens erstellt werden.

Die Client-Applikation muss mit folgenden Situationen umgehen und den Anwender passend leiten können:

- *Das refresh_token muss erneuert werden.*
Dies kann zwei Ursachen haben.
 - a) der refresh_token läuft bald ab
 - b) die damals zugewiesenen API scopes haben sich verändert und es ist eine erneute Autorisierung der scopes erforderlich.
- *Das refresh_token läuft bei der Verwendung ab.*
Beim Abrufen eines access_tokens stellt der Lexware AuthServer fest, dass das verwendete refresh_token abgelaufen ist. Diese Anfrage wird einmalig mit HTTP 403 quittiert. Das refresh_token wird danach in Lexware gelöscht und eventuell vorhandene Event-Subscriptions entfernt.

- *Das refresh_token ist bereits abgelaufen.*
Wenn das refresh_token abgelaufen ist, muss der Anwender die Autorisierung “from scratch” neu durchlaufen. Wenn die Client-Anwendung mit einem abgelaufenen refresh_token ein access_token abrufen, wird dies mit HTTP 400 quittiert.
- *Das refresh_token wurde seitens des Anwenders entzogen.*
Der Anwender hat in Lexware die Möglichkeit API Verbindungen zu trennen. Dies führt dazu, dass das zur Verbindung gehörende refresh_token, sowie eventuell bestehende Event-Subscriptions gelöscht werden.
Wenn die Client-Anwendung mit einem gelöschten refresh_token ein access_token abrufen möchte, wird dies mit HTTP 400 quittiert.
Mittels Einbindung des Event-Typs “token.revoked” in die Client-Anwendung kann eine vom Anwender in Lexware durchgeführte Trennung der API Verbindung per Webhook an den API Client gesendet werden.
- *Der Anwender löst die API Verbindung mit Lexware in der Client-Anwendung.*
In der Client-Anwendung muss dem Anwender eine Möglichkeit zur Verfügung stehen, eine mit Lexware aufgebaute API Verbindung zu trennen.
Rufen Sie in diesem Fall unbedingt die Funktion “POST {authorizationurl}/oauth2/revoke” der Lexware API auf. Nur damit ist sichergestellt, dass Lexware das refresh_token löscht und die API Verbindung inkl. eventuell vorhandener Event-Subscriptions korrekt terminiert.
- *Abo-Vertragsende.* Mit dem Vertragsende des Lexware Abos werden alle bestehenden API Connections getrennt und alle eventuell vorhandenen Event Subscriptions gelöscht.

access_tokens

access_tokens haben per Default eine Lebensdauer von vier Stunden ab dem Zeitpunkt der Ausstellung.

Im Feld “expires_in” der response von “POST {authorizationurl}/oauth2/token?...” steht die Lebensdauer des access_tokens in Sekunden (14400 sec = 4 h) . Mit gültigen access_tokens können beliebig viele REST API calls auf dem Lexware ResourceServer durchgeführt werden. Aufrufe mit abgelaufenen access_tokens werden mit HTTP 401 quittiert.

Hinweis: Mit gültigen Lexware access_tokens kann die Client-Anwendung im Rahmen der genehmigten scopes über die REST API auf Daten des zugehörigen Lexware Accounts

zugreifen. Die Client Anwendung muss access_tokens ebenso sensibel wie refresh_tokens behandeln.

Lexware insights

Lexware Verträge und deren Lebenszyklus

Lexware kennt Stand 02.2022 diese Verträge (vereinfachte Beschreibung):

- Test-Zugang (entspricht dem Funktionsumfang von “Lexware Office XL”):
Zugriff auf die Partner API steht in vollem Umfang zur Verfügung.
- Abo “Lexware Office S”:
Zugriff auf die Partner API steht in eingeschränktem Umfang zur Verfügung.
- Abo “Lexware Office M”:
Zugriff auf die Partner API steht in eingeschränktem Umfang zur Verfügung.
- Abo “Lexware Office L”:
Zugriff auf die Partner API steht in eingeschränktem Umfang zur Verfügung.
- Abo “Lexware Office XL”:
Zugriff auf die Partner API steht in vollem Umfang zur Verfügung.

Läuft ein Abo aus, geht dieser in einen “read only” Modus über. Der Anwender kann sich noch einloggen, lesend auf seine Daten zugreifen und Exporte durchführen. Alle vorhandenen API Connections werden getrennt und vorhandene Event Subscriptions werden gelöscht.

Test-Zugänge, die nach dem Testzeitraum direkt in den “read only” Modus gehen, werden nach einer festgelegten Zeitspanne gelöscht.

Berechtigungen in Lexware

Lexware verfügt über ein einfaches Berechtigungssystem. Die Einstellungen dazu sind auf der sandbox hier zu finden: <https://app.lexware-sandbox.de/user-administration/userList>

Aufrufe der REST API erfolgen immer im Kontext des Lexware Anwenders, der die API Autorisierungsanfrage genehmigt hat. Änderungen an den Rechten dieses Anwenders können Auswirkungen auf die Anbindung der Client-Anwendung haben.

Fehlen dem Lexware Benutzer beispielsweise die Rechte zum Anlegen, Lesen oder Bearbeiten von Daten, wird der entsprechende REST API request vom Lexware ResourceServer mit HTTP 403 quittiert.

Firmen- und Steuer-Relevante Einstellungen

In den Firmeneinstellungen (Menüpunkt Einstellungen -> Allgemeine Einstellungen, <https://app.lexware-sandbox.de/settings/#/general>) können die steuerrelevanten Daten des Unternehmens eingetragen werden.

Diese Einstellungen haben ggf. Auswirkungen auf die Partner API. Z.B. können für Umsatzsteuerbefreite Unternehmen keine Rechnungen mit Umsatzsteuer über den invoices Endpunkt angelegt werden. Ein solcher API request wird vom Lexware resource server mit HTTP 406 quittiert.

Testen der Anbindung auf der Lexware sandbox

Sobald auf der Entwicklungsumgebung ein Stand erreicht wird, der sich für den Testbetrieb in der Produktivumgebung eignet, findet ein technischer und fachlicher Test der Anbindung seitens Lexware statt. Melden Sie sich hierfür zu gegebener Zeit zur Vereinbarung eines Review Termins.

Nachdem die Tests für beide Seiten mit befriedigendem Ergebnis abgeschlossen wurden, kann mit dem Rollout der Anbindung für den Testbetrieb begonnen werden.

Rollout der Anbindung

Legal

Bevor die Anbindung von Endkunden genutzt werden kann, müssen die Allgemeinen Geschäftsbedingungen zur Nutzung der Lexware Partner API unterzeichnet werden. Sie bekommen rechtzeitig ein Exemplar des Dokuments zugesandt.

3rd Level Support & Ansprechpartner

Für Fragen rund um die Anbindung zwischen Ihrer Client-Anwendung und Lexware möchten wir Sie um die Kontaktdaten jeweils eines Ansprechpartners aus der Technik und dem Business bitten. Diese Daten hinterlegen wir bei uns an zentraler Stelle, damit im Falle eines Falles rasch Kontakt aufgenommen werden kann. Seitens Lexware erhalten Sie ebenfalls die Kontaktdaten jeweils eines Ansprechpartners aus Technik und Business.

Aufbau der Partner-Landingpage

Sobald sich die Anbindung in die Phase "Testen der Anbindung auf der sandbox" bewegt, können die Marketing-Unterlagen vorbereitet werden. Hierfür wird auf der Basis Ihrer und unserer Informationen zur Anbindung der Client-Anwendung mit Lexware eine Partner-Landingpage aufgebaut.

Die Lexware Partner-Landingpage enthält einen Link, der dem Anwender einen leichten Einstieg in die Nutzung der Anbindung beider Applikationen ermöglichen soll.

Testbetrieb / Silent Launch

Damit die Anbindung in die Produktivumgebung gelauncht werden kann, muss ein eigener API Client mit client-id & client-secret angelegt werden.

Stellen Sie hierfür bitte auf Nachfrage folgende Daten zur Verfügung:

- redirect_uri für Ihre Produktivumgebung

- Ein zur Anbindung passendes Logo als PNG auf weißem oder transparentem Hintergrund in der Größe 225x100 pixel
- Einen Titel zur Anbindung mit maximal 31 Zeichen (bitte beachten, dass encodiert wird. Ein "&" wird zu "&" und verbraucht 5 Zeichen).
- offizielle Bezeichnung ihrer Firmierung
- Einen Teaser-Text mit maximal 90 Zeichen (bitte beachten, dass encodiert wird).



Abbildung: Darstellung einer "Kachel" mit den Informationen zur Anbindung in der Lexware App

Hinweis: Ein Klick auf das Logo in der Kachel öffnet einen Browser-Tab und zeigt die Partner-Landingpage an.

Sie bekommen die Zugangsdaten des API Clients für die Lexware Produktivumgebung auf einem sicheren Übertragungsweg übermittelt. In der Regel handelt es sich um ein ZIP File mit Passwortschutz. Das Passwort bekommen Sie per SMS oder am Telefon, das ZIP auf einem anderen Übertragungsweg übermittelt.

Pilotphase / Silent Launch

Nach dem Setup des API Clients und erfolgreichen smoke-tests der Anbindung in der Produktivumgebung können Sie eine zuvor mit uns abgestimmte Anzahl von Interessenten über den Testbetrieb der Anbindung informieren.

Ziel dabei ist eine Verprobung der Anbindung mit echten Kunden, bevor an die breite Masse kommuniziert wird. Im Kontakt mit den Testern soll Feedback zur Anbindung eingeholt und bewertet werden, um die Anbindung bei Bedarf zu optimieren und Bugs zu beheben. Melden Sie sich nach Abschluss der Pilotphase bei uns, um die Veröffentlichung der Anbindung zu koordinieren.

Veröffentlichung der Anbindung

Mit Abschluss der Pilotphase und Bereitstellung der Partner-Landingpage kann die Anbindung der Client-Anbindung mit Lexware veröffentlicht werden.

Hierbei wird in Abstimmung mit Ihnen ein Newsletter mit Informationen zur Anbindung an unsere Lexware Newsletter-Abonnenten verschickt. Diese Email enthält einen Link auf die Landingpage, damit sich Anwender ein Bild zur Anbindung verschaffen können.