Einleitung

Die KeyHelp-API-Schnittstelle erlaubt es anderer Software mit KeyHelp zu interagieren und so bestimmte Aktionen auszulösen. Diese Funktion ist dann hilfreich, wenn diverse IT-Prozesse automatisiert werden sollen.

Die im KeyHelp implementierte API arbeitet nach dem **REST** Prinzip. Das bedeutet, es werden HTTP Anfragen für den Zugriff auf die Daten verwendet werden. Über die verschiedenen HTTP-Methoden werden entsprechende Aktionen abgebildet.

- GET - Abfrage von Daten
- PUT - Aktualisierung von Daten
- POST - Erstellen von Daten
- DELETE - Löschen von Daten

Entsprechend antwortet die API je nach Aktion mit den bekannten HTTP-Status-Codes:

- 200 - OK
- 201 - CREATED
- 400 - BAD REQUEST
- 404 - NOT FOUND
- usw.

Um die Gültigkeit einer API-Anfrage zu verifizieren, muss bei jeder Anfrage ein API-Schlüssel als Teil dieser gesendet werden werden. Dieser API-Schlüssel kann direkt über das KeyHelp-Benutzerinterface erstellt werden. Zusätzlich muss die API zunächst aktiviert werden. Alle relevanten Optionen finden Sie im **KeyHelp-Administrationsbereich** unter **Konfiguration** -> **API**.

Interaktive Dokumentation

Eine Vollständige API-Dokumentation finden Sie unter folgender URL: https://api.keyhelp.de
Dort erhalten Sie eine detaillierte Beschreibung aller API-Endpunkte und erfahren wie API-Anfragen aufgebaut und API-Antworten strukturiert sein können. Darüber hinaus können Sie sämtliche Endpunkte interaktiv, direkt über Ihren Browser testen.

Um die interaktive Test-Umgebung zu verwenden, betätigen Sie den Button **Try it out**, den Sie unter der Erklärung eines jeden Endpunktes finden. Klicken Sie anschließend den Button **Execute** um eine Anfrage abzuschicken. Um Anfragen direkt zu einem Server Ihrer Wahl zu schicken. Füllen Sie im oberen Bereich der API-Dokumentation zunächst die Eingabefelder **host** sowie die nach einem Klick auf dem Button **Authorize** erscheinenden Eingabefelder aus.

Sicherheit

Die Sicherheit der API-Schnittstelle wird durch verschiedenste Mechanismen sichergestellt, so dass es Angreifern fast unmöglich ist, sich per Brute-Force unberechtigt Zugriff zu verschaffen. Die Schnittstelle sollte dennoch nur als sicher angesehen, wenn der Zugriff auf ein oder mehrere IP-Adressen / IP-Bereiche beschränkt wird.
In der KeyHelp-Oberfläche können Sie über die Eigenschaften eines API-Schlüssels die gewünschten freigegebenen IPs hinterlegen.

Beispiel-Code

Um Ihnen den Einstieg zu erleichtern finden Sie unter Code-Beispiele kurze Anleitungen zur API. Beachten Sie, dass der dort gezeigte Code Ihnen lediglich den Umgang mit der API verdeutlichen soll, Fehlerbehandlungsroutinen und Ähnliches müssen entsprechend von Ihnen programmiert werden.

Im Beispielcode finden Sie Platzhalter nach dem Schema **<NAME>**, die Sie ersetzen müssen.
Ersetzen Sie **<HOSTNAME>** mit dem Hostnamen oder IP Ihres KeyHelp Servers.
Ersetzen Sie **<API-KEY>** mit Ihrem API-Schlüssel Ihres Servers.

Revision #8
Created 19 May 2022 13:12:14 by Alexander Mahr
Updated 24 May 2022 07:58:16 by Alexander Mahr