GIRA

# Gira Fernzugriffs-API Dokumentation

Stand: 06.05.2022

Version: v1

# Inhaltsverzeichnis

1 Über die Gira Fernzugriffs-API ..... 3
2 Voraussetzungen ..... 3
3 Funktionsumfang ..... 4
4 Nutzung ..... 5
5 Beispiele ..... 6
6 Digest access authentication ..... 7
7 Validierungsmethoden ..... 7
8 Unterstützung ..... 7

# 1 Über die Gira Fernzugriffs-API

Der Gira S1 ist ein Fernzugriffsmodul, das folgende Funktionen bietet:

- Einen sicheren Fernzugriff per Gira Geräteportal oder Gira Apps
- Eine Fernwartung per Gira Inbetriebnahmesoftware, z. B. den Gira Projekt Assistenten oder den Gira Experten

Neben den von Gira bereitgestellten Anwendungen und Apps ist auch ein Fernzugriff auf das lokale Netzwerk des Gira S1 mittels Drittanwendungen oder selbstentwickelten Apps möglich. Dazu kann die Gira Fernzugriffs-API genutzt werden.

# 2 Voraussetzungen

Voraussetzungen dafür sind ein auf HTTP oder HTTPS basierender Service auf einem Gerät im lokalen Netzwerk des Gira S1 und ein Client, der den Zugriff über eine frei konfigurierbare URL ermöglicht.

Sie benötigen für den Fernzugriff außerdem:

- Die Fernzugriffs-ID Ihres Gira S1
- Einen Authentifizierungsschlüssel

Jeder Benutzer, der im Gira Geräteportal Zugriff auf den Gira S1 hat, kann beides in der Rubrik „Applikationszugänge“ abrufen.

---

Sie erhalten den Authentifizierungsschlüssel wie folgt:

1. Legen Sie einen Applikationszugang an.
2. Öffnen Sie in der Spalte „Optionen“ den Link „Bearbeiten“.
   Auf dieser Seite können Sie nun den Authentifizierungsschlüssel kopieren.

---

# 3 Funktionsumfang

Die Gira Fernzugriffs-API unterstützt folgende Funktionen:

- Fernzugriff aus dem Internet auf einen lokalen Server
- Zugriff per HTTP und HTTPS (mit oder ohne Zertifikatsvalidierung des Servers)
- Zugriff per REST API oder WebSockets
- Zugriff auf Webseiten, die aus einem einzigen HTML-Dokument bestehen

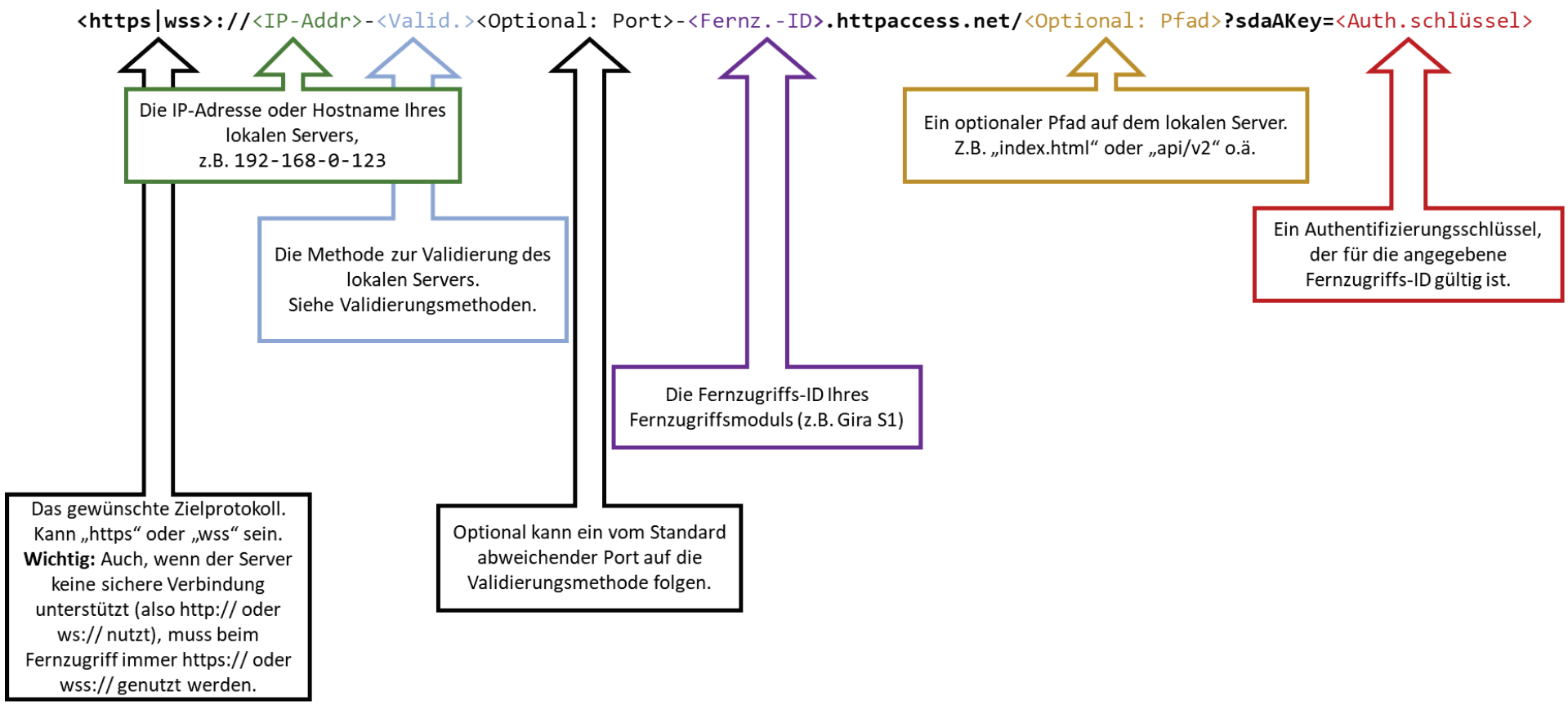
Die Gira Fernzugriffs-API kann in Verbindung mit der Gira IoT REST API (zur Doku), z. B. mit einem Gira X1 oder einem Gira HomeServer, effektiv genutzt werden.

**Hinweise:**

- Das Laden von Webseiten, die aus aufgeteilten Dokumenten bestehen wie HTML-Seiten, die CSS, Grafiken oder andere Ressourcen einbinden, wird nicht unterstützt. Der Grund ist, dass der Webbrowser beim Laden der nachfolgenden Ressourcen nicht die nötige URL-Transformation durchführen sowie nicht den nötigen Query-Parameter sdaAKey anhängen wird. Für dieses Anwendungsszenario wird empfohlen, die Funktion „Links“ Ihres Gira S1 auf dem Gira Geräteportal zu verwenden.
- Der Fernzugriff über andere Protokolle, z. B. SSH oder RDP, ist nicht möglich. Für dieses Anwendungsszenario wird empfohlen, den Gira S1 Windows Client zu verwenden (zum Download).

# 4 Nutzung

Um die Gira Fernzugriffs-API zu nutzen, müssen Sie die Ziel-URL zum lokalen Server gemäß dem folgenden Schema modifizieren:



# 5 Beispiele

Die folgenden Beispiele enthalten die fiktive Fernzugriffs-ID **GI-0123456** und den fiktiven Authentifizierungsschlüssel **AbCdEfG12345XyZ**.

**Beispiel 1:**

http://192.168.0.1/

wird zu

https://192-168-0-1-**h**-**gi0123456**.**httpaccess.net**/?**sdaAKey**=**AbCdEfG12345XyZ**

**Beispiel 2:**

https://192.168.0.123/api/v2/uiconfig?token=0815

wird zu

https://192-168-0-123-**u**-**gi0123456**.**httpaccess.net**/api/v2/uiconfig?token=0815&**sdaAKey**=**AbCdEfG12345XyZ**

**Beispiel 3:**

ws://192.168.0.123:4444/wsapi

wird zu

wss://192-168-0-123-**h4444**-**gi0123456**.**httpaccess.net**/wsapi?**sdaAKey**=**AbCdEfG12345Xy**

# 6 Digest access authentication

Bei einer Digest-Authentifizierung, die z. B. IP-Kameras häufig anfordern, kann es aufgrund von nicht-konformen Digest-Implementierungen auf den Geräten zu Problemen beim Fernzugriff kommen. Um die Probleme zu umgehen, ist die auf Seite 5 angegebene URL am Ende nach <Auth.schlüssel> mit dem Parameter [&sdaDigestProxy] zu ergänzen. Wenn der Parameter angegeben wird, werden alle Digest-Authentifizierungsanfragen als Basic-Authentifizierungsanfrage an den Client weitergeleitet. Der SDA-Proxy führt dann gegenüber dem Gerät (Server) die Digest-Authentifizierung mit den vom Client angegebenen Anmeldeinformationen durch.

---

Die Angabe des Parameters ist nicht standardmäßig, sondern nur im Bedarfsfall anzuwenden.

---

# 7 Validierungsmethoden

| Kürzel in der URL | Beschreibung | Standardport |
|---|---|---|
| s | Der lokale Server wird per HTTPS kontaktiert. Das Serverzertifikat wird validiert und bei fehlgeschlagener Validierung wird die Verbindung abgebrochen.<br>Gültig, wenn der lokale Server https:// oder wss:// nutzt. | 443 |
| u | Der lokale Server wird per HTTPS kontaktiert. Das Serverzertifikat wird nicht validiert. Nutzen Sie diese Validierungsmethode, wenn der Server kein gültiges Serverzertifikat liefern kann.<br>Gültig, wenn der lokale Server https:// oder wss:// nutzt. | 443 |
| h | Der lokale Server wird per HTTP kontaktiert.<br>Gültig, wenn der lokale Server http:// oder ws:// nutzt. | 80 |

# 8 Unterstützung

Bei Fragen und Anmerkungen rund um die Gira Fernzugriffs-API können Sie sich an developer@gira.de wenden. Ihre Anfragen werden in der Regel innerhalb von drei Werktagen bearbeitet.