GIRA

Gira Remote Access API Documentation

Date: 06.05.2022

Version: v1

Table of Contents

1 About the Gira Remote Access API

The Gira S1 is a remote access module that offers the following functions:

- Secure remote access via Gira Device Portal or Gira apps.
- Remote maintenance via Gira setup software, e.g. the Gira Project Assistant or the Gira Expert.

In addition to the applications provided by Gira, remote access to the local network of the Gira S1 is also possible using third-party applications or applications developed in-house. The Gira Remote Access API can be used for this purpose.

2 Prerequisites

Prerequisites for this are an HTTP or HTTPS-based service on a device in the local network of the Gira S1 and a client that allows access via a freely configurable URL.

For the remote access you also require:

- The remote access ID of your Gira S1
- An authentication key

Every user who has access to the Gira S1 in the Gira device portal can retrieve both in the “Remote Access” section.

ℹ You can obtain the authentication key as follows:

1. Create an application entry.
2. In the “Options” column, open the link “Edit”. On this page, you can now copy the authentication key.

---

3 Range of Functions

The Gira Remote Access API supports the following functions:

- Remote Access from the Internet to a local server
- Access via HTTP and HTTPS (with or without certificate validation of the server)
- Access via REST API or WebSockets
- Access to web pages that consist of a single HTML document

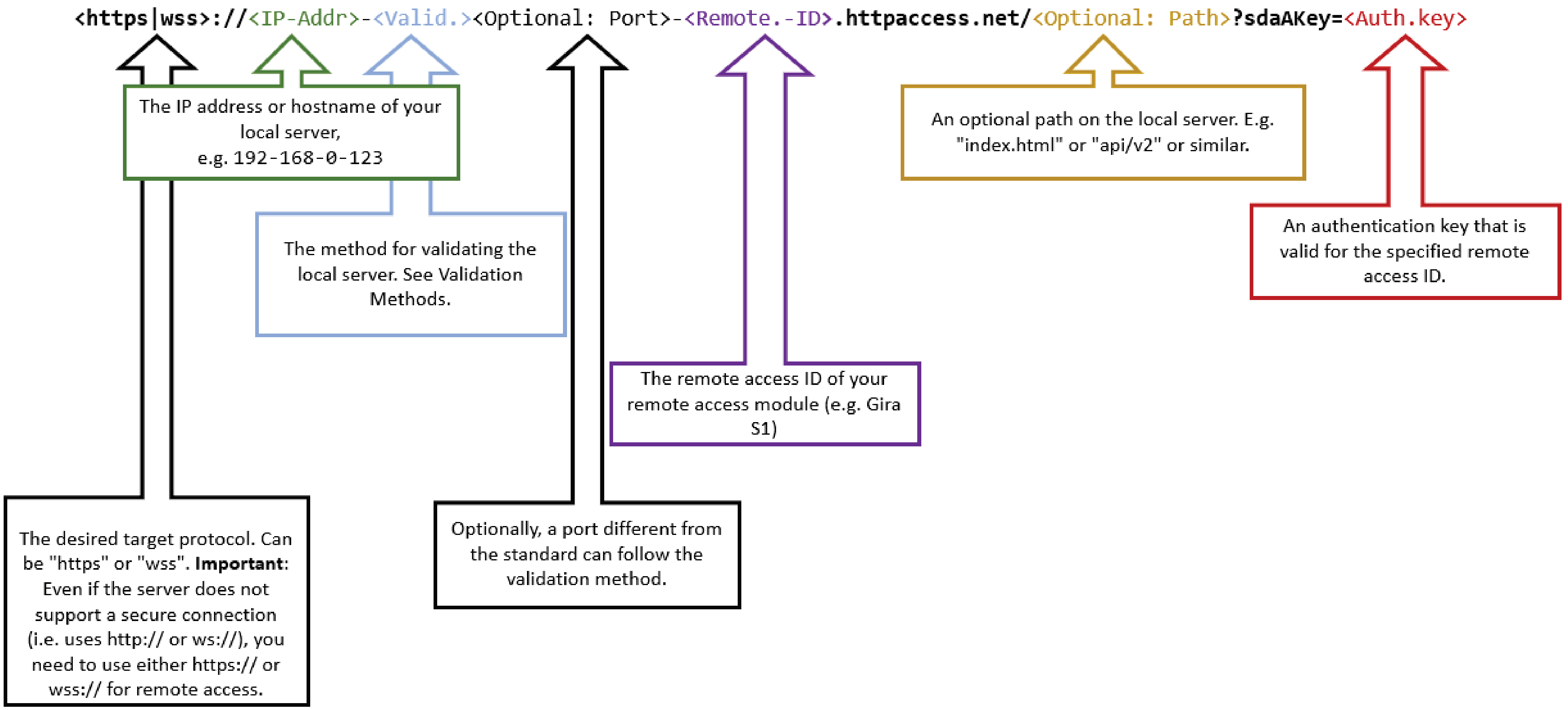
The Gira Remote Access API can be used effectively in conjunction with the Gira IoT REST API (to the documentation), e.g. with a Gira X1 or a Gira HomeServer.

Tips:

- Loading websites that consist of split documents like HTML websites that embed CSS, graphics, or other resources are not supported. The reason for this is that the web browser will not perform the necessary URL transformation when loading the subsequent resources and not append the necessary query parameter sdaAKey. For this application scenario, it is recommended to use the “Links” function of your Gira S1 on the Gira device portal.
- Remote access via other protocols, e.g. SSH or RDP, is not possible. For this application scenario, it is recommended to use the Gira S1 Windows Client. (Link to the download)

4 Usage

To use the Gira Remote Access API, you must modify the target URL to the local server in line with the following schema.



```
<https|wss>://<IP-Addr>-<Valid.><Optional: Port>-<Remote.-ID>.httpaccess.net/<Optional: Path>?sdaAKey=<Auth.key>
```

The IP address or hostname of your local server, e.g. 192-168-0-123

The method for validating the local server. See Validation Methods.

Optionally, a port different from the standard can follow the validation method.

The remote access ID of your remote access module (e.g. Gira S1)

An optional path on the local server. E.g. "index.html" or "api/v2" or similar.

An authentication key that is valid for the specified remote access ID.

The desired target protocol. Can be "https" or "wss". **Important**: Even if the server does not support a secure connection (i.e. uses http:// or ws://), you need to use either https:// or wss:// for remote access.

5 Examples

The following examples contain the fictitious remote access ID **GI-0123456** and the fictitious authentication key **AbCdEfG12345XyZ**.

Example 1:

http://192.168.0.1/

becomes

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

Example 2:

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

becomes

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

Example 3:

ws://192.168.0.123:4444/wsapi

becomes

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

6 Digest Access Authentication

With a Digest Authentication that is often required for IP-Cameras for example, it can lead to problems with remote access due to non-conforming digest implementations on the devices. To work around the problems, add the parameter [&sdaDigestProxy] to the end of the URL provided on page 5 after <Auth.key>. If the parameter is specified, all of the Digest Authentication requests will be forwarded to the client as basic authentication requests. The SDA proxy then performs the digest authentication against the device (server) using the credentials provided by the client.

ℹ The specification of this parameter is not to be used by default, but only in case of need.

7 Validation Methods

Abbreviation in the URL	Description	Standard Port
s	The local server is contacted via HTTPS. The server certificate is validated and if validation fails, the connection is terminated. Valid if the local server uses https:// or wss://.	443
u	The local server is contacted via HTTPS. The server certificate is not validated. Use this validation method if the server cannot provide a valid server certificate. Valid if the local server uses https:// or wss://.	443
h	The local server is contacted via HTTP. Valid if the local server uses http:// oder ws://.	80

8 Support

For questions and comments about the Gira Remote Access API, you can send an email to developer@gira.de. Your inquiries are usually processed within three working days.