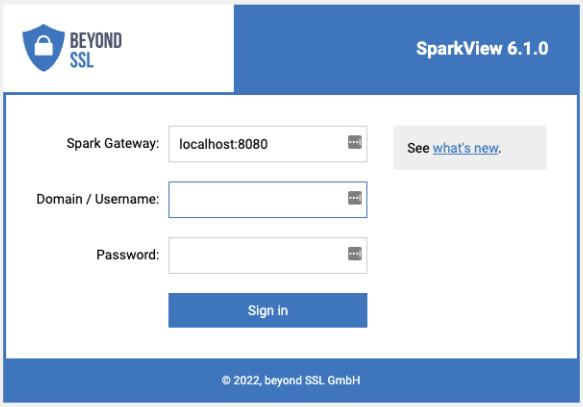
3.5 – Users

You can use users.json file to configure: users (name and password), RDP hosts (configured in servers.json) a user can access. User will have to log in when this file was used (starting from login.html)

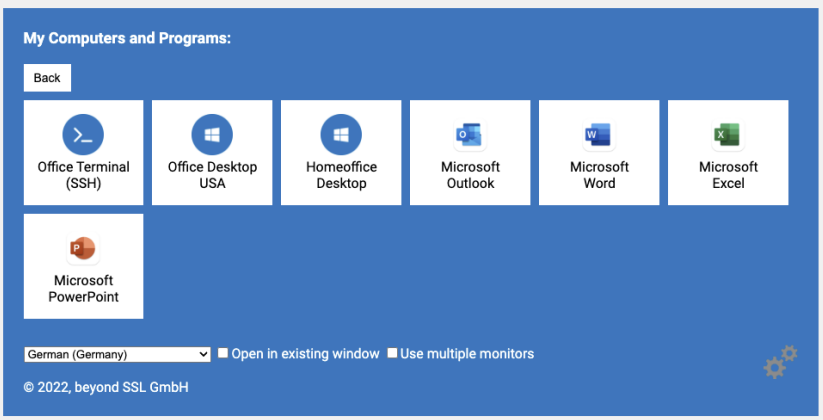


You can also log in with Google, Yahoo account etc with OAuth 2 integration. For OAuth integration

- You don't need to enter user name and password in the login.html.
- Make sure the user name in users.json is your email address (Gmail address if you are using Google Account).
- The password in users.json will be ignored, so you can give any passwords to user.

If you don't need this OAuth integration, you can remove following part from login.html:
`<a href="/OPENID?id=Google"><img src="google.png" title="Sign in with Google account"/></a>`

Please check Chapter 3.22 for more information about OAuth 2.
User will see a list of RDP hosts and applications they can use after logging in:



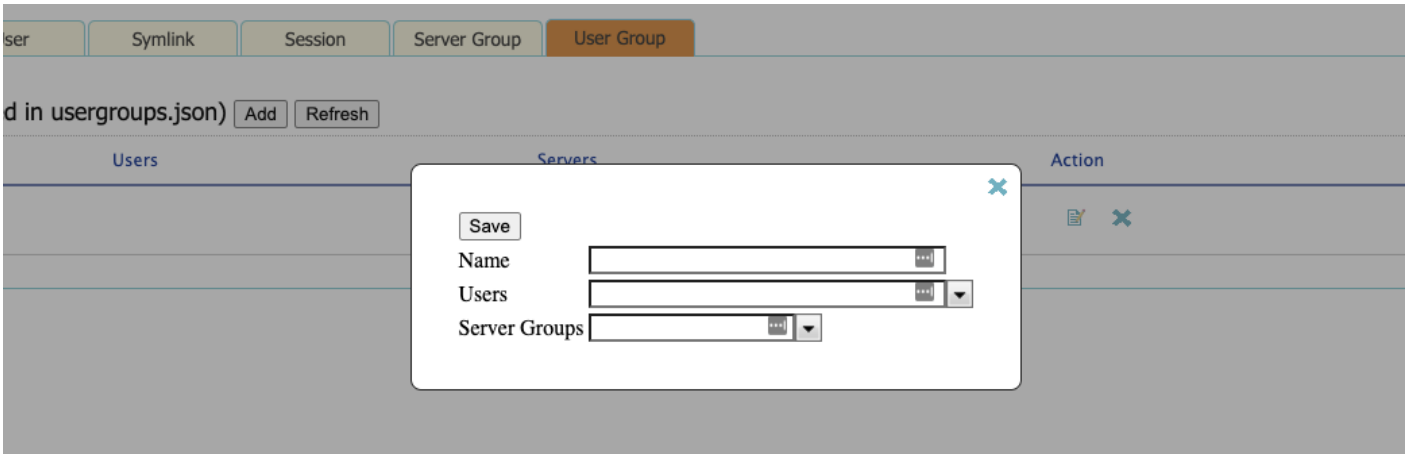
You can also use config.html to configure users.json. Use your browser and navigate to: http://localhost/config.html. For security reason, this page can be only accessed from localhost. The user name should be your email if you are using OpenID integration (log in with Google Account etc).

The following parameters can be stored when creating a user:

- Name
- Password
- Server, which the user is allowed to access
- Domain user (yes/no)
- Domain server
- Transfer credentials to connection
- Host name (for RDP connections)

You can import users from Active Directory too. These domain users will use active directory authentication and don't need to have passwords (default is ***).

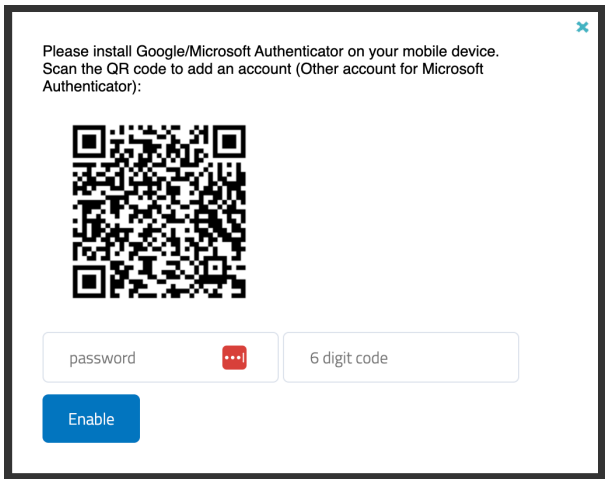
You can also configure user group, which is saved in userGroups.json by default:



Activate two-factor authentication (2FA)

An authenticator app (e.g. Google Authenticator) is required for use.

1. Set `twoFA=1` to activate or `twoFA=2` to force in gateway.conf
2. The user logs in to SparkView, a QR code appears



3. Scan the QR code with the Authenticator app and enter the 6-digit code

---

Reset second factor (2FA) for individual users

There are 3 ways to reset the second factor for individual users:

Java-Command

To do this, the SparkView service must first be stopped. Then use the following command in the SparkView root directory:
`sudo java -cp SparkGateway.jar com.toremote.gateway.tool.TwoFactor username`

For AD users, please use the following command:
`sudo java -cp SparkGateway.jar com.toremote.gateway.tool.TwoFactor "domain\user.name"`

For Windows users:
`java -cp SparkGateway.jar com.toremote.gateway.tool.TwoFactor username` or if AD:
`java -cp SparkGateway.jar com.toremote.gateway.tool.TwoFactor "domain\user.name"`

cURL-Request

The SparkView service must be running for this. Then please use the following command:
`curl -k -G --data-urlencode "target=twofa" --data-urlencode "user=username" http://sparkview-server.com/CONTROL`

For AD users, please use the following command:
`curl -k -G --data-urlencode "target=twofa" --data-urlencode "user=domain\user.name" http://sparkview-server.com/CONTROL`

HTTP request (API)

The SparkView service must be running and a hashed management password must be used. Then please call up the following URL:
`http://sparkview-`

server.com/CONTROL?target=twofa&user=username&gatewayPwd=21232f297a57a5a743894a0e4a801fc3

Revision #10
Created 5 April 2022 10:12:31 by Julian
Updated 28 February 2024 09:16:15 by Julian