Two-Factor Authentication (2FA) @ STRW

Please read this document carefully or jump to

Introduction

Timeline

We will not implement 2FA at the same time for all services, but will gradually enable 2FA according to this timeline.

Working with 2FA

Below we describe in detail how to work with 2FA. It is quite straight forward once you get the hang of it.

First Time Access

Before you can use 2FA we and you need to setup a few things.

- **You should own a Smart Phone or Personal Computer**: Since during the 2FA process you need to generate **passcodes (a six digit number)** automatically based on a secret key you and the 2FA system have exchanged, you need a program to perform this action. This program can either be on a Smart Phone or Personal Computer.

- **Verify your private email address**: We also need a private email address to mail you the verification email during the 2FA setup. Please contact the helpdesk to verify that your private email address is known and correct.

First time access:

- with a Smart Phone or
- with a Personal Computer
- remaining setup

Regular use of 2FA

WEB access

Each time you access a WEB page that needs authentication, you will have to go through the 2FA procedure. We do have Single SignOn set up, which means that once logged in onto the local Observatory WEBsite you do not have to re-login if you hit another page that needs authentication.

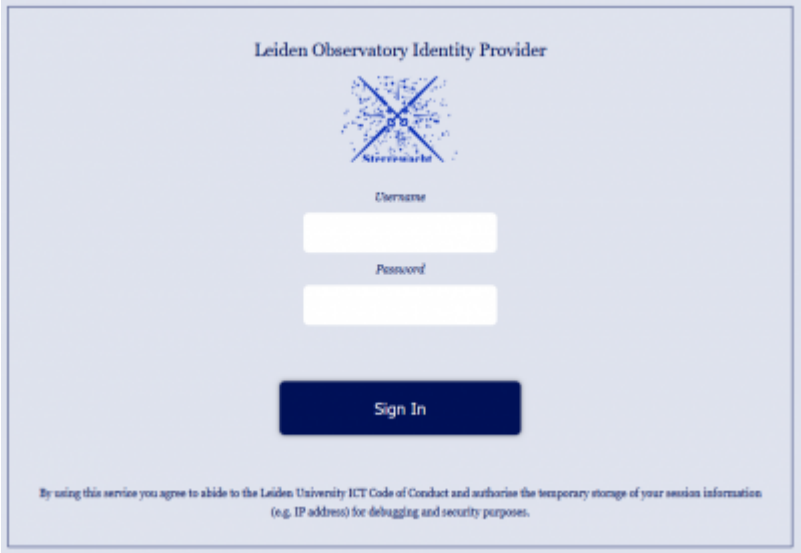

Figure 1: 2FA Main Login Screen (Click the image to enlarge).

You have already experienced the 2FA redirection when first setting up 2FA for your account. So this screen should now be familiar to you. Make note of the fact that in the first part of the URL of this form is hows that you have been redirected to our Identity provider: `idp.strw.leidenuniv.nl`. After successful login you are directed back to the original page you tried to access.

Fill in your STRW account credentials and click `Sign in`.

Figure 2: 2FA Codepass Confirmation Form (Click the image to enlarge).

You are now presented with the second authentication window asking for your passcode. So get your smart phone, open the authentication APP and find the block name `Leiden Observatory Intranet` and your account name. Click that block to obtain the passcode. Or execute your computer program to obtain a passcode.

Transfer the presented passcode into the WEB form. Then complete your login by clicking the `Sign in` button.

You should now end up at the page you tried to open in the first place.

In case of problems, look at the 2FA Problem section at the end of this page.

ssh

After you have setup your 2FA secret key the systems will know that you have done so and within a period of at most 30 minutes the `ssh` remote login, and all associated programs using this protocols such as `scp` and `sftp`, will start asking for your passcode as a second identity verification step.

Again it is straight forward to use 2FA in this case. Whatever program you use to ssh into the Observatory Computer system, you will be prompted for the passcode. So keep your smart phone or personal computer nearby always.

Here is a sample login:

```
# ssh <STRWComputer> -l <accountname>
Password:
One-time password (OATH) for `<accountname>':
    Welcome to the Sterrewacht Leiden workstations
    Access is allowed for authorized users only. Abuse will be tracked.

            Helpdesk     Room HL407          Tel 8444


Last login: Thu Mar  4 09:35:07 2021 from 132.229.xxx.yyy
```

where <STRWComputer> is the name of an Observatory desktop or server you want to access and <accountname> is the name of your Observatory account. At the `Password` prompt you provide your personal account password and at the `One-time password (OATH) for`

`<accountname>': prompt you enter the passcode you get from the smart phone APP or computer program.

That is all!

In case of problems, look at the 2FA Problem section at the end of this page.

Making ssh operations easier

Of course it is not very handy to have to authenticate each time you login between computers at the Observatory using the 2FA mechanism. Therefor, we have disabled 2FA for the case where you have implemented personal ssh keys. So if you setup ssh keys at the Observatory, you do not have to type in either your password, nor your passcode.

Setup ssh keys

Go to the how to setup sshkeys page for a detailed description on ssh key configuration.

Also read the generic dokuwiki page on ssh, section SSH Keys, on how to setup ssh keys in your Observatory account.

2FA Problems

Loss of or damaged to Smart Phone or Personal Computer

It might happen that you loose your smart phone or personal computer, or otherwise may be deprived of your secret key. In that case you need to perform the following actions to reset 2FA in the given order:

- Contact the Observatory helpdesk
- Reset your password
- Re-initiate the 2FA process as described above in the 'First Time Access' section

Error Message

If you see **Two-factor authentication has not been setup for your account <accountname> yet. Please refer to the computer documentation on the institute webpage for the description and setup of 2FA**, this means your secret code has not trickled down to this system yet. It may take up to 30 minutes after setting up 2FA before all Observatory systems know about your secret key. THus be patient ant try again in 30 minutes.

Code not accepted

Note that the passcodes have a lifespan of 30 seconds and that both the Observatory computers and

your Smart Phone or personal computer need to be in time sync. You must enter the 2FA app settings and select “**Time synchronisation**”. After this the codes should work again. You might also have been just a bit too late confirming your passcode. In that case repeat the process of creating the passcode en entering it into the prompt/web form.

In principle the system also allows passcodes that are from the previous or next timeslot. So you should have a total of 90 seconds to deliver a trusted passcode. This period is shortened if the Observatory time keeping differs slightly from your smart phone or personal computer time keeping.

Secret is compromised

You need to perform the following actions, in the given order, to reset 2FA and get a new key:

- Contact the Observatory helpdesk
- Reset your password
- Re-initiate the 2FA process as described above in the 'First Time Access' section