

Two-Factor Authentication (2FA)



Introduction

- Please read this document carefully or start from [here](#)

Why

After the recent increase in hacker activity and floods of phishing emails, it is clear that the Observatory Compute environment is under constant attack. One of the major deficiencies in our current setup is that it is enough to know a username and password to get access to a wide variety of resources and data. With the improper handling of phishing emails, but also when using public wifi services, it seems easy for people with not so good intentions to get account credential information. After that, there is no easy way to prevent misuse of accounts and computer resources.

We need to put a stop to that, and the only way to do that is to introduce a second step in identifying that you are the rightful owner of the account credentials. This second step is provided through the Two-Factor Authentication (2FA) mechanism. For this second verification, you need a physical device, for instance a smart phone or personal computer.

Where

In principle for every service where you need to identify yourself, 2FA is needed. In the beginning we will restrict 2FA to two major services: Web pages and ssh remote login. At a later stage 2FA will be implemented for other services as well. You will be informed well in advance.

WEB Pages & 2FA

For all Web pages where you need to login, we will enforce 2FA. This also, and in particular, includes webmail. The Observatory WEBSITE has many pages shielded by authentication and each page will be individually added to the 2FA facility.

ssh remote login & 2FA

One other major way to gain access to our resources and data is through the ssh protocol. So this means that using ssh to login from remote to the Observatory ssh gateway or to the local desktops or servers, you will be confronted with a second prompt to enter credentials. How this works is explained later on this page. In fact, 2FA is imposed on the ssh protocol, so scp, sftp, remote rsync and even tunnelier (Win) will also be affected.

How

The 2FA protocol that we have implemented is based on the Time-based One Time Password (TOTP) mechanism and we are using RedHat developed tools to implement this. TOTP means that for a limited amount of time you get a passcode, which you have to provide to the authentication program as a second 'password' to gain access to the resource. Initially, at first use of 2FA, you have been given a private secret key and have stored that on your mobile device. Then, for each login, you use that mobile device to generate (time limited) passcodes. This passcode you present (type in) to the login procedure and after verification it gives you access to the restricted resource. Details on this process are described below.

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.

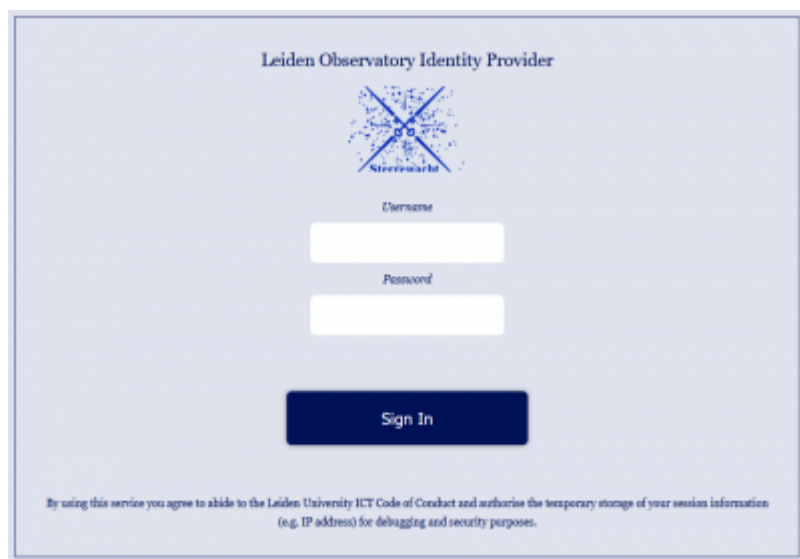
The image shows the 'Leiden Observatory Identity Provider' login screen. At the top is the title 'Leiden Observatory Identity Provider' and the STRW logo. Below the logo are two input fields: 'Username' and 'Password'. A dark blue 'Sign In' button is centered below the password field. At the bottom, there is a small line of text: 'By using this service you agree to abide to the Leiden University ICT Code of Conduct and authorize the temporary storage of your session information (e.g. IP address) for debugging and security purposes.'

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.

The image shows the 'Leiden Observatory Identity Provider' codepass confirmation screen. It features the same title and logo as Figure 1. Below the logo, it says 'Reauth login' and '(Six digit) One-time passcode'. There is a single input field for the passcode. A dark blue 'Sign In' button is at the bottom.

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. Therefore, 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

Please read the 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

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 might also have been just a bit too late confirming your passcode. In that case repeat the process of creating the passcode and 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

From:

<https://helpdesk.physics.leidenuniv.nl/wiki/> - **Computer Documentation Wiki**

Permanent link:

<https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=services:2fa&rev=1615797918>

Last update: **2021/03/15 08:45**

