Vera C. Rubin Observatory
Rubin Observatory Project Office

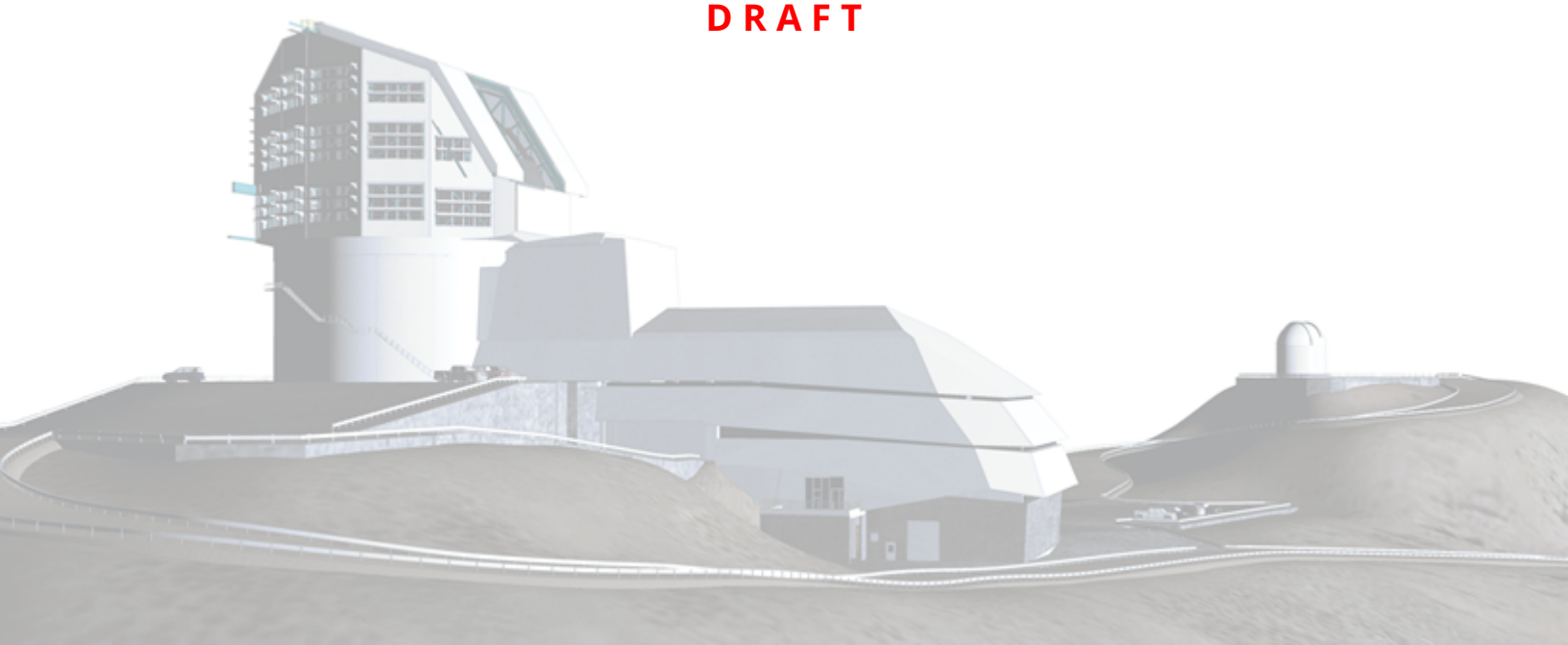
Securing VPN service with Multi-Factor Authentication

Hernán Stockebrand

ITTN-053

Latest Revision: 2021-11-15

DRAFT



Abstract

The Following documents details, alternatives to setup Multi-Factor authentication (**MFA**) for Rubin Observatory VPN users

Change Record

Version	Date	Description	Owner name
1	2022-11-22	Draft.	Hernán Stockebrand

Document source location: `https://github.com/lsst-it/ittn-053`

Contents

1 Introduction **1**

1.1 How Multi-Factor Authentication Works? 1

2 Requirements **2**

3 FreeIPA + OTP **3**

3.1 Test 5

4 DUO Authentication **6**

4.1 Test 7

5 Final Toughs **8**

A References **9**

B Acronyms **9**

Securing VPN service with Multi-Factor Authentication

1 Introduction

The MFA is a way of computer access control to secure data and applications, in a way that a user must prove with two or more ways his identity. It can be with a password, a time-based one-time password **(TOTP),** a digital certificate, or bio metrics.

Two-factor authentication **(2FA)** is a method that combines just two of the previously mentioned components. Multi-Factor authentication **(MFA)** combines more than two components.

MFA increases security because if just one of the credentials is compromised, the unauthorized user will not be able to know the MFA authentication requirement, and the access will be denied.

1.1 How Multi-Factor Authentication Works?

Because MFA needs at least two credentials at login to verify the identity before granting access. Each additional layer of authentication to the login increases security.

MFA requires the combination of the following:

- **Knowledge**- **Something you Know**: Password, pin, or answer to security questions
- **Possession**-**Something you Have**: Smart Card, Mobile token, hardware token.
- **Inherence** -**Something you Are**: Bio-metrics, voice recognition, fingerprint.

2 Requirements

The IT requirements are the following:

- Add and extra layer of security to the VPN connection.
- This can be an OTP or a "push" notification to an smartphone
- Compatibility with our systems
- Minor changes on our infrastructure for deployment
- Achieve regulatory compliance

3 FreeIPA + OTP

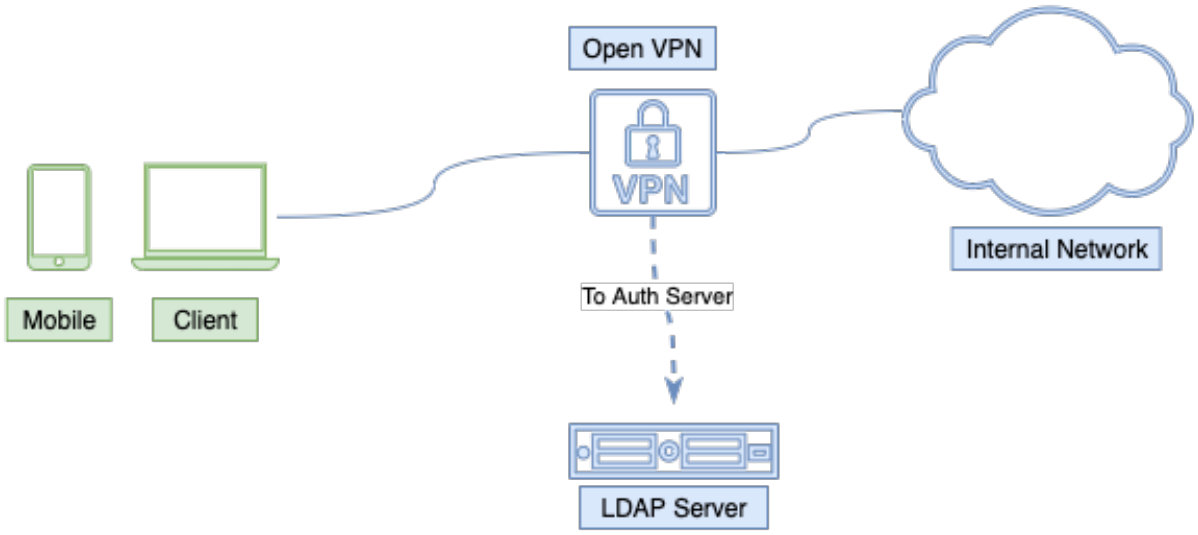


Figure 1: OpenVPN + FreeIPA Authentication Server

FreeIPA is a free and opensource Identity Managment System, aims to provide a centrally managed Identity, Policy and Audit (IPA)

FreeIPA native supports OTP authentication, and it can be enabled with just a few click inside a user profile, then a QR code is generated and is can be scan with an Smartphone with the app FreeOTP.

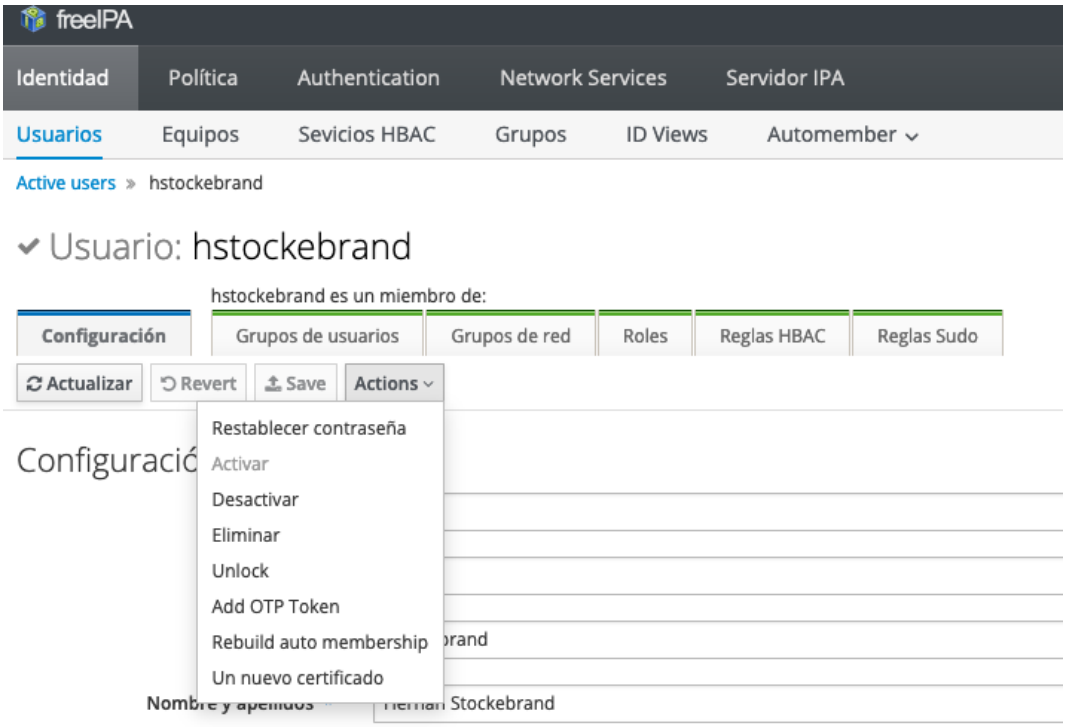


Figure 2: Enable OTP on IPA

Figure 3: QR Code to be Scan with the suggested app

No other change on any other service is needed, because this is transparent to the VPN service.

3.1 Test

In our test, when connecting with the VPN client, on this case OpenVPN Connect, there is no aditional field or box requesting the aditional OTP code, so the user password and OTP code must be write togheter on the password field, as the example shows on the next image

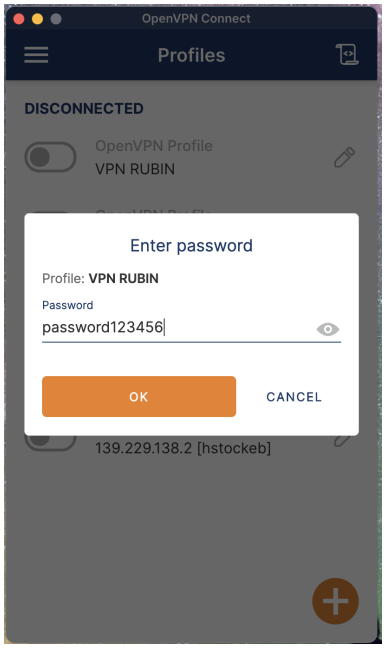


Figure 4: Password field on OpenVPN Connect client

The feature of a new field or a box requesting the OTP code is only available on the paid version of OpenVPN Acces Server. So this can be a litle confusing to users, due to the way to write the password and code on the same field.

4 DUO Authentication

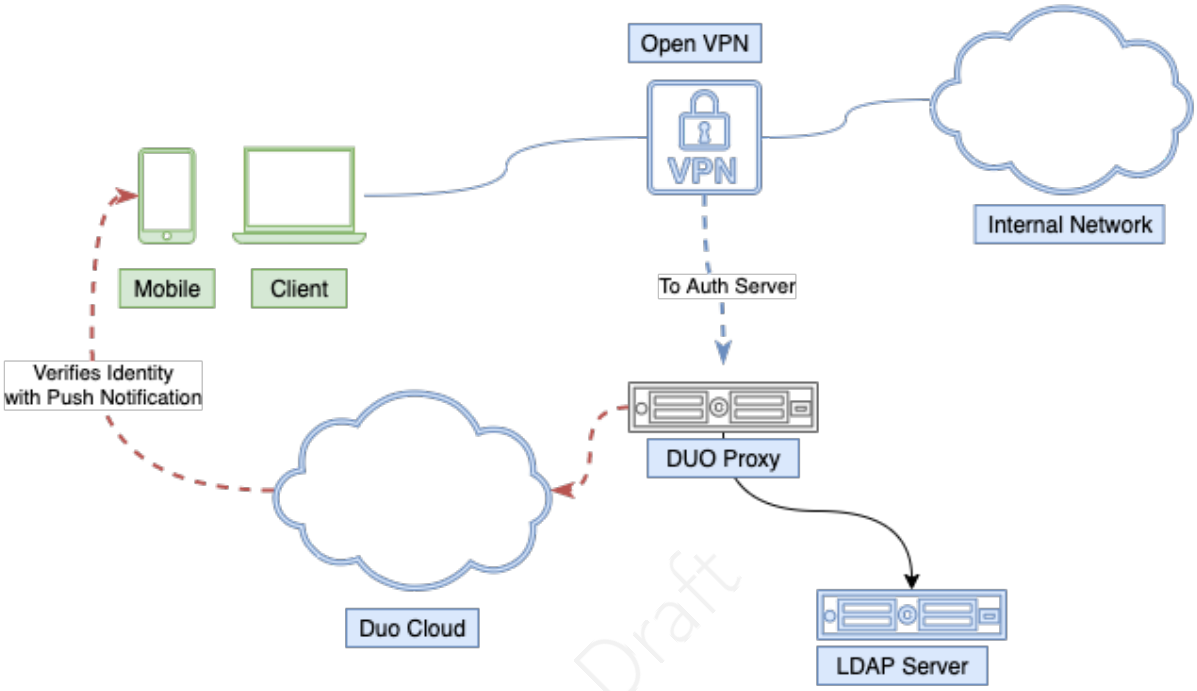


Figure 5: OpenVPN + DUO Proxy

Duo Security is a security platform that provides push notifications to authorize or deny a user log in, in our case, a VPN connection.

Users can be synchronized to the Duo Dashboard to automatically enroll users by sending a Welcome Email, letting the user install and sync the account with the app on his smartphone.

In this case, a service called "Proxy" needs to be installed on la machine inside the local network. On the OpenVPN configuration, a change is needed on the authentication servers, now it needs to be pointed to the proxy, so besides sending a LDAP request to the local LDAP server.

4.1 Test

Once everything is configured, we put the username and password account when we open a new VPN session. A push notification (on the user smarthphone) will ask if we are trying to log in on the named service in the next seconds. Now is possible to choose between allowing or denying. Once we press allow, the VPN connection is established.

5 Final Toughs

A References

B Acronyms

Acronym	Description
PMO	Project Management Office
VPN	virtual private network