True 2FA/MFA over SSH2/SFTP via keyboard-interactive authentication and Google Authenticator

> The technique explained in this article **requires WebClient, as well as scripting and event-handling** capabilities. Therefore, it can only be employed by customers who are running the Professional, Professional+WebClient, or Ultimate editions of our software. Furthermore, it requires a scripting function that is only available in Syncplify Server! v6.0.22+.

Every good system administrator knows that the SSH2 protocol (and, therefore, all of its subsystems, including SFTP) feature its own flavor of multi-phase authentication. But this is not what we're trying to accomplish with the technique explained in this knowledge base article.

What we're going to see is how to implement true 2FA/MFA via Google Authenticator (the same you use to log into the web UIs) by taking advantage of SSH2's keyboard-interactive authentication, and a little bit of scripting and event handling.

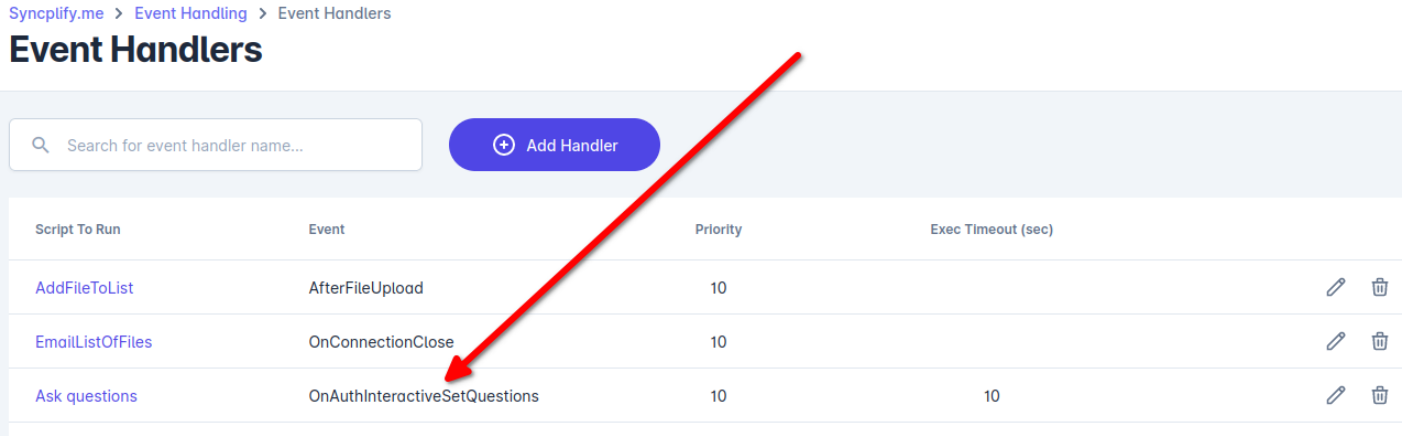
> Before we begin we need to make sure the user(s) that we want to go through this type of 2FA/MFA have actually **enrolled into Google Authenticator's 2FA via their WebClient!**

First of all we need to write a script to add the questions we want the user to be asked next time they try to log in. There are three possible types of questions, the example script here below shows them all:

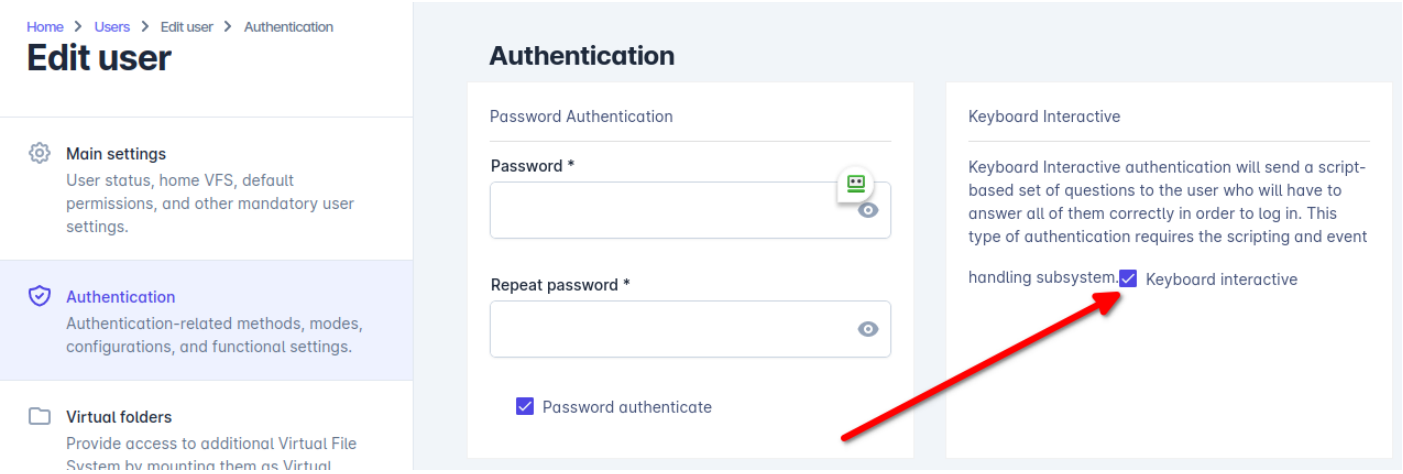
```
{
  // ask for user's password
  Session.AddQuestionPassword(0, "Password:");
  // then ask for [Google/Microsoft/...] Authenticator's current OTP
  Session.AddQuestionTOTP(1, "Authentication OTP:")
  // Finally ask a question with a pre-fixed answer
```

```
  Session.AddQuestion(2, "Your age:", 42, true);
}
```

Now we need to associate the above script to a very specific event handler: **OnAuthInteractiveSetQuestions**.

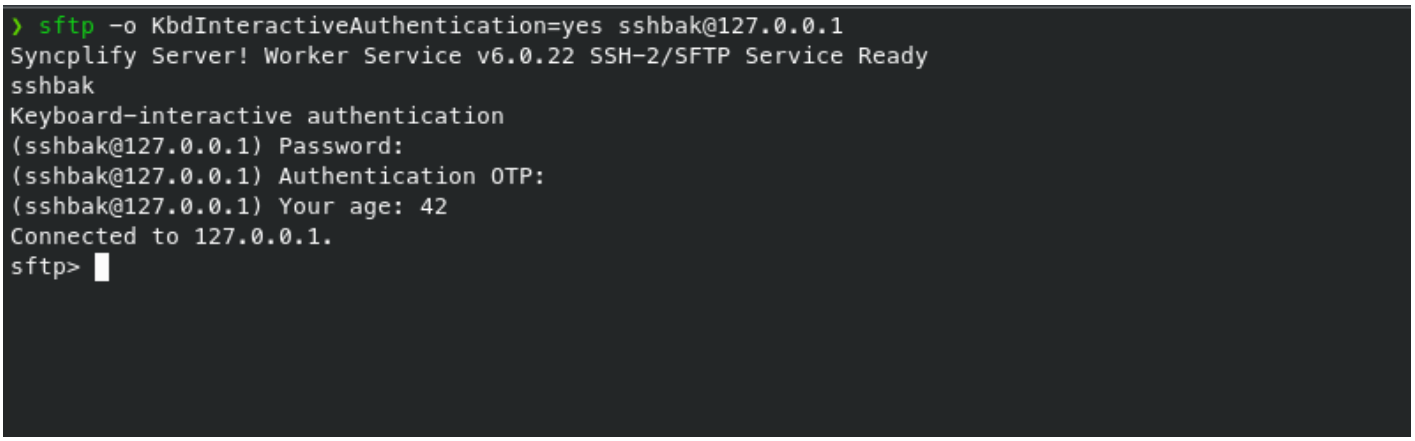


We also have to make sure that Keyboard-interactive authentication is enabled for the user(s) that we want to be able to log in this way:



> **IMPORTANT**: if this is the very first user you enable *Keyboard-Interactive* authentication for, at this point you will have to restart your Virtual Site, for the system service to activate KIA in its global authentication loop; a restart won't be needed for any other user, only for the first one.

And that's pretty much it. Next time the user tries to authenticate and attempts keyboard-interactive authentication, this is what happens:



Questions answered correctly, user logged in. Yay!

Revision #6
Created 12 March 2023 19:20:53 by DevTeam
Updated 26 September 2024 13:08:22 by DevTeam