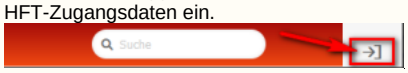
Multifaktor-Authentifizierung - Multifactor Authentication

Anleitungen zur Multifaktor-Authentifizierung (MFA)

Zur Einrichtung der Multifaktor-Authentifizierung, müssen Sie sich in den Räumen der HFT Stuttgart im hochschuleigenen Netz befinden!

Anleitung

Um sich erstmals ins Wiki einzuloggen, müssen Sie sich an einem Rechner an der HFT befinden oder das WLAN (Eduroam oder HFTwlan) der HFT nutzen.
Anschließend loggen Sie sich bitte oben rechts mit Ihrem HFT-Zugangsdaten ein.



Dann werden an dieser Stelle die entsprechenden weiterführenden Anleitungen zur MFA sichtbar:

Bei Auslandssemester oder Krankheit kann die Freischaltung der Multifaktor-Authentifizierung per E-Mail an ist@hft-stuttgart.de beantragt werden. Dazu senden Sie uns eine **Kopie der Vorderseite Ihres Personalausweises** und den ausgefüllten **Antrag** auf Freischaltung der Multifaktorauthentifizierung mit.

Was bedeutet Multifaktor-Authentifizierung?

Sie haben möglicherweise schon Erfahrung damit gemacht, beispielsweise bei Ihrem Online-Banking oder bei der Anmeldung bei Microsoft Office 365 oder Teams. Bei der Anmeldung in einer Online-Anwendung müssen Sie zusätzlich zu Ihrem Benutzernamen und Passwort einen zweiten Faktor eingeben.

Warum wird Multifaktor-Authentifizierung eingesetzt?

Heutzutage reicht der Schutz von Benutzernamen und Passwort allein nicht mehr aus, um den Zugriff auf Online-Anwendungen und die darin enthaltenen Informationen zu schützen. Die HFT bleibt auch nicht vor Cyberangriffen verschont. Aus diesem Grund werden relevante Online-Anwendungen mit sensiblen Daten und Informationen schrittweise mit Multifaktor-Authentifizierung gesichert.

Sie können aus verschiedenen zweiten Faktoren auswählen, die Sie verwenden möchten. Auf Ihrem Smartphone können Sie beispielsweise eine Authenticator-App oder eine Code-Zustellung per SMS verwenden. Alternativ ist auch die Verwendung eines Hardware-Tokens möglich, der derzeit jedoch nur für Mitarbeitende im Verwaltungs-VPN verfügbar ist. Ab 2023 wird die Nutzung von Hardware-Token schrittweise für alle Mitarbeitende eingeführt.

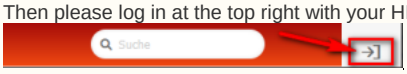
Instructions for multi-factor authentication (MFA)

To set up Multifactor Authentication, you must be on the HFT Stuttgart premises in the university's own network!

Instruction

To log in to the wiki for the first time, you must be connected to a computer at the HFT or use the HFT WLAN (Eduroam or HFTwlan).

Then please log in at the top right with your HFT access data.



The corresponding further instructions for MFA will then be visible here:

In the event of a semester abroad or illness, activation of multi-factor authentication can be requested by e-mail to ist@hft-stuttgart.de. To do this, please send us a **copy of the front of your ID card** and the completed **application** for activation of multi-factor authentication.

What does multi-factor authentication mean?

You may have already experienced it, for example, in your online banking or when logging into Microsoft Office 365 or Teams. When logging into an online application, you need to enter a second factor in addition to your username and password.

Why is multi-factor authentication used?

Nowadays, relying solely on usernames and passwords is no longer enough to protect access to online applications and the information contained within them. Even HFT is not immune to cyber attacks. For this reason, relevant online applications with sensitive data and information are gradually being secured with multi-factor authentication.

You can choose from various second factors that you want to use. For example, you can use an authenticator app or code delivery via SMS on your smartphone. Alternatively, it is also possible to use a hardware token, which is currently only available for employees in the administrative VPN. From 2023, the use of hardware tokens will be gradually introduced for all employees.