
YUBIKEY – SET-UP AND USE

Table of Contents

Revision History.....	i
Introduction.....	1
System Requirements.....	1
Purchasing the YubiKey.....	1
Activating Two-Factor Authentication.....	2
Using the YubiKey.....	4
Disabling a YubiKey.....	4

Implementing YubiKey

Revision History

Date	Revision Number	Revision Class¹	Comments
9/19/2014	1.0	Initial	Initial document release.
6/9/2016	2.0	Major	Updated new requirements and changed document format.
3/9/2017	2.1	Minor	Rebranding IAS to HAS

- ¹ Initial: Initial issue of document.
Minor: Minor updates (e.g., editorial, minor system updates)
Major: Significant updates

YubiKey Set-up and Use

Introduction

HAS provides the option for your firm to implement two-factor logon authentication using the YubiKey from Yubico.

Two-factor authentication is a logon process with enhanced security. Regular authentication is usually based on a user name and password. Two-factor authentication introduces an additional component. This is usually a hardware device that generates a one-time security token, and can either be keyed in or the device can be connected to the user's computer to provide it.

The YubiKey is a hardware device that uses the Advanced Encryption Standard (AES) encryption algorithm and generates a one-time token. The token is time encoded, which provides time-out ability so that copy/paste actions or key loggers aren't able to reuse the token at a later date.

System Requirements

Our system requires that the YubiKey has One-Time Password (OTP) functionality. The following models include this functionality:

- YubiKey 4
- YubiKey NEO

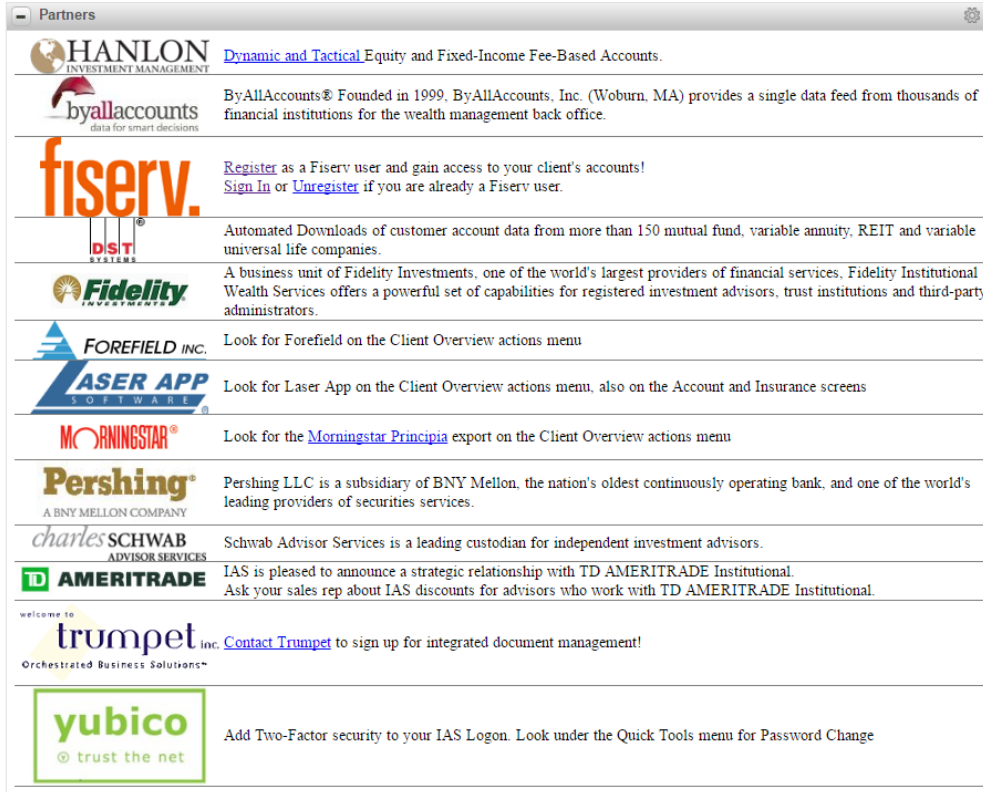
One-Time Password (OTP) is a password that is valid for a single use and, once used, cannot be used again for authentication. A Yubico OTP is a unique sequence of characters generated every time the YubiKey button is touched. It is comprised of a sequence of 32 Modhex characters representing information encrypted with a 128 bit AES-128 key.

Purchasing the YubiKey

The YubiKey is available for purchase from the Yubico website. The Dashboard **Partners** widget provides a link to the site where you can begin the purchase process.

- 1) Logon to the HAS Host.
- 2) On your Dashboard, locate the **Partners** widget and then click on the Yubico icon.

YubiKey Set-up and Use



3) Navigate the site to select and complete your purchase of the YubiKey.

Activating Two-Factor Authentication

Once you receive your YubiKey, you need to activate two-factor authentication within HAS.

- 1) Logon to the HAS Host.
- 2) Select **Password Change** from the **Quick Tools** dropdown menu. The **Change Password** page displays.

The screenshot shows the "Change Password" page. It features a large empty text box at the top. Below it, the text "Change Password" is displayed in green. There are three input fields: "Old Password", "New Password", and "Retype Password". A blue button labeled "Change Password" is positioned below the input fields. At the bottom of the page, there is a link that says "Click here to manage your 2-factor authentication key." with a small green box highlighting the text "Click here".

YubiKey Set-up and Use

- 3) Click the **here** link to manage the 2-factor authentication. The **2-Factor Key Setup** page displays.

2-Factor Signon Setup

Currently we support the Yubikey from Yubico.

In order to enable or disable the 2-Factor security, you must currently have the hardware key in hand.


Please enter your current password. Then place the cursor in key 1 and activate your Yubikey. Then select key 2 and activate your Yubikey a second time. Why do we ask for it twice? To make sure you actually have the key and are not copy/pasting the value.

Password:

Key 1:

Key 2:

Enable the above Yubikey for this account.



- 4) Follow the following instructions to activate your YubiKey:
- a. Enter your password in the **Password** field.
 - b. Place your cursor in the **Key 1** field and insert the YubiKey into the USB port of your computer.
 - c. Place your thumb or finger on the gold disc of the YubiKey. The **Key 1** field will fill in automatically.



- d. Place your cursor in the **Key 2** field and insert the YubiKey into the USB port of your computer.
 - e. Place your thumb or finger on the gold disc of the YubiKey. The **Key 2** field will fill in automatically.
- 5) Check the **Enable the above YubiKey for this account.** checkbox.
- 6) Click **Submit**.
- 7) Your HAS system is now enabled with two-factor authentication.

NOTE

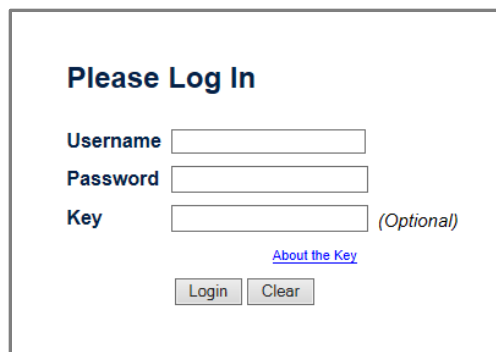
To disable two-factor authentication, the checkbox will display **Disable the above YubiKey for this account**. Check this box to disable the use of two-factor authentication.

YubiKey Set-up and Use

Using the YubiKey

Following are the steps for using YubiKey:

- 1) Insert the YubiKey into a USB port.
- 2) The device identifies itself to Windows as a Human Interface Device (HID). There is no need for any drivers or other software to be installed. After Windows accepts the device, the green ring around the activation button lights up.
- 3) Input your user name and password.



Please Log In

Username

Password

Key (Optional)

[About the Key](#)

- 4) Place your cursor in the **Key** field and touch the button on the YubiKey. A one-time password/token will be generated and an enter keystroke will be submitted.
- 5) On the server side,
 - a. Using web services, HAS contacts the Yubico server and validates that the token is good.
 - b. The time is returned and encrypted in the token. The time can be validated to ensure that the token was generated in a timely fashion.

Disabling a YubiKey

If you have lost your YubiKey or need it disabled, your firm's system administrator needs to submit an HAS help ticket requesting that the YubiKey be deactivated for your login.