How do I register my YubiKey for use with Duo 2FA?

Q: How do I register my YubiKey for use with Duo 2FA?

- How can I register my hardware token for use with Duo?
- Can I use a hardware token with Duo 2FA?

Context

You can use a Yubikey USB hardware token to generate a One Time Passcode (OTP) for use with Duo. This is useful if you don't have a smartphone, prefer a physical token for your second factor, or as a secondary backup option in case you don't have access to your phone.

> If you would like to request a Yubikey, please submit the Yubikey Request Form.

Registering a Yubikey with Duo Security requires two steps:

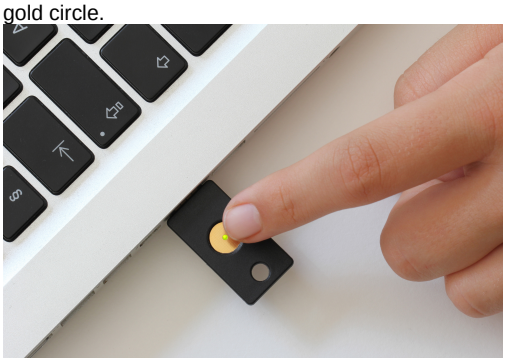
- Configuring the Yubikey hardware token
- Registering it with Duo Two-Factor authentication

Configuring the Yubikey hardware token

> The following steps will erase and reconfigure your Yubikey. If you received a new Yubikey from IS&T, it is safe to follow the steps. If you already had your own Yubikey and were using it for non-MIT services, be aware that erasing and reconfiguring your Yubikey will probably make it stop working for your other services. For safety we recommend getting a new Yubikey from IS&T.
>
> It should be possible to use a single Yubikey for multiple services if you:
>
> - Remove the Yubikey from all services that use it.
> - Reconfigure it following the instructions below.
> - Upload the configuration information to Yubico at https://upload.yubico.com/
> - Upload the configuration information to MIT's Duo portal: Registering it with Duo Two-Factor authentication
> - Re-attach the Yubikey to your other non-MIT services.
>
> IS&T does not support the above steps, and will not be able to help if things don't work. Using a single Yubikey with multiple services (MIT/Duo and non-MIT/Yubico) weakens the security of the key. IS&T recommends getting a dedicated Yubikey for MIT/Duo logins.

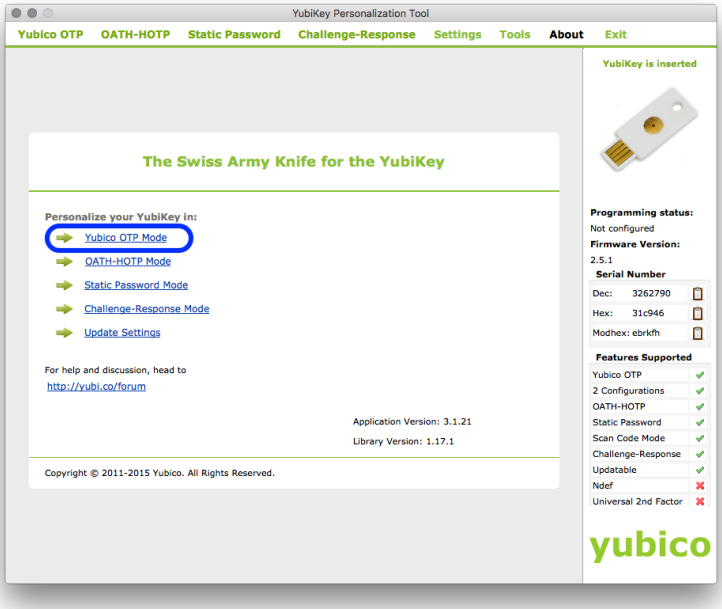
To configure your Yubikey with One Time Passcode:

1. Download and install the **Yubikey Personalization Tool** from the Yubico website.
2. Once installed, insert your Yubikey into the USB port. Verify it is plugged in correctly by the solid/blinking green light in the middle of the gold circle.

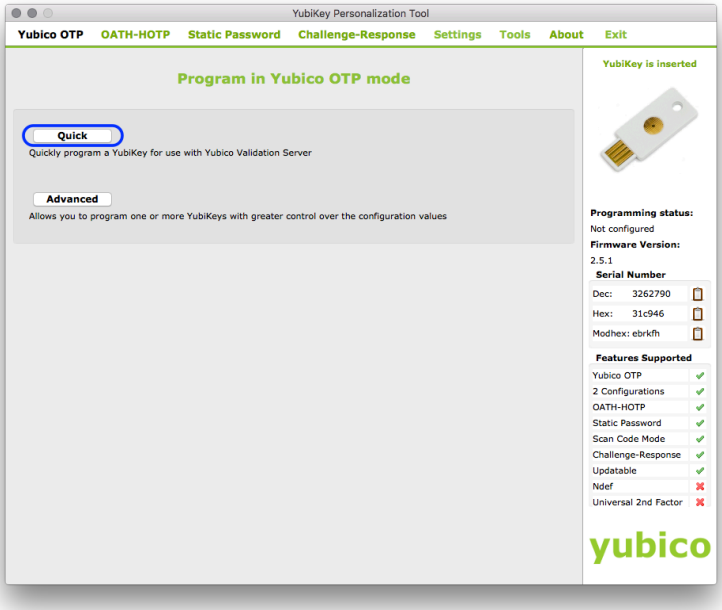


Mac OS X users might encounter a prompt to set up a new keyboard the first time a Yubikey is connected. If you encounter this prompt, close the window and continue with the setup.

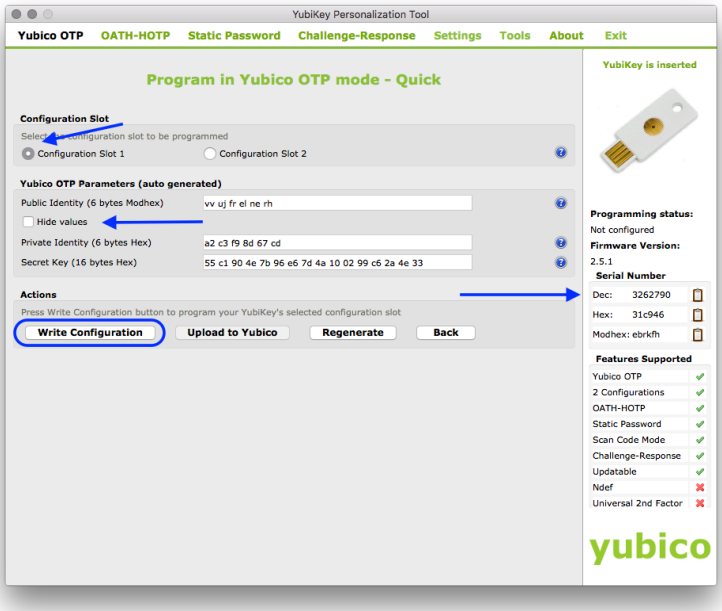
3. Open the Yubikey Personalization Tool. Under **Personalize your Yubikey in** select **Yubico OTP Mode**.



4. Select **Quick** for program mode.

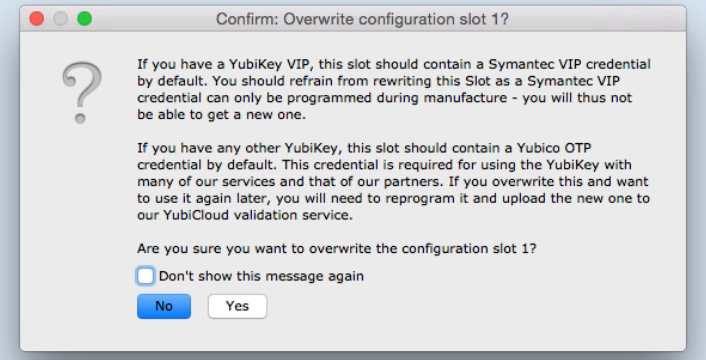


5. Next, select **Configuration Slot 1** and *uncheck* the **Hide values** box to reveal the Private Identity and Secret Key.
6. Click **Write configuration**.

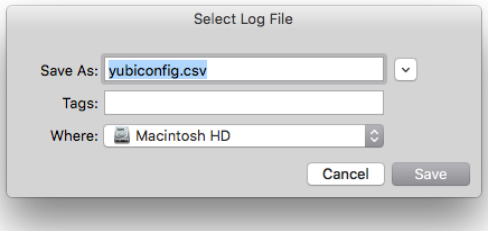


Keep this window and information open in order to register your token with Duo

Some users may encounter the following warning about overwriting the configuration in Slot 1. This is normal as some Yubikeys come pre-configured with YubiCloud credentials in slot 1.



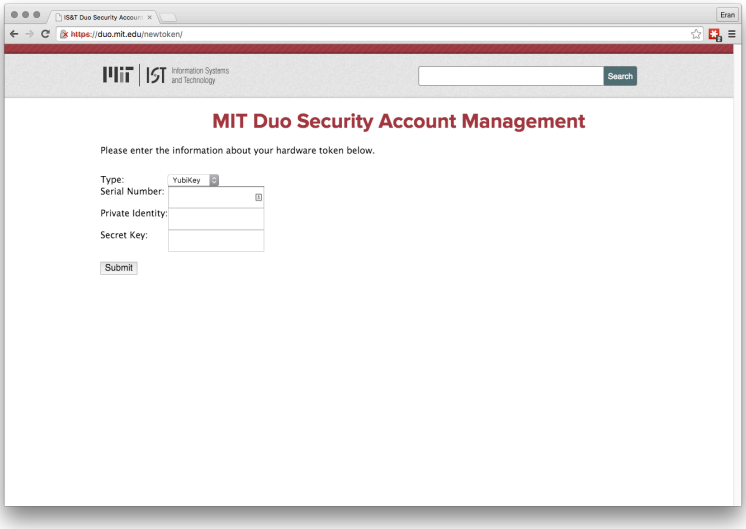
7. You **may** be prompted to save the log file.



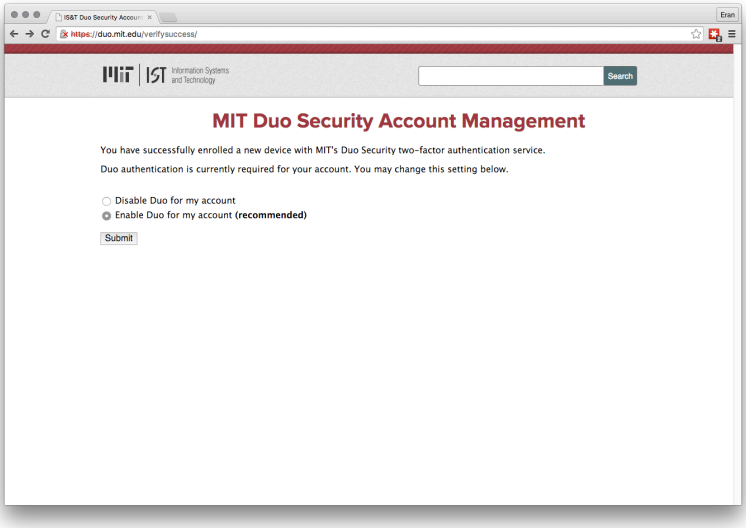
Registering it with Duo Two-Factor authentication

Once you have the token configured, you can add it to your Duo devices:

1. Navigate to https://duo.mit.edu.
2. Once signed in, click on **Register a new hardware token**.
   Result: You are brought to the registration page.



3. Make sure the appropriate token type is selected. For any model YubiKey, select **Yubikey**.
4. Enter (copy & paste) the **Serial Number** (in Decimal format), **Private Identity**, and **Secret Key** you generated when configuring your Yubikey and select **Submit**.
   Result: You will be returned to the Duo settings page with a message saying the enrollment was successful.



You can now test your hardware token by authenticating to an MIT service..

Troubleshooting

If you repeatedly get the error "Invalid Yubikey private ID or secret key." when attempting to register a YubiKey, you might inadvertently have two configurations set up in your YubiKey and be triggering the wrong one during verification. Recent models of YubiKeys can store two configurations: you trigger the first by a short press of 0.3-1.5 seconds, and you trigger the second by a long press of 2.5-5 seconds. YubiKeys are easier to use if only configuration 1 is set up, so you should delete configuration 2 if you are certain that nothing else needs it.