Introduction

Yubico is the leading provider of simple, open online identity protection. The company's flagship product, the YubiKey®, uniquely combines driverless USB hardware with open source software. More than a million users in 100 countries rely on YubiKey strong two-factor authentication for securing access to computers, mobile devices, networks and online services. Customers range from individual Internet users to e-governments and Fortune 500 companies. Founded in 2007, Yubico is privately held with offices in California, Sweden and UK.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Trademarks

Yubico and YubiKey are trademarks of Yubico Inc.

Contact Information

Yubico Inc
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
USA
info@yubico.com
## Contents

- Introduction ........................................................................................................................................... 2
- Disclaimer .............................................................................................................................................. 2
- Trademarks ............................................................................................................................................ 2
- Contact Information .............................................................................................................................. 2
- Setting up the Chrome Browser for U2F ............................................................................................ 4
- Registering your U2F Demo Account .................................................................................................. 6
- Logging into the Demo U2F service ..................................................................................................... 10
1 Setting up the Chrome Browser for U2F

The Google Chrome team is working to include U2F support natively in the Chrome Browser. However, today the current version of the U2F implementation requires an external App and an Extension. The Chrome browser setup will only be needed to be done once, and once U2F is fully integrated into the Chrome browser, will not be necessary.

The first step is to check and install any required U2F components to your Chrome browser. This can be easily done on a PC or a Mac by directing your Chrome browser to the following URL: [http://demo.yubico.com/u2f](http://demo.yubico.com/u2f)

If no U2F components are already installed on your Chrome browser, a Red box (like the one shown above) will indicate what is missing and provide links to install the U2F App and/or the U2F Extension.

Installing the U2F App and Extension will require logging into your Google/Gmail account, as well as user confirmation for each.
Once your Chrome browser has both the U2F App and Extension installed, return to http://demo.yubico.com/u2f. The red box should no longer be displayed.
2 Registering your U2F Demo Account

Once your Chrome browser is set up to handle U2F, the next step is to create an account and register a U2F device with the U2F Demo site.

First plug in your U2F Enabled YubiKey NEO into a USB port on your PC, and direct your Chrome browser to http://demo.yubico.com/u2f. On the Demo site, register with the U2F demo by typing in a username and either a PIN or a short password, then clicking “Next”. If you are attempting to register a username that is already in use, you will be instructed that it is not available.
On the first use of the U2F Demo site, Chrome may pop up a warning bar, asking if you want to allow the web site to access your U2F device (shown below). Click “Allow” to proceed.

At this point, a dialog will pop up asking for permission to access your U2F device connected to your USB port. Click the Button “Request device permission” and “Allow” to proceed.

If your U2F YubiKey NEO is not plugged into the USB port on your PC at this time, you will get a “Registration failed” error. To proceed, simply plug your U2F YubiKey NEO into your PC.
and register your username and PIN again.

If a U2F enabled YubiKey is present, a dialog will open asking the user to touch the Gold button on their U2F YubiKey NEO to proceed.

Touching the button on the U2F enabled YubiKey NEO will generate a new public/private key pair your NEO, with the response sent to the server.

Your U2F enabled Account is now created on the demo service. The technical details on the transaction can now also be viewed:
The following data shows information about the registration that just took place. After supplying your username and password, the server created a new enrollment. This enrol data was then presented to your device. When you approved the device, a new keypair was generated on your U2F device, and the public key was sent back in the response data to the server. The server has now stored that data and is ready to challenge the device when you log in.

Hover over the values for additional information.

**Login Data**
- **username**: CES
- **password**: 123

**Enroll Data**
- **v0**: BNWjR8d5CSM5-u-03kj2Z-46_cjIiZa6wY8HE5Lb-5F7h_zViVAc2nMXsD5111t6TL5dK78z5kIKEvJW08io=

**Response Data**
- **version**: 0
- **dh**: 8Awg1p0h6Nv50T6c6k8Ofo_0_9MxY3H9h65S10tbng047A2zq2Y-1FL0oVDj1lQVS6ooQ2vOB8zKevJ5W5g1=

**GMR**
- **UUsu73kJmFec-U1u8D5xtwoTQDn1nEwVqGlAll_S6r3x44DiSxkAQBNY3L5VqE8k3JXUL880wMNwurQKF3J5vJLSe
cpO02znjFtx5revnna3Y29oB5L1zweV4V2ZioF1gGz6XkD3L1QFQSWm6K63suvMichelleINwCk211P1yY36o6zX7YFustC1A9qKb
3411NVYqVt3m3P8nWw7qB3elv1a1WDQd9nfw6w2xh41wv3m6gwPbXk4x1348065_198_2x9t8NvnrQRGzMy1Z

**JSON**
- **username**: CES
- **password**: 123
- **v0**: BNWjR8d5CSM5-u-03kj2Z-46_cjIiZa6wY8HE5Lb-5F7h_zViVAc2nMXsD5111t6TL5dK78z5kIKEvJW08io=

**Attestation Certificate**
- **Date**: 2012-07-23 12:59:59 GMT
- **Subject Public Key Algorithms**: id-ecPublicKey
- **pub**: 04:11:01:83:46:58
- **Signature Algorithm**: edcsa-with-3SHA256
- **Issuer**: CN=Google Root
- **Not Before**: Jun 1 00:00:00 2012 GMT
- **Not After**: May 31 23:59:59 2032 GMT
- **Subject**: Dl6f5uST5Y.0ZK-FA35PlmWvAM2012-P6f0.3c5u2s5u6

---BEGIN CERTIFICATE-----
MIIBQgIBAgIgAgEBcAgEBk8zIza3Y29oB5L1zweV4V2ZioF1gGz6XkD3L1QFQSWm6K63suvMichelleINwCk211P1yY36o6zX7YFustC1A9qKb
3411NVYqVt3m3P8nWw7qB3elv1a1WDQd9nfw6w2xh41wv3m6gwPbXk4x1348065_198_2x9t8NvnrQRGzMy1Z
---END CERTIFICATE-----
3 Logging into the Demo U2F service

Once you have register an account with the Demo U2F service, you can demo the U2F Login experience.

First, go to http://demo.yubico.com/u2f, if not already there. Select the tab labeled “Login” and

On the Login section, type in the username and PIN/Password registered for your account, then click the “Login” button.
After clicking Login with a valid Username and PIN/Password, you will be taken to a page asking to Login with your U2F device.

Plug in your U2F enabled YubiKey NEO, and touch the gold button on it when prompted by the webpage:

After Authenticating the U2F NEO, the U2F demo page will report a successful Authentication: