

Yubikey module for ImpressCMS

Purpose

The Yubikey module improves some aspects of account security on ImpressCMS websites. It allows two-factor authentication to be enforced on designated user accounts using Yubikey hardware tokens. Since use requires purchase of a hardware token, it is most appropriately used to protect admin accounts.



Generating a one-time password with a Yubikey...insert to USB port, press the button and you're done.

Single-factor authentication vs two-factor authentication

A standard ImpressCMS install requires users to provide their password to login. This is single factor authentication ('something you know'). While this is the most common form of authentication in use today, it is also the most vulnerable: Anyone who knows your password, or who can steal it or guess it can login to your account. It is a fact that most people use weak passwords that are easy to brute force. It is also very easy to 'eavesdrop' on passwords being sent over the network, particularly from unencrypted wireless connections. Ever had an email from a friend who is 'travelling and lost their wallet' in need of a loan? What they actually lost was their password.

The Yubikey module adds another layer of security to protect your account in the event your password is compromised. It does this by requiring a second form of authentication: A one-time password (**OTP**) generated by a Yubikey hardware token ('something you have'). Both credentials are required to login to your account; either one alone is useless. This means that an Evildoer that steals your password doesn't have enough information to login. Similarly, a lost Yubikey can't be used to login to your account, because it is no good without the password. As its name suggests, a one-time password is only good for one session and becomes invalid once used.

How it works

Yubikeys and one-time passwords

A Yubikey is a small USB device about the same size as a regular house key which plugs into standard USB ports. There is no need to install drivers and you can use it anywhere, as it emulates a USB keyboard. It features a single button that emits a one-time password when pressed.

The one-time password contains a secret identity field unique to the key, a counter that increments each time the key is used, a 24-bit timer, a 16-bit random number and a CRC16 checksum of all fields. It is encrypted with AES-128 using a key that is embedded in the device, so the password can safely transit the network. For more information, see the Yubikey Manual:

http://static.yubico.com/var/uploads/pdfs/YubiKey_Manual_2010-09-16.pdf



Yubikeys are very convenient to carry around and weigh a mere 2.5 grams.

The Yubikey module

The Yubikey module allows you to associate Yubikeys with user accounts (see section on module set up). When a user attempts to login, the module checks to see if their account requires two-factor authentication. If so, the user is redirected to an alternative login page, where they must enter i) their regular account password and ii) a one-time password generated by their Yubikey.

The Yubico validation server

When a Yubikey-enabled account login is submitted, the Yubikey module contacts the Yubico validation servers over an encrypted connection, using a pre-shared API key to authenticate (see section on module set up). It hands off the one-time password supplied by the user to the validation server, which decrypts it and validates the contents. The validation servers track the private ID and counter fields and inspect the checksum to guard against replay attacks and modification. The validation server returns a response (OK or various error messages) to the Yubikey module depending on the result. If the result is good, ImpressCMS proceeds to validate the regular account password as well. Only if both passwords are good is the user permitted to login.

Note that the Yubikey module cannot decrypt the one-time password supplied by the user, that function is carried out by the Yubico validation server, which has a copy of the symmetric encryption key embedded in the hardware token. Validation requests expire after a period of time that can be set in the module preferences (default is 10 minutes).

If you would be more comfortable controlling your own validation server, you can. Several open source Yubikey validation server projects are available: <http://yubico.com/validation-server>. You can also flash a new encryption key into your Yubikey, if you are particularly paranoid (utility available at Yubico website).

Requirements

1. You **must** own at least one Yubikey hardware token to use this module. You can buy them from Yubico (www.yubico.com). They cost about US\$25 each but you can often get them slightly cheaper if you search online for a coupon code. You should probably get a spare, too.
2. Your webserver **must** have cURL installed, as this is used to communicate with Yubico's validation servers.
3. You **must** get a client ID and API key from Yubico (see Set up, below) or the module cannot operate.

Installation

Overwrite the file `/include/checklogin.php` with the modified version bundled with the module, which you will find in the `yubikey/extras` folder. This includes a section of code that checks if an account is Yubikey enabled. If you forget to upload this, the module will not work.

Secondly, install the yubikey module as per the standard ImpressCMS procedure. Upload it to the `/modules` folder of your site, visit the module administration area of the control panel and press the action button to install it.

Finally, you **must** ensure that your website 'server timezone' preference (system => preferences => general settings) and server clock are correct, as some aspects of this module are time sensitive.

Set up

The Yubikey module must be configured before it can operate. The essential steps are as follows:

1. Get a Client ID and API key from Yubico

Visit the Yubico API key generator website at the link below. Enter your email address and discharge your Yubikey in the one-time password field. You will be presented with a client ID and an API key, which you must record and keep secret: <https://upgrade.yubico.com/getapikey/>



Here you can generate a shared symmetric key for use with the Yubico Web Services. You need to authenticate yourself using a Yubikey One-Time Password and provide your e-mail address as a reference.

Your **e-mail** address:

YubiKey **one-time password**:

You need to get an API key from <https://upgrade.yubico.com/getapikey/>.

2. Enter your Client ID and API key in the module preferences

Visit the preferences page for the Yubikey module. Enter your Client ID and API key in the fields provided and submit the form. The module is now ready for use.

I recommend to leave the timestamp tolerance and cURL timeout preferences at the defaults. The timestamp tolerance is the acceptable time difference in seconds between a validation request and the local time of your webserver. Validation requests will be refused if the time difference exceeds this value. You want to keep it as low as practical, but you also need some leeway to account for discrepancies between clocks on different machines. The cURL preference is essentially how long your website will try to contact the Yubico validation server before it gives up.

Yubikey >> Preferences

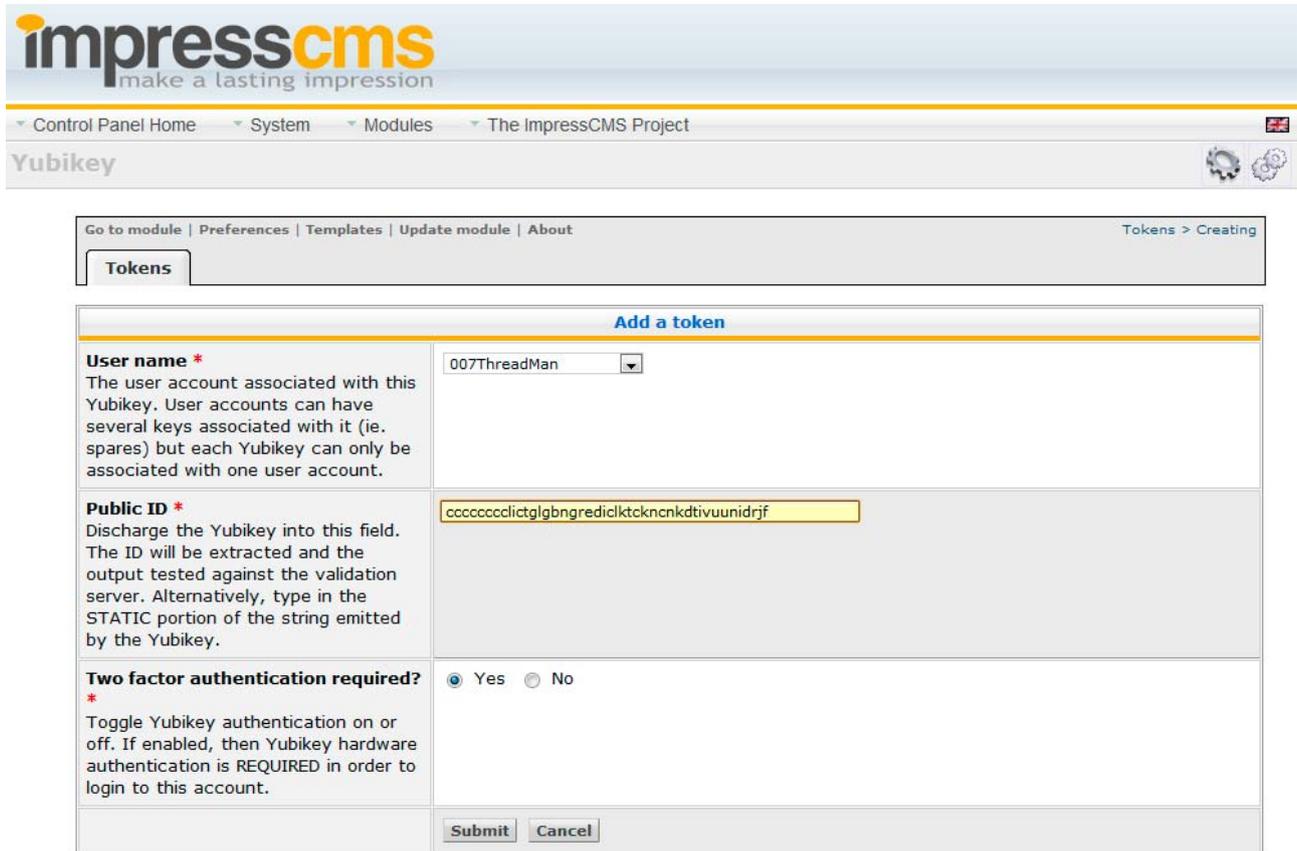
Module Config Options	
Yubikey client ID	<input type="text" value="8477"/>
Yubikey secret API key	<input "="" type="text" value="eGWriyKECGcZmeT8Y3LBRzny2Yj="/>
Timestamp tolerance (+/-seconds)	<input type="text" value="600"/>
CURL timeout (seconds)	<input type="text" value="10"/>
Show breadcrumb?	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Go!"/>	

Enter your Client ID and API key in the module preferences.

3. Register your Yubikey(s)

Click the 'add token' button. Select the user account you want to associate with a given Yubikey. Then discharge the Yubikey into the Public ID field. It's that easy!

Repeat for each account/key that you want to set up. One user account can have multiple keys associated with it (eg. spares), but each key can only be associated with one user account.



The screenshot shows the ImpressCMS interface for registering a Yubikey. The page title is "Yubikey". The navigation menu includes "Control Panel Home", "System", "Modules", and "The ImpressCMS Project". The main content area is titled "Add a token" and contains the following fields:

- User name ***: A dropdown menu with "007ThreadMan" selected. The description states: "The user account associated with this Yubikey. User accounts can have several keys associated with it (ie. spares) but each Yubikey can only be associated with one user account."
- Public ID ***: A text input field containing "ccccccclctglgbngrediclkckncnkdtivuunidrj". The description states: "Discharge the Yubikey into this field. The ID will be extracted and the output tested against the validation server. Alternatively, type in the STATIC portion of the string emitted by the Yubikey."
- Two factor authentication required? ***: Radio buttons for "Yes" (selected) and "No". The description states: "Toggle Yubikey authentication on or off. If enabled, then Yubikey hardware authentication is REQUIRED in order to login to this account."

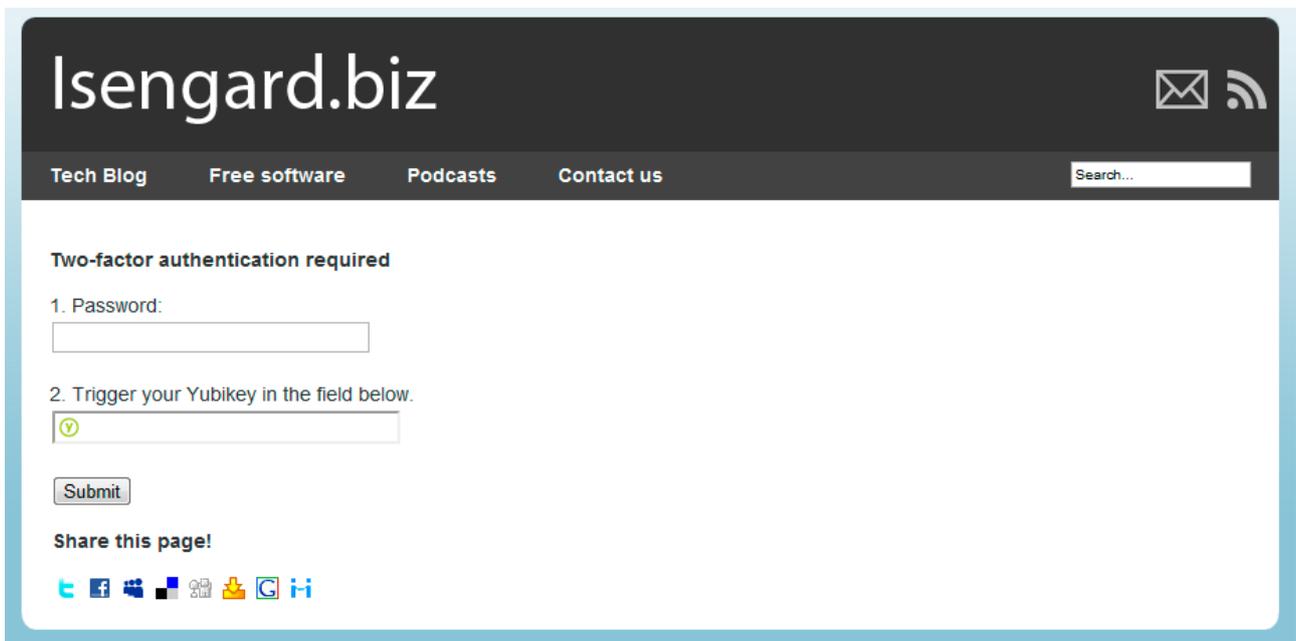
At the bottom of the form are "Submit" and "Cancel" buttons.

Register a Yubikey: Select the user account to associate with the key and discharge it in the Public ID field.

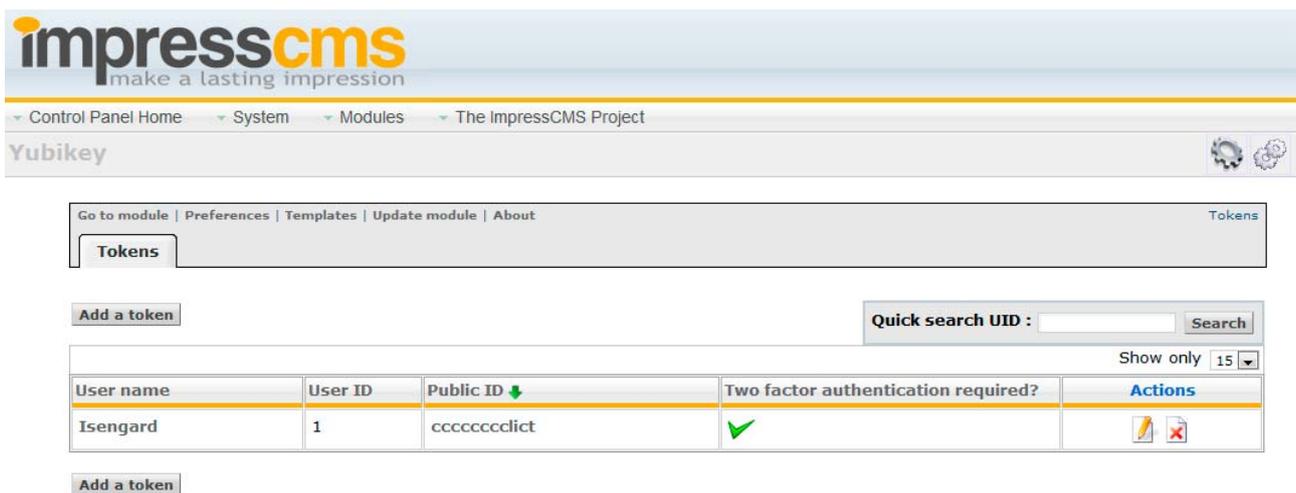
Warning: Once a Yubikey has been associated with user account, that user is **obliged** to use two-factor authentication to login in, ie. they must provide their regular account password and a one-time password generated by their Yubikey. If they try to login using their regular username/password only, they will be refused entry and redirected to the Yubikey login page.

You can temporarily disable two-factor authentication by clicking on the 'authentication required' icon for a key. This will toggle it on (green checkmark) or off (red cross). When disabled, the associated user account can login using the standard account username/password (single factor authentication). Similarly, deleting a key will return the associated user account to single factor authentication. However, if a user account has multiple keys associated with it, all must be disabled for single factor login to be permitted.

Please note: The Yubikey module does not protect you from man-in-the-middle (MIM) attacks, although it does prevent such an attacker from reusing captured login credentials to access your account in future. To reduce the possibility of MIM and passive eavesdropping, it is an excellent idea to use the Yubikey module in combination with an SSL certificate for your site (\$10 from www.namecheap.com). This will also help protect your other site members as well. It is also good practice to formally click the 'log out' link when leaving your site, thereby killing the session.



The Yubikey login page. Yubikey-enabled accounts will be redirected here if they try to login through the standard form.



Admin-side view of Yubikey-enabled accounts. Click the green checkmark to toggle two-factor authentication for this user on or off.

The alternative Yubikey login block

The Yubikey module provides an alternative login block, which you can configure to display in four different ways, according to your preference (see screenshots below). You can configure the block to support standard logins only, both standard login and Yubikey login, and Yubikey login only.

Don't forget that you can clone this block, if you want to have different options available in different sections of your site.

Display mode (block option)	Remarks
Username, password fields	Operates the same as the standard login block, it only provides fields for standard (no Yubikey) login. Yubikey-enabled accounts will be redirected to the Yubikey login page.
Username, password fields + link to Yubikey login page	Operates the same as the standard login block, but a link is also provided to the Yubikey login page for the use of people with Yubikey-enabled accounts. This is the default option.
Username, password, Yubikey fields	Both standard and Yubikey-enabled accounts can login directly through the block in this configuration. Standard accounts just fill in the username and password fields, Yubikey-enabled accounts fill in the password and Yubikey fields.
Password, Yubikey fields	Only Yubikey-enabled accounts can use the block in this configuration. This is best suited for sites where all users are required to use Yubikeys.

User name + password fields (standard login only)

Login

Username:

Password:

Remember me

[Lost Password?](#)
[Register now!](#)

Username, password and link to Yubikey login page

Login

Username:

Password:

Remember me

[Lost Password?](#)
[Register now!](#)

[Yubikey \(Admin\)](#)

Username, password and Yubikey login fields

Login

Username:

Password:

Yubikey (admin):

Remember me

[Lost Password?](#)
[Register now!](#)

Password and Yubikey fields (Yubikey login only)

Login

Password:

Yubikey (admin):

Remember me

[Lost Password?](#)
[Register now!](#)

More information about Yubikeys?

Full documentation, specifications and developer information are available from the Yubico website (www.yubico.com). I recommend that you also listen to this Security Now! podcast for a general overview of Yubikeys: <http://www.twit.tv/sn143>