Panel - Feature # 117: Two factor auth for https://panel.bitfolk.com/

Status:	Closed	**Priority:**	Normal
Author:	halleck	**Category:**	
Created:	2014-01-12	**Assigned to:**	
Updated:	2016-09-17	**Due date:**	
Subject:	Two factor auth for https://panel.bitfolk.com/		
Description:	It would be a good thing to have the option of making ones https://panel.bitfolk.com/ login two-factor, by also requiring a "Yubikey":https://www.yubico.com/products/yubikey-hardware/yubikey/.		

History

2014-03-22 15:02 - admin

- Subject changed from Yubikey auth for https://panel.bitfolk.com/ to Two factor auth for https://panel.bitfolk.com/

2014-03-22 15:03 - admin

Would people consider the Google two factor auth mobile app in TOTP mode good enough for this?

2014-04-10 15:58 - halleck

Yeah, I guess Google Auth style TOTP is a more realistic option, and a clear improvement.

Personally I'd be happy with that solution too.

2014-04-10 16:00 - halleck

(That is, a clear improvement to just having a regular password login.)

2016-05-03 17:57 - robert

I just wanted to register my support for this. TOTP is now a widely deployed, mature technology and given that gaining access to the panel is enough for a complete compromise of a customers VPS my view is that MFA is essential. Certainly when I am evaluating new services for running infrastructure, MFA is now a hard requirement.

2016-05-03 18:09 - admin

I assume use of optional 2FA should be incompatible with any form of automated email password reset, yes?

2016-05-03 18:27 - robert

Definitely, I think it's fair to say that someone prepared to enable MFA is accepting responsibility for not losing their password under any circumstances - and would probably want a very stringent process to get it unlocked if something goes bad (e.g. GPG, two forms of id, etc.). Most services I use that support MFA offer text message as a fallback, which is useful as a mobile number can be recovered if you lose access to the device that has all your MFA accounts attached to it.

2016-05-04 16:45 - admin

We are also going to need to either use the same 2FA for SSH to Xen Shell, or else allow it to be made key-only. As it stands you can't actually do anything destructive via web panel, but you certainly can from Xen Shell.

2016-05-05 05:52 - admin

Is it actually justified to disable email password resets just because two-factor authentication is enabled?

If 2FA is enabled then obtaining a new password by email still doesn't give an attacker access to anything.

Is it not the case that it's only the 2FA part that shouldn't be able to be reset/disabled by email?

2016-05-05 08:14 - admin

I've implemented TOTP 2FA on the panel test site and would appreciate some user testing of it to check it is fit for purpose.

You can log in at https://testpanel.bitfolk.com/ with your real credentials. It is currently connected to the real customer database so changes you make will be real. However, there is no 2FA on the real panel site yet so you can't lock yourself out of the real site. I will purge any TOTP keys and set everyone back to TOTP disabled before deploying it to live.

So please could you have a look at it and see if it works how you want/expect?

2016-05-05 08:28 - robert

I've just set up MFA on the test panel and it works perfectly!

2016-05-05 08:31 - halleck

Ok, I have now done some quick testing at enabling 2FA at https://testpanel.bitfolk.com/, and it logging in appear to succeed when it's supposed like, as well as failing when it's not supposed to.

I would suggest requiring that the user enters a valid TOTP code during the 2FA setup process.

2016-05-05 08:35 - admin

robert wrote:
> I've just set up MFA on the test panel and it works perfectly!

Good to hear. Are you happy with how it is set up, things likeâ€¦

* being able to see the QR code, key and three valid tokens at any time from the security page
* disabling of email password reset when MFA is enabled
* always show input box for MFA token on same page as user/password inputs regardless of whether it will actually be checked

etc?

2016-05-05 08:36 - halleck

halleck wrote:
> ...logging in appear to succeed when it's supposed like, as well as failing when it's not supposed to.

Ok, that part about the failing might have turned out a big ambiguous. What I meant is that the login is failing in situations where the login ought to fail, hence the failing being the desired result.

In short, it's all good.

2016-05-05 08:38 - admin

halleck wrote:
> I would suggest requiring that the user enters a valid TOTP code during the 2FA setup process.

Ah good idea, so like, it asks you to put a token in and only enables 2FA if you get that right?

2016-05-05 08:45 - halleck

admin wrote:
> Ah good idea, so like, it asks you to put a token in and only enables 2FA if you get that right?

Yepp.

2016-05-05 08:51 - robert

admin wrote:
> robert wrote:
> > I've just set up MFA on the test panel and it works perfectly!

>
> Good to hear. Are you happy with how it is set up, things likeâ€¦
>
> * being able to see the QR code, key and three valid tokens at any time from the security page

Without knowing enough about how TOTP works behind the scenes, it seems disclosing these pieces of information is akin to having a way for someone to see their current password. If the user wants to set up a new authentication device, I think the correct thing would be for them to regenerate a new key and invalidate the old one.

> * disabling of email password reset when MFA is enabled

That makes sense.

> * always show input box for MFA token on same page as user/password inputs regardless of whether it will actually be checked

Most sites I use ask for the digits on a subsequent page once you have entered your password, others have it under a show/hide box.

2016-05-05 09:24 - heavy-lifting

I've just added 2FA and configured it using 1Password and it seems to work fine. Even without really known what I was doing - the TOTP feature on 1Password was news to me - it was easy to set up.

2016-05-05 09:40 - admin

heavy-lifting wrote:
> the TOTP feature on 1Password was news to me - it was easy to set up.

Thanks, good to know that one works nicely. I've only tried Google Authenticator myself so far.

2016-05-06 02:55 - admin

There's a report that the key can't be added using Google Authenticator on iPhone 5s. The error message is:

> The barcode 'otpauth://totp/BitFolk Panel (XXX)?secret=â€¦' is not a valid authentication token barcode.

I don't have an iPhone I can test this with. Is anyone successfully using this with Google Authenticator on iPhone?

Personally I am using Google Authenticator on Android.

2016-05-06 14:41 - admin

robert wrote:
> admin wrote:
> > * being able to see the QR code, key and three valid tokens at any time from the security page
>
> Without knowing enough about how TOTP works behind the scenes, it seems disclosing these pieces of information is akin to having a way for someone to see their current password. If the user wants to set up a new authentication device, I think the correct thing would be for them to regenerate a new key and invalidate the old one.

Point taken, I will remove these.

> > * disabling of email password reset when MFA is enabled
>
> That makes sense.

But does it? Why? If MFA is enabled then even if you take over someone's email account you still can't gain access. Is there a reason to link enabling MFA with disabling email password reset? So far all I have seen is "if you've enabled MFA you're probably security-conscious enough to not want email password reset." In which case you could just disable that.

You might be shocked at how many BitFolk customers apparently do not keep any track of their account password and just reset it every time they want to use it. I am worried that forcing password reset to be disabled will reduce the number of people willing to enable MFA.

> > * always show input box for MFA token on same page as user/password inputs regardless of whether it will actually be checked
>
> Most sites I use ask for the digits on a subsequent page once you have entered your password, others have it under a show/hide box.

I use two sites that have it up front on the login page, and I copied that design because it means not having to wait for another form to load before logging in. I rejected the idea of having the token input field initially hidden for the same reason: so people don't have to click some UI element to show the token input field.

Is it better/necessary to not show the token input field by default?

I suppose something I could do is have it initially hidden but the first time someone displays it, a cookie is set that makes it always be displayed for them in future. That might be stretching my JS skills though, and that's probably not a good reason to delay deployment.

2016-05-06 15:33 - admin

admin wrote:
> There's a report that the key can't be added using Google Authenticator on iPhone 5s. The error message is:
>
> > The barcode 'otpauth://totp/BitFolk Panel (XXX)?secret=â€¦' is not a valid authentication token barcode.
>
> I don't have an iPhone I can test this with. Is anyone successfully using this with Google Authenticator on iPhone?
>
> Personally I am using Google Authenticator on Android.

Something to investigate:
> 16:11:18 <+Tolien> I get that error with the iOS Google auth app too. looks like it expects the name in the QR code to not have spaces in it

> 16:11:54 <+Tolien> if you change the "Bitfolk Panel (x)" to "BitfolkPanel(x)" it scans correctly

> 16:18:42 <@grifferz> interesting. I have existing keys for other web sites that have spaces in. but I will change it to underscores and see if it helps the original reporter. thanks!

2016-05-06 21:36 - sarah-jane

So I logged in to testpanel in Chrome, with TOTP enabled. I mistyped by OTP and got "Epic Fail". I typed the code in correctly and logged in.

I then opened up MS Edge (IE on Win10), went to the login page and was able to login with the SAME 6-digit OTP for Panel(448).

I had never been to the site before on MSIE as I only use this software when Chrome can't cope (i.e. very rarely) or if I want to keep it out my browsing history (ahem!)
Both connections are proxies by my EL5 Squid in Bitfolk.

2016-05-06 21:44 - sarah-jane

I can confirm that removing the spaces made Google Authenticator on iPhone work.

I can also confirm that replacing the spaces with %20 made it work, and showing the CORRECT authentication OTP's.

QR's generated at: http://dan.hersam.com/tools/gen-qr-code.html

It would be nice if you could also add to the URL: &issuer=Bitfolk%20Panel - to have a nice label at the top of the OTP as I have several codes in my authenticator now.

2016-05-06 21:56 - admin

> So I logged in to testpanel in Chrome, with TOTP enabled. I mistyped by OTP and got "Epic Fail". I typed the code in correctly and logged in.
>
> I then opened up MS Edge (IE on Win10), went to the login page and was able to login with the SAME 6-digit OTP for Panel(448).

Yes, this will happen because each token is valid for 30 seconds. Also to allow for clock skew the previous and next tokens are also considered. So a potential worst case is that a used token is still valid for almost 90 seconds.

I have access to 3 other services that use TOTP and all of them allow this reuse within the time period. It would be possible to avoid it by keeping track of last used token per user, which would also prevent yourself from logging in twice within 30 seconds. I'm not convinced this is really necessary, but if people are bothered by the possible reuse then I would be happy to work on it as a post-deployment improvement. I really don't want to make it a per-user option as that just starts to offer too many options.

The scenario that's being protected against here is something like a keylogger that gets all your credentials. They would then have up to 90 seconds to log in as you before the token expired.

So, expiry of token upon use - necessary or not?

2016-05-06 21:58 - admin

> I can also confirm that replacing the spaces with %20 made it work, and showing the CORRECT authentication OTP's.

Okay so rather than replacing with underscores I will try URI-encoding it.

> It would be nice if you could also add to the URL: &issuer=Bitfolk%20Panel - to have a nice label at the top of the OTP as I have several codes in my authenticator now.

Hmm, it already has a "label=BitFolk Panel (uid)" which shows as the title in Google Authenticator on Android. What are you using that also needs "issuer="? Is this GA in iPhone again?

2016-05-07 09:02 - admin

Okay, so based on your feedback I'veâ€¦

* Made it require the input of a valid token before 2FA is enabled for real
* Removed the ability to see the QR code and key
* Added a button to delete the key (which disables 2FA as well)
* URI-escaped the label ("BitFolk: UID %u") part of the otpauth URI
* Added an issuer of "BitFolk" as recommended by https://github.com/google/google-authenticator/wiki/Key-Uri-Format

I haven't yetâ€¦

* Done anything to address token reuse as I'm waiting for feedback
* Actually deployed the SSH part
* Changed anything regarding the automatic disabling of email password reset, as no one yet seems to disagree with it

Please could you test deleting your 2FA key and adding a new one again, especially on iPhone?

2016-05-07 10:33 - robert

I've tested that, works great for me (Google Authenticator on Android).

2016-05-07 11:04 - ra

Works for me adding a new 2FA key with Google Authenticator for iPhone.

When you successfully enter a valid token to confirm, is it worth highlighting the "Congratulations, â€¦" text? When I hit submit, it didn't seem like anything had happened until I noticed that block of text.

2016-05-07 15:25 - sarah-jane

I invalidated TOTP for UID 448 and then re-added to Google for iPhone using the latest barcode. Successfully added and verified. Looking good!

TBH I'm not too concerned about re-use, but RFC 6238 is clear that it MUST NOT be accepted. However, as you have discovered, very few implementations enforce this.

But because a successful login generates a very long-lived session cookie, if login's been replayed then the account could be compromised for a long time (I might raise this as a separate issue :)

2016-05-09 10:41 - admin

Okay, I will make it keep track of the last successful token and not accept it again.

2016-05-10 16:44 - admin

> When you successfully enter a valid token to confirm, is it worth highlighting the "Congratulations, â€¦" text? When I hit submit, it didn't seem like anything had happened until I noticed that block of text.

I've now added cheesy SVG warning / tick mark icons and made the page scroll to the correct place. Is that sufficient?

Ideally it would be done by a pop-over dialog that prompts you through each stage but that is beyond my web skills I'm afraid.

> Okay, I will make it keep track of the last successful token and not accept it again.

That's now done.

So as far as I am aware the only outstanding thing is to make it enable / disable 2FA on SSH to Xen Shell.

2016-05-11 02:14 - admin

- Status changed from New to Feedback

I've now put this live, including 2FA for SSH to Xen Shell. Please give it a bit more testing!

I've disabled 2FA for all of you so it doesn't affect your ability to connect to your Xen Shell, so you'll just need to re-enable it (keys will stay the same).

2016-05-11 10:02 - robert

Thanks Andy.

2016-09-17 08:54 - admin

- Status changed from Feedback to Closed

People seem happy with this now.