

Panel - Feature # 167: Add "require PGP signed instructions" feature

Status:	New	Priority:	Normal
Author:	admin	Category:	
Created:	2018-08-14	Assigned to:	
Updated:	2018-08-14	Due date:	
Subject:	Add "require PGP signed instructions" feature		
Description:	<p>A customer requested that no action be taken with regard to their VPS without the instructions being validly PGP signed.</p> <p>At the moment this cannot easily be accomplished since support requests come in by email, without any classification as to which VPS account they relate to. Although BitFolk can verify OpenPGP signatures, the vast majority of customers do not use PGP and this is unlikely to change, so almost all support requests will be unsigned. There is currently no easy way to indicate that the account requires signed correspondence.</p> <p>Upon receiving a support request the first thing that BitFolk does is determine which account it relates to. At the moment this is a rather manual process based on checking if the requester has specified an account, if the email address matches, etc. This could be made more formal by modifying BitFolk's ticketing software so that the account must be specified (by BitFolk, but also possibly automatically later on, if a means of submitting tickets from the Panel is added). Once that was set, the ticketing software could check the customer database to see if PGP signed instructions are required.</p> <p>So, a minimum viable version of this could be:</p> <ul style="list-style-type: none">* Customer database allows contact records to have one or more PGP fingerprints* Customer database includes flag for "require PGP signed correspondence before taking any action"* Ticketing system gets custom variable for VPS account, which BitFolk can set* Support procedure modified to involve setting the account as first action* Ticketing system checks on PGP requirements once the account is set <p>In the initial version customers probably would have to submit a support ticket to change any of that, as it wouldn't be exposed to the Panel web site at first.</p> <p>Questions:</p> <ul style="list-style-type: none">* Should the "require PGP signed correspondence before taking any action" flag be per-customer (all VPSes under that customer account require it or all don't) or per-VPS?* Is it enough to say "any of the PGP keys set on any contact record will do" or should it be restricted to the "technical contacts" role (doesn't yet exist, but is known that it should exist), or should it have a role all of its own? <p>The contact records live at https://panel.bitfolk.com/account/contacts/#toc-address-book and at the moment the only roles that exist are "Emergency" and "Alerting". It's already been established that there should also be "Billing" and "Technical".</p>		

History

2018-08-14 13:34 - admin

Also, what to do if someone turns on the "PGP required" flag and then is unable to send correctly signed email?

For the two factor authentication feature, BitFolk will ask you to log in to your VPS and echo something to the console. This proves you already have root access to the VPS, at which point BitFolk will disable 2FA and let you do a password reset. But what should BitFolk do if you've set "PGP required" and now (potentially months/years later) you're contacting support because you can't access your VPS?

I have a feeling that there will be wildly differing expectations here, so if this is to be pursued then the way that inability to sign is handled should be documented.