# Panel - Feature # 134: Transition from using ssh-vulnkey to using ssh-keygen to validate keys

| | | | |
|---|---|---|---|
| **Status:** | In Progress | **Priority:** | Normal |
| **Author:** | admin | **Category:** | |
| **Created:** | 2016-04-17 | **Assigned to:** | |
| **Updated:** | 2022-01-18 | **Due date:** | |
| **Subject:** | Transition from using ssh-vulnkey to using ssh-keygen to validate keys | | |
| **Description:** | It's not currently possible to add ed25519 algorithm SSH public keys to the panel because the blacklisted/valid key check is using a binary that's too old to understand that algorithm, so it just says it's an invalid key.<br><br>Short term this might mean disabling the validation (apart from some very simple sanity checks), or it may be possible to install a backport. | | |

## History

**2016-04-18 00:51 - admin**

*- Status changed from New to In Progress*

Okay, I've now added configuration that disables SSH public key validation so it's now possible to add keys that ssh-vulnkey isn't able to parse.

**2016-04-18 00:53 - admin**

*- Subject changed from Support ed25519 SSH key algorithm to Transition from using ssh-vulnkey to using ssh-keygen to validate keys*

ssh-vulnkey doesn't exist in jessie and really ssh-keygen should be used there to validate key data, so I'll now rename this feature to show that is the proper fix.

**2022-01-17 18:56 - thngateway**

Can confirm this works fine with "ssh-ed25519" keys.

I tried adding a "ecdsa-sha2-nistp521" format key that my laptop created but it doesn't accept those "That doesn't look like a valid SSH public key!" is the error message returned.

**2022-01-17 19:30 - halleck**

Neither does "ed25519-sk" keys seem to be accepted.

In case ssh-keygen is already in use it will need to be an OpenSSH 8.2+ ssh-keygen to recognize ed25519-sk and ecdsa-sk keys.

**2022-01-18 08:30 - admin**

It's not using @ssh-keygen@ yet, it's just a simple regex and I hadn't included @ecdsa-sha2-nistp521@ in the check even though they would work.

Here's the supported public key types:

* @ecdsa-sha2-nistp256-cert-v01@openssh.com@
* @ecdsa-sha2-nistp384-cert-v01@openssh.com@
* @ecdsa-sha2-nistp521-cert-v01@openssh.com@
* @ssh-ed25519-cert-v01@openssh.com@
* @rsa-sha2-512-cert-v01@openssh.com@
* @rsa-sha2-256-cert-v01@openssh.com@
* @ssh-rsa-cert-v01@openssh.com@
* @ecdsa-sha2-nistp256@
* @ecdsa-sha2-nistp384@
* @ecdsa-sha2-nistp521@
* @ssh-ed25519@
* @rsa-sha2-512@
* @rsa-sha2-256@
* @ssh-rsa@

Most of the dom0s are OpenSSH 7.9 at the moment so no FIDO key support like
@ed25519-sk@ yet I'm afraid.

**2022-01-18 08:31 - admin**

I've updated the regex to accept all of the above key types. Previously it was only the ones that begin with @ssh-@.