RDP/SSH Remote Login Integration Guide

Version 1.0 ● 7th September 2023

VeroGuard Systems

VeroGuard Systems – Melbourne, Australia – Phone: +61 3 9558 3090

Email: - info@veroguard.com.au

Table of Contents

1 Introduction

1.1 Scope and intended reading audience

This guide is primarily aimed at personnel who will be configuring and administering IT networks and provides information on setting up remote access environment so that your privileged users can subsequently access remote machines using their VeroCard.

This guide describes the steps required to integrate remote machines with the VeroCard login process. It is expected that the reader is familiar with the VeroGuard Platform and VeroCard user set up across AD, AAD and Fido2 environments, and that the integrator has an existing VeroCard.

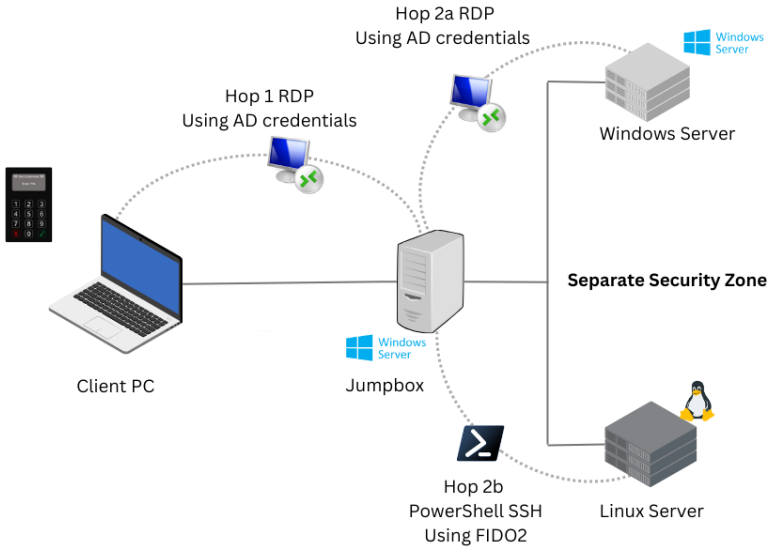
1.2 Initial checks

Before starting, ensure you have completed:

1. Initial integration with VeroGuard for your network environment
2. Setup and activation of your VeroCard
3. VeroCard firmware is 1078 or higher
4. Relevant User Accounts on the remote machines
5. Relevant resources created in the BoID for the remote machine for AD and Fido2
6. An account with “sudo” privileges on the remote Linux machine

1.3 Overview

VeroGuard supports remote logins using a VeroCard via RDP to Windows based machines, and through PowerShell using SSH to Linux Servers. Typically a user will initially access a Jumpbox and from there originate a second hop to access machines in a separate security zone. This document will guide the reader through the set up required for a 2 hop user scenario shown below.



2 Integrating VeroCard Login for RDP

2.1 Client Machine

2.1.1 Prerequisites

- Client is Windows 10 or Windows 11 with “22H2” or higher (webauthn redirection support) (Guide is based on Windows 10 22H2 19045.2913)
- A resource for the VeroCard user has been established in BoID for the account on the remote machine.

2.1.2 Client PC Setup

- Install Serenity Virtual Channel RDP Plugin 1.0.140.0 or higher on the Client PC
- Install Serenity Companion 1.0.84.0 or higher on the Client PC[1]
- Complete a Bluetooth pair with the VeroCard

The latest version of Serenity can be downloaded from https://support.veroguard.com.au/downloads

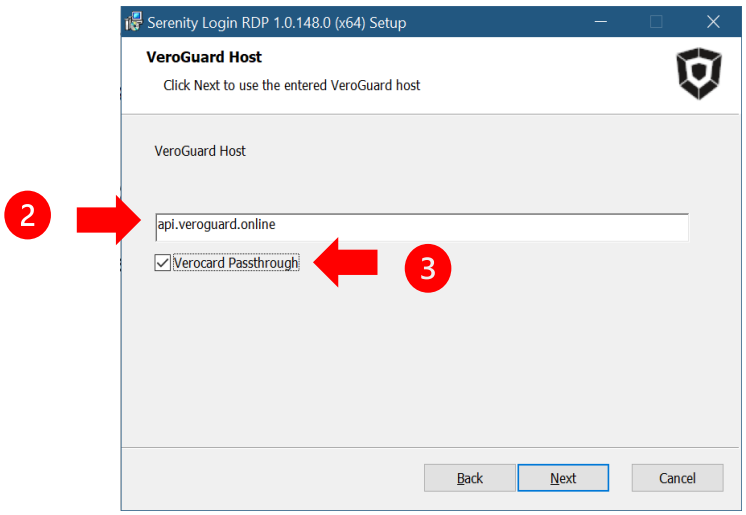
2.2 Jumpbox Setup for Windows RDP Login with VeroCard

2.2.1 Prerequisites

- Jumpbox is either Windows 10 or Windows 11 with “22H2” or higher (webauthn redirection support), Windows Server 2019 or Server 2022 with “21H2” or higher (webauthn redirection support) (Guide is based on Windows Server 21H2 20348.1668)

2.2.2 Jumpbox Setup

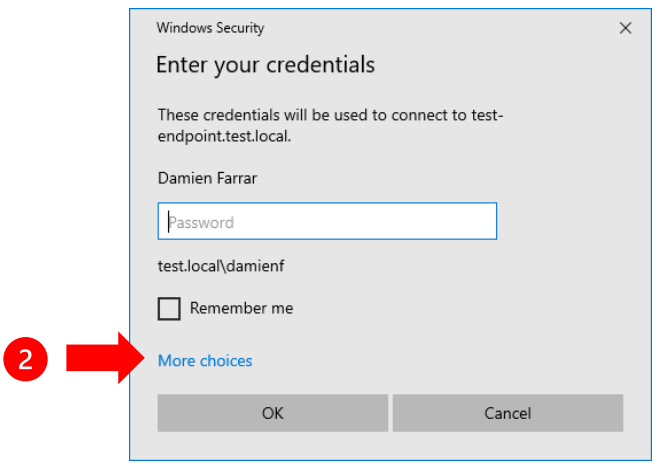
1. Download and install Serenity Login RDP 1.0.140.0 or higher on the Jumpbox
2. Enter the address of your VeroGuard platform, or if using the hosted service, leave the default address setting.
3. Select the VeroCard Passthrough option.

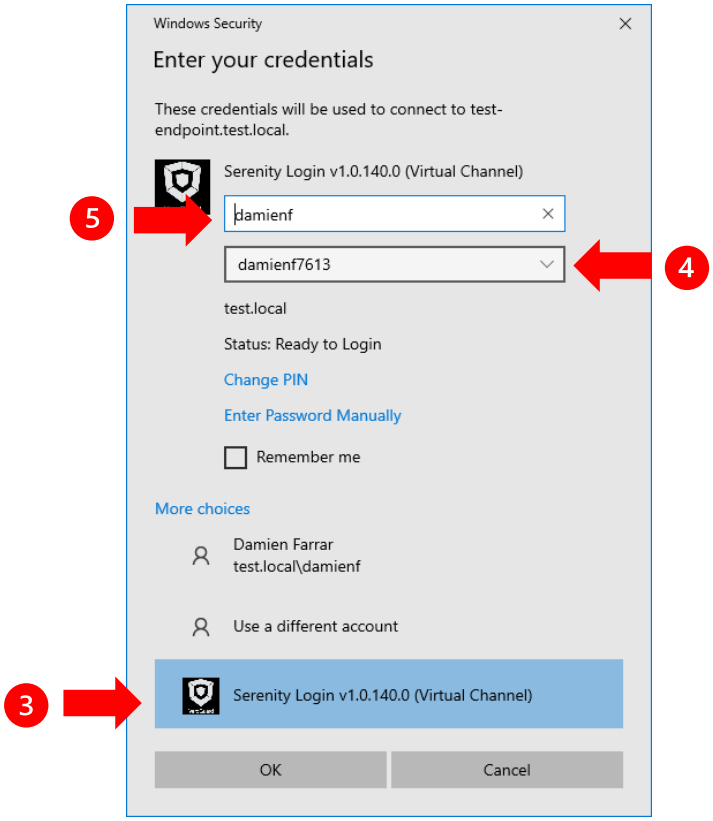


[1]Installation of Serenity Companion and Bluetooth pairing are only required if using Fido2 for authentication on Linux or Windows.

2.2.3 Test Windows Endpoint RDP Login with VeroCard

1. On the Client PC from 2.1.2 above, open Remote Desktop Connection and enter the address information for the Jumpbox
2. Click on the “More choices” link
3. Select the Serenity Login credential provider from the list
4. Power on your VeroCard and then select it from the dropdown list
5. Enter the domain\username for the remote server and then click the OK button to begin the login process
6. Follow the prompts on the VeroCard to enter your PIN and login to the endpoint
7. Repeat the process above to login to another Windows server from the Jumpbox





3 Integrating VeroGuard Login for Linux

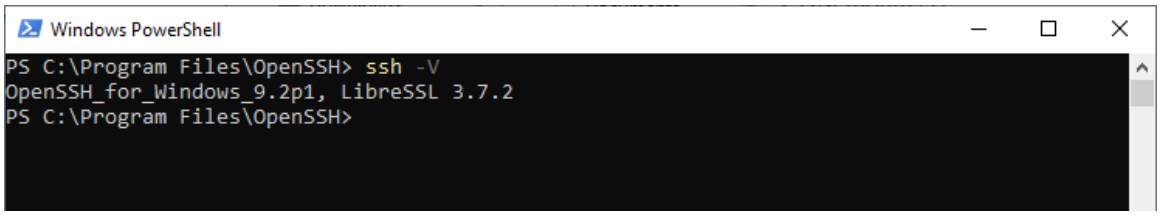
3.1 Jumpbox Setup for Linux SSH Login with VeroCard

3.1.1 Prerequisites

- Jumpbox requires the latest version of Win32-OpenSSH https://github.com/PowerShell/Win32-OpenSSH/releases as the included version of OpenSSH in Windows is unsupported.
- Linux endpoint with OpenSSH 8.3 or higher (Guide is based on Ubuntu 22.04.2 LTS)
- A resource for the VeroCard user has been established in BoID for FIDO2 for each endpoint "ssh:endpoint\openssh" replacing "endpoint" with the endpoint hostname. [2]
- User account and/or Admin (sudo) account on the Linux Box
- Serenity Companion has been installed on, and the VeroCard Paired with the Client PC

3.1.2 Jumpbox Setup

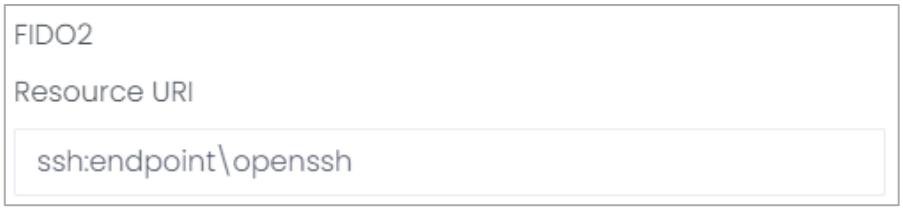
1. Login to the Jumpbox server
2. Open PowerShell and run the command "`ssh -V`" to verify that the latest version of OpenSSH is being used, upgrade if not.



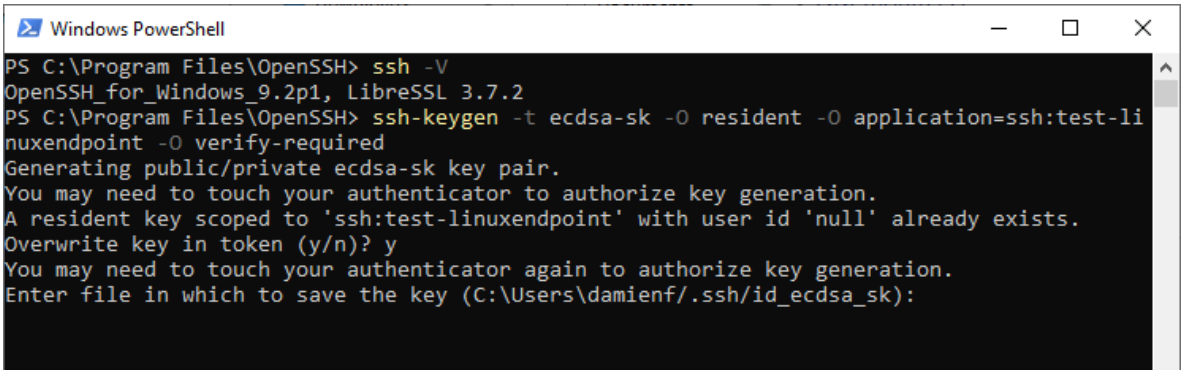
3. Run the following command to generate an ecdsa keypair replacing "`endpoint`" with the endpoint hostname.

```
ssh-keygen -t ecdsa-sk -O resident -O application=ssh:endpoint -O
verify-required
```

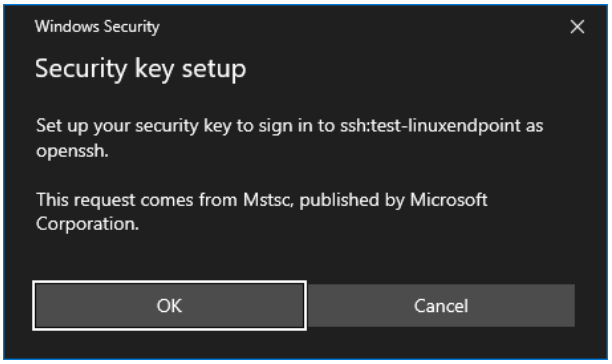
Note: The value for the application arg must always begin with ssh: and the endpoint can be customised, for example, as a reference to the endpoint name but it can be named anything as long as it matches with the FIDO2 Resource URI that is set through the VeroGuard Admin Portal. e.g.: If we called it 'endpoint' then the FIDO Resource URI would need to be named "ssh:endpoint" combined with "\openssh". See screen shot below.

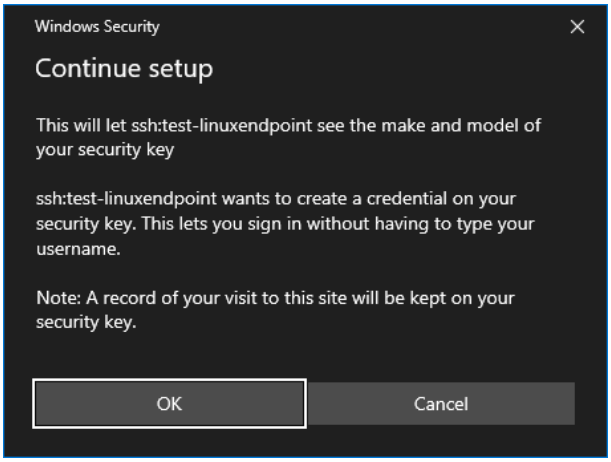


[2] The endpoint name used in the resource must be the same as the name used when creating the keypair. This can be created before or after you create the key pair in step 3.

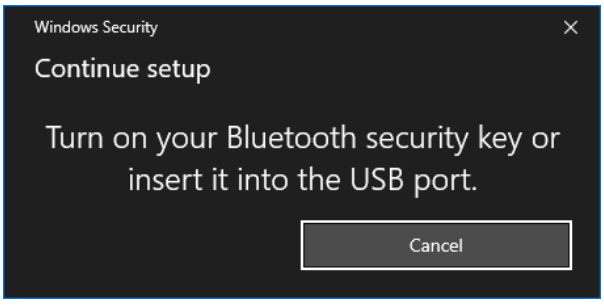


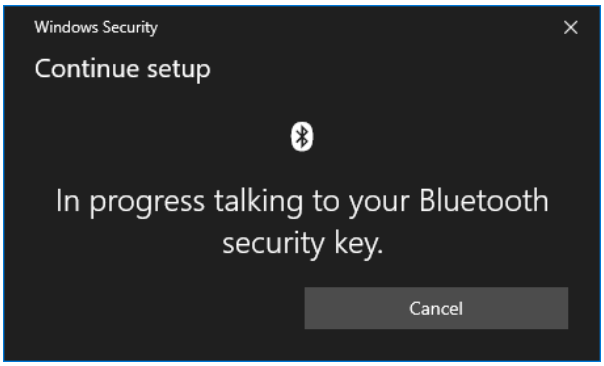
4. If you get a prompt to “Overwrite key in token”, enter “y” and hit enter as the VeroCard will store multiple keypairs.
5. The Windows Security prompt for “Security key setup” will redirect to the Client PC. Select OK and then OK again on the “Continue setup” prompt





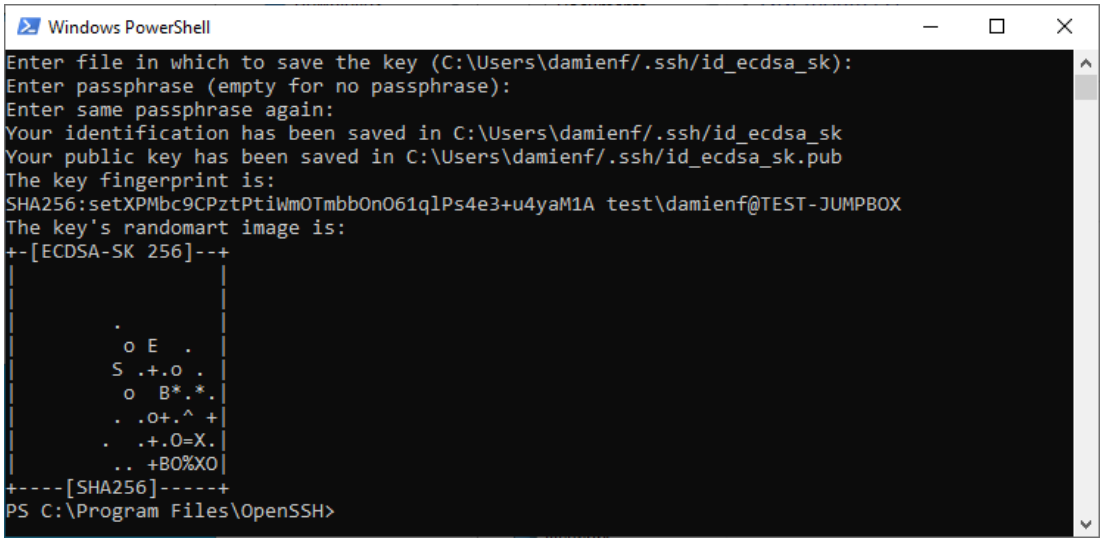
6. Turn on your VeroCard and wait for it to connect, the Windows Security prompt will update to show progress.





7. The VeroCard will prompt you to “Enter PIN” on the Fido2 register screen. Enter your PIN and press the green tick button.
8. On success, the VeroCard screen will display “credentials created”

9. Save the generated keypair to the .ssh folder. We advised this is named relevant to the endpoint and the User.



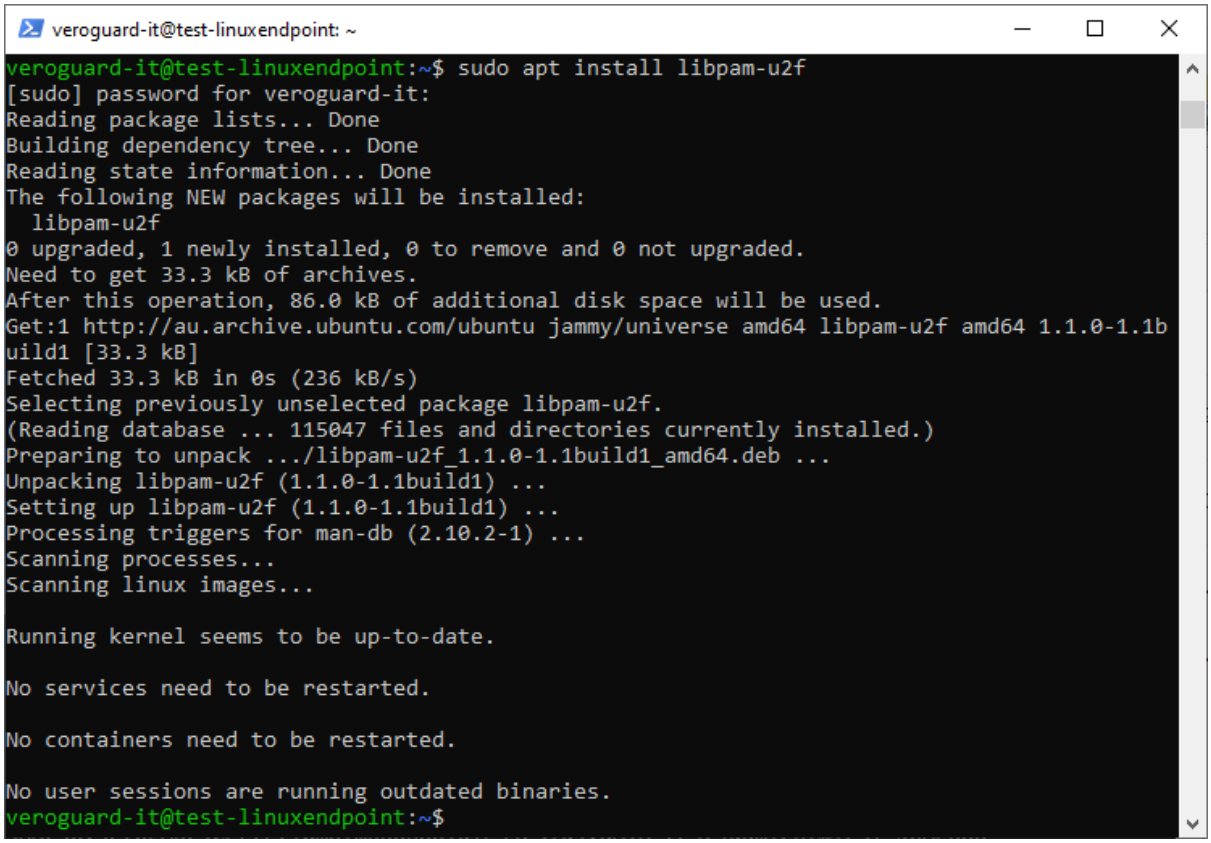
Notes:

a) The first file, id_ecdsa_sk, contains a reference to the private key credential stored on the VeroCard.
b) The second file, id_ecdsa_sk.pub, contains the public key which is used on a remote system to verify authentication.
c) **Keys cannot be shared between VeroCards** – the Private key does not leave the VeroCard.
d) It is possible to share a public key across multiple endpoints, so that a user can login to multiple Linux devices with the same credentials, however there can be only 1 resource for each endpoint URI in the BoID which could limit granular control.

3.1.3 Linux server setup

1. SSH to the Linux endpoint as a user with sudo privileges
2. Install the pam-u2f module using the following command.

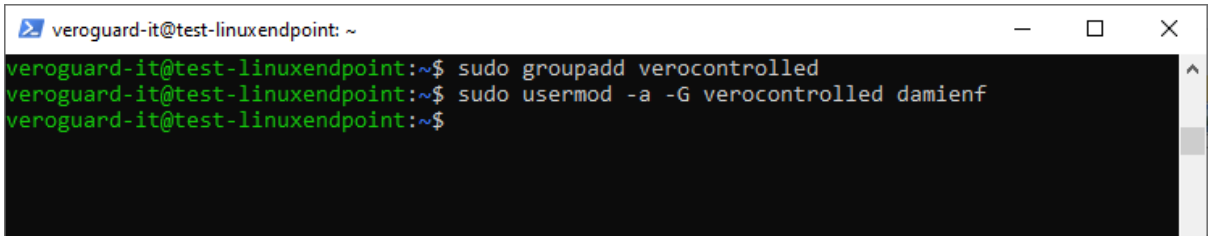
```
sudo apt install libpam-u2f
```



3. Add a new group verocontrolled and add the required user accounts to it.

```
sudo groupadd verocontrolled
```

```
sudo usermod -a -G verocontrolled username
```



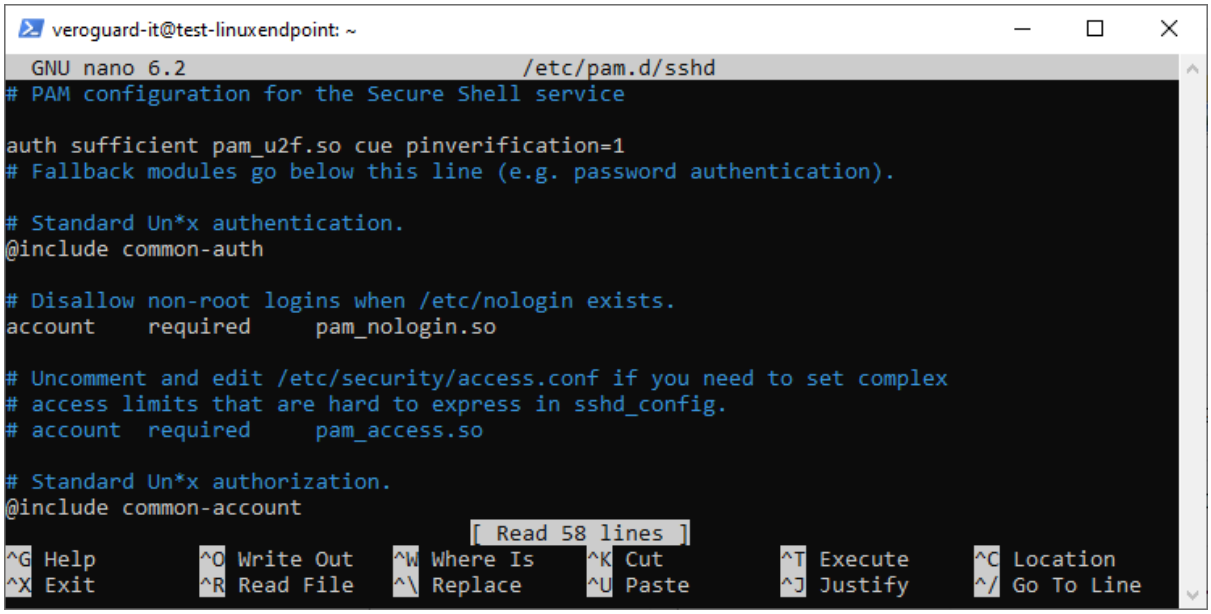
4. Edit the PAM sshd config

```
sudo nano /etc/pam.d/sshd
```

5. Insert the following towards the top of the configuration, this enables authentication using a VeroCard using PAM

```
auth sufficient pam_u2f.so cue pinverification=1
```

```
# Fallback modules go below this line (e.g. password
authentication).
```

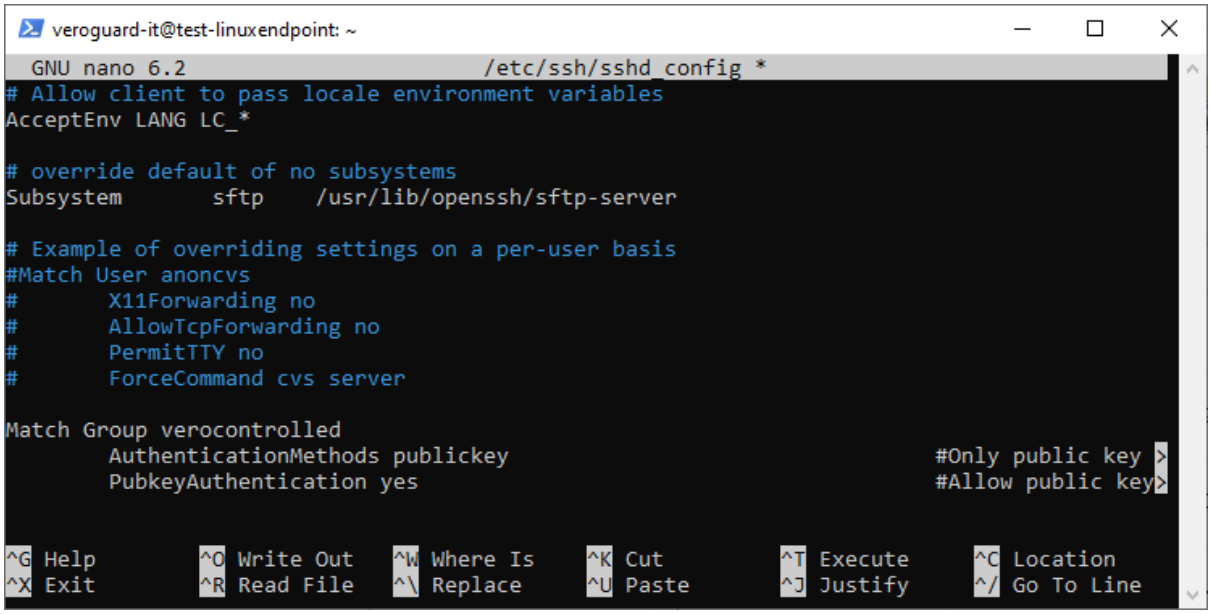


6. Edit the sshd_config and add the below configuration items to the bottom of the file.

```
sudo nano /etc/ssh/sshd_config

Match Group verocontrolled
        AuthenticationMethods publickey
#Only public key authentication allowed
        PubkeyAuthentication yes
#Allow public key authentication
```

Note: this configuration restricts users in the verocontrolled group from being able to use a password to login.



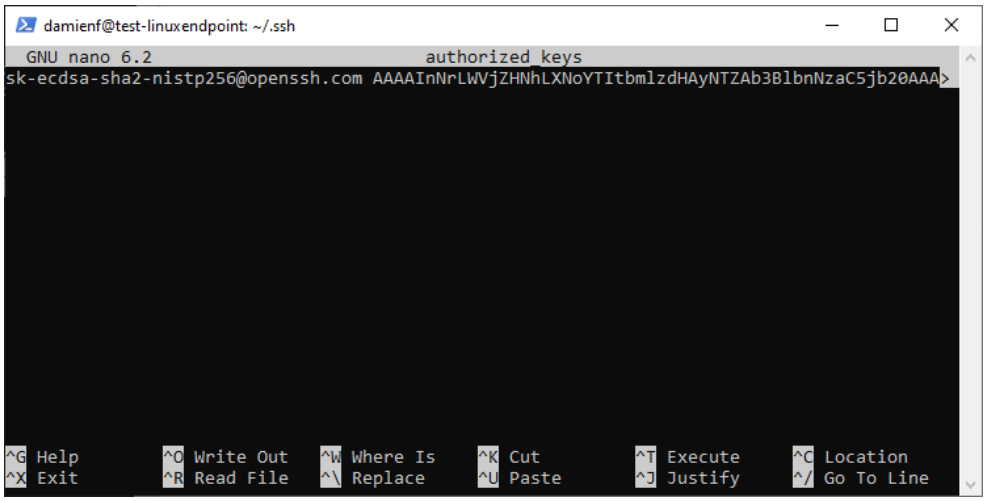
7. Restart ssh for the config changes to take effect

```
sudo systemctl restart ssh
```

NOTE: Once configured, any users added to this group will be required to authenticate with a VeroCard and will no longer be able to login with their password until they are removed from the group.

8. Add the public key ecdsa keypair generated on the JumpBox in 3.1.2 (steps 3 to 9) to the users authorized_keys file on the Linux endpoint. Confirm using the below command.

```
nano /home/$USER/.ssh/authorized_keys
```



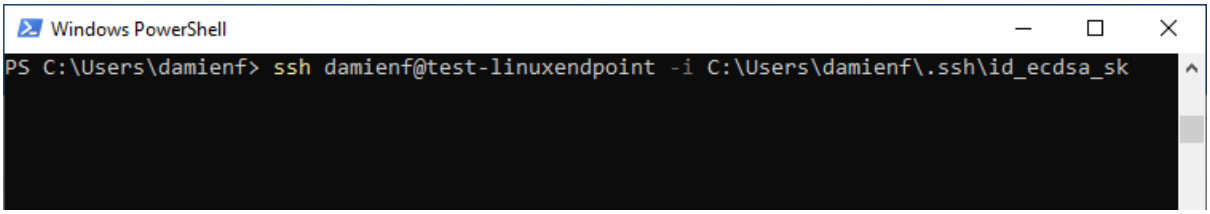
Note: This action is required for each user to be able to access the Server. Users can generate the required keypairs on the Jumpbox and email the public keys to the Linux administrator for distribution to the required Linux Boxes.

3.2 Test Linux Endpoint SSH Login with VeroCard

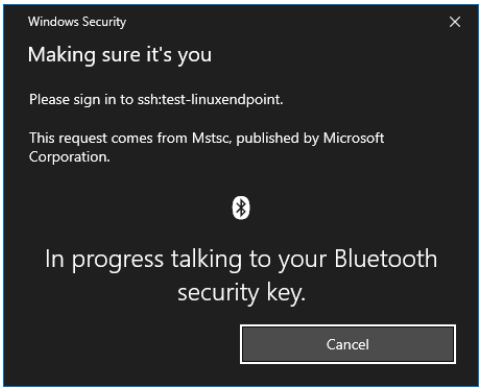
1. Login to the Jumpbox server using a VeroCard
2. Open PowerShell and run the following command to ssh login with VeroCard

```
ssh user@server -i id_ecdsa_sk
```

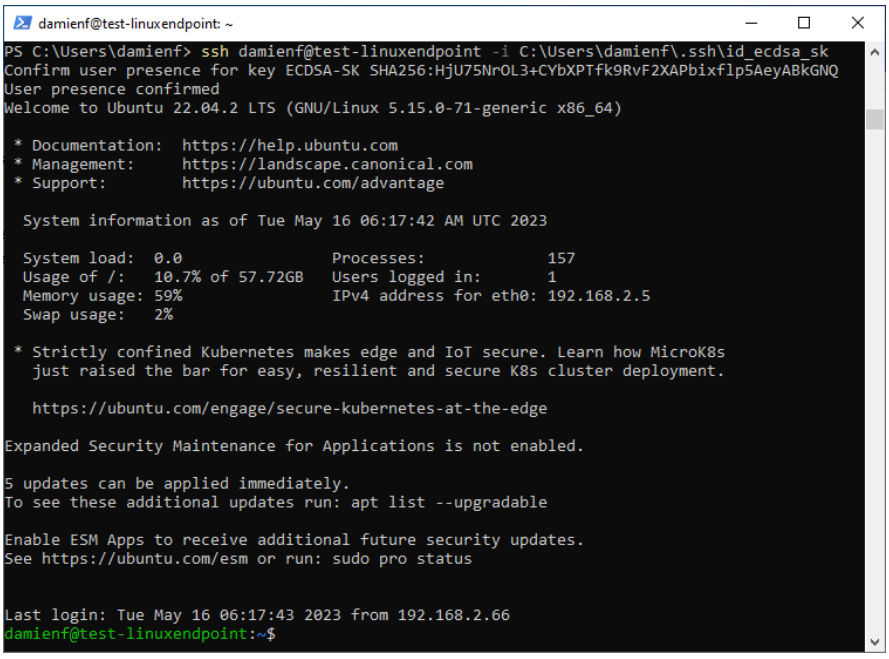
Note: in the command above "id_ecdsa_sk" should be replaced with the path and name of the key that was created in 3.1.2 which is typically stored in the users .ssh directory.



3. Windows Security prompt will redirect to the Client PC, ensure your VeroCard is powered on and paired to the Client PC.



4. Enter your PIN on the VeroCard when prompted
5. On successful PIN verification the User will be logged in



3.3 Reverting to password login (recovery)

1. To allow a user to login with a password again instead of a VeroCard, simply remove them from the verocontrolled group.
2. SSH to Linux endpoint as user with sudo privileges and run the following command:

```
sudo gpasswd -d username verocontrolled
```

Note:

Removing the user from the group will allow them to login with **either** their password or VeroCard.

a) If the file “id_ecdsa_sk” is still present in the .ssh folder then the user will still be prompted to use a VeroCard but the dialog can be cancelled and then a password can be entered. This behavior will only occur when the key file is named using the default name “id_ecdsa_sk”.
b) If the key file has been named differently, then this won’t occur unless the “- i" command is used with the path to a key file.

3.4 Removing User Access

1. To remove user access from logging in with the VeroCard, the FIDO2 Resource should be disabled or deleted from the users account in the VeroGuard Admin Portal.

4 Recommendation

VeroGuard strongly recommend that Linux Administrator (sudo) accounts be protected with 2 VeroCards, so that a backup exists in the event the first VeroCard is lost.