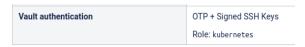
Logging into a machine using SSH via Vault

Since 2022, ISW is migrating to a more secure setup. Instead of sharing passwords via a Password Manager, we now use Vault to create OTP or sign ssh keys to give temporary access to a machine. This gives a lot security benefits, old members for example can no longer access those systems.

What is supported?

To see if the machine supports Vault login, go to the correct documentation page in the sysadmin documentation wiki. On the "Information" table you should see an entry which states the available Vault authentication methods. If a role is specified, you will need to use that role to login.



In this example, both OTP and SSH keys are supported. However you can only use the kubernetes role when signing in.

Logging in via OTP's

This login method is the most complex, it uses an extra helper for PAM to see if a password should be allowed. You can generate a password that can only be used once to login on the device.

More information is available at https://www.vaultproject.io/docs/secrets/ssh/one-time-ssh-passwords.

Manually

To receive an OTP you will need to ask Vault,

```
vault write ssh/creds/ROLE username=USERNAME ip=IP_ADDRESS
```

You will receive an output which has a key value. This is the OTP. You can now SSH to the machine and use that password to login.

Automatically

You can let Vault sign you in automatically, without a need to copy and paste a password:

```
vault ssh -role ROLE -mode otp USERNAME@IP_ADDRESS
```

```
→ ~ vault ssh -role kubernetes -mode otp isw@172.20.247.14

Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-97-generic x86_64)

* Documentation: https://help.ubuntu.com

* Management: https://landscape.canonical.com

* Support: https://ubuntu.com/advantage
```

Signed SSH Keys

More information is available at https://www.vaultproject.io/docs/secrets/ssh/signed-ssh-certificates.

- What is supported?
- Logging in via OTP'sManually
 - Automatically
- Signed SSH Keys