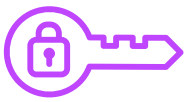
N-ABLE™

# Passportal data protection in transit and at rest

## Application

Your new password records are input into the internet browser on your computer. From there, they are protected by 2048-bit RSA keys encryption with a minimum of 300 different rounds, using six different randomly generated keys. Your unique encryption key (organization key) is the final step in unencrypting your data for view within the browser.



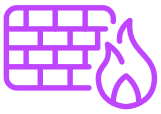


## 1.Organization key

Two of the encryption keys used are unique to each password record, and one of the encryption keys is not generated by or stored within our system. This encryption key is called the organization key and is created and stored only on the MSP side.

## 2.Password and passphrase transmission

All inbound and outbound data communication traffic with the Passportal Cloud happens over TLS 1.2 using 2048-bit RSA keys to help protect your data in transit.



## 3.Web application firewall proxy

Unique encryption keys are retrieved from numerous sources for each password.

## Key service cluster

- 256-bit symmetric encryption
- Password-specific key

## Database cluster

- Partner/MSP key
- Client key
- System key
- All internal transmissions happen over TLS 1.2

## Application service cluster

**Encryption keys are used on a completely randomized basis throughout the hundreds of rounds of encryption, while each stored password has its own unique key.**

## Fully encrypted password storage