CYBERARK®
The Identity Security Company™

PAM Administration

Accounts – Part 2

Agenda

By the end of this session, you will be able to:

1. Describe and configure linked accounts:
   - Logon accounts
   - Reconcile accounts
2. Describe and configure SSH key management

Linked Accounts

There are two types of linked accounts commonly used and supported by default for most platforms:

- Logon account
- Reconcile account

Logon Account

Root Account Best Practices

```
Using username "root".
root@10.0.0.20's password:
Access denied
```

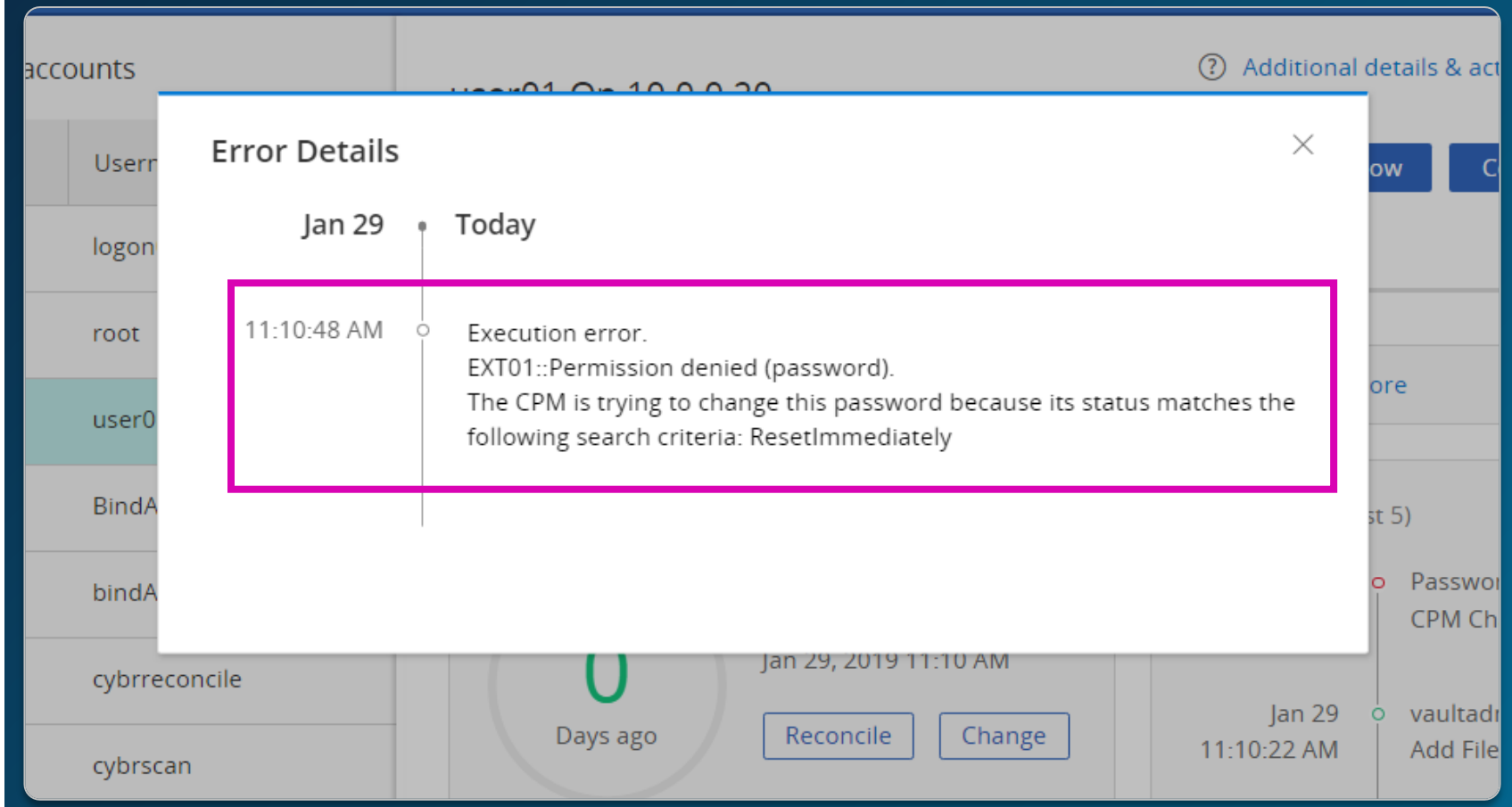
The root user is often prevented from logging in remotely as part of best practices (/etc/ssh/sshd_config > PermitRootLogin no)

The solution is to log in as a user with the authorization to switch to root in order to perform the password change

```
login as: logon01
logon01@10.0.0.20's password:
[logon01@centos-target01 ~]$ su - root
Password:
[root@centos-target01 ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated
successfully.
[root@centos-target01 ~]#
```

Root Password Change Failure

If the SSH policy on the target machine forbids root log on, the **CPM** will not be able to verify or change the root password

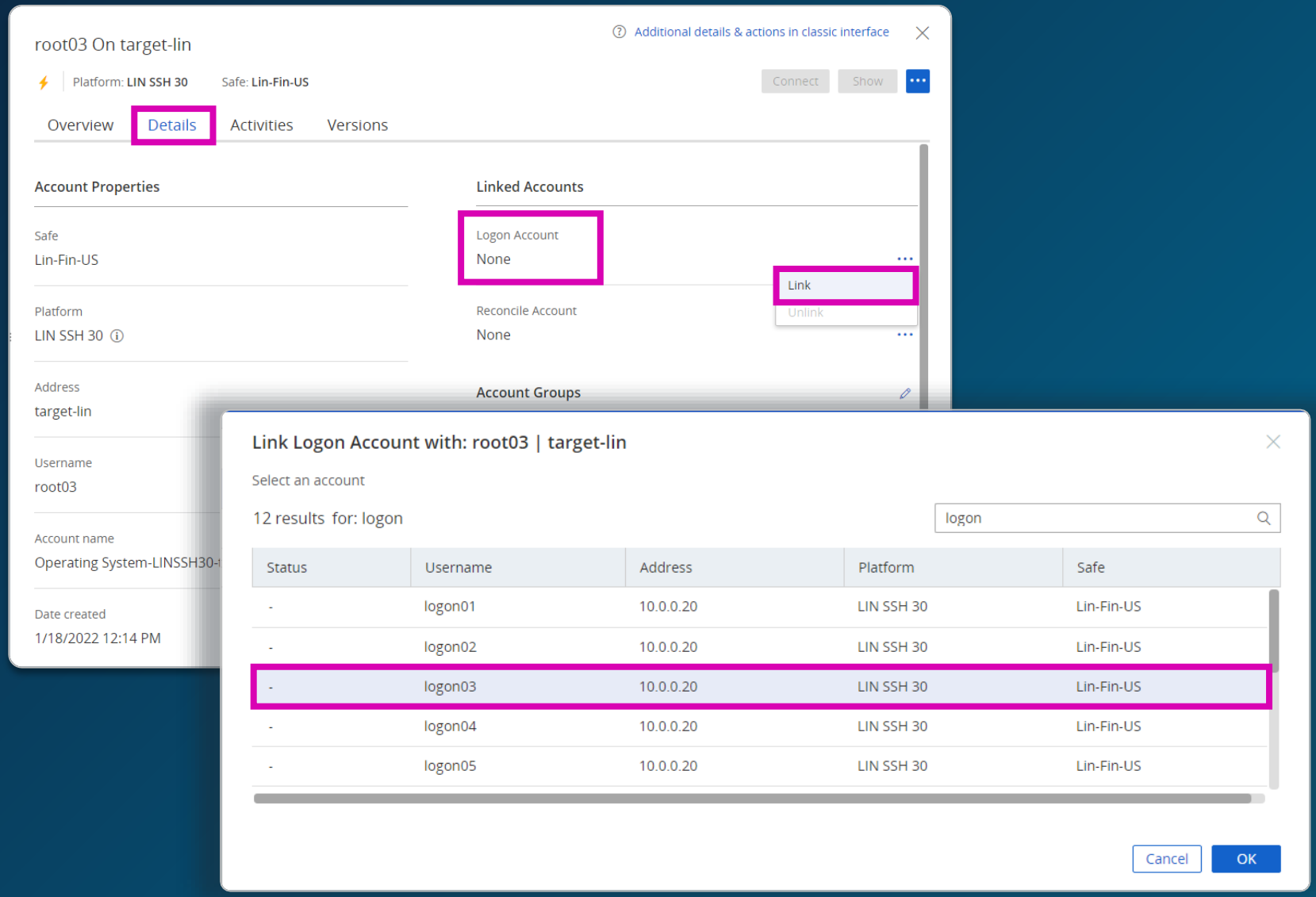


CYBERARK®

Associate Logon Account

The solution is to onboard a non-privileged account that we can use to connect and then switch to root in order to perform the password change. This account is the ***Logon Account***

To use a ***Logon Account***, you need to link it to the root account

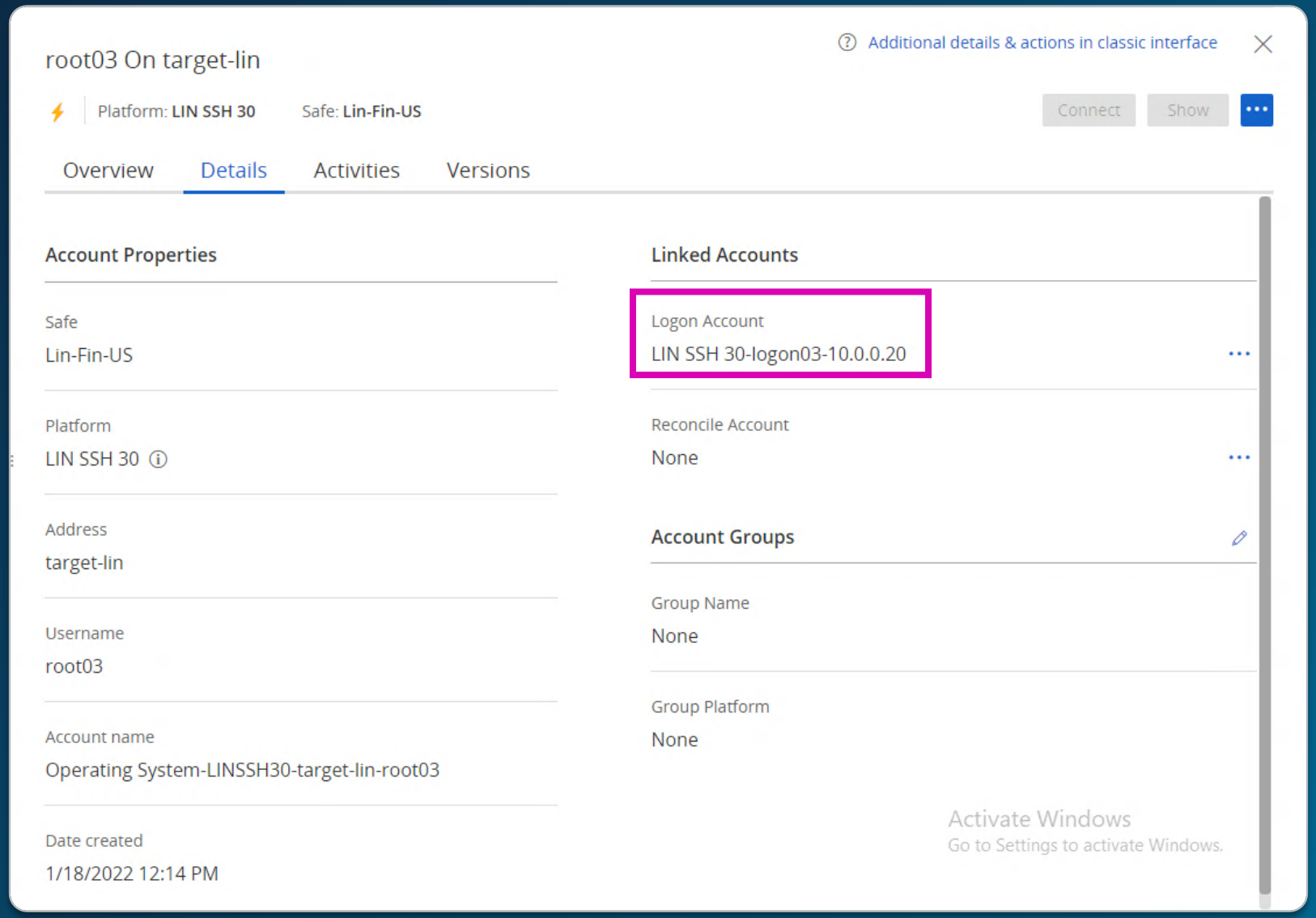


CYBERARK

Root Password Change Success

Now that we have specified a logon account, when we re-run a password change, we will see that the **PasswordManager** user has changed the password.

Note that the logon account is also used when connecting to the target system through the **PSM**

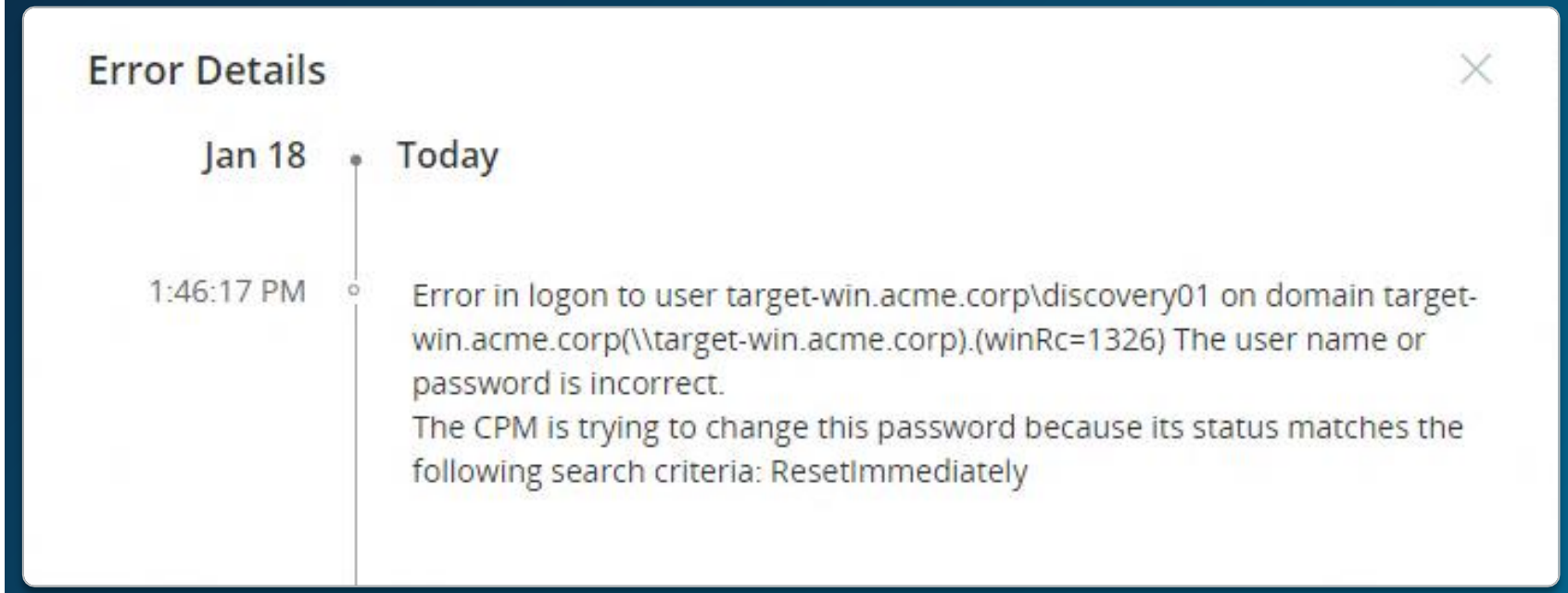


CYBERARK

Reconcile Accounts

Reconciliation – Unknown Password

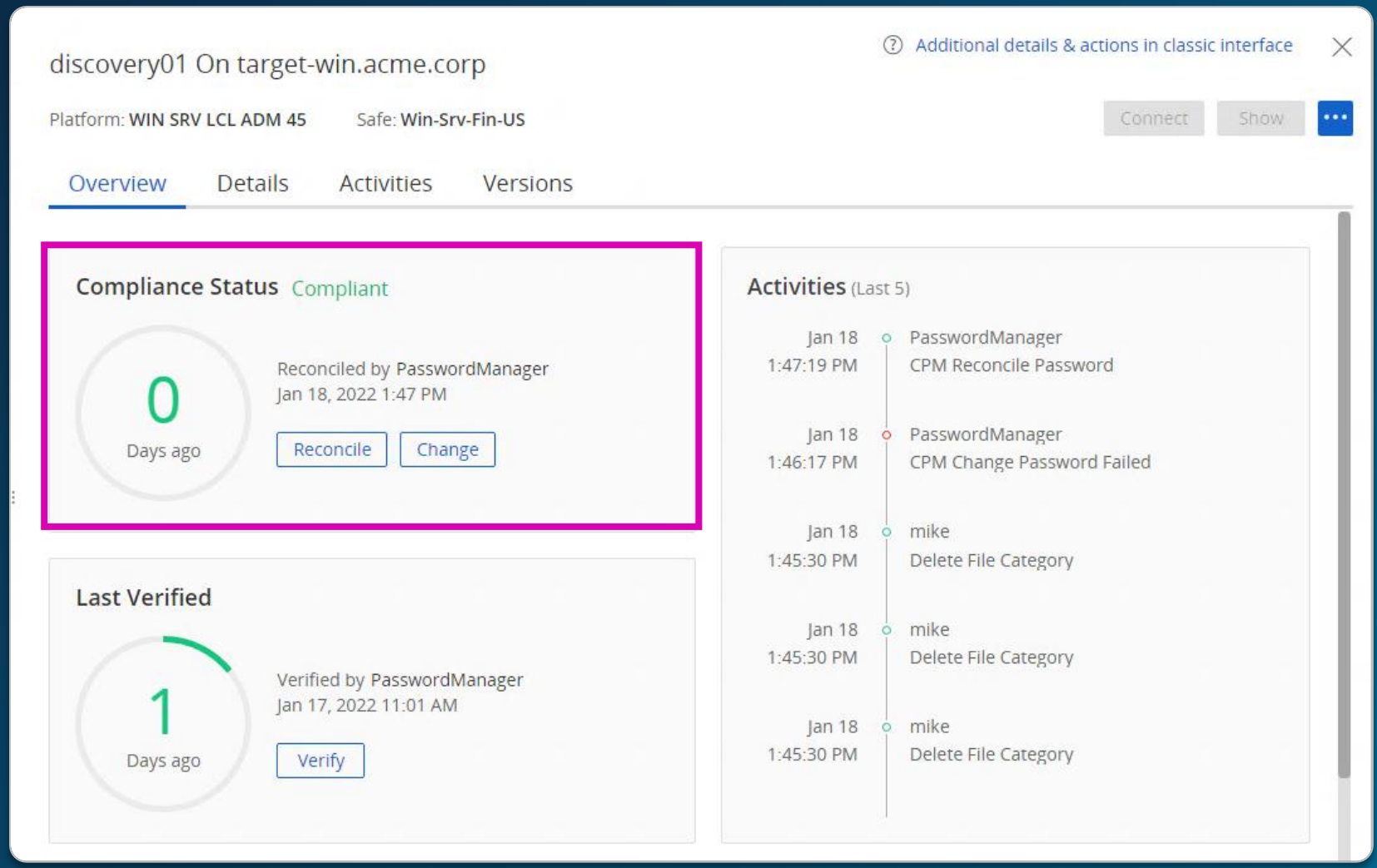
Reconciliation is used for situations where we don't know a password or if the use of individual passwords would be too onerous



CYBERARK®

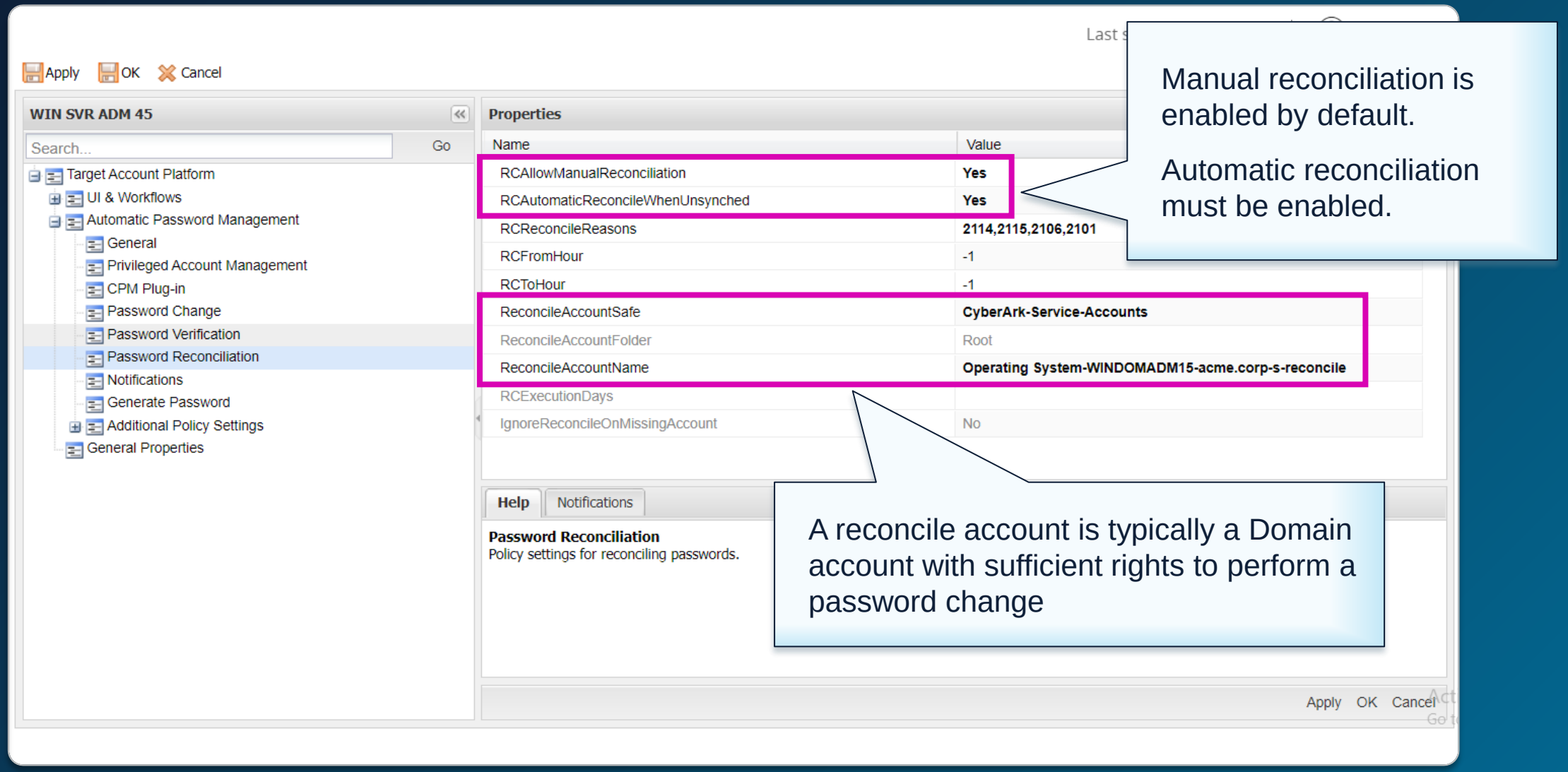
Reconciliation – Unknown Password

The verification process will discover passwords that are not synchronized with their corresponding password in the **Vault** and we can configure the **CPM** to reset the password in the **Vault** and on the Target



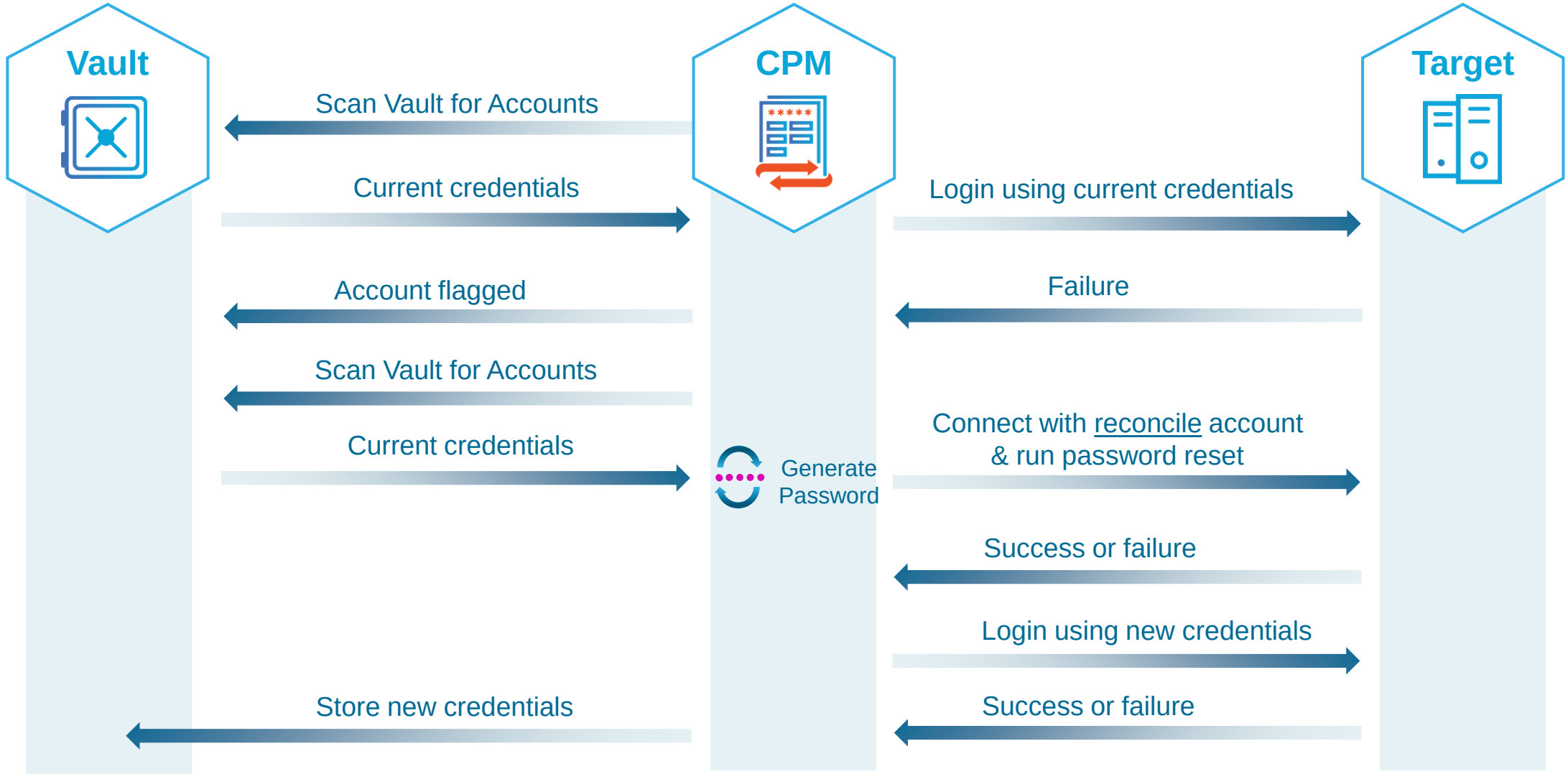
CYBERARK®

Associating a Reconcile Account



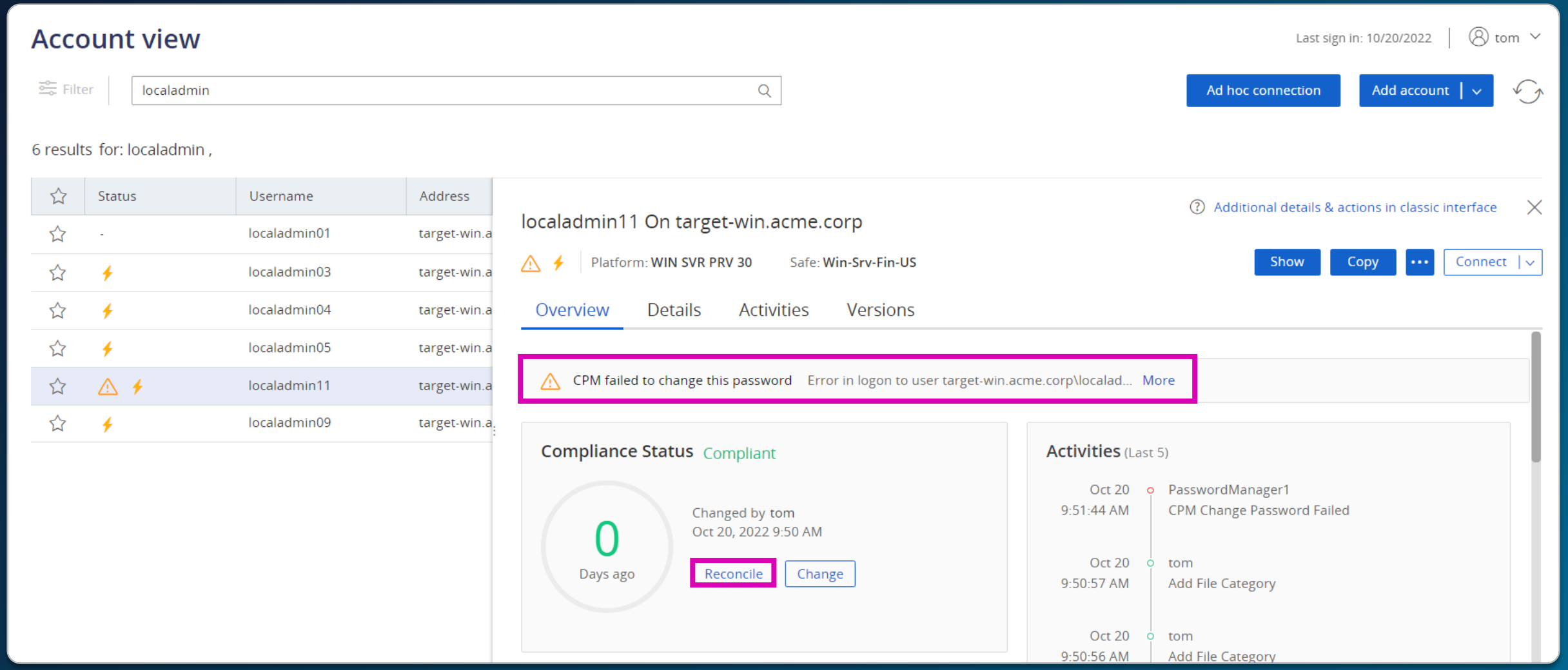
CYBERARK

Failed Verify and Reconcile Process



CYBERARK®

Manual Reconciliation



CYBERARK

Logon Account vs. Reconcile Account

Logon Account

- Used when a user is prevented from logging on and the password is known
- Used on a regular basis – i.e., it is common to block root access via SSH
- A ‘super user’ such as root should not be used as a logon account

Reconcile Account

- Used for ‘lost’ or unknown passwords
- Should be used infrequently
- Needs to have elevated privileges (member of local administrators)
- This account is usually a service account reserved for this purpose

SSH Key Management

SSH – Password Authentication

- Client launches the connection.
- Server presents its public key.
- Client and server negotiate a symmetric session key. All further communication is encrypted with the symmetric session key.
- User enters the account password and the Server authenticates it.

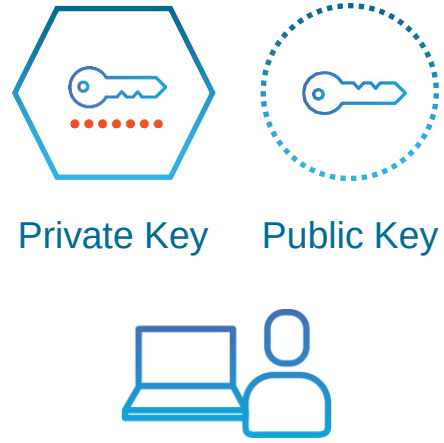
```
[root@centos-target01 ~]# ssh root@10.0.1.16
The authenticity of host '10.0.1.16 (10.0.1.16)' can't be
established.
RSA key fingerprint is
b0:38:8a:73:92:14:2a:92:f4:fa:25:68:5b:4e:80:77.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.16' (RSA) to the list of
known hosts.
root@10.0.1.16's password: ********
[root@psmp-psmgw ~]#
```

CYBERARK®

SSH – Asymmetric Key Authentication

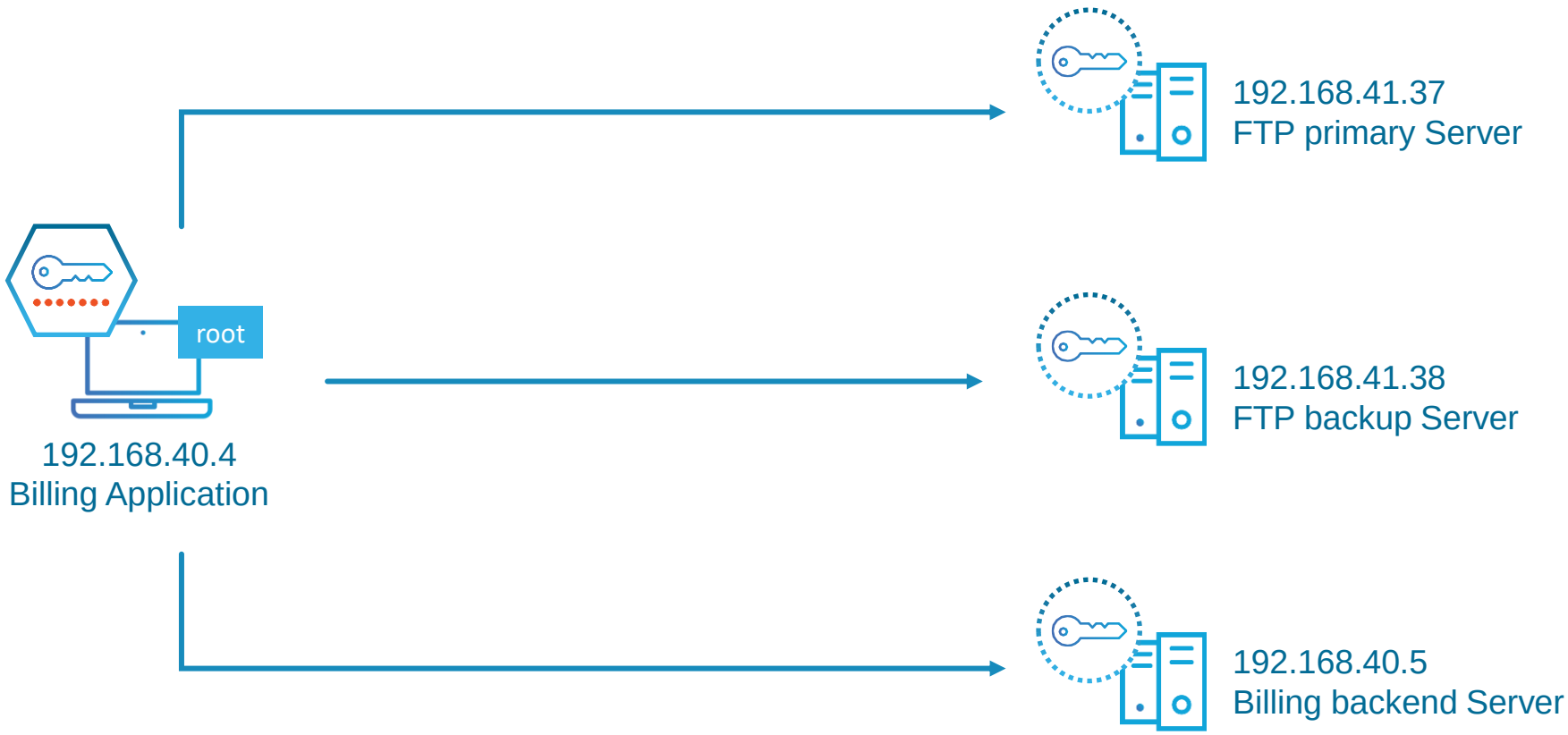
To authenticate with SSH keys, the user must first generate a public/private key-pair locally on her machine and then install the public key in her user directory on the target server (or servers) through a password authenticated session.

- Once that is done, the user can authenticate using the SSH keys.
- She launches a connection to the remote server.
- The server then encrypts a random prime number with the user's **public** key and transmits that back to the user, who must then decrypt the number with her corresponding private key.
- She then generates a hash of the prime number and returns it to the server.
- The server compares it with its own hash of the prime. If they match, then this proves that the user must have the private half of the key-pair
- The server therefore allows the connection to be established.



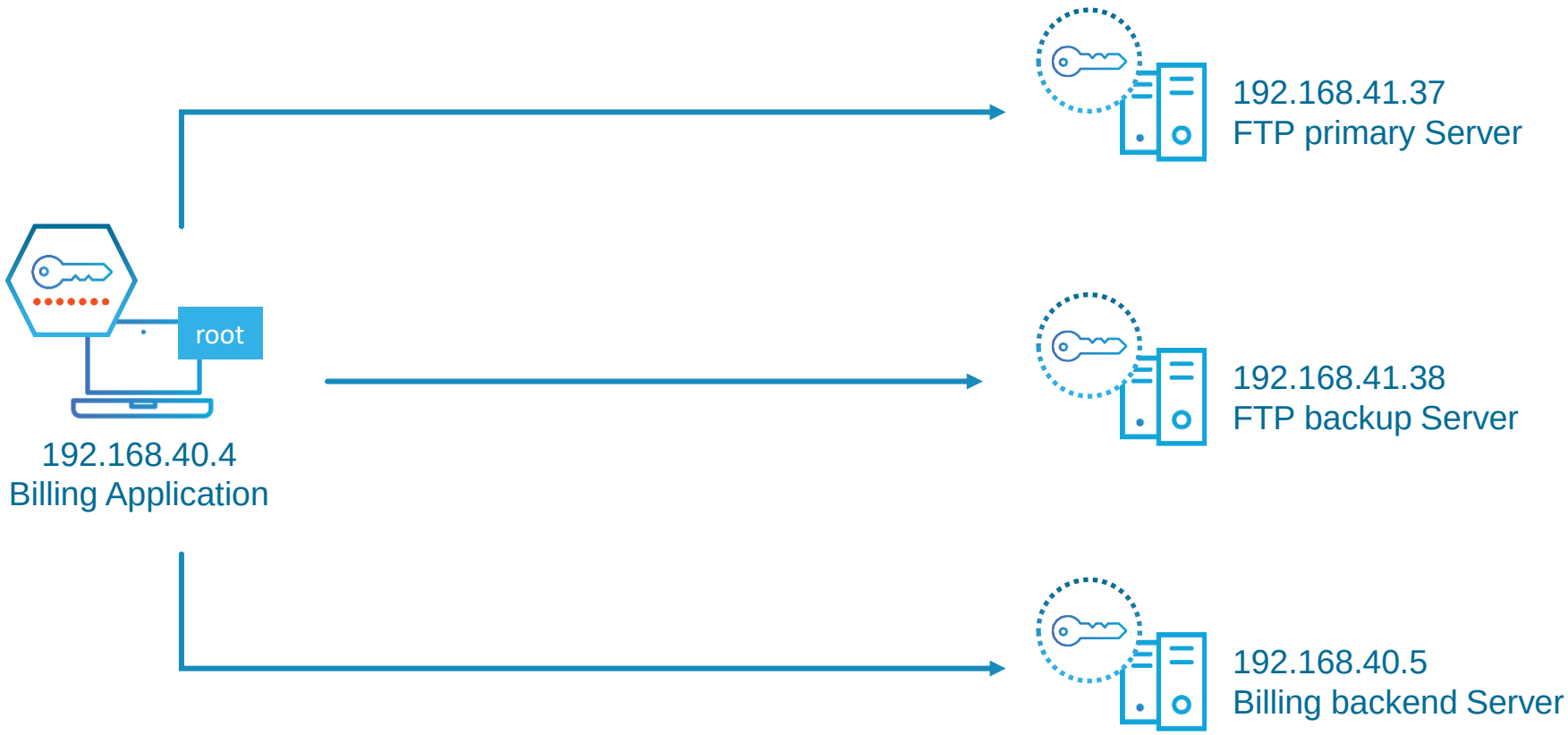
SSH Key Advantages

- SSH keys allow a substantially longer secret between client and server than a password.
- The secret is never transmitted over the network.
- One private key can be used to access multiple systems



SSH Key Disadvantages

- One private key can be used to access multiple systems. If it is compromised, all the systems that trust it are vulnerable
- SSH keys are more difficult to change than passwords

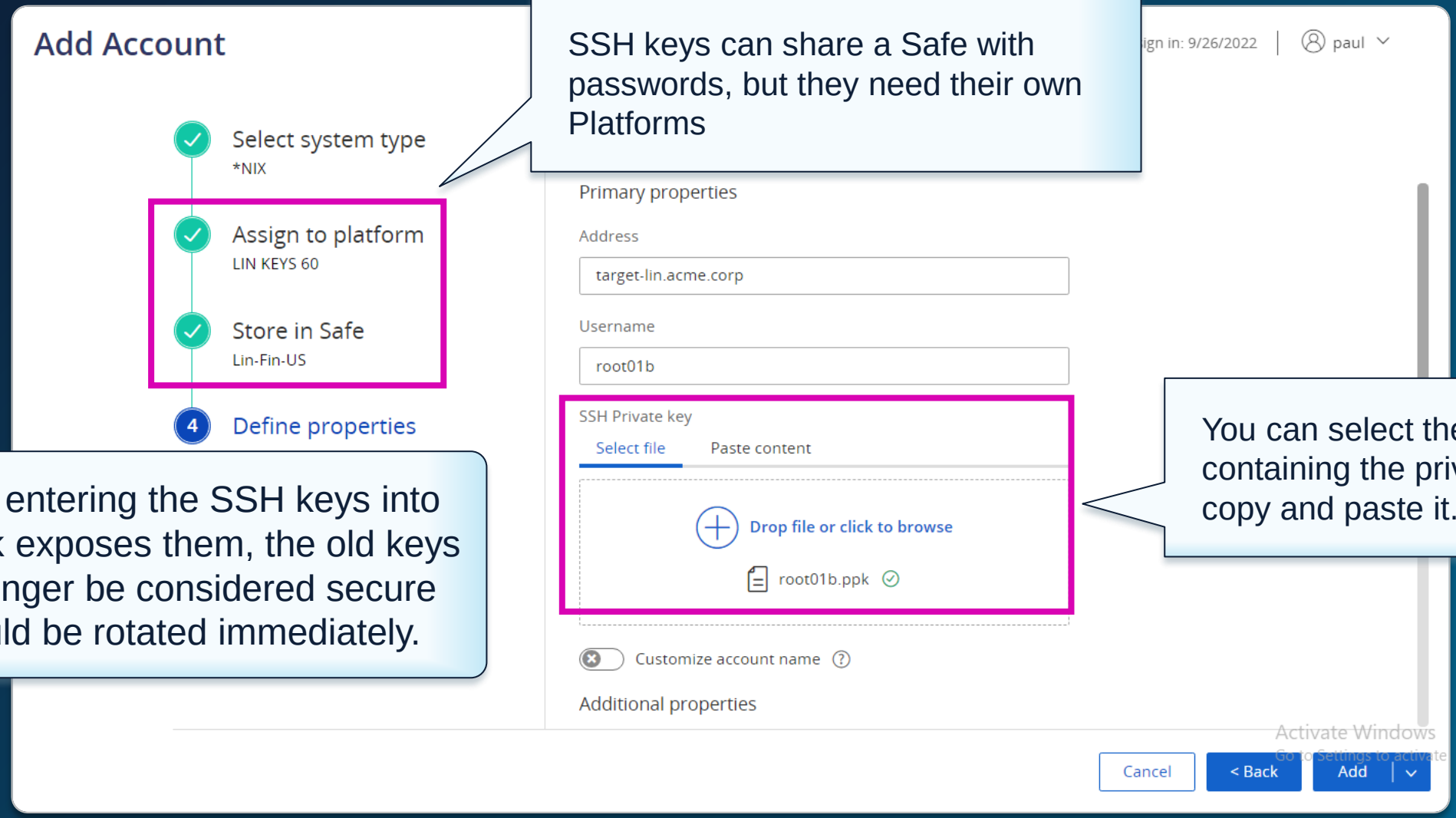


SSH Key Manager

- Creates unique key-pairs for each target system.
- Private keys are stored in the **Vault**, not on user workstations.
- The **CPM** changes key-pairs often and automatically disseminates public keys to target systems.
- End users retrieve the private key from the **Vault** to authenticate to the target system.

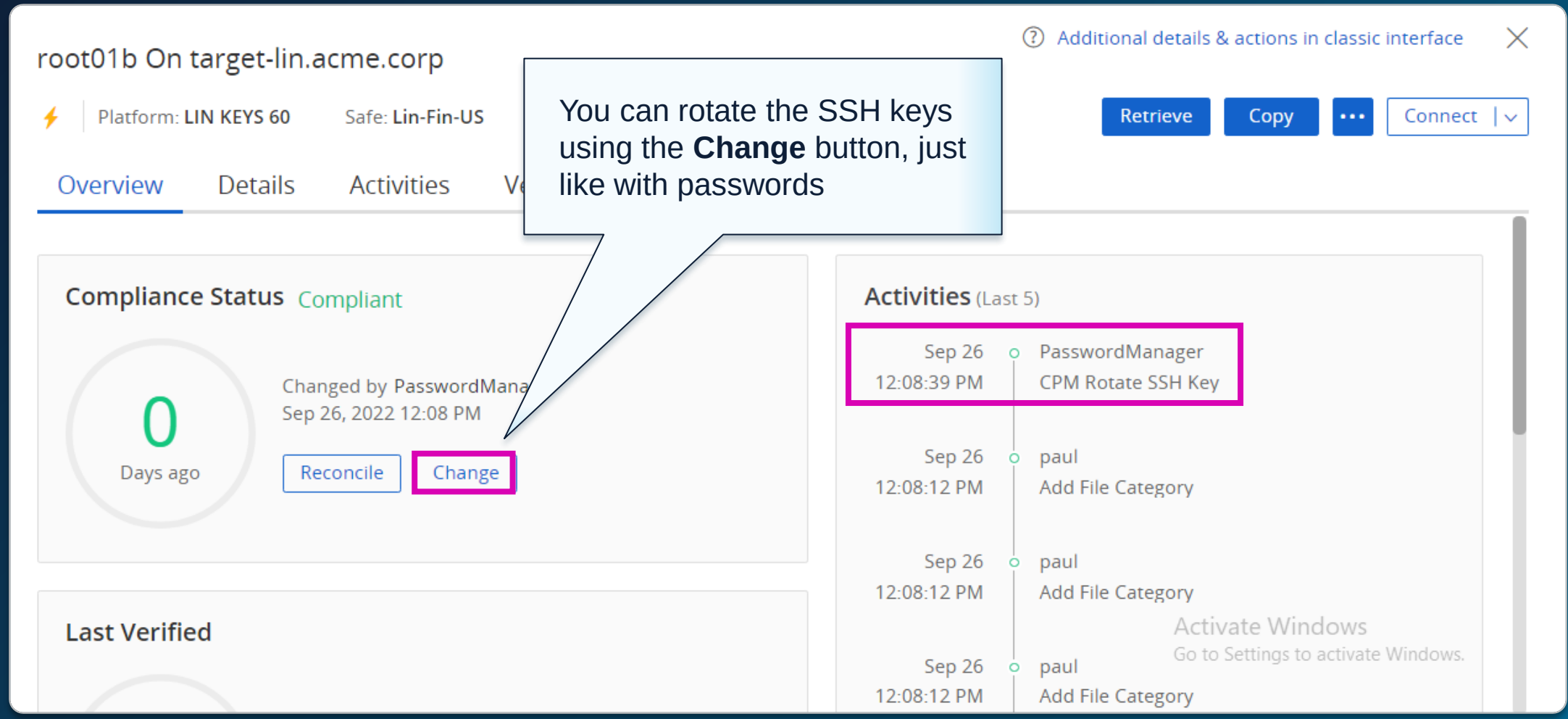
CYBERARK®

Adding Keys to the Vault



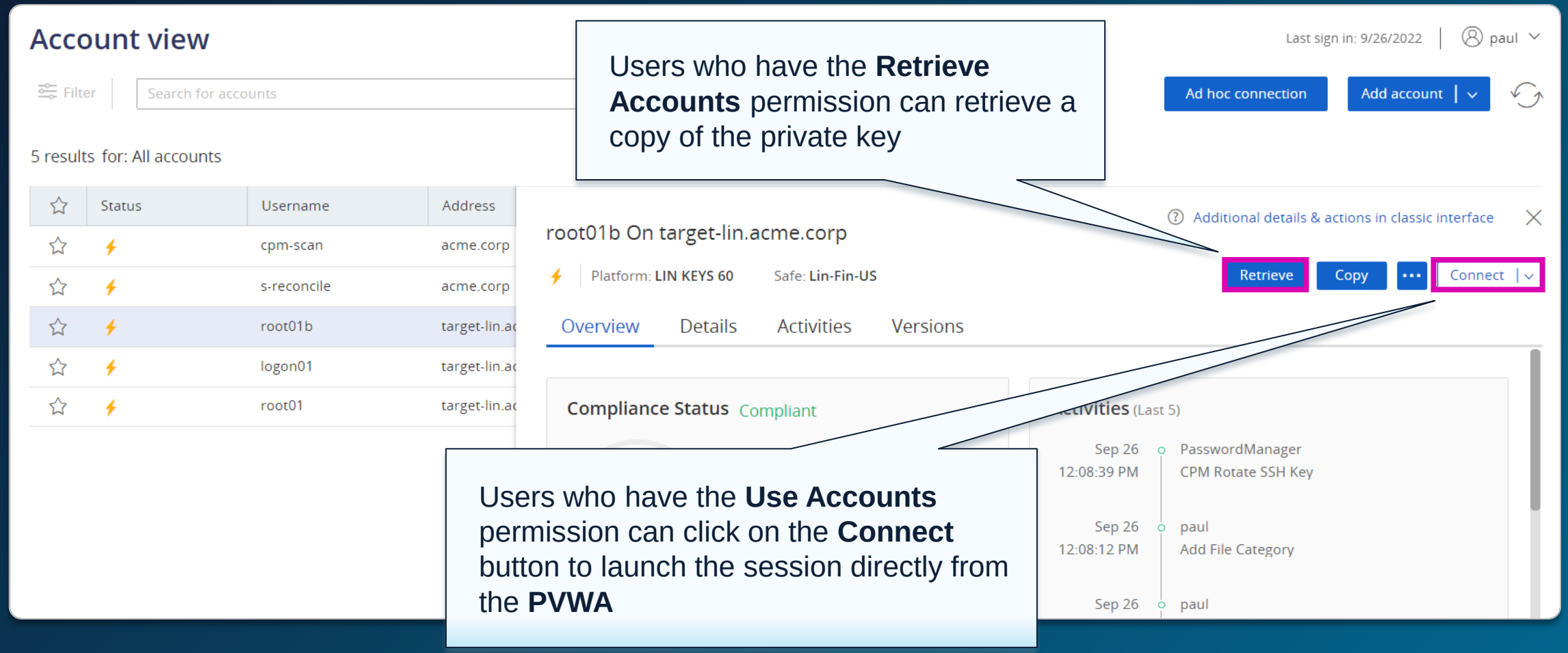
CYBERARK

Rotate Keys



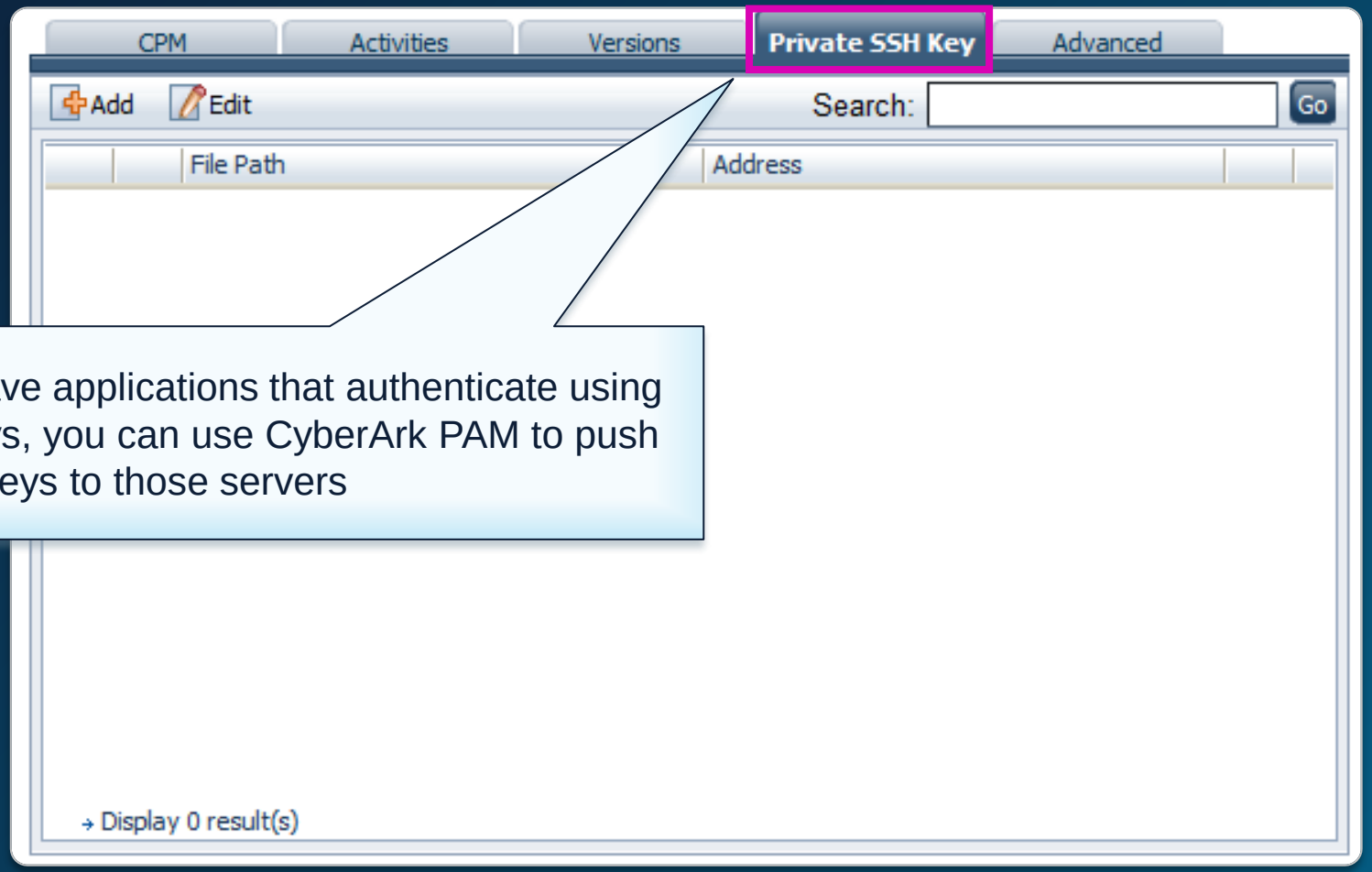
CYBERARK

Retrieve / Connect



CYBERARK

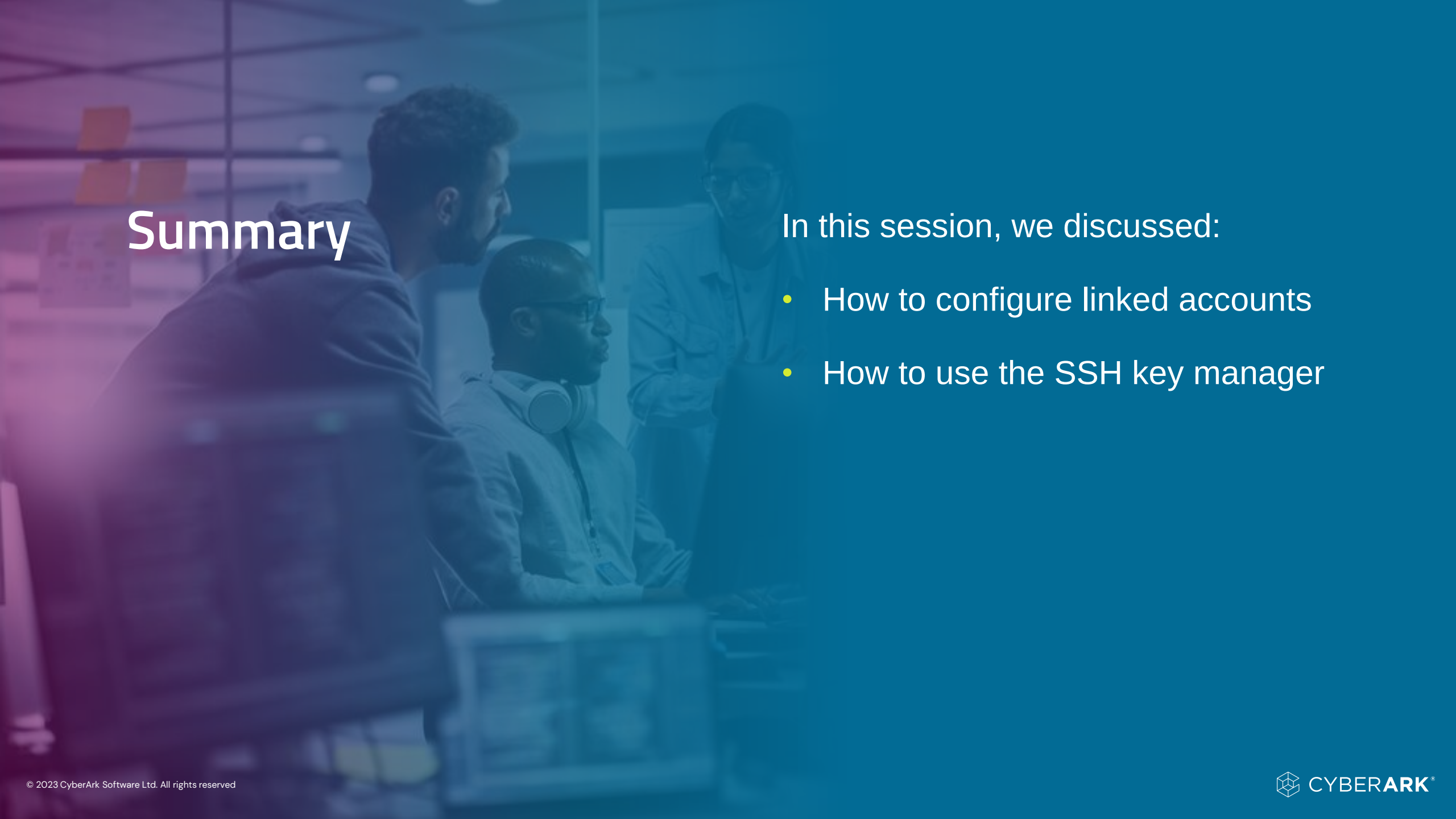
Push Private Keys to Application Servers



If you have applications that authenticate using SSH keys, you can use CyberArk PAM to push private keys to those servers

CYBERARK®

Summary



Summary

In this session, we discussed:

- How to configure linked accounts
- How to use the SSH key manager

CYBERARK®

Additional Resources

Online Training

Linked Accounts (login required)

You may now complete the following exercises:

Linked Accounts

- Securing SSH Accounts Using a Logon account
- Securing Windows Server Local Accounts via a Reconcile Account

Securing Unix Accounts With SSH Keys

- Generating a Key-Pair
- Verify you can login with the Private Key
- Duplicating a Platform
- Add an Account with an SSH Key