CYBERARK®

PAM Administration

Accounts – Part 2

Agenda

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

- Describe and configure linked accounts:
  - Logon accounts
  - Reconcile accounts
- 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
```

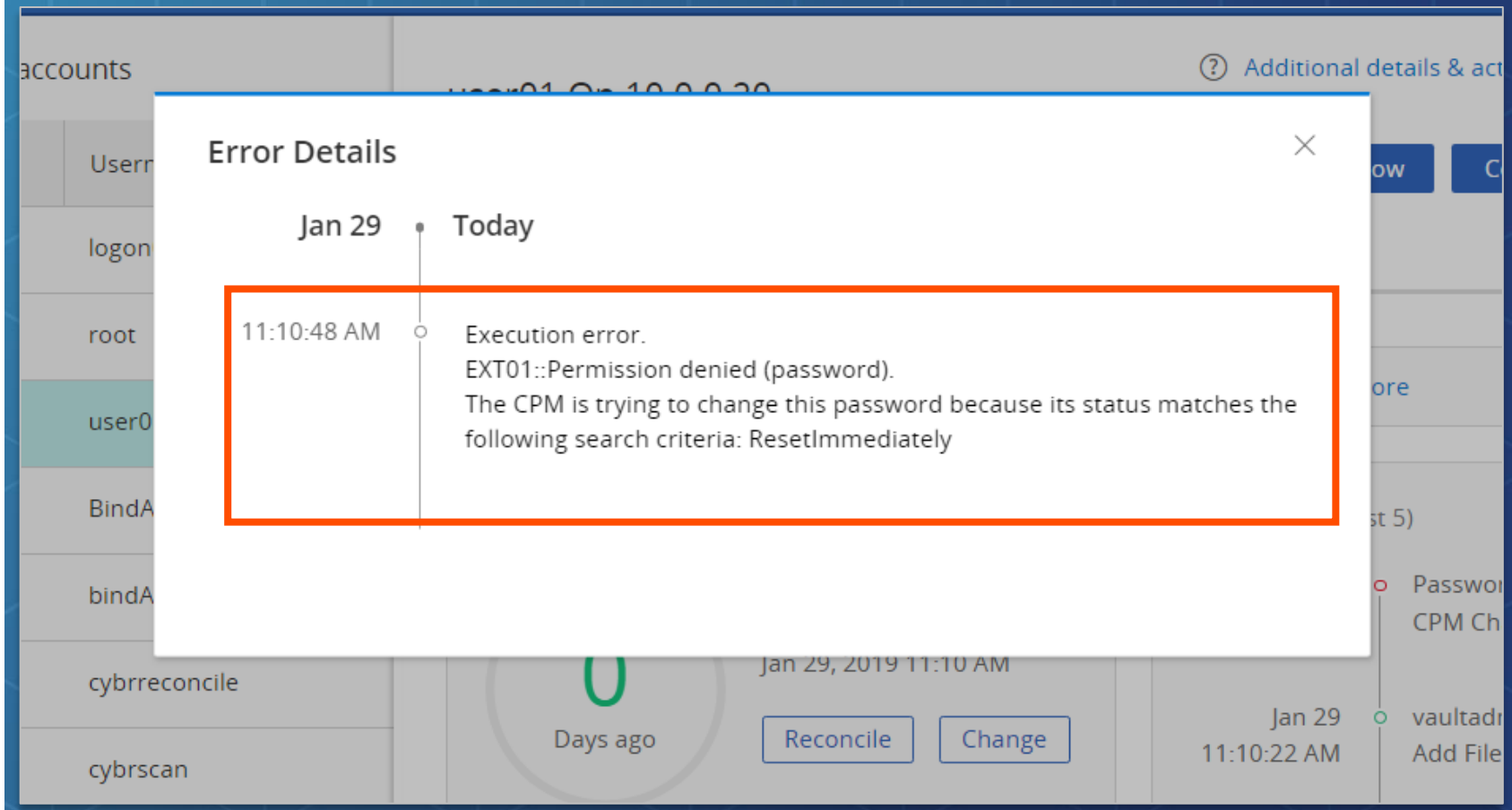
The root user is often prevented from logging in remotely as part of best practices (/etc/ssh/sshd_config > PermitRootLogin no)

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 ~]#
```

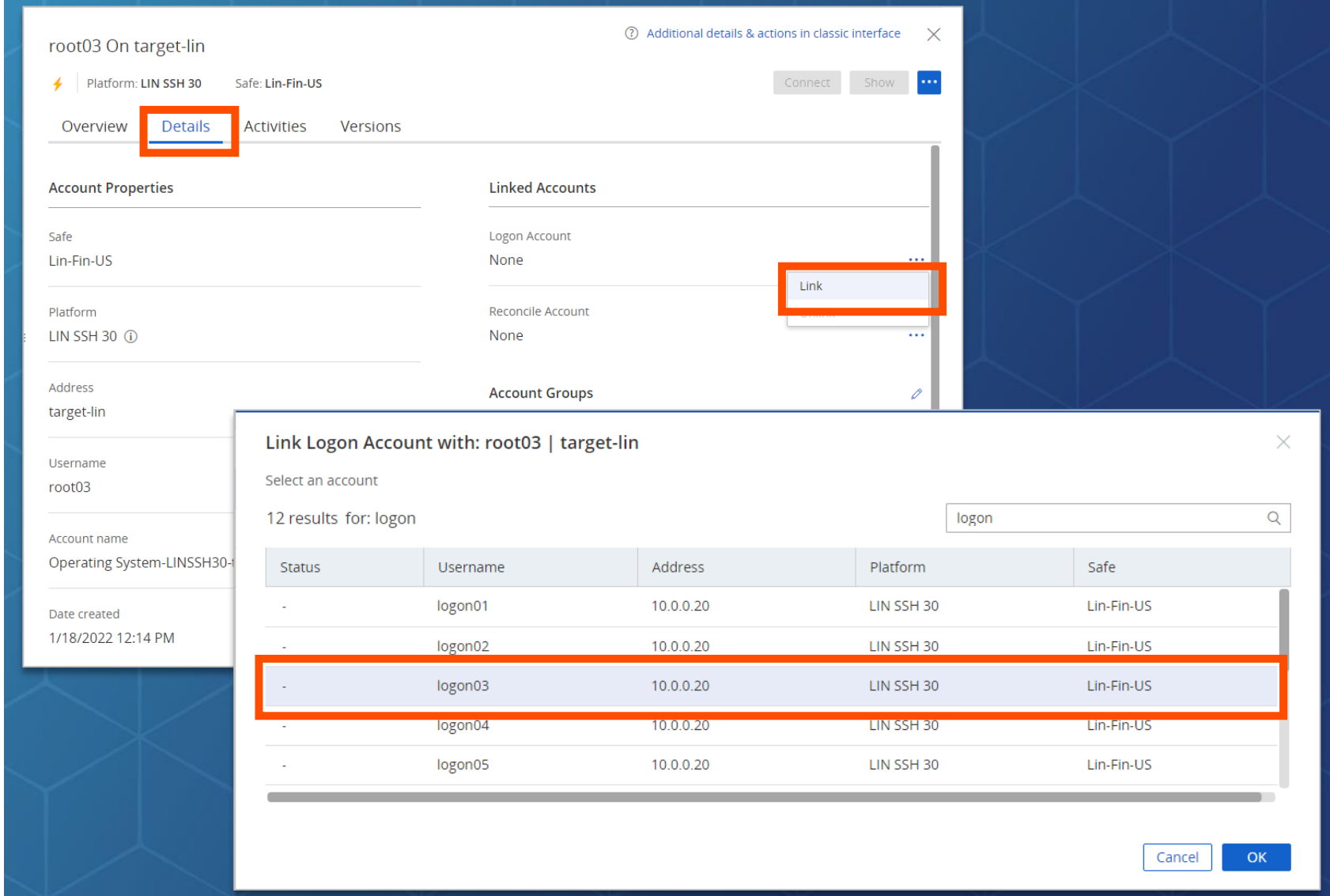
Root Password Change Failure

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



Associate Logon Account

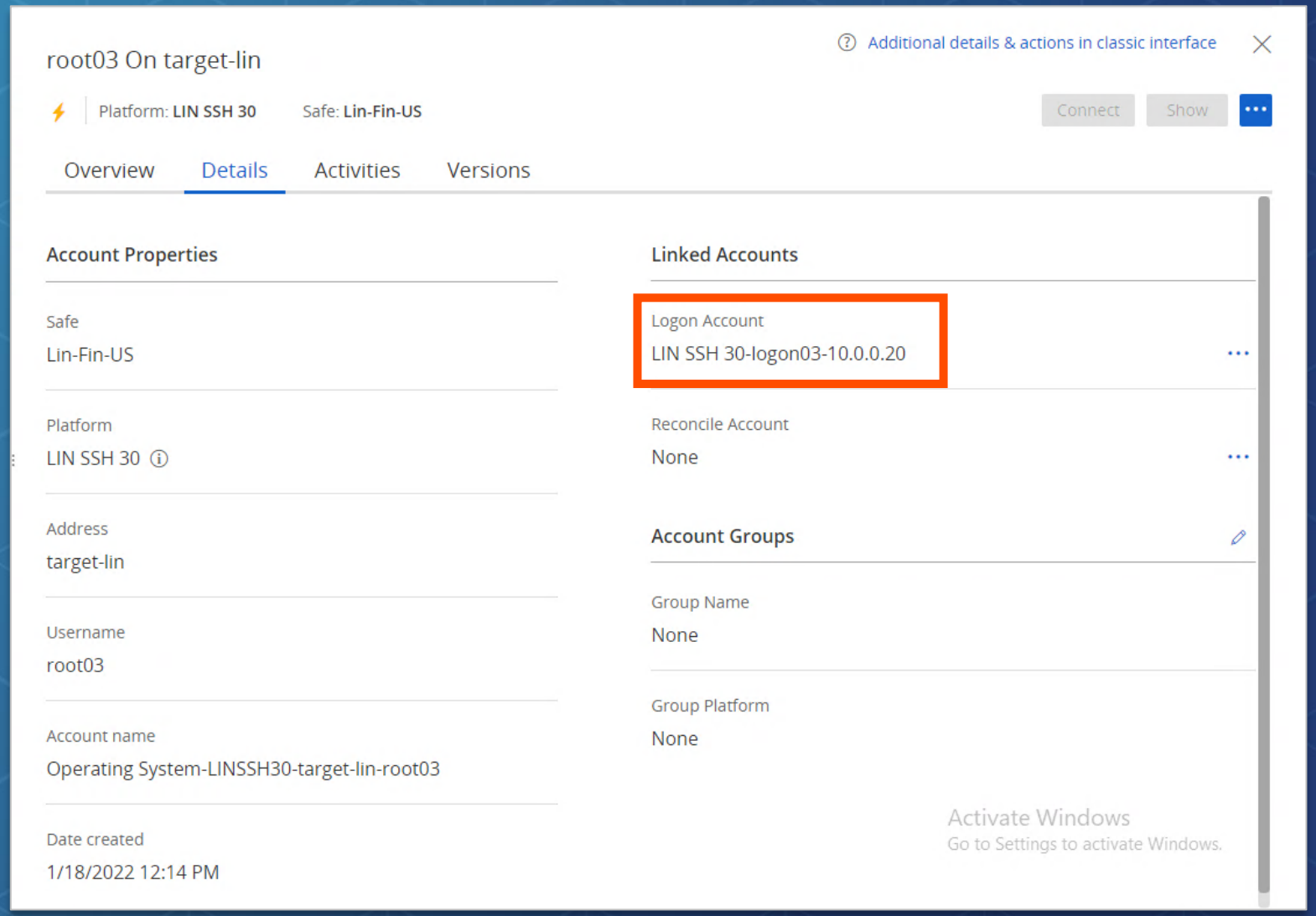
- The solution is to onboard a non-privileged account with the authorization to switch to root in order to perform the password change. This account is the ***Logon Account***
- To use a ***Logon Account***, you need to link it to the root account



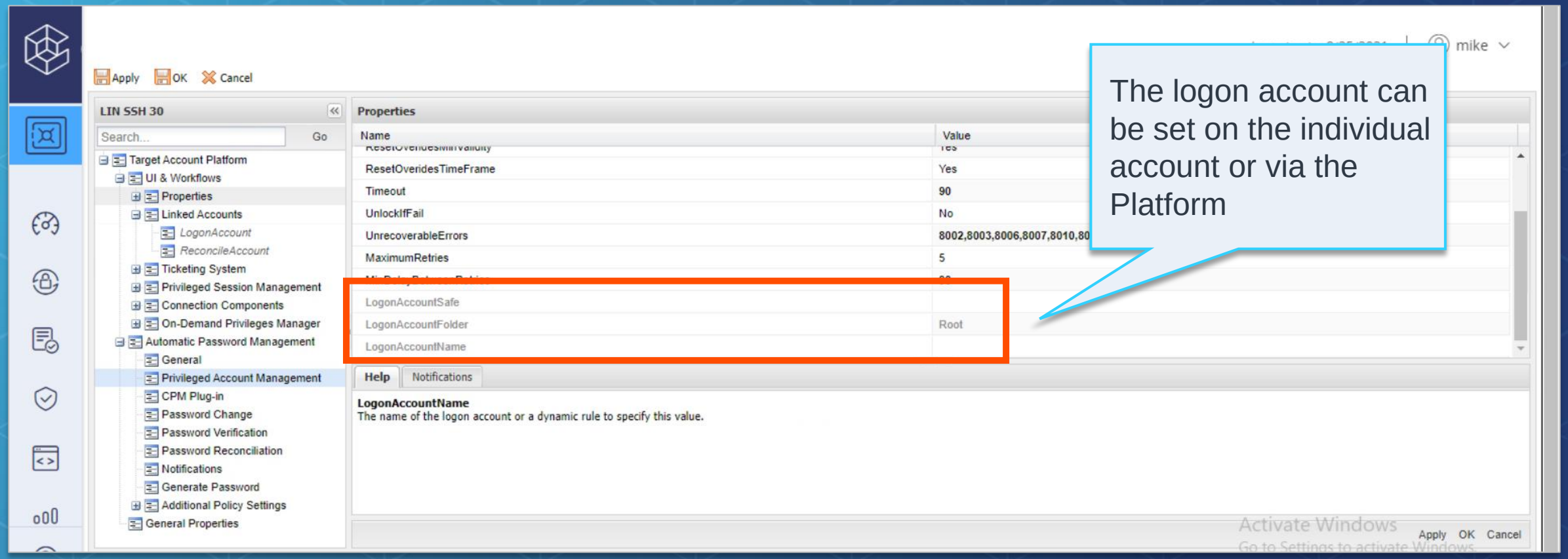
Root Password Change Success

- 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**



Logon Account – Platform Settings

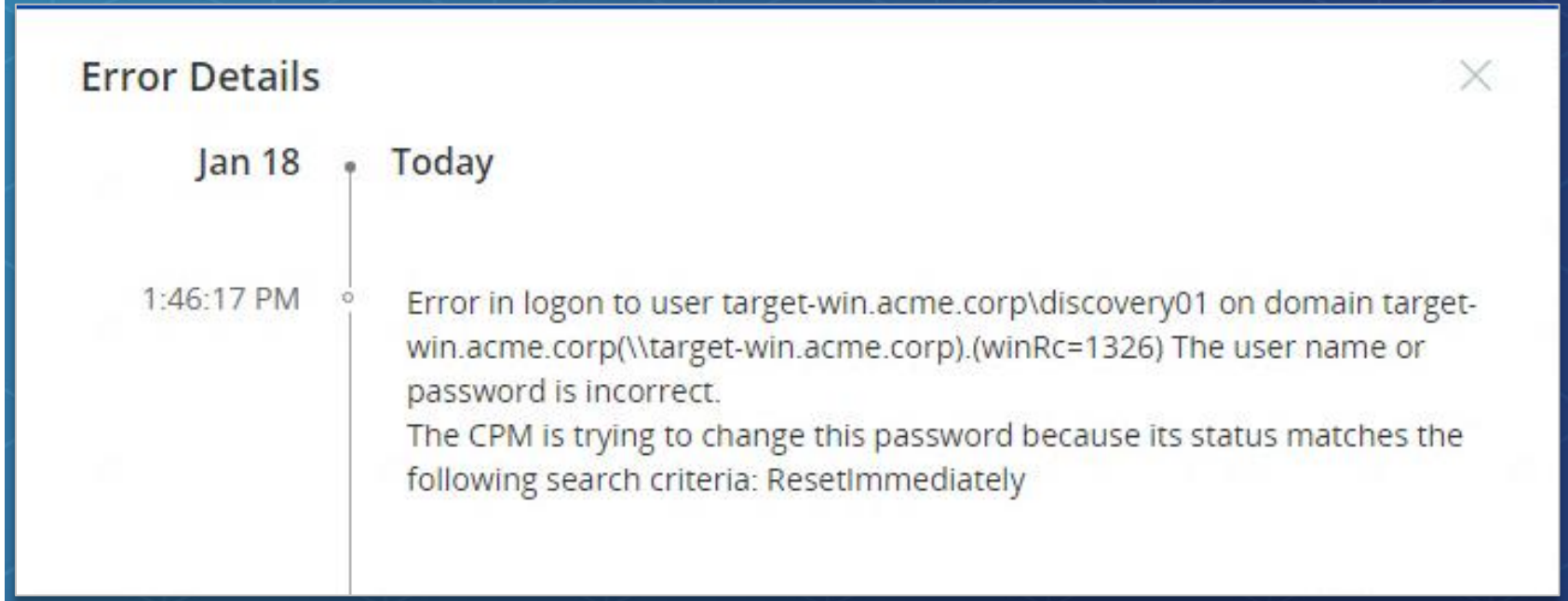


The logon account can be set on the individual account or via the Platform

Reconcile Accounts

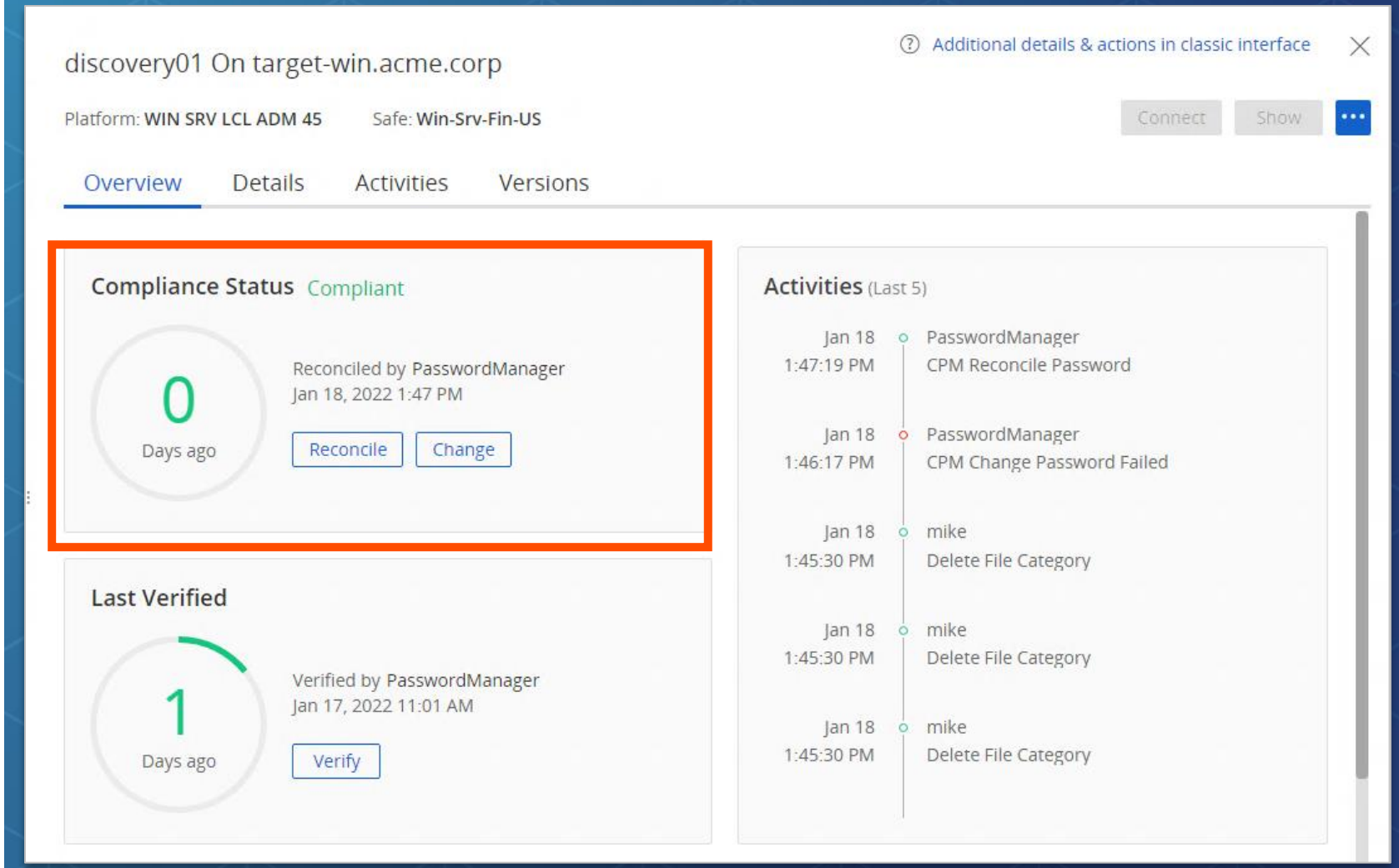
Reconciliation – Unknown Password

Reconciliation is used for situations where we don't know a password – for example, if the password in the **Vault** and on the Target machine have somehow become unsynchronized – or if the use of individual passwords would be too onerous – you have a fleet of Windows servers, each with its own local admin password, and you want to onboard them all at once, not one by one.

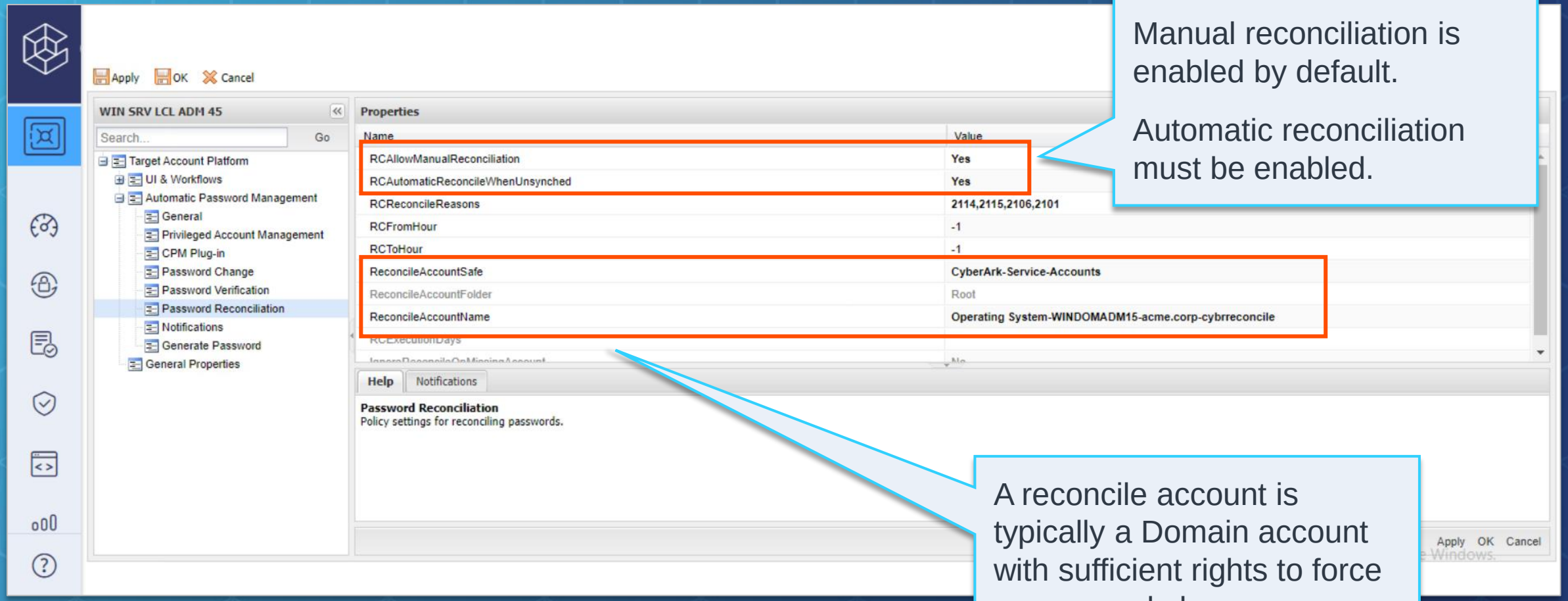


Reconciliation – Unknown Password

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



Associating a Reconcile Account

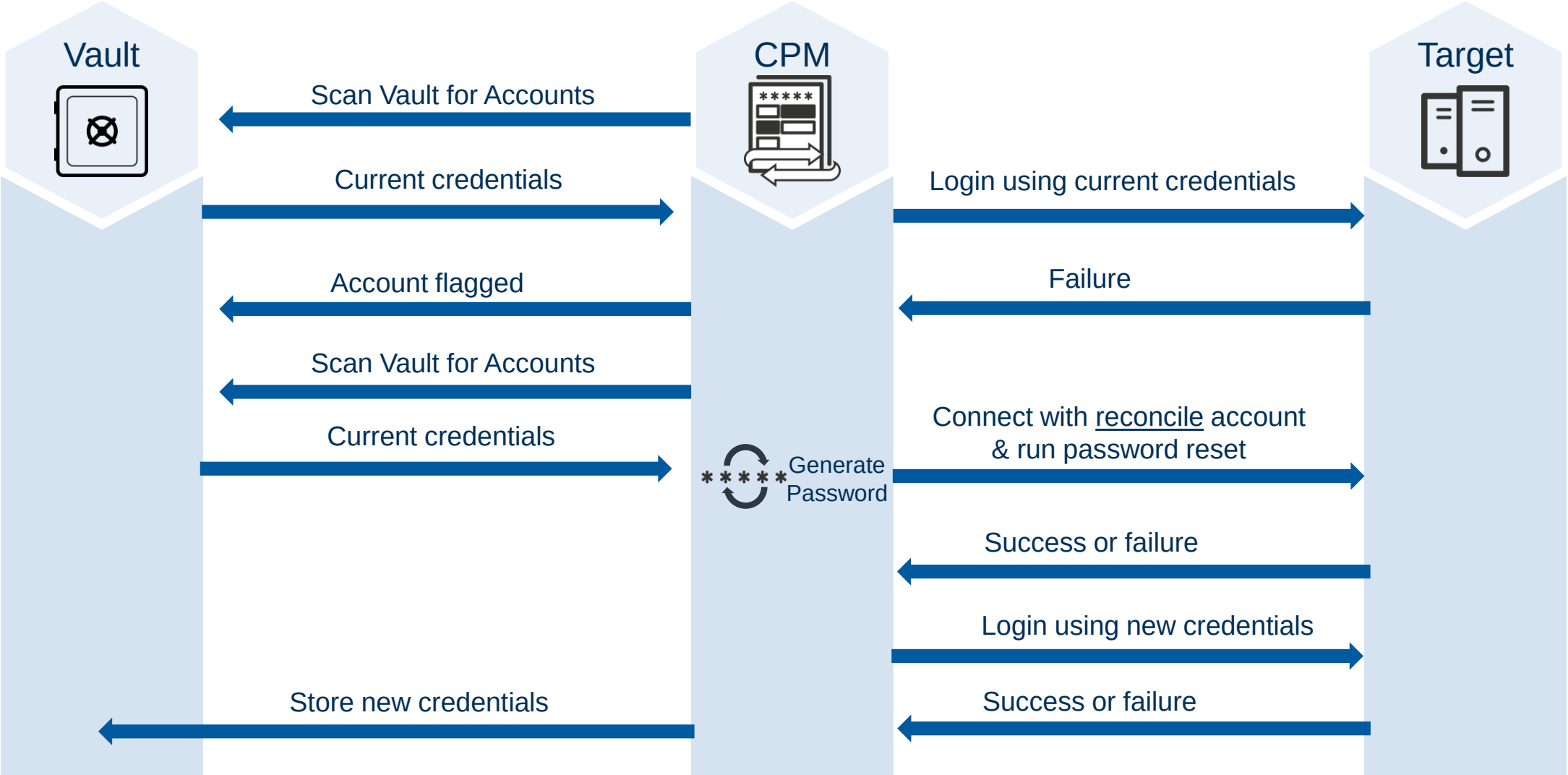


Manual reconciliation is enabled by default.

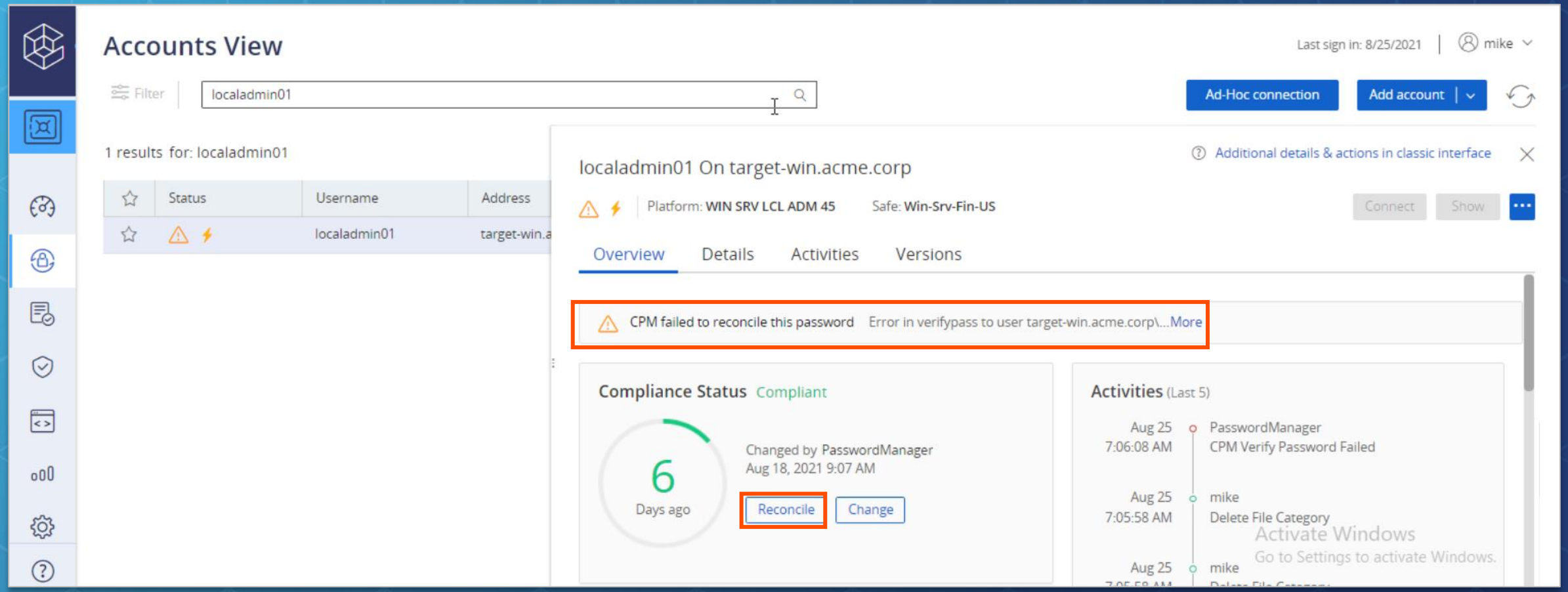
Automatic reconciliation must be enabled.

A reconcile account is typically a Domain account with sufficient rights to force a password change

Failed Verify and Reconcile Process



Manual Reconciliation



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 (i.e. Domain Admin) • This account is usually a service account reserved for this purpose

SSH Key Management

SSH – Password Authentication

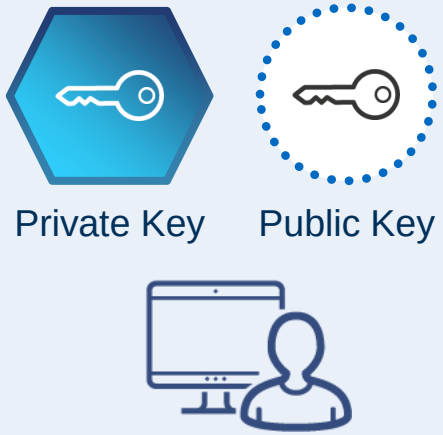
- Client launches the connection.
- Server presents its public key.
- Client and server negotiate a symmetric session key. All further communication is encrypted with the symmetric session key.
- User enters the account password and the Server authenticates it.

```
[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 ~]#
```

SSH – Asymmetric Key Authentication

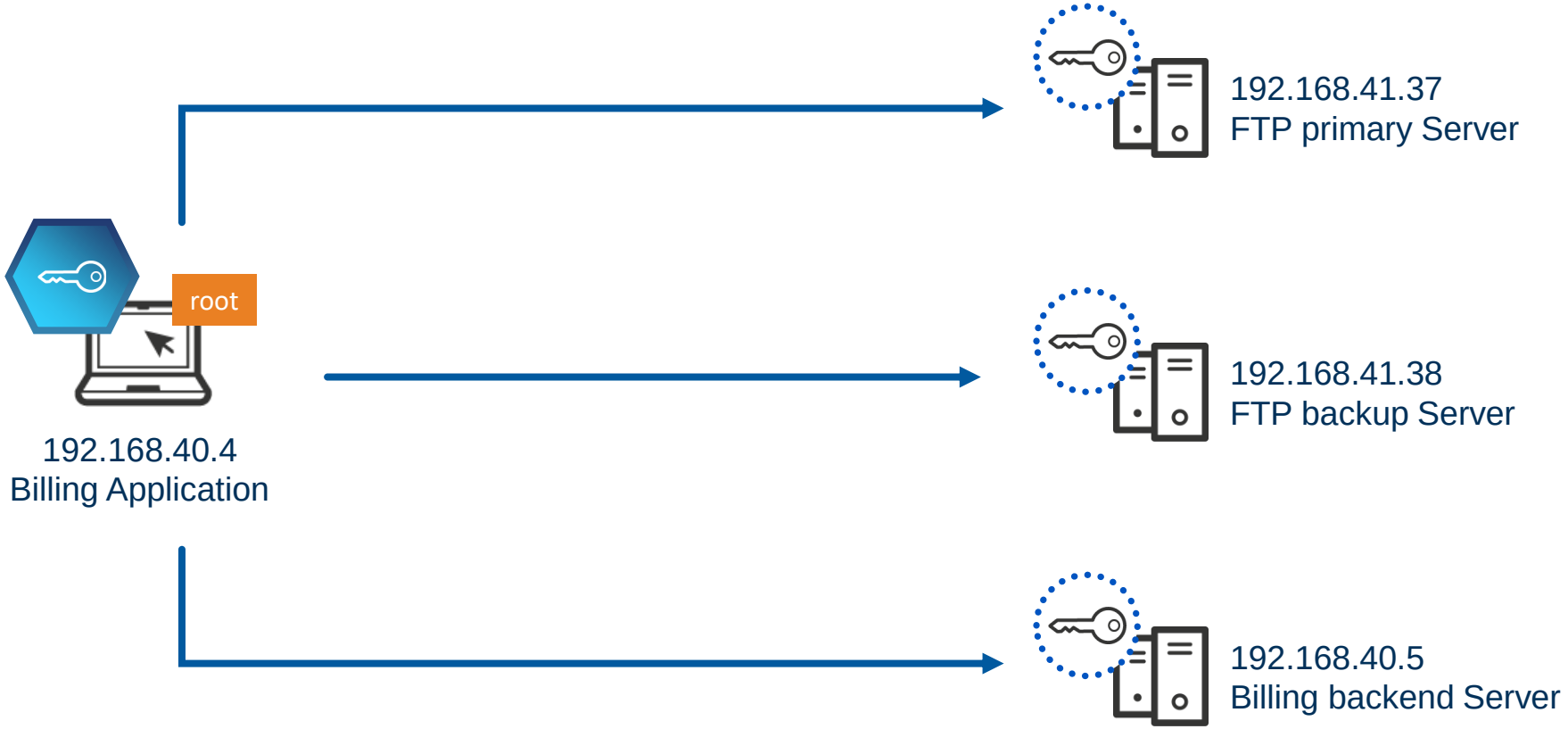
To authenticate with SSH keys, the user must first generate a public/private key-pair locally on her machine and then install the public key in her user directory on the target server (or servers) through a password authenticated session.

- 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 (because only the private key can decrypt what has been encrypted with the public key.)
- The server therefore allows the connection to be established.



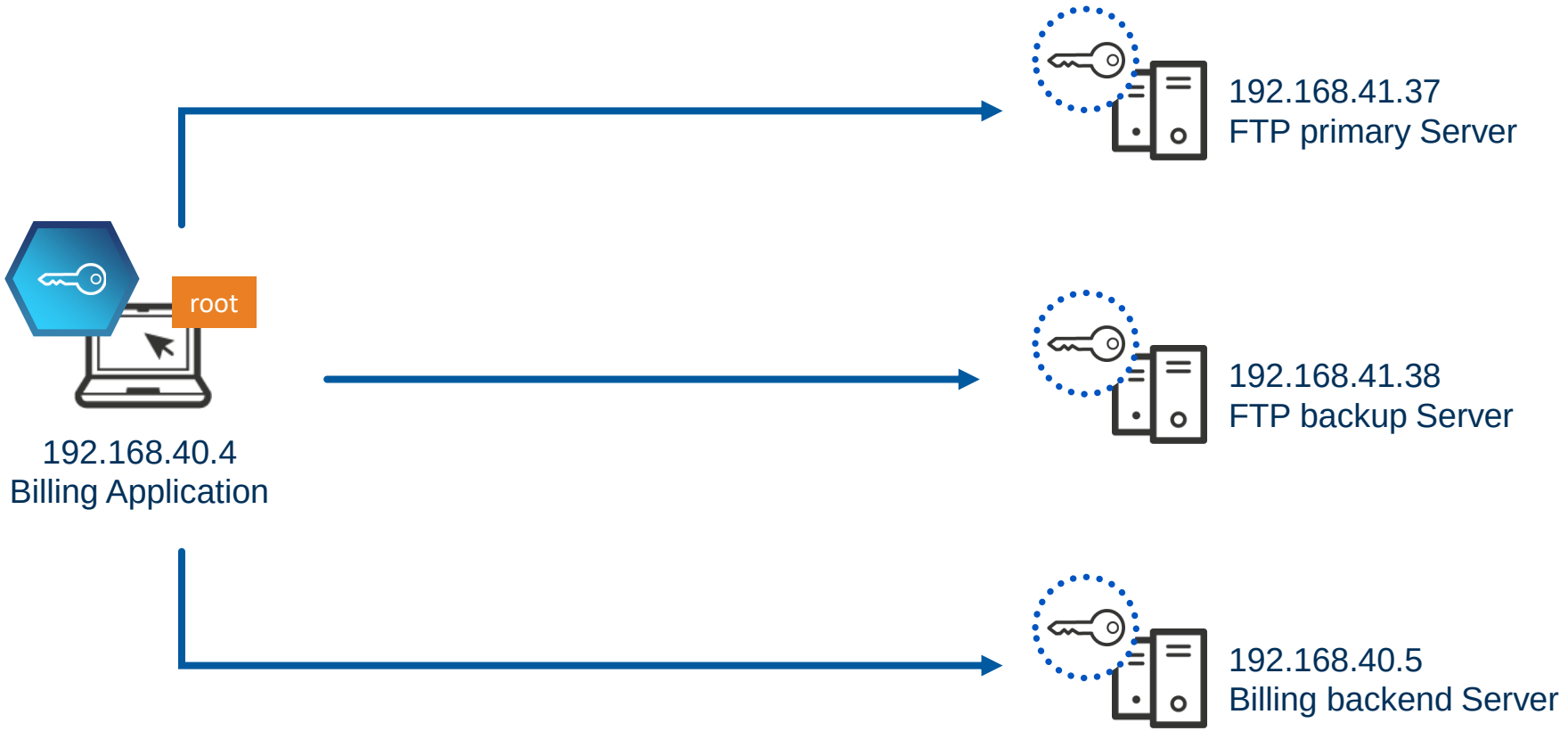
SSH Key Advantages

- 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

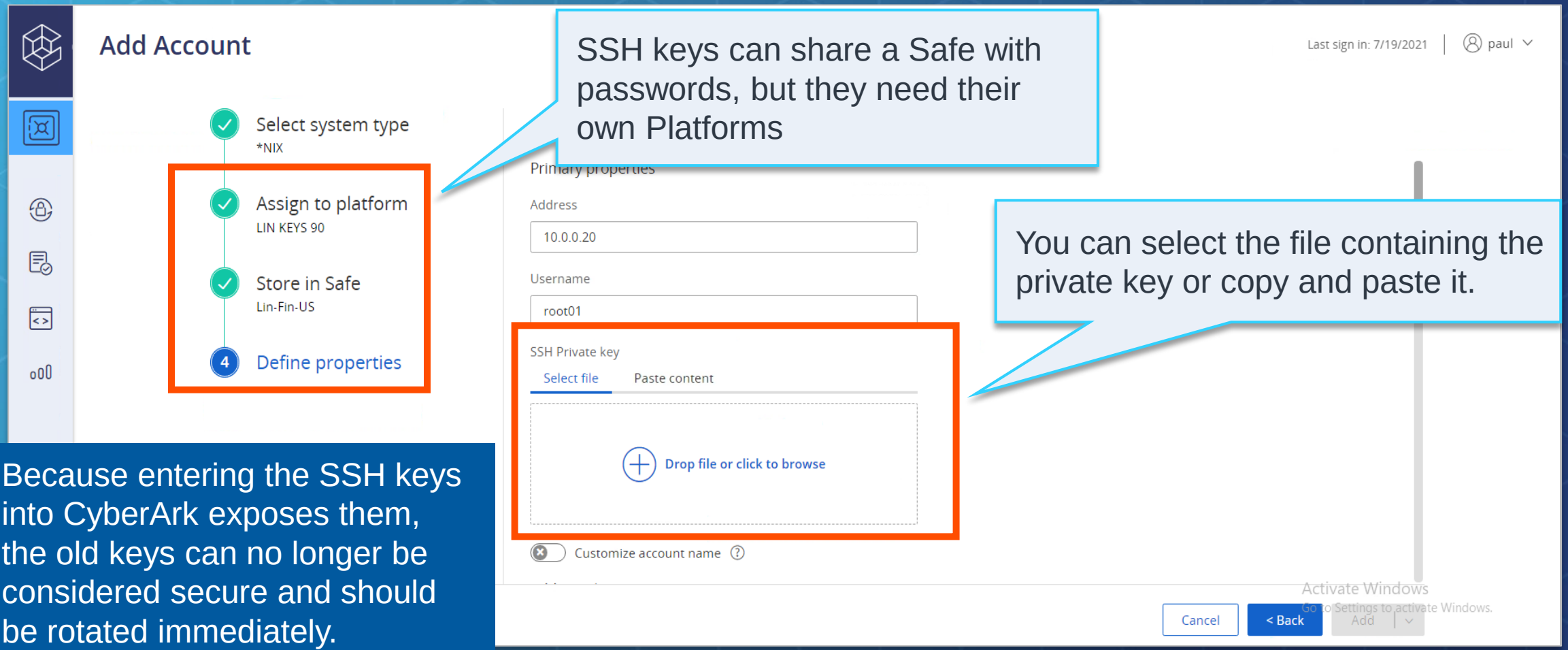
- One private key can be used to access multiple systems. If it is compromised, all the systems that trust it are vulnerable
- SSH keys are more difficult to change than passwords



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.

Adding Keys to the Vault

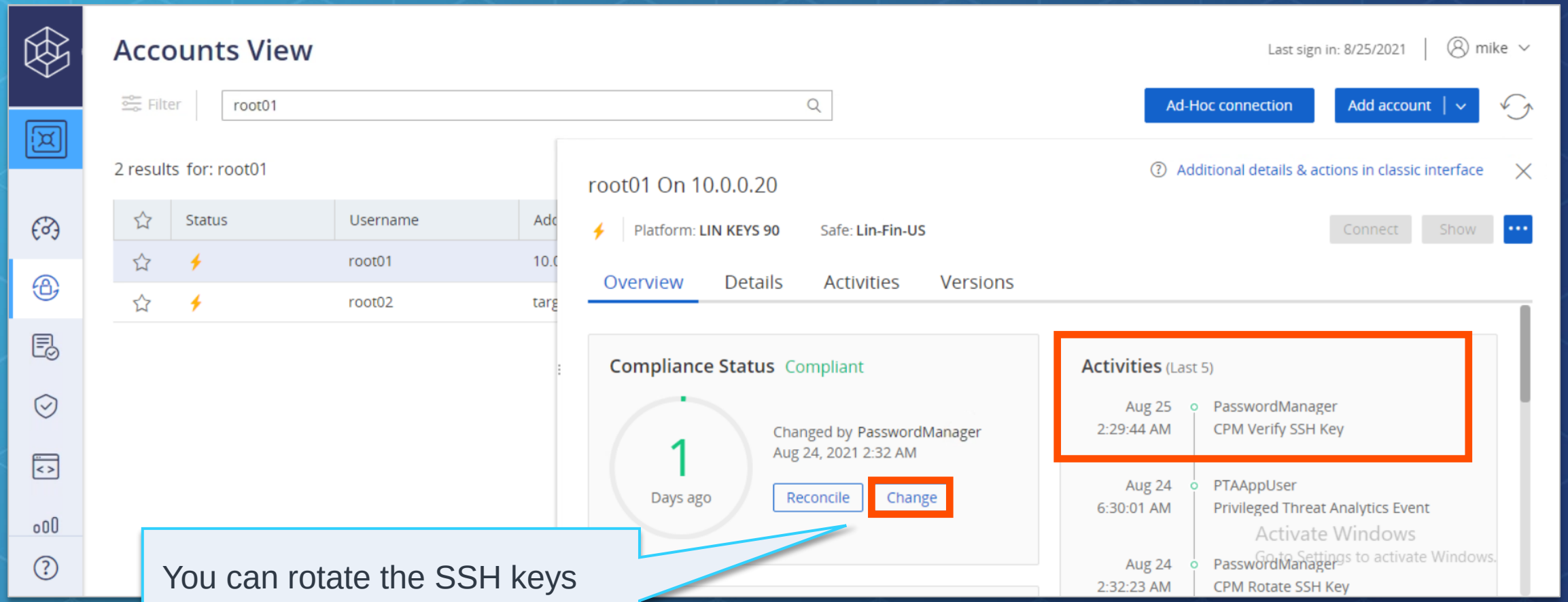


SSH keys can share a Safe with passwords, but they need their own Platforms

You can select the file containing the private key or copy and paste it.

Because entering the SSH keys into CyberArk exposes them, the old keys can no longer be considered secure and should be rotated immediately.

Rotate Keys



You can rotate the SSH keys using the **Change** button, just like with passwords

Retrieve / Connect

Accounts View

Filter | root01

2 results for: root01

Status	Username	Ad
	root01	10.
	root02	targ

Last sign in: 8/25/2021 | paul

Ad-Hoc connection | Add account

Additional details & actions in classic interface

Platform: LIN KEYS 90 Safe: Lin-Fin-US

Retrieve | Copy | ••• | Connect

Overview | Details | Activities | Versions

us Compliant

Changed by PasswordManager
Aug 24, 2021 2:32 AM

Reconcile | Change

Activities (Last 5)

Aug 25 2:29:44 AM — PasswordManager CPM Verify SSH

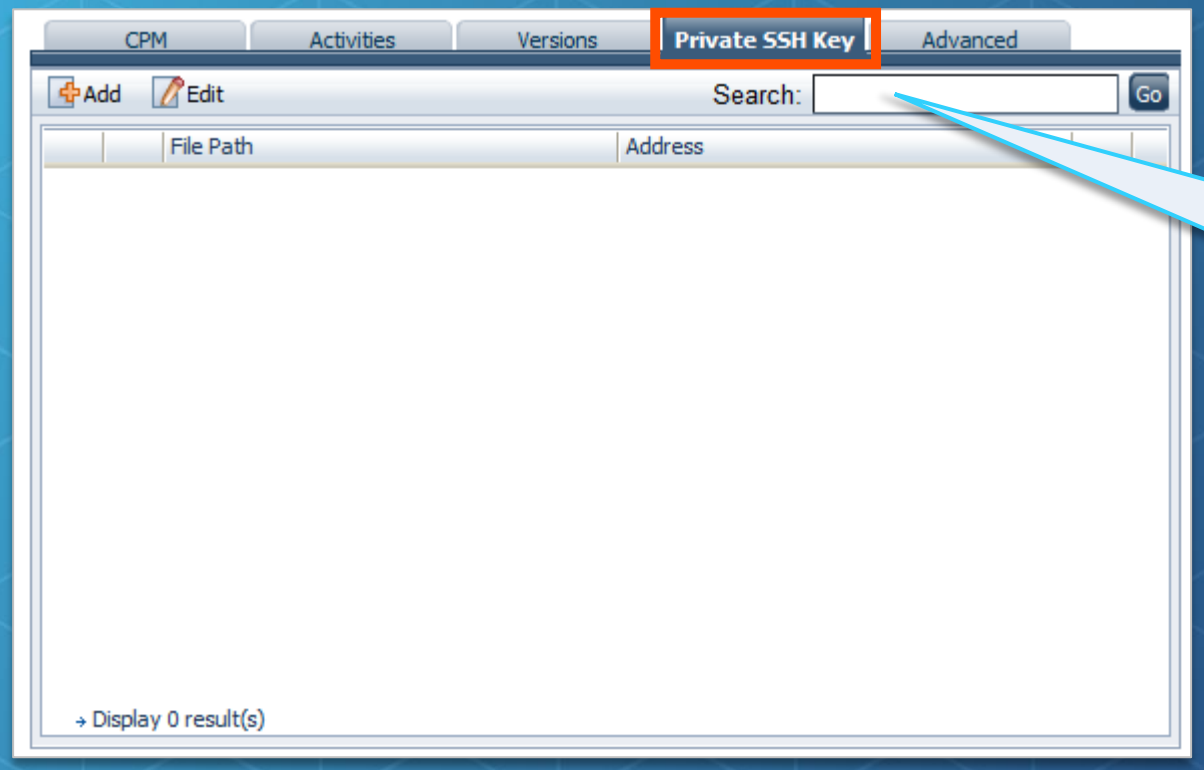
Aug 24 6:30:01 AM — PTAApp Privil cs Event

```
root@target-lin:~
Using username "root01".
Authenticating with public key "rsa-key-20210307"
Last login: Sun Mar  7 13:56:52 2021 from pvwa.acme.corp
[root@target-lin ~]#
[root@target-lin ~]#
```

Users who have the Retrieve Accounts permission can retrieve a copy of the private key

Users who have the **Use Accounts** permission can click on the Connect button to launch the session directly from the PVWA

Push Private Keys to Application Servers



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

Summary

Summary

In this session, we discussed:

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

Additional Resources

eLearning

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