CYBERARK®
The Identity Security Company™

PAM Administration

Accounts – Part 1

Agenda

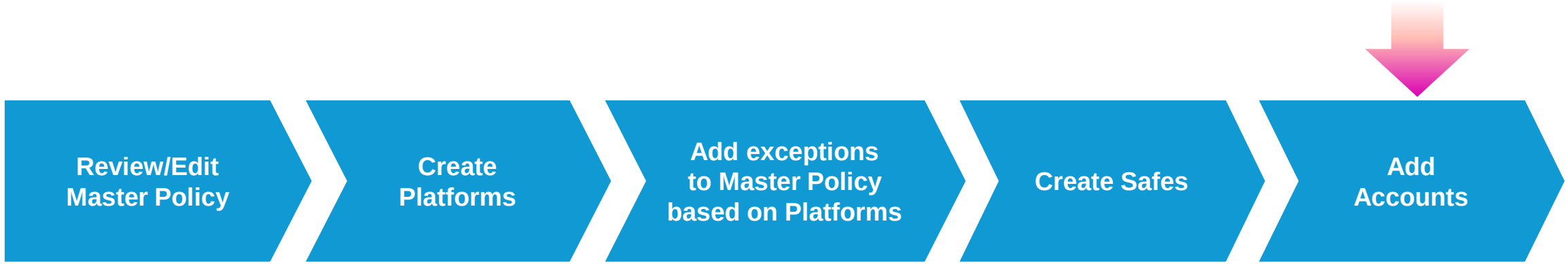
By the end of this session, you will be able to:

1. Add an **Account** via the **PVWA**
2. Understand the different password management operations

Overview

CYBERARK®

Policies, Platforms, Safes, and Accounts



- Business/audit rules for managing passwords
- Global policy settings

- Technical settings for managing passwords and connecting to target systems
- Basis for exceptions

- Exceptions to Master Policy rules

- Access control

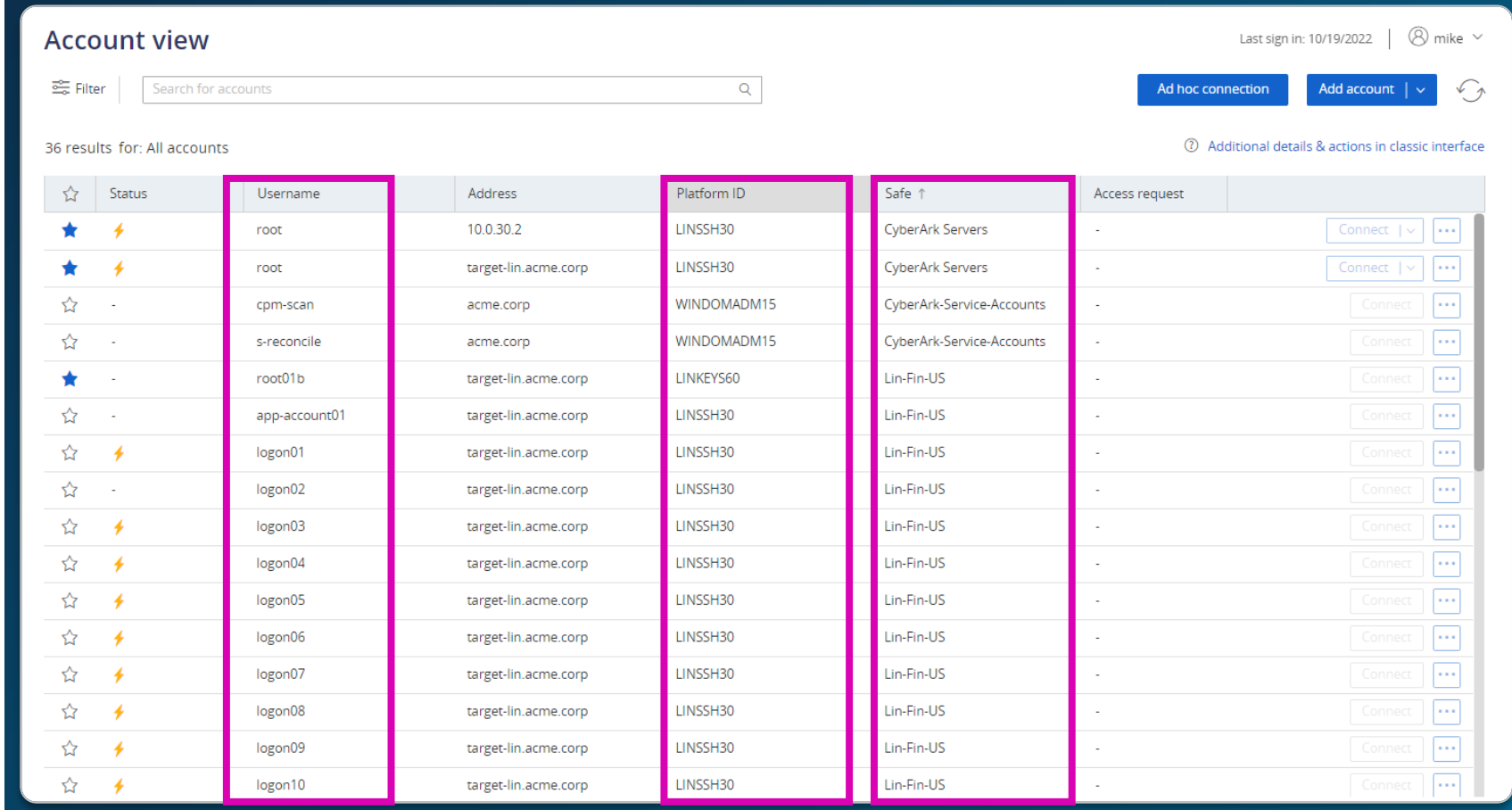
- Individual objects containing the required information (address, username, password, etc.) to manage privileged accounts

CYBERARK®

Accounts

Accounts – The actual privileged account IDs and passwords

- Stored in ***Safes***
- Examples include:
  - Domain administrators
  - Local administrators
  - Root accounts
  - Service accounts
  - And more
- Every account resides in a single ***Safe***
- Every account is associated with a single ***Target Account Platform***



CYBERARK

Add An Account

CYBERARK®

Add A New Linux Account

Master Policy

- Change passwords every 60 days

Platform: LIN SSH 30

- Password length should be 10 characters long
- Master Policy Exception: Change password every 30 days

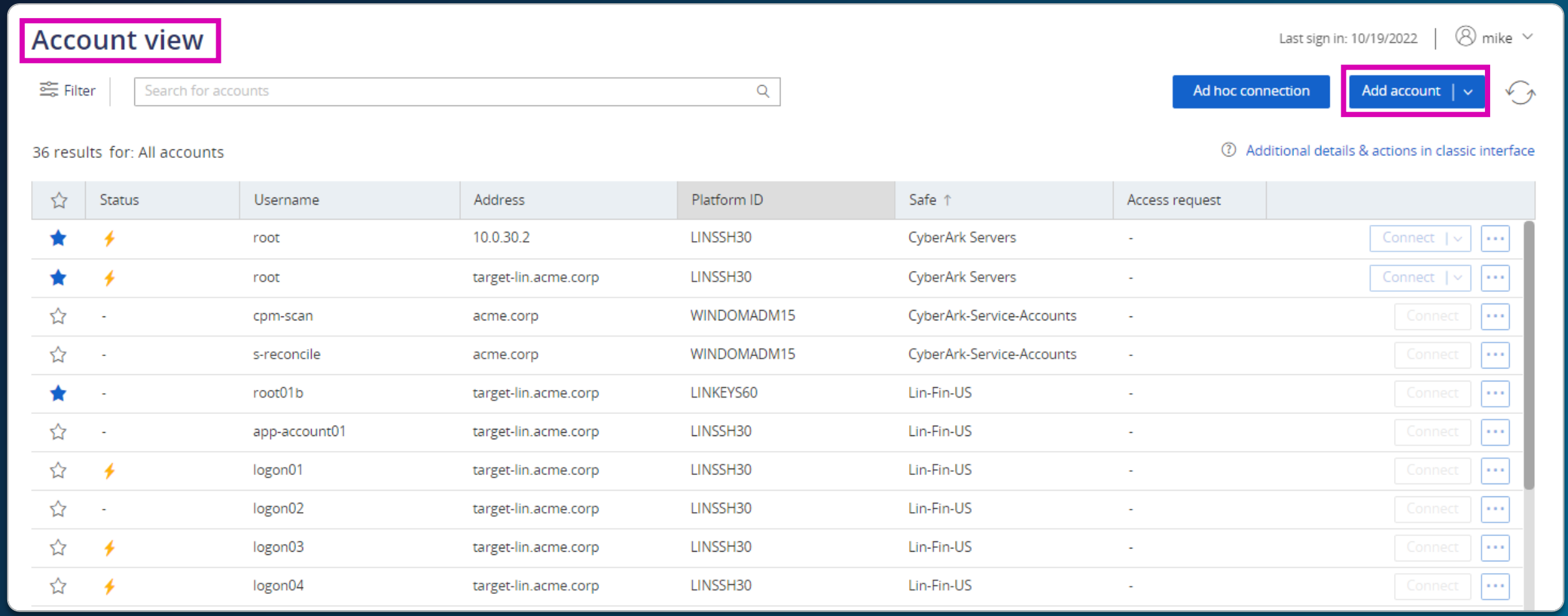
Safe: Lin-Fin-US

- Members of the “LinuxAdmins” Team group will have “Use and list” permissions

Account:

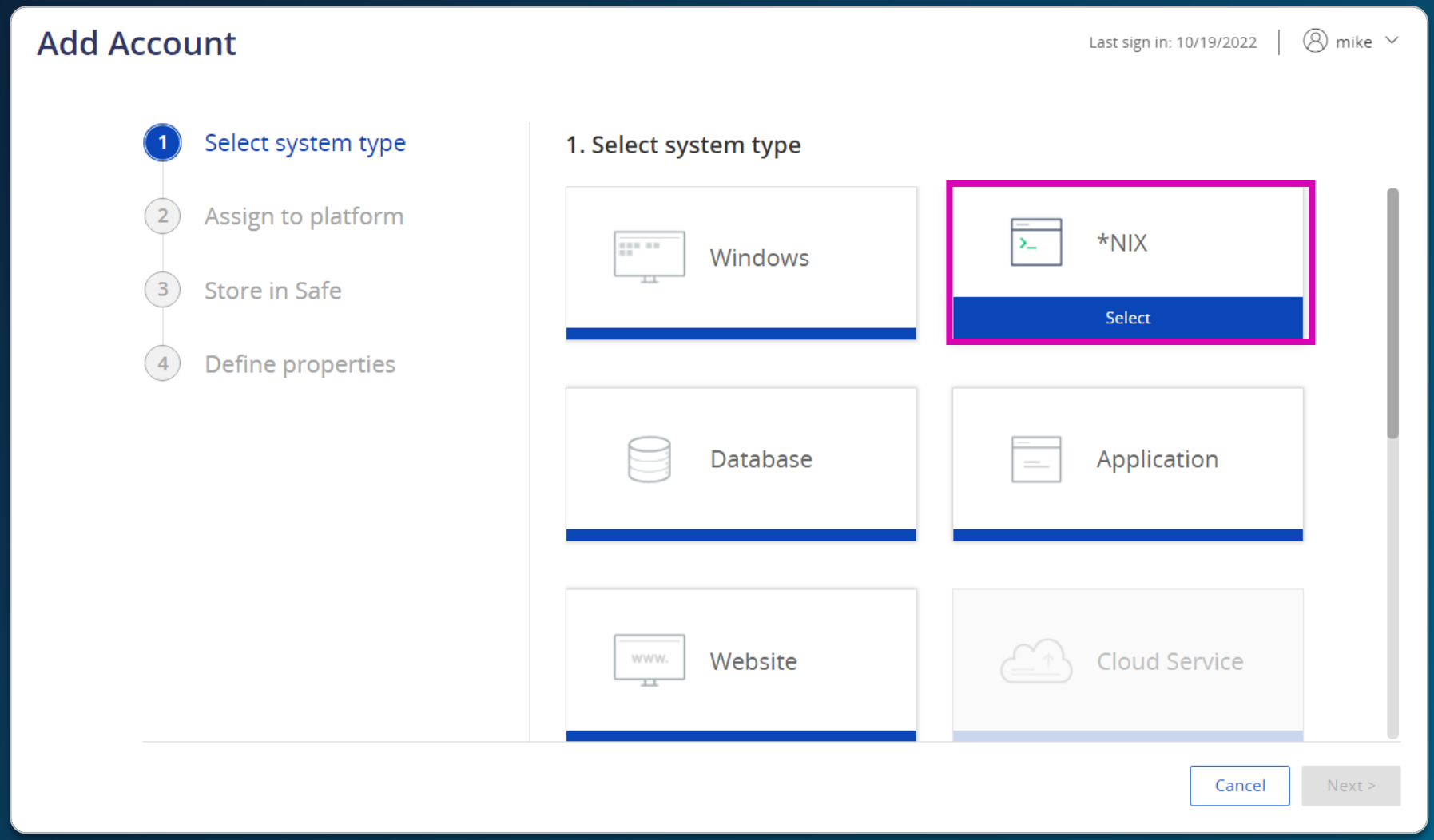
- Username: logon01
- Password: ******
- Address: target-lin.acme.corp

Accounts View – Add a Linux Account



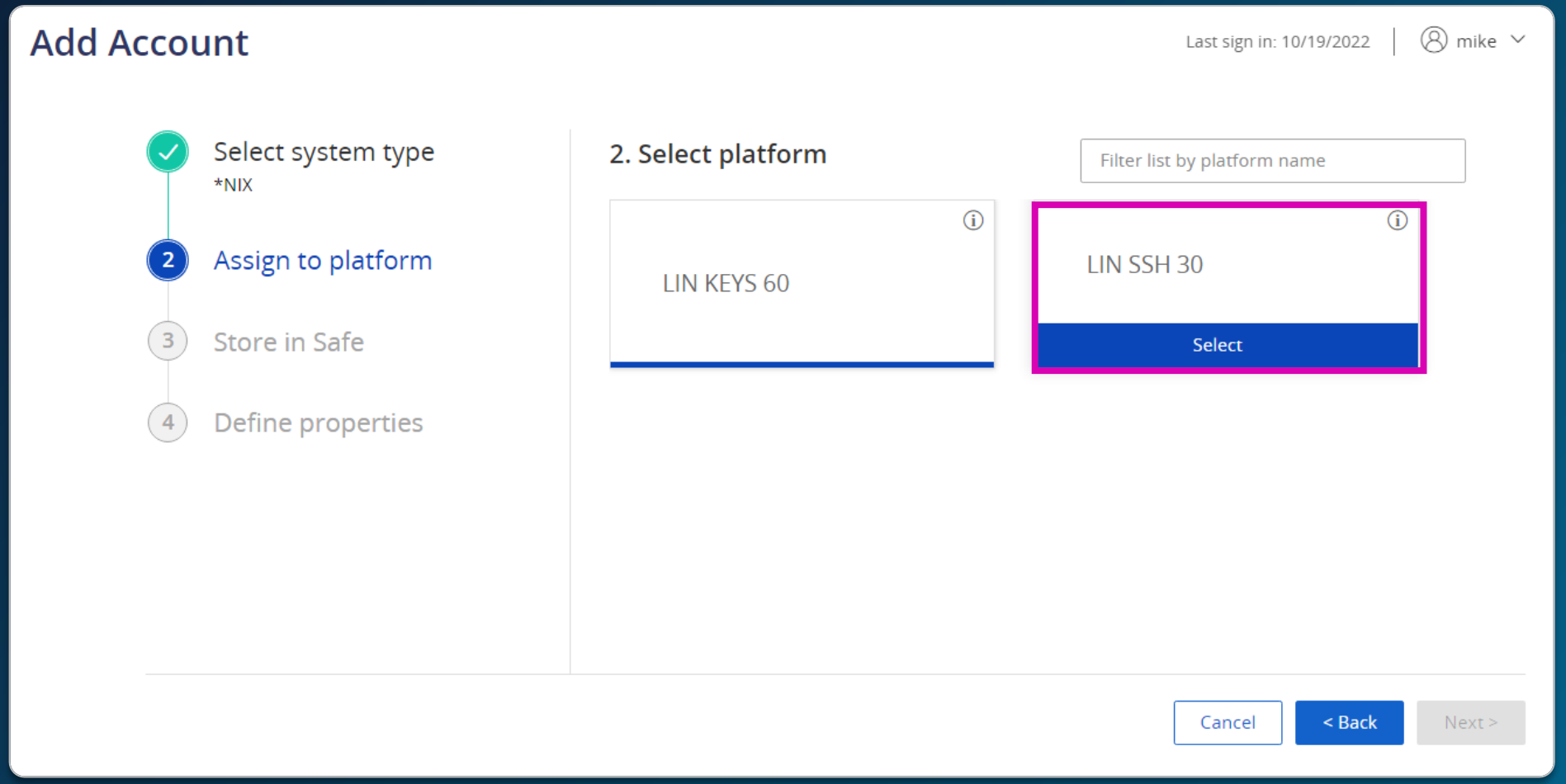
CYBERARK®

Accounts View – Add a Linux Account



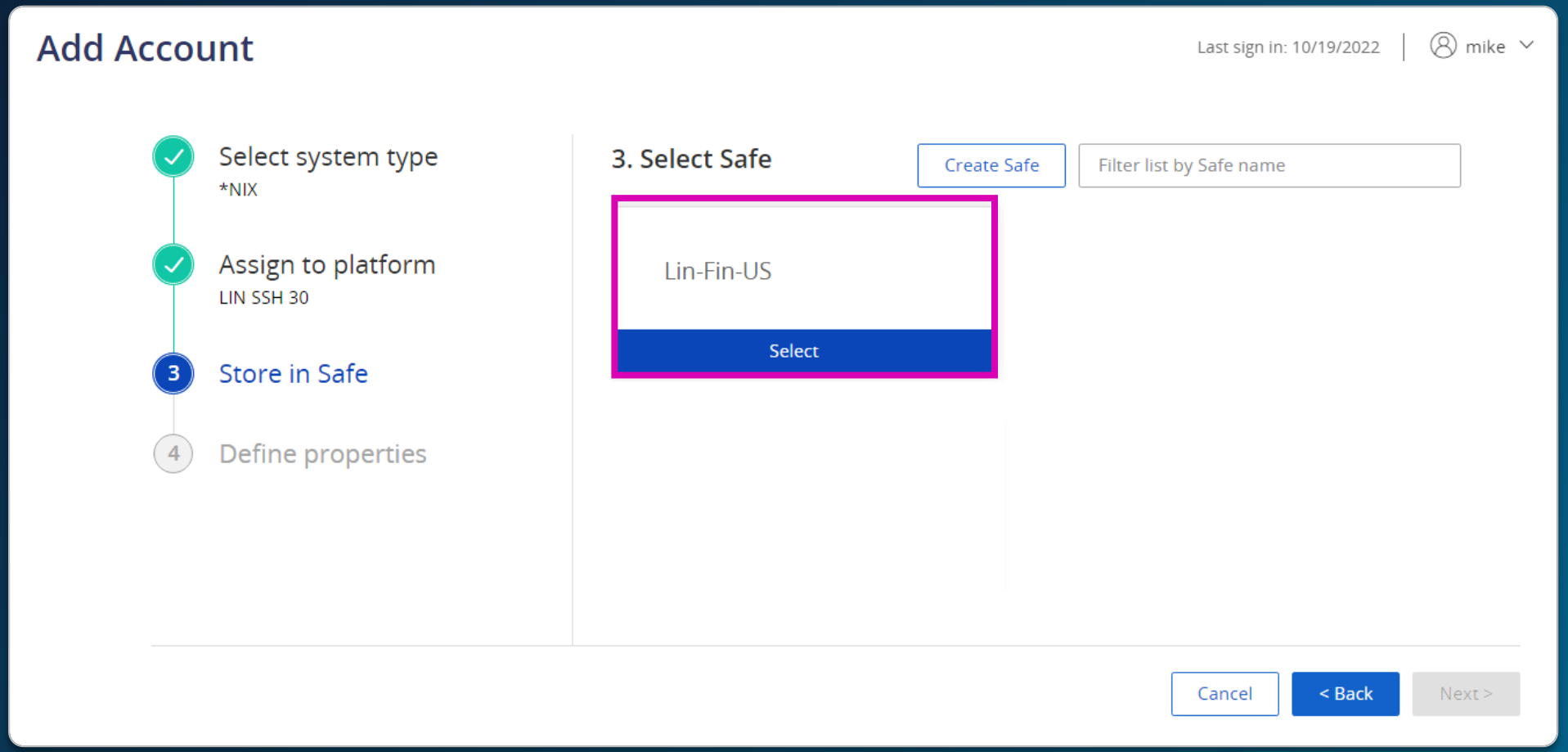
CYBERARK®

Accounts View – Add a Linux Account



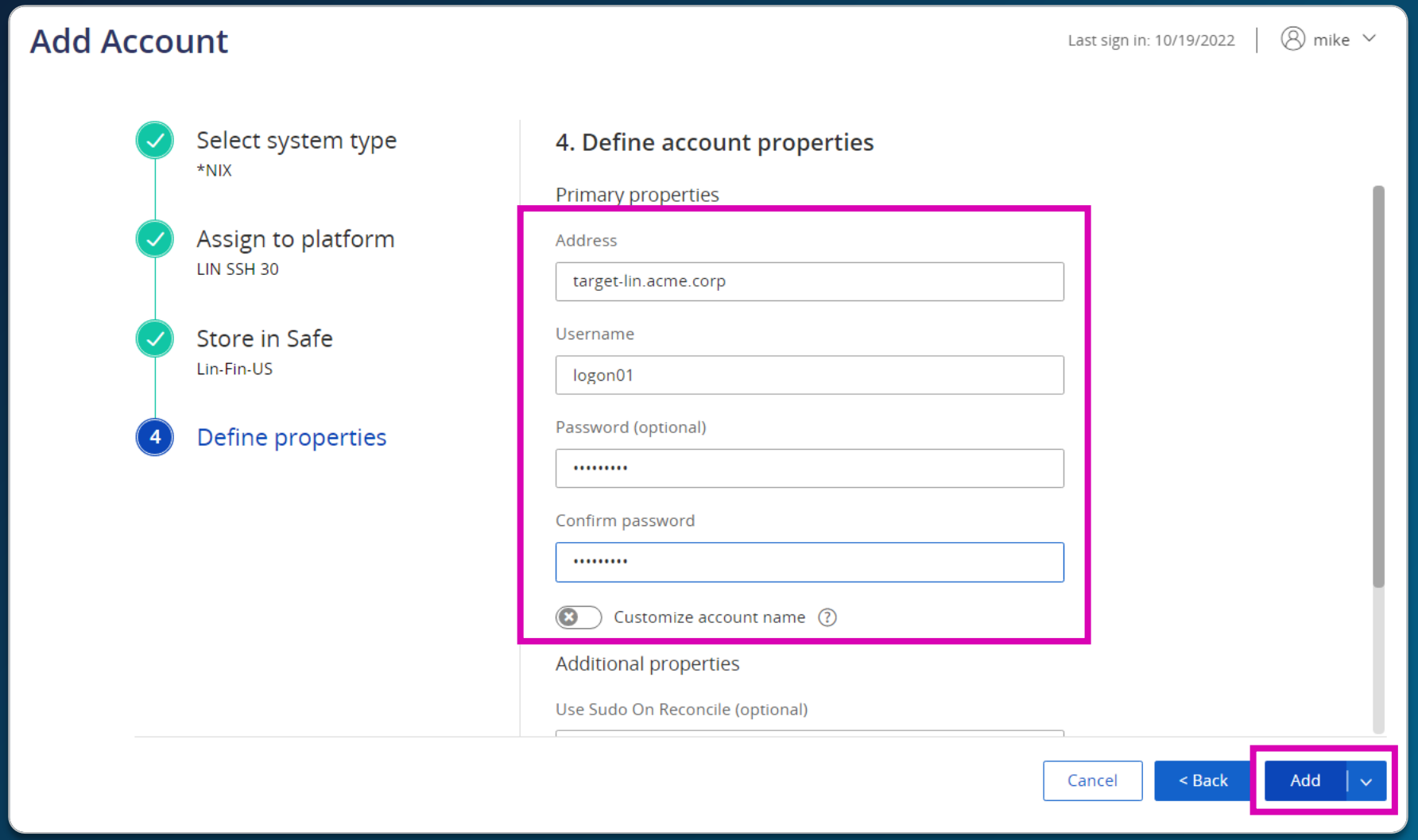
CYBERARK®

Accounts View – Add a Linux Account



CYBERARK®

Accounts View – Add a Linux Account



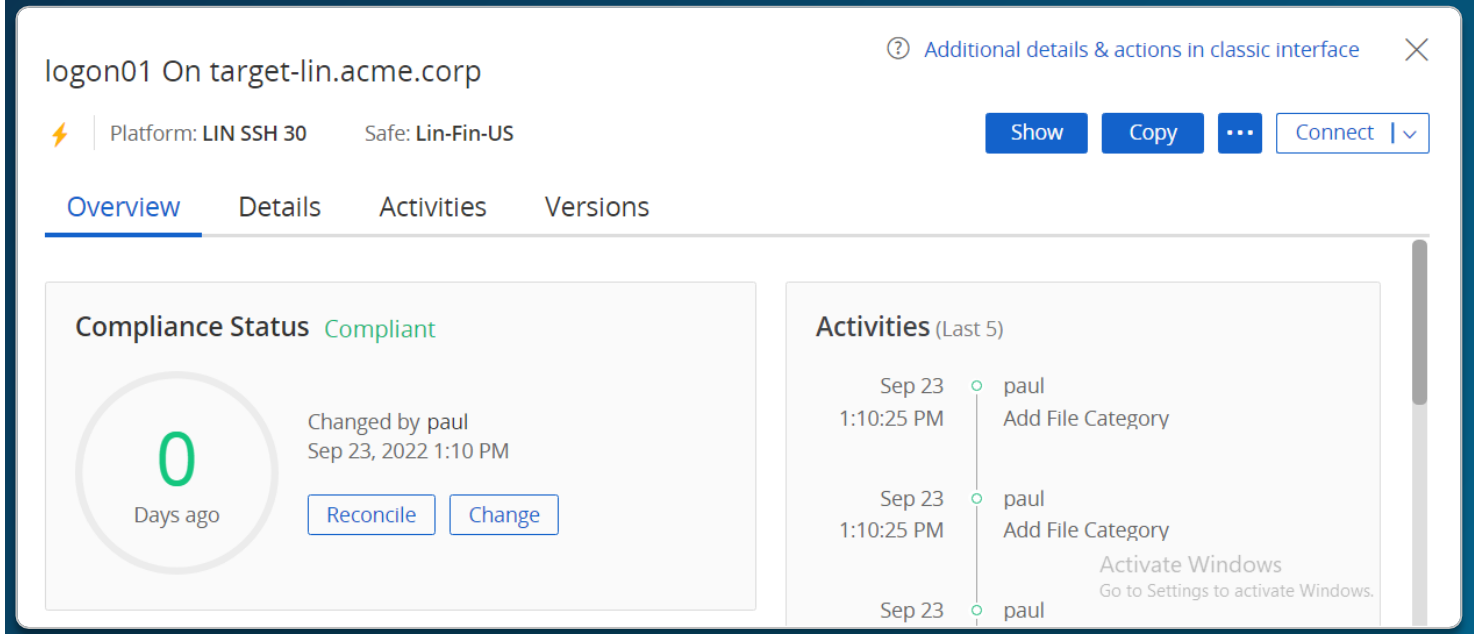
CYBERARK®

What Just Happened?

So, we have “created” an account. But what does that mean?

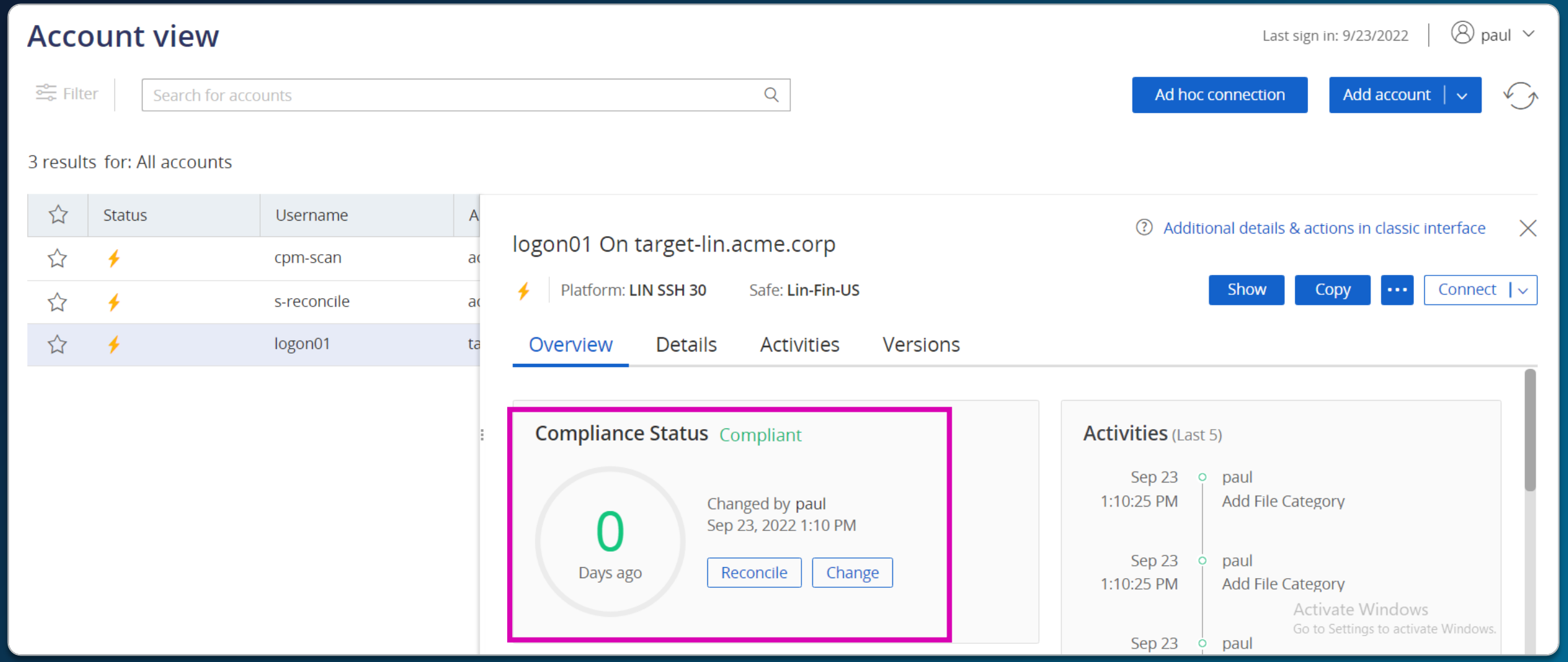
Did we create a new account called “logon01” on that target system?

No. All we have done is registered information in the **CyberArk PAM** database about an account named ***logon01***.



CYBERARK®

Accounts View – Add a Linux Account



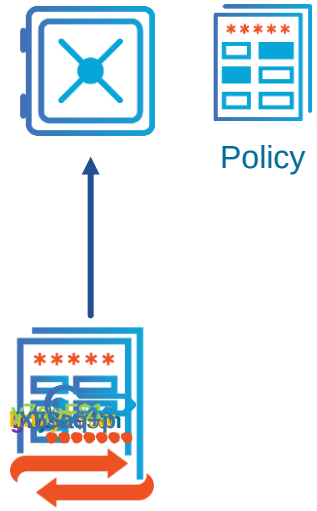
CYBERARK

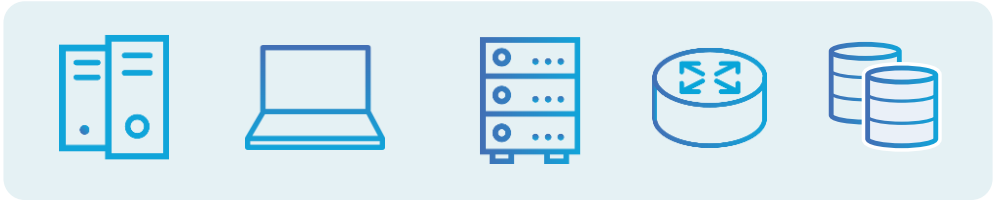
Account Management Operations

In this section we will discuss the account management operations performed by the **CPM**

Password Management is Performed By the CPM

The **CPM** manages passwords and SSH keys on devices based on the policies set by Vault Administrators





IT Environment

System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t

CYBERARK®

Password Management Overview

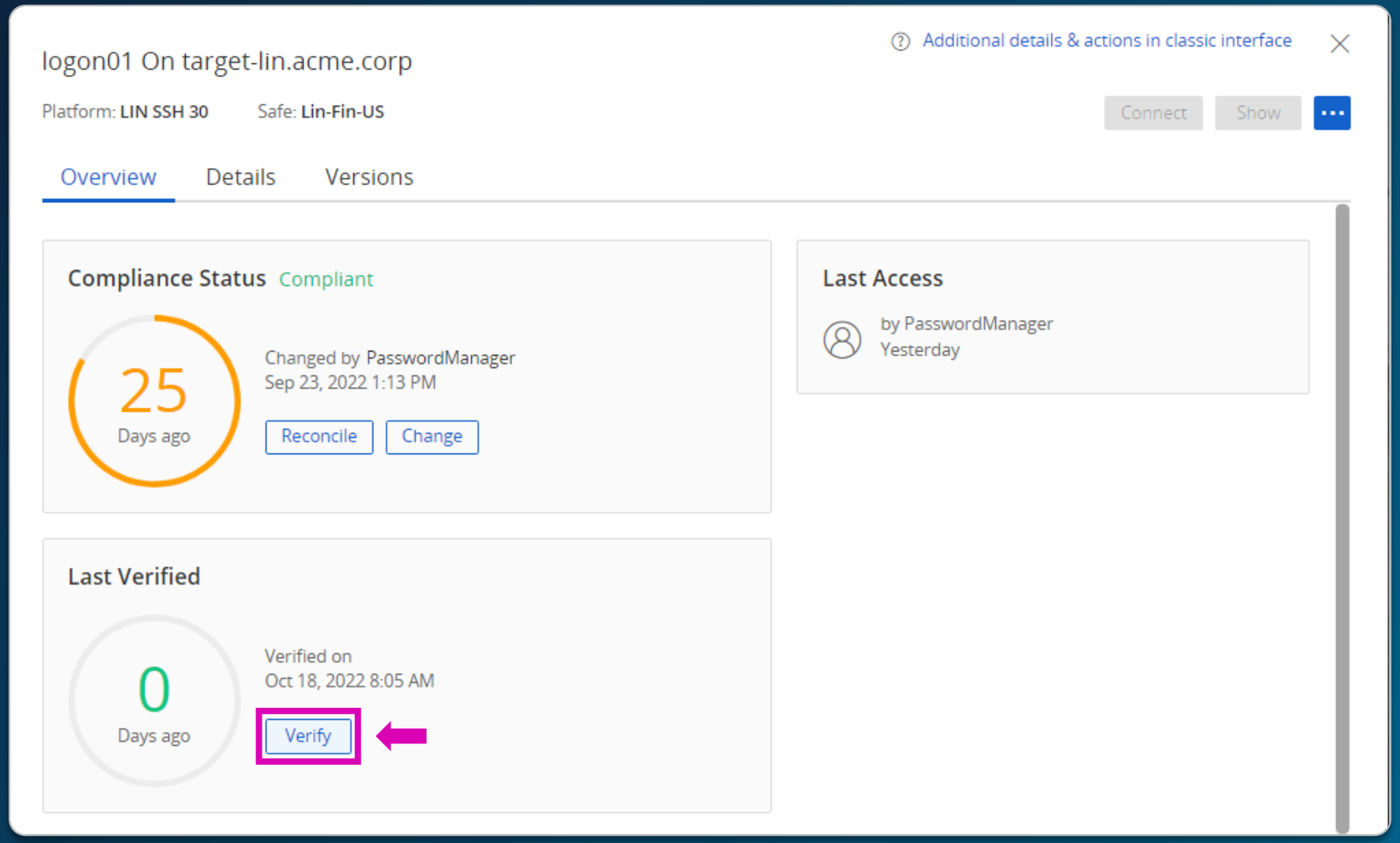
There are three actions performed by the CPM in order to manage privileged accounts:

1. **Password Verification:**
   Confirms the password stored in the Vault matches the password on the target system

2. **Password Change:**
   Changes the password automatically based upon an expiration period or by user intervention

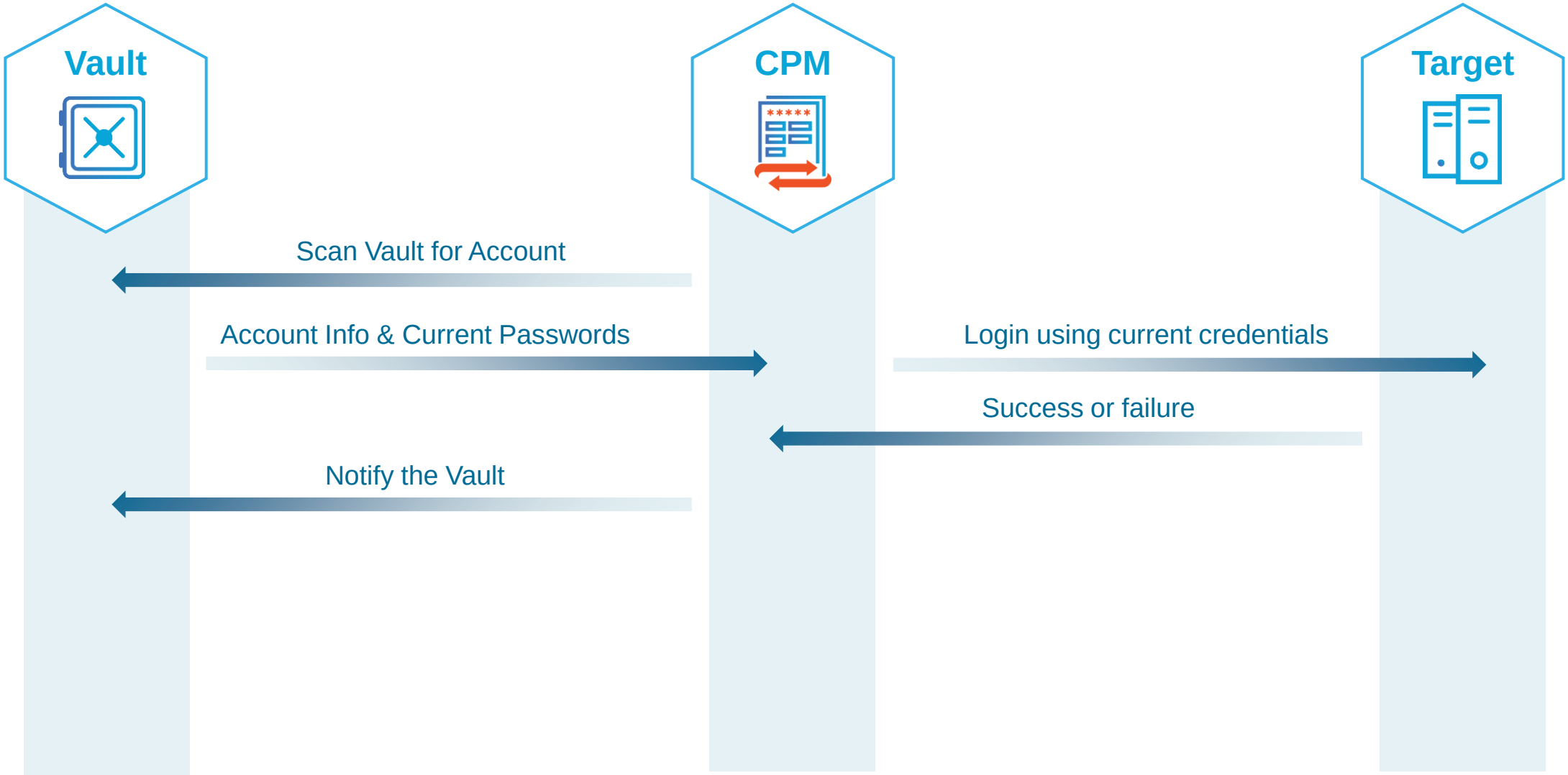
3. **Reconciliation of unknown or lost passwords:**
   Process used when the password stored in the Vault does not match the target system

Verifying the Account



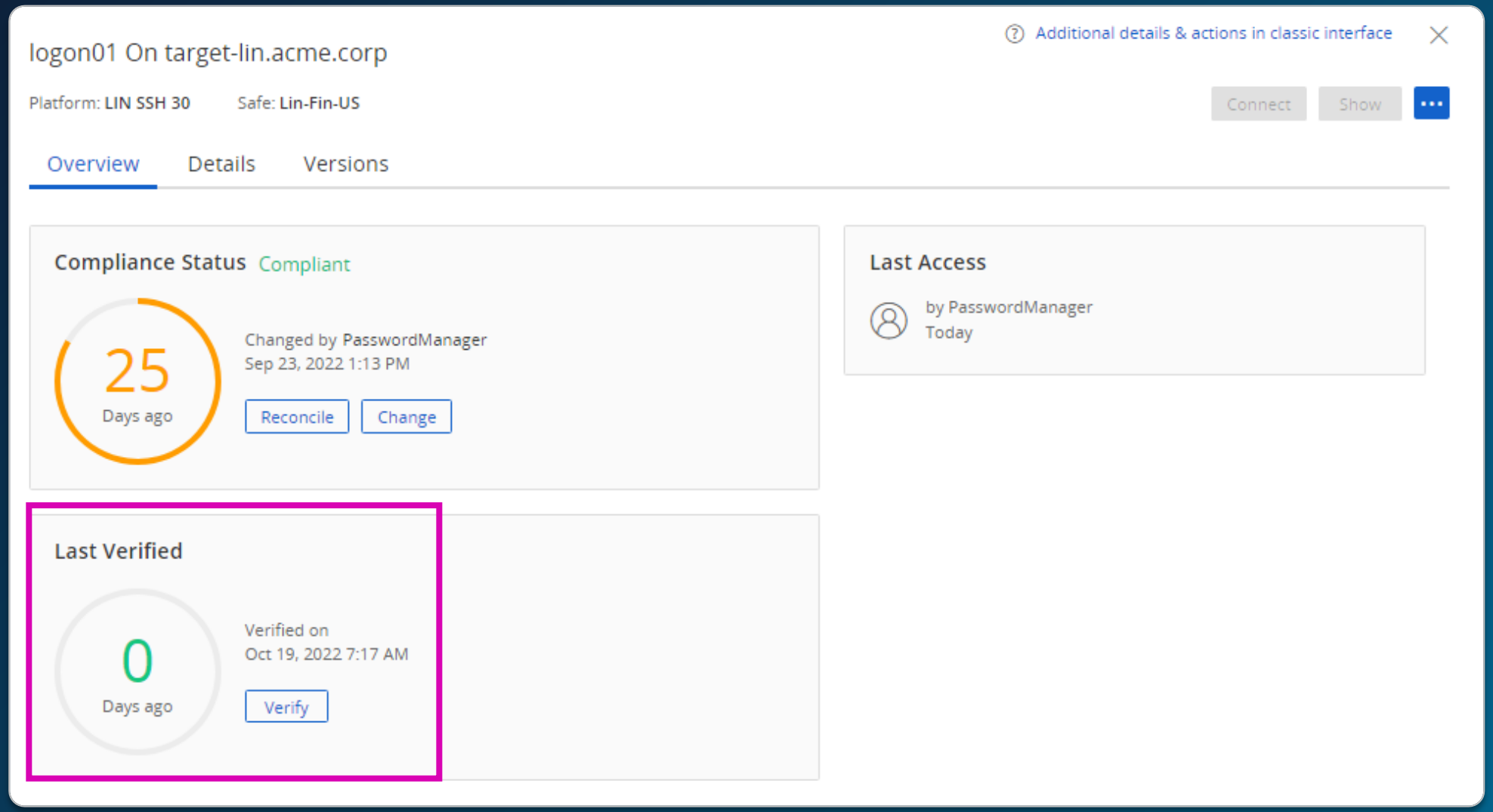
CYBERARK

Verify Process



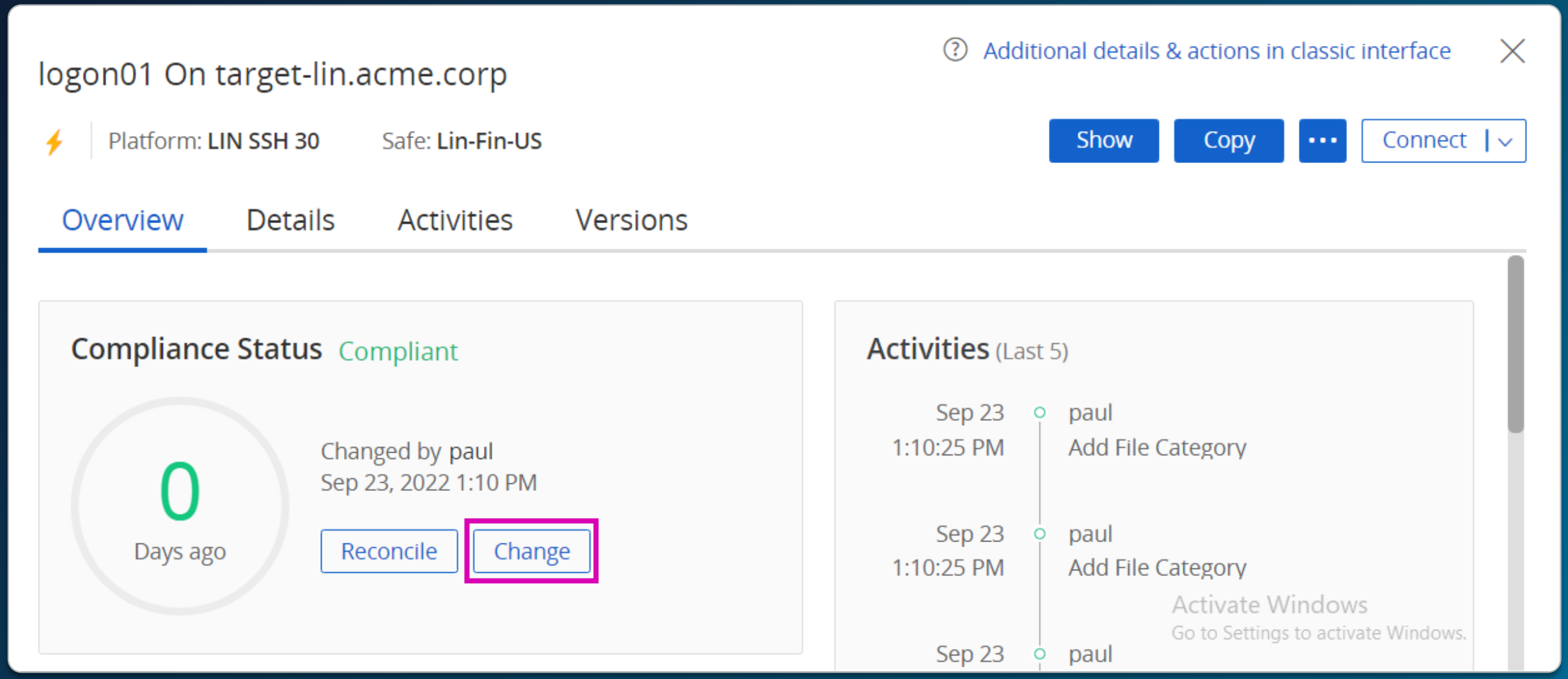
CYBERARK®

Completed Verification



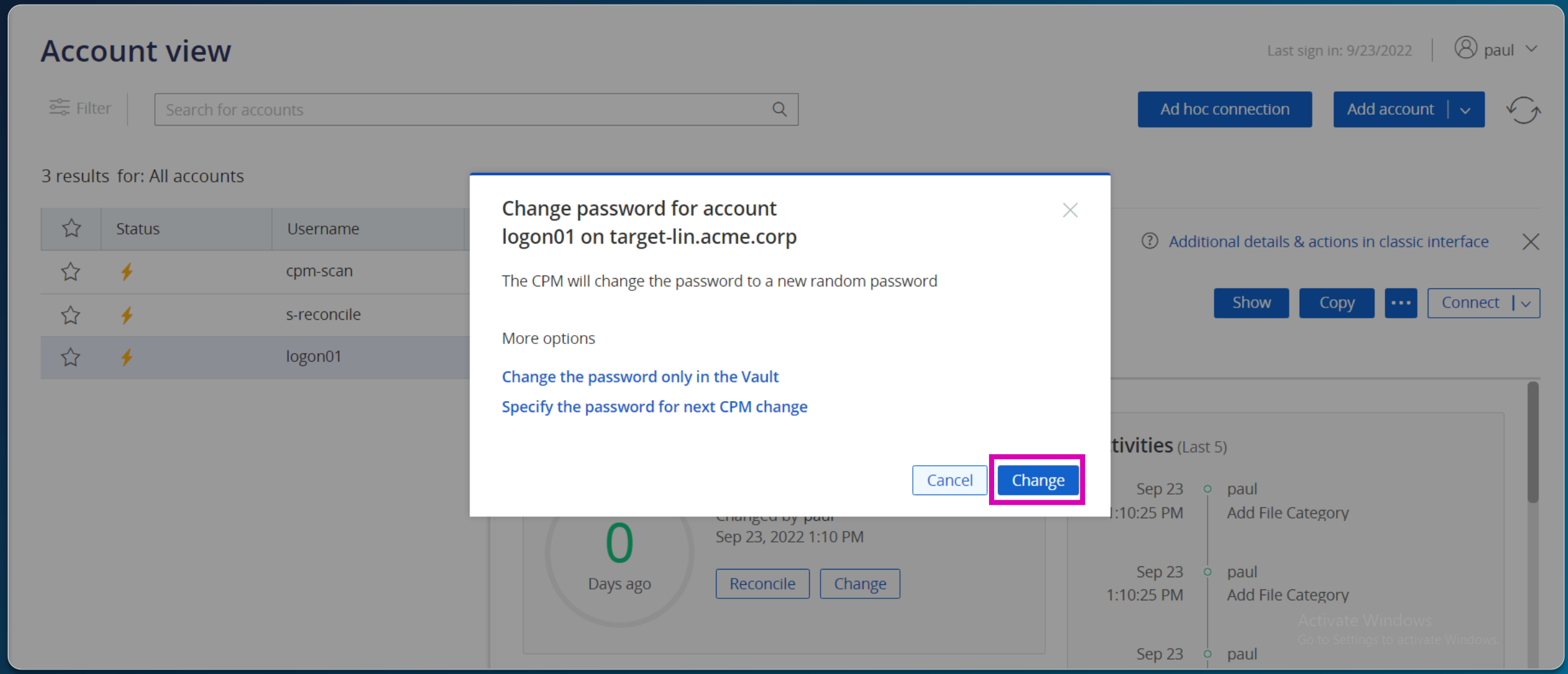
CYBERARK®

Password Change



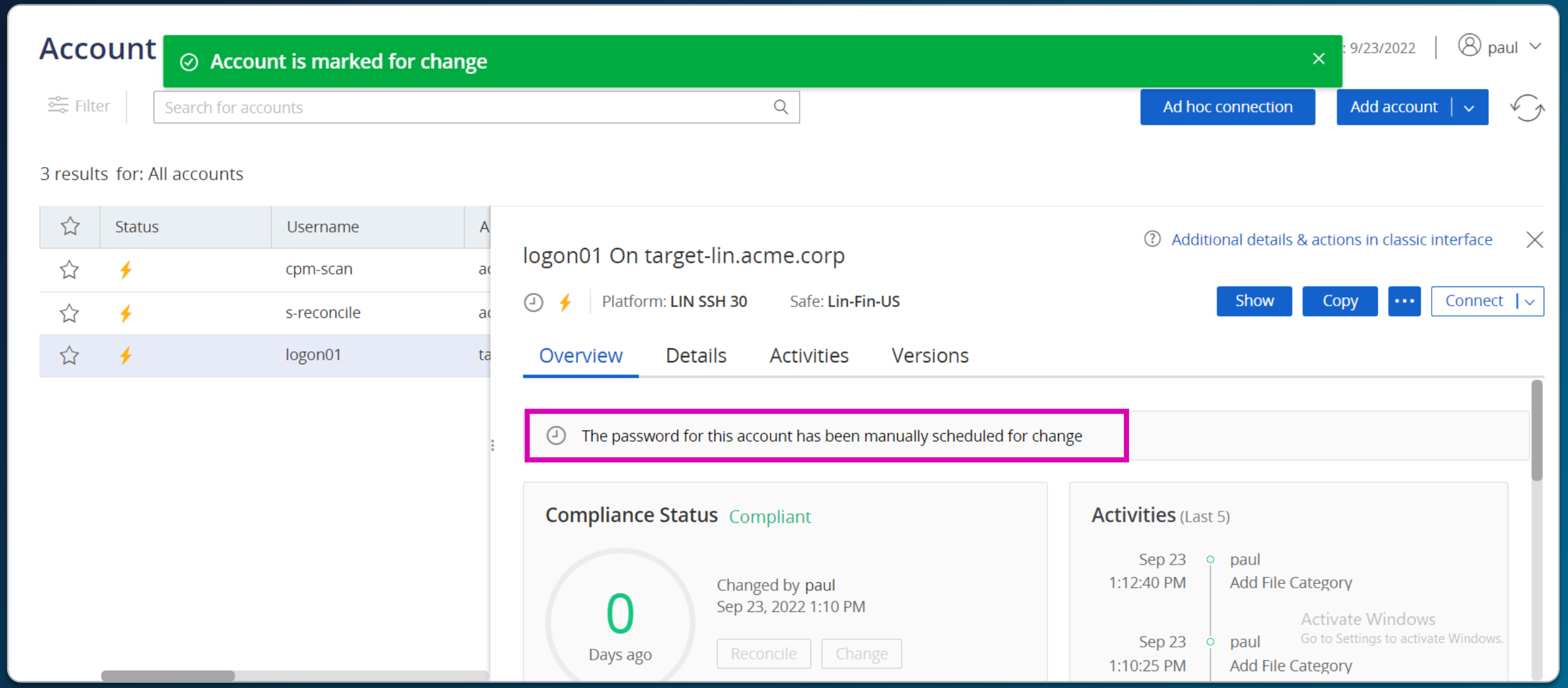
CYBERARK®

Confirm Change



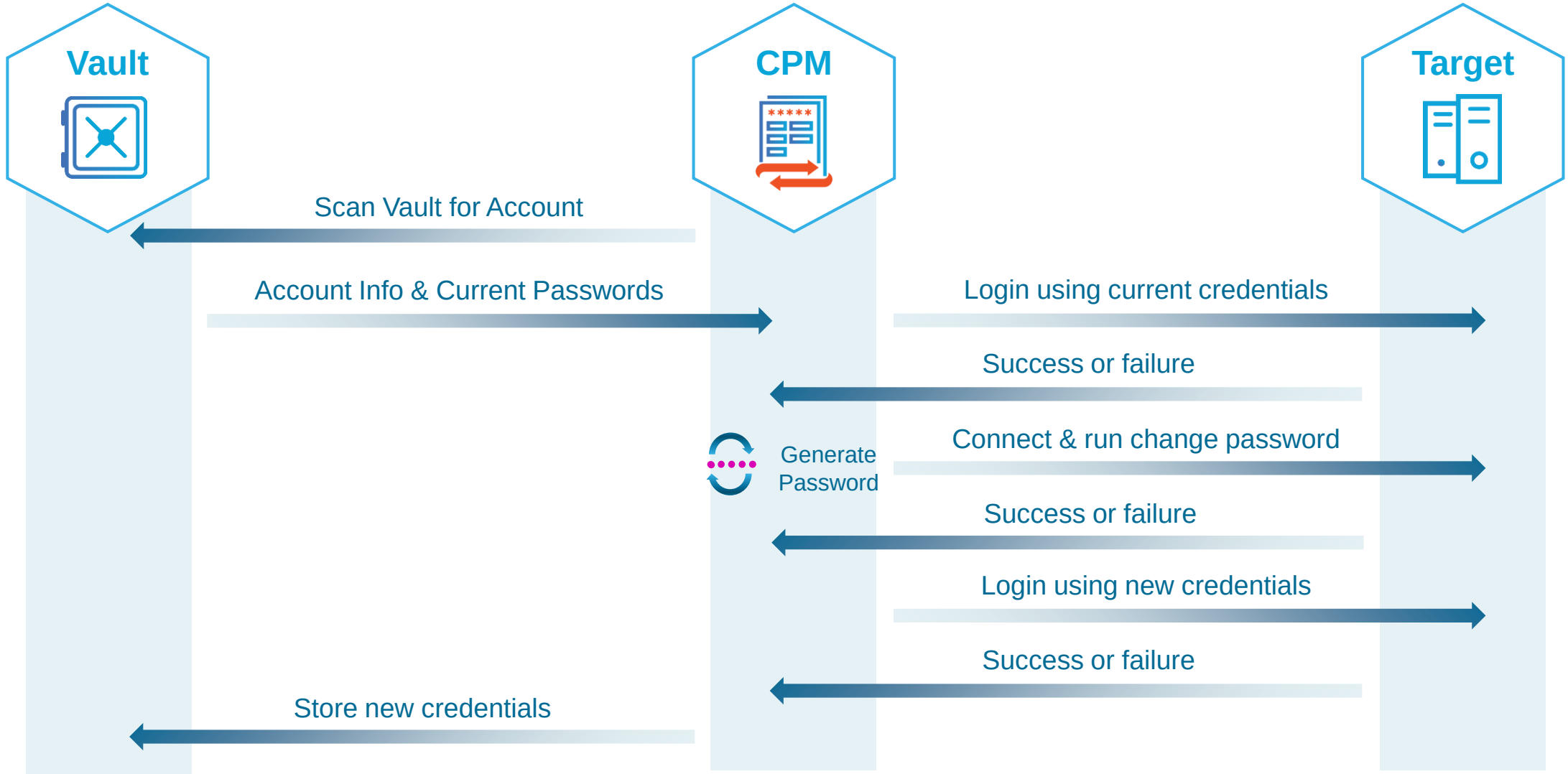
CYBERARK

Pending Change



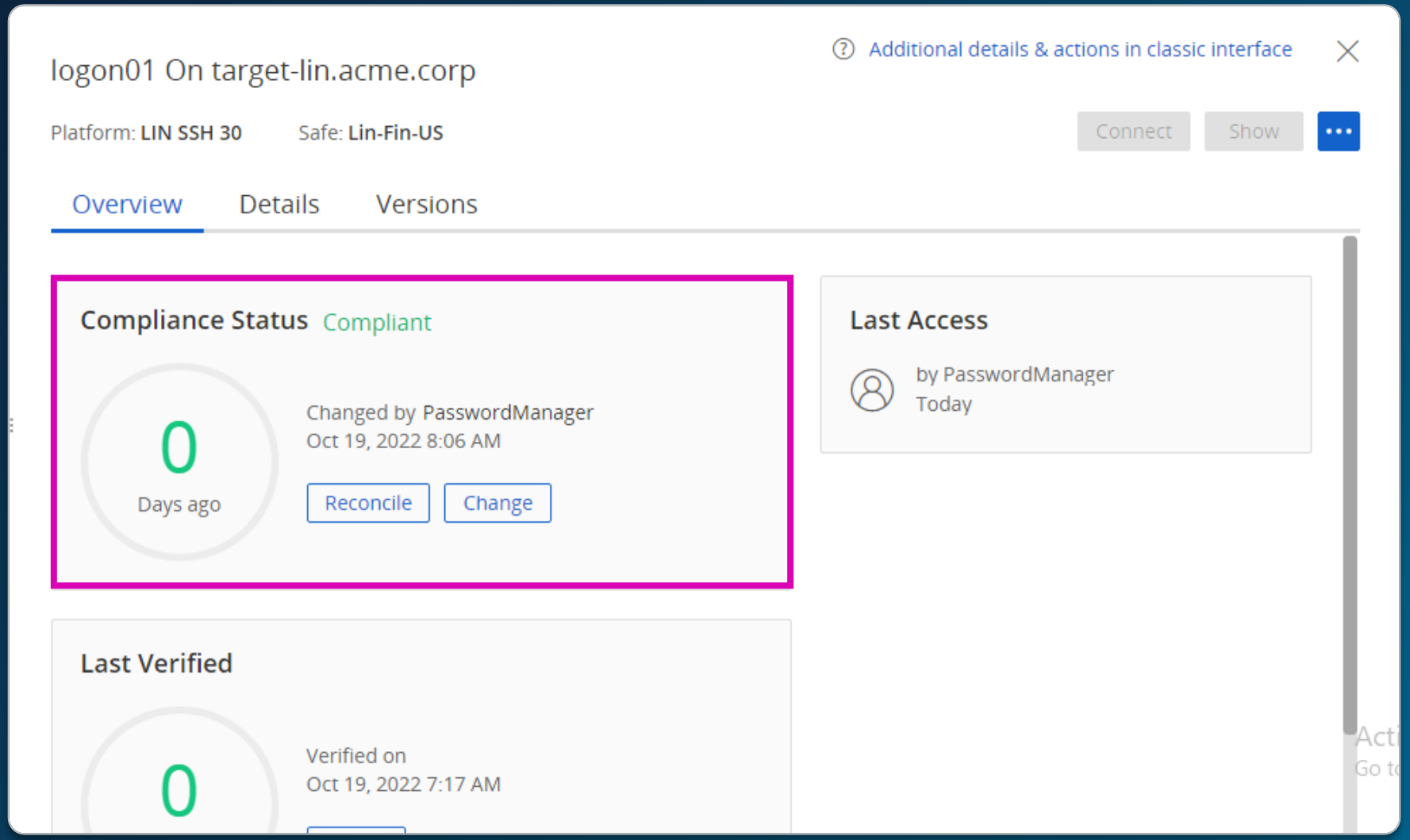
CYBERARK

Change Process



CYBERARK®

Completed Change



CYBERARK®

Summary

Summary

In this session we discussed:

- What accounts are
- How to add an account to CyberArk PAM via the PVWA
- The different password management operations

CYBERARK®

Additional Resources

Documentation

Rapid Risk Reduction:
A 30-Day Sprint to Protect Privileged Credentials

You may now complete the following exercises:

Securing Windows Domain Accounts

- Account Management
  - Add the reconcile account
  - Add the accounts discovery account

Securing Unix SSH Accounts

Securing Oracle Database Accounts