CYBERARK®

PAM Administration

Discovery and Onboarding

Part 1

Agenda

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

- Describe the main methods for discovering and onboarding accounts to the system
- Discover and onboard accounts using **Accounts Discovery**
- Configure and test **Automatic Onboarding Rules**

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Discover

Continually scan the environment to detect privileged credentials and accounts

Onboard

Add all discovered privileged accounts to the pending list to validate privilege

Manage

Automatically add privileged accounts to be managed and rotated in the digital vault

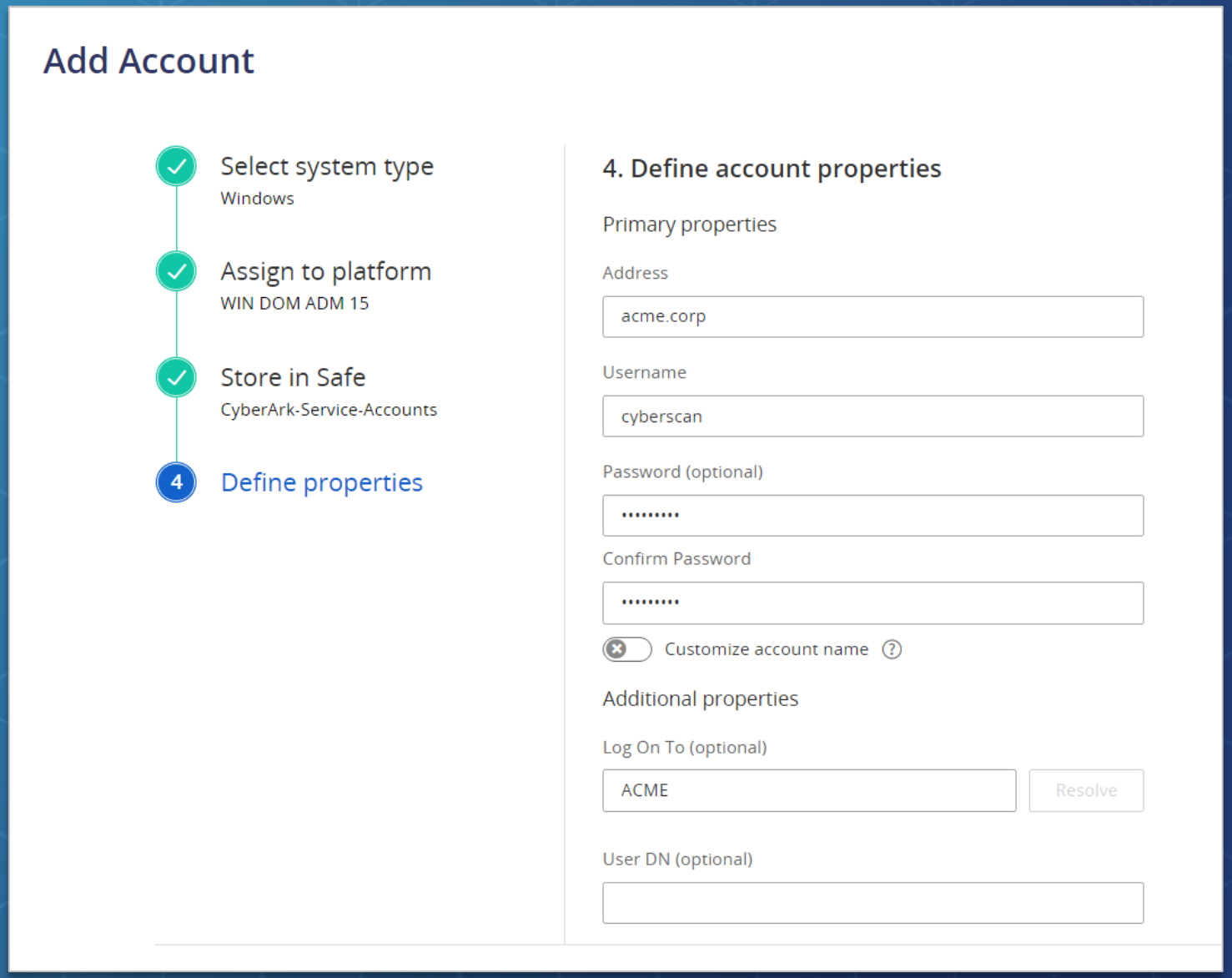
Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- Accounts Discovery
- Continuous Accounts Discovery
- Discovery and Audit (DNA)
- Rest API

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Add a Single Account

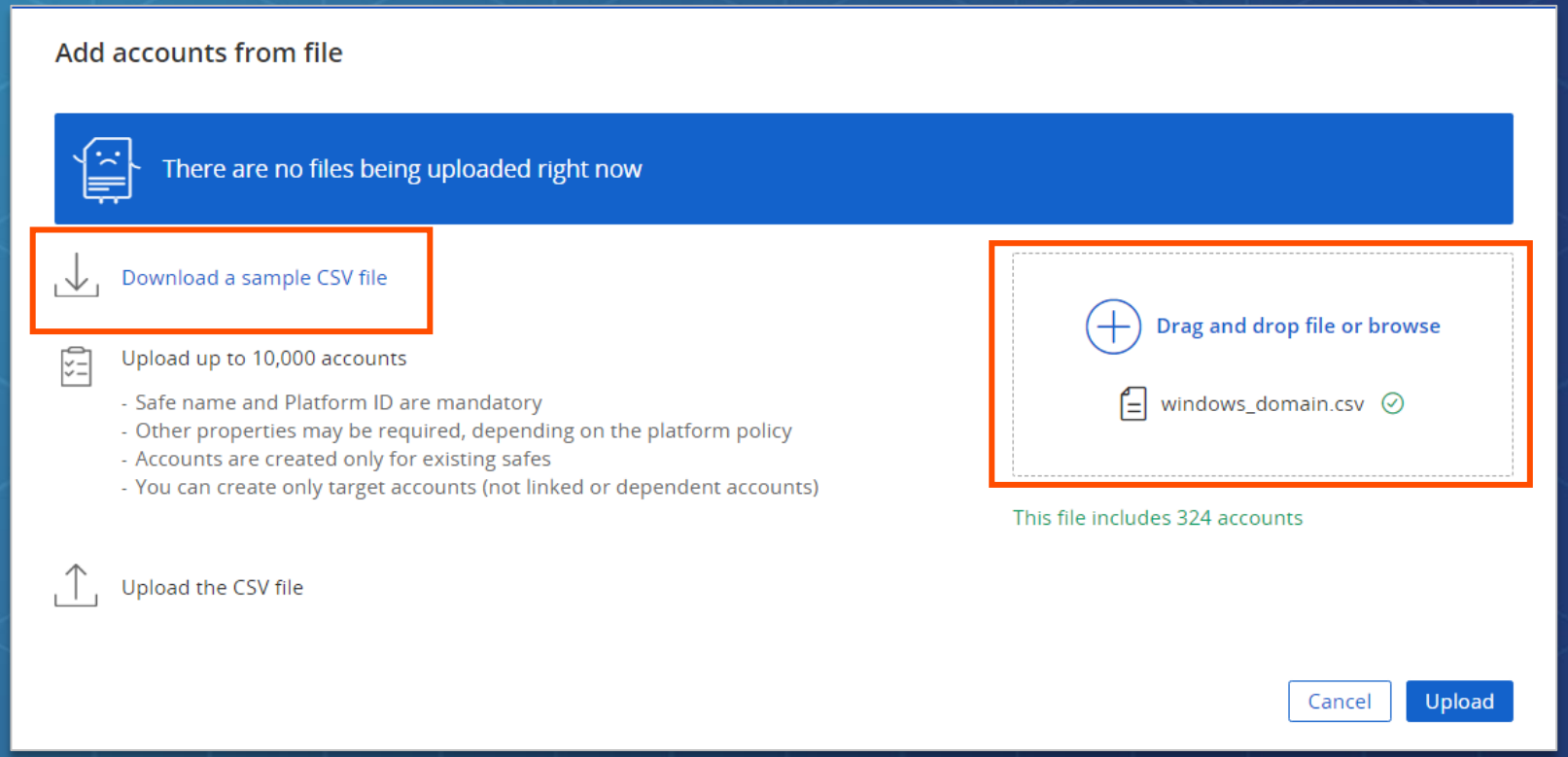
- Add a single account



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Add Multiple Accounts From File

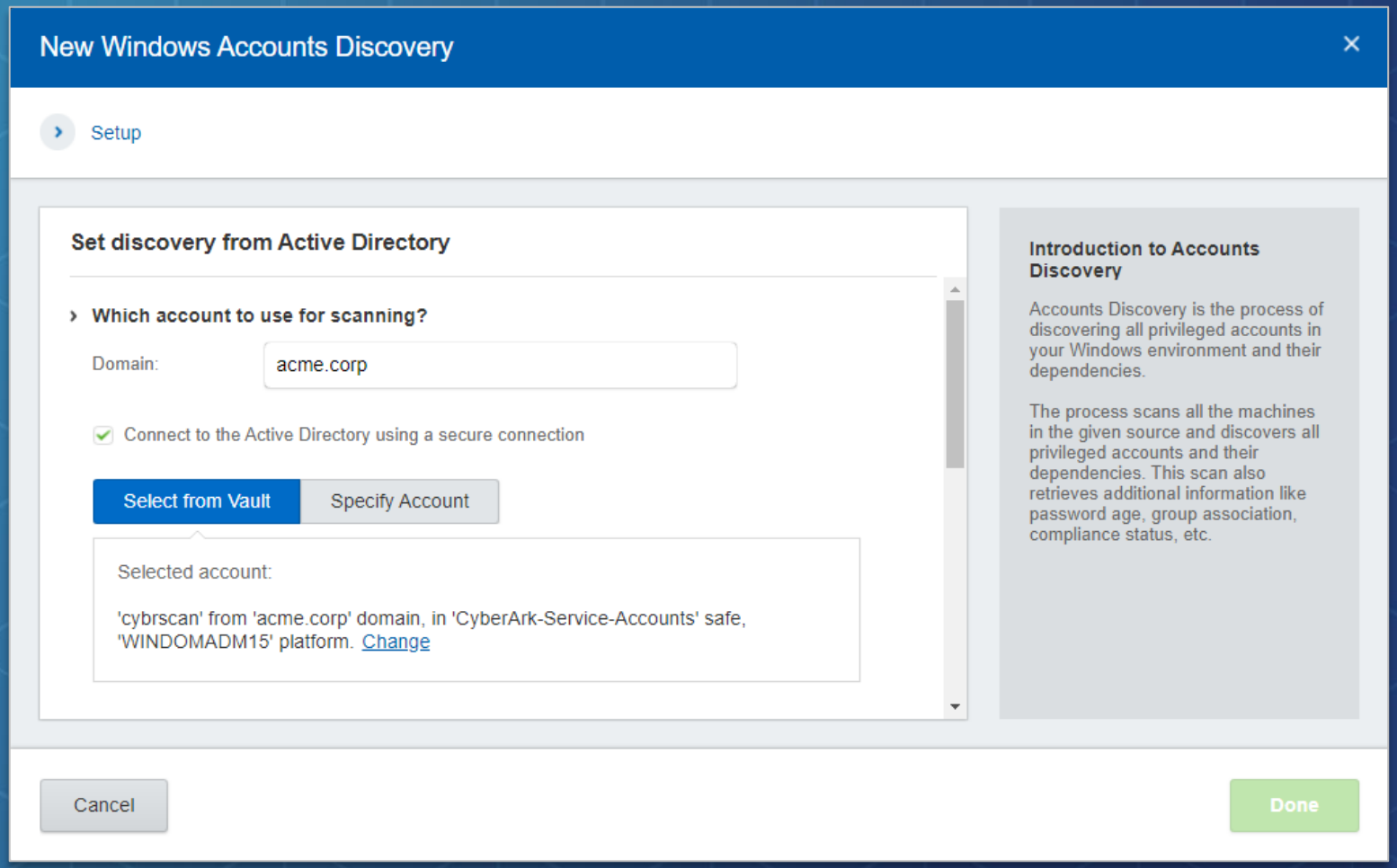
- Add a single account
- Add multiple accounts from file



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Accounts Discovery

- Add a single account
- Add multiple accounts from file
- Accounts Discovery

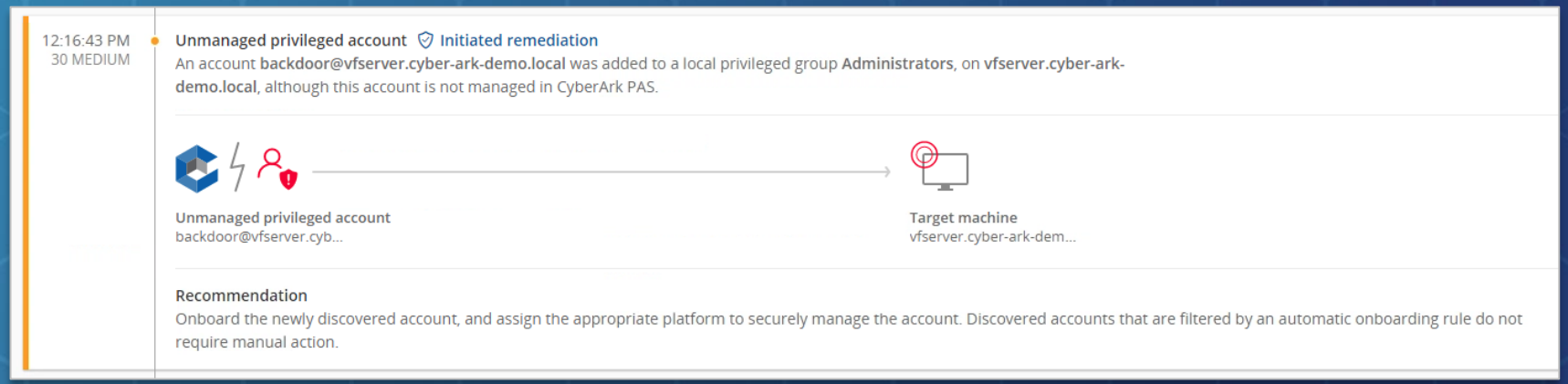


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Continuous Accounts Discovery (PTA)

- Add a single account
- Add multiple accounts from file
- Accounts Discovery
- Continuous Accounts Discovery

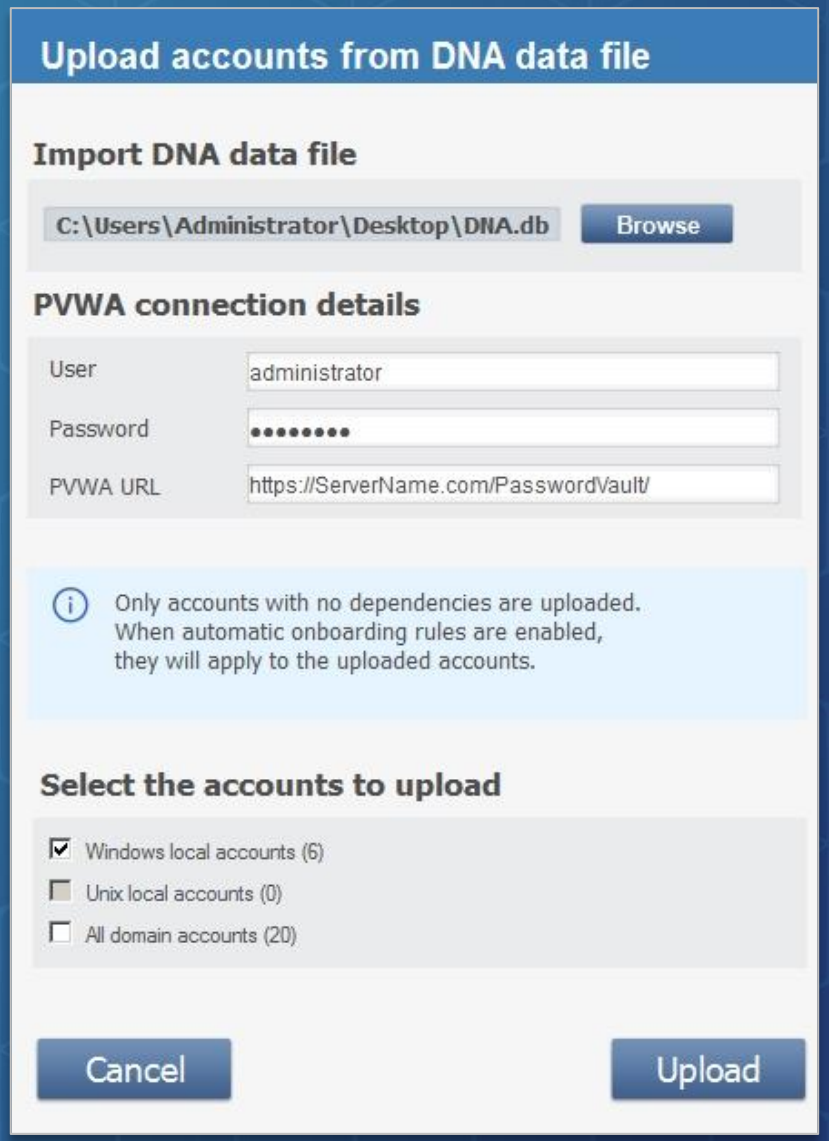
Detections by PTA



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Discover and Audit (DNA)

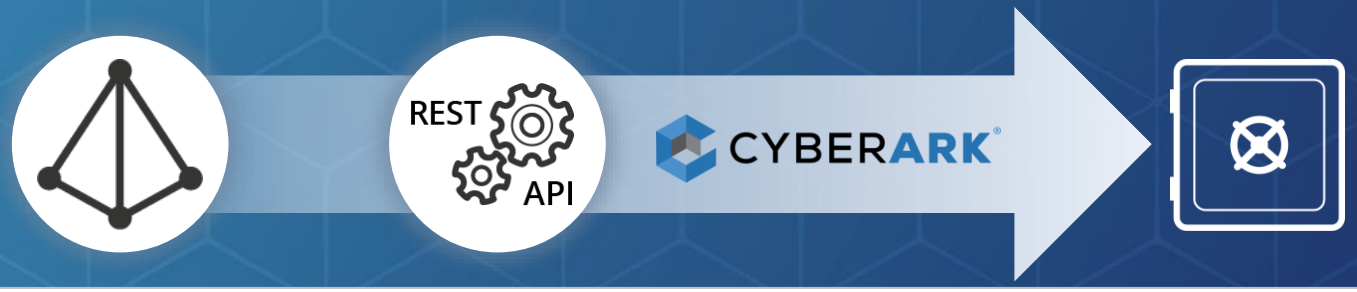
- Add a single account
- Add multiple accounts from file
- Accounts Discovery
- Continuous Accounts Discovery
- DNA



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Rest API

- Add a single account
- Add multiple accounts from file
- Accounts Discovery
- Continuous Accounts Discovery
- DNA
- Rest API



REST APIs

Use REST APIs to create, list, modify and delete entities in the PAS solution from within programs and scripts.

You can automate tasks that are usually performed manually using the UI, and to incorporate them into system and account-provisioning scripts.

REST APIs are part of the PVWA installation, and can be used immediately without any additional configuration. Make sure your CyberArk license enables you to use the CyberArk PAS SDK. For more information, contact your CyberArk support representative.

Note:

As a general rule, we recommend that you always use the newest REST API version. The newer versions include better performance, support versioning, and have more capabilities. If you cannot find a corresponding REST API for the task that you want to perform, you can use the command line interface (PACLI). For details, see Command Line Interface (PACLI) .

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

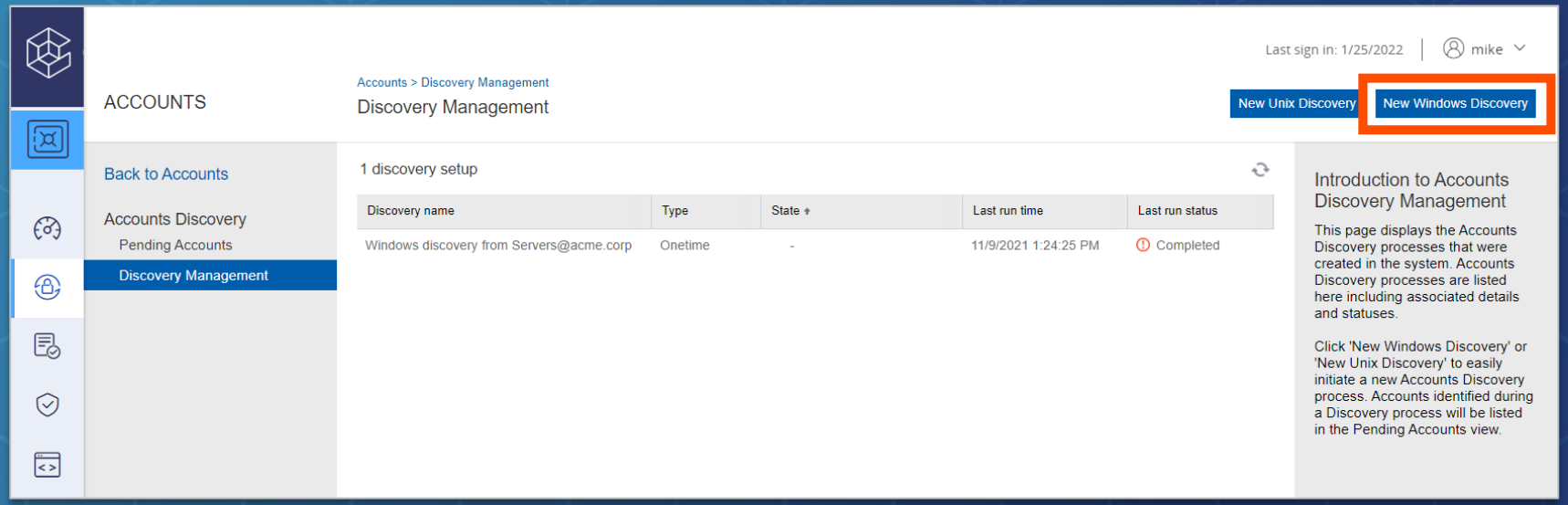
Accounts Discovery

Overview

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

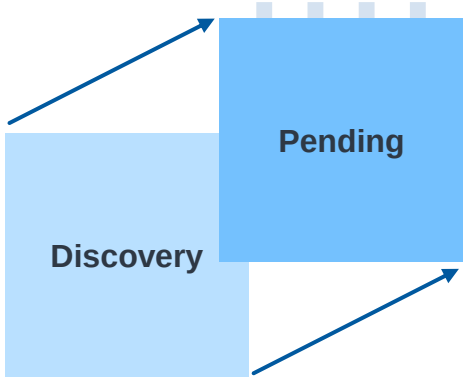
Accounts Discovery and Onboarding Steps

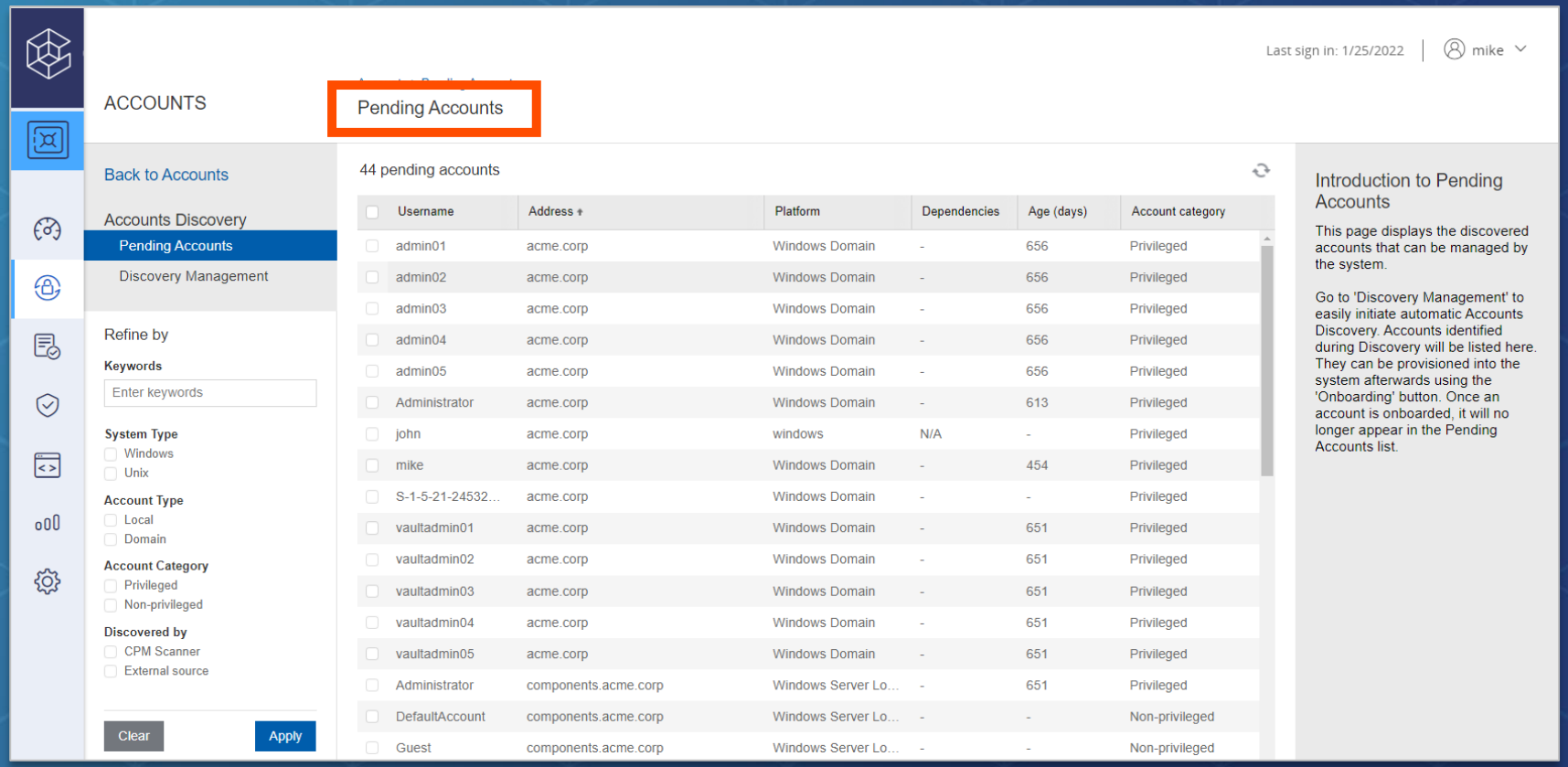
Discovery



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Accounts Discovery and Onboarding Steps

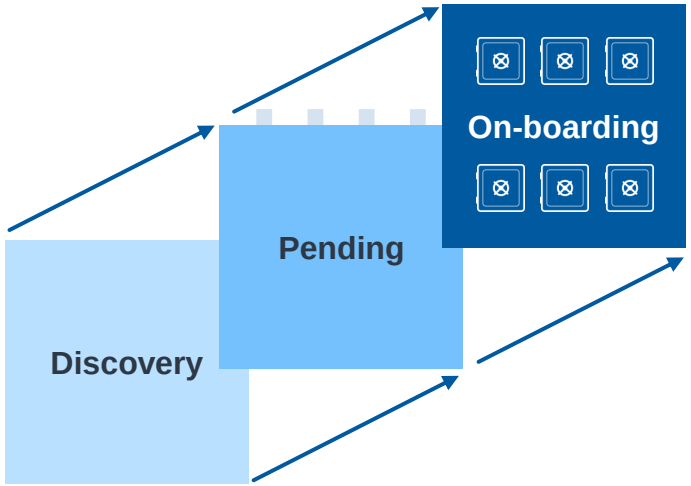


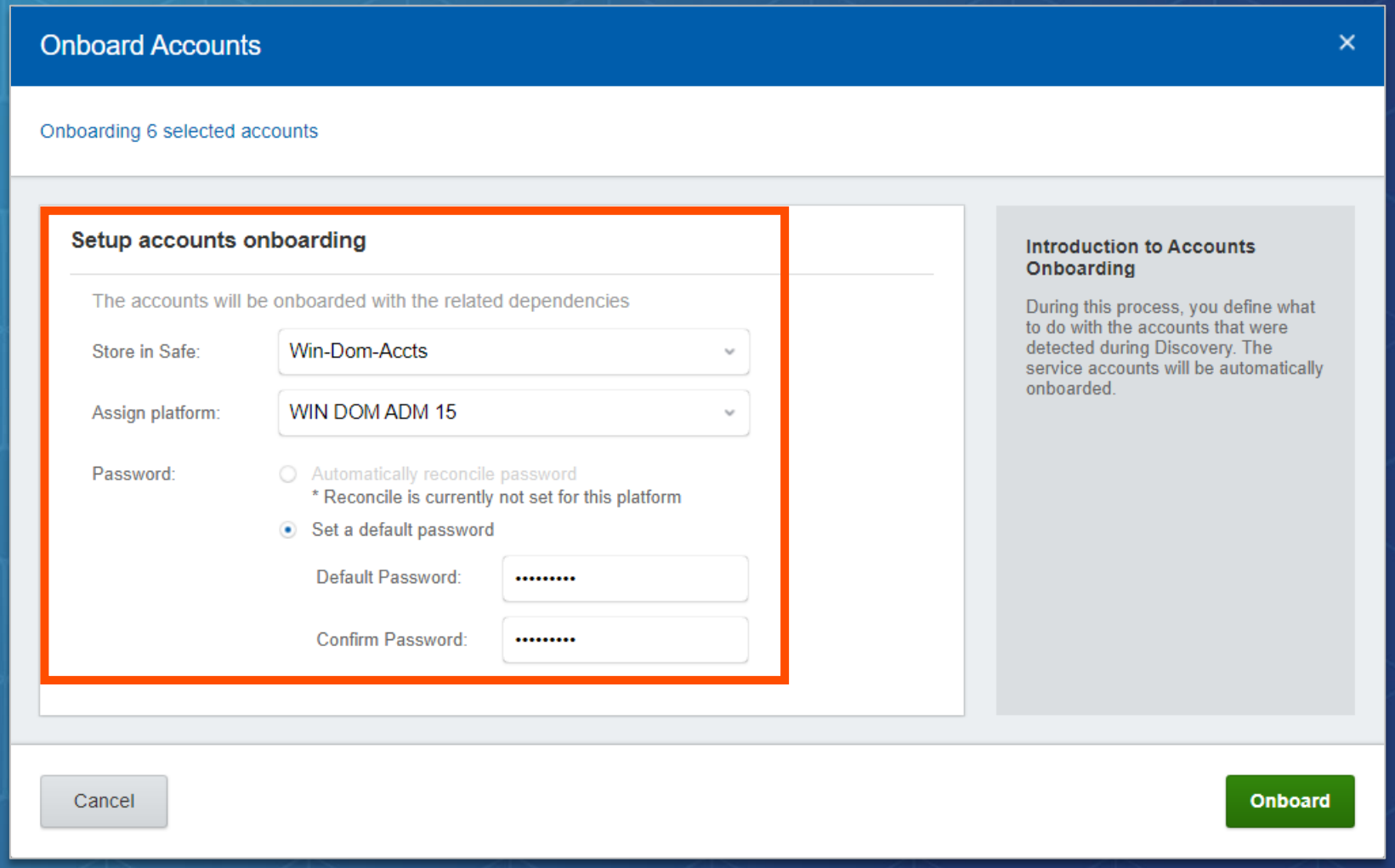


Username	Address	Platform	Dependencies	Age (days)	Account category
admin01	acme.corp	Windows Domain	-	656	Privileged
admin02	acme.corp	Windows Domain	-	656	Privileged
admin03	acme.corp	Windows Domain	-	656	Privileged
admin04	acme.corp	Windows Domain	-	656	Privileged
admin05	acme.corp	Windows Domain	-	656	Privileged
Administrator	acme.corp	Windows Domain	-	613	Privileged
john	acme.corp	windows	N/A	-	Privileged
mike	acme.corp	Windows Domain	-	454	Privileged
S-1-5-21-24532...	acme.corp	Windows Domain	-	-	Privileged
vaultadmin01	acme.corp	Windows Domain	-	651	Privileged
vaultadmin02	acme.corp	Windows Domain	-	651	Privileged
vaultadmin03	acme.corp	Windows Domain	-	651	Privileged
vaultadmin04	acme.corp	Windows Domain	-	651	Privileged
vaultadmin05	acme.corp	Windows Domain	-	651	Privileged
Administrator	components.acme.corp	Windows Server Lo...	-	651	Privileged
DefaultAccount	components.acme.corp	Windows Server Lo...	-	-	Non-privileged
Guest	components.acme.corp	Windows Server Lo...	-	-	Non-privileged

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Accounts Discovery and Onboarding Steps

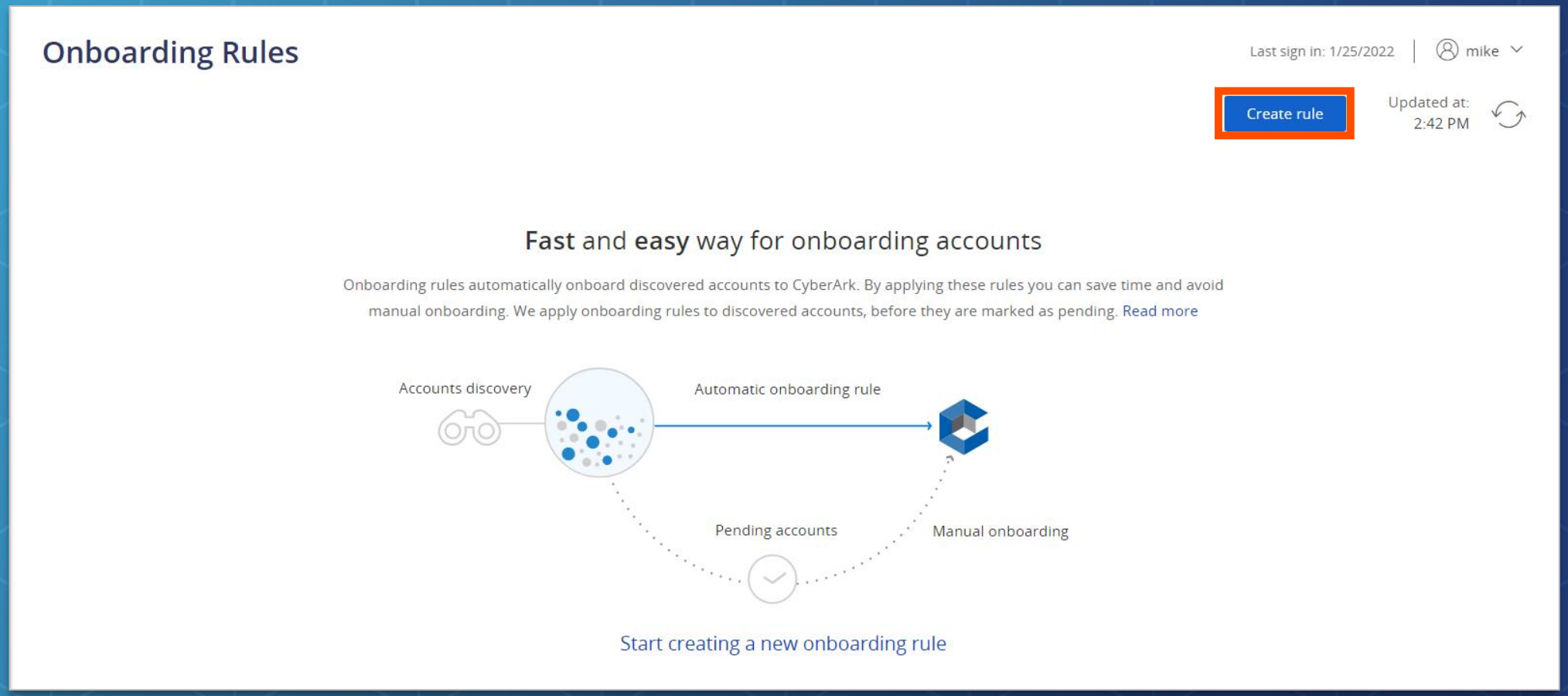




Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Automatic Onboarding Rules

Minimize the time it takes to onboard and securely manage accounts, reduces the time spent on reviewing pending accounts, and prevents human errors that may occur during manual onboarding



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

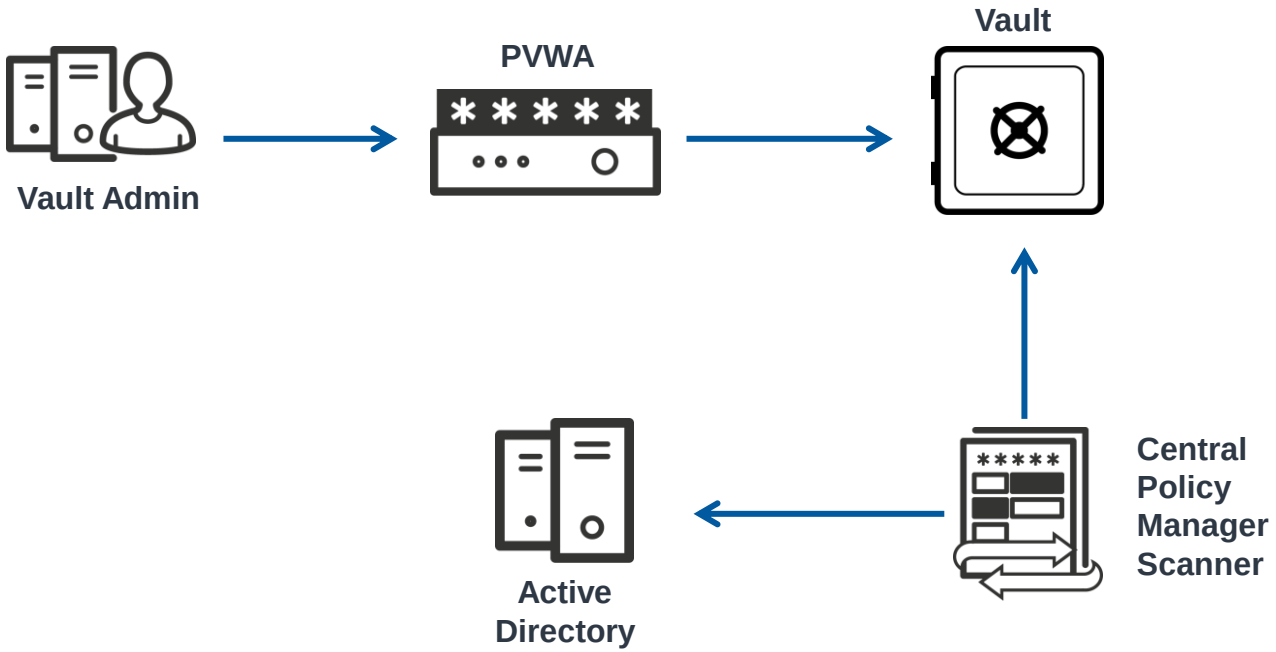
Windows Discovery

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Windows Discovery - Phase 1 of 2

The 1st phase of the Discovery:

- Log into the **PVWA**
- Configure the **Discovery**
- The **CPM** Scanner retrieves the Discovery…
- **CPM** scanner reads the directory to build the list of machines to scan



IT Environment

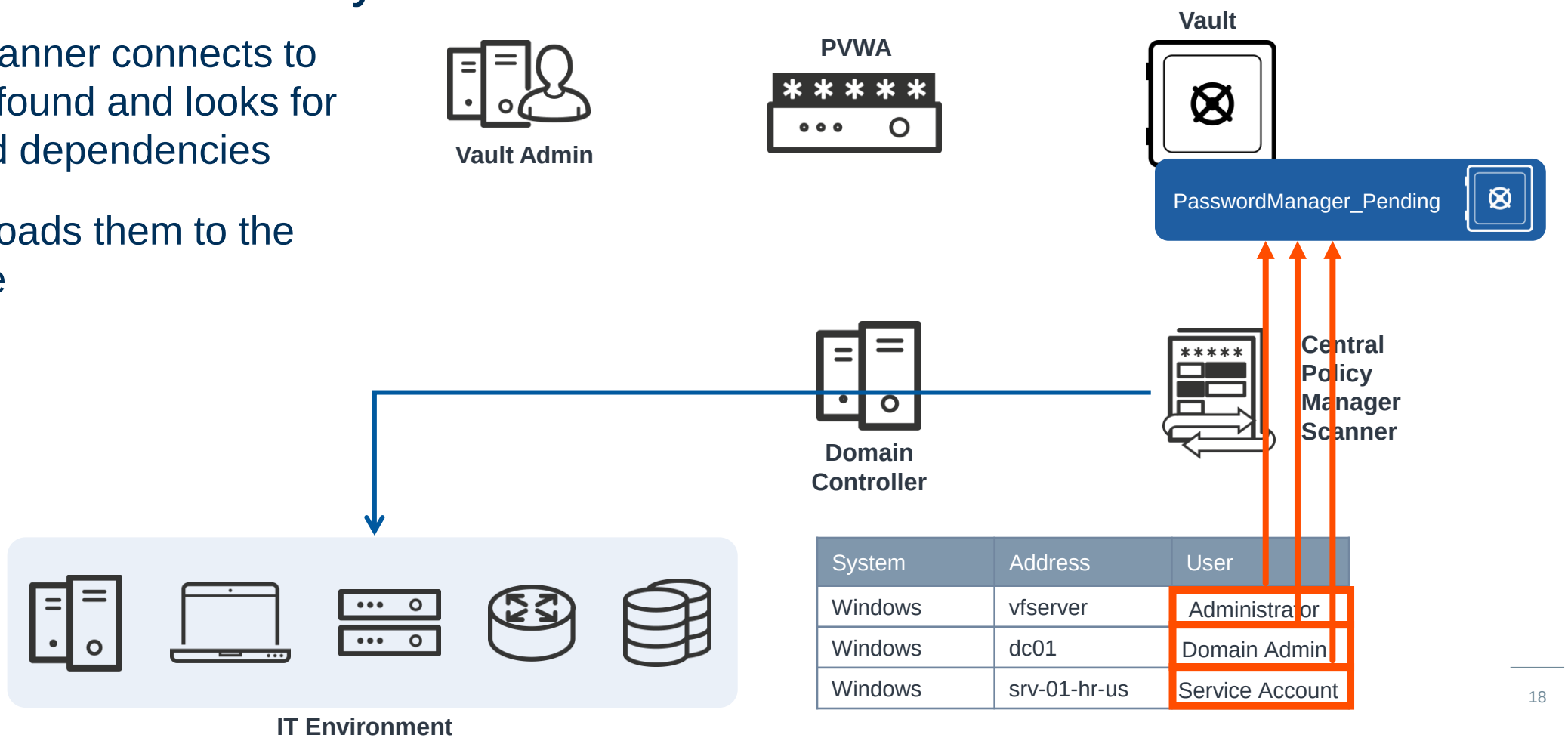
System	Address	User
Windows	vfserver	?
Windows	dc01	?
Windows	srv-01-hr-us	?

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Windows Discovery - Phase 2 of 2

In the 2nd phase of the Discovery:

- The CPM Scanner connects to each device found and looks for accounts and dependencies
- And then uploads them to the pending Safe

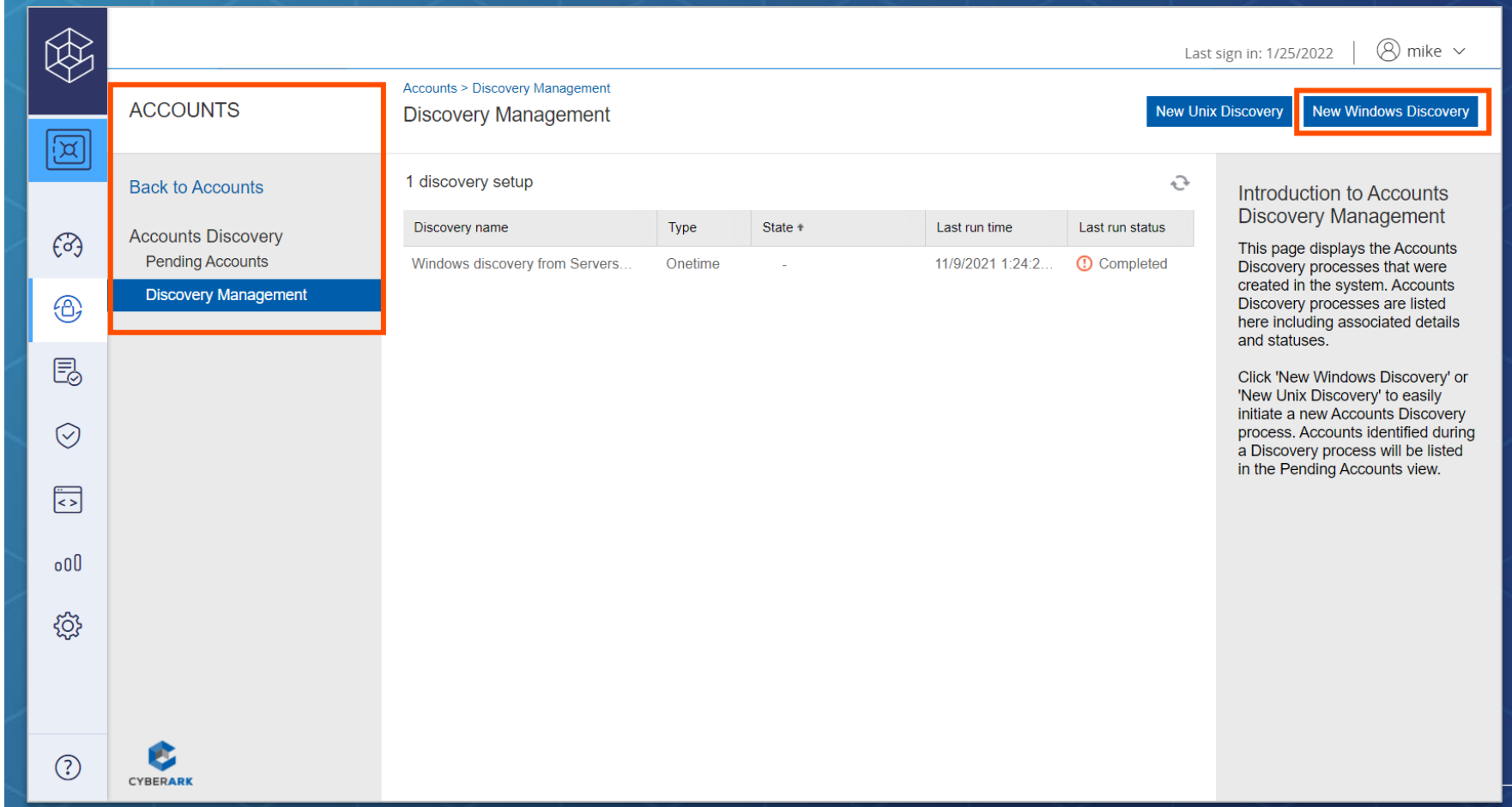


System	Address	User
Windows	vfserver	Administrator
Windows	dc01	Domain Admin
Windows	srv-01-hr-us	Service Account

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Running a New Windows Discovery

- Go to the ***Accounts*** tab. *Under* ***Accounts Feed***, click on ***Pending & Discovery*** and then ***Discovery Management***
- Available to members of the Vault Admins group
- Then click ***New Windows Discovery***

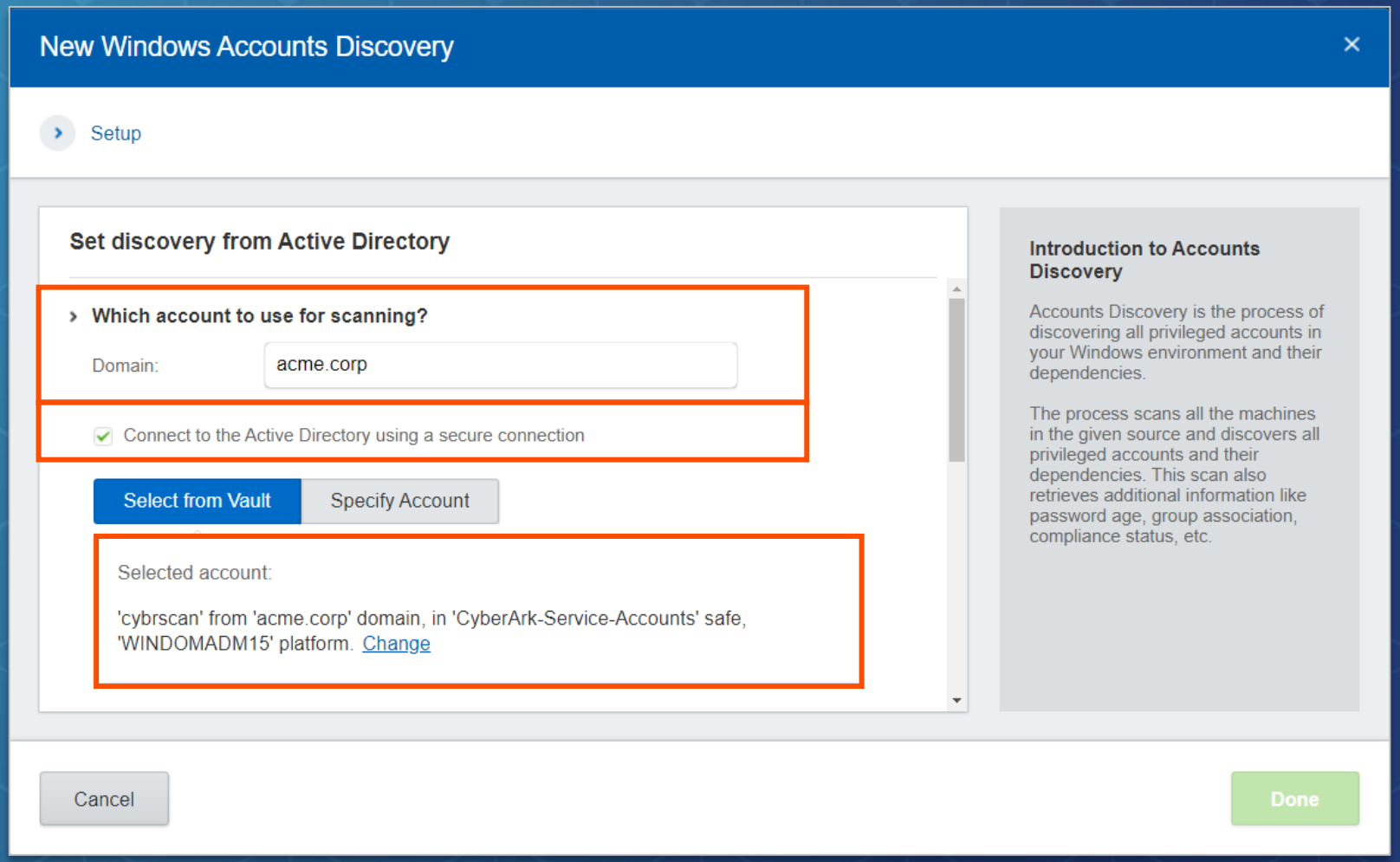


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Running a New Windows Discovery

Information needed for a Windows discovery:

- Domain Name
- Choose if a secure connection will be used to connect to Active Directory
- Scan account
- Continued…

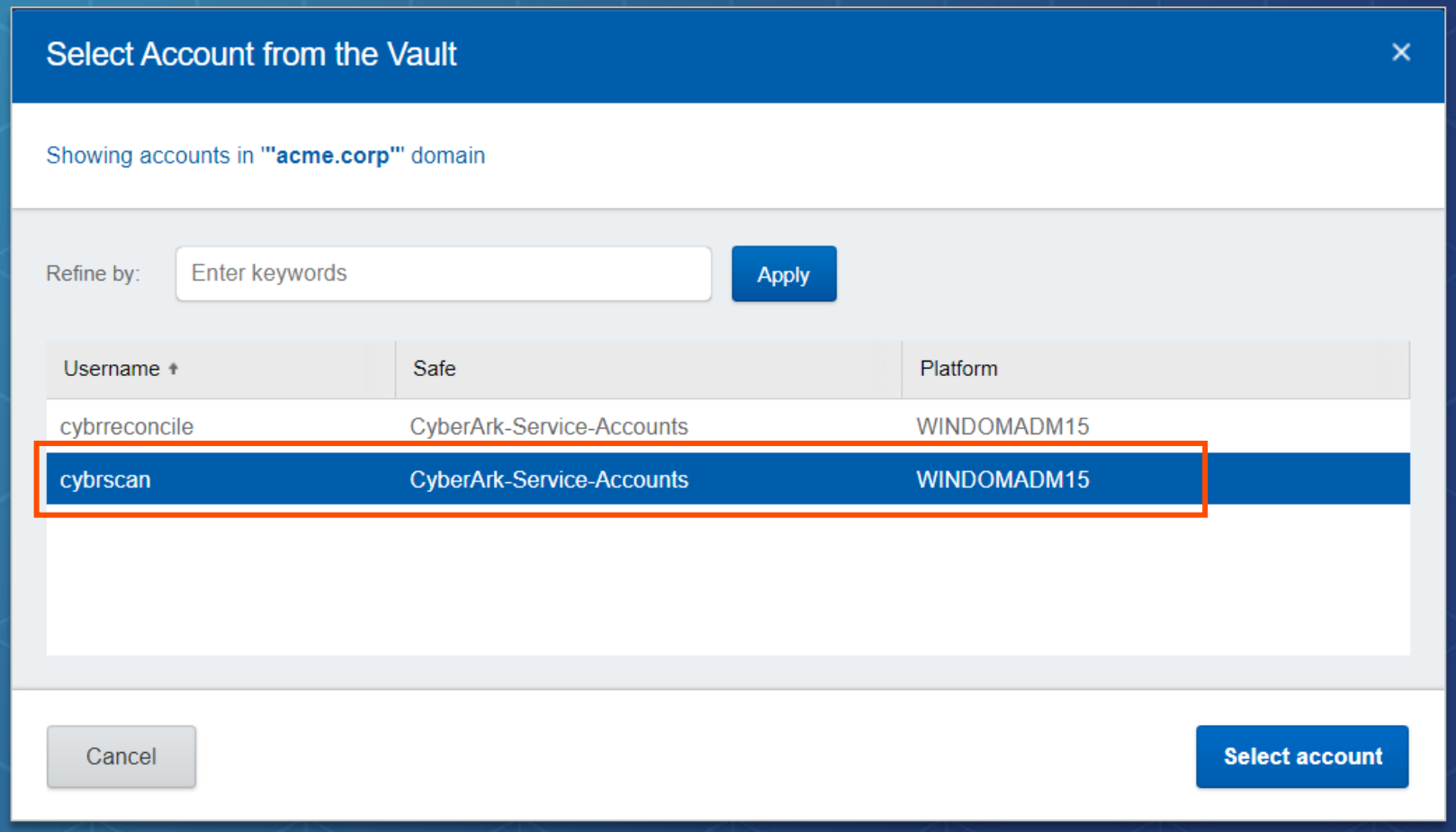


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Windows Discovery – Which Account to Use?

The account **must**:

- Be a domain account
- Have the following permissions:
  - ***Read*** permissions on the Active Directory
  - Local administrative rights on discovered Windows servers and workstations

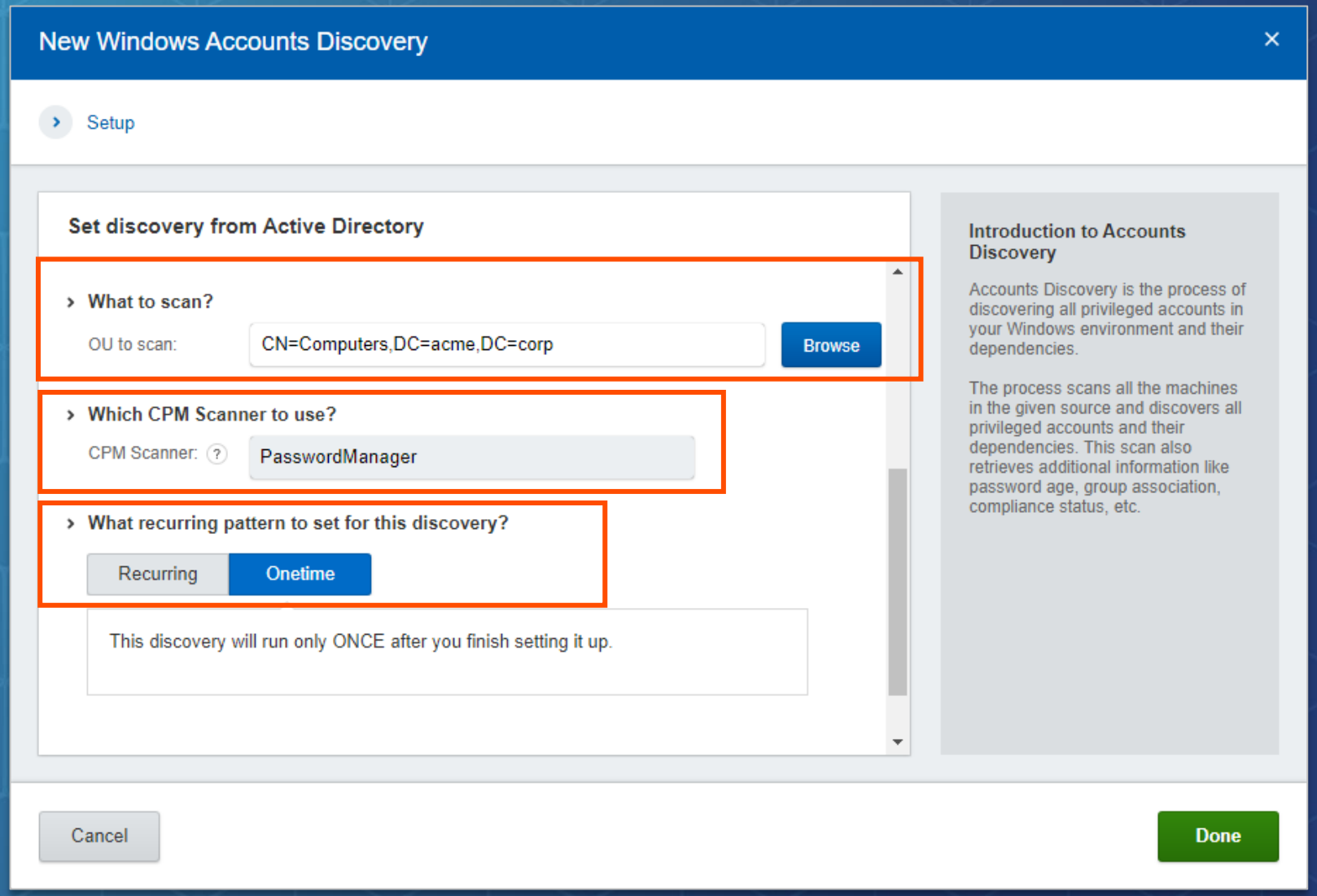


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Running a New Windows Discovery

Information needed for a Windows discovery:

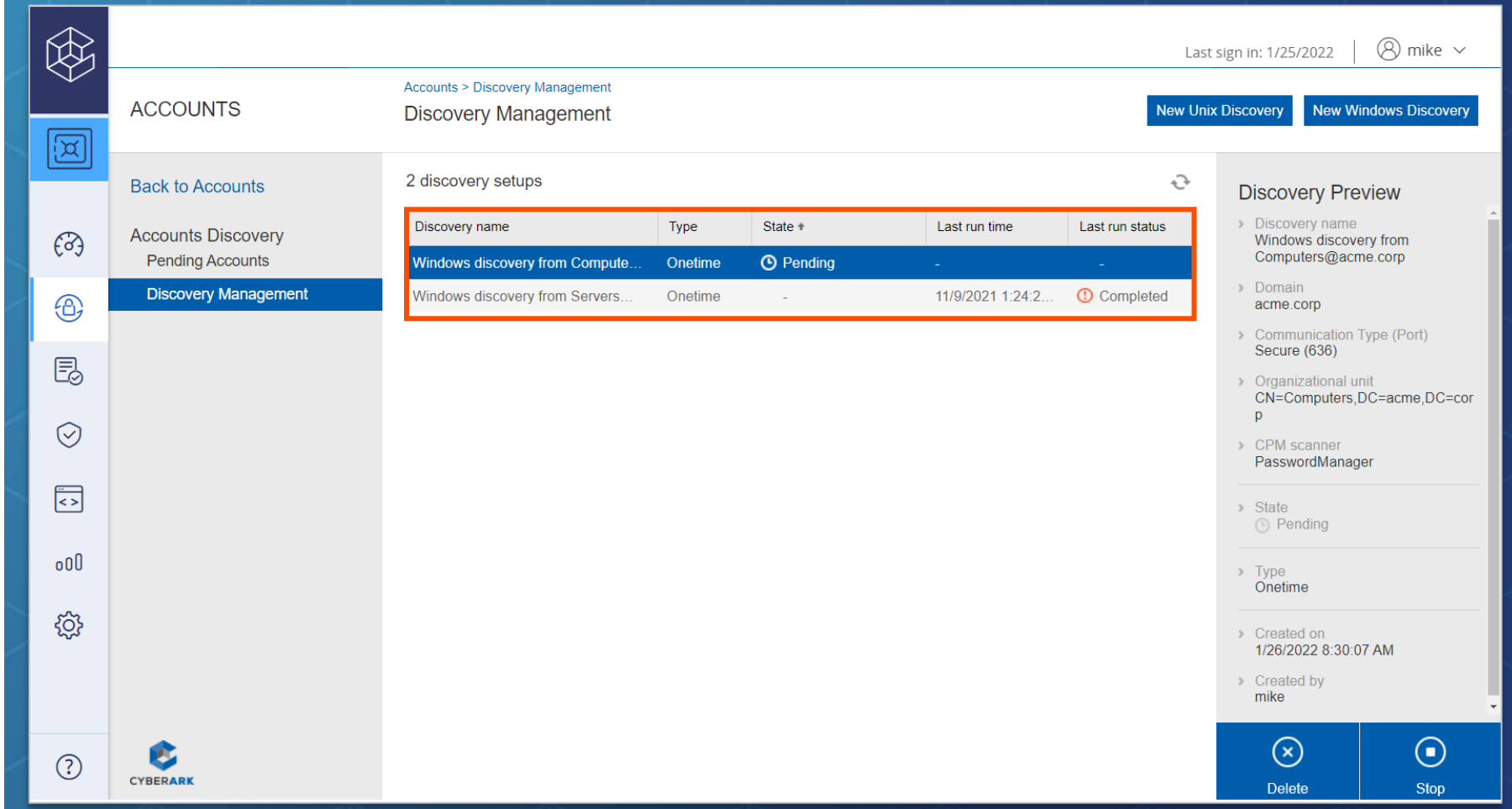
- Domain Name
- Choose if a secure connection will be used to connect to Active Directory
- Scan account
- OU of Servers / Workstations in AD
- CPM to perform the scan
- Whether to run a recurring or one-time discovery



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Completing the New Discovery

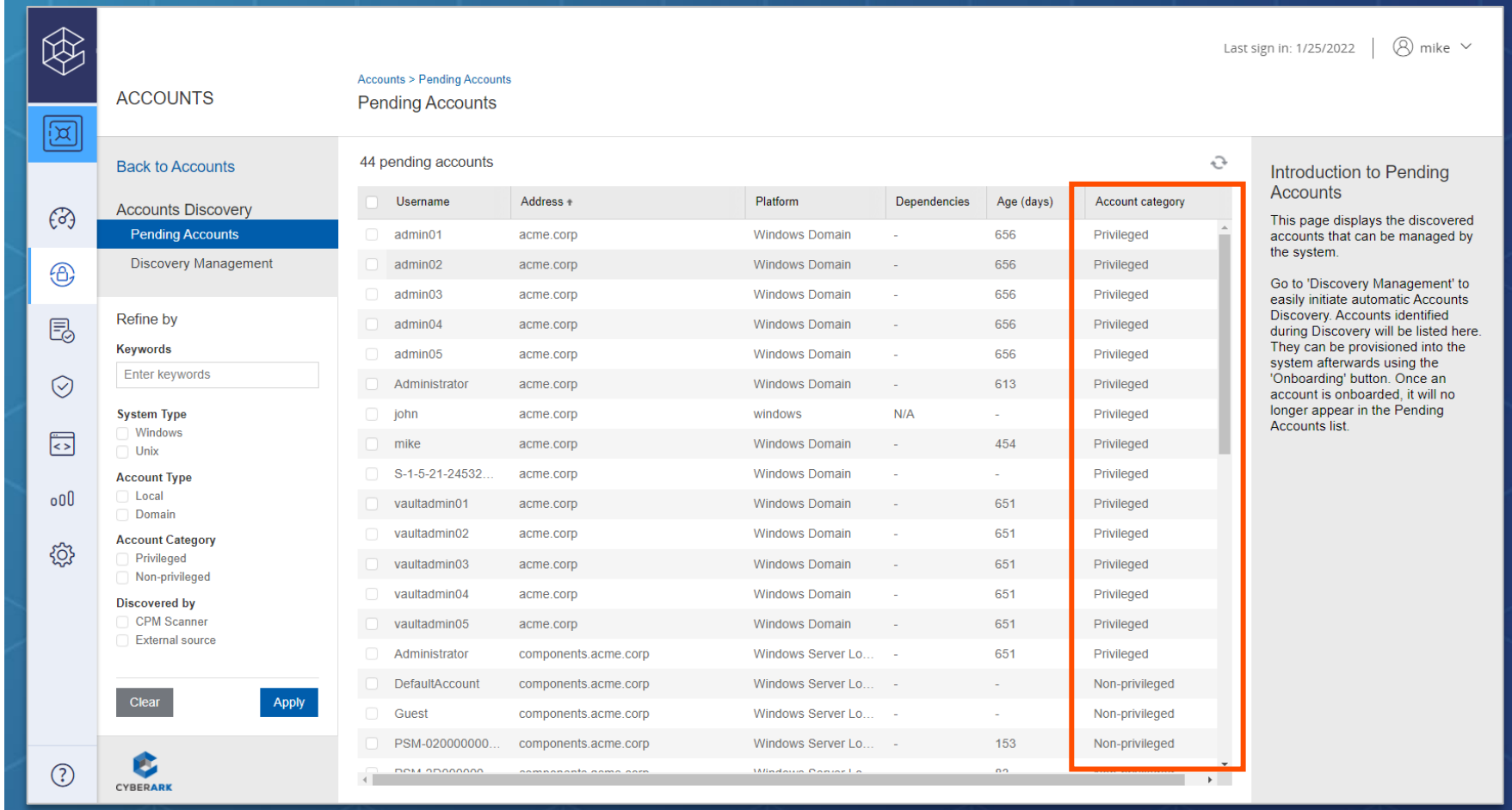
- The new discovery will be listed on the ***Discovery Management*** page
- The status will be listed as ***Pending*** until the process starts.
- The status will change to ***Running*** when the process starts
- At this point you can
  - Stop the Discovery
  - Delete the Discovery



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Windows Discovery Process

- Multiple discoveries from different **CPM Scanners** can run simultaneously
- Accounts found will be categorized as Privileged / Non-Privileged:
  - The categorization is based on the group membership
  - If the account is a member of any Local Administrators group, the account is privileged
  - The account will remain privileged until removed from all machines it was discovered on

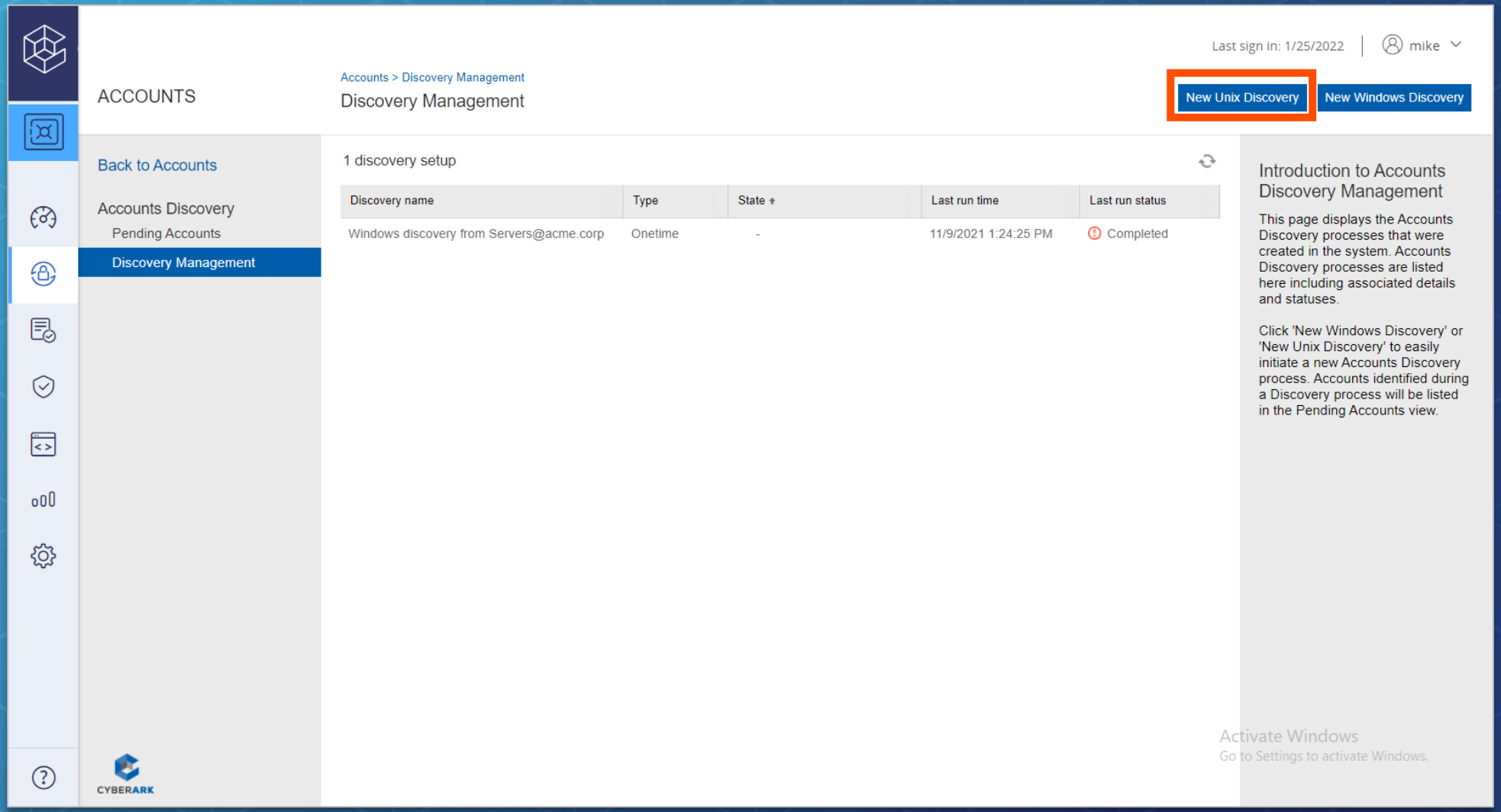


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Unix Discovery

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Set Up a New Unix Discovery

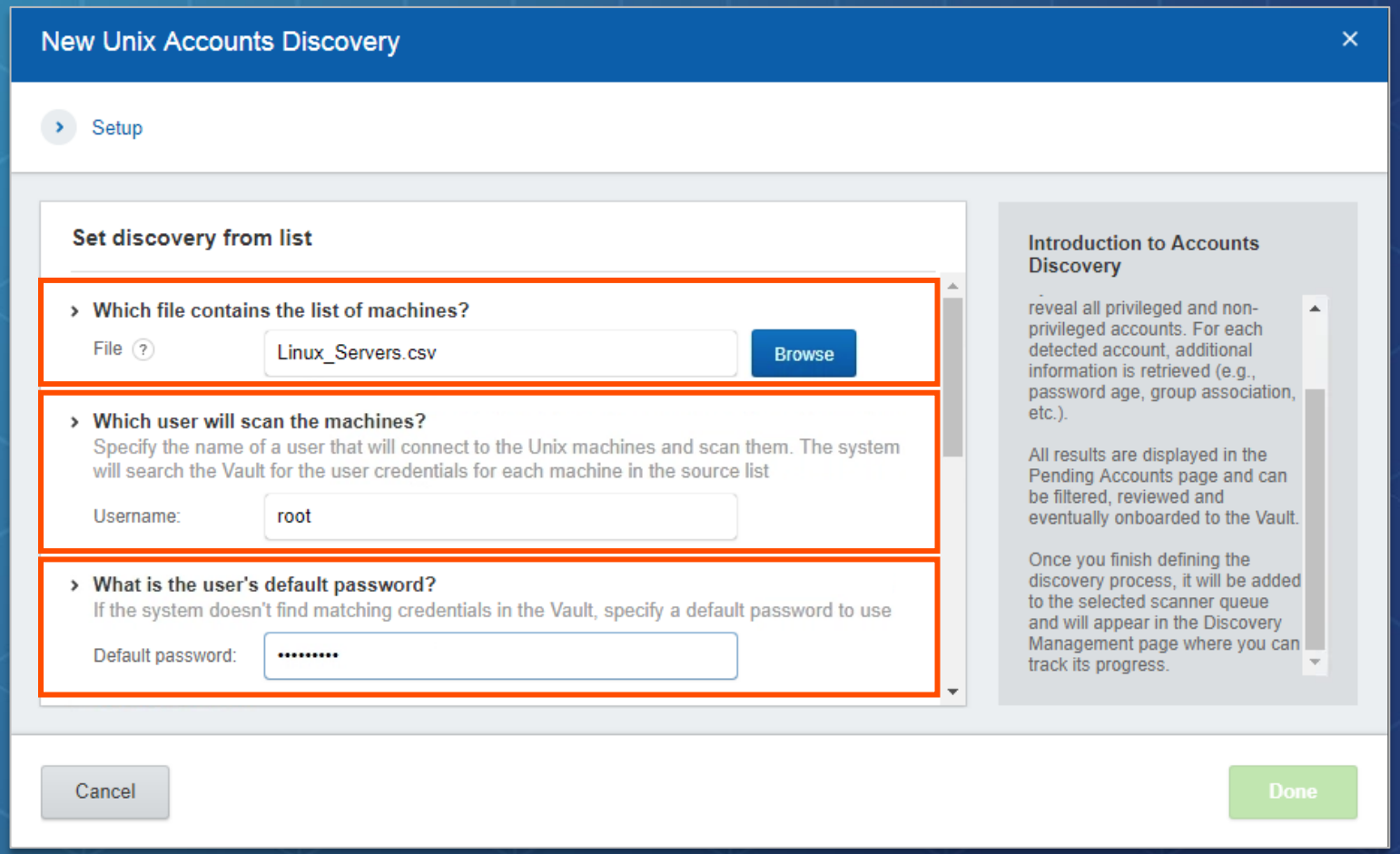


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Set Up a New Unix Discovery

Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password

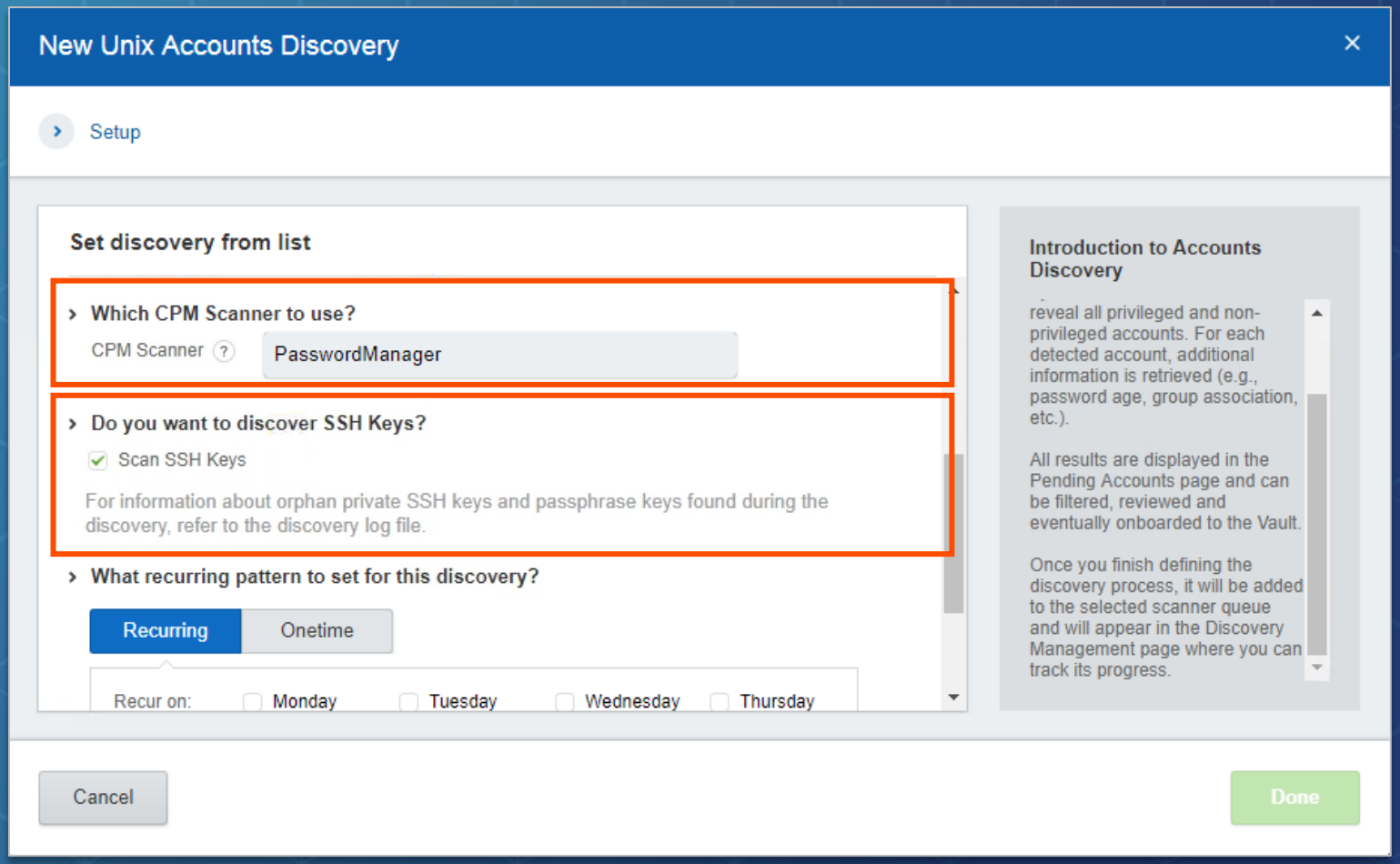


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Set Up a New Unix Discovery

Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password
- CPM Scanner
- Whether or not to scan for SSH Keys

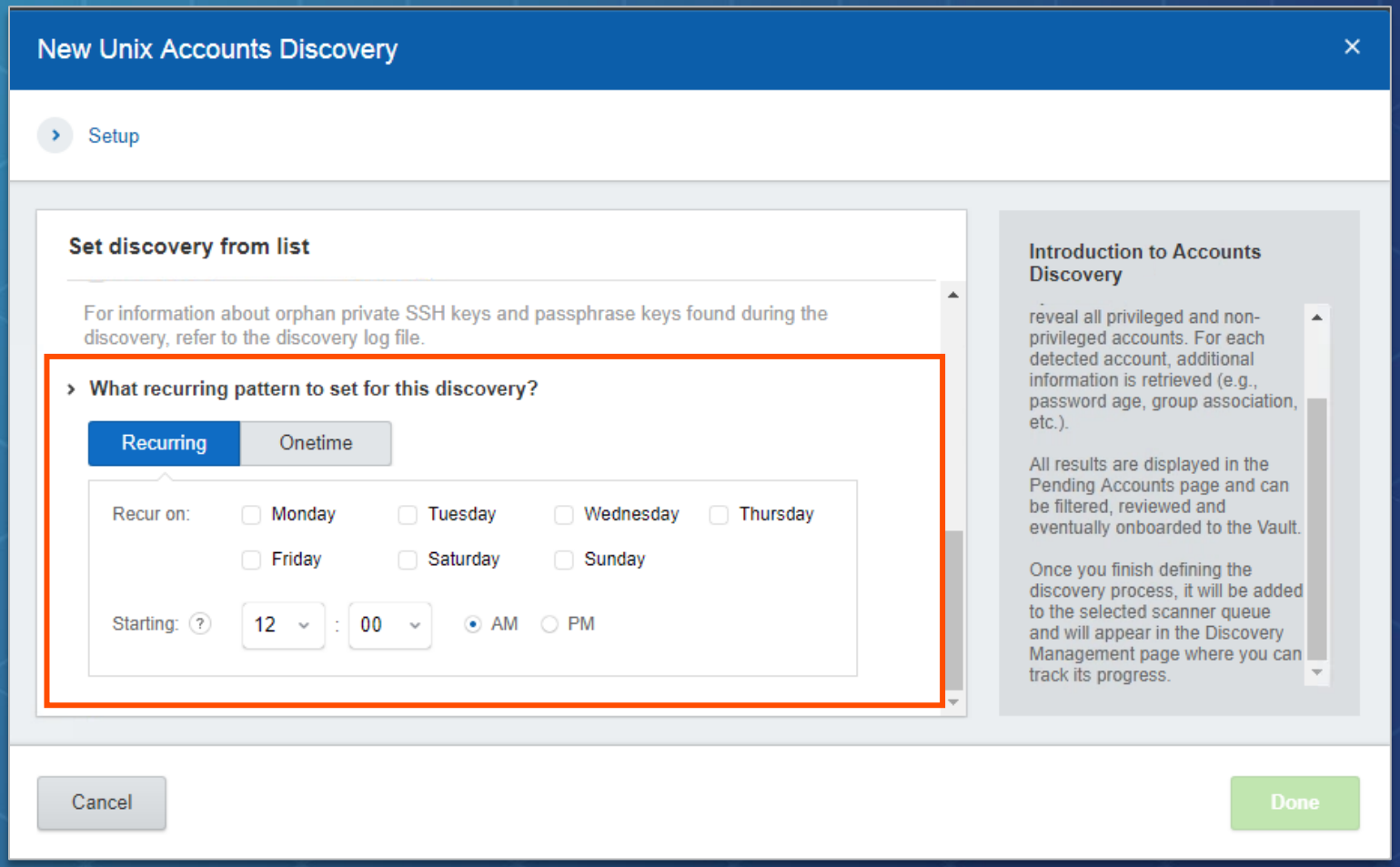


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Set Up a New Unix Discovery

Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password
- CPM Scanner
- Whether or not to scan for SSH Keys
- Recurring or One-time



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

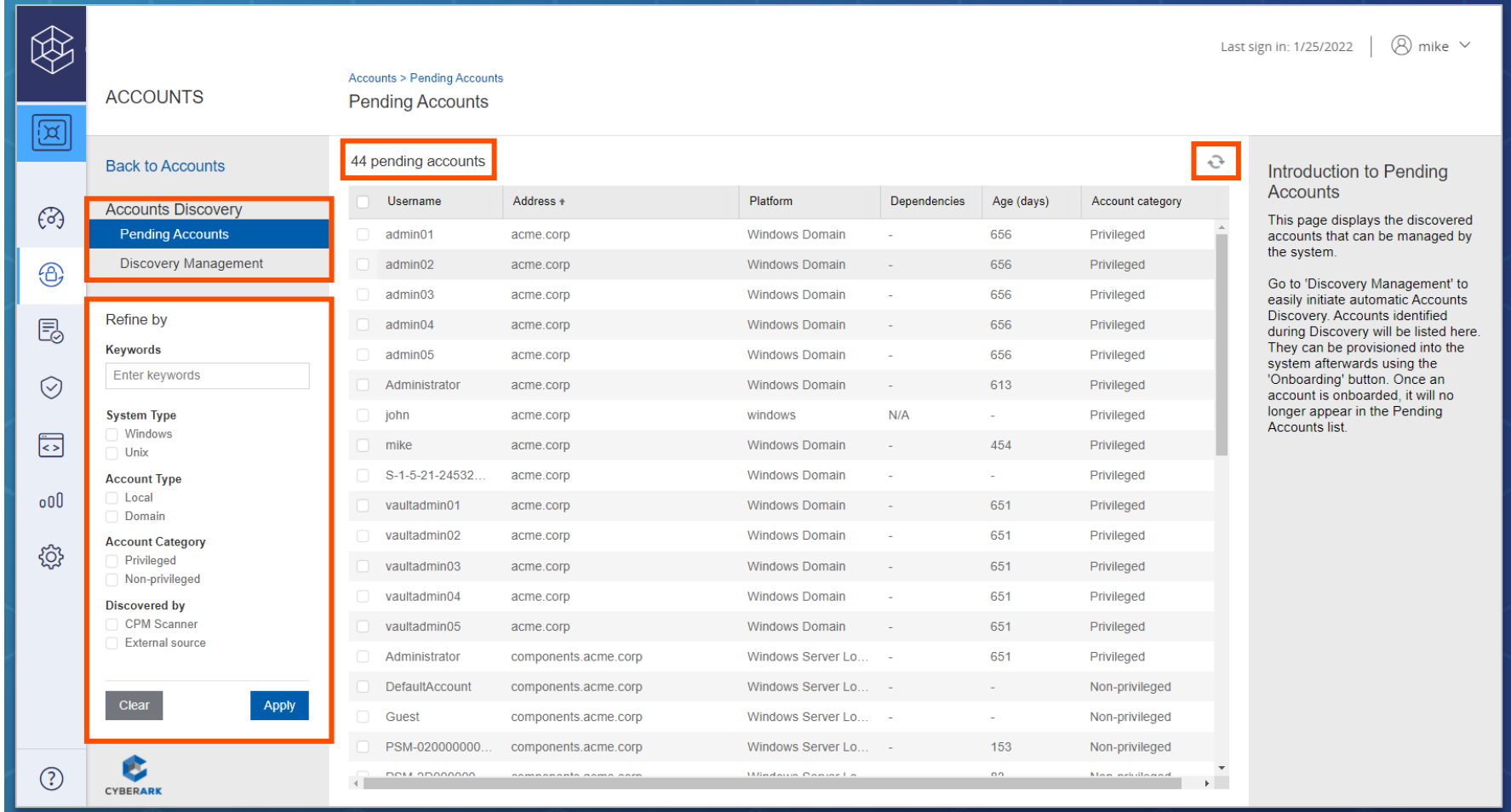
Pending Accounts

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Pending Accounts

Accounts that do not match any Onboarding Rule will be listed in ***Pending Accounts***

- Various search criteria are available under ***Refine by***
- The results of these queries are displayed above the list
- Click F5 to refresh the list or use the ***Refresh*** button

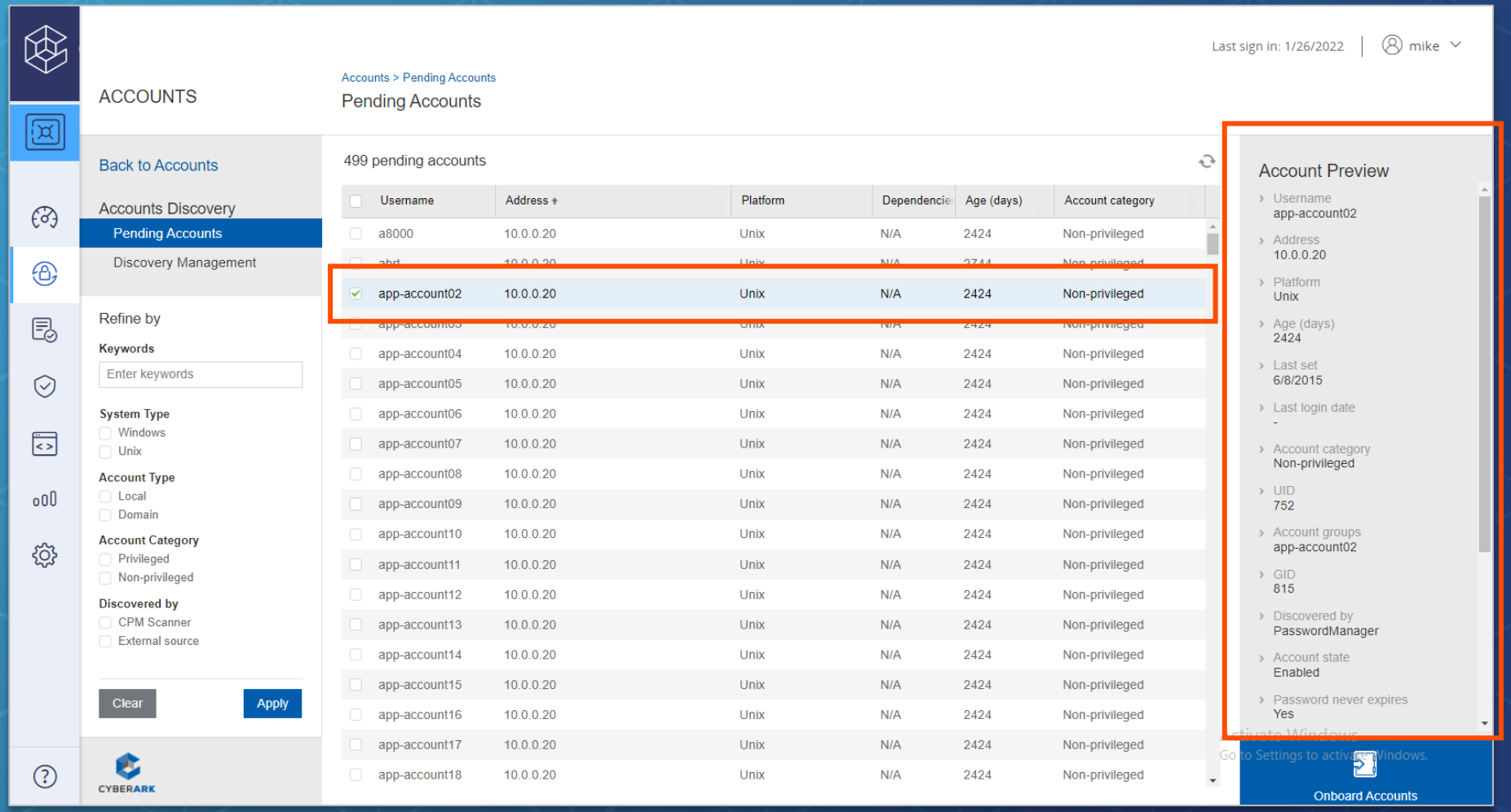


Username	Address	Platform	Dependencies	Age (days)	Account category
admin01	acme.corp	Windows Domain	-	656	Privileged
admin02	acme.corp	Windows Domain	-	656	Privileged
admin03	acme.corp	Windows Domain	-	656	Privileged
admin04	acme.corp	Windows Domain	-	656	Privileged
admin05	acme.corp	Windows Domain	-	656	Privileged
Administrator	acme.corp	Windows Domain	-	613	Privileged
john	acme.corp	windows	N/A	-	Privileged
mike	acme.corp	Windows Domain	-	454	Privileged
S-1-5-21-24532...	acme.corp	Windows Domain	-	-	Privileged
vaultadmin01	acme.corp	Windows Domain	-	651	Privileged
vaultadmin02	acme.corp	Windows Domain	-	651	Privileged
vaultadmin03	acme.corp	Windows Domain	-	651	Privileged
vaultadmin04	acme.corp	Windows Domain	-	651	Privileged
vaultadmin05	acme.corp	Windows Domain	-	651	Privileged
Administrator	components.acme.corp	Windows Server Lo...	-	651	Privileged
DefaultAccount	components.acme.corp	Windows Server Lo...	-	-	Non-privileged
Guest	components.acme.corp	Windows Server Lo...	-	-	Non-privileged
PSM-020000000...	components.acme.corp	Windows Server Lo...	-	153	Non-privileged

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Account Preview

Click on an account to see further details in the **Account Preview** pane.



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Dependencies

For Windows accounts, the ***Dependencies*** column shows you if any account is used anywhere else (a ***usage***), such as for a Windows service or scheduled task.

Accounts > Pending Accounts

Pending Accounts

99 results for: 'Windows','Local'

Username	Address	Platform	Dependencies	Age (days)	Accou
PSM-430000000...	COMP01A.cyber-ark-demo.local	Windows Server Lo...	-	5	Non-p
PSMAdminConn...	COMP01A.cyber-ark-demo.local	Windows Server Lo...	-	821	Non-p
PSMConnect	COMP01A.cyber-ark-demo.local	Windows Server Lo...	-	821	Non-p
test	COMP01A.cyber-ark-demo.local	Windows Server Lo...	-	1210	Non-p
Guest	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	-	-	Non-p
localadmin10	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privil
localadmin11	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privil
localadmin12	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privil
localadmin13	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privileged
localadmin14	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privileged
localadmin15	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privileged
localadmin16	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privileged
localadmin17	VFSERVER.cyber-ark-demo.local	Windows Server Lo...	1	1173	Privileged

Dependencies of Pending Account

localadmin17 on VFSERVER.cyber-ark-demo.local

Discovered 1 dependencies

Dependency Name	Address	Dependency Type
SchedTask17	VFSERVER.cyber-ark-demo.local	Windows Scheduled Task

Close

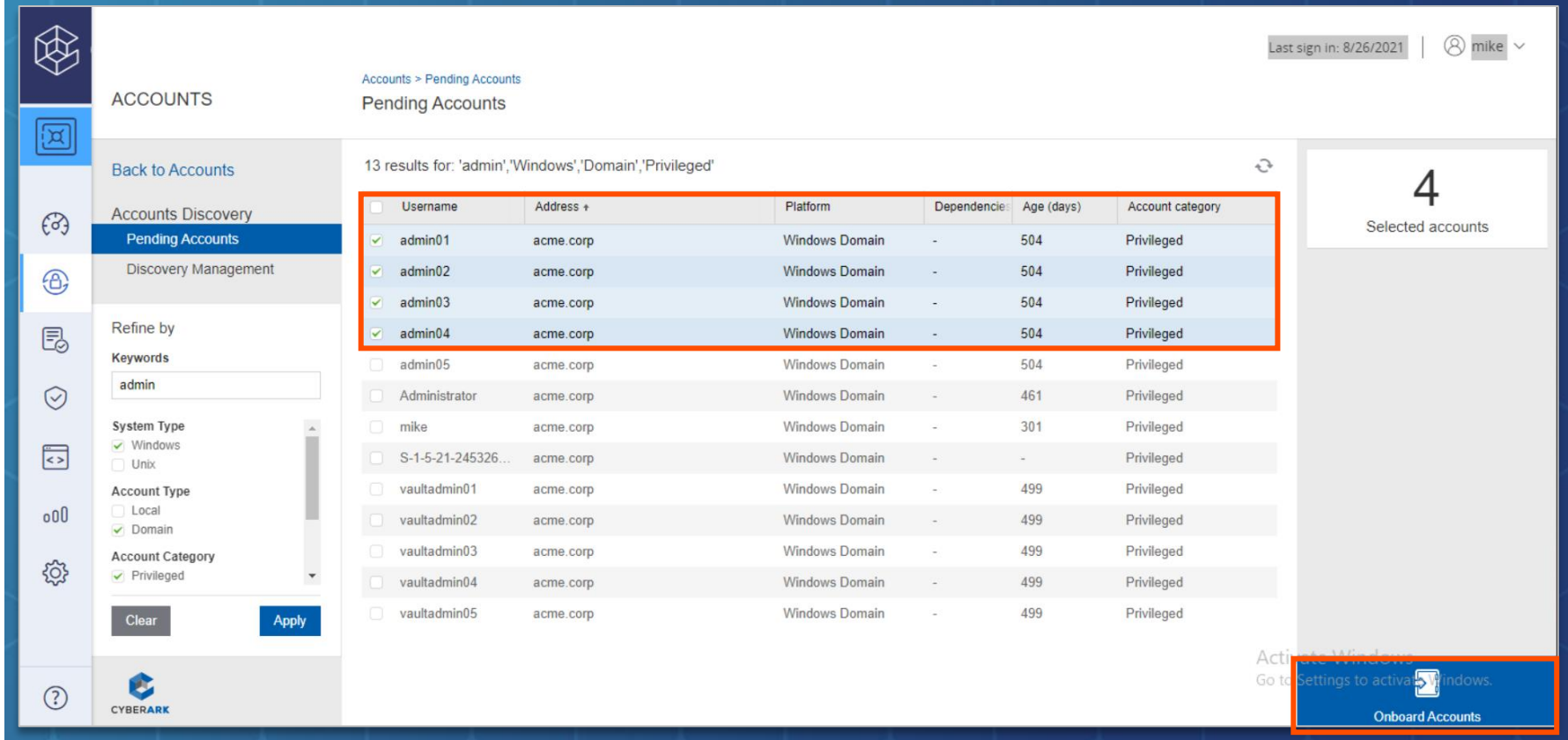
Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Accounts

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Pending Accounts - 1

Select one or more accounts from the list of Pending accounts and click ***Onboard Accounts***

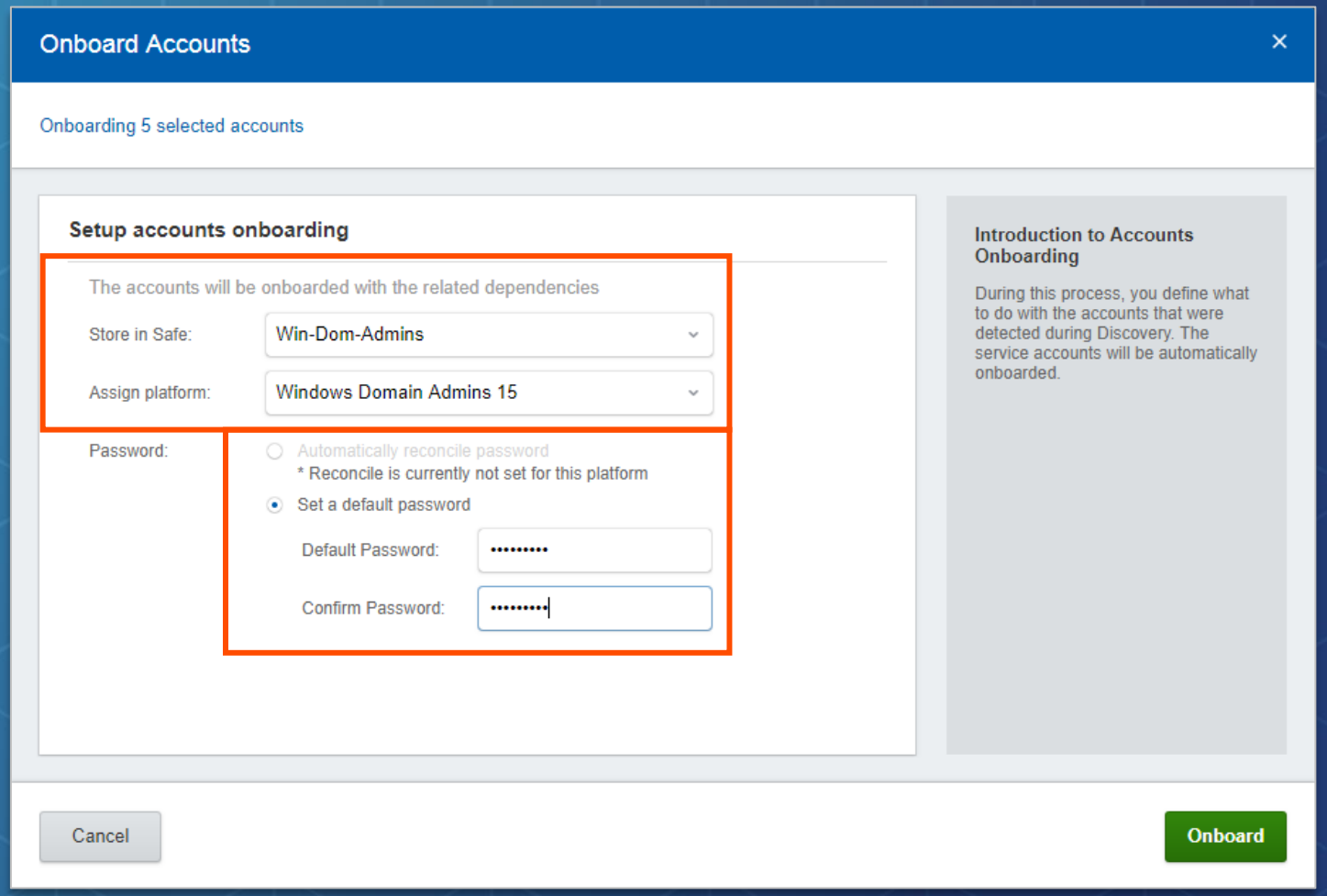


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Pending Accounts - 2

Information needed for onboarding accounts:

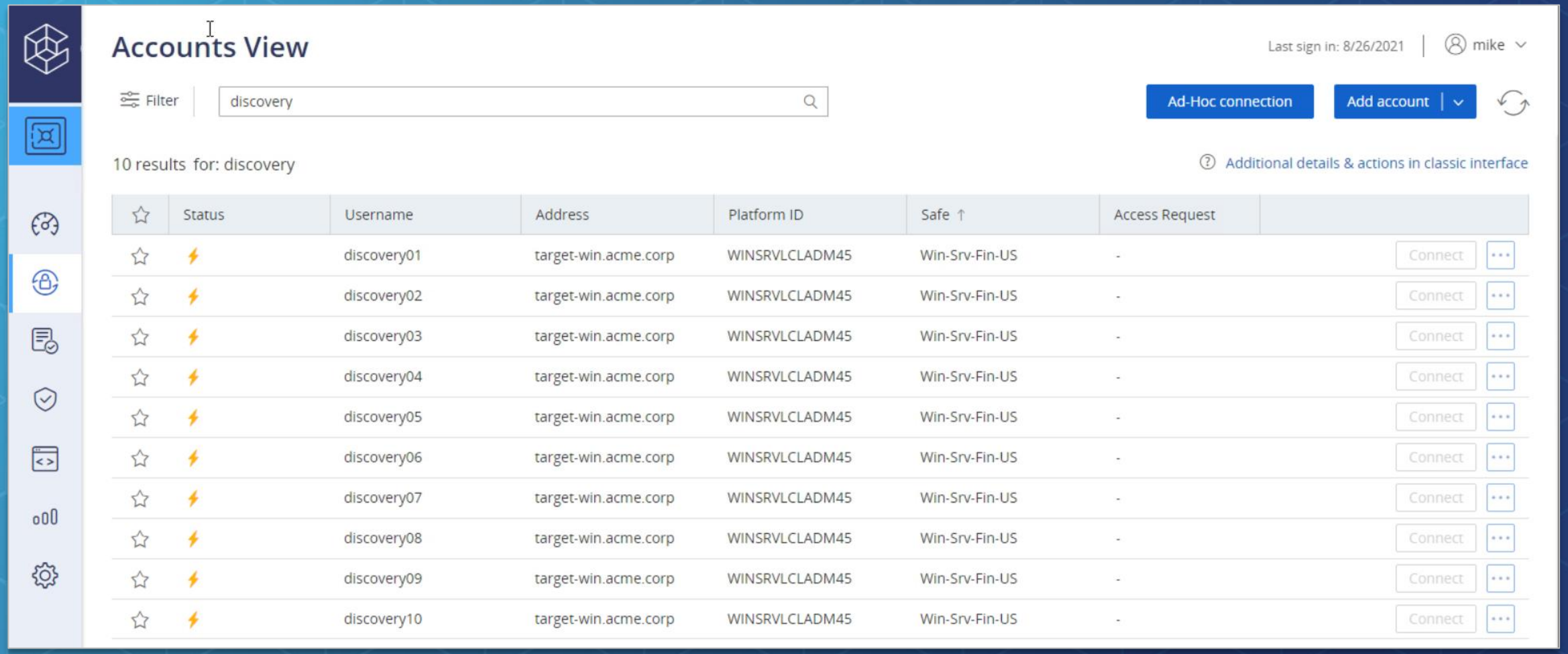
- The ***Safe*** in which these accounts should be stored. You can either choose an existing safe or create a new one
- The ***Platform*** –
  - What type of account are these?
  - Do they require a separate platform?
  - Is reconciliation available?



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Pending Accounts - 3

Onboarded accounts can now be found in the ***Accounts View***



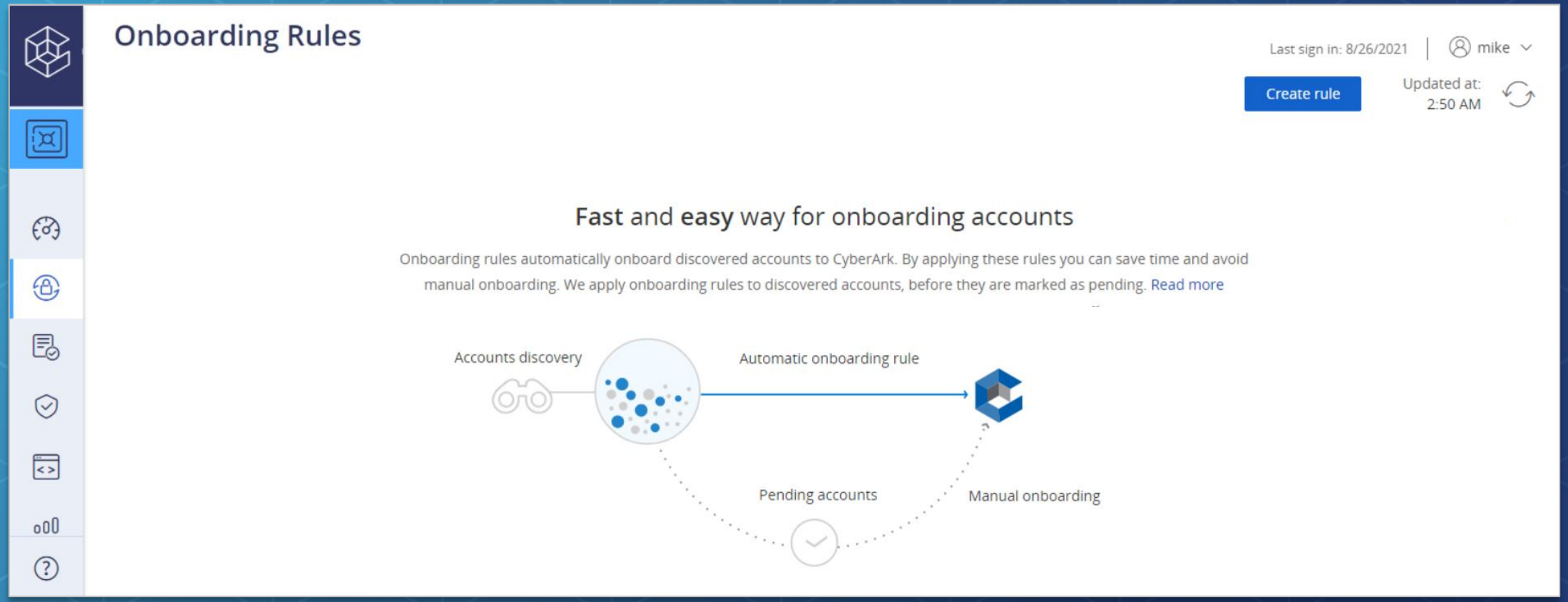
Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Rules

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Automatic Onboarding Rules

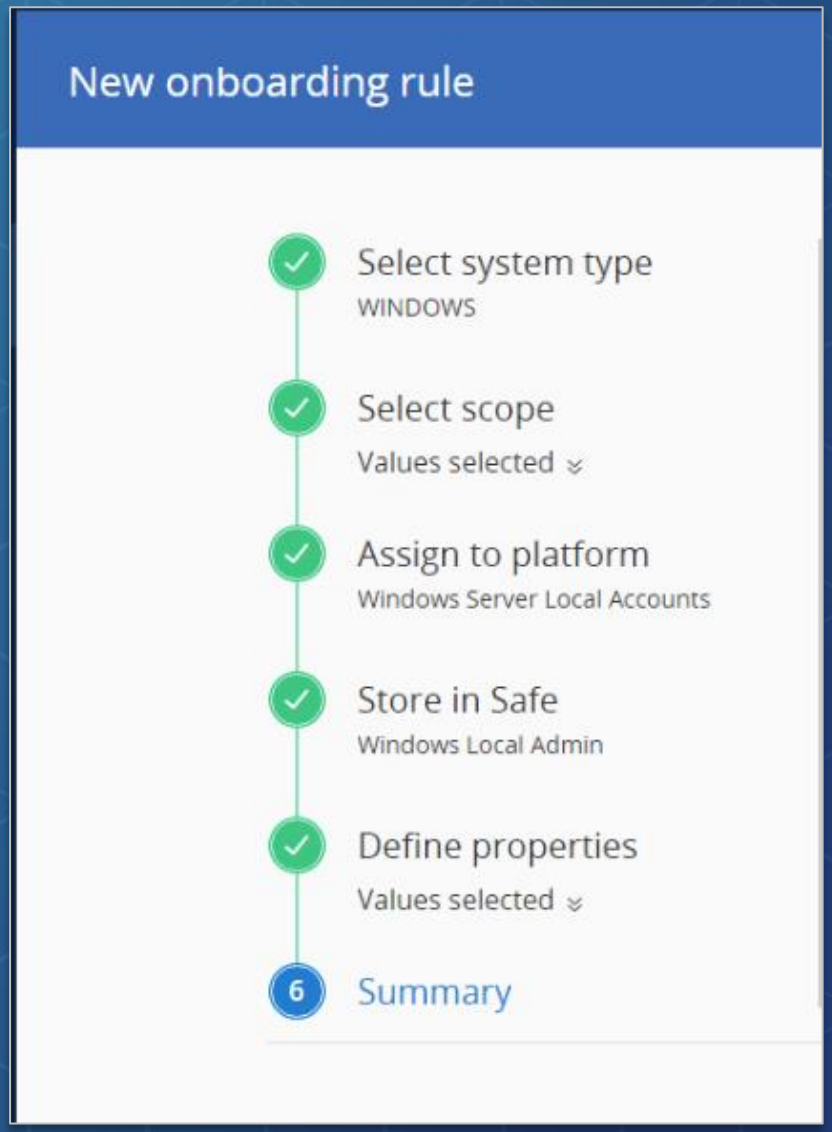
Minimize the time it takes to onboard and to manage accounts securely, reduce the time spent reviewing pending accounts, and prevent human errors from occurring during manual onboarding



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard

An intuitive wizard steps you through each stage of the rule creation process and ensures that each rule is unique

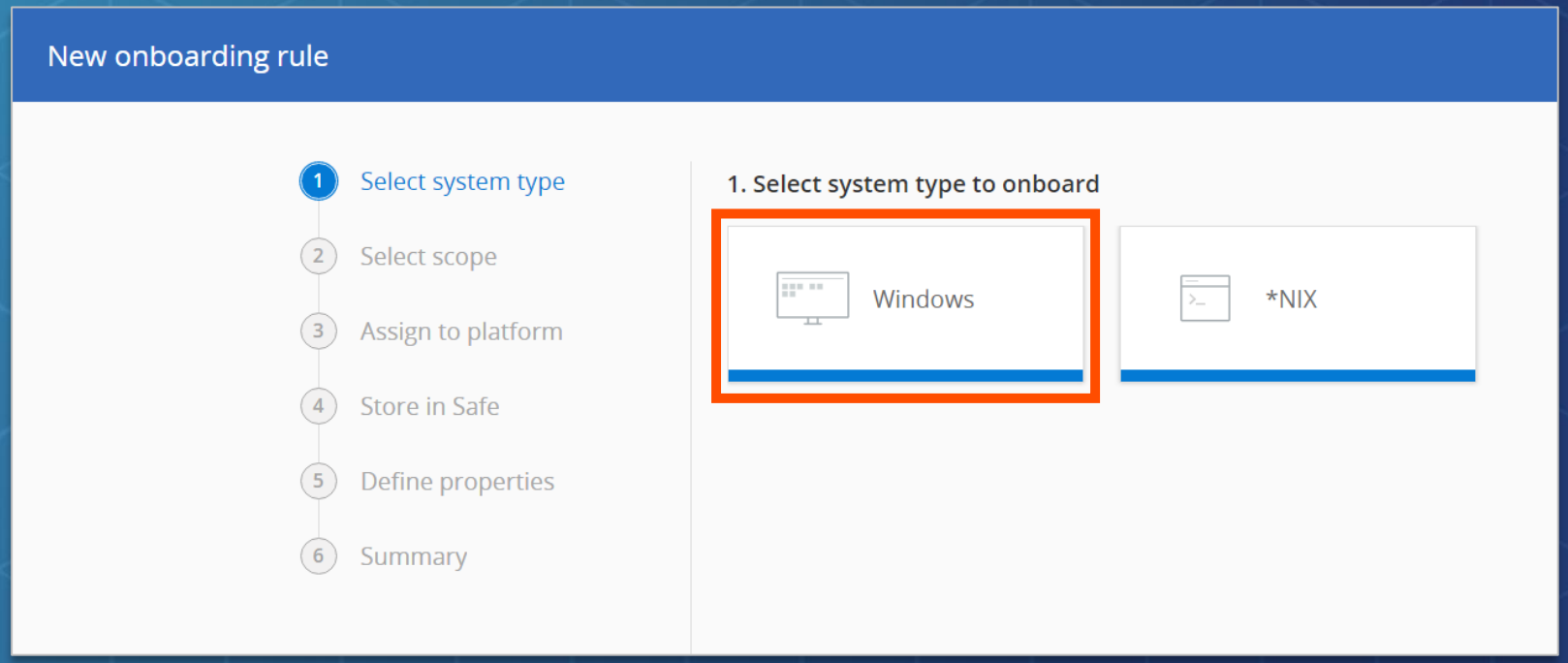


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard: Select System Type

Select the type of account to onboard:

- Windows
- *Nix

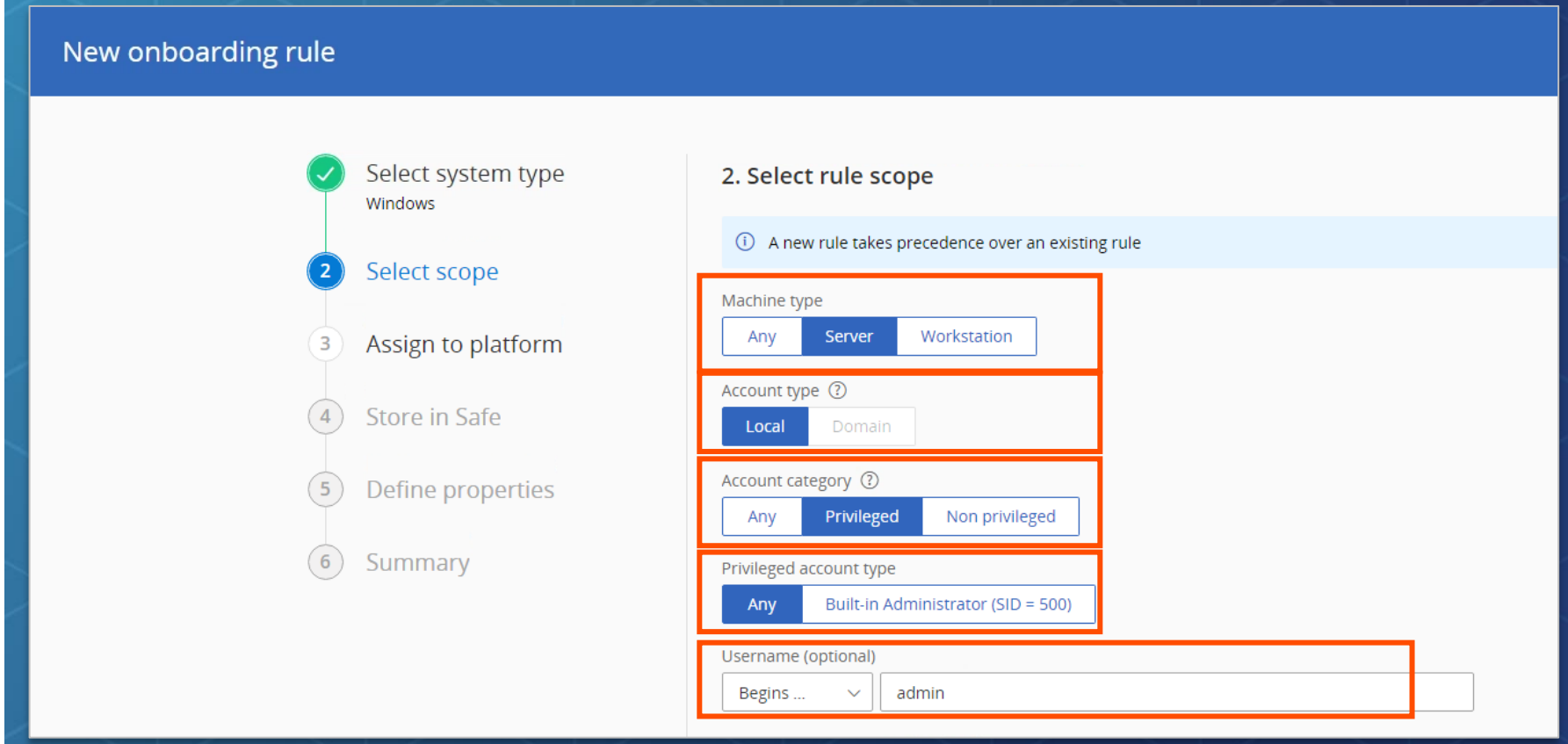


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard:

Select Scope

- Machine type
- Account type
- Account Category
- Privileged account type
- Optionally, a user name string to match

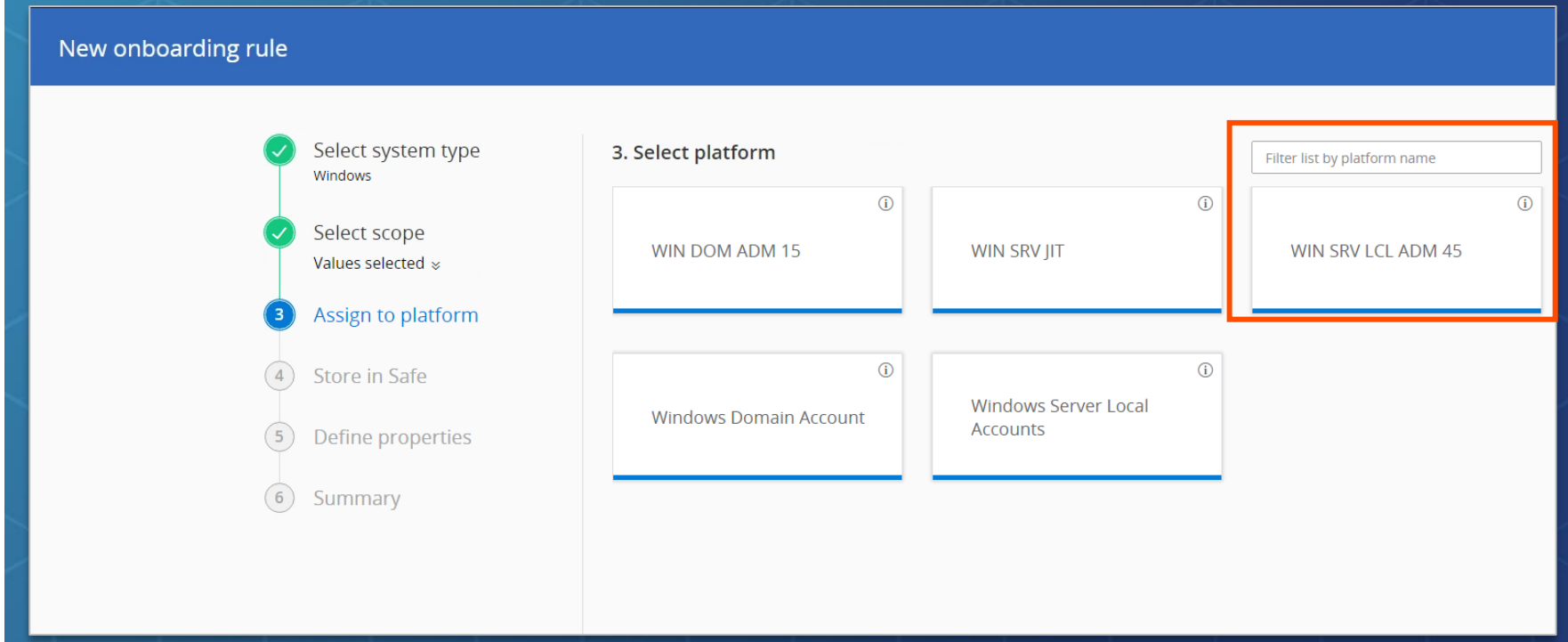


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard:

Select Platform

- Select the target ***Platform*** that will be associated with accounts that match this rule

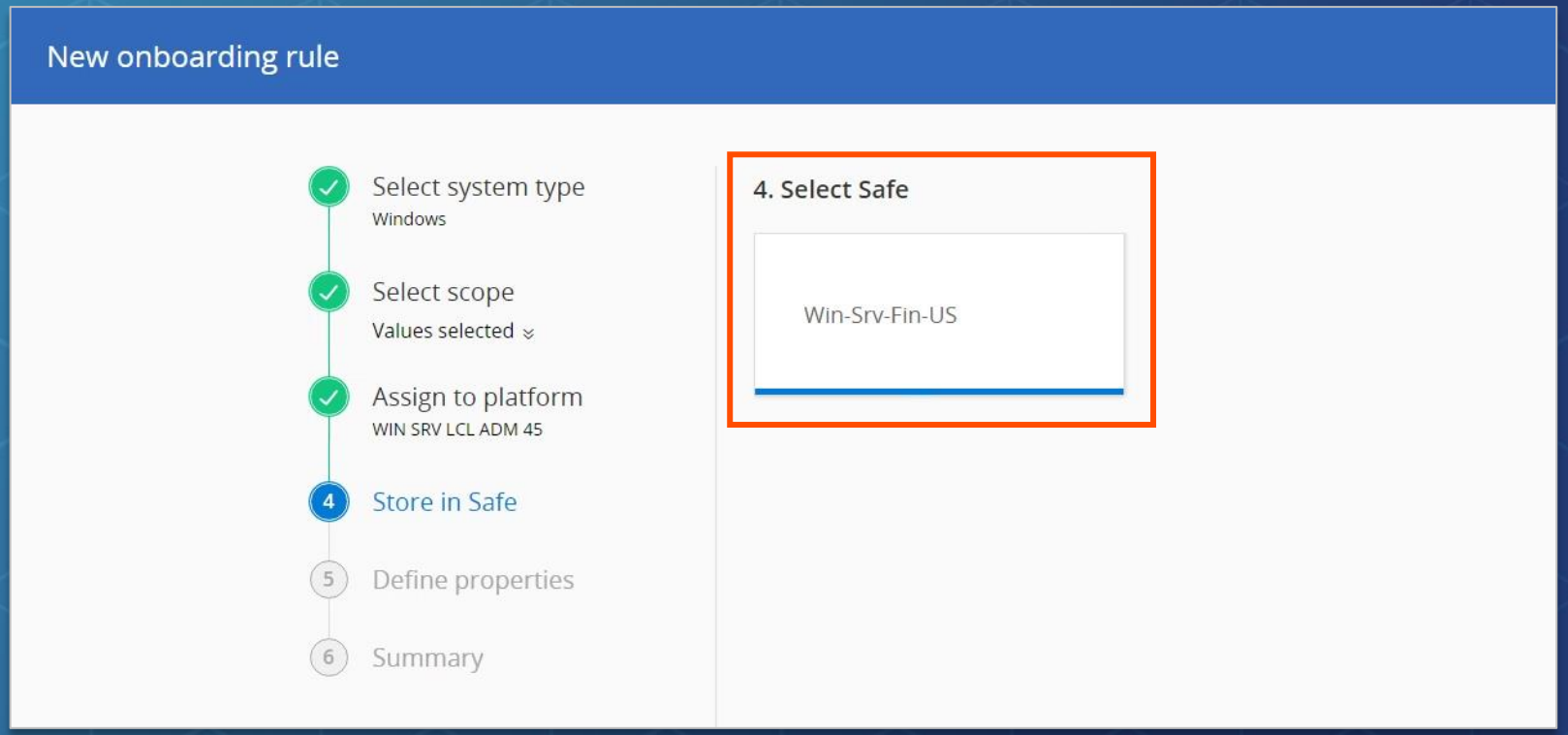


Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard:

Select Safe

- Select the ***Safe*** in which the accounts will be stored



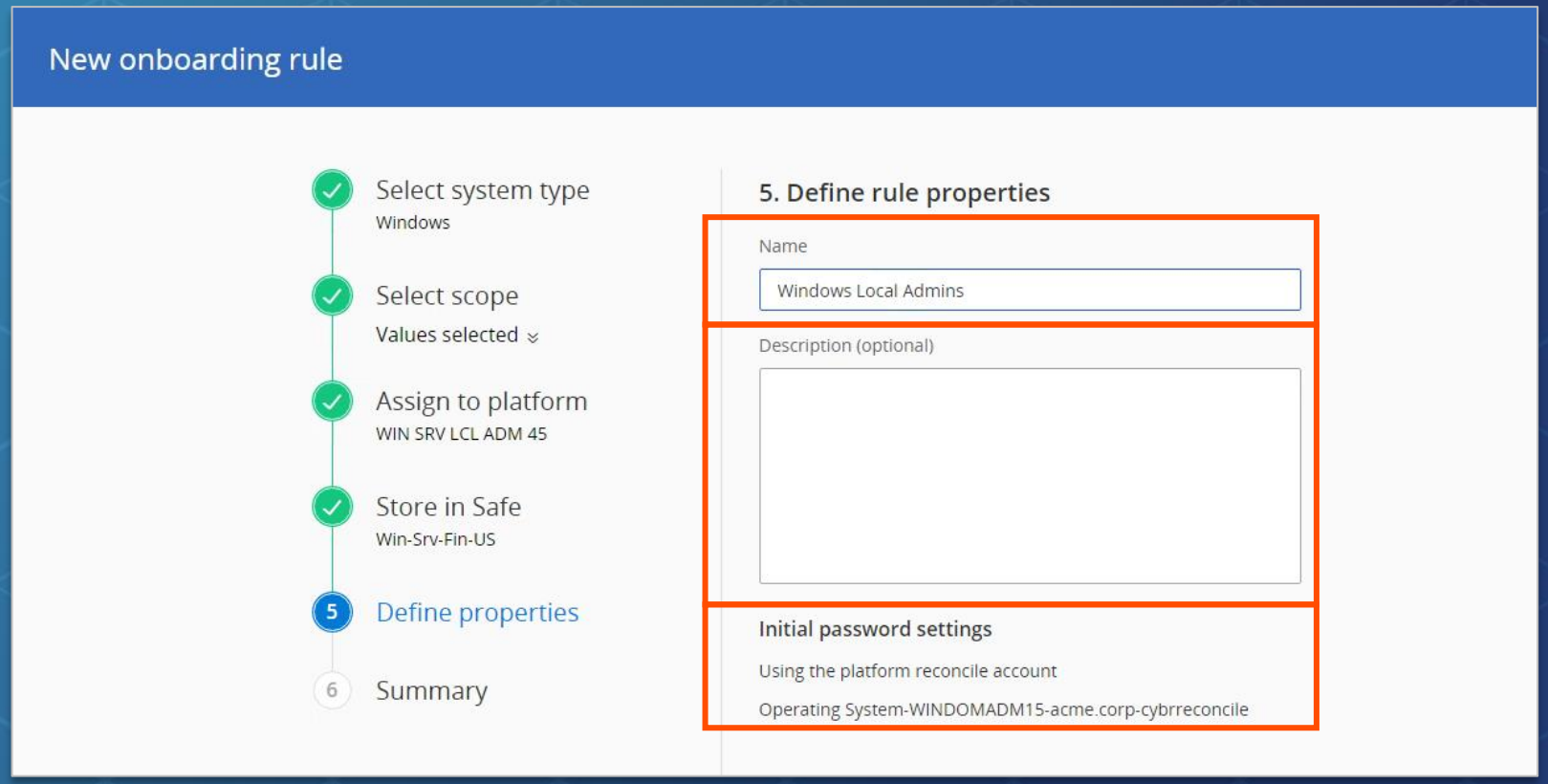
Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Onboarding Wizard:

Define Rule Properties

Define properties of this new rule

- Name
- Description
- Initial password settings



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

New Rule Creation Summary

New onboarding rule

- Select system type
  Windows
- Select scope
  Values selected
- Assign to platform
  WIN SRV LCL ADM 45
- Store in Safe
  Win-Srv-Fin-US
- Define properties
  Values selected
- 6 Summary

6. Summary

Rule scope

System type Windows	Account category Privileged
Machine type Server	Privileged account type Any
Account type Local	Username Begins with: admin

Destination

Platform WIN SRV LCL ADM 45	Safe Win-Srv-Fin-US

Rule properties

Cancel | < Back | Create rule

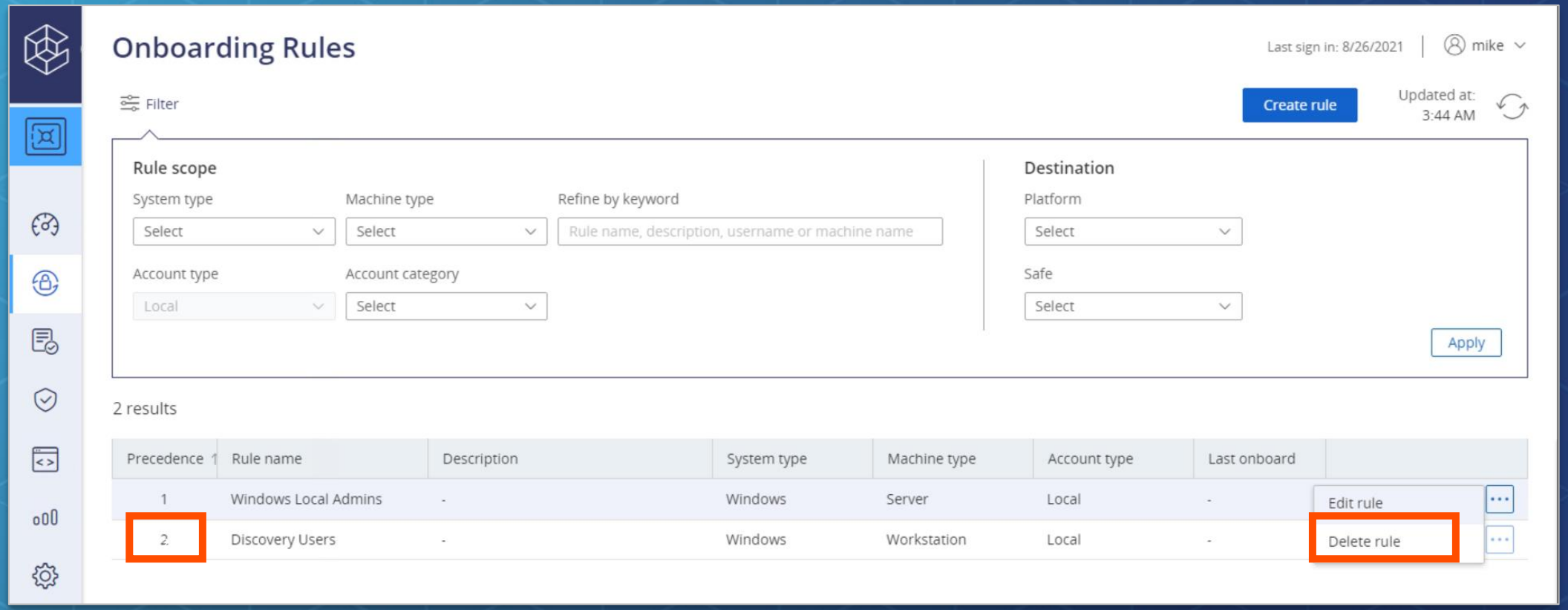
Activate Wi
Go to Settings t

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

New Rule on Rules List

The newly created rule appears in the list of **Onboarding Rules** and is assigned the highest precedence

- You can edit or delete existing rules
- You can configure the **Precedence** (priority) of any rule



Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Automatic Onboarding Rules - Notes

Onboarding Rules apply to both ***Accounts Discovery*** and using the Add discovered accounts feature of the REST API

Discovered accounts are automatically processed by the onboarding rules and provisioned in the Vault

Accounts that cannot be processed by any of the rules are added to the ***Pending Accounts*** list and can be reviewed and onboarded manually

Automatic Onboarding Rules only apply to accounts without dependencies.

A new rule takes precedence over an existing rule

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Summary

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

Summary

In this session we covered:

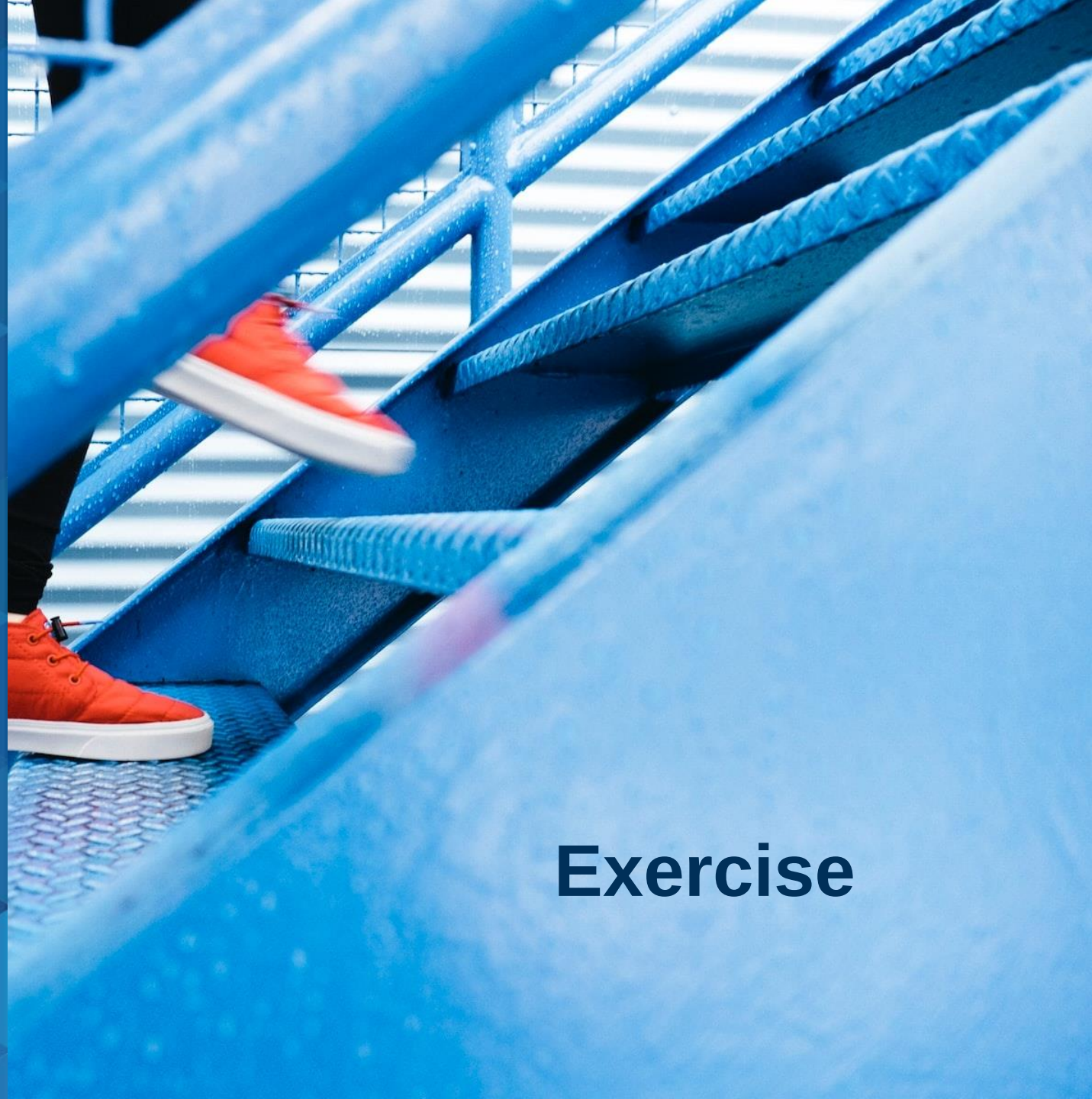
- The main methods for discovering and onboarding accounts to the system
- How to configure and run **Accounts Discovery**
- Configuring **Automatic Onboarding Rules**

Copyright © 2021 CyberArk Software Ltd. All rights reserved.

You may now complete the following exercise:

Discovery and Onboarding

- Accounts Feed
  - Configure Automatic Onboarding Rules
  - Configure and Run Windows Accounts Discovery
  - Manually onboard discovered accounts



Exercise

Copyright © 2021 CyberArk Software Ltd. All rights reserved.