CYBERARK®
The Identity Security Company™

PAM Administration

Policies & Platforms

Agenda

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

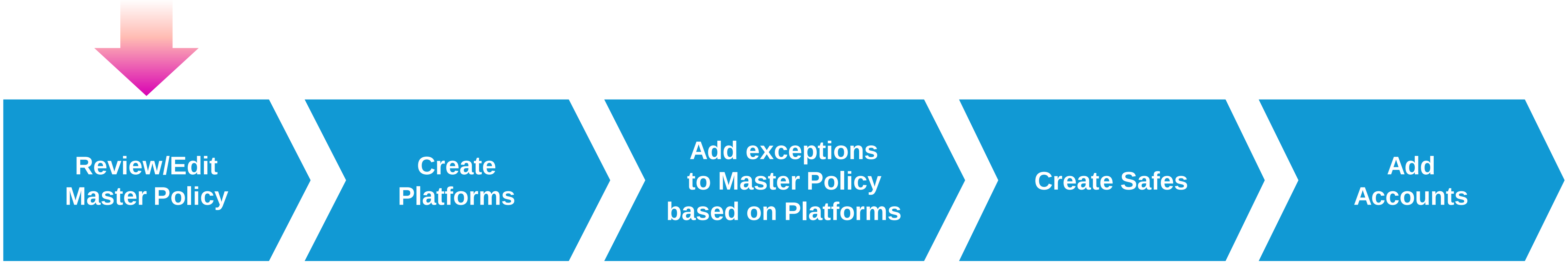
1. Describe the general workflow when working with **CyberArk PAM**

2. Configure key parameters in the **Master Policy**

3. Create and manage **Platforms**

Overview

Policies, Platforms, Safes, and Accounts



Review/Edit Master Policy

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

Create Platforms

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

Add exceptions to Master Policy based on Platforms

- Exceptions to Master Policy rules

Create Safes

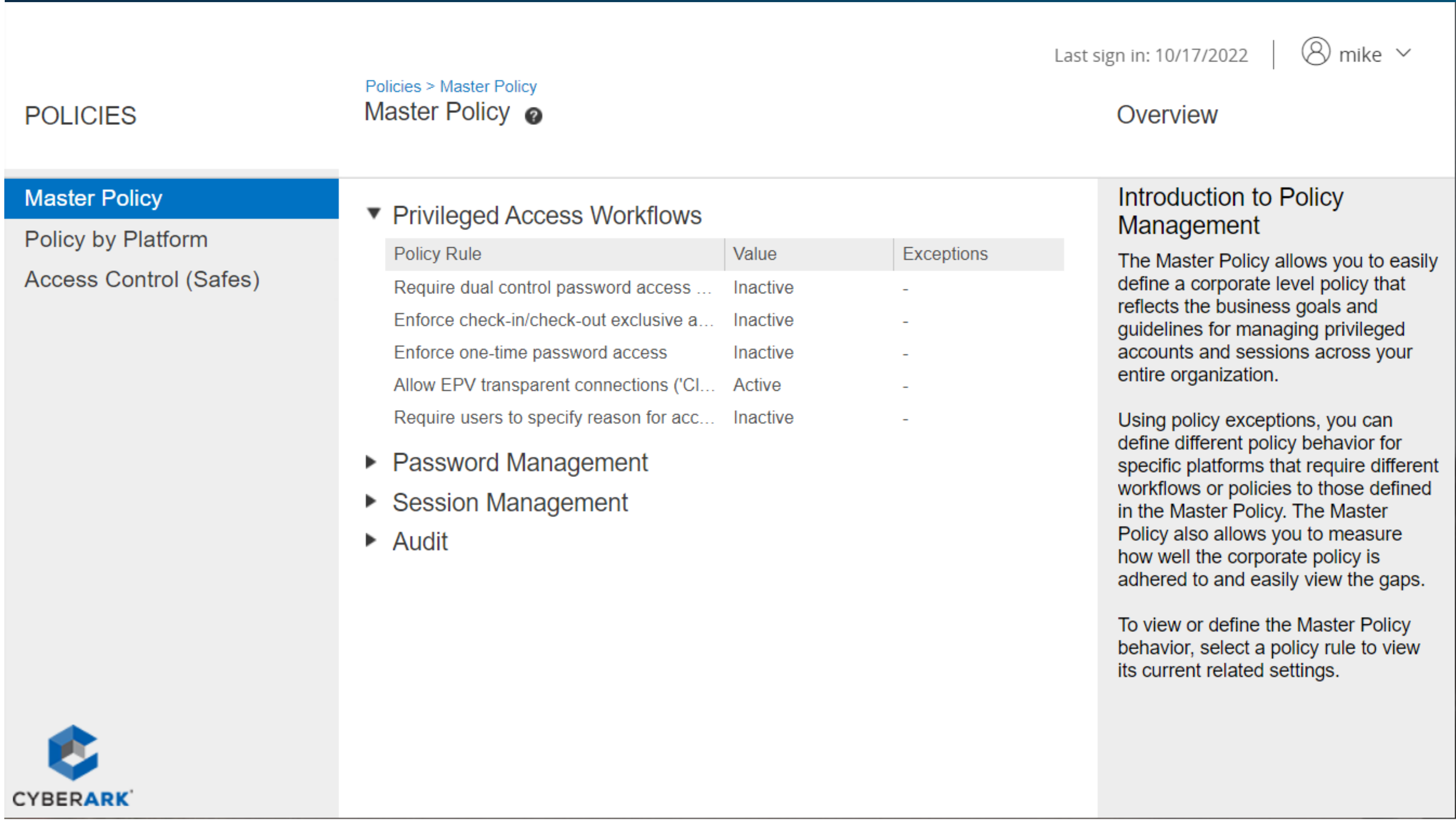
- Access control

Add Accounts

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

The Master Policy

- The **Master Policy** enables an organization to define a baseline for managing accounts in the organization.
- It is used for managing the Global policy settings.
- Exceptions to the **Master Policy** rules allow sets of accounts to vary from the Policy rule.



▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access ...	Inactive	-
Enforce check-in/check-out exclusive a...	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Cl...	Active	-
Require users to specify reason for acc...	Inactive	-

▶ Password Management

▶ Session Management

▶ Audit

Introduction to Policy Management

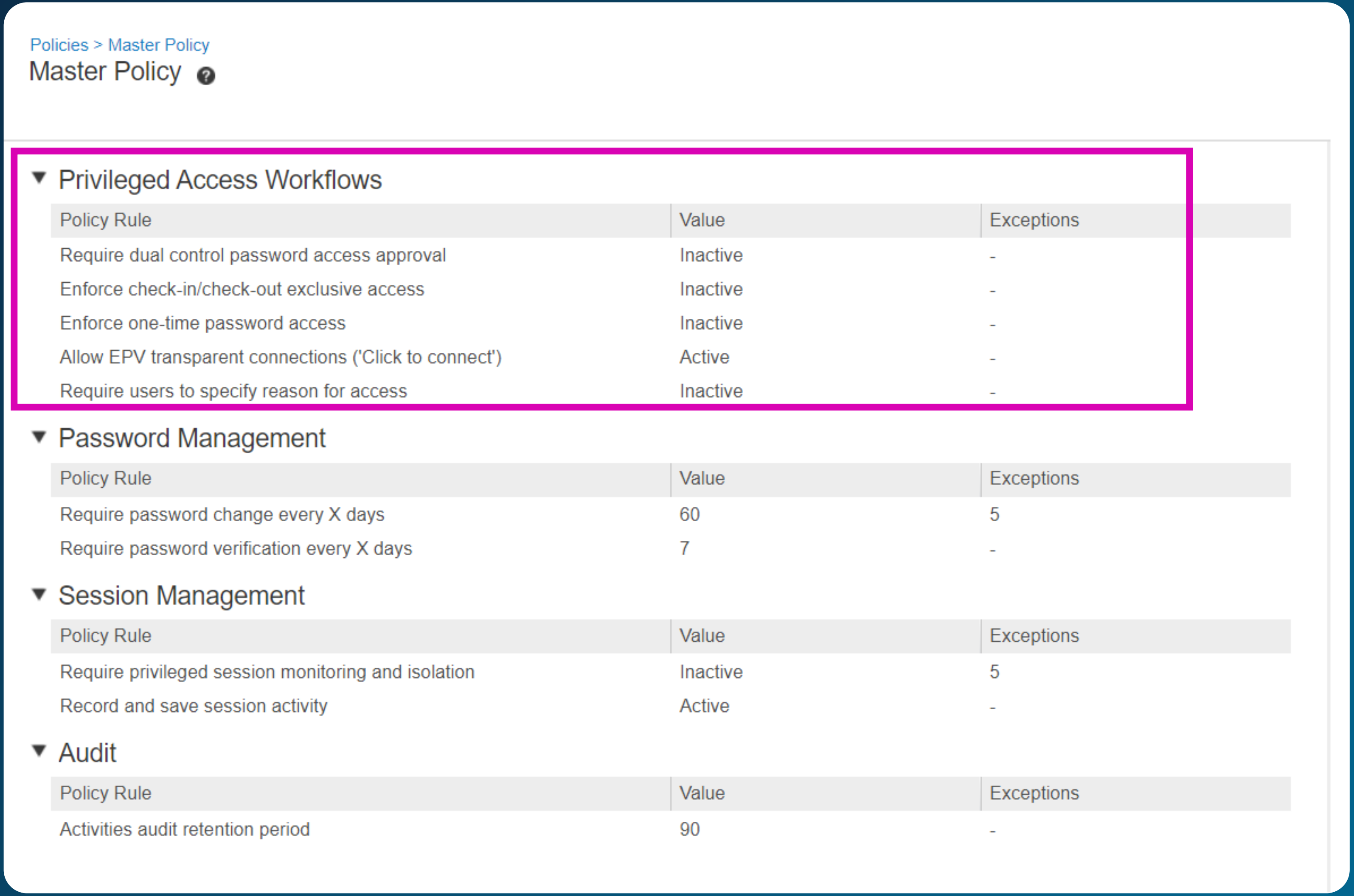
The Master Policy allows you to easily define a corporate level policy that reflects the business goals and guidelines for managing privileged accounts and sessions across your entire organization.

Using policy exceptions, you can define different policy behavior for specific platforms that require different workflows or policies to those defined in the Master Policy. The Master Policy also allows you to measure how well the corporate policy is adhered to and easily view the gaps.

To view or define the Master Policy behavior, select a policy rule to view its current related settings.

Master Policy: Global Policy

- Dual control
- Exclusive access
- One-time passwords
- Allow transparent connections
- Require reason for access



Policies > Master Policy

Master Policy

Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

Session Management

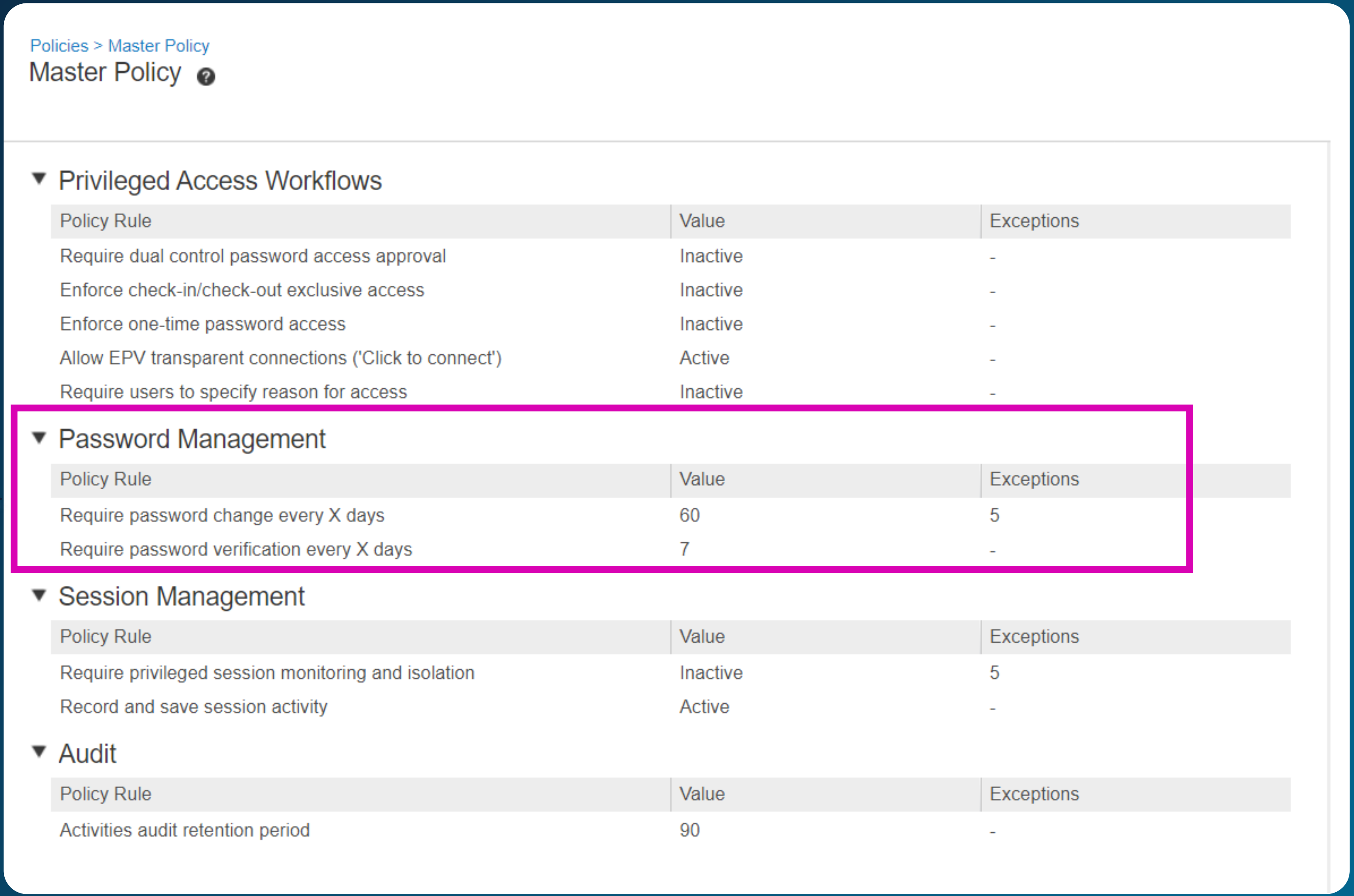
Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	5
Record and save session activity	Active	-

Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Master Policy: Global Policy

Set the global password change and verification requirements



Policies > Master Policy

Master Policy

Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

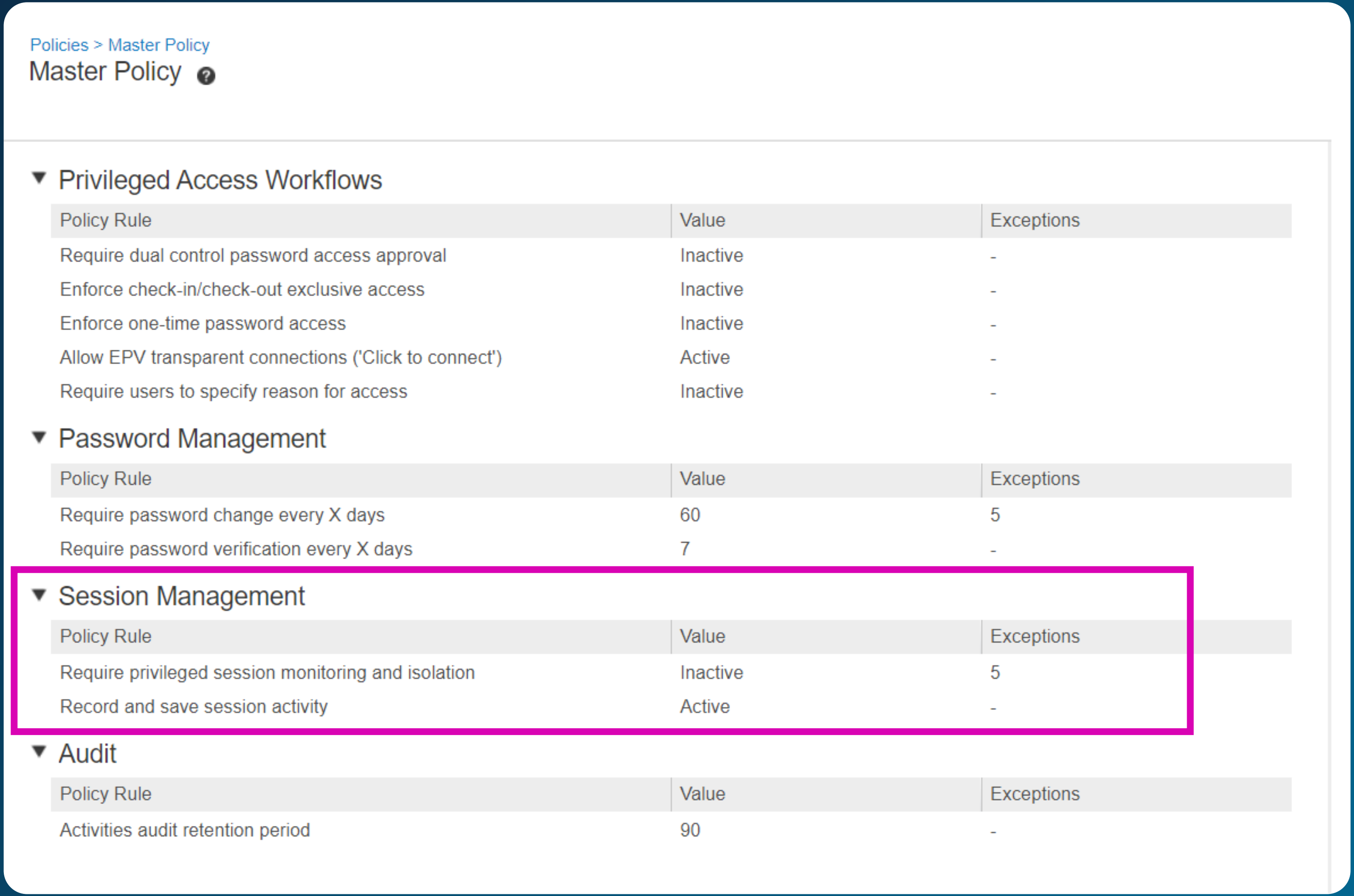
Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	5
Record and save session activity	Active	-

Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Master Policy: Global Policy



Policies > Master Policy

Master Policy

▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

▼ Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

▼ Session Management

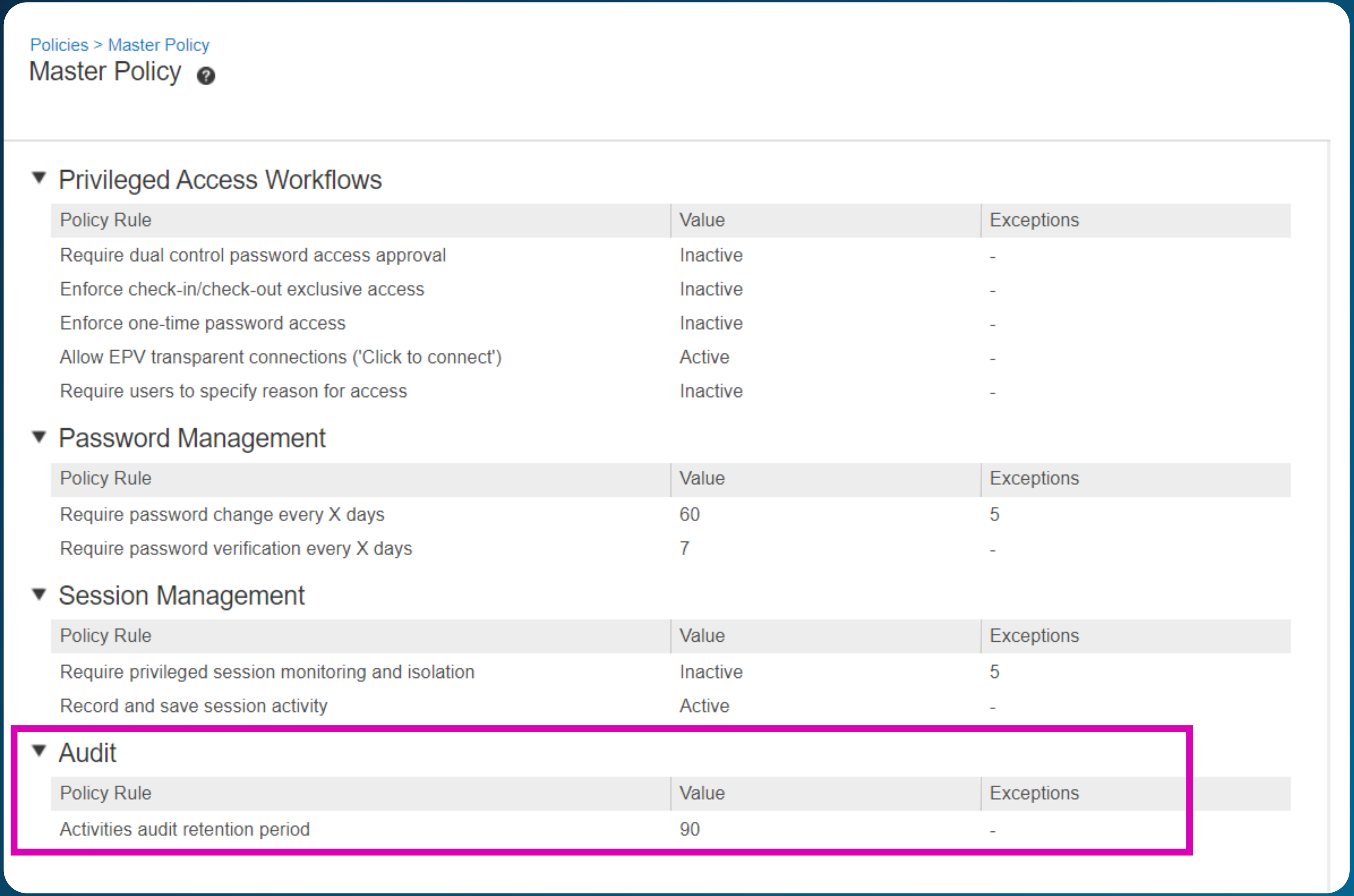
Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	5
Record and save session activity	Active	-

▼ Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Activate Privileged Session Management and its recordings

Master Policy: Global Policy



Policies > Master Policy

Master Policy

Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

Session Management

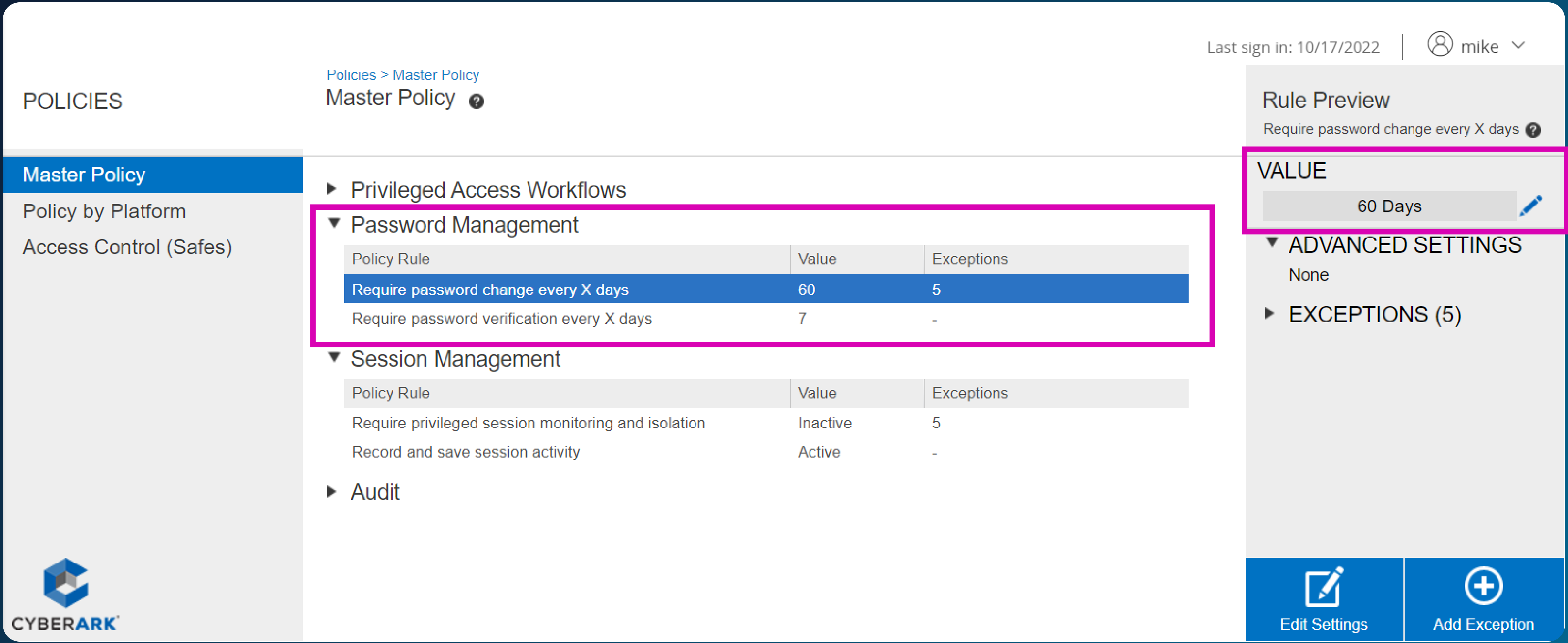
Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	5
Record and save session activity	Active	-

Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Set the retention policies for Vault audit data

Master Policy: Password Management



Policies > Master Policy

Master Policy

▸ Privileged Access Workflows

▾ Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

▾ Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Inactive	5
Record and save session activity	Active	-

▸ Audit

Rule Preview

Require password change every X days

VALUE

60 Days

▾ ADVANCED SETTINGS

None

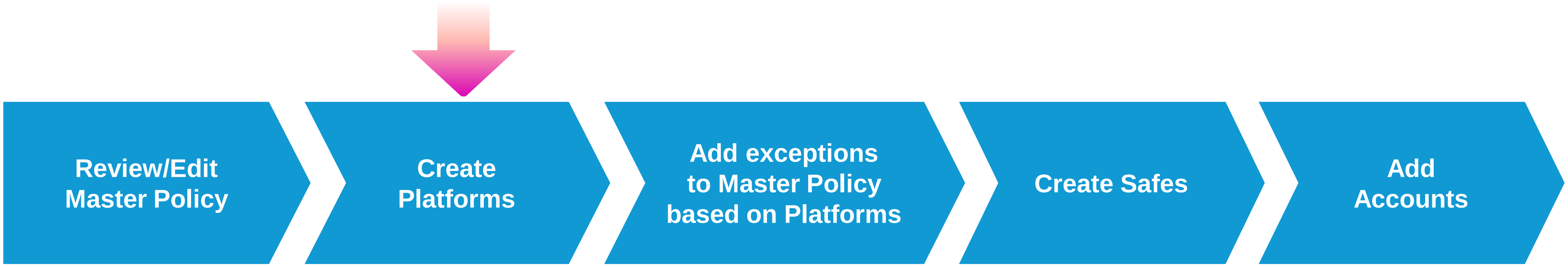
▸ EXCEPTIONS (5)

Platforms

In this section we will discuss Platforms:

- What they are
- How to create them
- How to manage them

Policies, Platforms, Safes, and Accounts



Review/Edit Master Policy

Create Platforms

Add exceptions to Master Policy based on Platforms

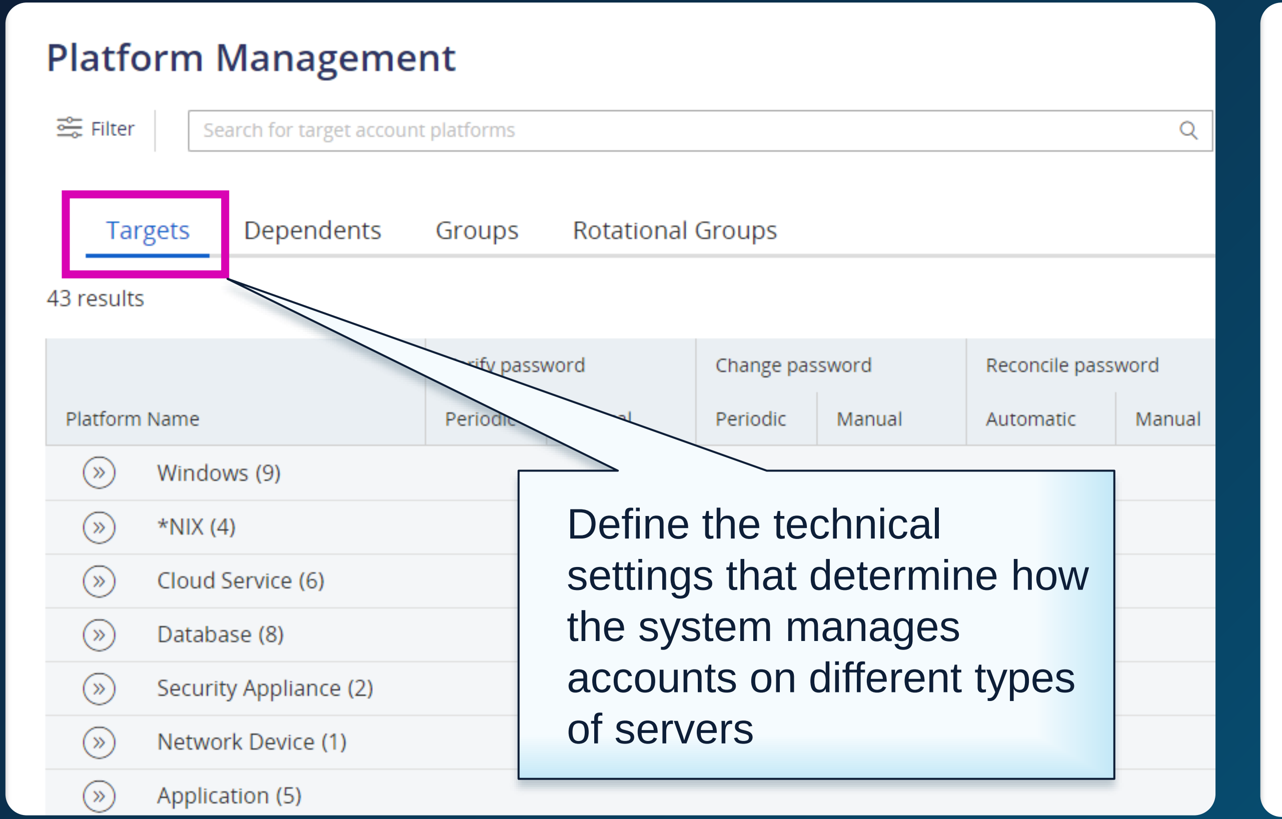
Create Safes

Add Accounts

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

Platform Types

There are two types of platforms:

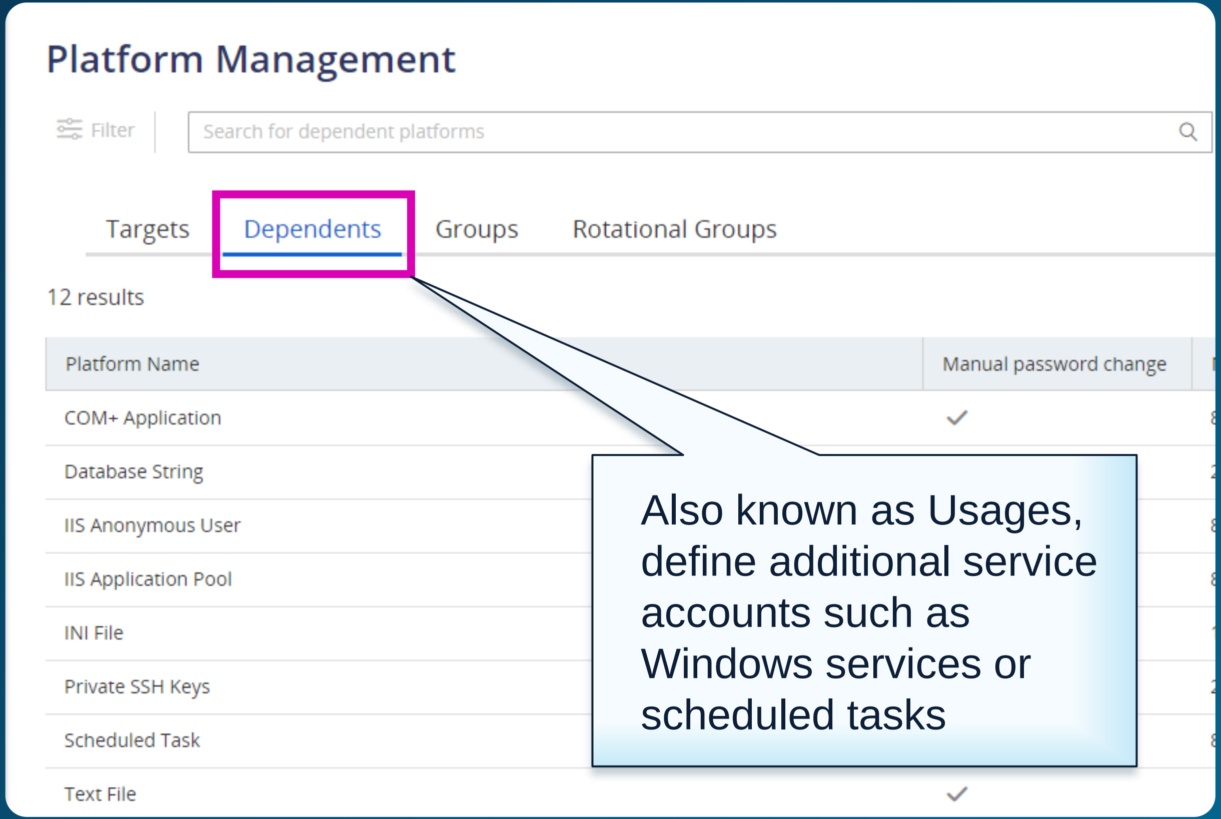


Platform Management

43 results

	…ify password		Change password		Reconcile password	
Platform Name	Periodi…	…l	Periodic	Manual	Automatic	Manual
Windows (9)						
*NIX (4)						
Cloud Service (6)						
Database (8)						
Security Appliance (2)						
Network Device (1)						
Application (5)						

Define the technical settings that determine how the system manages accounts on different types of servers



Platform Management

12 results

Platform Name	Manual password change
COM+ Application	✓
Database String	
IIS Anonymous User	
IIS Application Pool	
INI File	
Private SSH Keys	
Scheduled Task	
Text File	✓

Also known as Usages, define additional service accounts such as Windows services or scheduled tasks

What Are Platforms Used For?

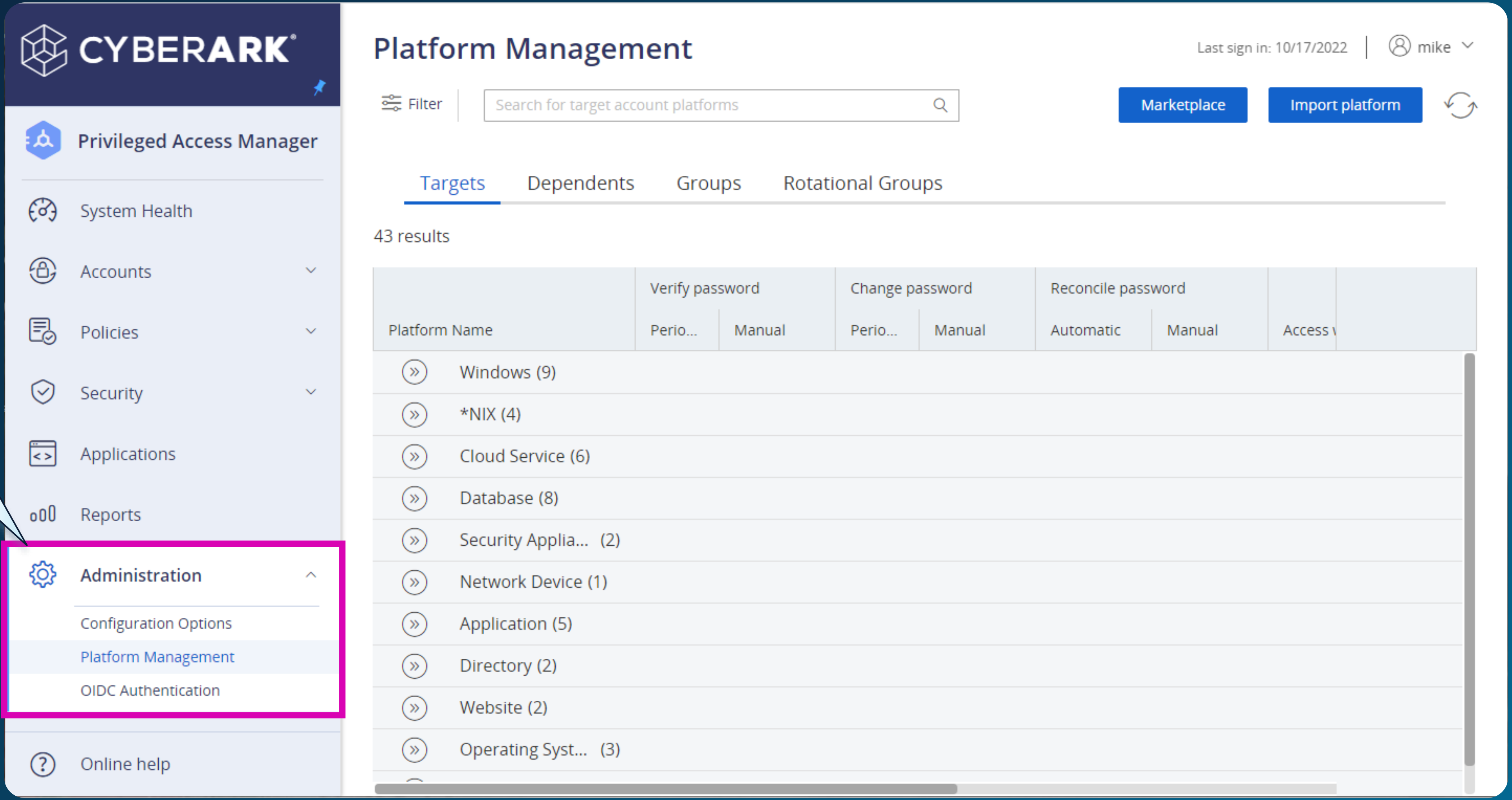
Platforms have three main functions:

Define the technical settings required to manage passwords	Password policy settings such as minimum length, forbidden characters, and so on.
Point to the relevant plug-ins and connection components	How you log in and change a password on a Unix server is very different than how you do the same thing on a Windows server. Different plug-ins must be used for different target systems.
The basis for exceptions to the Master Policy	Exceptions can be made to the Master Policy

Creating and Managing Platforms

Platform Management

Platforms are located under the **Administration** tab.



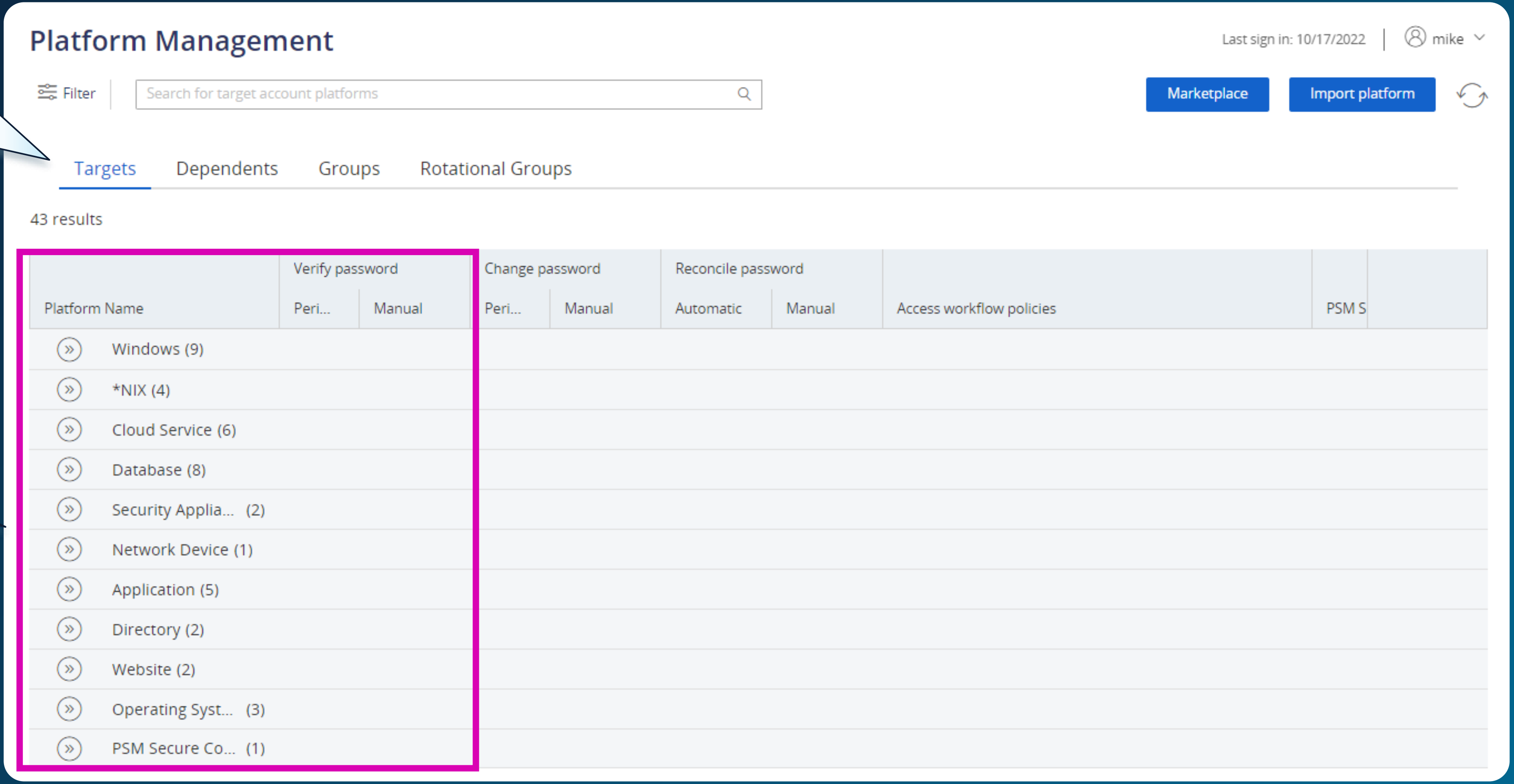
43 results

Platform Name	Verify password		Change password		Reconcile password		Access \
	Perio...	Manual	Perio...	Manual	Automatic	Manual	
Windows (9)							
*NIX (4)							
Cloud Service (6)							
Database (8)							
Security Applia... (2)							
Network Device (1)							
Application (5)							
Directory (2)							
Website (2)							
Operating Syst... (3)							

Platform Management

The platforms are grouped by target system type.

There are several dozen baseline platforms that function out of the box with little or no configuration.



Platform Management

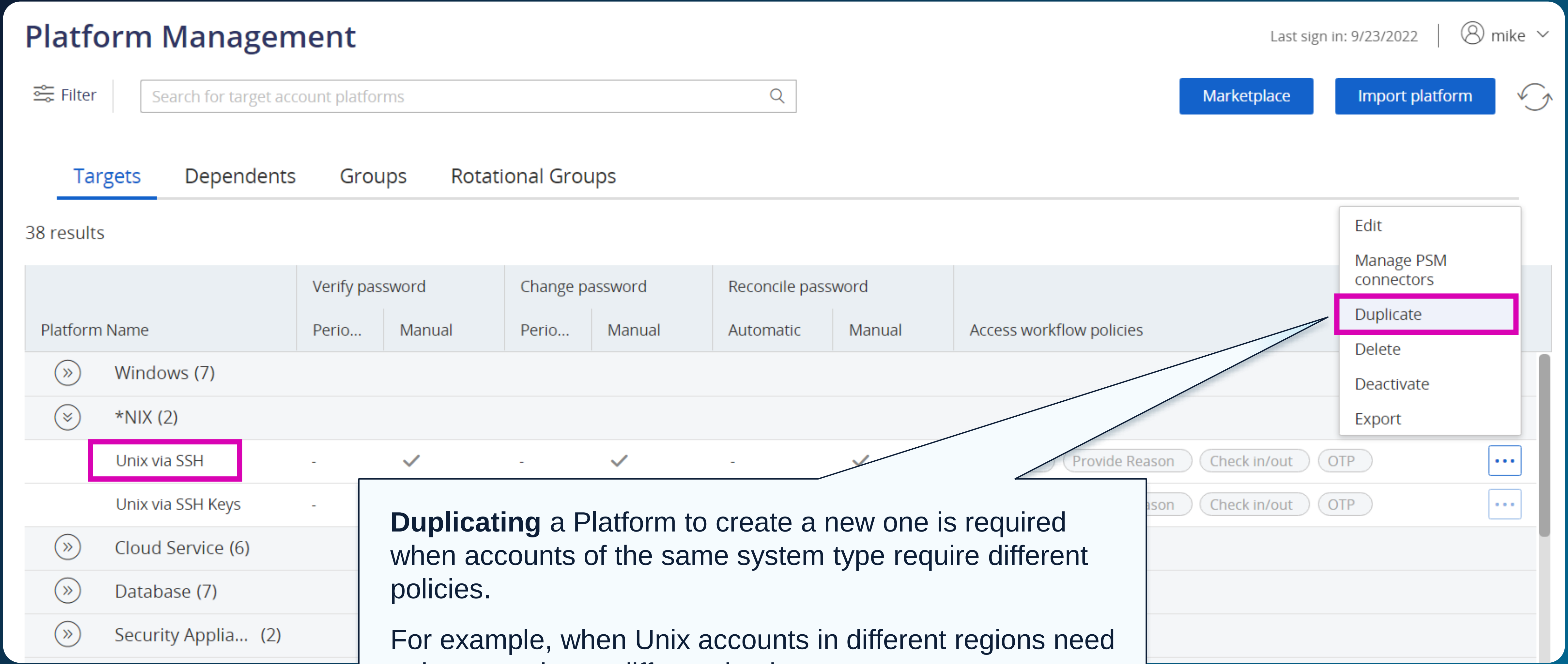
Last sign in: 10/17/2022 | mike

Targets | Dependents | Groups | Rotational Groups

43 results

	Verify password		Change password		Reconcile password			
Platform Name	Peri...	Manual	Peri...	Manual	Automatic	Manual	Access workflow policies	PSM S
» Windows (9)								
» *NIX (4)								
» Cloud Service (6)								
» Database (8)								
» Security Applia... (2)								
» Network Device (1)								
» Application (5)								
» Directory (2)								
» Website (2)								
» Operating Syst... (3)								
» PSM Secure Co... (1)								

Duplicating Platforms



Platform Management

Last sign in: 9/23/2022 | mike

38 results

Platform Name	Verify password Perio...	Manual	Change password Perio...	Manual	Reconcile password Automatic	Manual	Access workflow policies	
Windows (7)								
*NIX (2)								
Unix via SSH	-	✓	-	✓	-	✓	Provide Reason Check in/out OTP	•••
Unix via SSH Keys	-						ason Check in/out OTP	•••
Cloud Service (6)								
Database (7)								
Security Applia... (2)								

Duplicating a Platform to create a new one is required when accounts of the same system type require different policies.

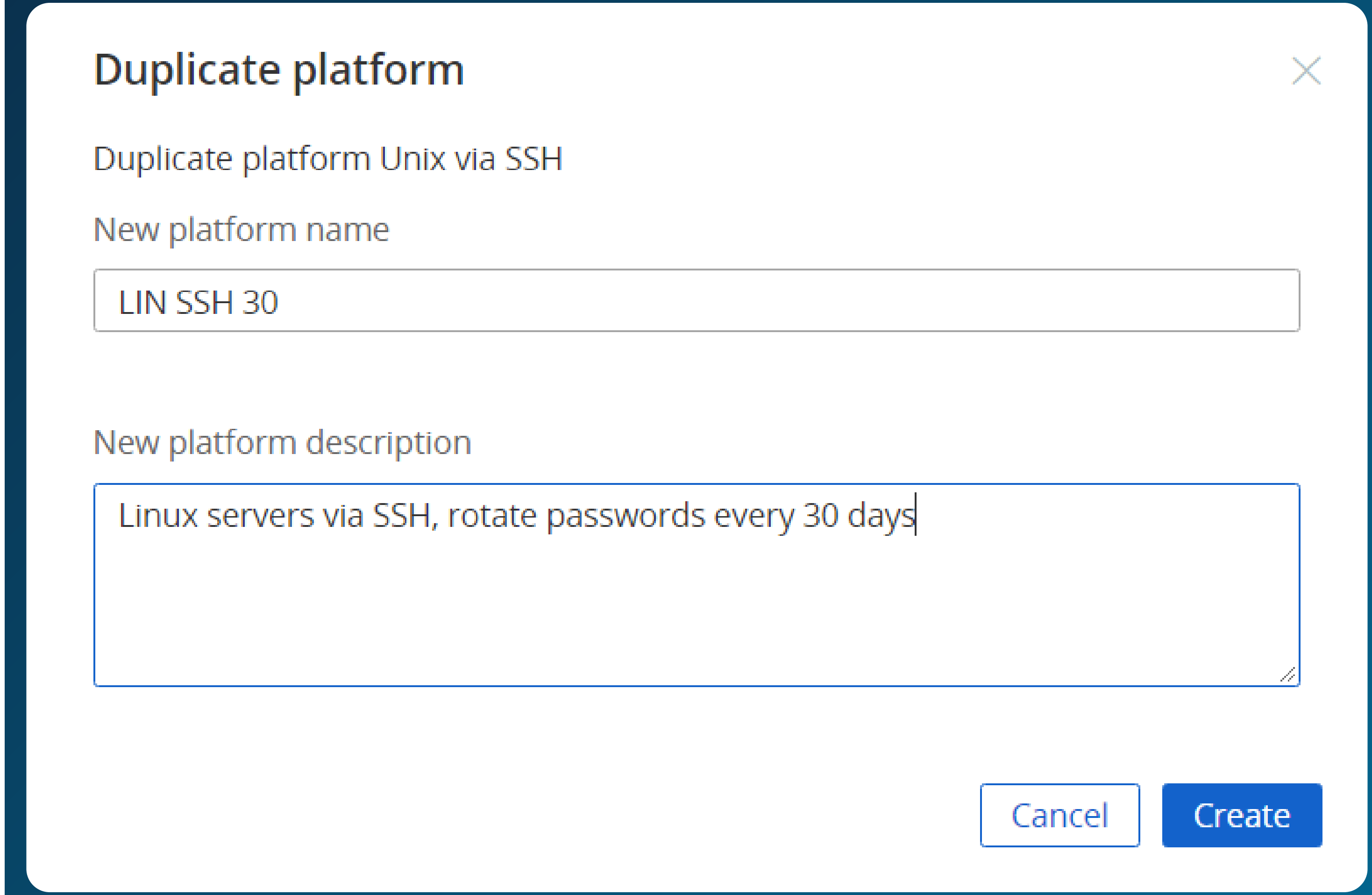
For example, when Unix accounts in different regions need to be rotated on a different basis.

Duplicating Platforms:
Platform Name

Use a logical naming convention based upon business rules

- *For example,* ***LIN SSH 30*** indicates this platform will be used to manage Linux accounts via SSH connections and that the passwords will be rotated every 30 days.

The Platform Name must be unique



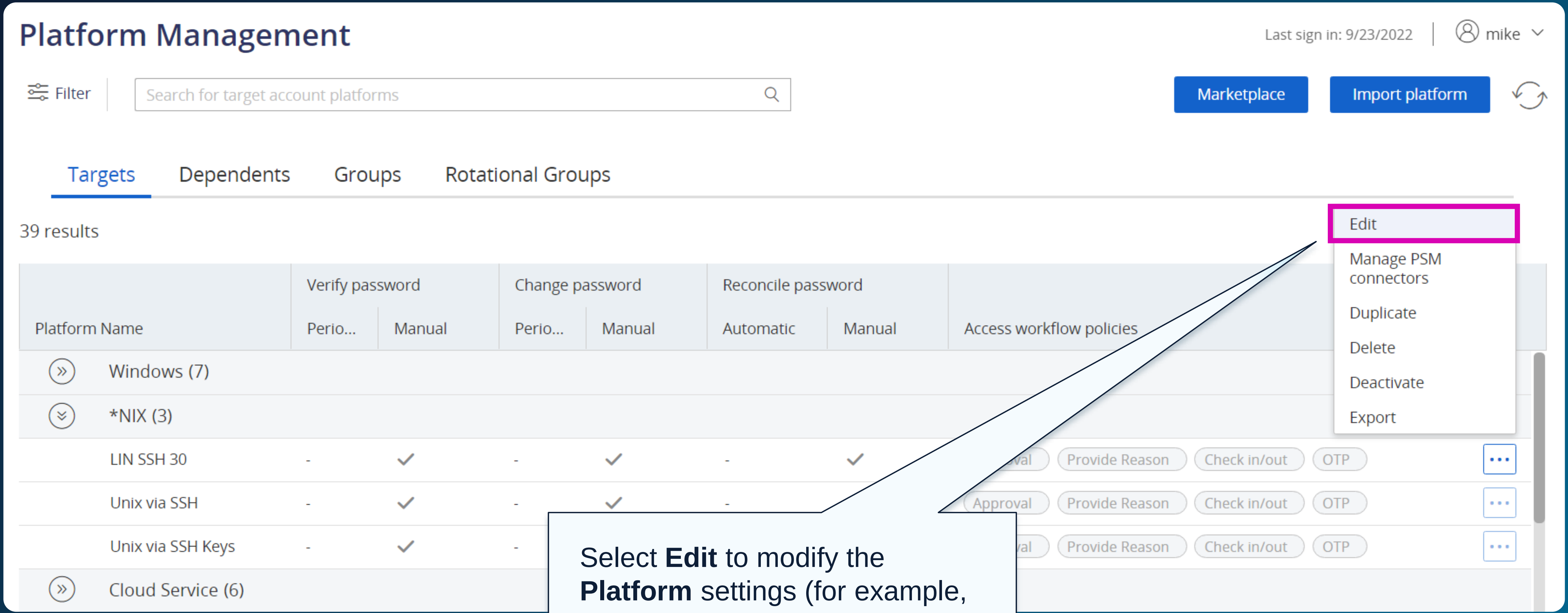
Duplicate platform

Duplicate platform Unix via SSH

New platform name: LIN SSH 30

New platform description: Linux servers via SSH, rotate passwords every 30 days

Edit Platform



Platform Management

Last sign in: 9/23/2022 | mike

39 results

Platform Name	Verify password Perio...	 Manual	Change password Perio...	 Manual	Reconcile password Automatic	 Manual	Access workflow policies	
Windows (7)								
*NIX (3)								
LIN SSH 30	-	✓	-	✓	-	✓	...val Provide Reason Check in/out OTP	⋯
Unix via SSH	-	✓	-	✓	-		Approval Provide Reason Check in/out OTP	⋯
Unix via SSH Keys	-	✓	-				...val Provide Reason Check in/out OTP	⋯
Cloud Service (6)								

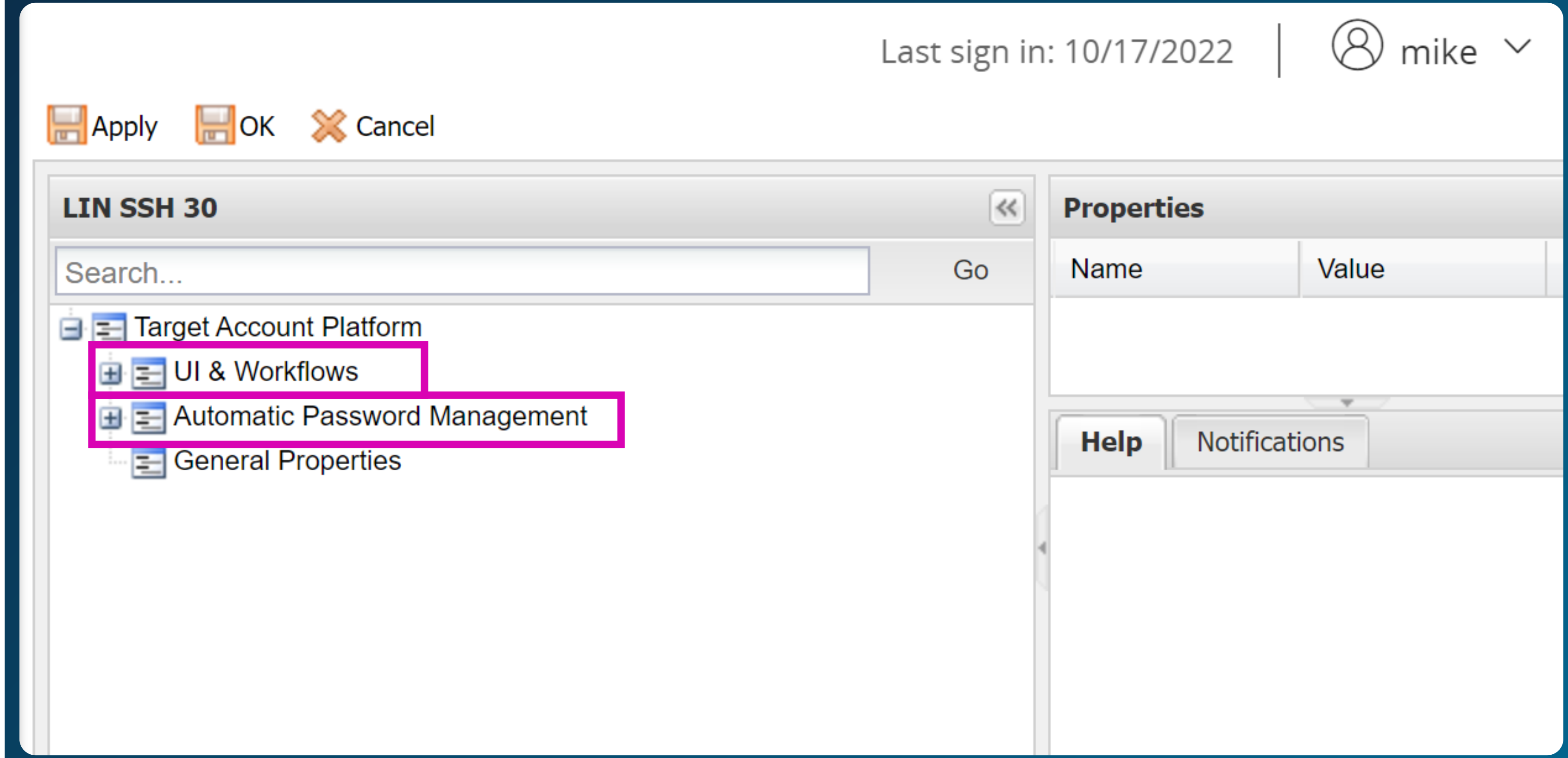
Select **Edit** to modify the **Platform** settings (for example, password policy settings)

Edit Platform

Platforms are divided into 2 broad sections:

1. ***UI & Workflows***
2. ***Automatic Password Management***

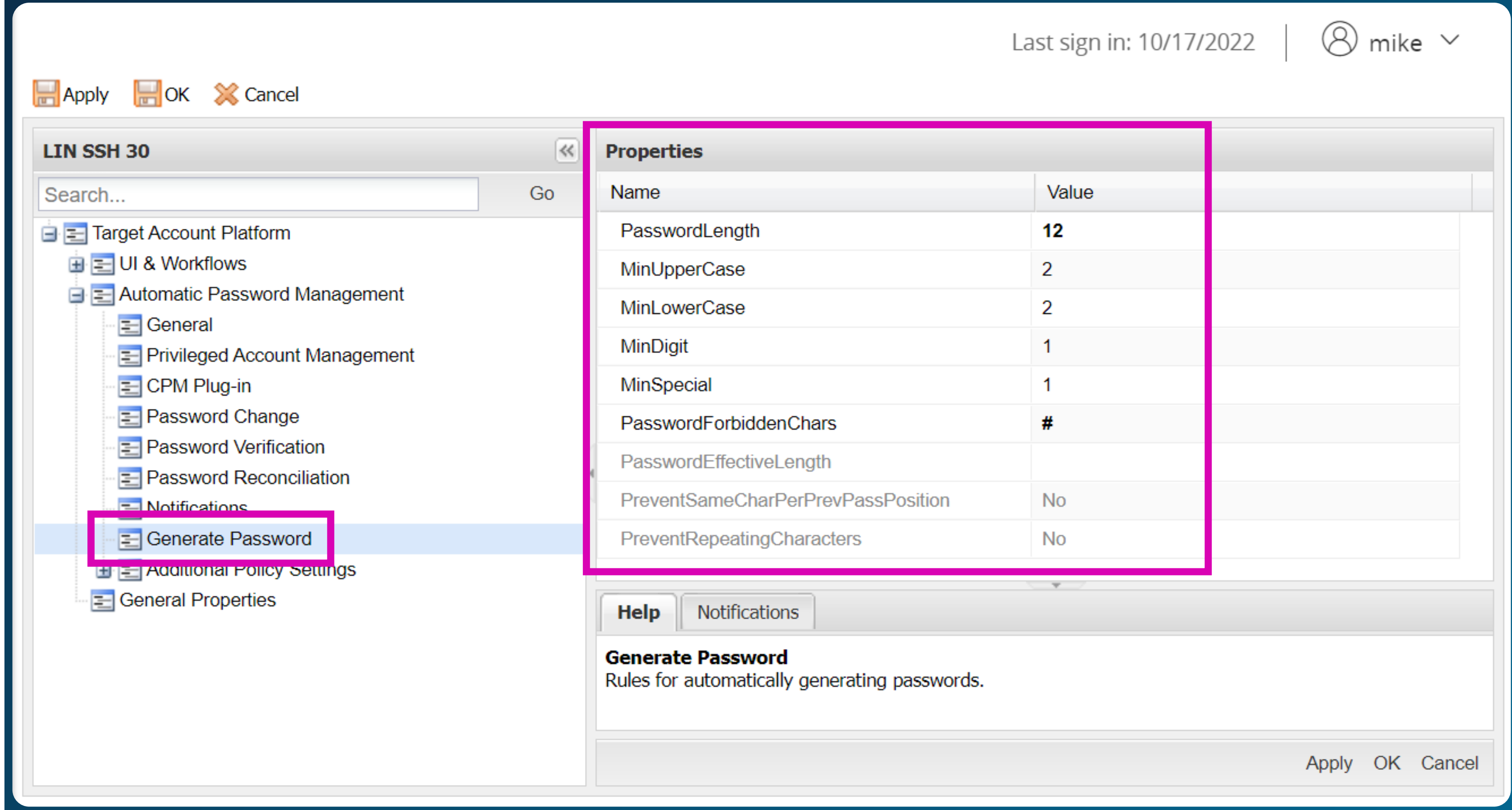
The settings for managing passwords can be found in the ***Automatic Password Management*** section.



Edit Platform: Password Complexity

The ***Generate Password*** section controls the password creation policy:

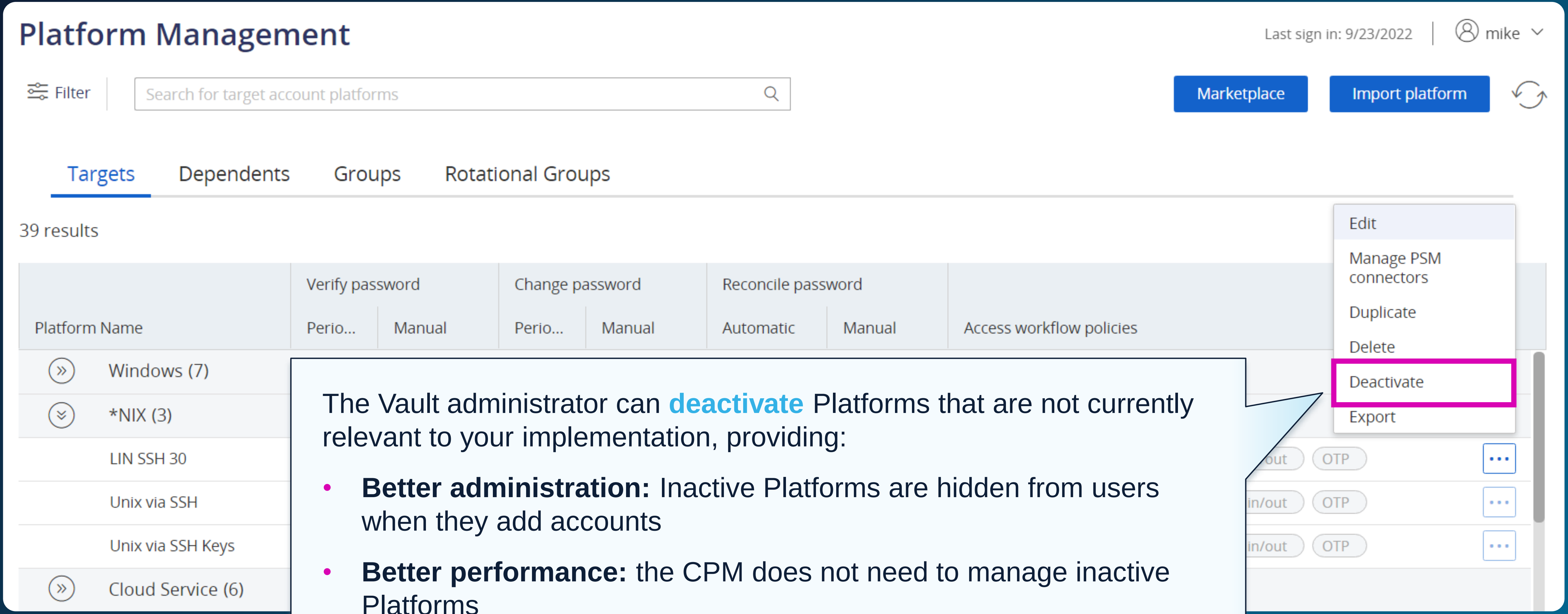
- Length
- Complexity
- Forbidden characters
- etc.



Name	Value
PasswordLength	**12**
MinUpperCase	2
MinLowerCase	2
MinDigit	1
MinSpecial	1
PasswordForbiddenChars	**#**
PasswordEffectiveLength	
PreventSameCharPerPrevPassPosition	No
PreventRepeatingCharacters	No

Generate Password
Rules for automatically generating passwords.

Activating/Deactivating Platforms



Platform Management

Last sign in: 9/23/2022 | mike

Filter | Search for target account platforms

Marketplace | Import platform

Targets | Dependents | Groups | Rotational Groups

39 results

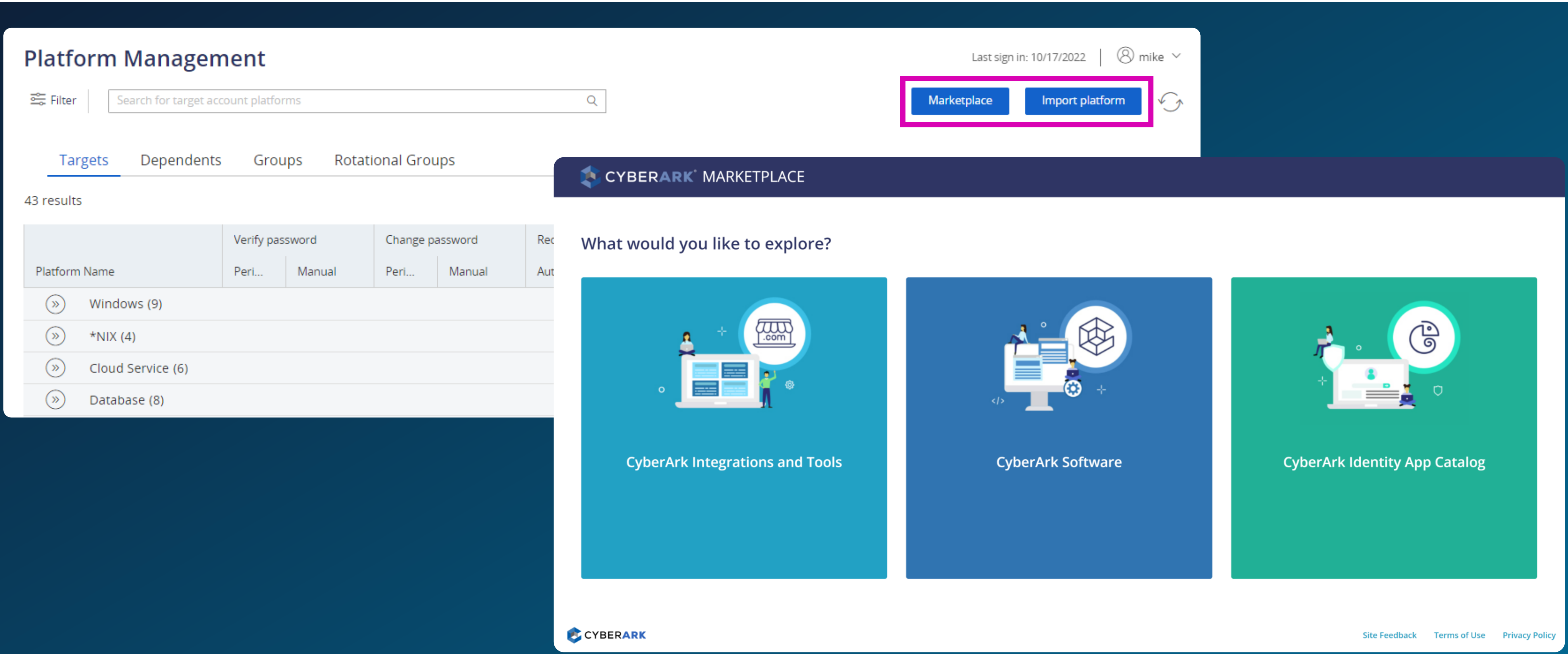
	Verify password		Change password		Reconcile password			
Platform Name	Perio...	Manual	Perio...	Manual	Automatic	Manual	Access workflow policies	
Windows (7)								
*NIX (3)								
LIN SSH 30							out OTP	•••
Unix via SSH							in/out OTP	•••
Unix via SSH Keys							in/out OTP	•••
Cloud Service (6)								

The Vault administrator can **deactivate** Platforms that are not currently relevant to your implementation, providing:

- **Better administration:** Inactive Platforms are hidden from users when they add accounts
- **Better performance:** the CPM does not need to manage inactive Platforms

Importing New Platforms

If you have a system that is not supported by one of the default **Platforms**, you can either create a new one or import one from the **CyberArk** Marketplace.



Platform Management

Last sign in: 10/17/2022 | mike

Filter | Search for target account platforms

Marketplace | Import platform

Targets | Dependents | Groups | Rotational Groups

43 results

	Verify password		Change password		Rec
Platform Name	Peri...	Manual	Peri...	Manual	Aut
» Windows (9)					
» *NIX (4)					
» Cloud Service (6)					
» Database (8)					

CYBERARK® MARKETPLACE

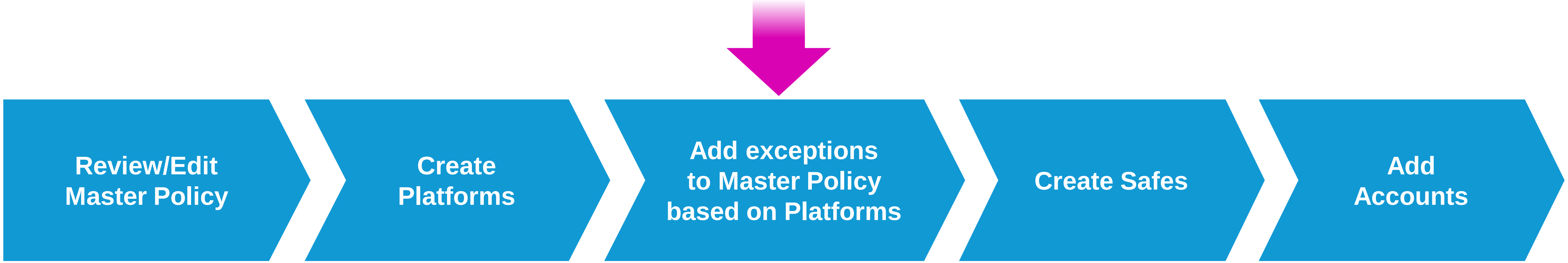
What would you like to explore?

- CyberArk Integrations and Tools
- CyberArk Software
- CyberArk Identity App Catalog

CYBERARK | Site Feedback | Terms of Use | Privacy Policy

Master Policy Exceptions

Policies, Platforms, Safes and Accounts



Review/Edit Master Policy

Create Platforms

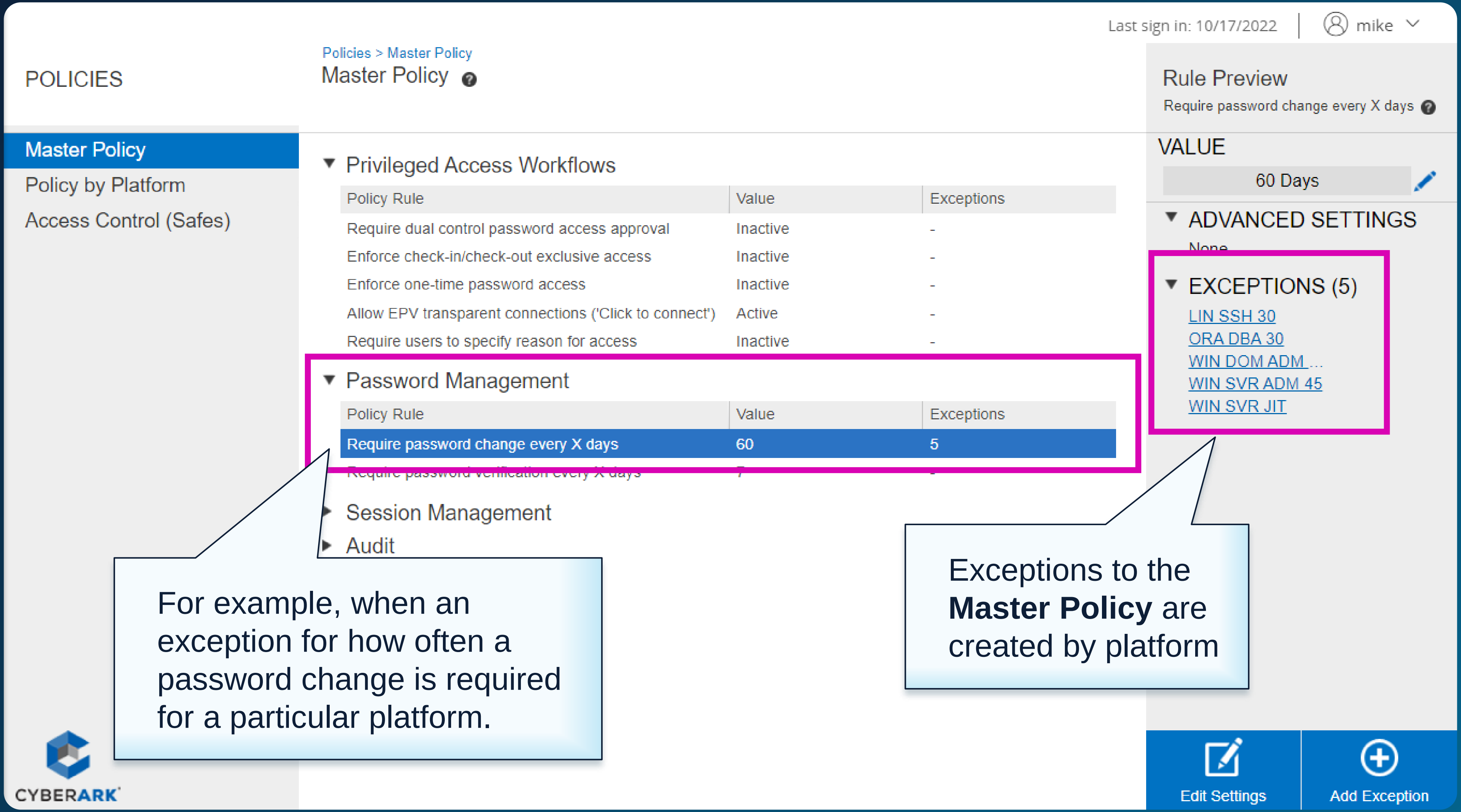
Add exceptions to Master Policy based on Platforms

Create Safes

Add Accounts

- Exceptions to Master Policy rules

Exceptions to the Master Policy



Last sign in: 10/17/2022 | mike

POLICIES

- Master Policy
- Policy by Platform
- Access Control (Safes)

Policies > Master Policy

Master Policy

▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Inactive	-

▼ Password Management

Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

▶ Session Management

▶ Audit

Rule Preview

Require password change every X days

VALUE

60 Days

▼ ADVANCED SETTINGS

None

▼ EXCEPTIONS (5)

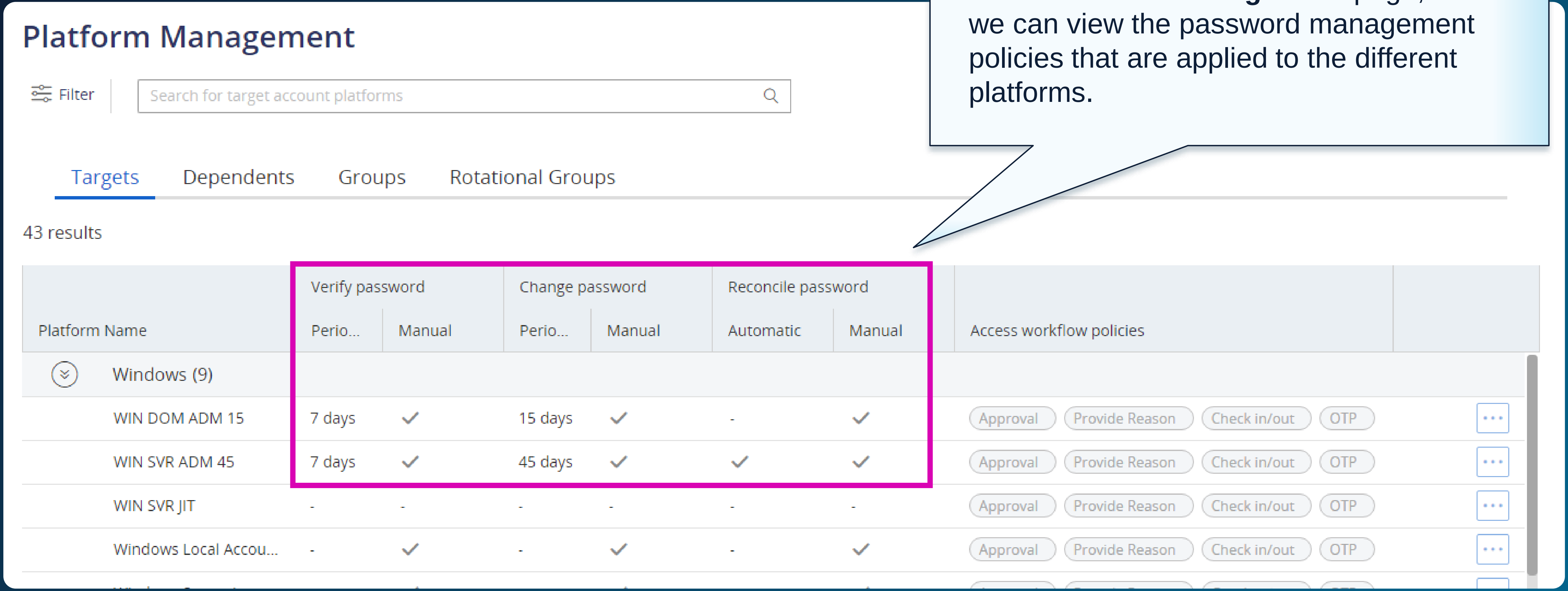
- LIN SSH 30
- ORA DBA 30
- WIN DOM ADM ...
- WIN SVR ADM 45
- WIN SVR JIT

For example, when an exception for how often a password change is required for a particular platform.

Exceptions to the **Master Policy** are created by platform

Policy By Platform

In the **Platform Management** page, we can view the password management policies that are applied to the different platforms.



Platform Management

Filter | Search for target account platforms

Targets | Dependents | Groups | Rotational Groups

43 results

	Verify password		Change password		Reconcile password		
Platform Name	Perio...	Manual	Perio...	Manual	Automatic	Manual	Access workflow policies
Windows (9)							
WIN DOM ADM 15	7 days	✓	15 days	✓	-	✓	Approval Provide Reason Check in/out OTP
WIN SVR ADM 45	7 days	✓	45 days	✓	✓	✓	Approval Provide Reason Check in/out OTP
WIN SVR JIT	-	-	-	-	-	-	Approval Provide Reason Check in/out OTP
Windows Local Accou...	-	✓	-	✓	-	✓	Approval Provide Reason Check in/out OTP

Summary

Summary

In this session we discussed:

- The general workflow when working with CyberArk PAM
- How to configure key parameters in the Master Policy
- How to configure key parameters in Platforms

Additional Resources

Customization

CyberArk Marketplace (login required)

You may now complete the following exercise:

Securing Windows Domain Accounts

- Platform Management
  - Duplicating a Platform
  - Configure Password Management
  - Editing the Master Policy