



# PAM Administration

Policies & Platforms



# Agenda

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

- Describe the CyberArk password management logic and flow
- Configure key parameters in the Master Policy
- Create and manage Platforms



# Overview



# Policies, Platforms, Safes and Accounts



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

- Technical settings for managing passwords
- Basis for exceptions

- Exceptions to Master Policy rules

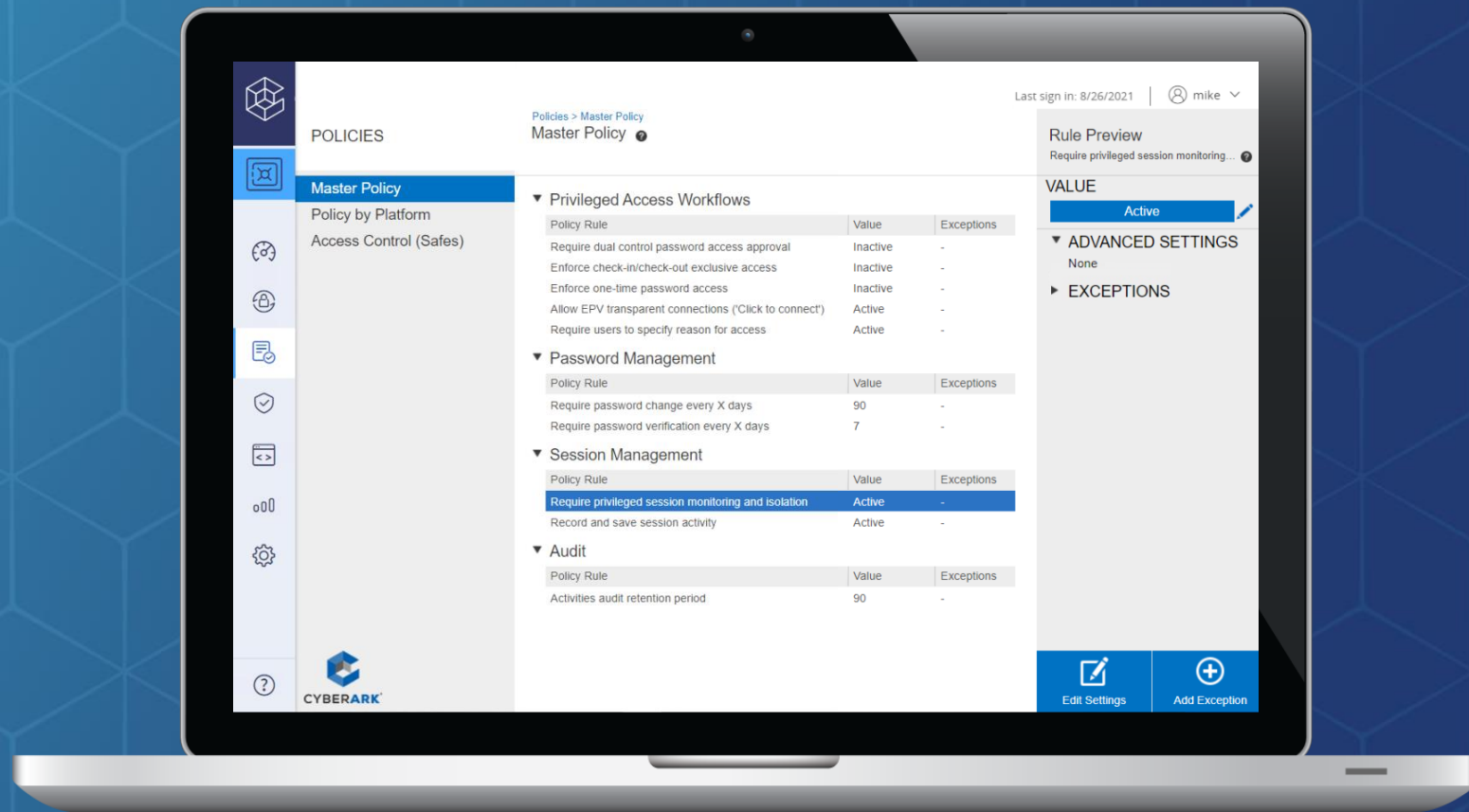
- Access control

- 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 allows sets of accounts to vary from the Policy Rule.



# Master Policy: Global Policy

- Dual control
- Exclusive access
- One-time passwords
- Set the global password change and verification
- Activate Privileged Session
- Set the retention policies for Vault audit data

POLICIES

Policies > Master Policy  
Master Policy

Last sign in: 8/26/2021 | mike

**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	Active	-

**Password Management**

Policy Rule	Value	Exceptions
Require password change every X days	90	-
Require password verification every X days	7	-

**Session Management**

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

**Audit**

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

**Rule Preview**  
Require privileged session monitoring...

**VALUE**  
Active

**ADVANCED SETTINGS**  
None

**EXCEPTIONS**

**EDIT SETTINGS** **ADD EXCEPTION**

# Master Policy: Password Management

The screenshot shows the CyberArk Master Policy configuration page. The left sidebar contains navigation icons for Policies, Master Policy, Policy by Platform, Access Control (Safes), and other settings. The main content area is titled 'Policies > Master Policy' and 'Master Policy'. It features three expandable sections: Privileged Access Workflows, Password Management, and Session Management. The Password Management section is expanded, showing a table of policy rules. The 'Require privileged session monitoring and isolation' rule is highlighted with a red box. The right sidebar shows the 'Rule Preview' for the selected rule, indicating it is 'Active' and has 'None' for advanced settings and exceptions. At the bottom right, there are buttons for 'Edit Settings' and 'Add Exception'.

**POLICIES**

Policies > Master Policy  
Master Policy

**Master Policy**

Policy by Platform  
Access Control (Safes)

**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	Active	-

**Password Management**

Policy Rule	Value	Exceptions
Require password change every X days	90	-
Require password verification every X days	7	-

**Session Management**

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

**Audit**

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

**Rule Preview**  
Require privileged session monitoring...

**VALUE**  
Active

**ADVANCED SETTINGS**  
None

**EXCEPTIONS**

**Edit Settings** **Add Exception**

# Platforms

In this section we will discuss Platforms: what they are, how to create them, and how to manage them





# Policies, Platforms, Safes and Accounts



- Technical settings for managing passwords
- Basis for exceptions



# Platform Types

There are two types of platforms:

**Platform Management**

Filter | Search for target account platforms

**Targets** Dependents Groups Rotational Groups

42 results

Platform Name	Verify password		Change password	
	Periodic	Manual	Periodic	Manual
				✓
				✓
	45 days			✓

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

**Platform Management**

Filter | Search for dependent platforms

Targets **Dependents** Groups Rotational Groups

12 results

Platform Name	Manual password char
COM+ Application	✓
Database String	✓
IIS Anonymous User	✓
IIS Application Pool	✓

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: min length, required special characters, forbidden characters, etc.

*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

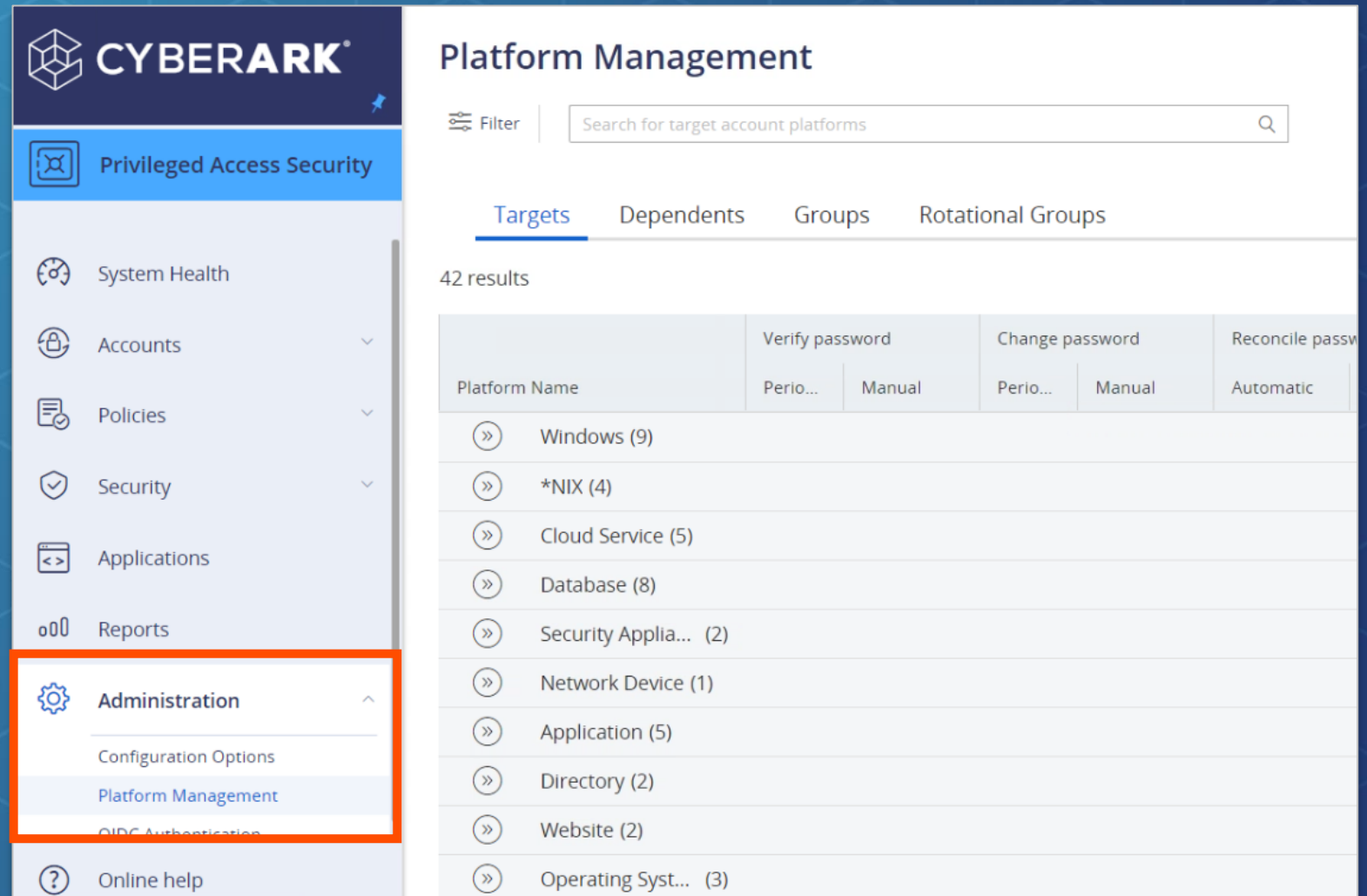


# Creating and Managing Platforms



# Platform Management

Platforms are located under **Administration**



**CYBERARK**

Privileged Access Security

- System Health
- Accounts
- Policies
- Security
- Applications
- Reports
- Administration**
  - Configuration Options
  - Platform Management
  - OIDC Authentication
- Online help

## Platform Management

Filter | Search for target account platforms

Targets | Dependents | Groups | Rotational Groups

42 results

Platform Name	Verify password		Change password		Reconcile passw
	Perio...	Manual	Perio...	Manual	Automatic
» Windows (9)					
» *NIX (4)					
» Cloud Service (5)					
» Database (8)					
» Security Appla... (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

The screenshot displays the 'Platform Management' dashboard. On the left is a sidebar with navigation icons. The main area has a 'Filter' search bar and tabs for 'Targets', 'Dependents', 'Groups', and 'Rotational Groups'. Below the tabs, it shows '42 results'. A table lists various platform categories, each with a '»' icon and a count in parentheses. The table is highlighted with an orange border.

Platform Name	Verify password	Change password	Reconcile password	Access workflow poli...	PSM Server
	Perio...	Manual	Perio...	Manual	
» Windows (9)					
» *NIX (4)					
» Cloud Service (5)					
» Database (8)					
» Security Appliance (2)					
» Network Device (1)					
» Application (5)					
» Directory (2)					
» Website (2)					
» Operating System (3)					
» PSM Secure Connect (1)					



# Duplicating Platforms

**Platform Management**

Last sign in: 8/25/2021 | mike

Filter | Search for target account platforms

Targets | Dependents | Groups | Rotational Groups

39 results

Platform Name	Verify password		Change password		Reconcile password		Access workflow policies	PSM Server
	Periodic	Manual	Periodic	Manual	Automatic	Manual		
Windows (8)								
*NIX (2)								
Unix via SSH	-	✓	-	✓	-	✓	Approval   Provide Reason   Check in/out   OTP	PSM Server on COMPO
<b>Unix via SSH Keys</b>	-	✓	-	✓	-	✓	Approval   Provide Reason   Check in/out   OTP	PSM Server on COMPO
Cloud Service (5)								
Database (8)								
Security Appliance (2)								
Network Device (1)								

**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.

Context menu options: Edit, Manage PSM connectors, **Duplicate**, Delete, Deactivate, Export



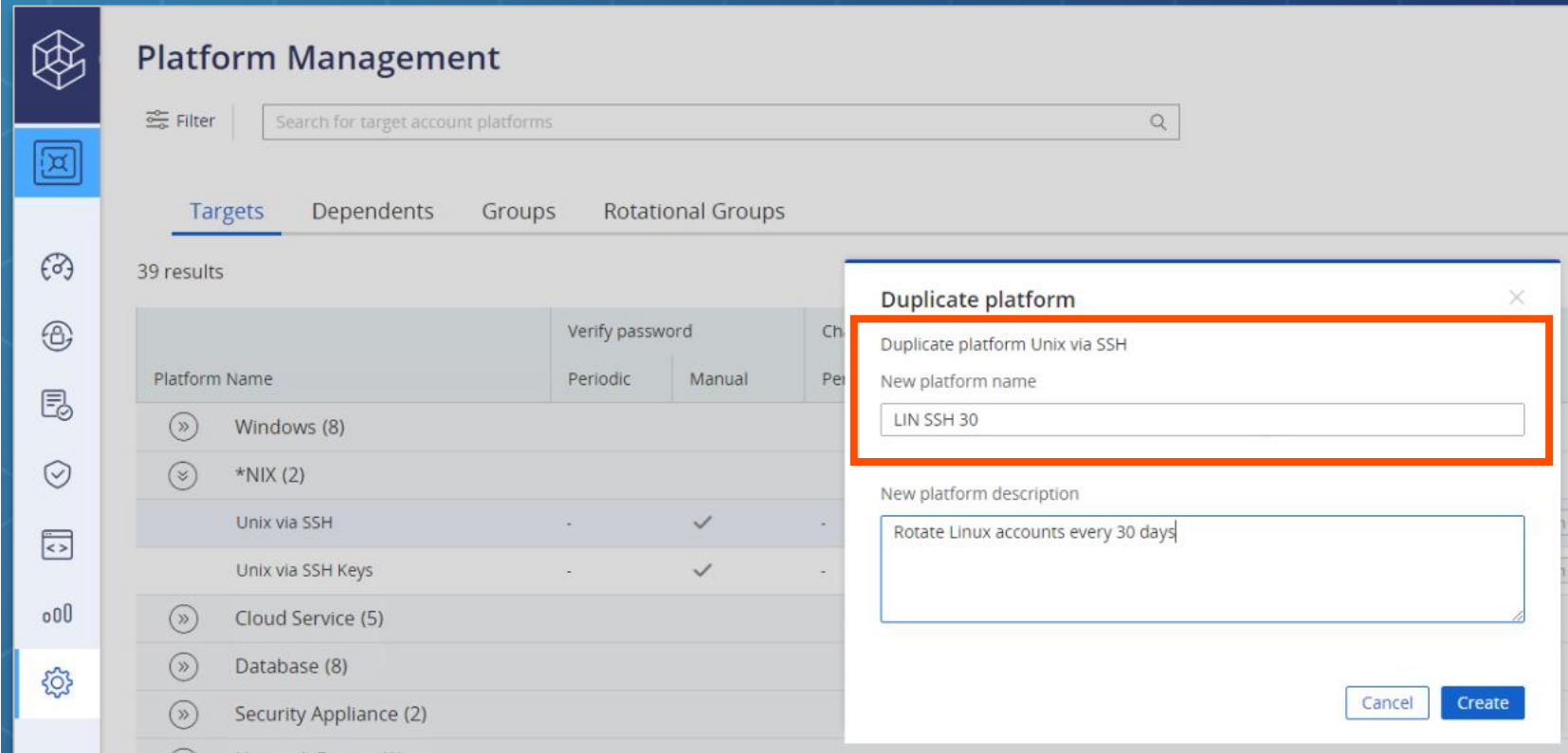


# Duplicating Platforms: Platform Name

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**





# Edit Platform

**Platform Management**

Last sign in: 8/25/2021 | mike

Filter | Search for target account platforms

Marketplace Import platform

Targets Dependents Groups Rotational Groups

40 results

Platform Name	Verify password		Change password		Reconcile password		Access workflow policies	PSM Server
	Periodic	Manual	Periodic	Manual	Automatic	Manual		
» Windows (8)								
» *NIX (3)								
LIN SSH 30	-	✓					Provide Reason Check in/out OTP PSM Server on COMPO	...
Unix via SSH	-	✓					Provide Reason Check in/out OTP PSM Server on COMPO	...
Unix via SSH Keys	-	✓					Provide Reason Check in/out OTP PSM Server on COMPO	...
» Cloud Service (5)								
» Database (8)								
» Security Appliance (2)								
» Network Device (1)								

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

Edit

Manage PSM connectors

Duplicate

Delete

Deactivate

Export

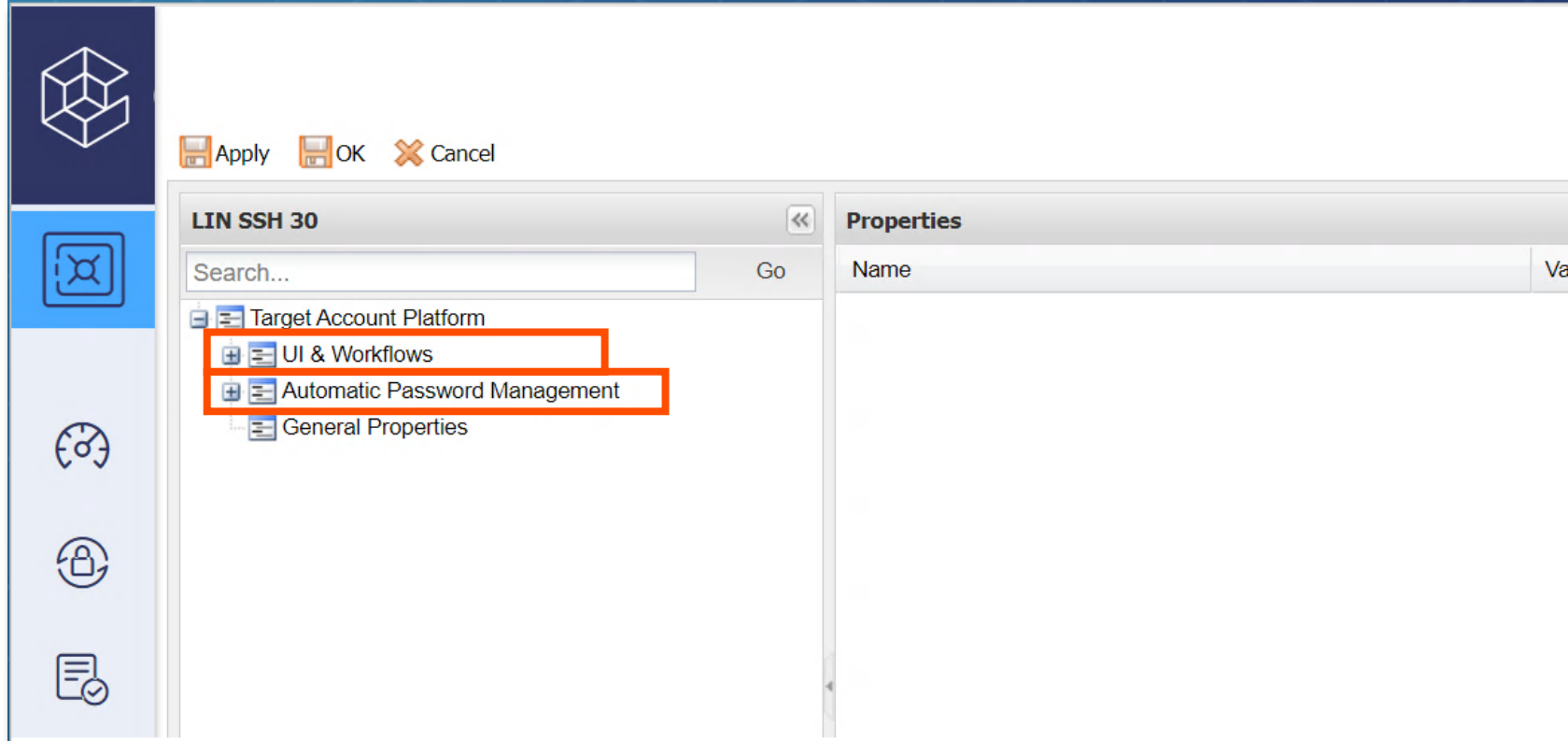


# Edit Platform

**Platforms** are divided into 2 broad sections:

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

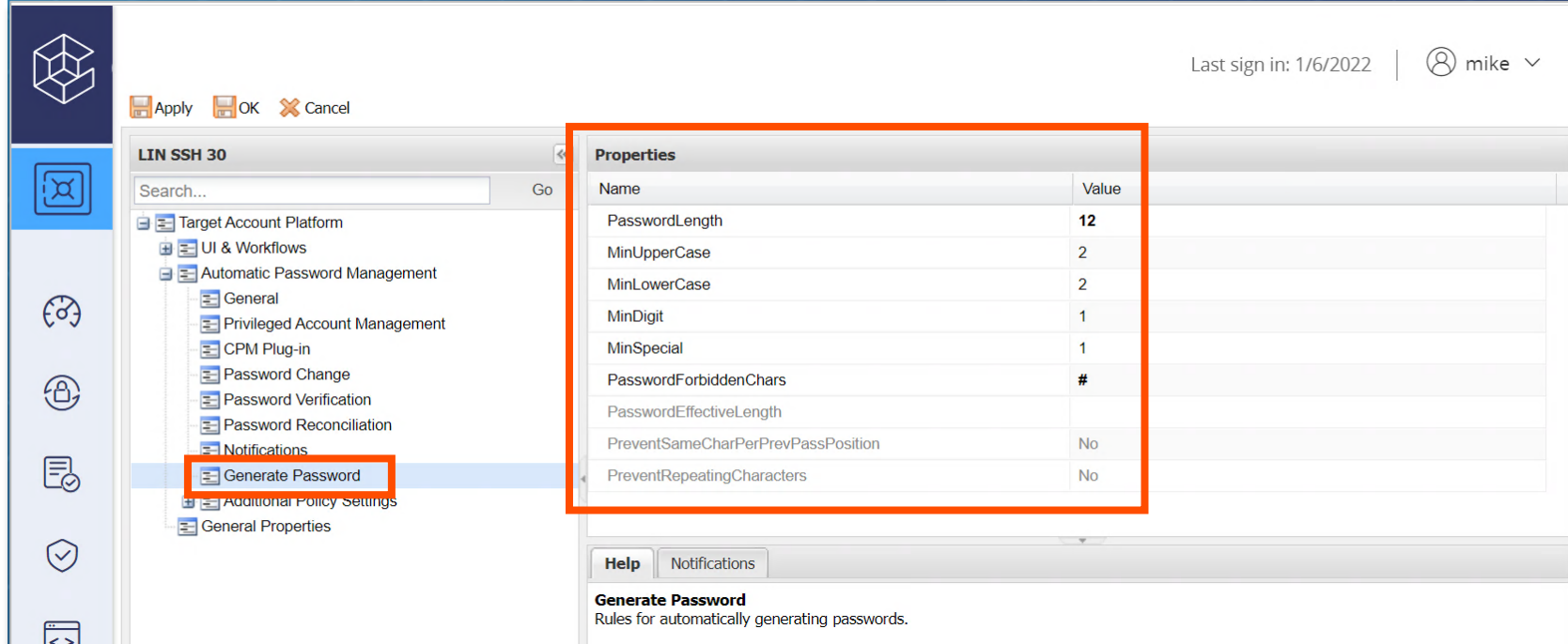
The settings for managing passwords can be found in the **Automatic Password Management** section.



# Edit Platform: Password Complexity

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

- Length
- Complexity
- Forbidden characters
- etc.



Apply OK Cancel

LIN SSH 30

Search... Go

Target Account Platform

- UI & Workflows
- Automatic Password Management
  - General
  - Privileged Account Management
  - CPM Plug-in
  - Password Change
  - Password Verification
  - Password Reconciliation
  - Notifications
  - Generate Password**
  - Additional Policy Settings
  - General Properties

**Properties**

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

Help Notifications

**Generate Password**  
Rules for automatically generating passwords.

Last sign in: 1/6/2022 | mike



# Activating/Deactivating Platforms

The screenshot shows the 'Platform Management' interface. At the top, there's a search bar and tabs for 'Targets', 'Dependents', 'Groups', and 'Rotational Groups'. Below the tabs, it says '40 results'. A table lists various platforms with columns for 'Platform Name', 'Verify password', 'Change password', and 'Reconcile password'. The table includes entries like 'Windows (8)', '\*NIX (3)', 'LIN SSH 30', 'Unix via SSH', 'Unix via SSH Keys', 'Cloud Service (5)', 'Database (8)', and 'Security Appla... (2)'. On the right side of the table, there are buttons for 'Approval', 'Provide Reas', and 'PSM Server on'. A context menu is open over the 'Unix via SSH Keys' row, showing options like 'Edit', 'Manage', 'Duplicate', 'Delete', 'Deactivate' (highlighted with a red box), and 'Export'. The 'Deactivate' option is the focus of the slide.

Platform Management

Last sign in: 8/25/2021 | mike

Filter | Search for target account platforms

Targets Dependents Groups Rotational Groups

40 results

Platform Name	Verify password		Change password		Reconcile password	
	Perio...	Manual	Perio...	Manual	Automatic	M
» Windows (8)						
» *NIX (3)						
LIN SSH 30	-	✓	-	✓	-	✓
Unix via SSH	-	✓	-	✓	-	✓
Unix via SSH Keys	-	✓	-	✓	-	✓
» Cloud Service (5)						
» Database (8)						
» Security Appla... (2)						

Approval Provide Reas PSM Server on Edit

Approval Provide Reas PSM Server on Manage

Approval Provide Reas PSM Server on Duplicate

Delete

**Deactivate**

Export

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 manage Inactive platforms



# Importing New Platforms

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

The image displays two overlapping screenshots from the CyberArk user interface. The background screenshot is the 'Platform Management' page, which includes a sidebar with navigation icons, a search bar for 'target account platforms', and tabs for 'Targets', 'Dependents', 'Groups', and 'Rotational Groups'. The 'Targets' tab is active, showing 43 results in a table with columns for Platform Name, Verify password, Change password, Reconcile password, Access workflow poli..., and PSM Server. The 'Verify password' column has sub-columns for 'Perio...' and 'Manual'. The 'Reconcile password' column has sub-columns for 'Automatic' and 'Manual'. The 'Access workflow poli...' column is partially visible. The 'PSM Server' column is also visible. In the top right corner of the 'Platform Management' page, there are two buttons: 'Marketplace' and 'Import platform', both highlighted with a red rectangle. The foreground screenshot is the 'CyberArk Integrations' page, which features a sidebar with 'Marketplace' and 'CyberArk integrations' sections. The 'Marketplace' section is active, showing a search bar and a list of integrations. The 'CyberArk integrations' section is expanded, showing a list of integrations with checkboxes and counts. The 'Marketplace' section shows 248 results and a 'Clear All Filters' button. Three integration cards are visible: 'Amazon Web Services (AWS) Access Keys', 'A10 Networks Thunder 1030 Admin', and 'A10 Networks Thunder 1030 Enable'. Each card includes a description, a 'Privileged Credentials Management' label, and a star rating.

**Platform Management**

Last sign in: 8/26/2021 | mike

Filter | Search for target account platforms

Targets Dependents Groups Rotational Groups

43 results

Platform Name	Verify password	Change password	Reconcile password	Access workflow poli...	PSM Server
	Perio... Manual	Perio... Manual	Automatic Manual		

**CYBERARK**

Marketplace

CyberArk integrations

Idaptive integrations

Technical Community

**CyberArk Integrations**

Search Apps

MY CONTRIBUTIONS

248 Results Clear All Filters

- All
- Newest
- Featured
- Most Popular
- Top Rated

✖ CyberArk Solution

- ☐ All CyberArk Solutions (724)
- ☐ Administrative Tools (51)
- ☐ Analytics and Threat Detection (39)
- ☐ Application Credentials Security (132)
- ☐ Credentials Access Workflow (10)

**aws** Amazon Web Services (AWS) Access Keys

Manage AWS Access Keys

Privileged Credentials Management

★★★★★

**A10** A10 Networks Thunder 1030 Admin

Manage A10 Networks ...

Privileged Credentials Management

★★★★★

**A10** A10 Networks Thunder 1030 Enable

Manage A10 Networks T...

Privileged Credentials Management

★★★★★



# Master Policy Exceptions



# Policies, Platforms, Safes and Accounts



- Exceptions to Master Policy rules





# Exceptions to the Master Policy

Exceptions to the Master Policy are created by platform

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

The screenshot displays the CyberArk console interface for configuring the Master Policy. The left sidebar shows the navigation menu with 'Master Policy' selected. The main content area is divided into sections: Privileged Access Workflows, Password Management, Session Management, and Audit. The Password Management section is highlighted with a red box, showing a table of policy rules. The 'Require password change every X days' rule is selected, and its exceptions are listed in a separate box on the right. The right sidebar shows the 'Rule Preview' and 'Advanced Settings' for the selected rule.

**Master Policy**

**Privileged Access Workflows**

Policy Rule	Status	Value
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	Active	-

**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	Active	-
Record and save session activity	Active	-

**Audit**

**Rule Preview**

Require password change every X days

**VALUE**

60 Days

**ADVANCED SETTINGS**

None

**EXCEPTIONS (5)**

- [LIN KEYS 90](#)
- [LIN SSH 30](#)
- [ORA DBA 30](#)
- [WIN DOM ADM...](#)
- [WIN SRV LCLA...](#)

**Edit Settings** **Add Exception**



# Policy By Platform

Platform Management

Last sign in: 8/26/2021 | mike

Filter | Search for target account platforms

Targets Dependents Groups Rotational Groups

42 results

Platform Name	Verify password		Change password		Reconcile password	
	Periodic	Manual	Periodic	Manual	Automatic	Manual
Windows (9)						
*NIX (4)						
LIN KEYS 90	7 days	✓	90 days	✓	-	✓
LIN SSH 30	7 days	✓	30 days	✓	-	✓
Unix via SSH	-	✓	-	✓	-	✓
Unix via SSH Keys	-	✓	-	✓	-	✓

Access workflow policies

PSM Server

Approval Provide Reason Check in/out OTP PSM Server on COMPONENTS

Approval Provide Reason Check in/out OTP PSM Server on COMPONENTS

Approval Provide Reason Check in/out OTP PSM Server on COMPONENTS

Approval Provide Reason Check in/out OTP PSM Server on COMPONENTS

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






# Summary



# Summary

In this session we discussed:

-  The CyberArk Password management logic and flow
-  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

