



PAM Administration

Privileged Access Workflows



Agenda

By the end of this session, you will be able to describe and configure the following Privileged Access Workflows:

- Allow transparent connections
- Require users to specify reason for access
- Dual Control
- Exclusive Passwords
- One-time Passwords



Accessing and Using Accounts

- Users who have **List** and **Retrieve Accounts** permissions are able to click on *Show* and *Copy*
- Users who have **List** and **Use Accounts** permissions are able to click on *Connect*
- CyberArk provides advanced access workflows on top of these permissions to determine how users can access accounts and for how long

The screenshot displays the CyberArk console interface for a specific account. At the top right, it shows the last sign-in date as 8/25/2021 and the user 'john'. A search bar is located at the top left. The account name 'localadmin01' is shown with the platform 'WIN SRV LCL ADM 45' and the safe 'Win-Srv-Fin-US'. Below this, there are tabs for 'Overview', 'Details', 'Activities', and 'Versions'. The 'Overview' tab is selected, showing a 'Compliance Status' of 'Compliant' with a '1 Days ago' indicator. A 'Last Verified' section is also present. The 'Activities' section lists recent actions, including 'PasswordManager CPM Verify Password' and 'john PSM Disconnect'. The 'Connect' button is highlighted with a blue box, indicating it is the primary action for this account.

localadmin01 On target-win.acme.corp

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

Overview Details Activities Versions

Compliance Status **Compliant**

1 Days ago

Changed by PasswordManager Aug 24, 2021 5:50 AM

Reconcile Change

Last Verified

Activities (Last 5)

- Aug 25 2:10:02 AM PasswordManager CPM Verify Password
- Aug 25 1:02:54 AM john PSM Disconnect
- Aug 25 1:02:43 AM john PSM Connect
- Aug 25 john

Activate Windows
Go to Settings to activate Windows.



Allow Transparent Connections



Allow EPV Transparent Connections

The screenshot displays the CyberArk Policy console interface. On the left, a sidebar contains navigation icons and the 'POLICIES' section. The main area shows the 'Master Policy' configuration. A table lists various policy rules under 'Privileged Access Workflows'. The rule 'Allow EPV transparent connections (Click to connect)' is highlighted with a red border and is set to 'Active'. A callout box points to this rule with the text: 'Provides corporate level control over users' ability to view passwords or launch privileged sessions'. On the right, a 'Rule Preview' panel shows the rule's value as 'Active' and includes sections for 'ADVANCED SETTINGS' and 'EXCEPTIONS'. The bottom of the interface features a blue bar with 'Activate Windows' and 'Go to Settings to activate Windows' text, along with 'Edit Settings' and 'Add Exception' buttons.

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	Inactive	-

► Password Management

► Session Management

► Audit

Rule Preview

Allow EPV transparent connections ('... ?)

VALUE

Active

► ADVANCED SETTINGS

Allow users to view passwords
Active

► EXCEPTIONS

Provides corporate level control over users' ability to view passwords or launch privileged sessions

Activate Windows
Go to Settings to activate Windows

Edit Settings Add Exception



Allow transparent connections: Advanced settings

- By clicking the **Edit settings** button, we can see that end users are able to **connect** transparently using privileged accounts and are allowed to **view** the passwords
- We can, however, change this behavior

Edit Rule Settings [X]

Privileged Access Workflows | Allow EPV transparent connections ('Click to connect')

Master Policy What's this ?

Basic Policy Rule

Allow EPV transparent connections ('Click to connect') **Active** Inactive

Advanced Settings

Allow users to view passwords **Active** Inactive

Save Save & Close Cancel



Reason for Access



Require Users to Specify Reason for Access

The screenshot displays the CyberArk Privileged Access Management (PAM) console interface. On the left is a navigation sidebar with icons for Policies, Access Control, Passwords, Sessions, and Audit. The main content area is titled 'POLICIES' and 'Master Policy'. It features a table of 'Privileged Access Workflows' with columns for 'Policy Rule', 'Value', and 'Exceptions'. The row 'Require users to specify reason for access' is highlighted with a red box and its 'Active' status is shown. A callout box points to this row with the text: 'Forces users to provide a reason why they are using a particular account'. On the right, a 'Rule Preview' panel shows the rule's name and a 'VALUE' section with an 'Active' toggle.

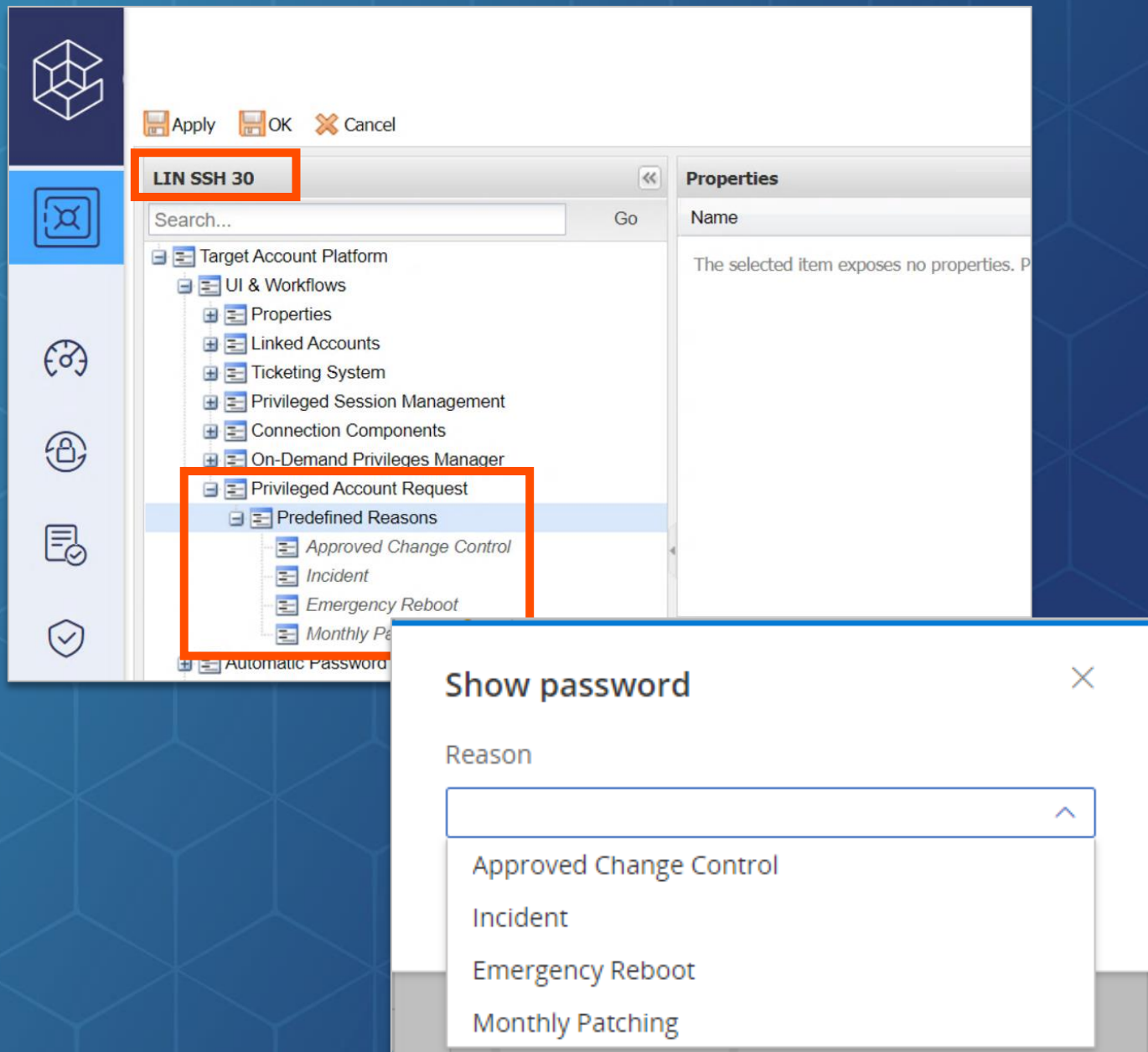
Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	-
Enforce check-in/check-out exclusive access	Inactive	-
Enforce one-time password access	Inactive	-
Allow EDV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

Forces users to provide a reason why they are using a particular account



Platform Settings: Privileged Account Request

- The list of options for the drop-down is defined at the **Platform** level, so we can have a different set of reasons on a platform-by-platform basis.
- In the **Privileged Account Request** section for a given Platform, we can add the Predefined Reasons to create a list of choices for our users when accessing a password in the **PVWA**.



Dual Control



Dual Control – Master Policy

Polices > Master Policy
Master Policy

POLICIES

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')	Inactive	-
Require users to specify reason for access	-	-

► Password Management
► Session Management
► Audit

Rule Preview
Require dual control password access approval

VALUE
Inactive

► ADVANCED SETTINGS
Require multi-level password access approval
Inactive
Only direct managers can approve password access requests
Inactive
Number of confirmers required to authorize requests
1

EXCEPTIONS

Dual control requires end users to get authorization before accessing privileged accounts.
Depending on the configuration, authorization must be given by one or more managers or peers.



Dual Control – Safe Membership




Dual Control is controlled through Safe membership

- **Requesters** are the people who want to use the privileged accounts. They need the permissions **Use** (and/or **Retrieve**) and **List**
- **Approvers** accept or reject requests to privileged accounts, but generally do not use the accounts. They will need **List** and **Authorize** permissions


Requester	Approver
<div><input type="checkbox"/> <u>Access</u> <input checked="" type="checkbox"/> Use accounts <input type="checkbox"/> Retrieve accounts <input checked="" type="checkbox"/> List accounts</div> <div><input type="checkbox"/> <u>Account Management</u></div> <div><input type="checkbox"/> <u>Safe Management</u></div> <div><input type="checkbox"/> <u>Monitor</u></div> <div><input type="checkbox"/> <u>Workflow</u> <input type="checkbox"/> Authorize account requests <input type="radio"/> Level 1 <input type="radio"/> Level 2 <input type="checkbox"/> Access Safe without confirmation</div> <div><input type="checkbox"/> <u>Advanced</u></div>	<div><input type="checkbox"/> <u>Access</u> <input type="checkbox"/> Use accounts <input type="checkbox"/> Retrieve accounts <input checked="" type="checkbox"/> List accounts</div> <div><input type="checkbox"/> <u>Account Management</u></div> <div><input type="checkbox"/> <u>Safe Management</u></div> <div><input type="checkbox"/> <u>Monitor</u></div> <div><div><input type="checkbox"/> <u>Workflow</u> <input checked="" type="checkbox"/> Authorize account requests <input checked="" type="radio"/> Level 1 <input type="radio"/> Level 2 <input type="checkbox"/> Access Safe without confirmation</div><div><input type="checkbox"/> <u>Advanced</u></div></div>




Dual Control – Request Connection












Accounts View




Last sign in: 1/19/2022 |  carlos ▾

 Filter |

16 results for: All accounts


	Status	Username
	-	root01
	-	app-account01
	-	logon01
	-	logon02
	-	logon03
	-	logon04
	-	logon05
	-	logon06

logon01 On 10.0.0.20

Platform: LIN SSH 30 Safe: Lin-Fin-US    **Request connection** ▾



[Overview](#) [Details](#) [Activities](#) [Versions](#)

Compliance Status Compliant







20
Days ago


Changed by PasswordManager
Jan 4, 2022 10:28 AM



Dual Control – Submitting a Request



Last sign in: 1/24/2022 |  carlos ▾

Request to connect with LIN SSH 30-logon01-10.0.0.20

Reason

Approved Change Control ▾

Timeframe

☒ Request timeframe

From

01/24/2022 8:00 AM ▾

To

01/26/2022 5:00 PM ▾


GMT+0000 (Coordinated Universal Time)


☒ Multiple access is required

Confirmation

One user must confirm the request

Confirmers List

 paul
Paul | paul@acme.corp

 ITManagers

Cancel

Send Request



Dual Control – Email Notification

From: CyberArk Vault (no_reply@acme.corp)
To: paul@acme.corp
Date: Mon, 24 Jan 2022 14:14:30 +0000
Subject: Notification: Password access request

Pending password access request

Dear, Paul
A password access request is pending your approval.

Requester details

Requester name: Carlos
Requester user: carlos
Requester email: carlos@acme.corp
Requester phone:

Account details

Account name: Root\Operating System-LINSSH30-10.0.0.20-logon01
Safe: Lin-Fin-US
Device User Name: logon01
Device Address: 10.0.0.20

Request details

Issued on: 1/24/2022 2:14:29 PM

Request Id: 4
Request start date: 1/24/2022 8:00:00 AM
Request end date: 1/26/2022 5:00:00 PM
Request type: Multi
Reason: (ConnectionClient=PSM-SSH) Approved Change Control



Dual Control – Incoming Request

The screenshot displays the CyberArk console interface for managing incoming requests. On the left, a sidebar shows navigation icons. The main area is titled "Incoming Requests" and shows a list of requests. The first request is for "carlos, Carlos" with the account "logon01, 10.0.0.20". The status is "Waiting: 1 more user(s) must confirm the request". The request details are as follows:

Request	
Requester username	carlos
Requester full name	Carlos
Reason	(ConnectionClient=PSM-SSH) Approved Change Control
Requested on	1/24/2022 02:14 PM
Time frame	1/24/2022 08:00 AM - 1/26/2022 05:00 PM
Permission to	Connect
Access	Multiple
Request ID	4

A modal dialog titled "Reason for request confirmation" is open in the center. It prompts the user to "Specify the reason for confirmation:" and has a text input field containing the word "Approved". At the bottom of the dialog are "Cancel" and "Confirm" buttons. In the top right corner of the console, there are "Confirm" and "Reject" buttons, with the "Confirm" button highlighted by a red box. Another "Confirm" and "Reject" button pair is visible on the right side of the interface, also with a red box around them.



Dual Control

The screenshot displays the 'Accounts View' interface. On the left, a sidebar contains navigation icons. The main area shows a list of 16 accounts. The 'logon01' account is selected, and its details are shown on the right. The 'Dual control' status is 'Confirmed request', and the 'Connect' button is highlighted. A compliance status section shows the account is 'Compliant' and was last changed 20 days ago.

Accounts View

Filter | Search for accounts

16 results for: All accounts

☆	Status	Username	Address
☆	-	root01	10.0.0.20
☆	-	app-account01	10.0.0.20
☆	-	logon01	10.0.0.20
☆	-	logon02	10.0.0.20
☆	-	logon03	10.0.0.20
☆	-	logon04	10.0.0.20

logon01 On 10.0.0.20

Platform: LIN SSH 30 Safe: Lin-Fin-US Dual control: Confirmed request **Connect** Show

[Overview](#) [Details](#) [Activities](#) [Versions](#)

Compliance Status Compliant

20 Days ago

Changed by PasswordManager
Jan 4, 2022 10:28 AM

[Reconcile](#) [Change](#)

The requester will receive notification of the approval in the PVWA and via email.



Peer Approval Process

Here we have a single group of admins setup with both requester and approver permissions

- In this scenario, anyone could be a requester or an approver, but since the system prevents a person from approving their own requests, it still requires at least two separate actors
- One person from this group will become the requester and one will become the approver

Windows Team

- ☐ Access
 - ☒ Use accounts
 - ☐ Retrieve accounts
 - ☒ List accounts
- ☐ Account Management
- ☐ Safe Management
- ☐ Monitor
- ☐ Workflow
 - ☒ Authorize account requests
 - ☒ Level 1
 - ☐ Level 2
 - ☐ Access Safe without confirmation
- ☐ Advanced



Bypass Dual Control

We may want to allow certain groups to bypass Dual Control

- Here our admin teams have the "**Access Safe without confirmation**" permission and are therefore allowed to bypass dual control
- The support team still needs to get approval

Admin Team	Support Team
<input type="checkbox"/> <u>Access</u> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts	<input type="checkbox"/> <u>Access</u> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts
<input type="checkbox"/> <u>Account Management</u>	<input type="checkbox"/> <u>Account Management</u>
<input type="checkbox"/> <u>Safe Management</u>	<input type="checkbox"/> <u>Safe Management</u>
<input type="checkbox"/> <u>Monitor</u>	<input type="checkbox"/> <u>Monitor</u>
<input type="checkbox"/> <u>Workflow</u> <ul style="list-style-type: none"><input type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input type="radio"/> Level 2	<input type="checkbox"/> <u>Workflow</u> <ul style="list-style-type: none"><input type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input type="radio"/> Level 2
<input checked="" type="checkbox"/> <u>Access Safe without confirmation</u>	<input type="checkbox"/> <u>Access Safe without confirmation</u>
<input type="checkbox"/> <u>Advanced</u>	<input type="checkbox"/> <u>Advanced</u>



Multi-Group Approval Process

If we setup more than one group with approver permissions, at least one person from each group must approve the request before the requester can use the password

Windows Team	IT Managers	Change Advisory Board
<input type="checkbox"/> Access <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts <input type="checkbox"/> Account Management <input type="checkbox"/> Safe Management <input type="checkbox"/> Monitor <input type="checkbox"/> Workflow <ul style="list-style-type: none"><input type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation <input type="checkbox"/> Advanced	<input type="checkbox"/> Access <ul style="list-style-type: none"><input type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts <input type="checkbox"/> Account Management <input type="checkbox"/> Safe Management <input type="checkbox"/> Monitor <input type="checkbox"/> Workflow <div><input checked="" type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input checked="" type="radio"/> Level 1<input type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation</div> <input type="checkbox"/> Advanced	<input type="checkbox"/> Access <ul style="list-style-type: none"><input type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts <input type="checkbox"/> Account Management <input type="checkbox"/> Safe Management <input type="checkbox"/> Monitor <input type="checkbox"/> Workflow <div><input checked="" type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input checked="" type="radio"/> Level 1<input type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation</div> <input type="checkbox"/> Advanced



Dual Control: Advanced Settings

In the advanced settings for **Dual Control**, we can enable a multi-level approval process

- With a **multi-level** process, a request must first be approved by one group before it is forwarded for approval to another group
- Also in advanced settings, we can enable direct manager approval, determined by the **Manager** attribute on the requester's AD user object

Edit Rule Settings [X]

Privileged Access Workflows | Require dual control password access approval

Master Policy [What's this ?](#)

Basic Policy Rule

Require dual control password access approval	Active	Inactive
---	---------------	----------

Advanced Settings

Require multi-level password access approval	Active	Inactive	?			
Only direct managers can approve password access requests	Active	Inactive	?			
Number of confirmers required to authorize requests	1	2	3	All	Other	!

Save **Save & Close** **Cancel**



Multi Level Approval Process

In this example, a request is sent first to the **IT Managers** group

- Once approved by at least one person from the **Managers** group, the request is forwarded to the **IT Directors** group
- At least one person from each group must approve before the password may be used

Windows Team	IT Managers	IT Directors
<input type="checkbox"/> Access <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts	<input type="checkbox"/> Access <ul style="list-style-type: none"><input type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input checked="" type="checkbox"/> List accounts	<input type="checkbox"/> Access <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use accounts<input type="checkbox"/> Retrieve accounts<input type="checkbox"/> List accounts
<input type="checkbox"/> Account Management	<input type="checkbox"/> Account Management	<input type="checkbox"/> Account Management
<input type="checkbox"/> Safe Management	<input type="checkbox"/> Safe Management	<input type="checkbox"/> Safe Management
<input type="checkbox"/> Monitor	<input type="checkbox"/> Monitor	<input type="checkbox"/> Monitor
<input type="checkbox"/> Workflow <ul style="list-style-type: none"><input type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation	<div><input type="checkbox"/> Workflow<ul style="list-style-type: none"><input checked="" type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input checked="" type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation</div>	<div><input type="checkbox"/> Workflow<ul style="list-style-type: none"><input checked="" type="checkbox"/> Authorize account requests<ul style="list-style-type: none"><input type="radio"/> Level 1<input checked="" type="radio"/> Level 2<input type="checkbox"/> Access Safe without confirmation</div>
<input type="checkbox"/> Advanced	<input type="checkbox"/> Advanced	<input type="checkbox"/> Advanced



Exclusive Access



Exclusive Passwords

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 shows the 'Privileged Access Workflows' section with a table of policy rules. The rule 'Enforce check-in/check-out exclusive access' is highlighted with a red box and has its value set to 'Active'. A callout box explains the function of this rule. On the right, the 'Rule Preview' and 'Advanced Settings' panels are visible.

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	1
Enforce check-in/check-out exclusive access	Active	-
Enforce one-time password access	Inactive	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

► Password Management

► Session Management

► Audit

Rule Preview

Enforce check-in/check-out exclusive ... ?

VALUE

Active

► ADVANCED SETTINGS

None

► EXCEPTIONS

When applied, only one user will be able to access and use an account at any given time.

When a user checks-out an account, it is **LOCKED** and cannot be retrieved by other users until it is checked-in.



Exclusive Password – Locked

The screenshot displays the 'Accounts View' interface. On the left, a table lists 14 accounts. The 'localadmin01' account is highlighted and marked with a lock icon in the status column. The main panel shows details for 'localadmin01 On target-win.acme.corp', including platform and safe information. A red box highlights a message: 'This account is checked-out by tom'. Below this, the compliance status is 'Compliant'. A callout box explains that if another user attempts to access the password, the status will show a lock button, indicating it is locked by the first user.

Accounts View

Last sign in: 1/25/2022 | john

Filter | Search for accounts

14 results for: All accounts

☆	Status	Username
☆	-	administrator
☆	🔒	localadmin01
☆	-	backdoor
☆	-	discovery01
☆	-	discovery02
☆	-	discovery03

localadmin01 On target-win.acme.corp

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

Show Copy ... Connect

Overview Details Activities Versions

🔒 This account is checked-out by tom

Compliance Status **Compliant**

Changed by PasswordManager Jan 19, 2022 10:04 AM

Reconcile Change

If another user attempts to access the password, the status will appear with a lock button, indicating that it is locked by the first user

Remember: By default, the password can only be released by the owner of the lock (Tom in this case) or by an administrator who has the rights to force a password release



Exclusive Password – Manual Check-In

The screenshot displays the 'Accounts View' interface. On the left is a sidebar with navigation icons. The main area shows a search filter for 'localad' resulting in 2 accounts. A table lists these accounts with columns for Status and Username. The account 'localadmin01' is selected, opening a detailed view. This view includes tabs for Overview, Details, Activities, and Versions. A red box highlights the 'Check-in' option in the 'Overview' tab's action menu. A callout box points to this option with the following text:

After accessing the account (using **Show** or **Connect**), the user will have the “Check-in” option to unlock the account and make it available to other users.

The detailed view for 'localadmin01' also shows platform information (WIN SRV LCL ADM 45), safe name (Win-Srv-Fin-US), and a recent password change by PasswordManager on Jan 19, 2022 at 10:04 AM. At the bottom of the detailed view are 'Reconcile' and 'Change' buttons.



Exclusive Password – Release and Change

The screenshot shows the 'Accounts View' interface. On the left is a sidebar with icons for Accounts, Connections, Groups, and Settings. The main area is titled 'Accounts View' and shows a search filter for 'localadm' with 2 results. A table lists accounts: localadmin01 and localadmin02. A modal window is open for 'localadmin01 On target-win.acme.corp'. It shows the account is checked out by 'tom'. A red box highlights a message: 'The password for this account has been manually scheduled for change'. Below this, it says 'This account is checked-out by tom'. The modal also has tabs for Overview, Details, Activities, and Versions, and buttons for Show, Copy, and Connect.

Accounts View

Filter | localadm

2 results for: localadm

Status	Username
☆	localadmin01
☆	localadmin02

localadmin01 On target-win.acme.corp

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

Additional details & actions in classic interface

Overview Details Activities Versions

The password for this account has been manually scheduled for change

This account is checked-out by tom

After the user checks-in the account, the password will be scheduled for an immediate change by the CPM

The CPM will then release and change the account password

The screenshot shows a timeline of events. The timeline is titled 'Jan 25 Today'. It shows three events: 1. 9:24:41 AM: PasswordManager CPM Change Password | Address: target-win.acme.corp, User Name: localadmin01. 2. 9:24:41 AM: PasswordManager CPM Release Password | Address: target-win.acme.corp, User Name: localadmin01. 3. 9:23:55 AM: tom Add File Category: ResetImmediately = ChangeTask. 4. 9:23:27 AM: tom Show Password - Training.

Jan 25 Today

9:24:41 AM PasswordManager CPM Change Password | Address: target-win.acme.corp, User Name: localadmin01

9:24:41 AM PasswordManager CPM Release Password | Address: target-win.acme.corp, User Name: localadmin01

9:23:55 AM tom Add File Category: ResetImmediately = ChangeTask

9:23:27 AM tom Show Password - Training



Exclusive Password – Auto Release by PSM

Beginning with CyberArk PAM version 11.7, the **PSM** can automatically release an account after the user closes the session

This is configured at the **Platform** level.

The screenshot displays two parts of the CyberArk PAM interface. The top part shows the 'Activities' tab for the account 'localadmin01 On target-win.acme.corp'. It lists 338 activities, with a specific activity highlighted: 'PSMApp_COMPONENTS Unlock File' on 'Jan 25' at '9:55:00 AM'. The bottom part shows the 'Properties' tab for the platform 'WIN SRV LCL ADM 45'. The 'Privileged Session Management' section is expanded, and the 'ExclusiveUnlockAfterPSMSession' property is highlighted with a red box, showing its value as 'Yes'.

localadmin01 On target-win.acme.corp

Platform: WIN SRV LCL ADM 45 Safe: Win-Srv-Fin-US [Show](#)

Overview Details **Activities** Versions

User Action

338 Activities for this account

Jan 25 Today

9:55:00 AM PSMApp_COMPONENTS
Unlock File

WIN SRV LCL ADM 45

Search... Go

- Target Account Platform
 - UI & Workflows
 - Properties
 - Linked Accounts
 - Usages
 - Ticketing System
 - Privileged Session Management**
 - Connection Components
 - Automatic Password Management
 - General Properties

Properties

Name	Value
ID	PSMServer
SubnetPolicy	No
SessionRecorderSafe	PSMRecordings
SessionRecorderSafeRetention	180
MaxSessionDuration	-1
ShowRecordedSessionNotification	Yes
RecordedSessionNotificationDisplayTime	5
ShowLiveMonitoringNotification	Yes
LiveMonitoringNotificationDisplayTime	5
DisableDualControlForPSMConnections	No
EnablePrivilegedSSO	Yes
UsePersonalPassword	No
ExclusiveUnlockAfterPSMSession	Yes



One-time Passwords



One-Time Passwords

- One-time passwords are enabled in the **Master Policy**
- It is possible for multiple users to access the same account simultaneously
- The password will be changed based on ***MinValidityPeriod***, as configured in the **Platform**

Enforce one-time password access (without exclusivity)

The screenshot shows the CyberArk console interface. On the left is a navigation sidebar with icons for Policies, Master Policy, Policy by Platform, Access Control (Safes), and other settings. The main content area is titled 'POLICIES' and 'Master Policy'. Under 'Privileged Access Workflows', there is a table with columns 'Policy Rule', 'Value', and 'Exceptions'. The row 'Enforce one-time password access' is highlighted with a red box, showing its value as 'Inactive' and exceptions as '1'.

Policy Rule	Value	Exceptions
Require dual control password access approval	Inactive	1
Enforce check-in/check-out exclusive access	Inactive	1
Enforce one-time password access	Inactive	1
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

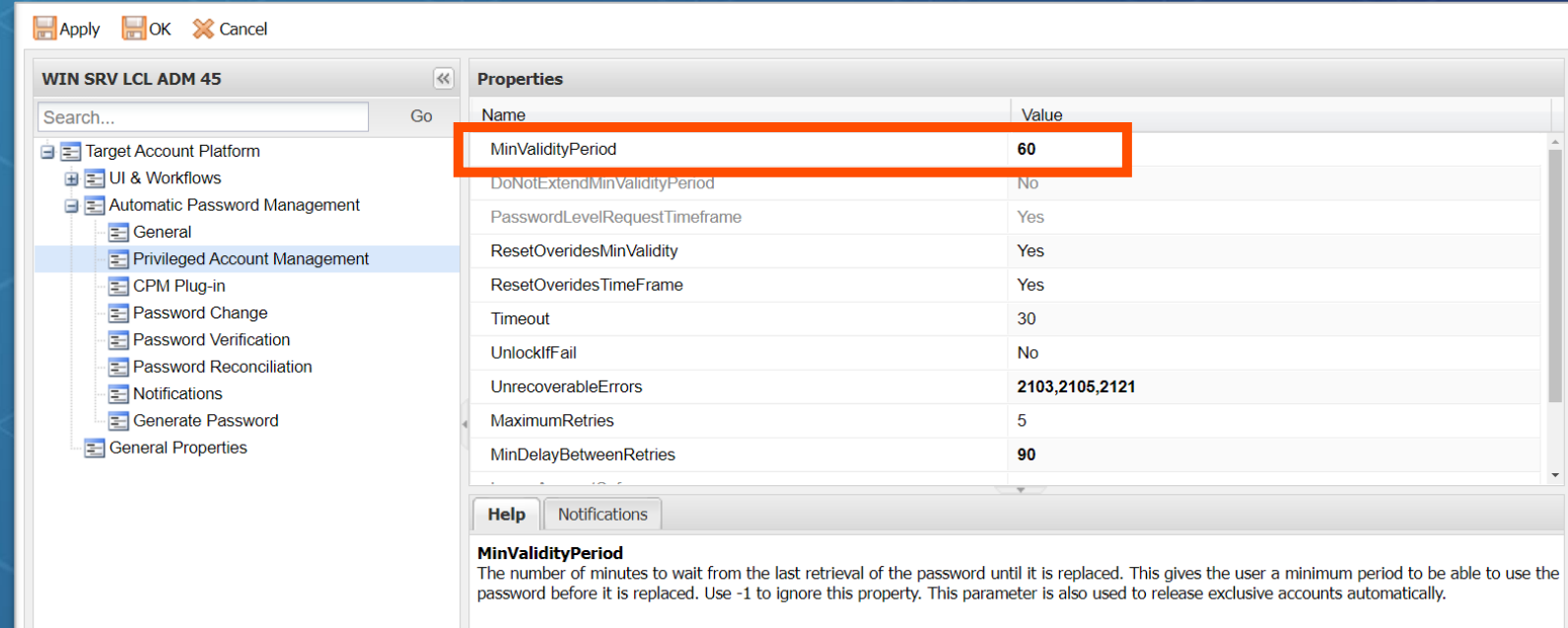
Below the table, there are sections for Password Management, Session Management, and Audit.

When a user retrieves an account, the account is flagged for change by the CPM after a specified time



MinValidityPeriod – Platform Configuration

- A **MinValidityPeriod** of 60 means that the password will be changed 60 minutes after it is accessed
- During that time, other users can access the password
- Each time the password is used, the **MinValidityPeriod** timer is reset
- The **MinValidityPeriod** should provide enough time for a user to make use of the password



Combining Workflows



Exclusive Access With One-time Password

POLICIES

Policies > Policy By Platform
Policy for: WIN SRV LCL ADM 45 ?

Change Platform

Master Policy

Policy by Platform

Access Control (Safes)

Privileged Access Workflows

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

► Password Management

► Session Management

► Audit

If **Exclusive access** and **One-Time Password** are enabled for the same Platform, the password will be marked for change 60 minutes (by default) after it is used.

This keeps the password exclusive, but enables automatic release after 60 minutes



Dual Control With One-time Passwords and Exclusivity

When using check-in/check-out exclusive access or one-time password access with **Dual Control**

Request to connect with Linux via SSH 30-logon01-10.0.0.20

Reason

Need to install a patch no. 789654

Timeframe

☒ Request timeframe

From

Jan 30, 2019

8:00 AM



To

Feb 1, 2019

5:00 PM



GMT+0000 (GMT Standard Time)

☒ Multiple access is required

If the **Request timeframe** is active, this setting overrides the **MinValidityPeriod** and the password will only be changed by the CPM after the timeframe has expired.



Exclusive and One-time Password Summary

Exclusive Passwords

- When a user accesses a password, the account is locked and no other user can access the password until it has been released.
- Password is changed automatically upon manual release
- In later versions, the password can be auto-released by the **PSM**

One-time Passwords

- After a user accesses a password, it is changed automatically based on the minimum validity period
- Multiple users can access the password simultaneously
- Minimum validity period is reset as each user accesses the password

Exclusive and One-time Passwords Combined

- Account is locked to a single user, no other user can access it
- If the user does not release the account manually, the system will release it automatically based on the Minimum validity period and change the password



Summary



Summary

In this session we discussed these workflows:

- ✔ Allow transparent connections
- ✔ Require users to specify reason for access
- ✔ Dual Control
- ✔ Exclusive Passwords
- ✔ One-time Passwords



Additional Resources



eLearning

[Customizing Privileged Account Requests](#) (login required)

You may now complete the following exercises:

Privileged Access Workflows

- Require users to specify reason for access
 - Activating the Policy
 - Add Predefined Reasons for Access
- Require dual control access approval
 - Activating the Policy
 - Adding an approver to a Safe
 - Testing Dual Control
- Exclusive Passwords with Automated Release and One-time Use
 - Adding a Master Policy exception for Exclusive Passwords
 - Adding a Master Policy exception for One-Time Passwords
 - Reducing the Minimum Validity Period
 - Testing Exclusive Passwords
 - Testing Automatic release by PSM