



**CYBERARK<sup>®</sup>**  
The Identity Security Company<sup>™</sup>

# 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:

1. Allow transparent connections
2. Require users to specify reason for access
3. Dual Control
4. Exclusive Passwords
5. 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 PAM** provides advanced workflows on top of these permissions to determine how users can access accounts and for how long

The screenshot displays the CyberArk PAM interface for a specific account. At the top right, it shows the last sign-in time as 8/25/2021 and the user 'john'. A search bar is located on the left. A blue button labeled 'Ad-Hoc connection' is in the top right. The main header shows the account name 'localadmin01 On target-win.acme.corp' and a link to 'Additional details & actions in classic interface'. Below this, there are buttons for 'Show', 'Copy', a menu icon, and 'Connect'. The 'Overview' tab is selected, showing a 'Compliance Status' of 'Compliant' with a circular progress indicator showing '1 Days ago'. It also indicates the account was 'Changed by PasswordManager Aug 24, 2021 5:50 AM' with 'Reconcile' and 'Change' buttons. The 'Activities' section shows a list of recent actions: 'PasswordManager CPM Verify Password' (Aug 25 2:10:02 AM), 'john PSM Disconnect' (Aug 25 1:02:54 AM), and 'john PSM Connect' (Aug 25 1:02:43 AM). A watermark 'Activate Windows Go to Settings to activate Windows.' is visible in the bottom right of the interface.

# Allow Transparent Connections

---

# Allow EPV Transparent Connections

Policies > Master Policy

## Master Policy ?

Last sign in: 11/25/2022 | 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	Inactive	-

► Password Management

► Session Management

► Audit

Rule Preview

Allow EPV transparent connections ('... ?)

VALUE

Active

▼ ADVANCED SETTINGS

Allow users to view passwords  
Active


► EXCEPTIONS

Edit Settings Add Exception

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

# 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 by default to **view** passwords

 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

Policies > Master Policy

## Master Policy ?

Last sign in: 11/29/2022 | mike ▾

### Rule Preview

Require users to specify reason for a... ?

VALUE

Inactive ✎

#### ADVANCED SETTINGS

Allow users to specify free text reason for access  
[Active](#)

#### EXCEPTIONS

Edit Settings Add Exception

### 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	-

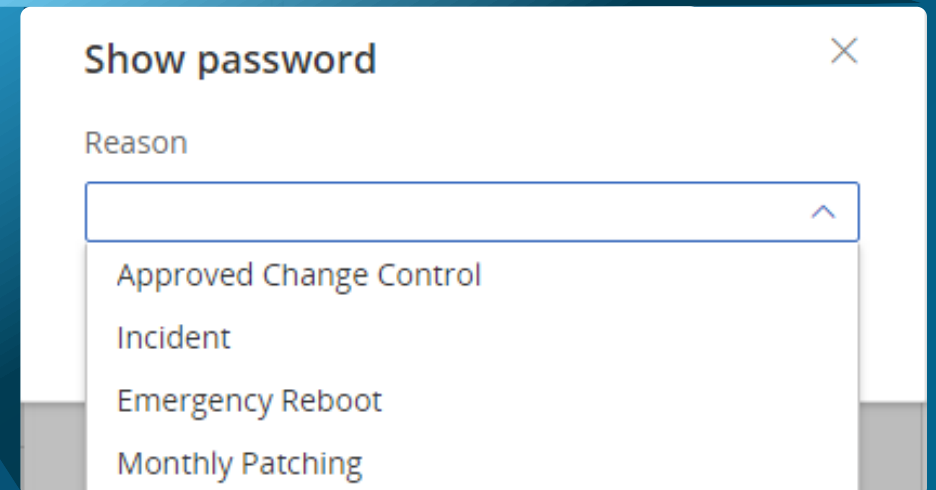
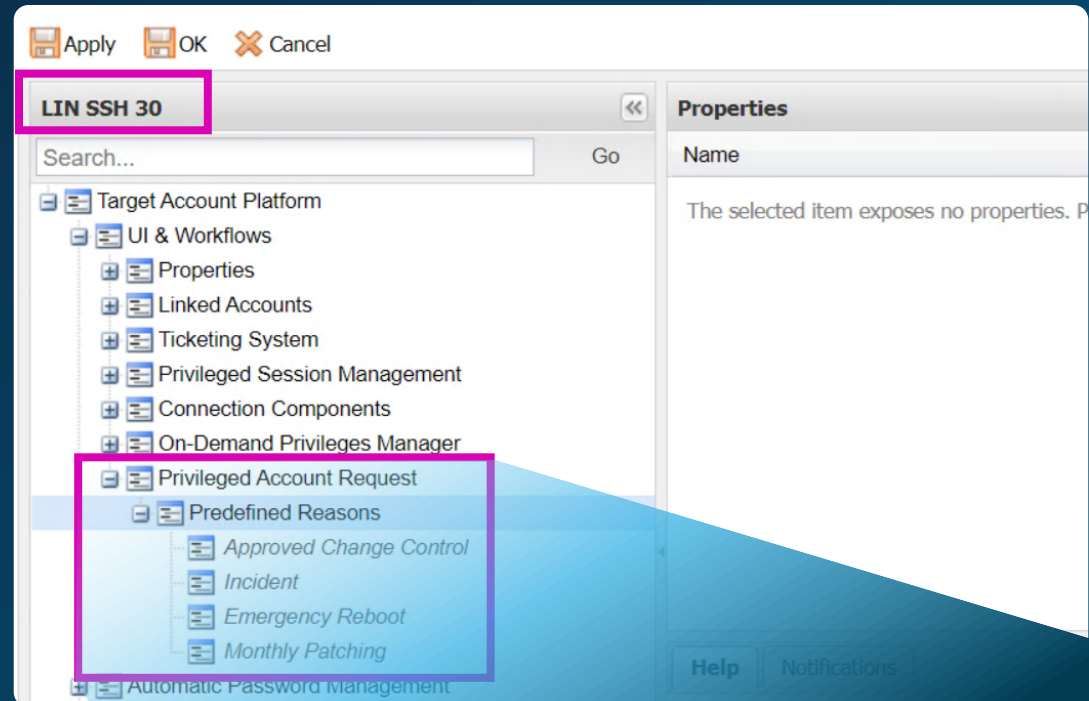
- ▶ Password Management
- ▶ Session Management
- ▶ Audit

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

Policies > Master Policy

## Master Policy ?

Last sign in: 11/29/2022 | 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		-

► Password Management

► Session Management

► Audit

### Rule Preview

Require dual control password acces... ?

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 requests

OPTIONS

Edit Settings Add Exception

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

☐ 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

## APPROVER

☐ 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

# Dual Control – Request Connection

## Accounts View

Last sign in: 1/19/2022 | carlos

Filter

Search for accounts

Ad-Hoc connection

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 show Request copy

Request connection

Overview

Details

Activities

Versions

Compliance Status


Compliant

20 Days ago

Changed by PasswordManager Jan 4, 2022 10:28 AM

Reconcile Change

# 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 'Incoming Requests' with a filter icon and a status filter set to 'Pending'. The main area shows a list of requests, with one request selected and its details expanded. The request is for account 'logon01' (IP: 10.0.0.20) and is in a 'Waiting' state, requiring confirmation from one more user. A modal dialog titled 'Reason for request confirmation' is open, prompting the user to specify the reason for confirmation. The text 'Approved' is entered in the provided text area. The dialog has 'Cancel' and 'Confirm' buttons. In the background, the request details are visible, including the requester's username 'carlos', full name 'Carlos', and the reason '(ConnectionClient=PSM-SSH) Approved Change Control'. The time frame is '1/24/2022 08:00 AM - 1/26/2022 05:00 PM' and the permission is 'Connect'. The access level is 'Multiple' and the request ID is '4'. The top right of the console shows the user 'paul' and the last sign-in time '1/24/2022'.

**Incoming Requests**

Filter

1 results for: Pending

Status

Go to Incoming Requests

carlos, Carlos

Connect for account: logon01, 10.0.0.20 Status: Waiting: 1 more user(s) must confirm the request

Details Confirmers

**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

Last sign in: 1/24/2022 | paul

Updated at: 2:34 PM

Confirm Reject

**Reason for request confirmation**

Specify the reason for confirmation:

Approved

Cancel Confirm

Confirm Reject

# Dual Control

## Accounts View

Last sign in: 1/24/2022 carlos

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

### 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

- ☐ 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

## SUPPORT 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

# 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

- ☐ 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

## IT MANAGERS

- ☐ 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

## CHANGE ADVISORY BOARD

- ☐ 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

# 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**

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 !

Selecting “**All**” in number of confirmers could lead to requests being unnecessarily delayed if certain users are out of office or otherwise unavailable.

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

☐ 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

## IT MANAGERS

☐ 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

## IT DIRECTORS

☐ 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




# Exclusive Access

---

# Exclusive Passwords

Last sign in: 1/24/2022 |  mike ▾

Policies > Master Policy

Master Policy 

▼ 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 has a lock icon in its status column. On the right, the details for 'localadmin01 On target-win.acme.corp' are shown. A pink box highlights a message: 'This account is checked-out by tom'. Below this, the status is 'Compliant' and it was 'Changed by PasswordManager Jan 19, 2022 10:04 AM'. A callout box explains that the lock icon indicates the password 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

**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

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. At the top, there's a search bar with 'localad' entered, showing '2 results for: localad'. Below this is a table with columns for Status and Username. The first row, 'localadmin01', is highlighted. To the right, a detailed view for 'localadmin01 On target-win.acme.corp' is shown. This view includes tabs for Overview, Details, Activities, and Versions. A dropdown menu is open, showing options: Edit, Check-in (highlighted with a pink box), Verify, Reconcile, Change, and Delete. A callout box points to the 'Check-in' option.

Accounts View

Last sign in: 1/19/2022 | tom

Filter localad

2 results for: localad

Status	Username
	localadmin01
-	localadmin02

localadmin01 On target-win.acme.corp

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

Overview Details Activities Versions

Additional details & actions in classic interface

Edit Check-in Verify Reconcile Change Delete

Connect

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.

5 Days ago

Reconcile Change

# Exclusive Password – Release and Change

The screenshot shows the 'Accounts View' interface. At the top, there's a search bar with 'localadm' entered, showing '2 results for: localadm'. Below this is a table with columns 'Status' and 'Username'. The first row shows 'localadmin01' with a lock icon. To the right, a detailed view for 'localadmin01 On target-win.acme.corp' is open. It shows 'Platform: WIN SRV LCL ADM 45' and 'Safe: Win-Srv-Fin-US'. A pink 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'. Buttons for 'Show', 'Copy', and 'Connect' are visible.

Status	Username
🔒	localadmin01
-	localadmin02

localadmin01 On target-win.acme.corp

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

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 view for 'Jan 25' and 'Today'. A pink box highlights two events from 'PasswordManager': 'CPM Change Password' and 'CPM Release Password', both for 'Address: target-win.acme.corp, User Name: localadmin01'. Below these, other events are listed: 'tom Add File Category: ResetImmediately = ChangeTask' and 'tom Show Password - Training'.

Jan 25 Today

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

9:23:55 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 the CyberArk PAM interface. The top section shows the account 'localadmin01' on target 'target-win.acme.corp'. Below this, the 'Activities' tab is selected, showing a timeline of activities for 'localadmin01'. A pink box highlights two activities: 'PSMApp\_COMPONENTS Unlock File' at 9:55:00 AM and 'tom PSM Disconnect' at 9:55:00 AM. To the right, the 'Properties' tab is selected, showing a list of properties for the 'WIN SRV LCL ADM 45' platform. A pink box highlights the 'ExclusiveUnlockAfterPSMSession' property, which is set to 'Yes'.

localadmin01 On target-win.acme.corp

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

Overview Details **Activities** Versions

User All

338 Activities for this account

Jan 25 Today

9:55:00 AM PSMApp\_COMPONENTS Unlock File

9:55:00 AM tom PSM Disconnect

**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
<b>ExclusiveUnlockAfterPSMSession</b>	<b>Yes</b>

# 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)

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	Inactive	1
<b>Enforce one-time password access</b>	<b>Inactive</b>	<b>1</b>
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	Active	-

► Password Management

► Session Management

► 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
- The **MinValidityPeriod** should provide enough time for a user to make use of the password

The screenshot displays the 'WIN SRV LCL ADM 45' configuration window. On the left, a tree view shows the hierarchy: Target Account Platform > UI & Workflows > Automatic Password Management > Privileged Account Management. The 'Properties' pane on the right lists various configuration items. The 'MinValidityPeriod' property is highlighted with a red box, showing a value of '60'. Other visible properties include 'DoNotExtendMinValidityPeriod' (No), 'PasswordLevelRequestTimeframe' (Yes), 'ResetOverridesMinValidity' (Yes), 'ResetOverridesTimeFrame' (Yes), 'Timeout' (30), 'UnlockIfFail' (No), 'UnrecoverableErrors' (2103,2105,2121), 'MaximumRetries' (5), and 'MinDelayBetweenRetries' (90). At the bottom, a 'Help' tab is active, displaying the definition of 'MinValidityPeriod': 'The number of minutes to wait from the last retrieval of the password until it is replaced. This gives the user a minimum period to be able to use the password before it is replaced. Use -1 to ignore this property. This parameter is also used to release exclusive accounts automatically.'

Name	Value
MinValidityPeriod	60
DoNotExtendMinValidityPeriod	No
PasswordLevelRequestTimeframe	Yes
ResetOverridesMinValidity	Yes
ResetOverridesTimeFrame	Yes
Timeout	30
UnlockIfFail	No
UnrecoverableErrors	2103,2105,2121
MaximumRetries	5
MinDelayBetweenRetries	90

**MinValidityPeriod**  
The number of minutes to wait from the last retrieval of the password until it is replaced. This gives the user a minimum period to be able to use the password before it is replaced. Use -1 to ignore this property. This parameter is also used to release exclusive accounts automatically.

# Combining Workflows

---

# Exclusive Access With One-time Password

Policies > Policy By Platform

Policy for: WIN SVR ADM 45

Last sign in: 11/29/2022 | mike

Change Platform

Overview

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		-

Password Management

Session Management

Audit

Introduction to Policy by Platform

The Policy by Platform view enables you to easily see the settings that will be applied to each platform and gives you an 'at a glance' picture of the effective policy that manages associated accounts.

You can see the base line of compliance-related settings implemented at system level through the Master Policy, combined with exceptions for specific platforms.

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**, the password will only be changed after the time frame has expired

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 | v

To

Feb 1, 2019 5:00 PM | v

GMT+0000 (GMT Standard Time)

☒ Multiple access is required

If the **Request** timeframe is active, this setting overrides the **MinValidityPeriod**

# 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



## Online Training

[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