**Cyber-Ark Privileged Identity Management**

**User Guide**

Version: 0.2

Revision Date: 26 Feb 2019

Contents

[Abbreviation 2](#_Toc536742693)

[Logon 3](#_Toc536742694)

[Logoff 4](#_Toc536742695)

[Account retrieval 5](#_Toc536742696)

[Search accounts 5](#_Toc536742697)

[Retrieve SSH Key 5](#_Toc536742698)

[Show password 6](#_Toc536742699)

[Copy password 7](#_Toc536742700)

[Request Approval Workflow - Requestor 8](#_Toc536742701)

[Request target account access 8](#_Toc536742702)

[Account retrieval after approval confirmation 10](#_Toc536742703)

[Request Approval Workflow - Approver 10](#_Toc536742704)

[Approve target account access 10](#_Toc536742705)

[Reject target account access 12](#_Toc536742706)

[Account Administration 14](#_Toc536742707)

[Add Account for Supported System 14](#_Toc536742708)

[Add Account for SSH Key 15](#_Toc536742709)

[Associate Account 17](#_Toc536742710)

[Un-Associate Account 19](#_Toc536742711)

[Delete Account 20](#_Toc536742712)

[Reference 21](#_Toc536742713)

# Abbreviation

Password Vault Web Access (PVWA)

* Used for retrieve target account and administration
* Web interface, no installation required on client PC
* Connect to PVWA server

# Logon

1. Open **Internet Explorer** (classic Desktop mode, not Edge)
2. Open PVWA website

[https://XXXXX/PasswordVault](https://xxxxx/PasswordVault)

1. Login with Active Directory LDAP domain account

Fill in username (example: user1)

**No need to enter domain prefix**



Note if ldap authentication is not shown here, click left button



Click LDAP



OR



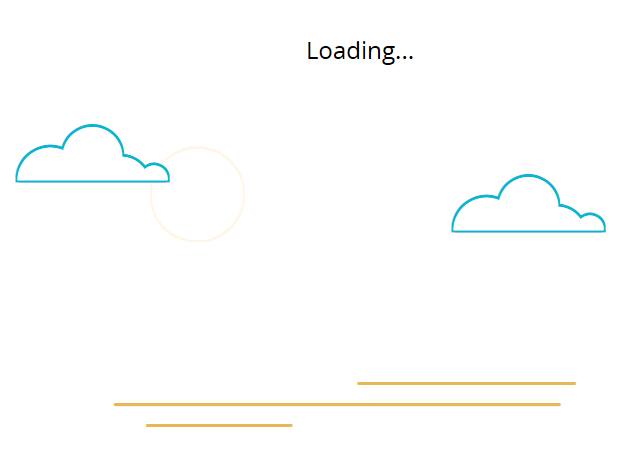
Note if ldap authentication is not shown here, click Change authentication method



Click LDAP

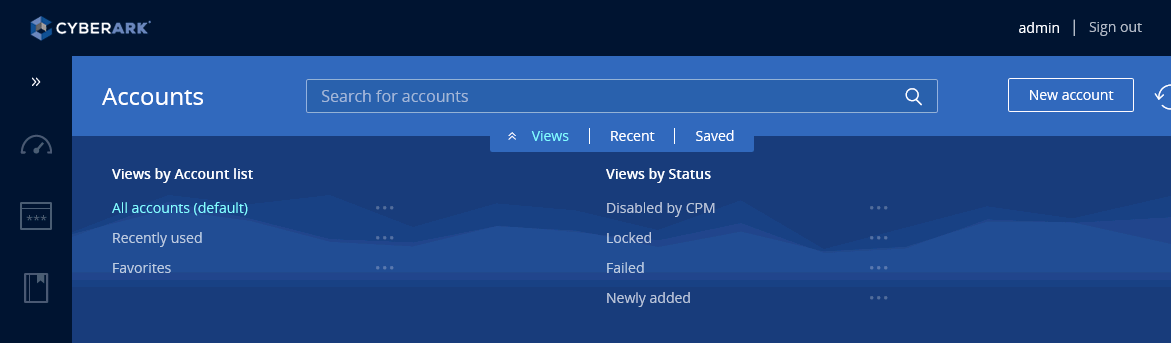


1. Wait for page to load



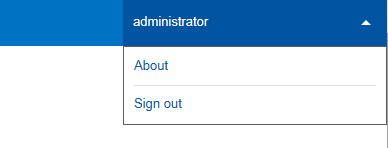
# Logoff

1. Click Sign out in upper right corner



OR

1. List down the user name at top right corner and click "Sign out" to log off



1. Confirmed signed out

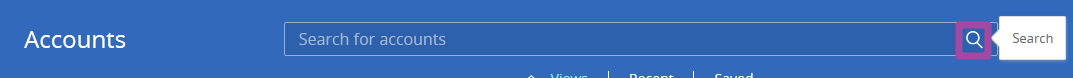


# Account retrieval

## Search accounts

To search for ALL accounts

1. Keep search box as empty
2. Click Search button

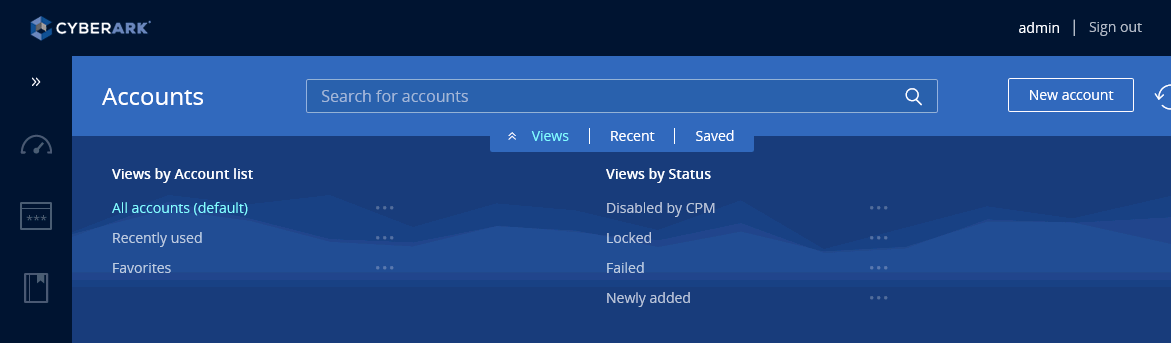


OR



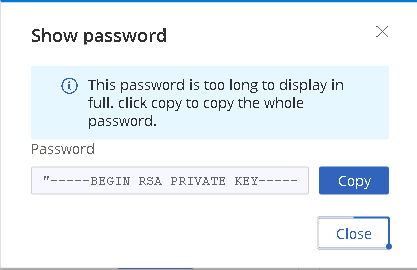
To search specific account

1. Enter keyword of account
2. Click Search button



## Retrieve SSH Key

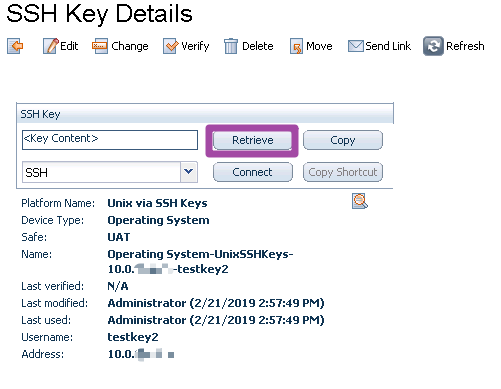
1. Click that target account
2. Click “Show”, enter reason when prompts, click “Copy”



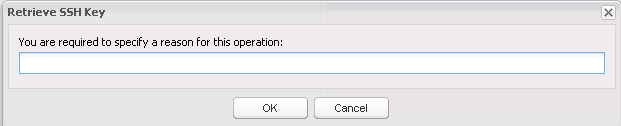
**Remove “ in the beginning and ” in the end**

OR

1. Click “Additional details & actions in classic interface”
2. Click Retrieve

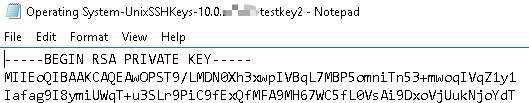


1. Enter reason



1. Key would be downloaded



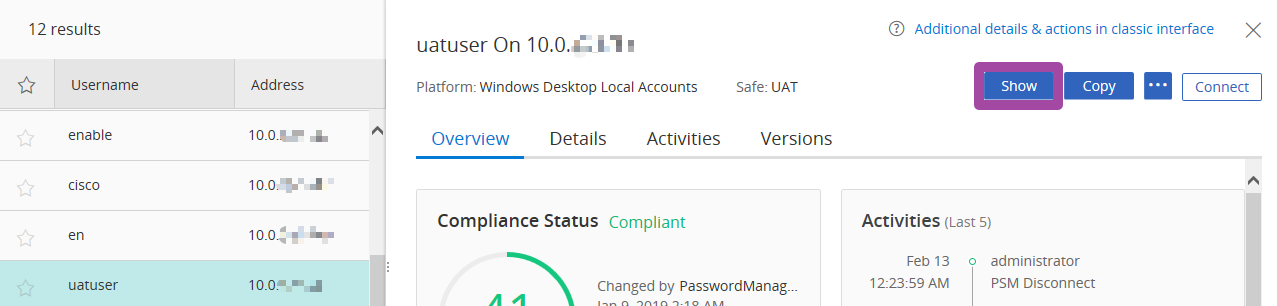


## Show password

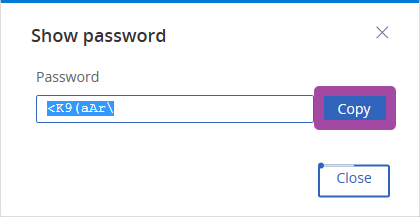
1. Click that target account



1. Click “Show”



1. Click “Copy” if needed

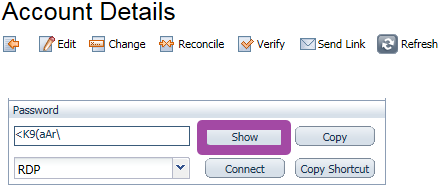


OR

1. Click “Additional details & actions in classic interface”

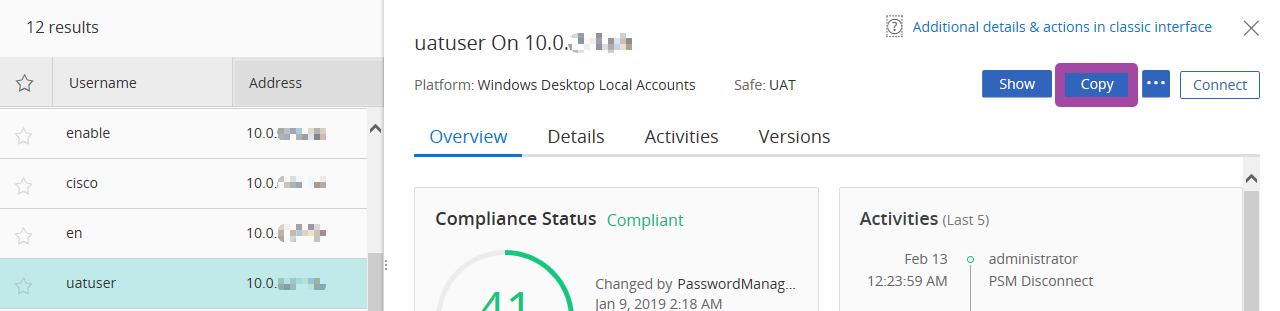


1. Click “Show”



## Copy password

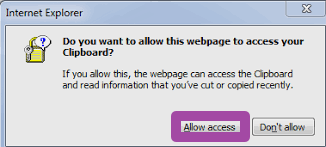
1. Click that target account



Note if Copy button is not shown, click …



1. Click “Copy”
2. Click “Allow access” if IE prompts



\*Other browsers use “Show password” as workaround

1. Password is copied

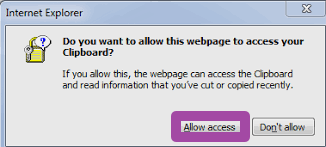


OR

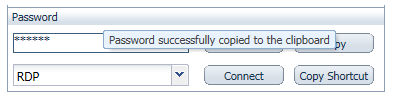
1. Click “Additional details & actions in classic interface”



1. Click “Copy”
2. Click “Allow access” if IE prompts



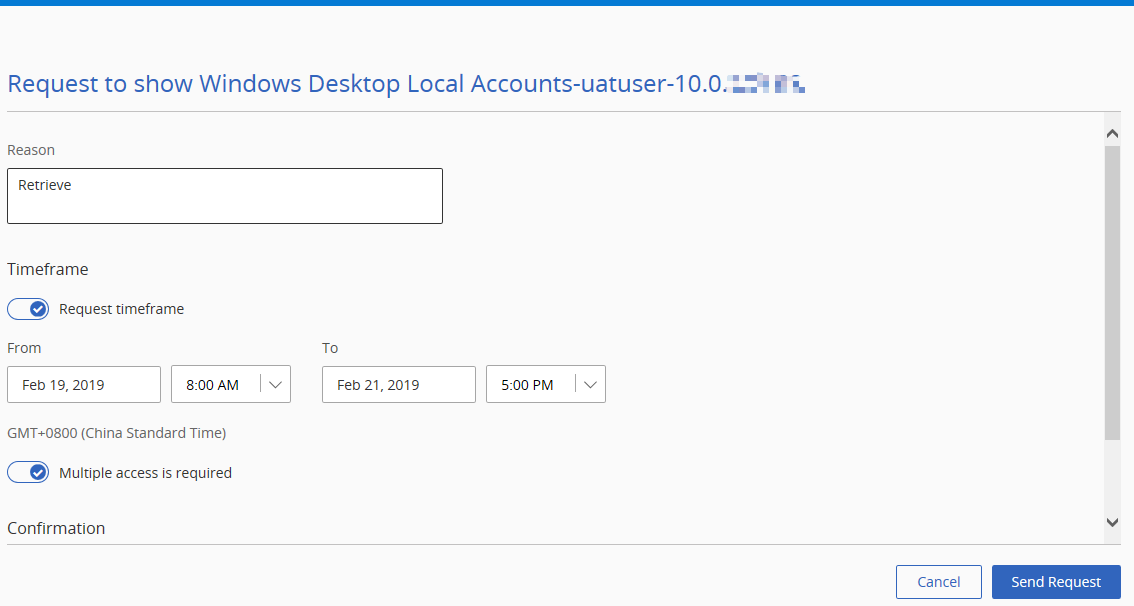
1. Password is copied



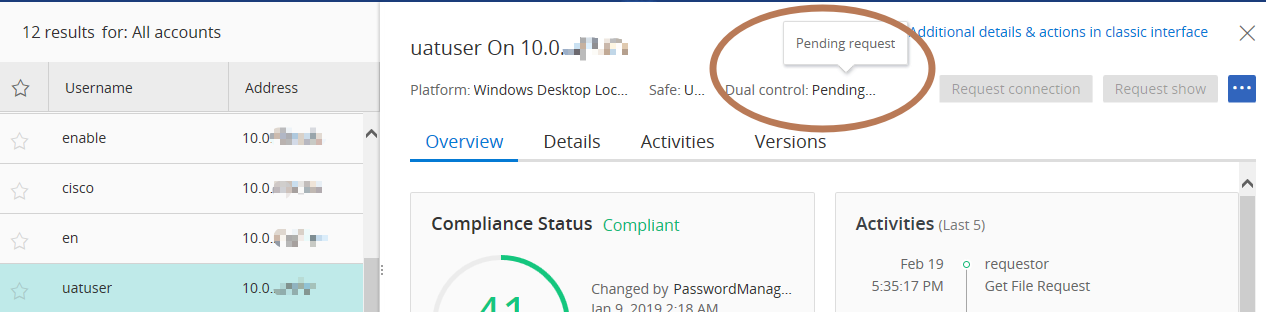
# Request Approval Workflow - Requestor

## Request target account access

1. After search for that account, click it
2. Retrieve account by click “Show” / “Copy”
3. Enter request reason



1. Select timeframe range if needed, note the end time
2. Click “Send Request”
3. Wait for approval



1. “Show/Copy” button would be available when request is approved.

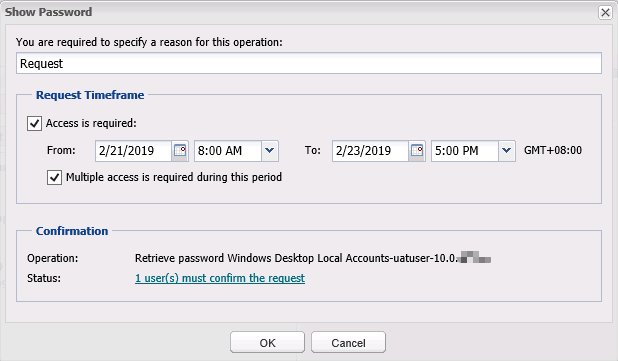
Note you would receive email notification when request is approved.

OR

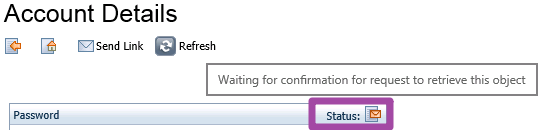
1. Click “Additional details & actions in classic interface”



1. Retrieve account by click “Show” / “Copy”
2. Enter request reason



1. Select timeframe range if needed, note the end time
2. Click “OK”
3. Wait for approval, after click Refresh button,

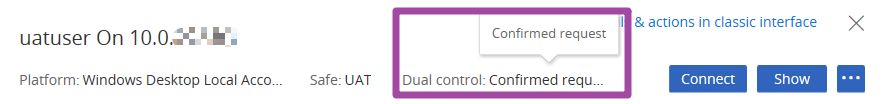


1. “Show/Copy” would be functioning when request is approved.

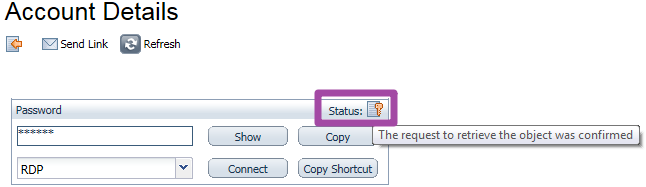
Note you would receive email notification when request is approved.

## Account retrieval after approval confirmation

1. Check status with below icon



OR

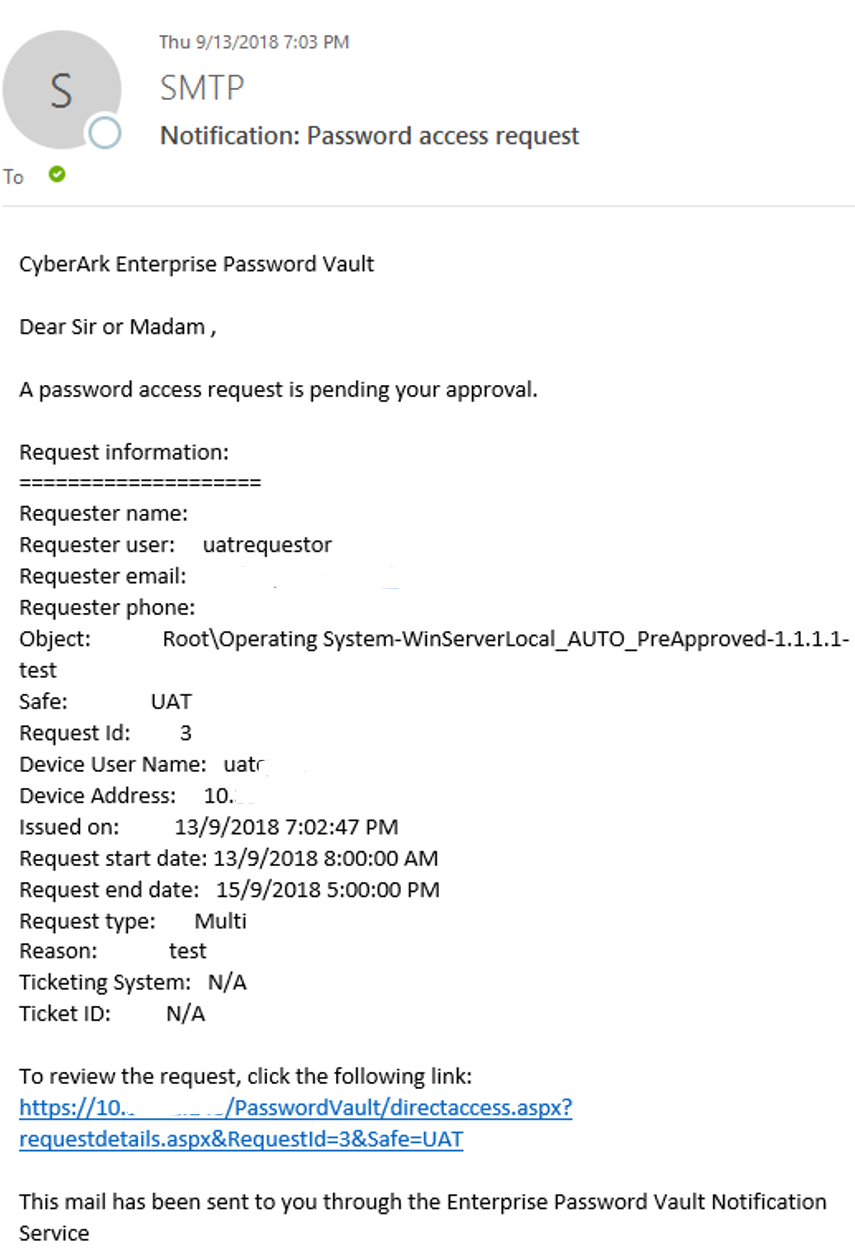


1. Refer to “Account retrieval” section for details

# Request Approval Workflow - Approver

## Approve target account access

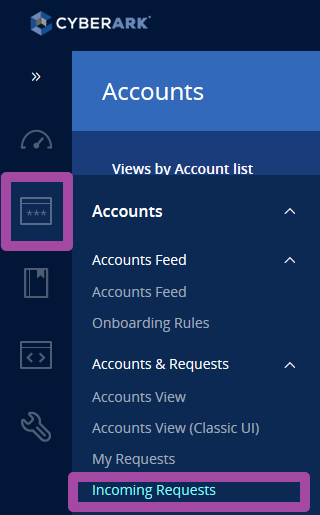
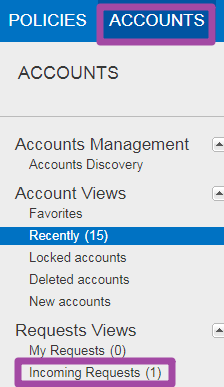
1. Receive email with Privileged Account requests from requestor



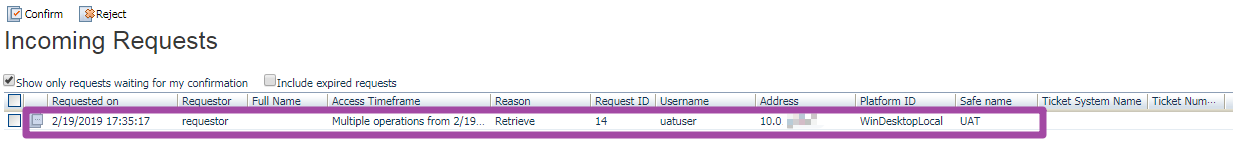
1. Review the details and click the embedded URL to open PVWA, Cyber-Ark Web Portal for approval.
2. Upon the PVWA, Cyber-Ark Web Portal is loaded, logon with LDAP AD account

OR

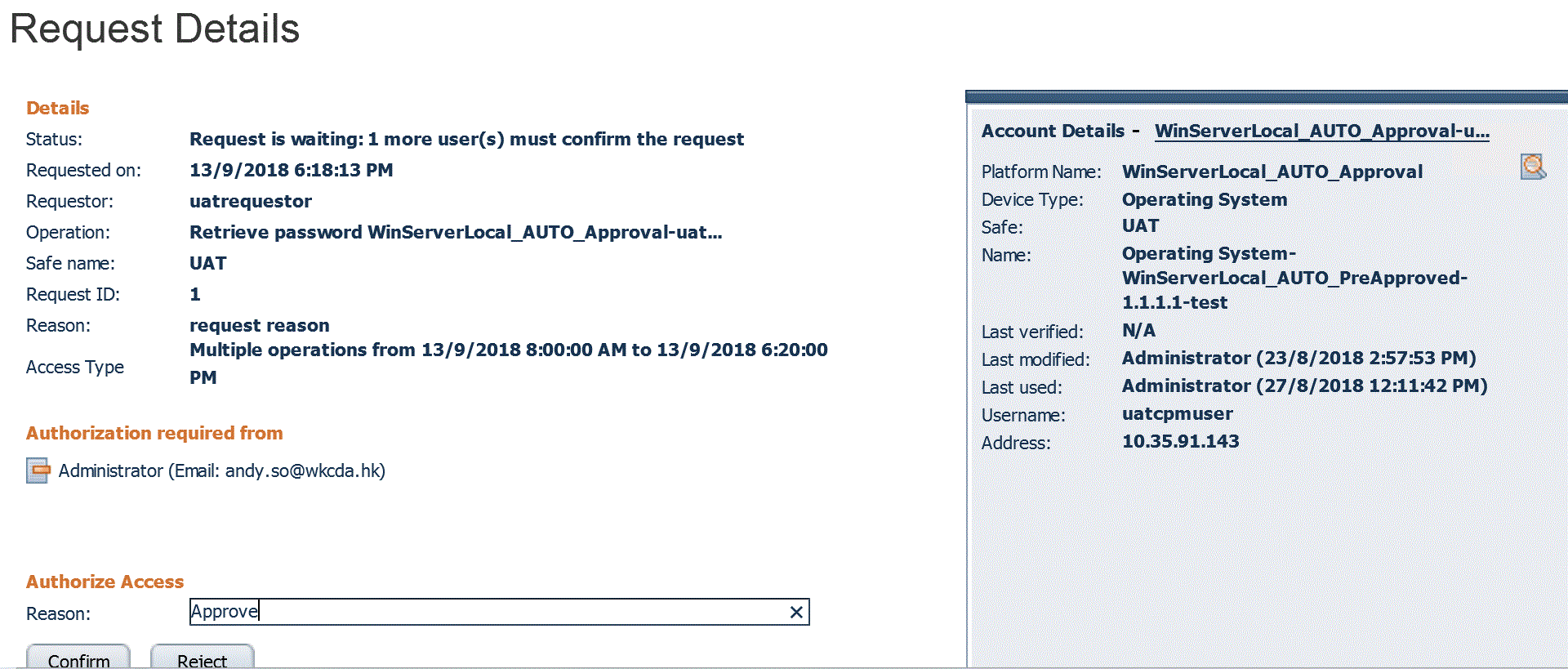
1. Click “Incoming Requests” in the left panel at Account Page.

1. Click that request



1. Enter approval reason



1. Click Confirm

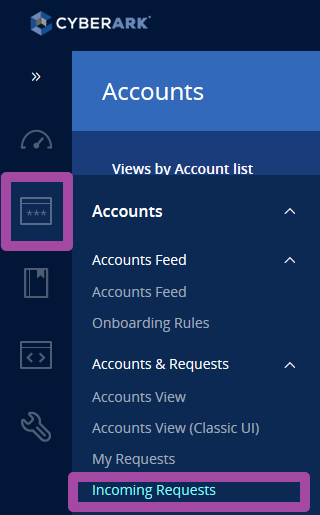
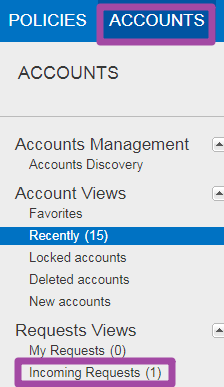
Note that user would receive email notification that the account request is approved with specified reason.

## Reject target account access

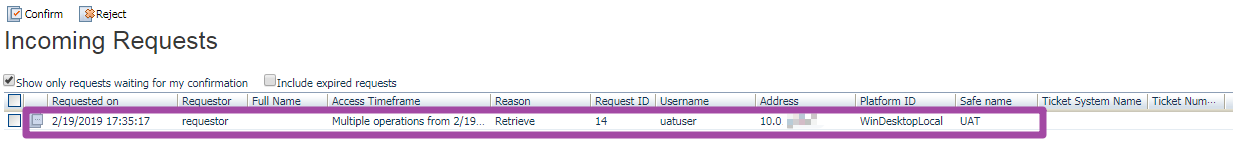
1. Receive email with Privileged Account requests from requestor
2. Review the details and click the embedded URL to open PVWA, Cyber-Ark Web Portal for approval.
3. Upon the PVWA, Cyber-Ark Web Portal is loaded, logon with LDAP AD account

OR

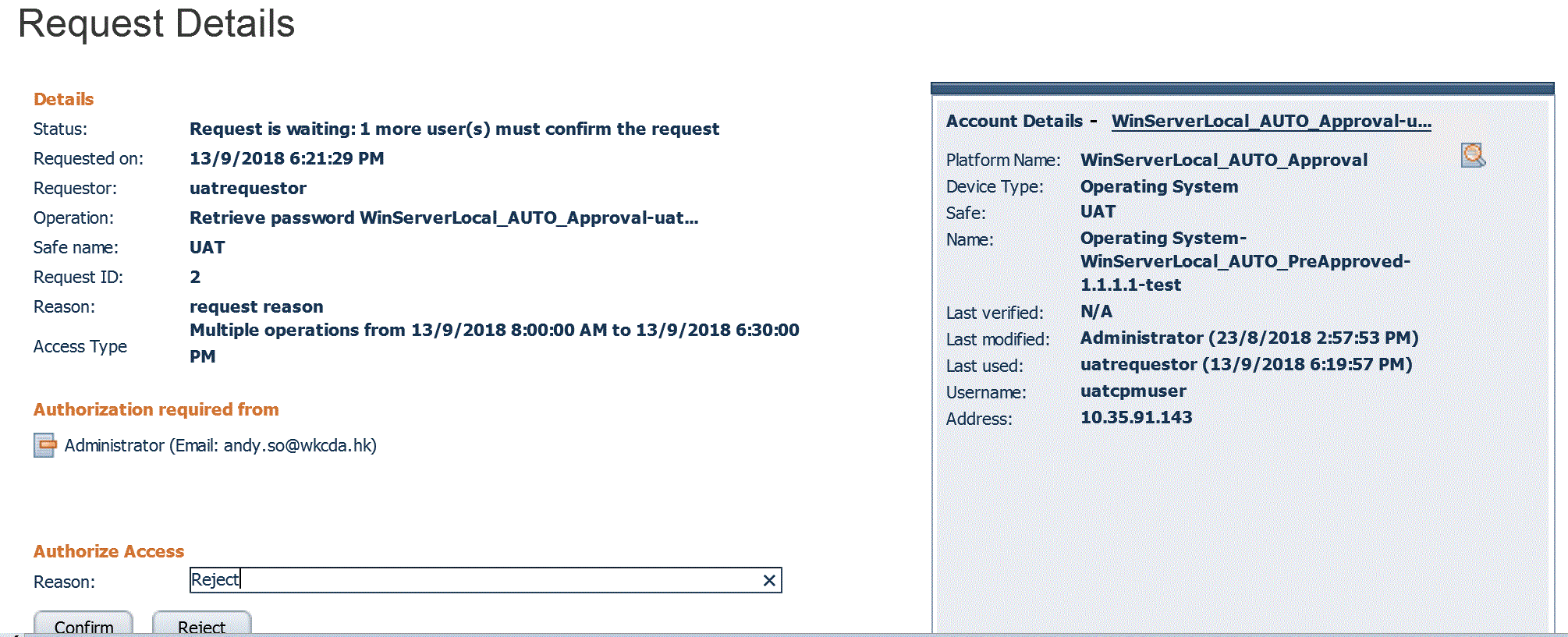
1. Click “Incoming Requests” in the left panel at Account Page.

1. Click that request



1. Enter reject reason



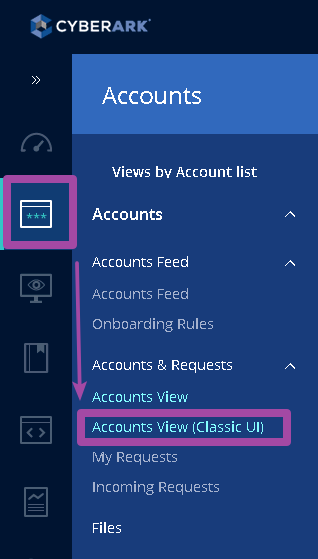
1. Click Reject

Note that user would receive email notification that the account request is rejected with specified reason.

# Account Administration

## Add Account for Supported System

1. Open Internet Explorer and login
2. Click Accounts View (Classic UI)



OR

1. Click “Accounts” Tab, and click “Add Account”



1. Select the appropriate Safe, System, and policy

Note:

For Domain account, select WinDomain related platform

For Server Local account, select WinServerLocal related platform

1. And then fill in the related information

Must be filled in:

Username,

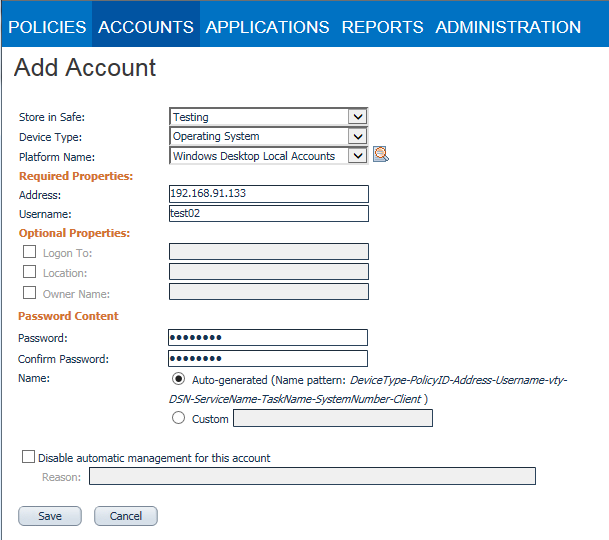
Address,

Password

For certain device, additional info may need to be provided

For example: Cisco one, need to choose ciscouser for main account

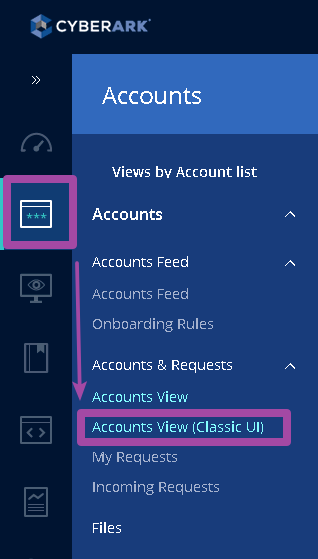
Refer to UAT safe target account as a sample to begin with.



1. Finally clicks “Save” button to complete.

## Add Account for SSH Key

1. Open Internet Explorer and login
2. Click Accounts View (Classic UI)



OR

1. Click “Accounts” Tab, and click “Add SSH Key”



1. Select the appropriate Safe, System, and policy
2. And then fill in the related information

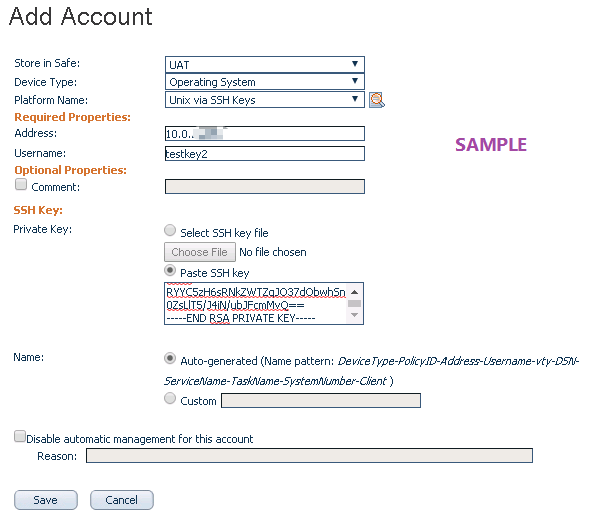
Must be filled in:

Username,

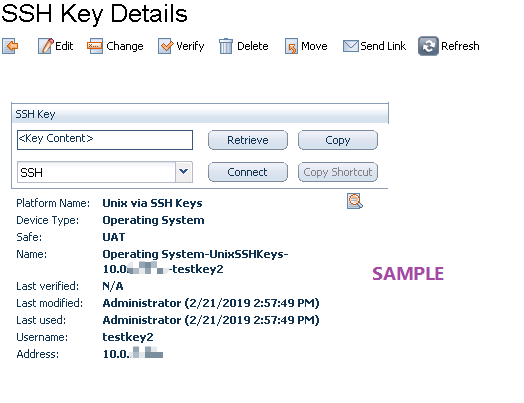
Address,

Password

Refer to UAT safe target account as a sample to begin with.

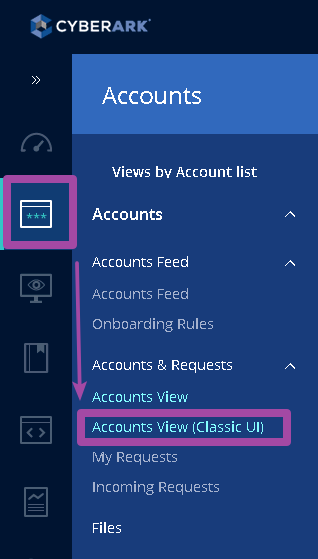


1. Finally clicks “Save” button to complete.



## Associate Account

1. Open Internet Explorer and login
2. Click Accounts View (Classic UI)

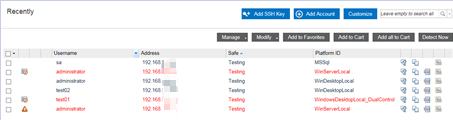


OR

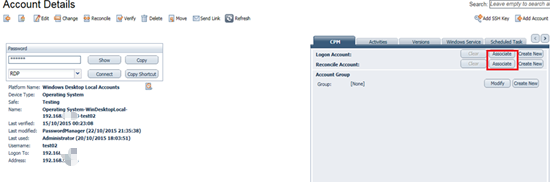
1. Click "Accounts" Tab



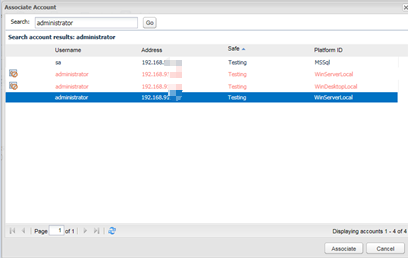
1. Search and click the main account



1. Click on the “Associate” button on the appropriate link type.

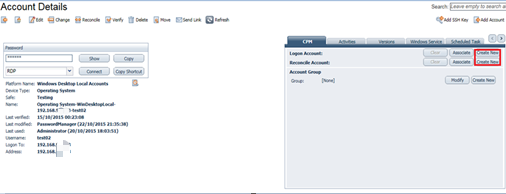


1. Click "Associate" to link with a high privileged account (e.g. Administrator for Windows, root for Unix)



Refer to UAT safe target account as a sample to begin with.

1. If the account is not listed, Click "Cancel" and Click "Create New" to create a reconcile account

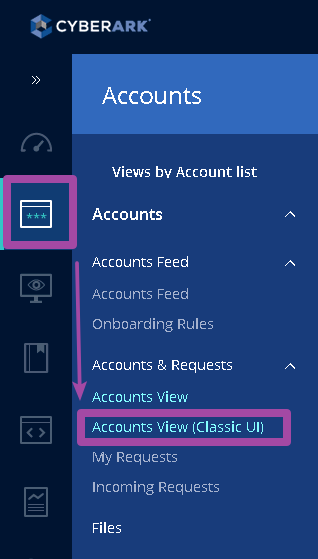


1. Check the password successfully associated



## Un-Associate Account

1. Open Internet Explorer and login
2. Click Accounts View (Classic UI)

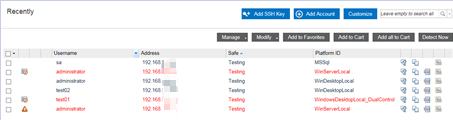


OR

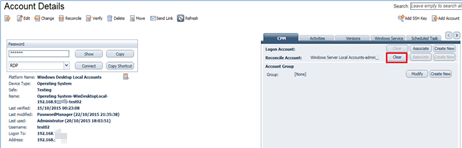
1. Click "Accounts" Tab



1. Search and select the To-Be-Unassociated account

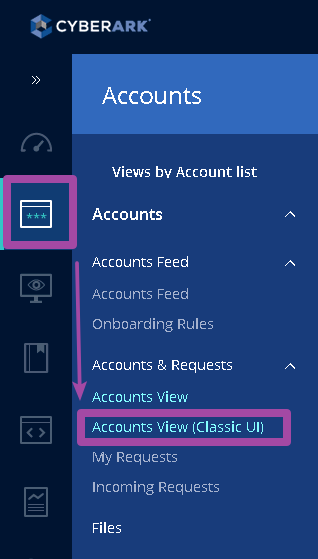


1. Click on the “Clear” button on the appropriate link type.



## Delete Account

1. Open Internet Explorer and login
2. Click Accounts View (Classic UI)

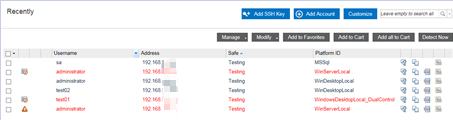


OR

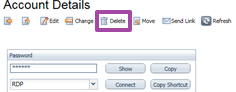
1. Click "Accounts" Tab



1. Search and click the To-Be-Deleted account in PIM



1. Click “Delete” after ensure the Address and username are correct to be deleted



1. Review and Click “OK” when popup “Are you sure want to delete account?”

Note: Depends on the retention period, the account will still visible for a period of time

# Reference

Official Privileged Access Security End-User Guide

- END -