



**CYBERARK®**  
The Identity Security Company™

# PAM Administration

Discovery and  
Onboarding



# Agenda

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

1. Describe the main methods for discovering and onboarding accounts to the system
2. Discover and onboard accounts using **Adding Multiple Accounts from file** and **Accounts Discovery** with **Automatic Onboarding Rules**

# Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- Accounts Discovery & Onboarding Rules
- Continuous Accounts Discovery
- Discovery and Audit (DNA)
- Rest API

# Add a Single Account

### Add Account

✓

Select system type

Windows

✓

Assign to platform

WIN DOM 15


✓

Store in Safe

CyberArk-Service-Accounts

4

Define properties

Last sign in: 12/5/2022 |  mike ▾

#### 4. Define account properties

Primary properties

Address

acme.corp

Username

s-reconcile

Password (optional)

.....

Confirm password

.....

☒ Customize account name ?

Additional properties

Log On To (optional)

acme.corp

User DN (optional)

Cancel

< Back

Add ▾

# Discovery and Onboarding Methods

- Add a single account
- **Add multiple accounts from file**
- Accounts Discovery & Onboarding Rules
- Continuous Accounts Discovery
- Discovery and Audit (DNA)
- Rest API

# Add Multiple Accounts from File

- Frequently there is a need to upload many known accounts from an existing repository
- This is especially valuable during the early stages of implementing **CyberArk PAM**, migrating from another solution, or when onboarding a new department into the **PAM** solution


The screenshot displays the 'Accounts View' interface. At the top right, it shows 'Last sign in: 1/31/2022' and a user profile for 'mike'. Below the title, there is a 'Filter' button and a search bar labeled 'Search for accounts'. To the right of the search bar are two buttons: 'Ad-Hoc connection' and a dropdown menu labeled 'Add account'. The dropdown menu is open, showing an option 'Add accounts from file' which is highlighted with a red box. Below the buttons, it says '37 results for: All accounts' and a link for 'Additional details & actions in classic interface'. The main part of the interface is a table with columns: Status, Username, Address, Platform ID, and actions. The table lists several accounts, including 'cybrreconcile', 'cybrscan', 'root01', 'app-account01', and several 'logon' accounts. Each row has a 'Connect' button and a three-dot menu icon.


Status	Username	Address	Platform ID	Actions
-	cybrreconcile	acme.corp	WINDOMADM1!	Connect ...
-	cybrscan	acme.corp	WINDOMADM1!	Connect ...
-	root01	10.0.0.20	LINKEYS90	Connect ...
-	app-account01	10.0.0.20	LINSSH30	Connect   ...
-	logon01	10.0.0.20	LINSSH30	Connect   ...
-	logon02	10.0.0.20	LINSSH30	Connect   ...
-	logon03	10.0.0.20	LINSSH30	Connect   ...
-	logon04	10.0.0.20	LINSSH30	Connect   ...
-	logon05	10.0.0.20	LINSSH30	Connect   ...
-	logon06	10.0.0.20	LINSSH30	Connect   ...
-	logon07	10.0.0.20	LINSSH30	Connect   ...


# Add Multiple Accounts from File

- You can download a sample CSV file
- Once you have provided the data on the accounts to create, you can then upload the file to the system for processing, either by browsing to the file or using drag & drop

### Add accounts from file


 There are no files being uploaded right now


 [Download a sample CSV file](#)



Upload up to 10,000 accounts

- Safe name and Platform ID are mandatory
- Other properties may be required, depending on the platform policy
- Accounts are created only for existing safes
- You can create only target accounts (not linked or dependent accounts)

 Upload the CSV file

 Drag and drop file or browse

[Cancel](#) [Upload](#)

# Accounts File

- Account parameters to be uploaded to the **Vault** are entered into a text file as Comma Separated Values (CSV)
- Each row represents an account and contains the properties for that account

accounts-Linux.csv - LibreOffice Calc

File Edit View Insert Format Styles Sheet Data Tools Window Help

Liberation Sans 10 pt B I U A % 0.0 0.00 0.00

G25

You are running version 7.0 of LibreOffice for the first time. Do you want to learn what's new?

	A	B	C	D	E	F	G
1	userName	address	safeName	platformID	secret	automaticManagementEnabled	manualManagementReason
2	logon02	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
3	logon03	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
4	logon04	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
5	logon05	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
6	logon06	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
7	logon07	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
8	logon08	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
9	logon09	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	
10	logon10	10.0.0.20	Lin-Fin-US	LINSSH30	Cyberark1	TRUE	



# Limitations

- Linked accounts and dependencies are not supported
- All accounts must be uploaded into existing Safes and groups
- Each file can contain a maximum of 10,000 accounts
- The upload process cannot be cancelled once started
- You must wait for the current file to finish uploading before you can upload another file
- Multiple users cannot upload files at the same time

# Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- **Accounts Discovery & Onboarding Rules**
- Continuous Accounts Discovery
- Discovery and Audit (DNA)
- Rest API

# Accounts Discovery Workflow



## Discover

Continually scan the Windows & Linux environment to detect privileged credentials and accounts



## Onboard

Add all discovered privileged accounts to the pending list to validate privilege



## Manage

Automatically add privileged accounts to be managed and rotated in the digital vault



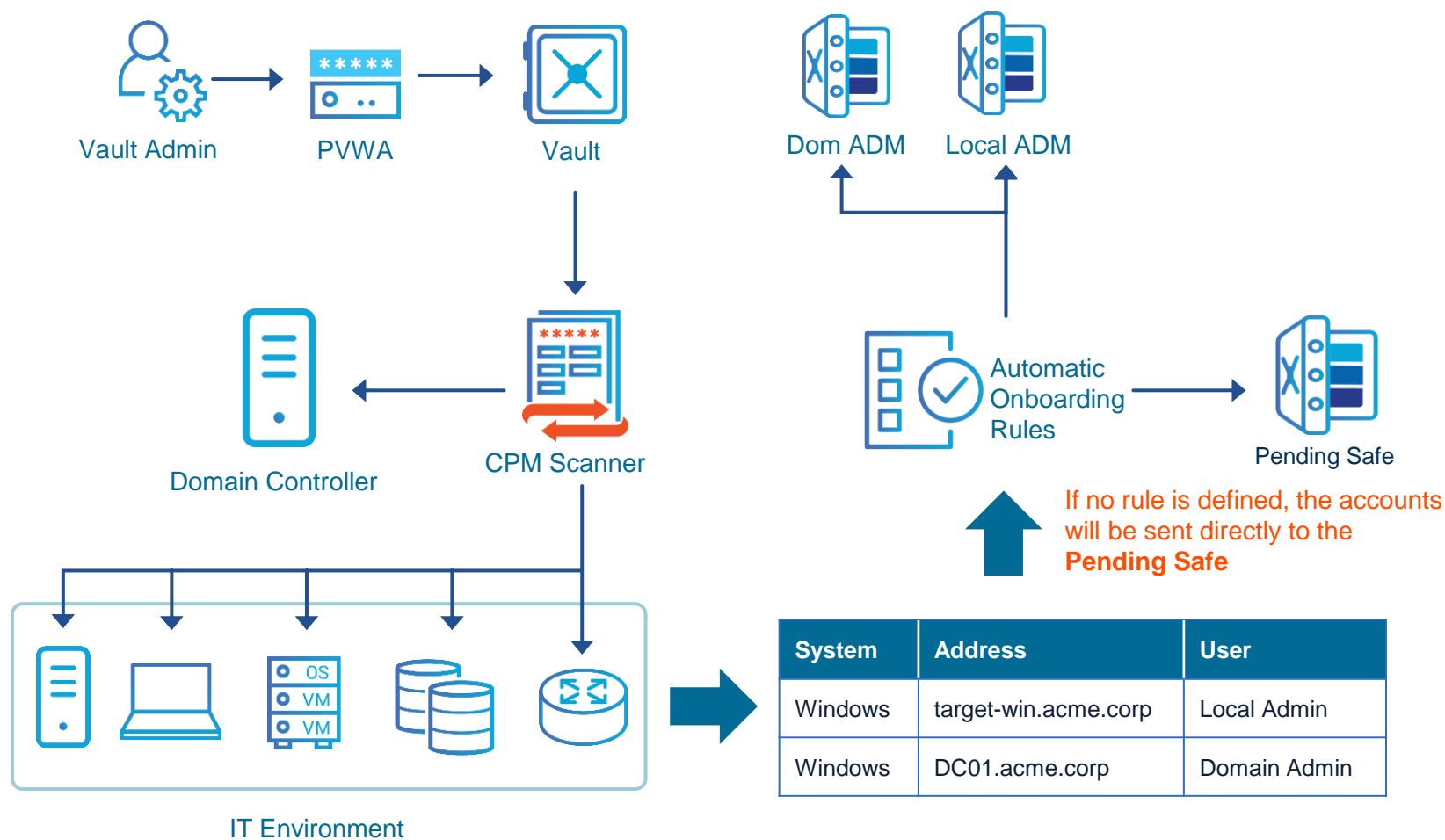
## Onboarding Rules

Minimize the time to onboard accounts and prevents human errors that may occur during manual onboarding

# Windows Discovery Workflow

---

# Windows Discovery



- **Vault Admin** creates the Discovery
- **CPM Scanner** connects to the Vault and collects the task
- **CPM** scans the Directory
- **CPM** authenticates to the targets and scan for Accounts
- Accounts are filtered by the **Automatic Onboarding Rules**
- Accounts which fit a rule are onboarded in the appropriate Safe
- Accounts which do not fit a rule are stored in the **Pending Safe** for manual onboarding

# Running a New Windows Discovery

The screenshot shows the CyberArk Accounts Discovery Management interface. At the top right, it indicates 'Last sign in: 10/7/2022' and a user profile for 'mike'. The breadcrumb trail is 'Accounts > Discovery Management'. The main header has 'ACCOUNTS' on the left and 'Discovery Management' on the right. Below 'ACCOUNTS' is a sidebar with 'Back to Accounts', 'Accounts Discovery', 'Pending Accounts', and 'Discovery Management' (highlighted with a pink box). To the right of the sidebar are two buttons: 'New Unix Discovery' and 'New Windows Discovery' (highlighted with a pink box). A callout box points to the 'New Windows Discovery' button with the text 'Then click **New Windows Discovery**'. Another callout box points to the 'Discovery Management' sidebar item with a list of instructions. On the right side of the interface, there is an 'Introduction to Accounts Discovery Management' section with descriptive text and a note about clicking the discovery buttons.

ACCOUNTS

Accounts > Discovery Management

Discovery Management

Back to Accounts

Accounts Discovery

Pending Accounts

Discovery Management

New Unix Discovery

New Windows Discovery

Then click **New Windows Discovery**

- Go to the **Accounts** tab. Under **Accounts Feed**, click on **Pending & Discovery** and then **Discovery Management**.
- Available to members of the Vault Admins group

Introduction to Accounts Discovery Management

This page displays the Accounts Discovery processes that were created in the system. Accounts Discovery processes are listed here including associated details and statuses.

Click 'New Windows Discovery' or 'New Unix Discovery' to easily initiate a new Accounts Discovery process. Accounts identified during a Discovery process will be listed in the Pending Accounts view.

CYBERARK

# Running a New Windows Discovery

## Information needed for a Windows discovery:

- Domain Name
- Choose if a secure connection will be used to connect to Active Directory
- Scan account

*Continued...*

New Windows Accounts Discovery

Setup

Set discovery from Active Directory

Which account to use for scanning?

Domain:

☒ Connect to the Active Directory using a secure connection

[Click to select an account from the Vault](#)

Introduction to Accounts Discovery

Accounts Discovery is the process of discovering all privileged accounts in your Windows environment and their dependencies.

The process scans all the machines in the given source and discovers all privileged accounts and their dependencies. This scan also retrieves additional information like password age, group association, compliance status, etc.

Cancel Done



# Windows Discovery – Which Account to Use?

The account must:

- Be a domain account
- Have the following permissions:
  - **Read** permissions on the Active Directory
  - Local administrative rights on discovered Windows servers and workstations

Select Account from the Vault

Showing accounts in "acme.corp" domain

Refine by:

Enter keywords

Apply

Username ↕	Safe	Platform
cpm-scan	CyberArk-Service-Accounts	WINDOM15
s-reconcile	CyberArk-Service-Accounts	WINDOM15

Cancel

Select account



# Running a New Windows Discovery

## Information needed for a Windows discovery:

- Domain Name
- Choose if a secure connection will be used to connect to Active Directory
- Scan account
- OU of Servers / Workstations in AD
- CPM to perform the scan
- Whether to run a recurring or one-time discovery

New Windows Accounts Discovery

> Setup

**Set discovery from Active Directory**

> What to scan?

OU to scan: CN=Computers,DC=acme,DC=corp Browse

> Which CPM Scanner to use?

CPM Scanner: ? PasswordManager

> What recurring pattern to set for this discovery?

Recurring Onetime

This discovery will run only ONCE after you finish setting it up.

**Introduction to Accounts Discovery**

Accounts Discovery is the process of discovering all privileged accounts in your Windows environment and their dependencies.

The process scans all the machines in the given source and discovers all privileged accounts and their dependencies. This scan also retrieves additional information like password age, group association, compliance status, etc.

Cancel Done

# Completing the New Discovery

ACCOUNTS Accounts > Discovery Management Discovery Management

Back to Accounts Accounts Discovery Pending Accounts Discovery Management

2 discovery setups

Discovery name	Type	State	Last run time	Last run status
Windows discovery from Compute...	Onetime	Pending	-	-
Windows discovery from Servers...	Onetime	-	11/9/2021 1:24:2...	Completed

Discovery Preview

- Discovery name: Windows discovery from Computers@acme.corp
- Domain: acme.corp
- Communication Type (Port): Secure (636)
- Organizational unit: CN=Computers,DC=acme,DC=corp
- CPM scanner
- Created on: 1/26/2022 8:...
- Created by: mike

At this point you can

- Stop the Discovery
- Delete the Discovery

Delete Stop

The new discovery will be listed on the **Discovery Management** page

The status will be listed as **Pending** until the process starts.

The status will change to **Running** when the process starts

# Windows Discovery Process

- Multiple discoveries from different **CPM Scanners** can run simultaneously
- Accounts found will be categorized as Privileged / Non-Privileged:
  - The categorization is based on the group membership
  - If the account is a member of any Local Administrators group, the account is privileged
  - The account will remain privileged until removed from all machines it was discovered on

Accounts > Pending Accounts

Pending Accounts

44 pending accounts

<input type="checkbox"/>	Username	Address +	Platform	Dependencies	Age (days)	Account category
<input type="checkbox"/>	admin01	acme.corp	Windows Domain	-	656	Privileged
<input type="checkbox"/>	admin02	acme.corp	Windows Domain	-	656	Privileged
<input type="checkbox"/>	admin03	acme.corp	Windows Domain	-	656	Privileged
<input type="checkbox"/>	admin04	acme.corp	Windows Domain	-	656	Privileged
<input type="checkbox"/>	admin05	acme.corp	Windows Domain	-	656	Privileged
<input type="checkbox"/>	Administrator	acme.corp	Windows Domain	-	613	Privileged
<input type="checkbox"/>	john	acme.corp	windows	N/A	-	Privileged
<input type="checkbox"/>	mike	acme.corp	Windows Domain	-	454	Privileged
<input type="checkbox"/>	S-1-5-21-24532...	acme.corp	Windows Domain	-	-	Privileged
<input type="checkbox"/>	vaultadmin01	acme.corp	Windows Domain	-	651	Privileged
<input type="checkbox"/>	vaultadmin02	acme.corp	Windows Domain	-	651	Privileged
<input type="checkbox"/>	vaultadmin03	acme.corp	Windows Domain	-	651	Privileged
<input type="checkbox"/>	vaultadmin04	acme.corp	Windows Domain	-	651	Privileged
<input type="checkbox"/>	vaultadmin05	acme.corp	Windows Domain	-	651	Privileged
<input type="checkbox"/>	Administrator	components.acme.corp	Windows Server Lo...	-	651	Privileged
<input type="checkbox"/>	DefaultAccount	components.acme.corp	Windows Server Lo...	-	-	Non-privileged
<input type="checkbox"/>	Guest	components.acme.corp	Windows Server Lo...	-	-	Non-privileged
<input type="checkbox"/>	PSM-020000000...	components.acme.corp	Windows Server Lo...	-	153	Non-privileged
<input type="checkbox"/>	PSM-020000000...	components.acme.corp	Windows Server Lo...	-	92	Non-privileged

Introduction to Pending Accounts

This page displays the discovered accounts that can be managed by the system.

Go to 'Discovery Management' to easily initiate automatic Accounts Discovery. Accounts identified during Discovery will be listed here. They can be provisioned into the system afterwards using the 'Onboarding' button. Once an account is onboarded, it will no longer appear in the Pending Accounts list.

# Pending Accounts

Accounts that do not match any Onboarding Rule will be listed in **Pending Accounts**

ACCOUNTS

Accounts > Pending Accounts

Pending Accounts

44 pending accounts

Back to Accounts

Accounts Discovery

Pending Accounts

Discovery Management

Refine by

Keywords

Enter keywords

System Type

☐ Windows

☐ Unix

Account Type

☐ Local

☐ Domain

Account Category

☐ Privileged

☐ Non-privileged

Discovered by

☐ CPM Scanner

☐ External source

Clear

Apply

Username

Address +

Platform

Dependencies

Age (days)

Account category

admin01

acme.corp

Windows Domain

-

656

Privileged

admin02

acme.corp

Windows Domain

-

656

Privileged

admin03

acme.corp

Windows Domain

-

656

Privileged

admin04

acme.corp

Windows Domain

-

656

Privileged

admin05

acme.corp

Windows Domain

-

656

Privileged

Administrator

acme.corp

Windows Domain

-

613

Privileged

john

acme.corp

windows

N/A

-

Privileged

mike

acme.corp

Windows Domain

-

454

Privileged

S-1-5-21-24532...

acme.corp

Windows Domain

-

-

Privileged

vaultadmin01

acme.corp

Windows Domain

-

651

Privileged

vaultadmin02

acme.corp

Windows Domain

-

651

Privileged

vaultadmin03

acme.corp

Windows Domain

-

651

Privileged

vaultadmin04

acme.corp

Windows Domain

-

651

Privileged

vaultadmin05

acme.corp

Windows Domain

-

651

Privileged

Administrator

components.acme.corp

Windows Server Lo...

-

651

Privileged

DefaultAccount

components.acme.corp

Windows Server Lo...

-

-

Non-privileged

Guest

components.acme.corp

Windows Server Lo...

-

-

Non-privileged

PSM-020000000...

components.acme.corp

Windows Server Lo...

-

153

Non-privileged

PSM-020000000...

components.acme.corp

Windows Server Lo...

-

62

Non-privileged

Introduction to Pending Accounts

This page displays the discovered accounts that can be managed by

Go to 'Discovery Management' to easily manage Accounts

Click F5 to refresh the list or use the **Refresh** button

The results of these queries are displayed above the list

Various search criteria are available under **Refine by**

# Account Preview

Click on an account to see further details in the **Account Preview** pane.

The screenshot displays the CyberArk Accounts management interface. On the left, a sidebar contains navigation links: 'Back to Accounts', 'Accounts Discovery' (with 'Pending Accounts' selected), and 'Discovery Management'. Below these are filters for 'Refine by', 'Keywords', 'System Type' (Windows, Unix), 'Account Type' (Local, Domain), 'Account Category' (Privileged, Non-privileged), and 'Discovered by' (CPM Scanner, External source). The main area shows '499 pending accounts' in a table. The table has columns: Username, Address, Platform, Dependence, Age (days), and Account category. The row for 'app-account02' is highlighted with a pink border. To the right, the 'Account Preview' pane is expanded for 'app-account02', showing details such as Username, Address, Platform, Age, Last set, Last login date, Account category, UID, Account groups, and Account state.

ACCOUNTS

Accounts > Pending Accounts

Pending Accounts

499 pending accounts

<input type="checkbox"/>	Username	Address	Platform	Dependence	Age (days)	Account category
<input type="checkbox"/>	a8000	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	abrt	10.0.0.20	Unix	N/A	2744	Non-privileged
<input checked="" type="checkbox"/>	app-account02	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account03	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account04	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account05	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account06	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account07	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account08	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account09	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account10	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account11	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account12	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account13	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account14	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account15	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account16	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account17	10.0.0.20	Unix	N/A	2424	Non-privileged
<input type="checkbox"/>	app-account18	10.0.0.20	Unix	N/A	2424	Non-privileged

Account Preview

- > Username  
app-account02
- > Address  
10.0.0.20
- > Platform  
Unix
- > Age (days)  
2424
- > Last set  
6/8/2015
- > Last login date  
-
- > Account category  
Non-privileged
- > UID  
752
- > Account groups  
app-account02
- > GID  
815
- > Discovered by  
PasswordManager
- > Account state  
Enabled
- > Password never expires  
Yes

Activate Windows  
Go to Settings to activate Windows.

Onboard Accounts

# Dependencies

For Windows accounts, the **Dependencies** column shows you if any account is used anywhere else (a **usage**), such as for a Windows service or scheduled task.

ACCOUNTS

Back to Accounts

Accounts Discovery

Pending Accounts

Discovery Management

Refine by

Keywords

sendmail

System Type

Windows

Unix

Account Type

Accounts > Pending Accounts

Pending Accounts

1 result for: 'sendmail'

<input type="checkbox"/>	Username	Address +	Platform	Dependencies	Age
<input type="checkbox"/>	sendmail02	target-win.acme.corp	Windows Serv...	1	4

Dependencies of Pending Account

sendmail02 on target-win.acme.corp

Discovered 1 dependencies

Dependency Name +	Address	Dependency Type
schedtask02	target-win.acme.corp	Windows Scheduled Task

Close

# Onboarding Pending Accounts - 1

Select one or more accounts from the list of Pending accounts and click ***Onboard Accounts***

ACCOUNTS

Accounts > Pending Accounts

Pending Accounts

13 results for: 'admin','Windows','Domain','Privileged'

<input type="checkbox"/>	Username	Address +	Platform	Dependencies	Age (days)	Account category
<input checked="" type="checkbox"/>	admin01	acme.corp	Windows Domain	-	504	Privileged
<input checked="" type="checkbox"/>	admin02	acme.corp	Windows Domain	-	504	Privileged
<input checked="" type="checkbox"/>	admin03	acme.corp	Windows Domain	-	504	Privileged
<input checked="" type="checkbox"/>	admin04	acme.corp	Windows Domain	-	504	Privileged
<input type="checkbox"/>	admin05	acme.corp	Windows Domain	-	504	Privileged
<input type="checkbox"/>	Administrator	acme.corp	Windows Domain	-	461	Privileged
<input type="checkbox"/>	mike	acme.corp	Windows Domain	-	301	Privileged
<input type="checkbox"/>	S-1-5-21-245326...	acme.corp	Windows Domain	-	-	Privileged
<input type="checkbox"/>	vaultadmin01	acme.corp	Windows Domain	-	499	Privileged
<input type="checkbox"/>	vaultadmin02	acme.corp	Windows Domain	-	499	Privileged
<input type="checkbox"/>	vaultadmin03	acme.corp	Windows Domain	-	499	Privileged
<input type="checkbox"/>	vaultadmin04	acme.corp	Windows Domain	-	499	Privileged
<input type="checkbox"/>	vaultadmin05	acme.corp	Windows Domain	-	499	Privileged

4  
Selected accounts

Activate Windows  
Go to Settings to activate Windows

Onboard Accounts

# Onboarding Pending Accounts - 2

Information needed for onboarding accounts:

Onboard Accounts

Onboarding 5 selected accounts

Setup accounts onboarding

The accounts will be onboarded with the related dependencies

Store in Safe:

Win-Dom-Admins

Assign platform:

Windows Domain Admins 15

Password:

☐ Automatically reconcile password

\* Reconcile is currently not set for this platform

☒ Set a default password

Default Password:

.....

Confirm Password:

.....|

Cancel

Onboard

The **Safe** in which these accounts should be stored. You can either choose an existing safe or create a new one

The **Platform** –

- What type of account are these?
- Do they require a separate platform?
- Is reconciliation available?



# Onboarding Pending Accounts - 3

Once onboarded, the new accounts can be found in the **Accounts View**

## Accounts View

Last sign in: 8/26/2021 | mike

Filter | discovery

Ad-Hoc connection | Add account |

10 results for: discovery

Additional details & actions in classic interface










☆	Status	Username	Address	Platform ID	Safe ↑	Access Request	
☆	⚡	discovery01	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery02	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery03	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery04	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery05	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery06	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery07	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery08	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery09	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...
☆	⚡	discovery10	target-win.acme.corp	WINSRVCLCLADM45	Win-Srv-Fin-US	-	Connect ...

# Onboarding Rules



---

# Automatic Onboarding Rules


Minimize the time it takes to onboard and to manage accounts securely, reduce the time spent reviewing pending accounts, and prevent human errors from occurring during manual onboarding



## Onboarding Rules

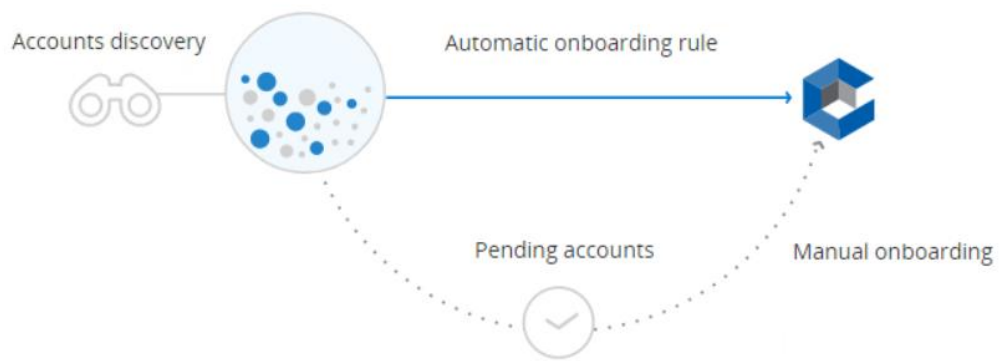
Last sign in: 8/26/2021 |  mike 

Create rule

Updated at: 2:50 AM 

### Fast and easy way for onboarding accounts

Onboarding rules automatically onboard discovered accounts to CyberArk. By applying these rules you can save time and avoid manual onboarding. We apply onboarding rules to discovered accounts, before they are marked as pending. [Read more](#)



```
graph LR; A[Accounts discovery] --> B[Automatic onboarding rule]; B --> C[Manual onboarding]; A -.-> D((Pending accounts)) -.-> C
```

# Onboarding Wizard

An intuitive wizard steps you through each stage of the rule creation process and ensures that each rule is unique

## New onboarding rule

- ✓ Select system type  
WINDOWS
- ✓ Select scope  
Values selected ∨
- ✓ Assign to platform  
Windows Server Local Accounts
- ✓ Store in Safe  
Windows Local Admin
- ✓ Define properties  
Values selected ∨
- 6 Summary

# Onboarding Wizard: Select System Type

Select the type of account to onboard:

- Windows
- \*Nix

## New onboarding rule

Last sign in: 10/3/2022 | mike

1 Select system type

2 Select scope


3 Assign to platform

4 Store in Safe


5 Define properties

6 Summary

### 1. Select system type to onboard

 Windows

Select

 \*NIX

Activate Windows

Go to Settings to activate Windows.

Cancel

Next >

# Onboarding Wizard: Select Scope

- Machine type
- Account type
- Account Category
- Privileged account type
- Optionally, a user or machine name string to match

New onboarding rule Last sign in: 10/3/2022 | mike

✓ Select system type  
Windows

**2 Select scope**

3 Assign to platform

4 Store in Safe

5 Define properties

6 Summary

### 2. Select rule scope

Machine type

Any Server Workstation

Account type ?

Local Domain

Account category ?

Any Privileged Non privileged

Privileged account type

Any Built-in Administrator (SID = 500)

Username (optional)

Begins with ▼ discovery

Machine name / address (optional)

Begins with ▼

Cancel

< Back

Next >

Activate Windows  
Go to Settings to activate Windows.

# Onboarding Wizard: Select Platform

Select the target **Platform** that will be associated with accounts that match this rule

## New onboarding rule

Last sign in: 10/3/2022 | mike

✓ Select system type  
Windows

✓ Select scope  
Values selected

3 Assign to platform

4 Store in Safe

5 Define properties

6 Summary

### 3. Select platform

Filter list by platform name

WIN DOM ADM 15

WIN SVR ADM 45

Select

Cancel

< Back

Next >

Activate Windows  
Go to Settings to activate Windows.

# Onboarding Wizard: Select Safe

Select the **Safe** in which  
the accounts will be stored

New onboarding rule

Last sign in: 10/3/2022 | mike

✓

Select system type

Windows

✓

Select scope

Values selected

✓

Assign to platform

WIN SVR ADM 45

4

Store in Safe

5

Define properties

6

Summary

4. Select Safe

Filter list by Safe name

Win-Srv-Fin-US

Select

Cancel

< Back

Next >

Activate Windows  
Go to Settings to activate Windows.



# Onboarding Wizard: Define Rule Properties

## Define properties of this new rule

- Name
- Description
- Initial password settings

### NOTE

if a reconcile account is associated with the Platform and the parameter **Auto Verify on Add** is set to **Yes**, you can completely automate the onboarding process by having the passwords for these accounts changed immediately and automatically by CyberArk PAM.

### New onboarding rule

Last sign in: 10/3/2022 | mike

✓ Select system type  
Windows

✓ Select scope  
Values selected ▾

✓ Assign to platform  
WIN SVR ADM 45

✓ Store in Safe  
Win-Srv-Fin-US

5 Define properties

6 Summary

#### 5. Define rule properties

Name

Discovery users

Description (optional)

Onboard users beginning with "discovery"

Initial password settings

Using the platform reconcile account

Operating System-WINDOMADM15-acme.corp-s-reconcile

Cancel

< Back

Next >

# New Rule Creation Summary

## New onboarding rule

Last sign in: 10/3/2022 | mike

✓ Select system type  
Windows

✓ Select scope  
Values selected

✓ Assign to platform  
WIN SVR ADM 45

✓ Store in Safe  
Win-Srv-Fin-US

✓ Define properties  
Values selected

6 Summary

### 6. Summary

#### Rule scope

System type	Account category
Windows	Any
Machine type	Privileged account type
Server	Any
Account type	Username
Local	Begins with: discovery

#### Destination

Platform	Safe
WIN SVR ADM 45	Win-Srv-Fin-US

#### Rule properties

Cancel

< Back

Create rule

# New Rule on Rules List

The newly created rule appears in the list of **Onboarding Rules** and is assigned the highest precedence

The screenshot displays the 'Onboarding Rules' management interface. At the top, there's a header with the title 'Onboarding Rules', a user profile 'mike', and a 'Last sign in' timestamp of '8/26/2021'. Below the header, a 'Filter' section allows refining results by 'System type', 'Machine type', 'Account type', and 'Account category'. A 'Create rule' button is visible in the top right. The main area shows a table of rules. The first rule, 'Windows Local Admins', has a precedence of 1. The second rule, 'Discovery Users', has a precedence of 2, which is highlighted with a pink box. To the right of the table, a callout box with the text 'You can edit or delete existing rules' points to the 'Edit rule' and 'Delete rule' buttons, which are also highlighted with a pink box.

**Onboarding Rules**

Last sign in: 8/26/2021 | mike

[Create rule](#) Updated at: 3:44 AM

**Rule scope**

System type: Select Machine type: Select Refine by keyword: Rule name, description, username

Account type: Local Account category: Select

[Apply](#)

2 results

Precedence	Rule name	Description	System type	Machine type	Account type	Last onboard
1	Windows Local Admins	-	Windows	Server	Local	-
2	Discovery Users	-	Windows	Workstation	Local	-

[Edit rule](#) [Delete rule](#)

# Automatic Onboarding Rules - Notes

- **Onboarding Rules** apply to both **Accounts Discovery** and using the **Add discovered accounts** feature of the REST API
- Discovered accounts are automatically processed by the onboarding rules and provisioned in the **Vault**
- Accounts that cannot be processed by any of the rules are added to the **Pending Accounts** list and can be reviewed and onboarded manually
- Automatic Onboarding Rules only apply to accounts without dependencies.
- A new rule takes precedence over an existing rule


# Unix Discovery Workflow

---

# Set Up a New Unix Discovery

ACCOUNTS

Accounts > Discovery Management  
Discovery Management

Last sign in: 1/25/2022 |  mike ▾


Back to Accounts

Accounts Discovery

Pending Accounts

Discovery Management

1 discovery setup

Discovery name	Type	State ▴	Last run time	Last run status
Windows discovery from Servers@acme.corp	Onetime	-	11/9/2021 1:24:25 PM	 Completed

Introduction to Accounts Discovery Management

This page displays the Accounts Discovery processes that were created in the system. Accounts Discovery processes are listed here including associated details and statuses.

Click 'New Windows Discovery' or 'New Unix Discovery' to easily initiate a new Accounts Discovery process. Accounts identified during a Discovery process will be listed in the Pending Accounts view.

New Unix Discovery

New Windows Discovery

# Set Up a New Unix Discovery

## Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password

### New Unix Accounts Discovery

Setup

#### Set discovery from list

> Which file contains the list of machines?

File ?  Browse

> Which user will scan the machines?

Specify the name of a user that will connect to the Unix machines and scan them. The system will search the Vault for the user credentials for each machine in the source list

Username:

> What is the user's default password?

If the system doesn't find matching credentials in the Vault, specify a default password to use

Default password:

#### Introduction to Accounts Discovery


reveal all privileged and non-privileged accounts. For each detected account, additional information is retrieved (e.g., password age, group association, etc.).

All results are displayed in the Pending Accounts page and can be filtered, reviewed and eventually onboarded to the Vault.

Once you finish defining the discovery process, it will be added to the selected scanner queue and will appear in the Discovery Management page where you can track its progress.

CancelDone

© 2023 CyberArk Software Ltd. All rights reserved

 CYBERARK®

# Set Up a New Unix Discovery

## Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password
- CPM Scanner
- Whether or not to scan for SSH Keys

### New Unix Accounts Discovery

> Setup

#### Set discovery from list

> Which CPM Scanner to use?

CPM Scanner ? PasswordManager

> Do you want to discover SSH Keys?

☒ Scan SSH Keys

For information about orphan private SSH keys and passphrase keys found during the discovery, refer to the discovery log file.

> What recurring pattern to set for this discovery?

Recurring Onetime

Recur on: ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday

#### Introduction to Accounts Discovery

reveal all privileged and non-privileged accounts. For each detected account, additional information is retrieved (e.g., password age, group association, etc.).

All results are displayed in the Pending Accounts page and can be filtered, reviewed and eventually onboarded to the Vault.

Once you finish defining the discovery process, it will be added to the selected scanner queue and will appear in the Discovery Management page where you can track its progress.

Cancel Done



# Set Up a New Unix Discovery

## Information needed for running a Unix Discovery

- CSV file containing IP addresses of Unix/Linux machines
- Unix user to perform the scan and get the accounts
- A default password
- CPM Scanner
- Whether or not to scan for SSH Keys
- Recurring or One-time

### New Unix Accounts Discovery

> Setup

#### Set discovery from list

For information about orphan private SSH keys and passphrase keys found during the discovery, refer to the discovery log file.

> What recurring pattern to set for this discovery?

RecurringOnetime

Recur on:

☐ Monday☐ Tuesday☐ Wednesday☐ Thursday☐ Friday☐ Saturday☐ Sunday

Starting: ?

12

:

00

☒ AM☐ PM

#### Introduction to Accounts Discovery

reveal all privileged and non-privileged accounts. For each detected account, additional information is retrieved (e.g., password age, group association, etc.).

All results are displayed in the Pending Accounts page and can be filtered, reviewed and eventually onboarded to the Vault.

Once you finish defining the discovery process, it will be added to the selected scanner queue and will appear in the Discovery Management page where you can track its progress.

CancelDone

# Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- Accounts Discovery & Onboarding Rules
- **Continuous Accounts Discovery**
- Discovery and Audit (DNA)
- Rest API

# Continuous Accounts Discovery by the PTA

Continuous accounts discovery via log-in events for:

- Windows
- UNIX-like
- Oracle
- AWS
- Azure
- Other

Continuous discovery via group membership for Windows Accounts

## Detections by PTA

12:16:43 PM  
30 MEDIUM

### Unmanaged privileged account Initiated remediation

An account `backdoor@vfserver.cyber-ark-demo.local` was added to a local privileged group `Administrators`, on `vfserver.cyber-ark-demo.local`, although this account is not managed in CyberArk PAS.



Unmanaged privileged account  
`backdoor@vfserver.cyb...`




Target machine  
`vfserver.cyber-ark-dem...`

### Recommendation

Onboard the newly discovered account, and assign the appropriate platform to securely manage the account. Discovered accounts that are filtered by an automatic onboarding rule do not require manual action.

# Continuous Account Discovery: Login Events

- **CyberArk Privileged Threat Analytics** detects unmanaged privileged access events
- The **PTA** can detect when a connection to a machine or a cloud service is made with a privileged account that is **not stored** in the **Vault** and automatically onboard the account
- This detection is supported out of the box for **Windows**, **UNIX**, **AWS**, and **Azure** accounts
- Other platforms can be supported by building custom plug-ins for **PTA**

Jan 31	Today
10:53:57 AM MEDIUM	<p><b>Unmanaged privileged account</b> Privileged account <code>root04@target-lin</code> was used to access <code>target-lin</code>, although this account is not managed in CyberArk PAS.</p> <div><p>Unmanaged privileged account <code>root04@target-lin</code></p><p>Target machine <code>target-lin</code></p></div> <p><b>Recommendation</b> Consider onboarding the unmanaged privileged account to CyberArk PAS.</p>

# Continuous Account Discovery: Group Membership

- The **PTA** continuously monitors **Windows Local Administrator** groups
- Faster response time
- Automatic response



Nov 23 2021

8:35:52 AM  
MEDIUM


Tuesday

Unmanaged privileged account Initiated remediation

An account john@acme.corp was added to a local privileged group Administrators, on target-win.acme.corp, although this account is not managed in CyberArk PAS.

Unmanaged privileged account  
john@acme.corp



Target machine  
target-win.acme.corp

Recommendation

Onboard the newly discovered account, and assign the appropriate platform to securely manage the account. Discovered accounts that are filtered by an automatic onboarding rule do not require manual action.

ID 619cab2bc2dc61e19a942a1a

Close

# Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- Accounts Discovery & Onboarding Rules
- Continuous Accounts Discovery
- **Discovery and Audit (DNA)**
- Rest API

# Discover and Audit (DNA)

## Upload accounts from DNA data file

### Import DNA data file

C:\Users\Administrator\Desktop\DNA.db

Browse

### PVWA connection details

User

administrator

Password

••••••••

PVWA URL

https://ServerName.com/PasswordVault/



Only accounts with no dependencies are uploaded.  
When automatic onboarding rules are enabled,  
they will apply to the uploaded accounts.

### Select the accounts to upload

☒ Windows local accounts (6)

☐ Unix local accounts (0)

☐ All domain accounts (20)

Cancel

Upload

# Discovery and Onboarding Methods

- Add a single account
- Add multiple accounts from file
- Accounts Discovery & Onboarding Rules
- Continuous Accounts Discovery
- Discovery and Audit (DNA)
- **Rest API**



# PAM Web Services API

- The **PAM Web Services API** is a set of REST- based services running on the **PVWA** that allow scripts and applications to communicate with the **Vault**.
- It is used by **CyberArk** applications as well as third-party applications, allowing organizations to develop custom interactions with the **Vault** to automate business processes.

## EXAMPLE:

Integrating the process of adding a new Windows machine to the company's network with automatic provisioning of the target server local Administrator account in the **Vault**



# Onboarding Rest Methods

There are three main REST methods that are relevant for the process of onboarding accounts:

1. Add account
2. Add discovered accounts
3. Create bulk upload of accounts

The screenshot shows the CyberArk Privileged Access Manager documentation page for the 'Accounts' REST API section. The page has a dark blue header with the CyberArk logo and 'Privileged Access Manager' text. A search bar is located in the top right corner. Below the header, a breadcrumb trail reads 'Home > Developer > REST APIs > Accounts'. On the right side of the header, there are links for 'Highlights', 'Expand all', 'Print', 'Previous', and 'Next'. Below the breadcrumb, there is a 'Was this topic helpful?' section with thumbs up and down icons. The main content area is divided into two columns. The left column contains a table of contents with links to 'User management', 'LDAP Integration', 'Safes', 'Session Management', 'Platforms', 'Accounts' (expanded), 'Bulk upload of accounts', 'Update account', 'Delete account', 'Account groups', 'Account actions', and 'Discovered accounts'. The right column contains the 'Accounts' section header, a description of the REST APIs for managing accounts, and a list of API endpoints. The endpoints listed are: 'Get accounts', 'Get account details', 'Get account activity', 'Get secret versions', 'Add account', 'Bulk upload of accounts', 'Update account', 'Delete account', 'Account groups', 'Account actions', 'Discovered accounts', and 'Linked accounts'. The 'Add account', 'Bulk upload of accounts', and 'Discovered accounts' endpoints are highlighted with red rectangular boxes. A 'Send feedback' button is located on the far right side of the page.

**CYBERARK** Privileged Access Manager

Search the docs

Home > Developer > REST APIs > Accounts

Highlights | Expand all | Print | Previous | Next >

Was this topic helpful?

## Accounts

This section includes REST APIs for managing accounts, account groups, account activities, and discovered accounts.

In this section:

- [Get accounts](#)
- [Get account details](#)
- [Get account activity](#)
- [Get secret versions](#)
- [Add account](#)
- [Bulk upload of accounts](#)
- [Update account](#)
- [Delete account](#)
- [Account groups](#)
- [Account actions](#)
- [Discovered accounts](#)
- [Linked accounts](#)

Send feedback

# Add Account

The **Add Account** method will be used when the target **Safe** and **Platform** are known to the onboarding utility

Home > Developer > REST APIs > Accounts > Add account

Highlights | Expand all | Print | Previous | Next

Was this topic helpful?

Send feedback

> End user  
> Administrator  
▼ Developer  
    ▼ REST APIs  
        > Authentication  
        > Server  
        > System Health  
        > User management  
        > LDAP Integration  
        > Safes  
        > Session Management  
        > Platforms  
    ▼ Accounts  
        Get accounts  
        Get account details  
        Get account activity  
        Get secret versions  
        Add account

## Add account

This method adds a new privileged account or SSH key to the Vault.

**Note:**  
Make sure there are no spaces in the URL.  
The following characters are not supported in URL values: + & %

Select the method you want to use:

2nd gen API (recommended) ^

To run this web service, you must have the following permission in the Vault:

- Add account
- Update password or Update password properties

**Note:**  
You require an additional license to add SSH keys to the Vault. For more information, contact your CyberArk representative.

URL

`https://<IIS_Server_Ip>/PasswordVault/api/Accounts`

# Add Discovered Accounts

CyberArk discovery and upload mechanisms, as well as third-party discovery mechanisms, will use the **Add Discovered Accounts** method in order to upload discovered accounts (and dependencies) to the Pending Safe or onboard the accounts directly via automatic onboarding rules.



# Create Bulk Upload of Accounts

- The **Create bulk upload of accounts** method is used to upload multiple accounts to existing Safes
- It is also used when adding multiple accounts from a file via the **PVWA** Web UI

The screenshot shows the CyberArk Privileged Access Manager documentation interface. The header includes the CyberArk logo, the product name 'Privileged Access Manager', a search bar, and navigation links. The breadcrumb trail is: Home > Developer > REST APIs > Accounts > Bulk upload of accounts > Create bulk upload of accounts. A left-hand navigation menu lists various topics, with 'Accounts' expanded to show 'Create bulk upload of accounts' as the selected item. The main content area features a title 'Create bulk upload of accounts' in a pink-bordered box, followed by a description: 'This method allows a developer to add multiple accounts to existing Safes. The response contains the ID of the bulk account upload that was performed.' Below this is a 'Note' box stating that the option is only available with specific permissions. The 'URL' section provides the endpoint: `https://{PVWA_SERVER}/passwordvault/api/bulkactions/accounts`. Another 'Note' box advises ensuring no spaces are in the URL and lists unsupported characters: + & %.

**CYBERARK** Privileged Access Manager

Search the docs

Our Products

Home > Developer > REST APIs > Accounts > Bulk upload of accounts > Create bulk upload of accounts

Highlights | Expand all | Print | Previous | Next

Was this topic helpful?

**Create bulk upload of accounts**

This method allows a developer to add multiple accounts to existing Safes. The response contains the ID of the bulk account upload that was performed.

**Note:**

This option is only available if you have **Add accounts**, **Update account content**, and **Update account properties** authorization in at least one Safe.

**URL**

`https://{PVWA_SERVER}/passwordvault/api/bulkactions/accounts`

**Note:**

Make sure there are no spaces in the URL.

The following characters are not supported in URL values: + & %

**In this topic**

- URL
- Resource information
- Header parameter
- Body parameters
- Result

Send feedback

# Summary

---



# Summary

In this session we covered:

- The main methods for discovering and onboarding accounts to the system
- How to configure Adding Accounts from a file and run Accounts Discovery
- Configure Automatic Onboarding Rules



# Additional Resources



## Other resources to consider

[PowerShell module for CyberArk Privileged Account Security Web Service RestAPI](#)

## You may now complete the following exercises:

### *Discovery and Onboarding*

- Configure Automatic Onboarding Rules
- Configure and Run Windows Accounts Discovery
- Manually onboard discovered accounts
- Add multiple accounts from file