



PAM Administration

Discovery and Onboarding Part 2



Agenda

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

- Add multiple accounts from a file
- Describe the main capabilities of **Continuous Accounts Discovery via PTA**
- Describe the main capabilities of onboarding accounts via the **REST API**

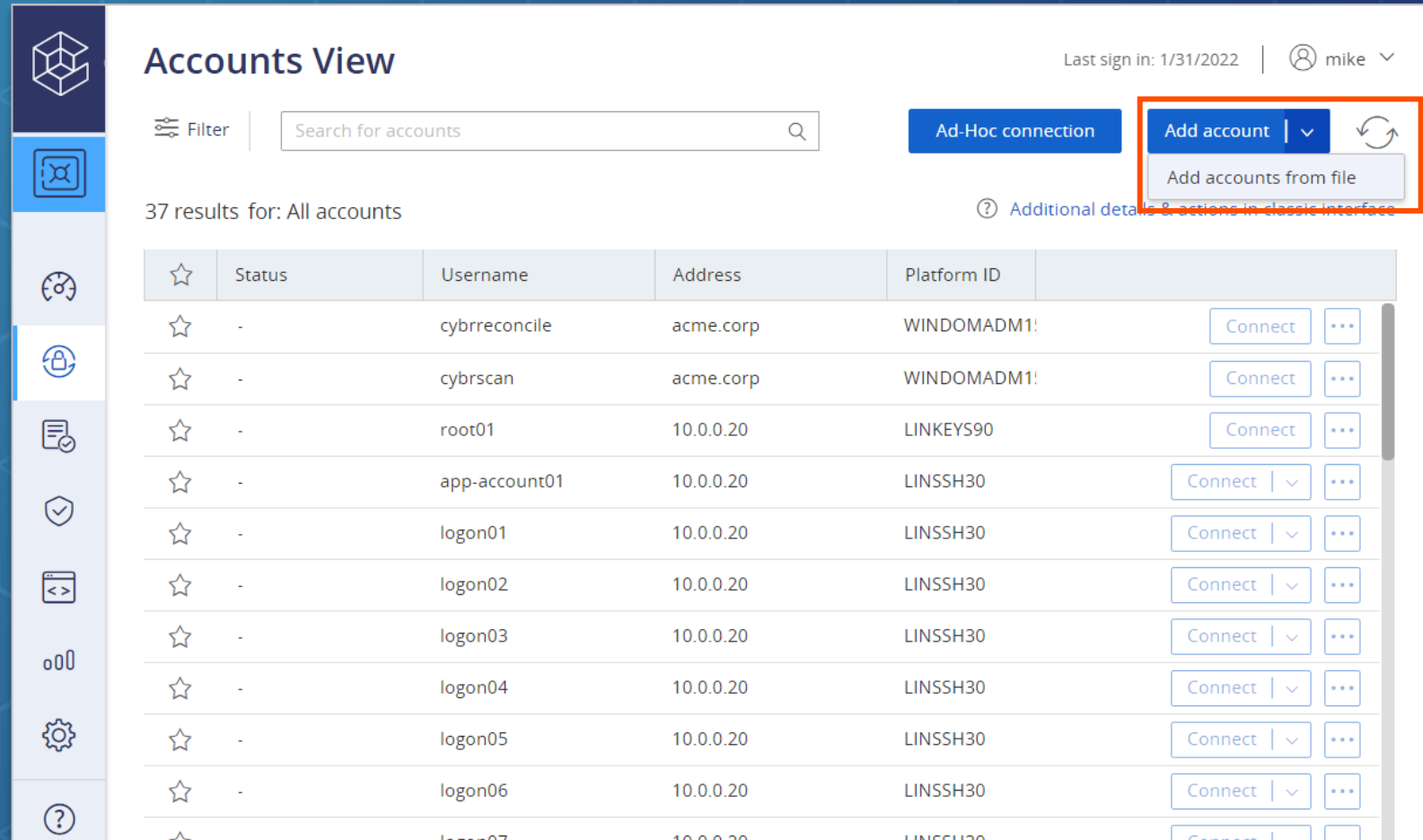


Add Multiple Accounts From File



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 in CyberArk. The top navigation bar includes the CyberArk logo, a filter icon, a search bar labeled 'Search for accounts', and buttons for 'Ad-Hoc connection', 'Add account' (with a dropdown arrow), and a refresh icon. The 'Add account' dropdown menu is highlighted with a red box, showing the option 'Add accounts from file'. Below the navigation bar, the text '37 results for: All accounts' is displayed. A table lists the accounts with columns for Status, Username, Address, and Platform ID. Each row has a 'Connect' button and a three-dot menu icon.


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





Add Multiple Accounts from File

- You can download a sample CSV file
- Once completed, 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

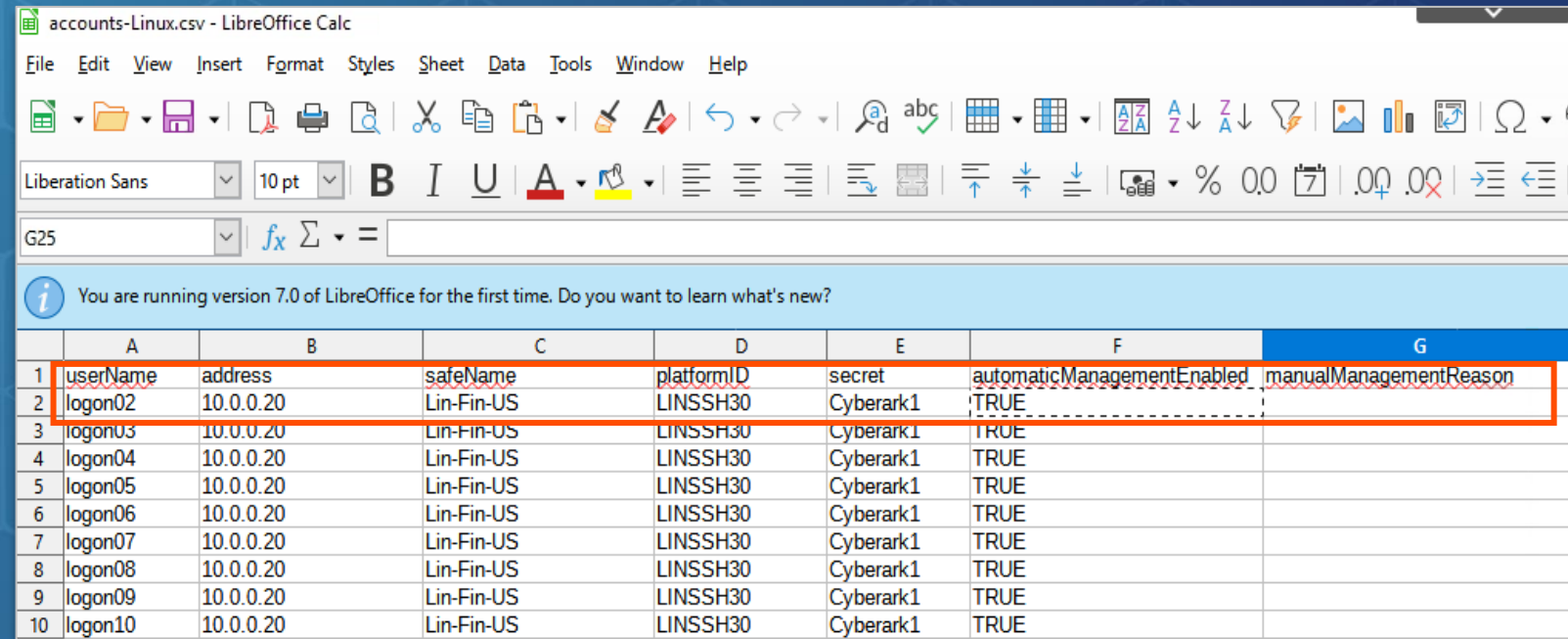
 Drag and drop file or browse

[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 \sum =

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



Continuous Account Discovery

- Continuous accounts discovery via log-in events for:
 - Windows
 - UNIX-like
 - Oracle
 - AWS
 - Azure
 - Other
- Continuous discovery via group membership for Windows Accounts






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

Unmanaged privileged account
root04@target-lin


Target machine
target-lin

Recommendation

Consider onboarding the unmanaged privileged account to CyberArk PAS.




Continuous Account Discovery: Group Membership

- The **PTA** continuously monitors **Windows Local Administrator** groups to identify when users are added to these privileged groups. As soon as an account is granted privileged permissions, the **PTA** responds with an alert and can take control of this unmanaged privileged account
- This shortens the time it takes to detect an attacker or a malicious insider who attempts to create a backdoor account, bypassing the organizational policy

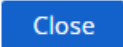
Nov 23 2021




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.

ID 619cab2bc2dc61e19a942a1a 

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.





Continuous Discovery Demonstration



Name

Local Data Source

- admin01\centos01
- Administrator\VFSERVER
- root01\centos01

Administrator\VFSERVER

Actions



Open Session



New Entry



Properties

Overview

Macros/Scripts/Tools

Management Tools

Information

Attachments



Administrator\VFSERVER

RDP (Microsoft Remote Desktop)

HOST comp01a.cyber-ark-demo.local

USERNAME Bill

DOMAIN cyber-ark-demo

Rest API

- Add discovered accounts
- Add account
- Create bulk upload of accounts



PAM Web Services API

- The **PAM Web Services API** is a set of REST-based calls that are installed 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

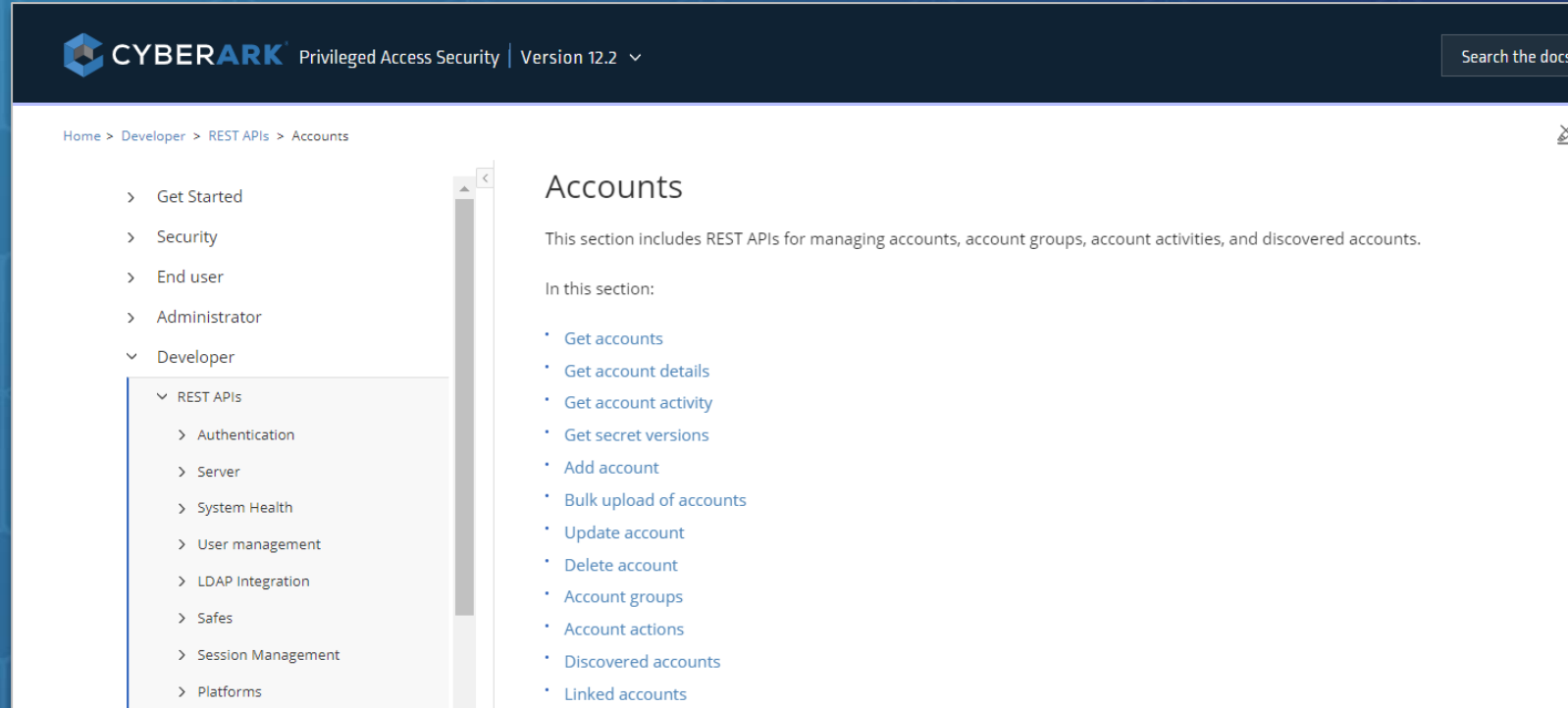
EXAMPLE: Integrating the process of adding a new Windows machine to the company's network with automatic provisioning of the target server local Administrator account in the **Vault**



Onboarding Rest Methods

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

- Add account
- Add discovered accounts
- Create bulk upload of accounts



The screenshot shows the CyberArk Privileged Access Security documentation interface. The top navigation bar includes the CyberArk logo, the product name "Privileged Access Security", the version "Version 12.2", and a search bar labeled "Search the docs". The breadcrumb trail indicates the current location: "Home > Developer > REST APIs > Accounts". A left-hand sidebar contains a tree view of the documentation structure, with "REST APIs" expanded to show sub-categories like Authentication, Server, System Health, User management, LDAP Integration, Safes, Session Management, and Platforms. The main content area is titled "Accounts" and provides an overview of the REST APIs for managing accounts, account groups, account activities, and discovered accounts. It lists the following methods 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, and Linked accounts.

CYBERARK Privileged Access Security | Version 12.2 Search the docs

Home > Developer > REST APIs > Accounts

Accounts

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

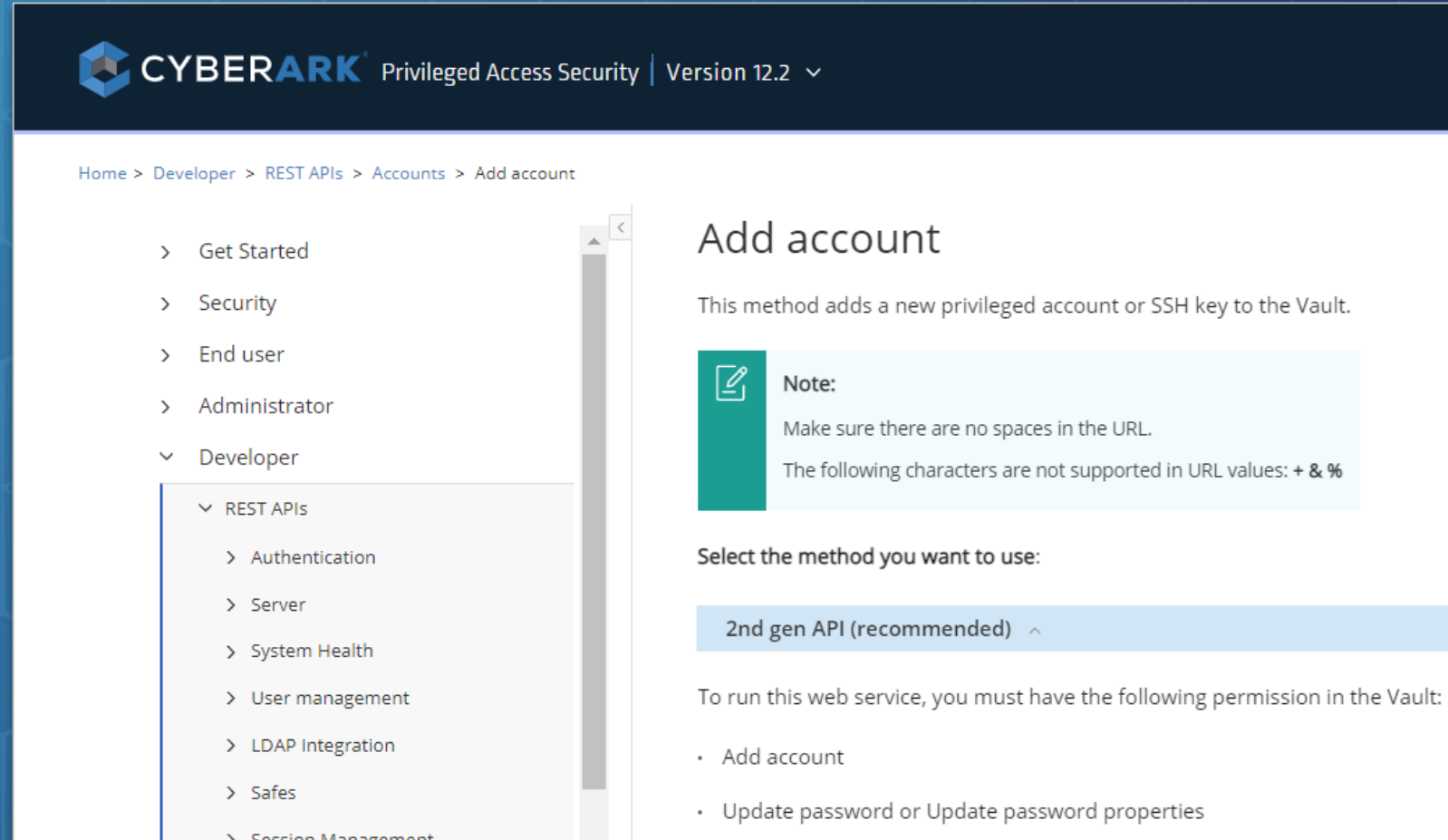
In this section:

- [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](#)



Add Account

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



The screenshot displays the CyberArk Privileged Access Security interface. At the top, the header shows the CyberArk logo, the product name 'Privileged Access Security', and the version 'Version 12.2'. Below the header, a breadcrumb trail reads 'Home > Developer > REST APIs > Accounts > Add account'. On the left, a navigation menu is visible with categories: 'Get Started', 'Security', 'End user', 'Administrator', and 'Developer'. The 'Developer' category is expanded, showing a sub-menu with 'REST APIs' selected. Under 'REST APIs', several options are listed: 'Authentication', 'Server', 'System Health', 'User management', 'LDAP Integration', 'Safes', and 'Session Management'. The main content area on the right is titled 'Add account'. It contains a note stating: 'This method adds a new privileged account or SSH key to the Vault.' Below the note, a section titled 'Select the method you want to use:' shows '2nd gen API (recommended)' as the selected option. At the bottom, it specifies the required permission for running this web service: 'Add account' and 'Update password or Update password properties'.

CYBERARK Privileged Access Security | Version 12.2

Home > Developer > REST APIs > Accounts > Add account

- > Get Started
- > Security
- > End user
- > Administrator
- ▼ Developer
 - ▼ REST APIs
 - > Authentication
 - > Server
 - > System Health
 - > User management
 - > LDAP Integration
 - > Safes
 - > Session Management

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



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 Security (PAS) REST API documentation page for the 'Create bulk upload of accounts' method. The page is titled 'Create bulk upload of accounts' and includes a breadcrumb trail: Home > Developer > REST APIs > Accounts > Bulk upload of accounts > Create bulk upload of accounts. The main content area is highlighted with a red border and contains the following information:

- 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: + & %



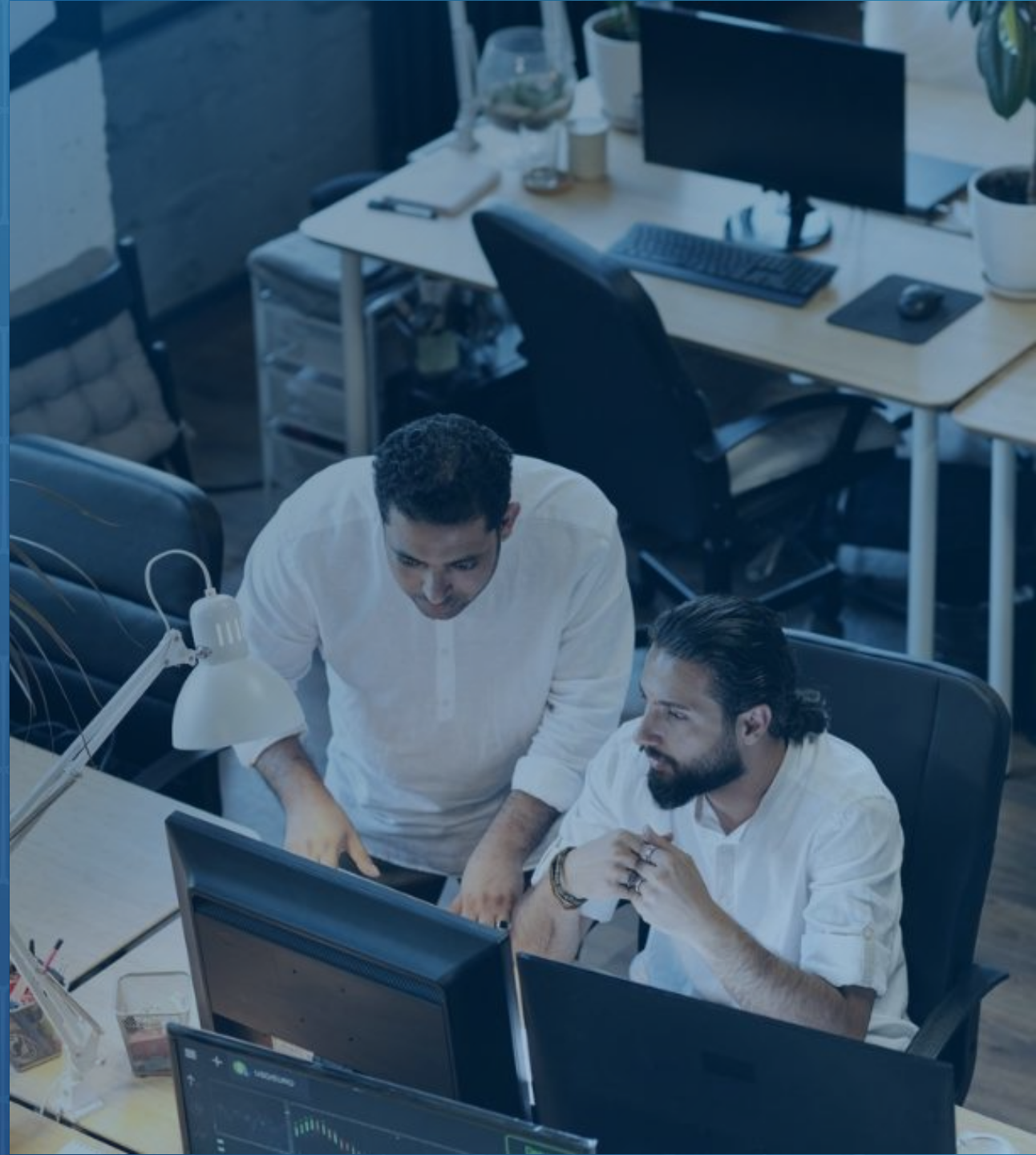
Summary



Summary

In this session we covered:

- ✔ How to add multiple accounts from file
- ✔ Continuous Account Discovery via PTA
- ✔ Onboarding via REST API



Additional Resources



Utilities

PowerShell module for CyberArk
Privileged Account Security Web Service
RestAPI*

You may now complete the following exercises:

Discovery and Onboarding

- Add multiple accounts from file