



PAM Administration

Dependent Platforms



Agenda

By the end of this session the participant will be able to:

- Configure various types of Dependent Platforms




Overview





Dependents


Dependents are another type of **Platform** and are used for managing **Usages**


- A **usage** refers to an instance when an account, which is created at the operating system or domain level, is also used to perform some task somewhere else
- When we change the password for the target account, we must also make sure that any other occurrences (or usages) of the password are also changed



























Platform Management

 Filter

Targets

Dependents

Groups

Rotational Groups

12 results

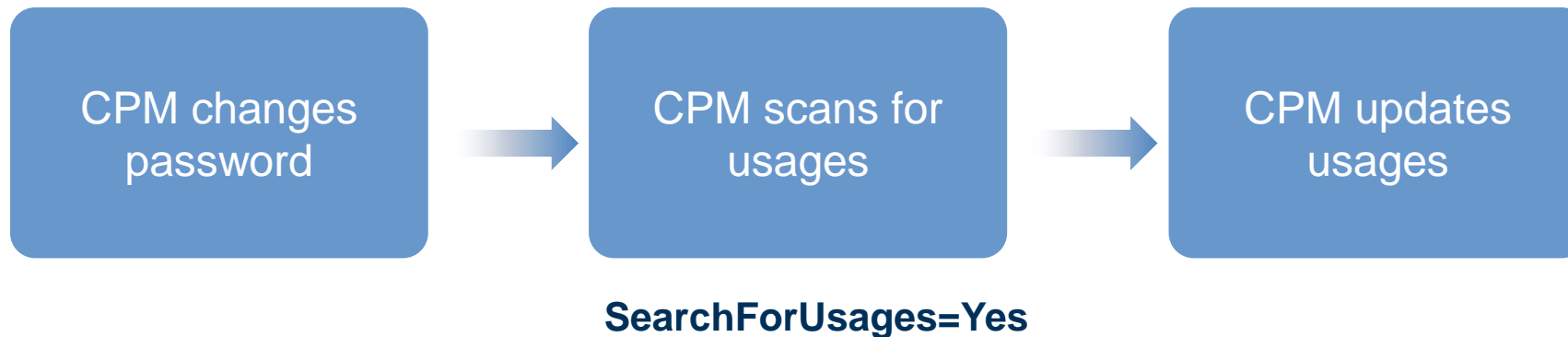
Platform Name	Manual password change	Number of target platforms
COM+ Application	✓	8
Database String	✓	2
IIS Anonymous User	✓	8
IIS Application Pool	✓	8
INI File	✓	1
Private SSH Keys	✓	2
Scheduled Task	✓	8
Text File	✓	
Web File	✓	



Usages

The **CPM** can synchronize an account password with all other occurrences of the same password on the same server or anywhere in the network, provided that those occurrences are registered in **CyberArk PAM**.

- This is done through **Usages**



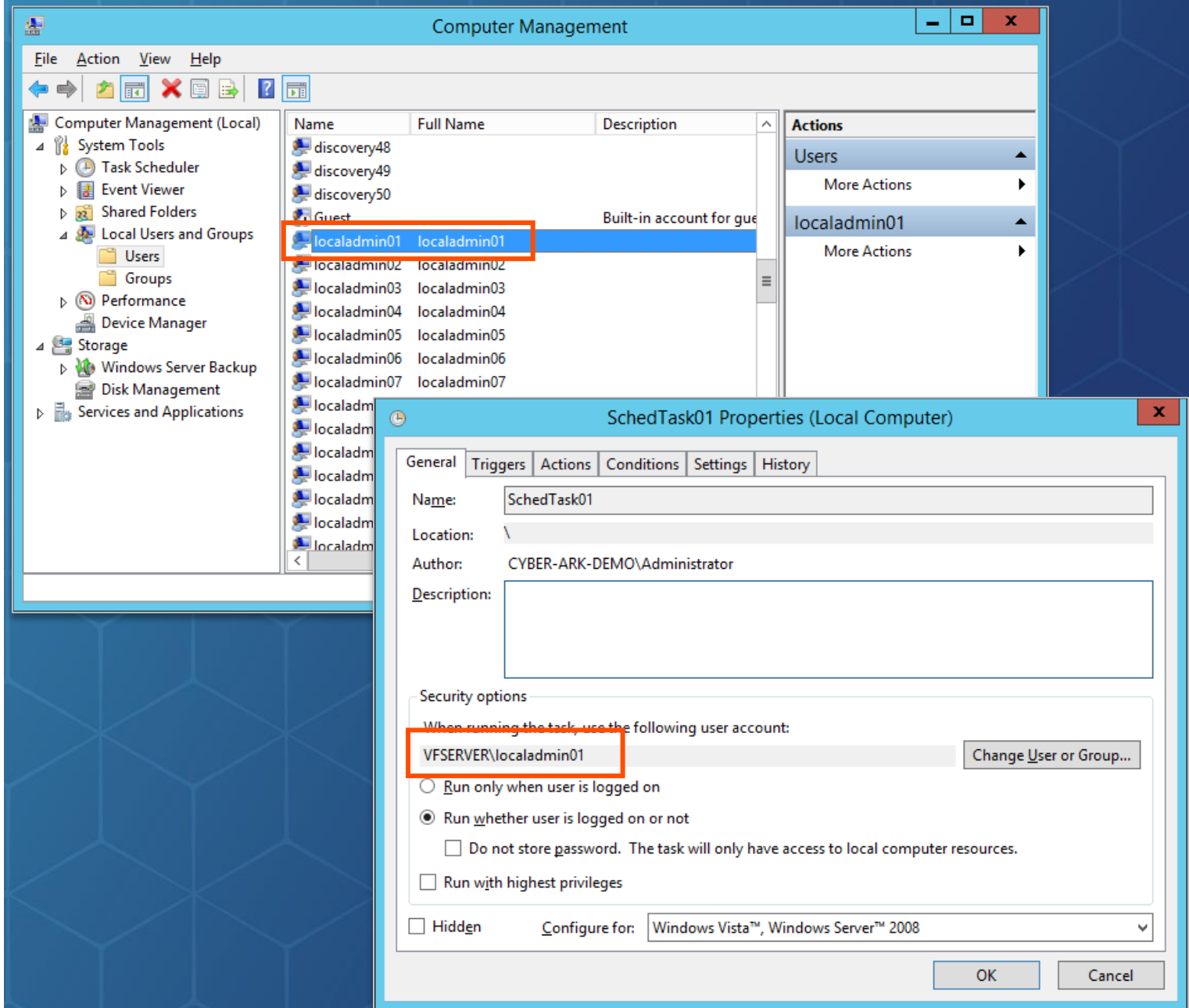
Scheduled Task Example



Scheduled Task Example

In our example, a local Windows user – **localadmin01** – is used to run a scheduled task – **SchedTask01**.

- When we change the password for **localadmin01**, we must also change the copy of the password that is stored with the scheduled task.
- If we don't, the scheduled task will no longer run.



Scheduled Task Example

- Viewing the account details for **localadmin01** in the Classic Interface, you will see the **Scheduled Task** tab. This is where we need to add the task, providing the name of the task and the server address.
- When the **CPM** changes the password for **localadmin01**, it will also change the password in the Scheduled Tasks.

The screenshot displays the 'Account Details' page for a user named 'localadmin01'. The page is divided into two main sections. The left section contains account metadata: Platform Name (WIN SRV LCL ADM 45), Device Type (Operating System), Safe (Win-Srv-Fin-US), Name (Operating System-WINSRVLCLADM45-target-win.acme.corp-localadmin01), Last verified (1/17/2022 10:58:09 AM), Last modified (PasswordManager (1/17/2022 10:57:09 AM)), Last used (john (1/18/2022 1:44:31 PM)), Username (localadmin01), Log On To (TARGET-WIN), and Address (target-win.acme.corp). The right section shows a list of scheduled tasks. A red box highlights the 'Scheduled Task' tab, which contains a table with columns for Task Name and Address. The table lists a task named 'schedtask01' with the address 'target-win.acme.corp'. Another red box highlights the 'Username' field in the account details, showing 'localadmin01'.

Account Details

Last sign in: 1/19/2022 | mike

Search: Go

Add SSH Key Add Account Customize

Platform Name: WIN SRV LCL ADM 45
Device Type: Operating System
Safe: Win-Srv-Fin-US
Name: Operating System-WINSRVLCLADM45-target-win.acme.corp-localadmin01
Last verified: 1/17/2022 10:58:09 AM
Last modified: PasswordManager (1/17/2022 10:57:09 AM)
Last used: john (1/18/2022 1:44:31 PM)
Username: localadmin01
Log On To: TARGET-WIN
Address: target-win.acme.corp

CPM Activities Versions Windows Service Scheduled Task

Task Name Address

<input type="checkbox"/>	schedtask01	target-win.acme.corp
--------------------------	-------------	----------------------



Windows Usages: Platform Configuration

Windows **Usages** are enabled by default in all the Windows **Target Platforms**.

- The **Target Platform** must reference the **Dependent Platforms** for the **Usages**.
- And have the parameter **SearchForUsages** set to **Yes**.

The image displays two screenshots of the Windows Server Local Accounts configuration interface, showing the configuration of Windows Usages.

Top Screenshot: The 'Windows Server Local Accounts' window is open. The 'Target Account Platform' is selected. Under 'Usages', the 'SchedTask' usage is highlighted. The 'Properties' table shows the 'Name' property set to 'SchedTask'.

Name	Value
Name	SchedTask

Bottom Screenshot: The 'Windows Server Local Accounts' window is open. The 'Automatic Password Management' section is selected. Under 'General', the 'SearchForUsages' property is highlighted, showing a value of 'Yes'.

Name	Value
PolicyID	WinServerLocal
PolicyName	Windows Server Local Accounts
PolicyType	Regular
ImmediateInterval	5
Interval	1440
MaxConcurrentConnections	3
SearchForUsages	Yes
LooselyConnectedDevices	No
AllowedSafes	*



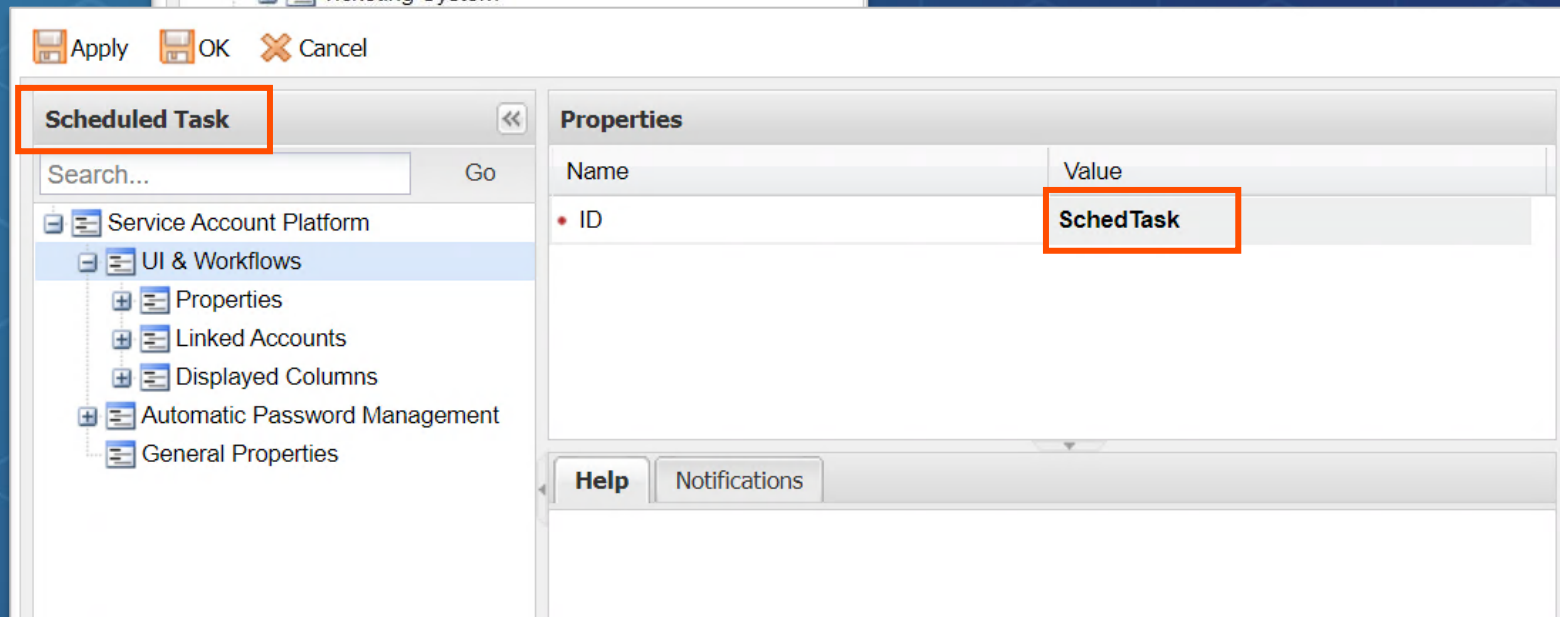
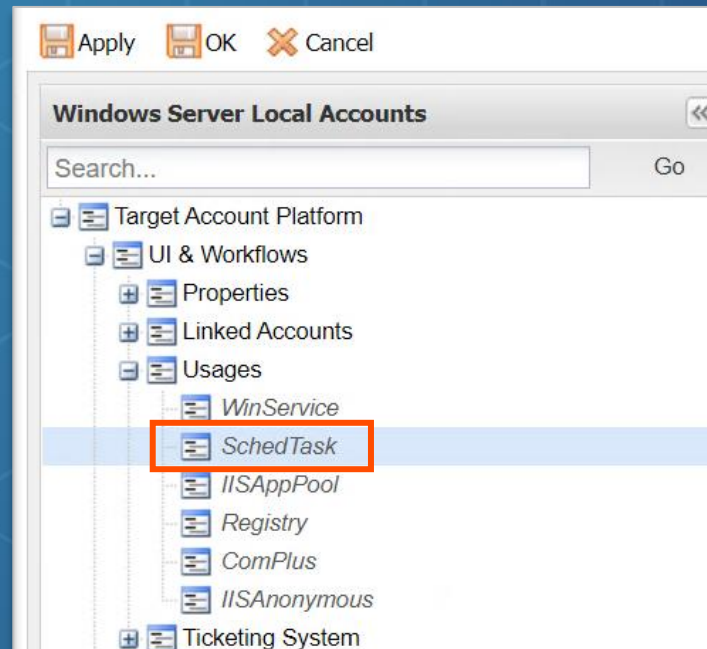
Windows Usages: Platform Configuration

The names listed under **Usages** reference the **PAM** object IDs for the **Dependent Platforms**.

Here we see the usage **SchedTask**.

If we look at the dependent platform **Scheduled Task**, we will see that its ID is also **SchedTask**.

This parameter informs the **Target Platform** what kinds of **Dependents** it should look for when scanning for usages.



Configuration File Example



Config File Example

Certain applications are hard-coded to retrieve credentials from configuration files

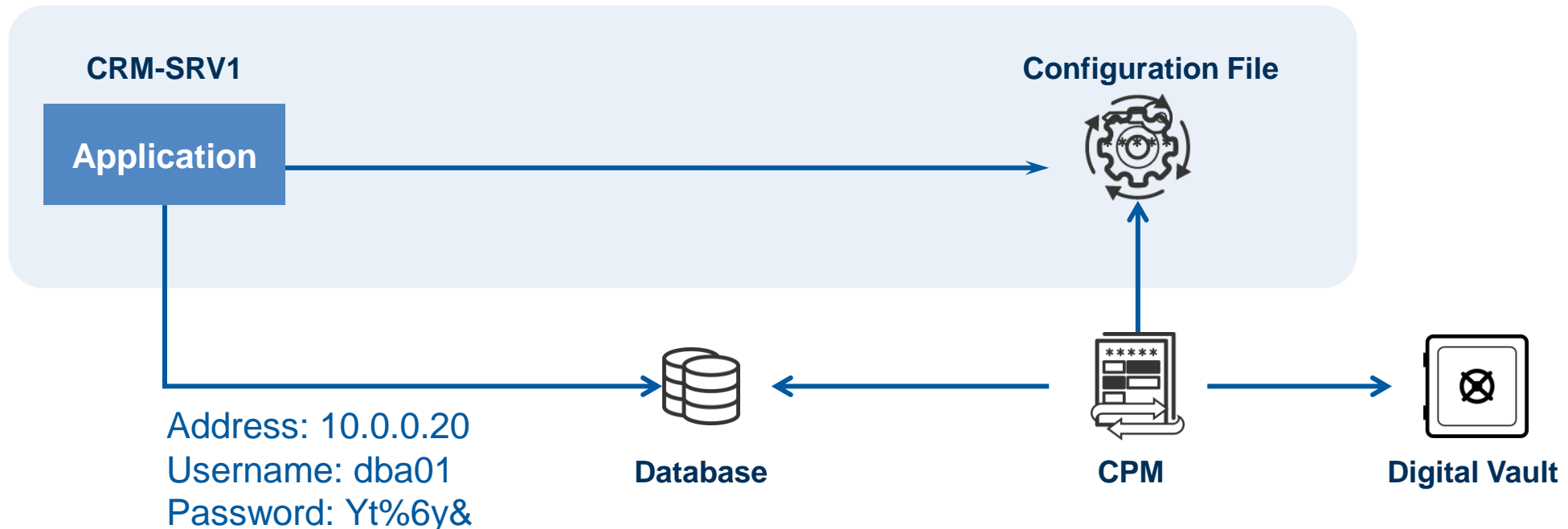
- The **CPM** can manage application accounts in the following types of files:
 - Plain text
 - INI files
 - XML files
 - Web configuration files
- These usages must be added manually to the appropriate **Target Platforms**

```
1  [Startup]
2  Product=App Server
3  ProductGUID=bf1f0850-d1c7-11d3-8e83-0000e8efafe3
4  CompanyName=CyberArkDemo
5  CompanyURL=www.cyber-ark-demo.com
6  MediaFormat=1
7  LogMode=1
8  SmallProgress=N
9  SplashTime=
10 CheckMD5=Y
11 CmdLine=
12 ShowPasswordDialog=N
13 ScriptDriven=4
14
15 [Languages]
16 Default=0x0409
17 Supported=0x0409
18 RequireExactLangMatch=0x0404,0x0804
19 RTLLangs=0x0401,0x040d
20
21 [Server]
22 Hostname=DBServer01
23 Password=Cyberark1
24
25 [Database]
26 Db=MySQL
27 Port=3306
28
29
```



Config File Usage Explained

- In this example, we have an application that uses a database account – **dba01** – to retrieve data for processing. The application retrieves the password for (the privileged account) from a configuration file and uses the credentials to authenticate to a target database.
- When the CPM changes the password for **dba01**, it must also push the updated password to the config file that is used by the application.



Add Config File Usage (1)

- To add a configuration file usage, you will first need to add manually the relevant usage in the target account platform
- Then enable the parameter ***SearchForUsages***

The image displays two screenshots of the CyberArk console interface, illustrating the steps to add a configuration file usage.

Top Screenshot: The 'ORA DBA 30' configuration window is shown. In the left-hand tree view, the 'Usages' folder is highlighted, and the 'INIFile' sub-item is selected. The 'Properties' pane on the right shows a table with the following data:

Name	Value
Name	INIFile

Bottom Screenshot: The 'ORA DBA 30' configuration window is shown again. In the left-hand tree view, the 'Automatic Password Management' folder is highlighted, and the 'General' sub-item is selected. The 'Properties' pane on the right shows a table with the following data:

Name	Value
MaxConcurrentConnections	3
SearchForUsages	Yes
LooselyConnectedDevices	No
AllowedSaves	Ora-



Add Config File Usage (2)

- Then you must associate the specific INI config file usage with the relevant account
- Notice that, in addition to providing the server address and the full path to the INI file, this usage also specifies where in the file the password can be found: in the section **Server** at the parameter **Password**

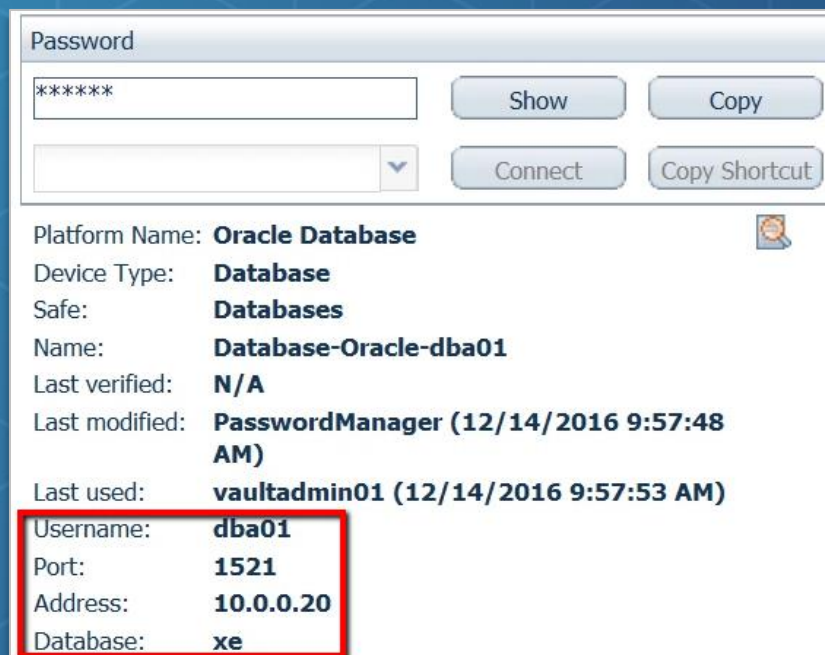
The screenshot shows a software interface with tabs: CPM, Activities, Versions, **INI Config File**, and Database String. Below the tabs are buttons for '+ Add' (highlighted with a red box) and 'Edit'. A search bar with a 'Go' button is also present. Below the buttons is a table with columns: File Path, INI Parameter Name, and Address.

The 'INI Config File' dialog box is open, showing 'Required Properties' and 'Optional Properties' sections. The 'INI Section' field is highlighted with a red box and an orange arrow points to it from the 'Add' button. The 'INI Section' field contains 'Server' and the 'INI Parameter Name' field contains 'Password'. Other fields include 'Address' (10.0.0.20), 'File Path' (/var/opt/app/app01.ini), and 'Connection Type' (SSH). There are also 'Optional Properties' for Port, Backup Password File, and Usage Display Name, and a checkbox for 'Disable automatic management for this account'.



Configuration Files

In this example, when the **CPM** changes the password for **dba01**, it will also change the password in the file **/var/opt/app/app01.ini** on the server 10.0.0.20.



Password

Show Copy

Connect Copy Shortcut

Platform Name: **Oracle Database**

Device Type: **Database**

Safe: **Databases**

Name: **Database-Oracle-dba01**

Last verified: **N/A**

Last modified: **PasswordManager (12/14/2016 9:57:48 AM)**

Last used: **vaultadmin01 (12/14/2016 9:57:53 AM)**

Username: **dba01**

Port: **1521**

Address: **10.0.0.20**

Database: **xe**



	File Path	INI Parameter Name	Address	
<input type="checkbox"/>	/var/opt/app/app01.ini	Password	10.0.0.20	



Logon Account

- If an extra account is required to log onto the remote machine where the usage exists, you will need to associate one with the usage.

The screenshot displays the CyberArk interface with the 'INI Config File' tab selected. The interface includes a table with columns for 'File Path', 'INI Parameter Name', and 'Address'. A red box highlights the first row of the table, which contains the following data:

File Path	INI Parameter Name	Address
/var/opt/app/app01.ini	Password	10.0.0.20

Below the table, the 'Logon Account' section is visible, showing the account name 'Unix via SSH-app-account01-10.0.0.20...' and buttons for 'Clear', 'Associate', and 'Create New'. An orange arrow points from the 'Add' button in the 'INI Config File' tab to the 'Logon Account' section.



Encrypting the Password in config Files

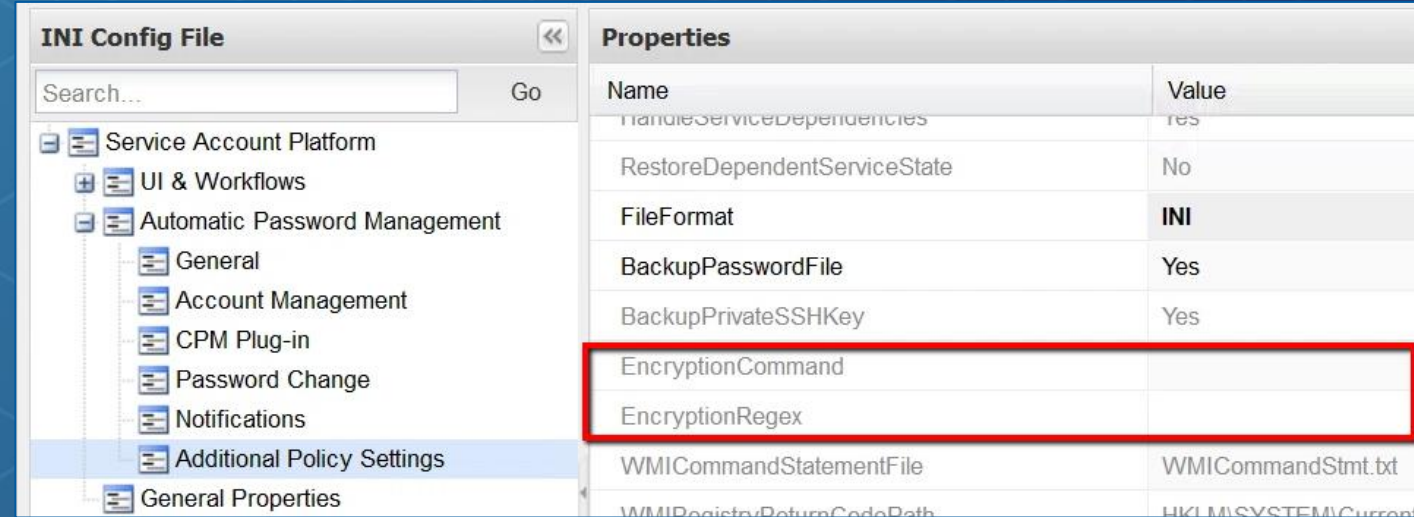
Passwords stored in configuration files can be encrypted using an external command:

- **Encryption Command**

The full path of the encryption command that will encrypt the password. The encryption file can be stored in any location on the CPM machine.

- **Encryption Regex**

The regex parameter that handles the output of the Encryption Command parameter. If this parameter is not defined, it will behave as if "(.*)" has been specified. This parameter is only relevant when the Encryption Command parameter is defined.



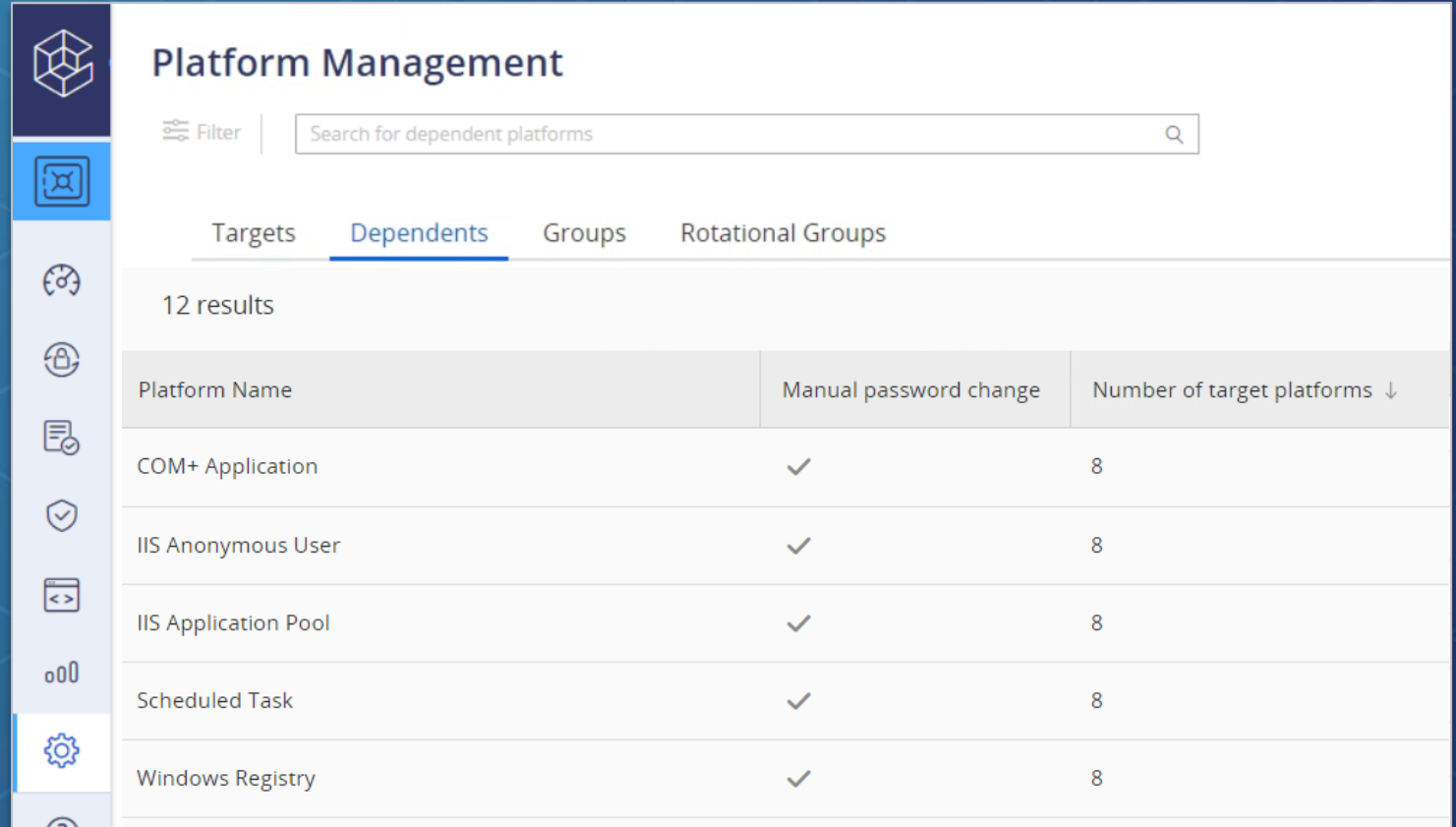
Discovering Dependencies



Discoverable Dependents

The **Accounts Discovery** process can detect the following Windows dependencies and automatically onboard them:

- Windows Services accounts
- Scheduled Tasks accounts
- IIS Application Pool accounts
- IIS Directory Security (Anonymous Access) accounts
- COM+ Applications accounts



The screenshot shows the 'Platform Management' interface. On the left is a sidebar with icons for various system components. The main area has tabs for 'Targets', 'Dependents' (which is selected), 'Groups', and 'Rotational Groups'. Below the tabs, it says '12 results'. A table displays the following data:

Platform Name	Manual password change	Number of target platforms ↓
COM+ Application	✓	8
IIS Anonymous User	✓	8
IIS Application Pool	✓	8
Scheduled Task	✓	8
Windows Registry	✓	8

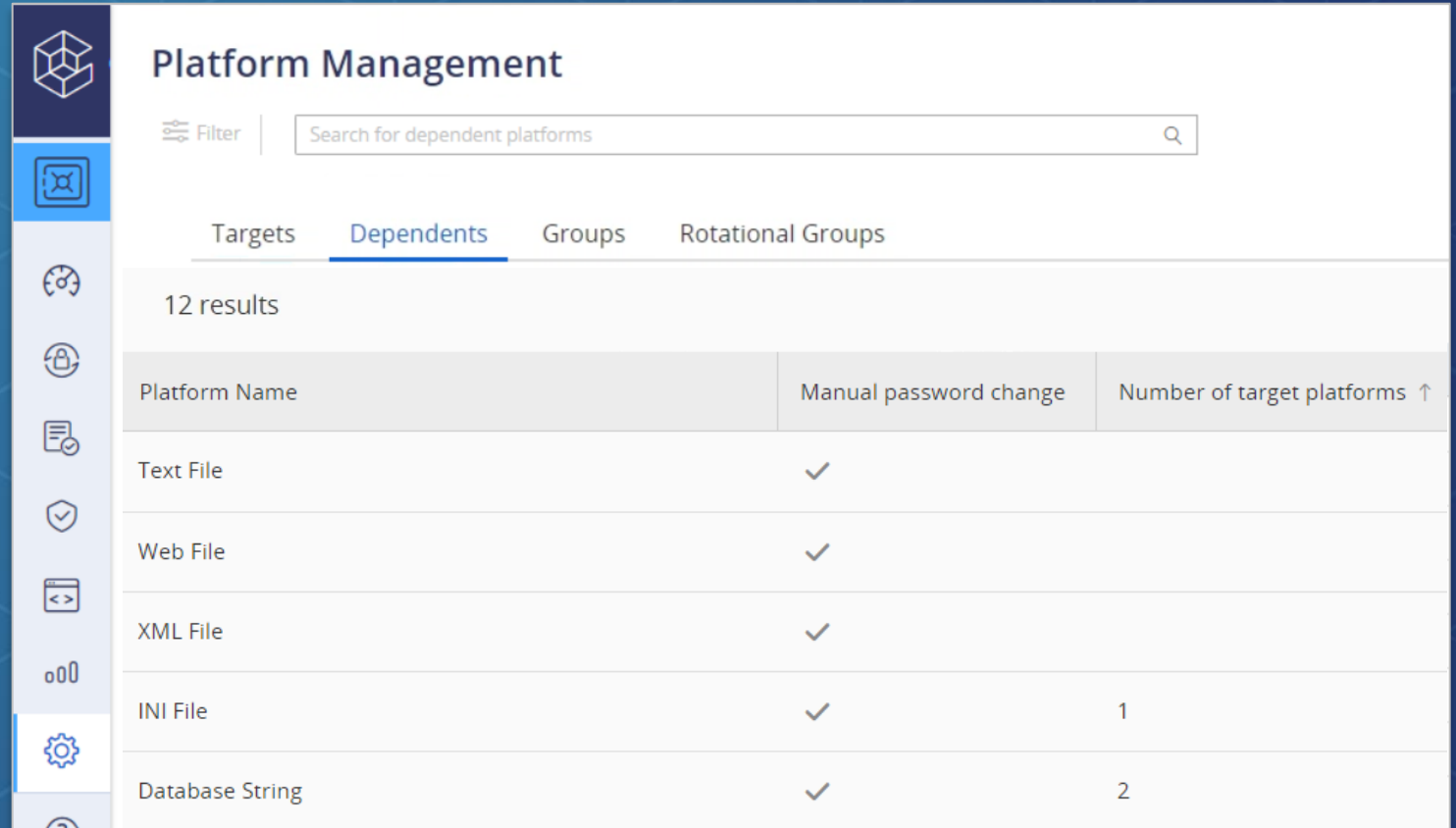


Non-Discoverable Dependents

The following types of dependent accounts cannot be discovered and must be added manually:

- Database String
- INI File
- Text File
- Web File
- XML File
- Private SSH Key
- Windows Registry

We will discuss Accounts Discovery in more detail in a later session



The screenshot shows the 'Platform Management' interface. The 'Dependents' tab is selected, displaying a table with 12 results. The table has three columns: 'Platform Name', 'Manual password change', and 'Number of target platforms'. The results are as follows:

Platform Name	Manual password change	Number of target platforms
Text File	✓	
Web File	✓	
XML File	✓	
INI File	✓	1
Database String	✓	2



Summary



Summary

In this session we discussed,

- ⚙️ Dependent platforms
- ⚙️ How to configure various types of usages



You may now complete the following exercise:

Dependents – Securing Usages

- Manage a Scheduled Task Usage
- Managing a Configuration File Usage
 - Create a Logon account
 - Configure Usages on the Oracle platform
 - Add the Usage to the target account

Exercises

