

Workforce Identity Management: Single Sign-On

Hands-On Training Lab Guide

Legal notice

Conditions and Restrictions

This Guide is delivered subject to the following conditions and restrictions:

This guide contains proprietary information belonging to Cyber-Ark® Software Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Cyber-Ark Vault.

No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Cyber-Ark® Software Ltd.

The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.

The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Third party components used in the Cyber-Ark Vault may be subject to terms and conditions listed on www.cyber-ark.com/privateark/acknowledgement.htm.

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eyay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com). This product includes software written by Ian F. Darwin.

This product includes software developed by the ICU Project (<http://site.icu-project.org/>) Copyright © 1995–2009 International Business Machines Corporation and other. All rights reserved.

This product includes software developed by the Python Software Foundation. Copyright © 2001–2010 Python Software Foundation; All Rights Reserved.

This product includes software developed by Infracore. Copyright (c) 2004 Infracore. All rights reserved.

This product includes software developed by Michael Foord. Copyright (c) 2003–2010, Michael Foord. All rights reserved.

Copyright

© 2000–2020 Cyber-Ark Software, Ltd. All rights reserved. US Patent No 6,356,941.

Cyber-Ark®, the Cyber-Ark logo, the Cyber-Ark slogan, IDaptive and MFA Everywhere are registered trademarks of Cyber-Ark Software Ltd. in the United States and other countries. All other product names mentioned herein are trademarks of their respective owners.

Information in this document is subject to change without notice. No part of this material may be disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Cyber-Ark® Software Ltd.

IDaptive and MFA Everywhere are registered trademarks of IDaptive in the United States and other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Pre-Requisites

The lab exercises provide students the opportunity to practice skills learned in the *Single Sign-on* course. The following requirements must be completed before attempting this lab.

- Completed the course *Workforce Identity Management: Basics*.
- Have access to a CyberArk Identity tenant.
- Have users and roles in the CyberArk Identity tenant.



NOTE: If you completed the *Workforce Identity Management: Basics* course you can use the same tenant. The tenant is valid for 30 days.






The context of each of these tasks will be discussed and demonstrated from the course modules. Specific directions will be provided when it is time to complete the tasks and practice the skills.

Preferred Browsers

These labs will work in any browser, however, the preferred browser for most exercises is *Google Chrome*. The lab exercises are written using the Google Chrome browser.

Symbols

Symbols are used in this guide to identify specific things. Below is an explanation of each symbol you may find in this guide.

	Scenario – This identifies the scenario and helps to identify why a task would be completed.
	Note – This identifies a note, usually within a procedural step to explain additional information.
	Important or Critical Note – This identifies a note or comment of high importance.
	Best Practice – This identifies a <i>best practice</i> recommendation from CyberArk, security governing bodies, or industry standards.
	End of Lab – This identifies the end of the lab. When this symbol is displayed, return to the course for the next steps.

Contents

The Simulated Environment	5
Lab 1: Add an App From the Catalog	6
Task 1: Add an app from the catalog with shared credentials	6
Task 2: Log in as a Contractor to see the Southwest Airlines tile.....	7
Lab 2: Recommended Apps	9
Task 1: Add an app from the catalog with individual credentials	9
Task 2: Add a recommended app	10
Lab 3: Install the CyberArk Identity Browser Extension	11
Task 1: Install the CyberArk Identity Browser Extension	11
Task 2: Explore the CyberArk Identity Browser Extension.....	12
Lab 4: Add a Custom App	13
Task 1: Add a Custom Bookmark App	13
Task 2: Using a Custom Bookmark App	14
Lab 5: Using Land and Catch	15
Task 1: Enable the Land and Catch feature	15
Task 2: Reset the CyberArk Identity Browser Extension	15
Task 3: Capture an app using Land & Catch	16
Lab 6: Request and Approval Workflow	17
Task 1: Create and Assign the App Workflow Admin role	17
Task 2: Add a Web App	17
Task 3: Enable the App Workflow	18
Task 4: End-User POV – Request an App.....	19
Task 5: Approver POV – Approve an App Request	19
Task 6: Requester POV – Verify the App Request is Complete.....	19

The Simulated Environment

This Workforce Identity Management: Single Sign-On course has a simulated environment for a fictitious company, Acme.corp. As the Identity Administrator for Acme.corp, you will use an Identity Security Platform tenant. If you have a tenant from a previous Identity micro course, you can use that tenant for these labs.

This guide covers:

- Adding web apps in CyberArk Identity using built-in templates.
- Installing the CyberArk Identity Browser Extension.
- Adding a custom web app in CyberArk Identity.
- Using the Land and Catch feature to capture login information.
- Implementing and experiencing the request and approval process.

Remember:

- Creating MFA policies may cause login issues. Be sure to follow the instructions in this lab carefully.

Lab 1: Add an App From the Catalog

Pre-requisites	Complete the Lesson: Single Sign-On Overview .
Objectives	<i>Add</i> an app from the Identity Catalog with shared credentials. <i>Deploy</i> the app to end users. <i>Experience</i> the end user perspective.

Task 1: Add an app from the catalog with shared credentials

This task will add the CDW app as an **admin** and experience it in the Secure Access portal as an **end-user**. The lab does not have a valid CDW account, so actually launching the account will not be possible, however, if you have personal credentials for these apps, you may use them and fully utilize the web app tiles.

1. Login to the Identity Security Platform as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Apps & Widgets > Web Apps**.
4. Click **Add Web Apps**.
5. Search for **CDW**.



NOTE: If you do not have a CDW account, and would like the *full experience*, you can create one for free at <https://www.cdw.com/account/logon/createaccount>, or select another username password type app that you can log into.

6. Click **Add** next to the *CDW User Password App*.
7. Click **Yes**.
8. Click **Close** on the Add Web Apps window.
9. Update the Application Description.

Suggested: **Users will share a single username and password to use the CDW app.**

10. Click **Account Mapping**.
11. Choose **All users share one name**.
12. Enter your *CDW* credentials.



NOTE: Use your personal **CDW credentials** to login to this app. The username field corresponds with the username field on the sign-in page of the web app.

13. Verify that *Allow users to view credentials* is unchecked.
14. Click **Save**.



NOTE: For username/password type apps, the online account must be established prior to configuring the app. In this case, all users will share the same login, and end users will not see this information.

15. Click **Permissions**.
16. Click **Add**.



BEST PRACTICE: Try out the new app prior to deploying it to a role or group of users.

17. Search for **Contractors**.
18. Select the **Contractors** role.
19. Click **Add**.
20. Click **Save**.
21. Navigate to **Secure Access**.

The *CDW App* tile does not appear because it was not deployed to the system administrator role, but to the contractor role.

Task 2: Log in as a Contractor to see the CDW tile

The *CDW App* tile requires the CyberArk Identity Browser Extension. Install the browser extension if you want to experience the end users' perspective.

1. Click the username at the top right of the screen and **Sign Out**.
2. Enter Carrie Cairo's username: [Carrie.Cairo@acme\[IdentityID\].com](mailto:Carrie.Cairo@acme[IdentityID].com).
3. Click **Next**.



NOTE: If you are using a tenant from a previous lab, you may have some MFA policies in place. If prompted, use the email confirmation code to authenticate.

4. Enter the confirmation code and click **Authenticate**.
5. Enter the password for Carrie Cairo – **Password:** Cyberark1!
6. Click **Next**.

You can verify you are logged in as Carrie Cairo by checking the username at the top right of the screen. Another clue is that the *Waffle* menu is no longer present.

7. Verify the *CDW App tile* is present. Refresh if necessary.

The tile has a red exclamation point indicating that the CyberArk Identity browser extension is required.

8. Log out of CyberArk Identity as Carrie Cairo.



You are finished with this Lab.

Lab 2: Recommended Apps

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: Single Sign-On Overview .
Objectives	<i>Add an app from the Identity Catalog with individual credentials.</i> <i>Deploy the app to end users as a recommended app.</i> <i>Add the recommended app as an end user.</i>

Task 1: Add an app from the catalog with individual credentials



SCENARIO: Acme.corp recommends that their users use the calendly web app for appointment scheduling, however, end users can choose whichever program they like. As the Acme Identity admin, we will add the Calendly app as a recommended app in Identity.

1. Login to the Platform Identity Administration as the default admin account.
2. Click the *Waffle* menu and select **Identity Administration**.
3. Navigate to **Apps & Widgets > Web Apps**.
4. Click **Add Web Apps**.
5. Search for **Calendly**.



NOTE: There are numerous Calendly app templates to choose from. This lab will focus on the username/password template. The SAML + Provisioning template require additional configurations on the web app side and will be covered in a later lesson.

5. Click **Add** next to the *Calendly User Password App*.
6. Click **Yes**.
7. Click **Close** on the Add Web Apps window.
8. Update the Application Description.

Suggested: This app is recommended by management for the purpose of scheduling appointments.

9. Click **Account Mapping**.
10. Verify that **Prompt for user name** is selected.
11. Click **Save**.

12. Click **Permissions**.
13. Click **Add**.
14. Search for **Everybody**.
15. Select the **Everybody** role.
16. Click **Add**.
17. Remove the checkmark under **Automatically Deploy**.
18. Click **Save**.

Task 2: Add a recommended app

1. Navigate to **Secure Access**.
2. Click **Add**.
3. Click **Catalog or imported app**.



NOTE: By default, the catalog will open to the Recommended tab if there are recommended apps available.

4. Click **Add** next to the *Calendly* app.
5. Click **Yes** on the confirmation window.
6. Click **Close**.
7. Add **test@acme.com** to the *username* field.

NOTE: Test@acme.com is a fictitious username and will not work to log into the web app. You can add a real username to the Calendly app if you like.

8. Click **Save**.

The Calendly app is added to the user portal. A red exclamation point indicates that the CyberArk Identity browser extension is required to launch the web app.



You are finished with this Lab.

Lab 3: Install the CyberArk Identity Browser Extension

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: CyberArk Identity Browser Extension .
Objectives	<i>Install</i> the CyberArk Identity Browser Extension. <i>Explore</i> the CyberArk Identity Browser Extension. <i>Launch</i> an app as an end user.

Task 1: Install the CyberArk Identity Browser Extension

There are numerous ways to install the CyberArk Identity Browser Extension. Refer to the [documentation](#) for other ways to install the Browser Extension.

1. Login to the User portal as [carrie.cairo@acme\[IdentityID\].com](mailto:carrie.cairo@acme[IdentityID].com).
2. Click the CDW tile.




NOTE: A new tab will open up prompting you to install the CyberArk Identity Browser Extension.

3. Click **Install**.
4. Click **Download** on the CyberArk Identity Browser Extension popup.
5. Click **Add to Chrome**.
6. Click **Add extension**.
7. Close the confirmation popup.



NOTE: The *Turn on sync...* button is a google sync feature that will add the CyberArk Identity Browser Extension to any chrome browser. **This requires a google account and is not necessary for these labs.**

8. Click the **extension** icon  at the top right of the browser.
9. Click the **pin** next to the *CyberArk Identity Browser Extension*.
10. Click anywhere to close the *extension* popup.
11. Click the **CyberArk Identity Browser Extension** icon to the right of the *address bar*.
12. Click **Sign In**.
13. Login using **Carrie.cairo@acme[IdentityID].com**.



NOTE: A popup window will prompt the user to login to the CyberArk Identity Browser Extension when you log into the user portal.

14. Click **Sign In**.
15. Click the **CDW** tile in the user portal.

If you used valid credentials, the tile will take you to the CDW site and successfully log you into the web app. If you used the fake credentials listed in this lab, the system will attempt to log you in and fail.

Task 2: Explore the CyberArk Identity Browser Extension

The CyberArk Identity Browser Extension has many features and capabilities available to users. Take a moment to explore some of the features in the extension.

1. Click the **Settings** icon in the navigation on the right.
2. Click the dropdown next to **Advanced**.
3. Click on the **User Portal** icon to launch the CyberArk Identity User Portal.
4. Click on the **Password Generator** icon.
5. Log out as Carrie Cairo.



You are finished with this Lab.

Lab 4: Add a Custom App

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: Scenario: Adding Custom Apps .
Objectives	<i>Add an app using a custom template.</i>

Task 1: Add a Custom Bookmark App

There are various custom templates available from CyberArk. This task will explore the bookmark app.



SCENARIO: Acme has decided to recommend the CyberArk Identity online documentation to their end users. You have been tasked with creating the Bookmark app and deploying to as a *Recommended* app.

1. Login to the Platform Identity Administration as the default admin account.
2. Click the *Waffle* menu and select **Identity Administration**.
3. Navigate to **Apps & Widgets > Web Apps**.
4. Click **Add Web Apps**.
5. Click the **Custom** tab.
6. Locate the Bookmark template. Click **Add**.
7. Click **Yes** to confirm.
8. Click **Close** on the Add Web Apps window.
9. Enter https://docs.cyberark.com/Product-Doc/OnlineHelp/Idaptive/Latest/en/Content/UserPortal/UsingTabs.htm?tocpath=End%20User%7C_____0 in the *URL* field.
10. Click **Save**.



NOTE: Bookmarks created from the Admin Portal are available in any browser or machine that can access the CyberArk Identity User Portal. This is a very convenient way to provide webpage links to end users.

11. Click **Description**.
12. Replace the text in the *Application Name* field with **The CyberArk Identity Resource Center**.
13. Update the Application Description.

Suggested: **Bookmark for CyberArk Identity End User documentation.**

14. Click **Browse** next to the *Logo*.
15. Navigate to the *Course Materials* and upload the **CyberArkIdentity.png** file.
16. Click **Permissions**.
17. Click **Add**.
18. Search for the **Contractors** role.
19. Select the **Contractors** role.
20. Click **Add**.
21. *To make this a Recommended App*, remove the checkmark under *Automatically Deploy*.
22. Repeat steps 15 – 19 to deploy this bookmark as a recommended app to the **System Administrator** role.
23. Click **Save**.
24. Click the *Waffle* menu and navigate to **Secure Access**.
25. Sign out as the *cloudadmin*.

Task 2: Using a Custom Bookmark App

1. Login as *Carrie.Cairo@Acme[IdentityID].com*.
2. Click **Add Apps**.
3. From the Recommended tab, click **Add** next to **The CyberArk Identity Resource Center** app.
4. Click **Yes**.
5. Click **Close**.
6. Click **The CyberArk Identity Resources Center** tile to test the new bookmark app.



You are finished with this Lab.

Lab 5: Using Land and Catch

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: Scenario: Using Land and Catch .
Objectives	<i>Enable</i> the Land and Catch feature. <i>Capture</i> an app using land and catch.

Task 1: Enable the Land and Catch feature

Land and Catch is not enabled by default. Administrators first need to turn the feature on in a policy before anyone can use the feature when capturing website login credentials.

1. Login to the Platform Identity Administration as the default admin account.
2. Click the *Waffle* menu and select **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the *Name* to **Land and Catch**.
6. Enter a description.

Suggested: This policy applies to everyone and enables the Land and Catch feature.

7. Under *Policy Assignment* leave the default at **All users and Devices**.
8. Click **Application Policies**.
9. Click **User Settings**.
10. Click the dropdown next to *Allow users to add personal apps* and click **Yes**.
11. Click the dropdown next to *Enable Browser Extension Land & Catch* and click **Yes**.
12. Click **Save**.
13. Click **Push Policy**.

Task 2: Reset the CyberArk Identity Browser Extension

More likely than not, the CyberArk Identity Browser Extension will be logged in when making the policy change to enable Land and Catch. This task will log out of and back into the CyberArk Identity Browser Extension to use the Land and Catch feature.

1. Click the *CyberArk Identity Browser Extension* icon to the right of the address bar.
2. Click the gear icon on the right.
3. Verify that Land and Catch is not the second setting in the list.

4. Click the **Sign Out** link.
5. Log in as the default administrator.
6. Click the *CyberArk Identity Browser Extension* icon to the right of the address bar.
7. Click the gear icon on the right.
8. Verify that *Enable Land & Catch on this computer* is turned on.

Task 3: Capture an app using Land & Catch

With Land & Catch enabled, and the CyberArk Identity Browser Extension logged in, Land & Catch will attempt to capture login information and offer to store them in the user portal for end users.



NOTE: This task will use LinkedIn as the web app. Be sure you have a LinkedIn login and that you are logged out of LinkedIn prior to this task.

1. Open a new browser tab and navigate to linkedin.com.
2. Click the **Sign In** button.
3. Enter your username and password for the LinkedIn account.
4. Click **Yes** on the *Add this site to your User Portal?* popup.
5. Click the *CyberArk Identity Browser Extension* icon and select the **User Portal** icon.
6. Click the three dots on the top right corner of the amazon tile and choose **Settings**.
7. Add tags or a note and click **Save**.



You are finished with this Lab.

Lab 6: Request and Approval Workflow

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: Request Access Workflows .
Objectives	<p><i>Create a role for App Workflow Admin with specific admin permissions.</i></p> <p><i>Enable the workflow on the DocuSign web app.</i></p> <p><i>Request access to the DocuSign web app from the end-user POV.</i></p> <p><i>Approve the request from the approver POV.</i></p>

Task 1: Create and Assign the App Workflow Admin role



SCENARIO: Acme.corp management wants you to create a role for the App Workflow Admins. This role should not have limited admin permissions to support app approval. Assign Allister Harris as the designated approver for the app workflows.

1. Log in as the default administrator.
2. Click the *Waffle* menu and click **Identity Administration**.
3. Navigate to **Core Services > Roles**.
4. Add a role for the **App Workflow Admin**. Add a description, leave the organization blank, and the role type as **Static**.
5. Click **Save**.
6. Click **Members**.
7. Click **Add**.
8. Search for *Allister*. Select **Allister** and click **Add**.
9. Click **Save**.
10. Navigate to **Core Services > Users**.
11. Locate and open H

Task 2: Add a Web App

1. Navigate to **Apps & Widgets > Web Apps**.
2. Click **Add Web Apps**.
3. Search for **DocuSign**.
4. Click **Add** next to the *DocuSign User Password*.

5. Click **Yes**.
6. Click **Close** on the Add Web Apps window.
7. Click **Permissions**.
8. Click **Add**.
9. Search for **Angela**.
10. Select the **Angela.coleman** account.
11. Click **Add**.
12. Click **Save**.
13. Click **Back to Web Apps**.

Task 3: Enable the App Workflow



SCENARIO: DocuSign may need to be accessed by the various users, depending on the situations. Rather than providing this app to all users, Acme.corp wants you to enable an App Workflow that users can request access when they need it. Assign the App Workflow Admin as the designated approver for the workflows.

1. Click on the **DocuSign** app.
2. Click **Workflow**.
3. Check the box next to **Enable workflow for this application**.
4. Click **Add**.
5. Click the **Approver Type** dropdown.
6. Choose **Specified User or Role**.



NOTE: Requestor's Manager looks for the manager configured in CyberArk Identity to use this option. If the Manager isn't configured, the alternative approver specified in the workflow will receive the request.

7. Click **Add**.
8. Search for the **App Workflow Admin** role.
9. Select the *App Workflow Admin* role and click **Add**.
10. Click **Save**.
11. Click the *Waffle* menu and navigate to **Secure Access**.
12. Sign out of the portal.

Task 4: End-User POV – Request an App



SCENARIO: Carrie Cairo is working with the Sales team and has been asked to prepare some sales documents in DocuSign. Carrie does not have access to DocuSign currently, but Acme has established a request and approval workflow for this app.

1. Log in as `Carrie.Cairo@acme[IdentityID].com`. Click the **Add** button.
2. Choose **Catalog or imported app**.
3. Search for **DocuSign**.
4. Click the **Request** button.
5. Type in a *Reason* for the request.
6. Change the assignment type to **Windowed**.
7. Leave the Start Date as the default.
8. Change the End Date to be one week from today.
9. Click **Submit**.
10. Click **Close**.
11. Log out of CyberArk Identity.

Task 5: Approver POV – Approve an App Request



SCENARIO: The CyberArk Identity Admin has granted Allister Harris the permission to review and approve app requests.

1. Log in as `Allister.Harris@acme[IdentityID].com`. Click **Access requests**.
2. Locate and click the *Application access request* from `Carrie.Cairo@acme[IdentityID].com`.
3. Review the request information.
4. Click **Approve**.
5. Review the *Windowed* settings but do not make any changes.
6. Click **Submit**.

Task 6: Requester POV – Verify the App Request is Complete

1. Log in as [Carrie.Cairo@acme\[IdentityID\].com](#).
2. Verify that *DocuSign* is a tile in the User Portal.
3. Log out as Carrie.

You are finished with this Lab.

