Workforce Identity Management

Workforce Password Management 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 (eay@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 Infrae. Copyright (c) 2004 Infrae. All rights reserved.
This product includes software developed by Michael Foord. Copyright (c) 2003-2010, Michael Foord. All rights reserved.

Copyright

Contents

The Lab Environment

The Workforce Identity Management courses use a simulated environment for a fictitious company, Acme.corp. Each micro course can use the same Identity tenant.

This guide covers:

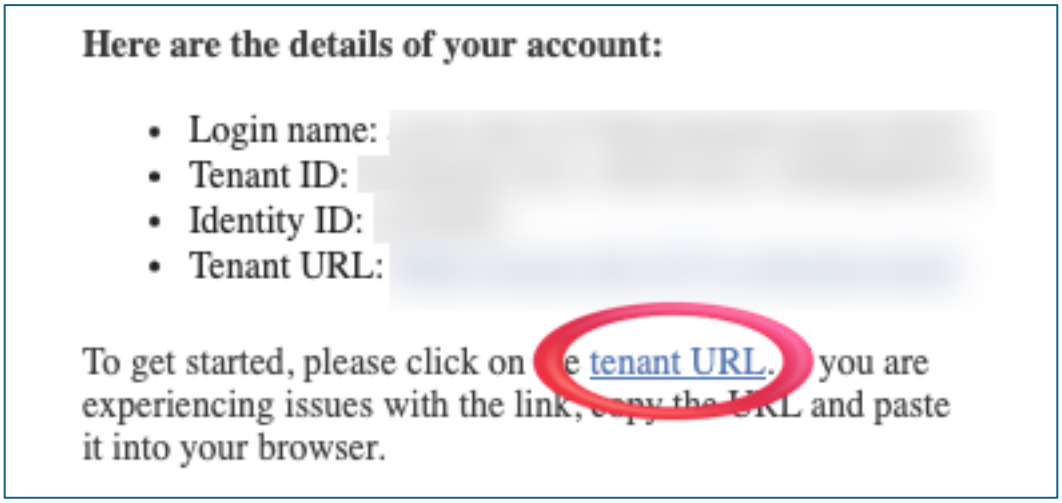
- Configuring the Identity tenant with users and roles specific to this micro-course.
- Configuration of web apps, wpm specific policies, and multi-factor authentication.
- Testing end user experiences of WPM policies and features.
- Hardening and best practices for a WPM deployment.

Lab 1: Preparing the WPM Lab

This lab will get the Identity tenant ready for this course including populating the users table with specific users and adjusting MFA permissions for the administrator account.

Task 1: Log into the CyberArk Identity Tenant.

1. Locate the CyberArk Identity email invitation from *The CyberArk Team*.
2. Click the **tenant URL** link in the email to set the password.



3. Enter the password for the default administrator account. You may use any password you like, however, we recommend using **Cyberark1**. This is the same password as all the other user accounts in this training.

Perform the rest of the lab inside of Skytap. This will alleviate any potential issues with corporate setups, GPOs, and any personal configurations to your web browser.

Task 2: Create a Login Suffix

1. Launch the Skytap instance. ***This may take several minutes***.
2. Click the **Training Desktop** VM. All work can be in the Training Desktop VM, but the Domain Controller VM must be running.
3. Open the Google browser.
4. Navigate to your Identity tenant URL. If you copy it from the email, use the copy/paste button in Skytap. Refer to the training for instructions.
5. Log into your CyberArk Identity tenant using the default admin account.
6. Click the *Waffle menu* and select **Identity Administration**.

7. Navigate to **Settings > Customization** and click on **Suffix**.
8. Click **Add**.
9. Enter the login suffix **acme[IdentityID].com**.

   Example: acmeabh5167.com.
10. Click **Save**.

Task 3: Create Custom Roles

1. Navigate to **Core Service > Roles**.
2. Click **Add Role**.
3. In the *Name* field, type **Marketing Team**.
4. Enter a description.

   Suggested: A role used to assign applications and policies to the Marketing team.

5. Click **Save**.

Task 4: Bulk User Import into a Role

This task will use the User Bulk Import feature to upload a list of users from the Marketing team into the CyberArk Cloud Directory. To complete this task, you will need to locate the spreadsheet included in the course materials titled Acme_Marketing_Team.csv.

1. Locate the spreadsheet included in the course materials titled: **Acme_Marketing_Team.csv.**
2. Open the file for editing.
3. Update the existing login suffix with your unique login suffix - **@acme[IdentityID].com**.

   NOTE: The login suffix for these users should match the one created earlier, acme[IdentityID].com. Verify the users' login name contains a login suffix that exists in your tenant, prior to bulk import or the bulk import will fail.

4. Verify that the Marketing Team role name is spelled exactly as it is in your tenant UI. Remember that it is case sensitive.
5. Save the updated .csv as a new .csv.

6. Close the file.
7. From the Identity Administration Portal, navigate to **Core Services > Users**.
8. Click the **Bulk User Import** button.
9. Click **Browse** and locate your edited *Acme_Marketing_Team.csv* file.
10. Click the file to upload and click **Open**.
11. Click **Next**.

    NOTE: An error here may indicate that the login suffix on the .csv file is incorrect. Check the spelling of the login suffix and the Roles.

12. Click **Next**.
13. **Uncheck** the box next to *Send email invites for user portal setup*.
14. Enter your email address for report delivery.
15. Click **Confirm**.

    NOTE: This process may take a few minutes to complete. Refresh your browser until the new users appear in the users table.

16. Navigate to **Roles**.
17. Open the **Marketing Team** role.
18. Click **Members**.
19. Verify that the imported users are now members of the *Marketing Team* role. Click **Reload** if you do not see the new members in this role.

    NOTE: Role names must be identical. If you still do not see any users in the Marketing Team role, double check the spelling of the role name in your tenant and the role name in the .csv file. Make any changes as necessary to the spreadsheet and try again.

Task 5: Create a 1 Factor MFA Policy

This course will require you to log in and out of the platform as different users to experience various points of view. Requiring multi-factor authentication for every login attempt will become tedious and frustrating.

IMPORTANT: This process is not recommended for a production environment. This is strictly for training purposes only.

1. Navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **ACME MFA User Policy – Training Only**.
4. Under *Policy Assignment*, select **All users and Devices**.
5. Navigate to **Authentication Policies > CyberArk Identity Security Platform**.
6. Click the down arrow next to Enable authentication policy controls and select **Yes**.

   NOTE: Skip the rules section for now. This policy will apply 100% of the time. For more information on rules, see **The Adaptive Multi-Factor Authentication** course.

7. Under *Default Profile (used if no conditions matched)* choose **Add New Profile**.
8. Type **ACME Users 1FA** in the *Profile Name* field.
9. Check the box next to **Password**.
10. Click **OK**.
11. Click **Save**.

Task 6: Install a Shared WebApp

This task will add the CDW app as a web app for all users. More in-depth training on webapps in the **Single Sign-On** micro course located in CyberArk University.

1. Navigate to **Apps & Widgets > Web Apps**.
2. Click **Add Web Apps**.
3. Search for **CDW**.
4. Click **Add** next to the *CDW User Password* App.
5. Click **Yes**.
6. Click **Close**.

   NOTE: It is recommended to use the credentials provided. They are not valid credentials so the webapp will not open properly. This is fine for this training.

7. Click **Account Mapping**.
8. Choose **All users share one name**.
9. Enter the following credentials.
    - Username: ACME@acme.corp
    - Password: Cyberark1
10. Verify that **Allow users to view credentials** is unchecked.
11. Click **Save**.
12. Click **Permissions**.
13. Click **Add**.
14. Search for **Everybody**.
15. Select the **Everybody** role.
16. Click **Add**.
17. Click **Save**.
18. Navigate to the **Secure Access** Portal.

The CDW App tile should with a red exclamation point. This is expected and will be resolved in later labs.

Lab 2: Install the CyberArk Identity Browser Extension

This lab requires a CyberArk Identity tenant configured with users. Complete this lab in the **Skytap** environment to be sure that the browser extension installation does not fail.

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. Log in as Carrie Cairo.
    a. **Username:** Carrie.Cairo@acme[IDENTITYID].com
    b. **Password:** Cyberark1
2. Click the *Waffle menu* and select **Secure Access**.

    NOTE: The CDW tile has a red exclamation mark (!) indicating that it requires the browser extension to run this application.

3. Click the **CDW** tile.

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

4. Click **Install**.
5. Click **Download** on the CyberArk Identity Browser Extension popup.
6. Click **Add to Chrome**.
7. Click **Add extension**.
8. 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.

9. Click the **extension icon** at the top right of the browser. This looks like a puzzle piece.
10. Click the **pin** next to the CyberArk Identity Browser Extension.
11. Click anywhere to close the extension popup.

12. Click the **CyberArk Identity Browser Extension icon** to the right of the address bar.
13. Click **Sign In**.
14. 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.

15. Click **Sign In**.
16. Click the **CDW** tile in the *Secure Access* 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, as indicated in Lab 1, 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 CyberArk Identity Browser Extension icon.
2. Click the Settings icon in the navigation on the right.
3. Click the dropdown next to Advanced.
4. Click on the User Portal icon to launch the Secure Access Portal.
5. Click the CyberArk Identity Browser Extension icon.
6. Click on the Password Generator icon.

Lab 3: Password Sharing

In this lab, you'll create several items that store password information and share them with other users. You'll experience both perspectives—sharing items and accessing items that have been shared with you.

Task 1: Configure the tenant for Password Sharing

Holly Wood is the Marketing Team Lead. She has login credentials to the corporate social media platforms. She wants to share these credentials with her manager and members of her team. The administrator needs to configure the tenant to allow her to share credentials.

1. Log into your CyberArk Identity tenant using the default admin account.
2. Click the *Waffle menu* and select **Identity Administration**.
3. Navigate to **Core Services > Roles**.
4. Click **Add Role**.
5. Type **Marketing Management** in the *Name* field.
6. Click **Save**.
7. Click **Administrative Rights**.
8. Click **Add**.
9. Type **Shared** in the *Search* field.
10. Click the checkbox next to **Shared Credentials** and click **Add**.
11. Click **Save**.
12. Click **Members**.
13. Click **Add** and search for *Holly Wood* and *Daniel Carter*.
14. Click **Save**.

Task 2: Create Password Items to Share

Holly Wood is the Marketing Team Lead. She has login credentials to the corporate social media platforms.

1. Log into your CyberArk Identity tenant using the following credentials:
   - **Username:** Holly.Wood@acme[IDENTITYID].com
   - **Password:** Cyberark1

2. Click the *Waffle menu* and select **Secure Access**.
3. Click **Add** and choose *Catalog or imported app*.
4. In the *Search* field type **LinkedIn**.
5. Locate the *LinkedIn User Password* item and click **Add**.
6. Click **Yes** to confirm and then click **Close**.
7. In the *Application Settings*, enter your LinkedIn credentials.

   NOTE: If you do not have a LinkedIn account you can create one for free. Click here to register an account.

8. Click **Save**.
9. Click the tile to launch **LinkedIn**.
10. Close the *LinkedIn* tab.
11. Click **Add** and choose *Password*.
12. Type **Connect Login** in the *Name* field.
13. Type **Acme_Stats@acme.corp** in the *User Name* field.
14. Type **Acme_Password** in the *Password* field.
15. Click **Save**.

Task 3: Share the LinkedIn Web App

Share the LinkedIn app information with the Marketing manager and another team member.

1. Click the 3 ellipses on the LinkedIn tile and click **Settings**.
2. Click the *Sharing* tab.
3. Click **Add**.
4. Locate and add the following users:
   - Daniel Carter
   - Carrie Cairo
5. Click **Add**.
6. Set Daniel's password permissions to *View Password*.
7. Verify that Carrie's password permissions are set to *None*.

8. Click **Save**.

Task 4: Share the Password Secured Item

Share the secured item with the Marketing manager and another team member

1. Click the 3 ellipses on the Connect Login tile and click **Settings**.
2. Click the *Sharing* tab.
3. Click **Add**.
4. Locate and add the following users:
   - Daniel Carter
   - Carrie Cairo
5. Click **Add**.
6. Set Daniel's password permissions to *Edit Password*.
7. Verify that Carrie's password permissions are set to *View Password*.

   NOTE: The none password permission is not present on the secured item. This is because this item is solely a password storage item.

8. Click **Save**.

Task 5: Experience the Shared Password

Experience the POV of Daniel Carter, the Marketing manager. He has been granted view permissions on the LinkedIn webapp and edit permissions on the Connect Login secured item.

1. Log out as Holly Wood.
2. Log into your CyberArk Identity tenant using the following credentials:
   a. **Username:** Daniel.Carter@acme[IDENTITYID].com
   b. **Password:** Cyberark1
3. Click the *Waffle menu* and select **Secure Access**.
4. Click the 3 ellipses on the LinkedIn tile and click **Settings**.
5. Expand the **User Identity** section.
6. Review the credentials and attempt to change the password.

7. Click **Cancel**.
8. Click the 3 ellipses on the Connect Login tile and click **Settings**.
9. Review the credentials and attempt to change the password.
10. Click **Save**.

Experience the POV of Carrie Cairo, a member of the Marketing team. She has not been granted view permissions on the LinkedIn webapp and view permissions on the Connect Login secured item.

1. Log out as Daniel Carter.
2. Log into your CyberArk Identity tenant using the following credentials:
   - **Username:** Carrie.Cairo@acme[IDENTITYID].com
   - **Password:** Cyberark1
3. Click the *Waffle menu* and select **Secure Access**.
4. Click the 3 ellipses on the LinkedIn tile and click **Settings**.

NOTE: There is no **User Identity** section since the user was not granted any permissions to the password.

5. Click **Cancel**.
6. Click the LinkedIn.
7. Verify that you can access the LinkedIn account.
8. Close the LinkedIn browser tab.
9. In the Secure Access portal, click the 3 ellipses on the Connect Login tile and click **Settings**.
10. Review the credentials and attempt to change the password.
11. Click **Cancel**.
12. Log out as Carrie Cairo.

Lab 4: Secured Notes

Secured Items include secured passwords and secured notes. In this lab we will examine creating and sharing Secured notes.

Task 1: Create secured notes

1. Log in as Carlos Burg.
   - **Username:** Carlos.Burg@acme[IDENTITYID].com
   - **Password:** Cyberark1
2. Click the *Waffle menu* and select **Secure Access**.
3. Click **Add** and choose *Secured Note*.
4. Type **Wifi Information** in the *Name* field.
5. Type the following information in the *Notes* field.
   - SSID: CyberArk Training
   - Password: W1f1_pass
6. Click **Save**.
7. Log out as Carlos Burg.

Task 2: Creating and Sharing a Secured Note

1. Log in as Holly Wood.
   - **Username:** Holly.Wood@acme[IDENTITYID].com
   - **Password:** Cyberark1
2. If necessary, click the *Waffle menu* and select **Secure Access**.
3. Click **Add** and choose *Secured Note*.
4. Click the pencil next to the icon.
5. Choose BPImage.png and click **Open**.
6. Type **Camtasia License Key** in the *Name* field.
7. Type the following information in the *Notes* field.
   - CPMS-1579-GTCW
8. Click **Save**.

9. Click the *Camtasia License Key* tile.
10. Click the *Sharing* tab.
11. Click **Add**.
12. Locate and add the following users:
    - Carrie Cairo
    - Carlos Burg
13. Click **Add**.
14. Change *Carlos's* permission to **Owner**.
15. Click **Save**.
16. Log out as Holly Wood.

Task 3: Viewing a Shared Secured Note.

1. Log in as Carlos Burg.
    - **Username:** Carlos.Burg@acme[IDENTITYID].com
    - **Password:** Cyberark1
2. If necessary, click the *Waffle menu* and select **Secure Access**.
3. Click the *Camtasia License Key* tile.

When the tile opens, notice the *sharing* tab is not present, even though Carlos was made an owner of the note.

4. Log out as Carlos Burg.

Lab 5: Transfer Ownership

Transferring ownership of shared applications, secured item or folder from the item's original owner to a recipient user provides a seamless experience for all users of those shared items.

Task 1: Create a Transfer Ownership Policy

1. Log in to your Identity tenant as the default administrator.
2. If necessary, click the *Waffle menu* and select **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the name to **Transfer Ownership Policy**.
6. Navigate to **User Security Policies > User Account Settings**.
7. Change the dropdown to **Yes** next to *Transfer ownership of shared items*.
8. Click **Add**.
9. Click the dropdown next to *Owner Type* and choose **Manager**. Click **Add**.
10. Click **Add**.
11. Click the dropdown next to *Owner Type* and choose **Specified User**. Click **Add**.
12. Search for Daniel Carter, select the user, and click **Add**.

We did not configure a manager in the user table, so we need to adjust the priority order.

13. Click and drag *Daniel.carter@acme[IDENTITYID].com* to the top of the list.
14. Click **Save**.

Task 2: Manually Transfer Ownership

Prior to transferring ownership, suspend both the original owner and the target user's accounts to prevent any new items to be created during the transfer process. In this task we will transfer ownership from Carlos to Holly.

1. Navigate to **Core Services > Users**.
2. Select Carlos Burg's account.
3. Click **Actions** and choose **Suspend User**.
4. Click **Yes** to continue.

5. Repeat these steps with Holly Wood's account.
6. With both accounts suspended, select **Carlos Burg's** account.
7. Click **Actions** and choose **Transfer Ownership**.

   NOTE: Since Carlos does not have a Manager configured the transfer ownership popup defaults to *Specific User*.

8. Click **Select**.
9. Search for **Holly Wood**, select her account, and click **Add**.
10. Click **Transfer**.

Task 3: View the Transfer Status

1. Select and open **Holly Wood's** account.
2. Navigate to **Activity**.
3. Verify that the *Transfer Ownership* has completed.
4. Click **Actions** and choose **Activate User**.
5. Click **Yes** to continue.
6. Confirm the account status is set to **Active**.
7. Sign out of the tenant.

Lab 6: Add a Personal Web App

This lab will add a personal web app as an end user.

Task 1: Add an app from the catalog

1. Log in as Carrie Cairo.
    a. **Username:** Carrie.Cairo@acme[IDENTITYID].com
    b. **Password:** Cyberark1
2. Click the *Waffle menu* and select **Secure Access**.
3. Click **Add** and choose *Catalog or imported app*.
4. Search for Amazon.com (User Password) and click **Add**.

    NOTE: You will need to use your personal Amazon.com credentials for this configuration. If you do not have an amazon account, you can get one free here.

5. Click **Yes**.
6. Click **Close**.
7. In the application settings enter *your personal username and password*.
8. Click **Save**.
9. Click the **Amazon.com** tile in the *Secure Access* portal.

Lab 7: Basic Policies

Application policies are a powerful mechanism for enforcing granular security controls across web applications integrated with the platform.

Task 1: Create a Basic Application Policy

1. Log in to your Identity tenant as the default administrator.
2. If necessary, click the *Waffle menu* and select **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the name to **Basic Application Policy**.
6. Navigate to **Application Policies > User Settings**.
7. Click the dropdown next to *Allow users to add personal apps* and select **Yes.**
8. Click the dropdown next to *Enable Browser Extension Land & Catch* and select **Yes.**
9. Click **Save**.

Task 2: Review the User Account Settings

1. Open the **Basic Application Policy**.
2. Navigate to **User Security Policies > User Account Settings**.
3. Click the dropdown next to *Enable passkey authentication* and select **Yes.**
4. Click the dropdown next to *Enable users to configure Security Questions* and select **Yes.**
5. Click the dropdown next to *Permit device enrollment* and select **Yes.**
6. Click the dropdown under *Authentication Profile required to enroll device* and select **Default New Device Login Profile**.
7. Click **Save**.

Lab 8: WPM Policies

Workforce Password Management specific policies address password and passphrase requirements, application access controls, user permissions, and security enhancements.

Task 1: Create a WPM Specific Policy

1. Navigate back to the policy list.
2. Click **Add Policy Set**.
3. Change the name to **WPM Specific Policy**.
4. Navigate to **Workforce Password Management > Password Requirements**.
5. Click the dropdown next to *Allow generation of passphrase* and select **Yes.**
6. Navigate to **Workforce Password Management > User settings**.
7. Click the dropdown next to *Allow users to attach files to Secured Items* and select **Yes.**
8. Click the dropdown next to *Allow users to get passwords from Safes for personal accounts* and select **Yes.**
9. Click the dropdown next to *Enable users to access applications and Secure Passwords using TOTP* and select **Yes.**
10. Click **Save**.

Lab 9: Using Land and Catch

Task 1: Check the CyberArk Identity Browser Extension Settings

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 *Enable Land & Catch on this computer* is turned on.

Task 2: 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 UPS as the web app. Be sure you have an UPS login and that you are logged out of UPS prior to this task. To create a UPS account, click here.

1. Open a new browser tab and navigate to UPS.com.
2. Click the **Sign In** button.
3. Enter your username and password for the UPS 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 UPS tile and choose **Settings**.
7. Add tags or a note and click **Save**.

Lab 10: Configure Compromised Password Detection

Compromised password detection is a critical capability for modern identity security platforms, designed to proactively identify and mitigate risks associated with exposed credentials.

Task 1: Block the Use of Compromised or Aged Passwords

1. Log in to your Identity tenant as the default administrator.
2. If necessary, click the *Waffle menu* and select **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the name to **Compromised Password Detection Policy**.
6. Navigate to **Workforce Password Management > Password Requirements**.
7. Click the dropdown next to *Block users from launching, sharing or auto-login to applications, or Secured Items that have compromised passwords* and select **Yes**.
8. Click the dropdown next to *Block users from saving compromised passwords* and select **Yes**.
9. Navigate to **User Security Policies > Password Settings**.
10. Scroll down to *Password Age* and set the *Maximum password age* to be **45** days.
11. Click **Save**.

Task 2: Test the Compromised Password

1. Click the *Waffle menu* and select **Secure Access**.
2. Notice the CDW webapp now has a warning.
3. Mouse over the warning to verify it is for a compromised or bad password.

Lab 11: Enabling Security Images

Enabling security images is a recommended step in hardening your WPM environment.

Task 1: Enabling the Security Image

4. Log in to your Identity tenant as the default administrator.
5. If necessary, click the *Waffle menu* and select **Identity Administration**.
6. Navigate to **Settings > Authentication > Security Settings**.
7. Under *Login screen options*, check the box next to **Enable anti-phishing security image**.
8. Click **Save**.

Task 2: Set your Security Image

1. Click the user account name in the top right corner of the screen.
2. Click **Manage your account**.
3. Scroll down to *Security image* and click the **Security Image** button.
4. Select an image and click **Select**.
5. Click **Save**.

Task 3: Test the Security Image

1. Sign out of the tenant.
2. Log in to your Identity tenant as the default administrator.
3. Verify that the security image you selected is displayed on the password page.
4. Enter the password and click **Next**.