

Workforce Identity Management: Adaptive Multi-Factor Authentication

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 *Adaptive Multi-Factor Authentication* 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 free-trial tenant. The Free-trial tenant is valid for 30 days. All the lab exercises in the pre-requisite course meet the requirements for this course.






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.

Personal 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

Pre-Requisites.....	3
The Simulated Environment	5
Lab 1: Explore Existing MFA Policies and Authentication Profiles	6
Task 1: View existing MFA related policies and authentication profiles	6
Task 2: Create an Authentication Profile	6
Task 3: Create an Authentication Profile for Admins	7
Task 4: Test the Authentication Profile for Admins	8
Lab 2: Create Basic MFA Policies.....	9
Task 1: Require MFA at portal login for Contractors	9
Task 2: Update User Data to Meet the MFA Policy Requirements.....	10
Task 3: Test the MFA Policy	10
Task 4: Create a Device Enrollment Policy	11
Lab 3: Add MFA to the User Portal.....	12
Task 1: Enable MFA for CyberArk Identity Security Platform	12
Task 2: Setup Security Question in the Secure Access Portal.....	13
Task 3: Verify MFA Require to Login to the User Portal	14
Lab 4: Create an Adaptive MFA Policy.....	15
Task 1: Restrict Login to Business Days for Contractors	15
Task 2: Test the New Policy	16
Task 3: Update the New Policy	16
Task 4: Test the Updated Policy	17
Task 5: Remove the <i>Contractor MFA for Business Days</i> policy	17
Lab 5: Create Custom Attributes	18
Task 1: Create a custom attribute in CyberArk Identity	18
Task 2: Add the custom attribute to the Security Settings	18

The Simulated Environment

This Workforce Identity Management: Adaptive Multi-Factor Authentication course has a simulated environment for a fictitious company, Acme.corp. As the Identity Admin for Acme.corp, you will use an Identity platform tenant. If you have an Identity tenant from a previous Identity course, use that tenant for these labs.

This guide covers:

- Creating basic Multi-Factor Authentication in CyberArk Identity.
- Creating an adaptive MFA policy based on Risk Score.
- Creating an MFA policy in front of the CyberArk Identity User Portal.
- Add step up MFA Authentication policy in front of the CyberArk Identity Admin Portal.
- Create and use custom attributes for Multi-Factor Authentication.

Remember:

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

Lab 1: Explore Existing MFA Policies and Authentication Profiles

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: Multi-Factor Authentication Overview .
Objectives	<i>Review the Default Policy.</i> <i>Review the Authentication Profiles.</i> <i>Create an Authentication Profile with MFA challenges.</i> <i>Create an Authentication Profile for Administrators.</i>

Task 1: View existing MFA related policies and authentication profiles

The default policy has Multi-factor authentication configured for the Identity Secure Access portal. In this task we will look at reviewing the default policy and the choices that can be made.

1. Log into the Identity tenant and use the waffle menu to navigate to **Identity Administration**.
2. Navigate to **Core Services > Policies**.
3. Locate and open **Default Policy**.
4. Click **Authentication Policies**.
5. Click **CyberArk Identity Security Platform**.
6. Locate the *Default Profile (used if no conditions matched)*. It should be set to **Default Other Login Profile**.



NOTE: Policies and Authentication Profiles are separate entities and can be created at the same time. Authentication Profiles can be created prior to setting up policies, however, you must assign a profile to a policy when creating the policy.

7. Take note of the default *Session Parameters*.
8. Click **Cancel** without making any changes.
9. Navigate to **Settings > Authentication**.
10. Click to open the **Default Other Login Profile**.
11. Click **Cancel**.

Task 2: Create an Authentication Profile

It is important to create profiles that contain enough authentication mechanism choices for users to

be able to meet any MFA challenge. For increased security and MFA compliance, CyberArk recommends selecting mechanisms from different categories.

1. Click **Add Profile**.
2. Enter **MFA Required for Users** in the *Profile Name*.
3. For *Challenge 1*, check:

- Mobile Authenticator
- Email Confirmation Code
- Security Questions – leave the default number of questions at 1
- Do NOT check Password

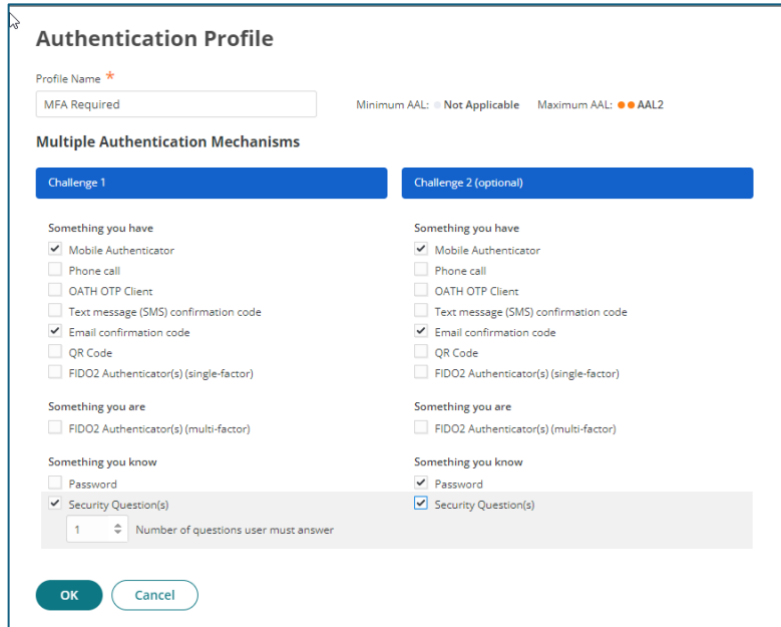


NOTE: Phone call and SMS are not available in Free Trial tenants.

4. For *Challenge 2*, check:

- Mobile Authenticator
- Email Confirmation Code
- Security Questions
- Password

5. Scroll down to **Single Authentication Mechanism**.
6. Set the *Challenge Pass-Through Duration* to **No Pass-Through**.
7. Click **OK**.



Task 3: Create an Authentication Profile for Admins

This course requires multiple logins from various users to test MFA. Create an authentication profile and policy specific for Admins that reduces the amount of MFA required. **This is not recommended in production.**

1. From the *Identity Administration Portal*, navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **1FA for Administrators**.
4. Enter a description.

Suggested: **This policy will allow Administrators to login with the password only. (Not recommended for Production environments).**

5. Under *Policy Assignment*, select **Specified Roles**.

6. Click **Add**.
7. Select the **System Administrator** role.
8. Click **Add**.
9. Navigate to **Authentication Policies > CyberArk Identity Security Platform**.
10. Click the down arrow next to *Enable authentication policy controls*, and click **Yes**.
11. Under *Default profile (used if no conditions matched)* click the down arrow and choose – **Add New Profile –**.
12. Enter **1FA for Admins** in the *Profile Name* field.
13. For *Challenge 1*, check:
 - Password
14. Leave *Challenge 2*, blank.
15. Click **Save**.
16. Verify that **1FA for Admins** is displayed in the *Default profile* field.
17. Click **Save**.
18. Click **Push Policy**.
19. Click **Yes** to confirm.

Task 4: Test the Authentication Profile for Admins

1. Click the username at the top right to **Sign Out** of the portal.
2. Log in as the **default administrator**.

The authentication policy should only prompt for a password.



You are finished with this Lab.

Lab 2: Create Basic MFA Policies

Pre-requisites	Complete the Lesson: Adaptive MFA in Identity .
Objectives	<p>Create a basic MFA authentication policy.</p> <p>Review the MFA policy settings that are active for a user.</p> <p>Verify that users can Authenticate with the MFA policy.</p> <p>Create a basic MFA device enrollment policy.</p>

Task 1: Require MFA at portal login for Contractors



SCENARIO: Acme.corp wants to follow ZeroTrust best practice and put additional security controls in place for Contractors and other CyberArk Identity Cloud Directory users when they log into the User Portal.

1. From the *Identity Administration Portal*, navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **Contractor MFA**.
4. Enter a description.

Suggested: This policy will require Contractors, who are CyberArk Cloud users, to meet an MFA challenge for Portal Login.

5. Under *Policy Assignment*, select **Specified Roles**.
6. Click **Add**.
7. Select the **Contractors** role.
8. Click **Add**.
9. Click **Authentication Policies**.
10. Click **CyberArk Identity Security Platform**.
11. Click the down arrow next to *Enable authentication policy controls*, and click **Yes**.



NOTE: Skip the rules section for now. This policy will apply 100% of the time. Later in this course we will set conditional MFA.

12. Under *Default Profile (used if no conditions matched)* click the dropdown and choose **MFA Required for Users**.

13. Scroll down to the *Other Settings* section.
14. Check the box next to **Remember and suggest last used authentication factor**.
15. Click **Save**.
16. Move **1FA for Administrators** to the top of the list.
17. Click **Push Policy**.
18. Click **Yes** on the confirmation window.

Task 2: Update User Data to Meet the MFA Policy Requirements

It is important to confirm that users who are subject to a login policy can *meet* the requirements. Update email addresses to a valid email address you have access to, to meet the MFA challenge requirements.

1. Navigate to **Core Services > Users**.
2. Locate and open **Carrie Cairo**'s user account.
3. Update the email address with a **valid email address**.
4. Click **Save**.
5. Click **Policy Summary**.
6. Verify that the new policy **Required MFA for Contractors** is present under *Authentication Policies>CyberArk Identity*.

Task 3: Test the MFA Policy

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



NOTE: An email confirmation code request will display instead of a password field. Check the email address you assigned to Carrie.Cairo's account. This may take a few minutes depending on your email service.

5. Enter the confirmation code and click **Authenticate**.
6. Enter the password for Carrie Cairo – **Password:** Cyberark!!
7. 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.

8. Click the username *Carrie Cairo* in the top right corner and choose **Sign Out**.

Task 4: Create a Device Enrollment Policy

Policies can apply to user identities as well as devices. In this task we will create a generic device policy to allow users to enroll their personal device to the Identity User Portal. This is not what is used for corporate-owned devices.

1. Log in as the default administrator account.
2. Click the *Waffle* menu and click **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the *Name* to **General Device Enrollment Policy**.
6. Enter a description.

Suggested: This policy applies to everyone and allows users to enroll personal devices to the Identity portal. This is NOT mobile device management for corporate owned devices.

7. Under *Policy Assignment* leave the default at **All users and Devices**.
8. Click **Endpoint Policies**.
9. Click **Device Enrollment Settings**.
10. Click the down arrow next to *Permit device enrollment*, and click **Yes**.
11. Click **Yes** next to *Skip MFA for invite-based enrollment*.
12. Click the dropdown next to *Invite based enrollment link expiration (default 60 minutes)* and choose **30**.
13. Click **Common Settings** on the left navigation.
14. Click **Mobile Settings**.
15. Click **Restrictions Settings**.
16. Click the dropdown next to *Permit user to unenroll devices* and click **Yes**.
17. Click the down arrow next to *Report mobile device location* and click **Yes**.
18. Leave all other settings at default.
19. Click **Save**.
20. Move **1FA for Administrators** to the top of the list.



You are finished with this Lab.

Lab 3: Add MFA to the User Portal

Pre-requisites	Complete the Lesson: MFA for the CyberArk Identity User Portal .
Objectives	<i>Create an MFA policy for the CyberArk Identity Security Platform.</i> <i>Configure end user MFA mechanisms in the Secure Access portal.</i> <i>Verify that users can Authenticate with the MFA policy.</i>

Task 1: Enable MFA for CyberArk Identity Security Platform

This policy will apply to all users and devices, and will place MFA requirements to log into the Secure Access portal.

1. From the *Identity Administration* portal, navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **MFA for the Identity Security Platform**.
4. Enter a description.

Suggested: This policy will force MFA when logging into the Identity Security Platform.

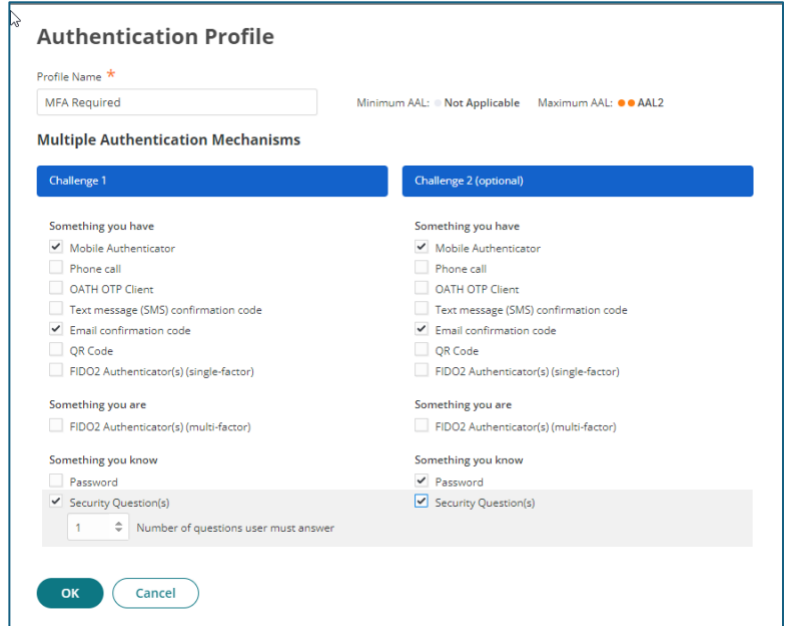
5. Under *Policy Assignment* leave the default at **All users and Devices**.
6. Click **Authentication Policies**.
7. Click **CyberArk Identity Security Platform**.
8. Click the down arrow next to *Enable authentication policy controls*, and click **Yes**.
9. Click the dropdown arrow under *Default Profile (used if no conditions matched)* to view the existing authentication profiles.
10. Click **-Add New Profile-**.
11. Enter **MFA Required** in the Profile Name.

12. For Challenge 1, check:

- Mobile Authenticator
- Email Confirmation Code
- Security Questions – leave the default number of questions at 1
- Do **NOT** check Password

13. For Challenge 2, check:

- Mobile Authenticator
- Email Confirmation Code
- Security Questions
- Password



14. Scroll down to Single Authentication Mechanism.

15. Set the Challenge Pass-Through Duration to **No Pass-Through**.

16. Click OK.

17. Verify that MFA Required is listed under *Default Profile (used if no conditions matched)*.

18. Scroll down to the *Other Settings* section.

19. Check the box next to **Remember and suggest last used authentication factor**.

20. Click Save.

21. Move **1FA for Administrators** to the top of the list.

22. Click **Push Policy**.

23. Click **Yes** on the confirmation pop up.

Task 2: Setup Security Question in the Secure Access Portal

This policy applies to all users and devices, so we need to configure the security question to use as an MFA mechanism.

1. Click the *Waffle* menu and navigate to **Secure Access**.
2. Log out as the default admin and log in as **Carrie.Cairo@acme[IdentityID].com**.
3. Click the username **Carrie Cairo** on the top right corner of the screen.
4. Click **Manage your account**.
5. Navigate to **Authentication factors**.

6. Click **Set** next to *Security Question*.
7. Click *Question* and type **What's CyberArk's signature color?**



NOTE: The question and answer here are merely suggestions. It is fine to use a different question and answer combination. Be sure you remember the answer to your question to use this mechanism for authentication.

8. Click *Answer* and type **Blue**.
9. Click **Save**.

Task 3: Verify MFA Require to Login to the User Portal

1. Click the username at the top right of the screen and **Sign Out**.
2. Enter `carrie.cairo@acme[TenantID].com`.
3. Click **Next**.
4. Click the dropdown under *Choose authentication method*.
5. Click **Security Question**.
6. Click the *Security Question* and type in the answer.
 - Security Question: **What's CyberArk's signature color?**
 - Answer: **Blue**
7. Click **Answer these questions**.
8. Click the dropdown under *Choose second authentication method*.
9. Click **Password**.
10. Enter the cloudadmin password and click **Next**.



You are finished with this Lab.

Lab 4: Create an Adaptive MFA Policy

Pre-requisites	Complete the Lesson: Adaptive MFA using Risk Score .
Objectives	<i>Create an adaptive MFA policy.</i> <i>Verify that users can Authenticate with the MFA policy.</i> <i>Update policy filters on an existing MFA policy.</i>

Task 1: Restrict Login to Business Days for Contractors

This policy will restrict login attempts from our contractors to business days only. Outside of pre-configured business days, login will be disabled. This procedure follows the same steps required for using a Risk Score.

1. From the *Admin Portal*, navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **Contractor MFA for Business Days**.
4. Enter a description.

Suggested: This policy restricts access to CyberArk Identity Security Platform for the Contractor role to approved business days only.

5. Under *Policy Assignment*, select **Specified Roles**.
6. Click **Add**.
7. Select the **Contractors** role.
8. Click **Add**.
9. Click **Authentication Policies**.
10. Click **CyberArk Identity Security Platform**.
11. Click the down arrow next to *Enable authentication policy controls*, and click **Yes**.
12. Click **Add Rule**.
13. Click **Add Filter**.
14. Click the dropdown next to *Filter* and choose **Day of the Week**.
15. Check the days of your normal work week. Be sure to include the current day for testing.
16. Click **Add**.
17. Under *Authentication Profile* choose **MFA Required**.
18. Click **Ok**.

19. Under *Default Profile (used if no conditions matched)* click the dropdown and choose **-Not Allowed-**.
20. Click **Save**.
21. Click **Push Policy** to force the policy update.
22. Click **Yes** on the confirmation pop up.

Task 2: Test the New Policy

Use Carrie Cairo's account since she is a member of the Contractors role.

1. Click the *Waffle* menu and navigate to the **Secure Access Portal**.
2. Click the username at the top right of the screen and **Sign Out**.
3. Enter Carrie Cairo's username: [Carrie.Cairo@acme\[IdentityID\].com](mailto:Carrie.Cairo@acme[IdentityID].com).
4. Click **Next**.
5. Check your *email* for the **confirmation code**.
6. Enter the confirmation code and click **Authenticate**.
7. Enter the password for Carrie Cairo – **Password**: Cyberark1!
8. Click **Next**.
9. Verify you can successfully log into CyberArk Identity.
10. Click the username *Carrie Cairo* in the top right corner and choose **Sign Out**.

Task 3: Update the New Policy

In this task we will simulate what will happen when a member of the Contractors role tries to log in outside of the approved days of the week.

1. Login as the default admin.
2. Click the *Waffle* menu and navigate to **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click the *Contractor MFA for Business Days* policy.
5. Navigate to **Authentication Policies > CyberArk Identity Security Platform**.
6. Click the *Day of the week* rule.
7. Click the *trash can* icon to the right of the rule to remove it.
8. Click **Add Filter**.
9. Click the dropdown next to *Filter* and choose **Day of the Week**.
10. Check the days of your normal work week removing the current day for testing.

11. Click **Add**.
12. Click **Ok**.
13. Click **Save**.
14. Click **Back to Policies** at the top left of the screen.
15. Click **Push Policy** to force the policy update.
16. Click **Yes** on the confirmation pop up.

Task 4: Test the Updated Policy

Use Carrie Cairo's account since she is a member of the Contractors role. This time the login should be blocked because it is outside of the approved days of the week.

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

If the policy is setup correctly, you should receive the following error message:

User does not have the attributes required to login. Please contact your administrator.

Task 5: Remove the *Contractor MFA for Business Days* policy

Remove the policy to avoid any login issues in future labs.

1. Login as the default admin.
2. Click the *Waffle* menu and navigate to **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click the checkbox next to *Contractor MFA for Business Days* policy.
5. Click the **Actions** button and choose **Delete**.
6. Click **Yes** to confirm.



You are finished with this Lab.

Lab 5: Create Custom Attributes

Pre-requisites	Complete the Lesson: Use Custom Attributes for MFA .
Objectives	<i>Create a custom attribute in CyberArk Identity.</i> <i>Configure security settings with custom attributes.</i>

Task 1: Create a custom attribute in CyberArk Identity

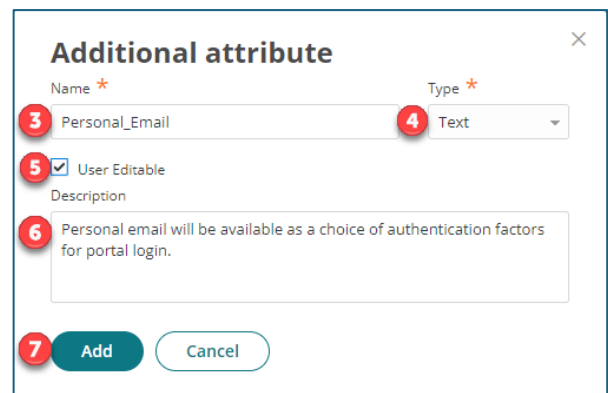
Custom attributes can extend the directory schema in the CyberArk Identity Cloud Directory.

1. Login as the default administrator.
2. Navigate to **Settings > Customization > Additional Attributes**.
3. Click **Add**.
4. Enter **Personal_Email** in the *Name* field.



NOTE: The attribute name must start with a letter and can only be letters or numbers. There must be an underscore (_) present in the name field for additional attributes.

5. Under *Type*, select **Text**.
6. **Check** the box to make this attribute *User Editable*.
7. Enter a description.
Suggested: Personal email will be available as a choice of authentication factors for portal login.
8. Click **Add**.



Additional attribute

Name * Type *

☒ User Editable

Description

Task 2: Add the custom attribute to the Security Settings

Custom attributes can be directly from the CyberArk Identity Cloud Directory or a connected directory schema.

1. Navigate to **Settings > Authentication > Security Settings**.
2. Locate the *Additional Attributes for MFA* option.
3. Click the *Attribute* drop-down and choose **Personal_Email**.
4. Under *Type*, choose **Email**.

5. Click **Add**.
6. Click **Save**.



You are finished with this Lab.