

Workforce Identity Management: Basics

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 (ey@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 *Workforce Identity Management: Basics* 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.






The exercises will build upon each other, requiring that they are completed before moving on to the next lab. Complete all of the exercises unless it is labeled as optional.

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

THE SIMULATED ENVIRONMENT	5
LAB 1: CYBERARK IDENTITY SETUP	6
Task 1 – Request an Identity Tenant.....	6
Task 2 - Explore the UI	7
Task 3 – Add a Suffix	7
LAB 2: CREATE USER ACCOUNTS.....	8
Task 1: Manually add a new User to Identity	8
Task 2: User Management Page	10
LAB 3: WORKING WITH ROLES	11
Task 1: View the default roles and policies	11
Task 2: Create Custom Roles.....	12
Task 3: Adding/removing an Individual to/from a Role	13
Task 4: Nesting Roles	15
LAB 4: BULK IMPORTS.....	16
Task 1: Bulk User Import into a Role	16
LAB 5: SYSTEM ADMINISTRATOR ROLE	18
Task 1: Add the Admin user to System Administrator.	18
Task 2: Create a granular admin role for Identity and Access Management	19
LAB 6: INTRODUCTION TO IDENTITY POLICIES	20
Task 1: Enable Self Service Password Reset and Account Unlock	20
Task 2: Create an Authentication Profile for Contractors.....	21
Task 3: Use the Authentication Profile for Contractors in a New Policy.....	22
Task 4: Test the New Policy for Contractors	23

The Simulated Environment

This Workforce Identity Management: Basics course has a simulated environment for a fictitious company, Acme.corp. As the brand-new Identity Admin for Acme.corp, you will begin with your own Identity tenant and a set of Virtual Machines (VMs) to simulate a real-world production environment.

This guide covers:

- Request an Identity Security Platform tenant. Use the form in the course with your work email and phone number.
- Set the password for the default Identity administrator account. **Remember this password.**
- Set the initial login suffix to **Acme[IdentityID].com**. The **IdentityID** is located in the welcome email.
- Run a bulk import to populate the Users Table with users.

Lab 1: CyberArk Identity Setup

This course requires a CyberArk Identity tenant.

Scenario	You are the new administrator for the fictitious company Acme . You have just subscribed to CyberArk Identity and have received your initial administrator login credentials for your Identity tenant.
Pre-requisites	Complete the Lesson: CyberArk Identity Platform .
Objectives	<i>Request</i> your Identity tenant. <i>Locate</i> the Identity ID. <i>Add</i> an additional admin user for your tenant.

The tenant initial admin username is in the welcome email from CyberArk Identity. This is the initial admin user.

Task 1 – Request an Identity Tenant

1. Complete and submit the form in the training. This should create a preconfigured email request. Copy and mail to Training-labs@cyberark.com.

NOTE: An email will arrive from **The CyberArk Team** with your tenant information. This will include the tenant url, the Identity ID, the default administrator user account, and a link to configure the default administrator password.

2. Locate the welcome email from **The CyberArk Team**.
3. Underneath the *details of your account*, click the link to get started.

To get started, please click the Log In Now button below. If you are experiencing issues, please copy the Tenant URL link above and paste it into your browser.



4. Add the password for the default administrator account. Be sure to document the password.
5. Click **Next**.

Your tenant may log you into Identity Administration directly or into one of the other configured products. If you are not in the Identity Administration portal, click the waffle menu and select **Identity Administration**.

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 – Explore the UI

1. Click **Core Services**. This is where users, roles, and policies are configured.



HINT: This is where a lot of the admin tasks are located. Most of this course will cover configurations in *Users*, *Roles*, and *Policies*.

2. Click **Users** to navigate to the *Users Table*.
3. Click your username to open the user account.
4. Click **Roles** to see the roles the default administrator is a member of.
5. Click **Apps & Widgets** in the navigation bar on the left. This is where you will configure apps for the Secure Access portal.
6. Click **Settings** in the navigation bar on the left. This is where tenant configurations will happen.

Task 3 – Add a Suffix

1. Navigate to **Settings > Customization** and click on **Suffix**.
2. Click **Add**.
3. Enter the suffix as **Acme[IdentityID].com** replacing *[IdentityID]* with the alphanumeric number in your welcome email. **Example: AcmeABT1234.com**.
4. Click **Save**.



You are finished with this Lab.

Lab 2: Create User Accounts

Scenario	As a best practice create a secondary admin account
Pre-requisites	Complete the Lesson: CyberArk Identity User Management .
Objectives	<p>Create a new user manually in the Cloud Directory.</p> <p>Add the new user to the System Administrator role.</p>

Task 1: Manually add a new User to Identity

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Users**.
4. Click **Add User**.
5. Enter **Admin** in the *Login Name* field.
6. Enter a **valid email address** in the *Email address* field. This is an email address that you can check.
7. Enter **Admin** in the *Display Name* field.
8. Under *Password Type* verify that **Manual** is selected.
9. Enter **Cyberark1!** in the *Password* and *Confirm Password* fields.
10. Under *Status*, **check** the box for *Password never expires*.
11. **Uncheck** the box next to *Send email invite for user portal setup*.

Status

- ☐ Locked
- ☒ Password never expires
- ☐ Require password change at next login (**recommended**)
- ☐ Is service user
- ☐ Is OAuth confidential client
- ☐ Send email invite for user portal setup
- ☐ Send SMS invite for device enrollment

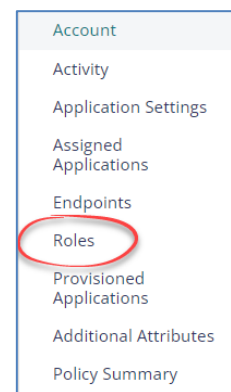


BEST PRACTICE: An admin can enter a phone number in a new account to expand the Multi-Factor Authentication (MFA) options for the initial login.

12. Click **Create User**.
13. Repeat steps 2 – 10 to create the following users in the Cloud Directory.

Login Name	Email Address	Display Name
John.Watson	John.Watson@acme.corp	John Watson
Melissa.Cohen	Melissa.Cohen@acme.corp	Melissa Cohen
Angela.Coleman	Angela.Coleman@acme.corp	Angela Coleman
Patrick.Martinez	Patrick.Martinez@acme.corp	Patrick Martinez
Allister.Harris	Allister.Harris@acme.corp	Allister Harris

14. In the Users table, click the **Admin** account to open the user account for editing.
15. Click **Roles** in the User menu to view the automatic role assignments.



Task 2: User Management Page

This task is using the **Sets Panel** to filter users in the *Users Table*.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Users**.
4. Filter the displayed users using the Sets Panel.
 - **CyberArk Cloud Directory Users**
 - **Active Directory Users**
 - **All Users**
5. Click the ellipses to the right of **All Interactive Users**.
6. Verify this set is the default view.
7. Click the arrow next to the Sets to collapse the filter view.



You are finished with this Lab.

Lab 3: Working with Roles

Scenario	<p>Before Acme can efficiently assign policies, configure Multi-Factor Authentication, and provision and deprovision Single Sign-On (SSO) apps, roles need to be setup.</p> <p>Acme wants you to be able to provision certain applications and policies for your contractors. You will need to create a Contractors role in the CyberArk Identity Directory.</p> <p>Additionally, Acme wants to have an IAM administrator with granular level Identity administrative permissions to provision applications to a large set of users.</p>
Pre-requisites	<p>Complete the lesson: CyberArk Identity Roles.</p> <p>Complete all the tasks from Labs 1 and 2 of this lab guide.</p>
Objectives	<p><i>View</i> the CyberArk Identity Default roles.</p> <p><i>Explore</i> the relationship between roles and policies.</p> <p><i>Create</i> an Identity and Access Management (IAM) Admin role with granular permissions.</p> <p><i>Create</i> custom roles.</p>

Task 1: View the default roles and policies

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Roles**.



NOTE: Depending on the CyberArk products, various built-in roles will be available. In this course we focus on the Everybody and System Administrator default roles.

4. Click the **Everybody** role and read the description.
5. Click **Members**. Membership to this role is not editable.
6. Click **Administrative Rights**.



BEST PRACTICE: When you are ready to assign tenant admin rights, create a role specifically for that purpose. **It is NOT recommended** to ever create admin rights for the Everybody role.

7. Click **Assigned Applications**. The User Portal has been assigned to Everybody. This is the default setting.
8. Click **Cancel**.
9. Click **System Administrator**. Read the description.
10. Click **Members**.



NOTE: The System Administrator role provides full Administrative Rights.

11. Click **Administrative Rights**. All Rights are included with this role and these rights are not editable.
12. Click **Cancel**.

Task 2: Create Custom Roles

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Roles**.
4. Click **Add Role**.
5. In the Name field, type **Contractors**.
6. Enter a description.

Suggested: **A role used to assign applications and policies to Contractors.**

7. Click **Save**.



NOTE: Roles may be populated manually or using the Bulk Import feature.

6. Repeat steps 1-12 for the following roles:

Role Name	Role Description
Travel Agents	Travel Agents group
Finance	Finance group
HR	HR group
IT	IT group
Marketing	Marketing group

7. Verify that the following roles are created in the *Roles Table*:

- Contractors
- Finance
- HR
- IT
- Marketing
- Travel Agents



NOTE: These roles will be used in later labs to assign users and apply policies.

Task 3: Adding/removing an Individual to/from a Role



SCENARIO: Patrick Martinez is a new member of the HR team. Add Patrick Martinez to the HR role in Identity.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Roles**.
4. Use the Search box to locate the **HR** role.
5. Click **HR** to open the role.
6. Click **Members**.
7. Click **Add**.
8. Use the search bar to locate **Patrick Martinez**.
9. **Check** the box next to his name.

10. Click **Add**.
11. Click **Save**.
12. Navigate to **Core Services > Users**.
13. Click **Patrick Martinez**.
14. Click **Roles**.
15. **Verify** that *Patrick Martinez* is a member of the **HR** role.



SCENARIO: We've just learned that Patrick has moved to the Marketing team. He must be removed from the *HR* role and added to the Marketing role.

1. Navigate to **Core Services > Roles**, locate, and open **HR**.
2. Click **Members**.
3. Check the box next to Patrick's name.
4. Click the **Actions** button.
5. Click **Delete**.



NOTE: This does NOT delete Patrick's user account. This action just removes him from this role.

6. Click **Save**.
7. Navigate to the **Marketing** role.
8. Click **Members**.
9. Click **Add**.
10. Use the search bar to locate **Patrick Martinez**.
11. **Check** the box next to his name.
12. Click **Add**.
13. Click **Save**.
14. Navigate to **Core Services > Users**.
15. Click **Patrick Martinez**.
16. Click **Roles**.
17. **Verify** that *Patrick Martinez* is a member of the **Marketing** role now.

Task 4: Nesting Roles



SCENARIO: Acme outsources some of the Finance work to contractors. We want to add the contractors role to the Finance role for application deployments.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Roles**.
4. Use the Search box to locate the **Finance** role.
5. Click **Finance** to open the role.
6. Click **Members**.
7. Click **Add**.
8. Use the search bar to locate the **Contractors** role.
9. **Check** the box next to the role.
10. Click **Add**.
11. Click **Save**.



You are finished with this Lab.

Lab 4: Bulk Imports

Scenario	You have received a list of names for the contractors, and your colleague has started a CSV file. You will need up update the csv file and import the users into the Cloud Directory.
Pre-requisites	Complete the lesson: CyberArk Identity Roles . Complete all the tasks from Labs 1 – 3 of this lab guide.
Objectives	<i>Update</i> the Acme_Contractors.csv file with your Identity suffix. <i>Perform</i> a bulk import of the Contractors. <i>Validate</i> the import completed successfully and the added contractors are in the Contractor role.

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

Task 1: Bulk User Import into a Role

1. *Locate* the spreadsheet included in the course materials titled: **Acme_Contractors.csv**.
2. **Save** it to your desktop or an accessible location.
3. **Open** the file for editing.
4. 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.

5. **Verify** that the *Contractors* role name is spelled exactly as it is in your tenant UI. **Remember that it is case sensitive.**
6. **Save** the updated .csv as a new .csv.
7. **Close** the file.
8. Log in to the Identity Platform tenant as the default admin.
9. Click the *Waffle* menu and choose **Identity Administration**.
10. Navigate to **Core Services > Users**.

11. Click the **Bulk User Import** button.
12. Click **Browse** and locate your edited **Acme_Contractors.csv** file.
13. Click the file to upload and click **Open**.
14. 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.

15. Click **Next**.
16. **Uncheck** the box next to *Send email invites for user portal setup*.
17. **Enter** your email address for report delivery.
18. Click **Confirm**.



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

19. Navigate to **Roles**.
20. Open the **Contractors** role.
21. Click **Members**.
22. **Verify** that some of the imported users are now members of the Contractors role. Click **Reload** if you do not see the new members in the Contractors role.



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



You are finished with this Lab.

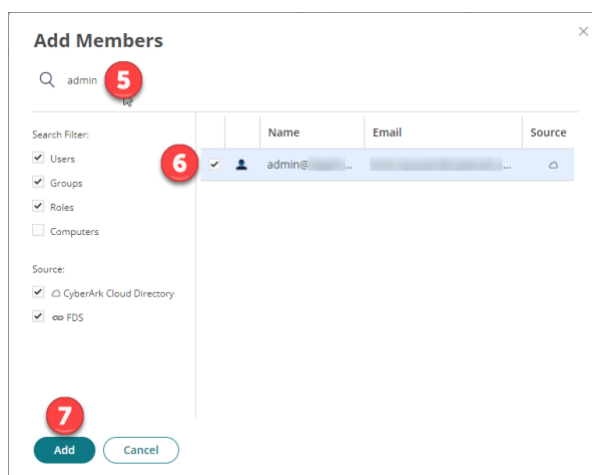
Lab 5: System Administrator Role

Scenario	With an Admin account created, it needs to be added to the appropriate role to have full system admin permissions within <i>CyberArk Identity</i> .
Pre-requisites	Complete the lesson: CyberArk Identity Roles . Complete all the tasks from Labs 1 – 4 of this lab guide.
Objectives	<i>Add</i> the new Admin account to the Systems Administrator role. <i>Create</i> a custom Administrator role with granulated admin permissions.

This lab will add the new Admin user you created to the System Administrator role. This will provide the account with the permissions necessary to administer the tenant.

Task 1: Add the Admin user to System Administrator.

1. Log into the Identity tenant with the default admin account.
2. Click the *Waffle* menu and choose **Identity** Administration.
3. Navigate to **Core Services > Roles**.
4. Locate and click on the **System Administrator** role.
5. Click **Members**.
6. Click **Add**.
7. In the search box, type **Admin**.
8. **Check** the box next to **admin**.
9. Click **Add** to add this user to the System Administrator role.



10. Click **Save**.



BEST PRACTICE: Create and use roles to provision policies and applications using Roles Based Access Controls (RBAC).

Task 2: Create a granular admin role for Identity and Access Management

1. Navigate to **Core Services > Roles**.
2. Click **Add Role** in the top right of the screen.
3. In the Name field, type **Identity and Access Admins**.



NOTE: Role names are case sensitive.

4. Enter a description.

Suggested: **Members have granular administrative rights for adding and managing applications, users, and roles.**

5. Click **Save**.
6. Click the **Identity and Access Admins** in the *Roles* table.
7. Click **Administrative Rights**.
8. Click **Add**.
9. Select the following Rights:
 - Admin Portal Login
 - ApplicationManagement
 - MFA Unlock
 - Role Management
 - User Management
10. Click **Add**
11. Click **Save**.



You are finished with this Lab.

Lab 6: Introduction to Identity Policies

Scenario	The ability to centralize policies and policy enforcement while consolidating identities is the backbone of Identity's ZERO TRUST approach. Acme wishes to leverage the Identity policy engine to establish login controls, access controls, and to secure users identities.
Pre-requisites	Complete the Lesson: Introduction to Policies You have completed Labs 1-3 in this guide.
Objectives	<i>Explore</i> the Policies engine page. <i>Create</i> a Self-Service Password Reset and Account Unlock Policy for CyberArk Cloud Directory users. <i>Create</i> a Login Policy for Contractors to require MFA.

Task 1: Enable Self Service Password Reset and Account Unlock

Enabling Self Service Password Reset (SSPR) is a very common administrative task.



SCENARIO: Acme wants to reduce the administrative overhead of their contractor accounts. If the accounts password needs to be reset, or the account needs to be unlocked, Acme wants the users to be able to resolve this issue themselves. Create a policy set that enables self-service password reset and account unlocks for the Contractors role only.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the *Name* to **Self Service PW Reset and Account Unlock**.
6. Enter a description.

Suggested: **This policy will allow Contractors to reset their Identity portal login password and unlock Account when MFA challenges are met.**

7. Under *Policy Assignment*, select **Specified Roles**.
8. Click **Add**.
9. Select the **Contractors** role.

10. Click **Add**.
11. Click **User Security Policies**.
12. Click **Self Service**.
13. Click the down arrow next to *Enable self service controls*, and click **Yes**.
14. Leave the default options:
 - Enable password reset
 - User must log in after successful password reset
15. Under *Password Reset Authentication Profile* choose **Default Password Reset Profile**.



NOTE: You can view the profile configuration by clicking the **View Profile** button. We will work with authentication profiles in a later lab.

16. Scroll down to *Account Unlock* and check **Enable Account Unlock**.
17. Under *Account Unlock Authentication Profile* choose **Default Other Login Profile**.
18. Click **Save**.
19. Navigate **Core Services > Users**.
20. Locate and open **Annie Arctica**'s user account.
21. Click **Policy Summary**.
22. Scroll down to *User Security Policy > Self Service* to verify that the new policy is applied.



NOTE: Users must be able to meet MFA challenges to reset their passwords and unlock their account.

Task 2: Create an Authentication Profile for Contractors

Authentication Profiles can be created in a number of ways. In this task, we will create a new profile directly and then a policy that uses this profile. Authentication Profiles can also be created while creating the policy at the same time.



SCENARIO: Acme does not have an Authentication Profile that matches the requirements of contracted employees. Acme would like the first Challenge to **not** include a password as a MFA option.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Settings > Authentication**.

4. Click **Add Profile**.
5. Enter **MFA Required for Contractors** in the *Profile Name*.
6. 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.

7. For *Challenge 2*, check:

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

8. Scroll down to **Single Authentication Mechanism**.
9. Set the *Challenge Pass-Through Duration* at **2 hours**.
10. Click **OK**.

Task 3: Use the Authentication Profile for Contractors in a New Policy



SCENARIO: Acme wants to follow a ZeroTrust best practice and put additional security controls in place for Contractors when they log into the User Portal.

1. Log in to the Identity Platform tenant as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Core Services > Policies**.
4. Click **Add Policy Set**.
5. Change the *Name* to **Require MFA at Login for Contractors**.
6. Enter a description.

Suggested: This policy will require Contractors, who are CyberArk Cloud Directory users,

to meet an MFA challenge for Portal Login.

7. Under *Policy Assignment*, select **Specified Roles**.
8. Click **Add**.
9. Select the **Contractors** role.
10. Click **Add**.
11. Click **Authentication Policies**.
12. Click **CyberArk Identity**.
13. 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. The Adaptive Multi-Factor Authentication course will cover using rules to apply different MFA requirements based on criteria.

14. Leave the default options.
15. Under *Default Profile (used if no conditions matched)* choose **MFA Required for Contractors**.



NOTE: If you don't see the new profile you created in Task 2, refresh the Identity tenant.

16. Scroll down to the *Other Settings* section.
17. Check the box next to **Remember and suggest last used authentication factor**. Leave all other settings the same.
18. Click **Save**.



NOTE: It is important to confirm that users who are subject to a login policy can *meet* the requirements.

Task 4: Test the New Policy for Contractors

1. Navigate to **Core Services > Users**.
2. Locate and open **Carrie Cairo**'s user account.



NOTE: An error alert should be displayed next to her email address because it is not a valid address. Replace the invalid email address with an authentic email address. You will need to be able to access this email address.

3. Update the email address with a **valid email address** you have access to.

4. Click **Save**.
5. Click **Policy Summary**.
6. Verify that the new policy **Required MFA for Contractors** is present under *Authentication Policies > CyberArk Identity*.
7. Navigate to the User Portal.
8. Click the **Admin** name at the top right of the screen and click **Sign out**.



Note: Carrie Cairo does not have permission to log into the Admin Portal. By navigating to the User Portal and logging out, you can then log in as Carrie without issue.

9. Login with **Carrie.Cairo@acme[IdentityID].com**.



Note: You should not be prompted with a password, but asked to enter a code sent to the email address.

10. Locate the email from Identity and copy the code into the Identity prompt.
11. Enter the password **Cyberark1!**.



You are finished with this Lab.