Workforce Identity Management: Custom Tenant Configurations

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 changewithout 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

Pre-Requisites

The lab exercises provide students the opportunity to practice skills learned in the *Identity Tenant Configuration* 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.

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 *best practice* 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

This Workforce Identity Management course has a simulated environment for a fictitious company, Acme.corp. As the Identity Administrator for Acme.corp, you will make branding changes to the UI and the messaging in your own Identity tenant. If you have a tenant from a previous Identity micro course, you can use that for these labs.

This guide covers:

- Customizing the tenant UI including the user and admin portals and the login page.
- Customizing the email messaging.
- Adding additional login suffixes to the tenant.

Lab 1: Customizing the User and Admin Portal

Pre-requisites	Complete the Lesson: **Customizing the Portal**.
Objectives	*Customize* the tenant with brand colors and logos.
	Configure the Company name and support links.

SCENARIO: You are the new administrator for the fictitious company **Acme.corp**. You are tasked with rebranding the CyberArk Identity tenant to match your organizations branding guidelines.

Task 1 – Customizing the Tenant

1. Login to the Identity Security Platform as the default admin.

2. Click the *Waffle* menu and choose **Identity Administration**.

3. Navigate to **Settings > Customization**.

4. Under the *Portal Ribbon Accent* type **#FO261C**.

5. Click the **Select Color** button under *Portal Ribbon Color*. Choose the "white" box (bottom left corner).

6. In the *Company Name* field, enter **Acme Corporation**.

7. In the *Company Support Link* field, enter **https://support.acme[IdentityID].com**.

NOTE: The URL for the *Company Support Link* is fictious. It is just added here as a placeholder to demonstrate the proper way to input the link.

8. Under *Portal Image* click **Upload**.

9. Locate the **AcmeLogo.png** in the *course materials* folder.

10. Click **Open** to upload.

11. Under *Short Portal Image* click **Upload**.

12. Locate the **Acmeshortlogo.png** in the *course materials* folder.

13. Click **Open** to upload.

14. Click **Save.**

Task 2 – View the Updated Support Link

The portal image and color changes are immediately visible, other changes require some portal movement.

1. Click the Waffle menu and choose **Secure Access**.

⚠️ **NOTE:** If you have the CyberArk Identity Browser Extension enabled you may receive a popup prompting you to sign in. You can sign in or click cancel. This does not affect these labs.

2. Toggle the "push pin" icon on the bottom right of the logo. This will toggle between the portal logo and the short logo.

3. Click the Waffle menu and choose **Identity Administration**.

4. Click the username at the top right corner of the screen.

5. Click **Reload Rights**.

6. Click **Reload rights** on the confirmation popup.

7. Click the **Help** button at the top right of the screen.

8. Choose **Support**.

9. In the popup section under *Online Support*, the last entry should be **Contact Acme Corporation support**.

⚠️ **NOTE:** Clicking the link for *Acme Corporation support* will load an error page because the URL was fictious.

10. Close the popup window.

STOP You are finished with this Lab.

Lab 2: Customizing the Login Screen

Pre-requisites	Complete the Lesson: **Customizing the Portal**.
Objectives	*Customize* the login experience.

Task 1 – Customizing the Login

1. Login to the Identity Security Platform as the default admin.

2. Click the *Waffle* menu and choose **Identity Administration**.

3. Navigate to **Settings > Customization**.

4. Locate the *Login Customization* section.

5. Change the *User Name Hint Text at Login* to **Name@acme[IdentityID].com**.

6. Under *Login Image* click **Upload**.

7. Locate the **AcmeLogo.png** in the *course materials* folder.

8. Click **Open** to upload.

9. Under *Login Background Image* click **Upload**.

10. Locate the **background.png** in the *course materials* folder.

11. Click **Open** to upload.

12. In the *Terms of Use Link* field, enter **https://acmeterms.com**.

13. In the *Privacy Policy Link* field, enter **https://acmeprivacypolicy.com**.

⚠️ **NOTE:** The URLs for the *Terms of Use Link* and *Privacy Policy Link* are fictious. They are added here as a placeholder to demonstrate the proper way to input the links.

14. Click **Save**.

Task 2 – The Login Experience

1. Click the username in the top right corner and select **Sign Out**.

2. Notice the following updates:

   - Background image

   - Acme logo

   - Login hint

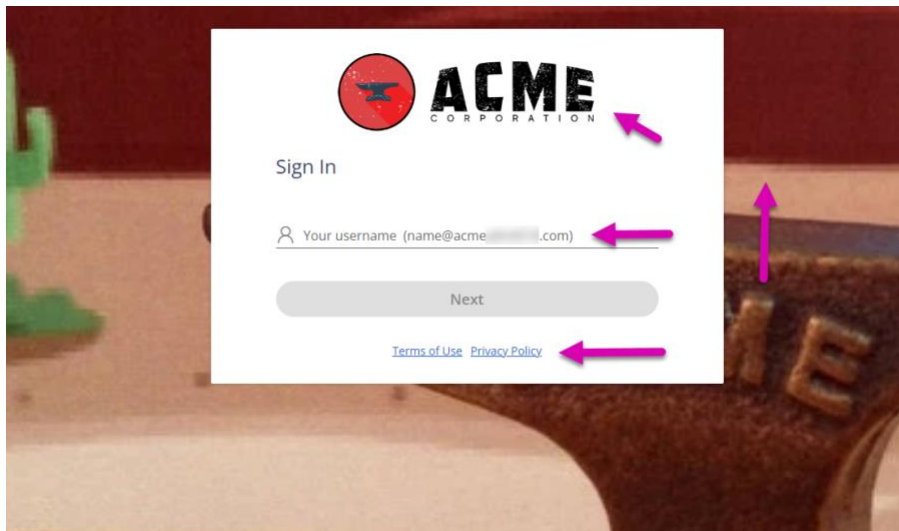   - Terms of Use and Privacy Policy links

Image may look different depending on your Identity tenant version.

⚠️ **NOTE:** Clicking the link for *Terms of Use* or *Privacy Policy* will lanuch a new tab with an error message because the URLs were fictious.

3. Login as the default administrator.

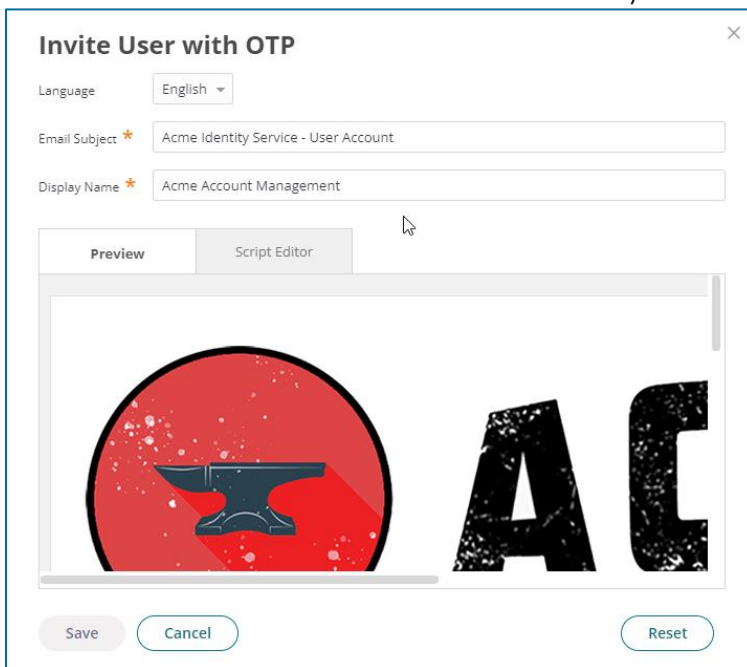4. Click **Next**.

5. Enter the *password*.

6. Click **Next**.

You are finished with this Lab.

Lab 3: Customizing the Message

Pre-requisites	Complete the Lesson: **Customizing the Portal**.
Objectives	*Customize* the email messaging.

Task 1 – Customizing the Email Messaging

1. Login to the Identity Security Platform as the default admin.

2. Click the *Waffle* menu and choose **Identity Administration**.

3. Navigate to **Settings > Customization**.

4. Scroll down to the *Message Customization* section.

5. Under *Email Image* click **Upload**.

6. Locate the **AcmeLogo.png** in the *course materials* folder.

7. Click **Open** to upload.

8. Scroll down, locate, and click the **Invite User with OTP** email message.

9. Change the *Email Subject* from CyberArk Identity Service – User Account to **Acme Identity Service – User Account**.

10. Change the *Display Name* from CyberArk Account Management to **Acme Account Management**.

11. Click **Save**.

12. Click **Save** on the *Account Customization*.

Task 2 – Verifying the Email Messaging

1. Navigate to **Core Services > Users**.

2. Locate and open *Carrie@acme[IdentityID].com*.

3. Verify and update, as needed, the *Email address* field to **your email address**.

> ⚠️ **NOTE:** If you update the email address, be sure to click **Save** before moving on to the next step.

4. Check the box next to *Carrie Cairo's* name.

5. Click the **Action** button.

6. Click **Send email invite for user portal setup**.

7. Click **Yes** on the popup to confirm.

> ⚠️ **NOTE:** The email may take a few minutes to come through.

8. Check your email to see the updates made.

🛑 **STOP** You are finished with this Lab.

Lab 4: Custom Login Suffix

This lab will create a custom login suffix. A custom suffix can be used to make login easier for end users and align with your organizations naming convention and branding guidelines.

Pre-requisites	Complete the Lesson: **Custom Login Suffix**.
Objectives	*Create* a new login suffix.
	Apply the new login suffix

📣 **SCENARIO:** Acme.corp wants you to create a custom login suffix for Contractors. This will align with their current login credentials for their apps.

Task 1 – Create a Custom Login Suffix

1. Login to the Identity Security Platform as the default admin.
2. Click the *Waffle* menu and choose **Identity Administration**.
3. Navigate to **Settings > Customization**.
4. Click **Suffix**.
5. Click **Add** on the *Suffix* page.
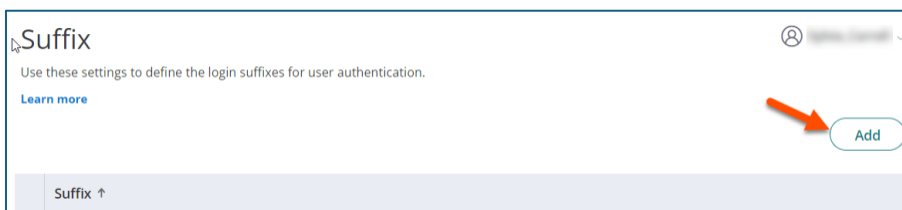
6. Leave the option to *Modify CyberArk Cloud Directory users* selected.
7. Enter **ca.acme[IdentityID].com** in the input box next to *username@*.
8. Click **Save**.

Task 2 – Applying the New Login Suffix

1. Navigate to **Core Services > Users**.
2. Locate and open *Carrie@acme[IdentityID].com*.
3. Click the dropdown under *Suffix*.
4. Click **Save**.

🛑 You are finished with this Lab.ß