Workforce Identity Management: The Identity Connector

Hands-On Training Lab Guide

Legal notice

Conditions and Restrictions

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 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 *best practice* recommendation from CyberArk, security governing bodies, or industry standards.
STOP	**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: Identity Connector course has a simulated environment for a fictitious company, Acme.corp. As the Identity Admin for Acme.corp, you will use an Identity tenant and a set of Virtual Machines (VMs) to simulate an on-premise active directory structure. Use the provisioned tenant for the Workforce Identity Management – Basics course.

This guide covers:

- Configuring the secure built-in InstallerUser account to establish a connection between CyberArk Identity and an on-prem Active Directory.
- Installation and configuration of the CyberArk Identity Connector.
- Utilizing CyberArk Identity's self-service password reset for Active Directory users.

Lab 1: Creating the InstallerUser Service Account

This lab requires a CyberArk Identity tenant configured with users.

Pre-requisites	Complete the Lesson: **The InstallerUser**.
Objectives	*Set* the InstallerUser password.

Task 1: Set the *InstallerUser* service account password

SCENARIO: You want to connect the Acme.corp active directory to the CyberArk Identity Cloud Directory. This will allow you to manage CyberArk Identity Cloud Directory users and Active Directory users in one location. This will also allow AD users to utilize CyberArk Identity's Multi-Factor Authentication and Single Sign-On features without having to manage multiple user accounts for the same user.

1. Log into the Identity tenant and use the waffle menu to navigate to **Identity Administration.**
2. Navigate to **Core Services > Users**.

NOTE: The **InstallerUser** service account resets its password automatically every 24 hours. The ***first step*** in a production environment, when installing the CyberArk Identity Connector, is to reset the InstallerUser account password.

3. On the *Sets* panel, click **All Service Users**.
4. Locate and click the checkbox next to the **InstallerUser** account.
5. Click the **Actions** button and select **Set Password**.
6. Enter and confirm a new password.

   NOTE: Remember this password. You will need this password in the next lab when you install the Identity Connector on the virtual machine.

7. Click **Save**.

You are finished with this Lab.

Lab 2: Install the Identity Connector

Pre-requisites	Complete the Lesson: **Installing the Identity Connector**.
Objectives	*Download* the Identity Connector in the Skytap virtual environment. *Install* the Identity Connector on a domain joined machine. *Configure* the Identity Connector on the domain joined machine with the Identity tenant.

Task 1: Download and install the CyberArk Identity Connector.

1. If the VM does not automatically log in, use the following credentials:
    - **Username**: mike.sing
    - **Password**: Cyberark1

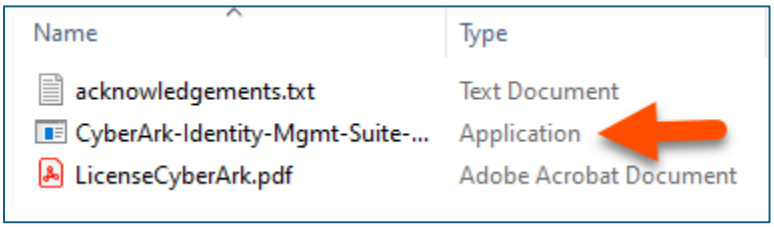
BEST PRACTICE: Click to expand the Skytap viewer to full screen. This will make it easier to see, navigate, and complete tasks within the virtual machines.

2. **Launch** the Chrome browser.
3. Navigate to your Identity tenant using your new tenant URL.
4. Log out of the identity portal and login as the default admin account.

BEST PRACTICE: Click **NEVER** if Chrome prompts you to remember the password.

5. Navigate to **Identity Administration**.
6. Navigate to **Settings > Network > CyberArk Identity Connectors.**
7. Click **Set up Connectors**.
8. **Download** the *Windows 64-bit* connector package.
9. Navigate to the *Downloads* folder in *Windows Explorer*.
10. Right-click the file name **CyberArk-Identity-Management-Suite-win64**.
11. Click **Extract All**.
12. Click **Extract**.

NOTE: The zip file that downloads will have multiple files included. Choose the file with the Application type. The extracted application will have the CyberArk logo.



13. Double click on the Application to launch the **CyberArk-Identity-Mgmt-Suite…** application.
14. Click **Next** when the *CyberArk Identity Connector [version number] Installation Wizard* opens.
15. **Accept** the *End-User License Agreement* and click **Next**.
16. In the *CyberArk Identity Connector [version number] Setup* screen, click the drop-down arrow next to **CyberArk Identity for Mobile Tools**.
17. Click the red X next to **Entire feature will be unavailable**.

NOTE: Step 18 is for the lab environment specifically. This will speed up the installation because not as many features will be installed. Since our lab environment does not deal with mobile devices, we have chosen to remove the mobile tools from the installation.

18. Click **Next**.
19. Click **Install**. The installation may take several minutes to install.
20. Click **Yes** on the User Access Control window.

NOTE: If you lose the installer window, you can find it on the taskbar with the CyberArk logo icon.

21. Click **Finish**. The Connector Configuration Wizard will open within a few seconds.

Task 2: Register your CyberArk Identity Connector to your Identity tenant

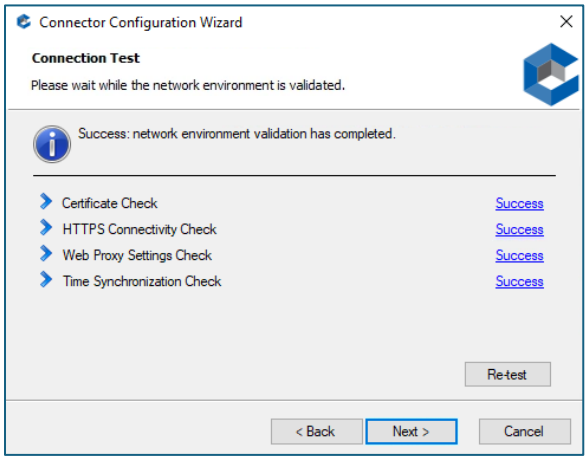
The *Connector Configuration Wizard* begins automatically when the Connector Installation Wizard finishes. It may be behind other windows open on the virtual machine. You can find it on the taskbar with the CyberArk logo icon.

1. Click **Next**.
2. Enter the **InstallerUser@acme[IdentityID].com** login name in the *Admin User Name* field.
3. Enter the **password** you created for the InstallerUser account.
4. Click **OK**.

5. Verify the checkbox next to **Enable strong encryption protocols system-wide** is checked.
6. Click **Next**.
7. Verify that *Use a Web proxy server for the Identity Platform connection* is **unchecked**.
8. Click **Next**.
9. Check the box next to *travelcom.local* to give the CyberArk Identity Connector read permissions to the deleted objects folder in Active Directory.
10. Click **Next**.
11. Click **Yes** in the pop-up pane to update container ownership.

NOTE: The connector user, InstallerUser, must have container ownership in the domain. This is only required on the first installation of the connector in the domain. Any subsequent installations, including removing and reinstalling the connector will bypass this step.

12. The configuration wizard will perform a connections test. Wait until you see 4 Successes.



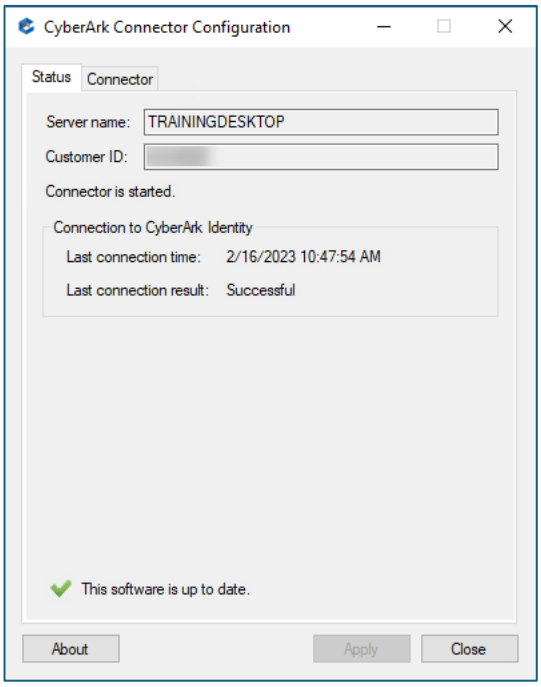
13. Click **Next**.

NOTE: The configuration wizard will start the connector service and register your Active Directory to your Identity tenant. This action may take several minutes.

14. Click **Finish** when the *Connector Setup* is complete.

Task 3: The CyberArk Connector Configuration Utility

The *CyberArk Connector Configuration Utility* window launches automatically when the *Connector Configuration Wizard* finishes.



1. Verify your **[IdentityID]** in the *Customer ID* field.
2. Click **About** to view the *Connector version*.
3. Click **OK** to close the *About* dialog box.
4. Confirm that the *Connector is started*.
5. Click the **Connector** tab.
6. Notice the options here but **do not** make any changes.
7. Click **Close**.
8. **Restart** the server if prompted. The connector is installed and configured once the system has restarted.

Task 4: Verifying the Connector in the CyberArk Identity Admin Portal

Complete this task after the *TrainingDesktop VM* has successfully restarted.

HINT: As part of the ***CyberArk Identity Connector*** installation, a shortcut to the **Admin Portal** is created on the desktop. This shortcut will launch the *legacy UI* for the Admin Portal. **This is NOT recommended for this course.**

1. From the *Identity Administration Portal,* navigate **Settings > Network**.
2. Locate the **TrainingDesktop** connector in the table.
3. Verify the connector is **Active** in the Status column.

Task 5: Managing active directory accounts in CyberArk Identity

After the Identity connector is installed and configured, the Identity admin can manage both cloud and active directory users from the Identity tenant.

1. From the *Identity Administration Portal*, navigate to **Core Services > Roles**.
2. Open the *System Administrator* role.
3. Click **Members**.
4. Click **Add**.

5. Seach for **Mike.Sing**.

NOTE: Mike Sing is an Active Directory user. Under the source column, there is a yellow triangle that identifies this as an Active Directory user.

6. Click the checkbox next to Mike's name and click **Add**.
7. Click **Save**.

Although Mike Sing is now a System Administrator, he will not show up in the users table until he logs into the Identity platform the first time. Identity does not duplicate records from Active Directory so it can only manage accounts that have logged into the system, however, because of the connector, admins in Identity can see users in Active Directory and manage their roles, web apps, policies, and more.

8. Sign out as the default admin and sign is as Mike Sing.

- **Username**: mike.sing
- **Password**: Cyberark1

9. Navigate to **Core Services > Users**.
10. Verify that **Mike Sing** is in the *Users Table*.

You are finished with this Lab.

Lab 3: Create a Self-Service Password Reset Policy

Pre-requisites	Complete the Lesson: **Scenario: Self-Service Password Reset Policy**.
Objectives	*Create* a self-service password reset policy. *Verify* the self-service password reset policy works.

Task 1: Verify that Self Service Password Reset is Disabled in Default Profile

Self-Service Password Reset should be disabled by default in the Default Profile, however this setting may have been changed in previous labs or when exploring all the settings. For this lab to work correctly we need to make sure that this setting is disabled in the default profile.

1. From the *Identity Administration Portal*, navigate to **Core Services > Policies**.
2. Click **Default Policy**.
3. Click **User Security Policies**.
4. Click **Self Service**.
5. Verify that the *Enable self service controls* is set to **--**. Adjust as needed.
6. Click **Save**.

Task 2: Enable Self Service Password Reset

Enabling Self Service Password Reset (SSPR) is a very common administrative task. This task can be used for Active Directory accounts as well as CyberArk Identity Cloud Directory accounts.

SCENARIO: Acme.corp wants to reduce the administrative overhead of their contractor accounts. If the accounts password needs to be reset, users should 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. Click **Add Policy Set**.
2. Change the *Name* to **Self Service PW Reset for Contractors**.
3. Enter a description.

   Suggested: **This policy will allow Contractors to reset their Identity portal login password when MFA challenges are met. (This does not apply toActive Directory users).**
4. Under *Policy Assignment*, select **Specified Roles**.
5. Click **Add**.
6. Select the **Contractors** role.
7. Click **Add**.

8. Click **User Security Policies**.
9. Click **Self Service**.
10. Click the down arrow next to *Enable self service controls*, and click **Yes**.
11. Leave the default options:
    - Enable password reset
    - User must log in after successful password reset

NOTE: By default, self service password reset is not allowed for Active Directory users. Some organizations do use this self-service option to allow AD users to reset their password. It is strongly recommended to use MFA authentication with this option.

12. Under *Password Reset Authentication Profile* choose **Require MFA at Login for Contractors**.
13.
14. Click **Save**.
15. Navigate **Core Services > Users**.
16. Locate and open **Annie Arctica**'s user account.
17. Click **Policy Summary.**
18. Scroll down to *User Security Policy > Self Service* to verify that the new policy is applied.
19. Verify that *Allow password reset for Active Directory users* is set to **No**.

NOTE: Users must be able to meet MFA challenges.

20. Click **Back to Users**.

Task 3: Enable Self Service Password Reset for AD Users

1. From the *Identity Administration Portal*, navigate to **Core Services > Policies**.
2. Click **Add Policy Set**.
3. Change the *Name* to **Self Service PW Reset for All Users**.
4. Enter a description.

   Suggested: **This policy will allow all users, including Active Directory users, to reset their Identity portal login password when MFA challenges are met.**
5. Under *Policy Assignment*, select **All Users and Devices**.
6. Click **User Security Policies**.

7. Click **Self Service**.
8. Click the down arrow next to *Enable self service controls*, and click **Yes**.
9. Check the box next to **Allow for Active Directory users**.
10. Under *Password Reset Authentication Profile* choose **Default Password Reset Profile**.
11. Click **Save**.
12. Navigate to **Core Services > Policies**.
13. Click **Push Policy**.
14. Navigate to **Core Services > Users**.
15. Locate and open **Mike Sing**.
16. Click **Policy Summary**.
17. Verify that *Self Service > Allow password reset for Active Directory users* is set to **Yes**.

You are finished with this Lab.