Linux Server Access Via CyberArk – UCP User Guide

CLOUD4C SERVICES PVT LTD

Document control

Prepared By

Version	Author	Date
V 1.0	Sai Krishna	29-04-2022

Reviewed By

Version	Reviewer	Date
V 1.0	Priyadarshi Mishra	30-04-2022

Approved By

Version	Approver	Date
V 1.0	Harmandeep Singh	30-04-2022

Change Control

Version	Change Reason	Effective Date
V 1.0	Initial Release	

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating CtrlS & Cloud4C Datacentres' Ltd. The information contained herein is to be considered confidential. Customer, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by Ctrl S Datacentres' Ltd.
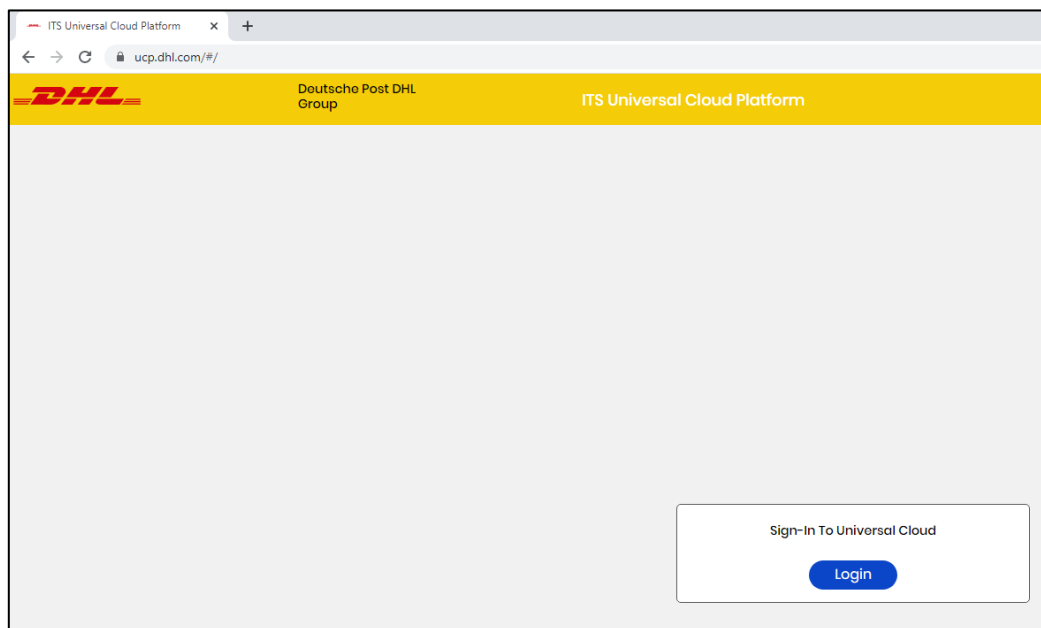
Contents

1. Introduction to UCP

Welcome to the UCP user guide

This document emphasizes on accessing a server via Cyberark

1. Ordering for server access via UCP
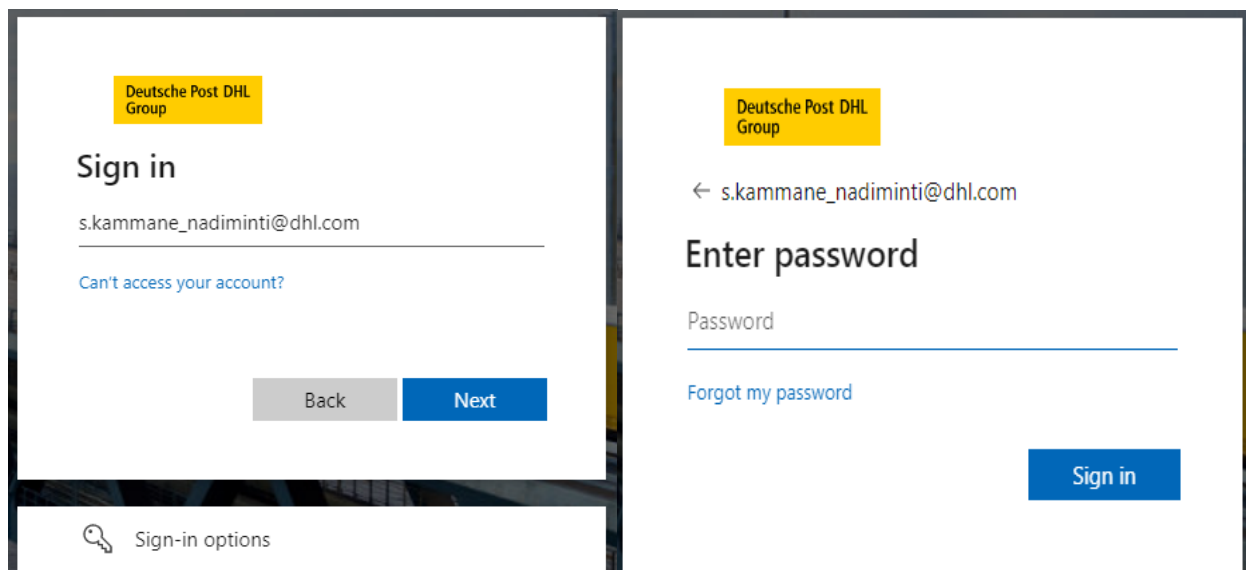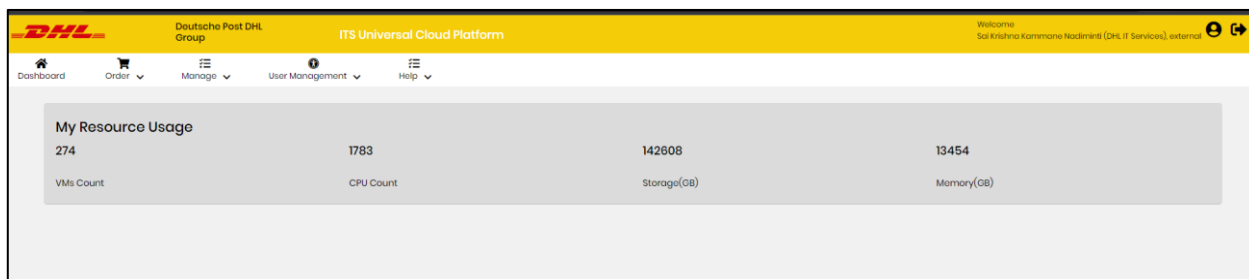2. Steps in Cyberark to access VM

2. Procedure

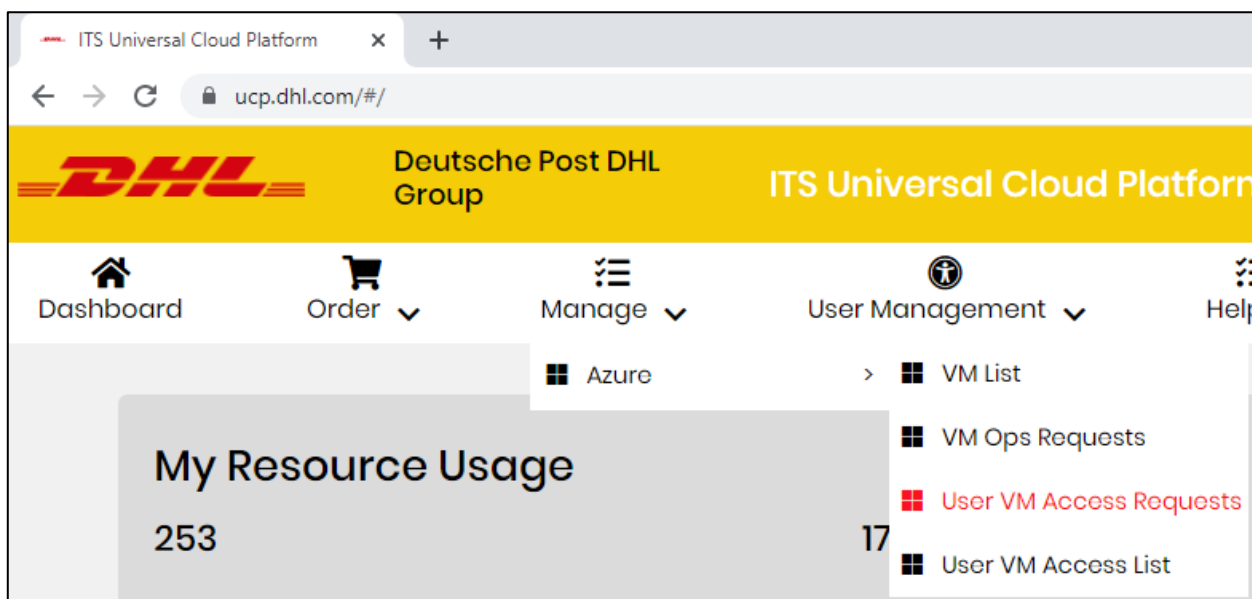Step 1 – Navigate to https://ucp.dhl.com

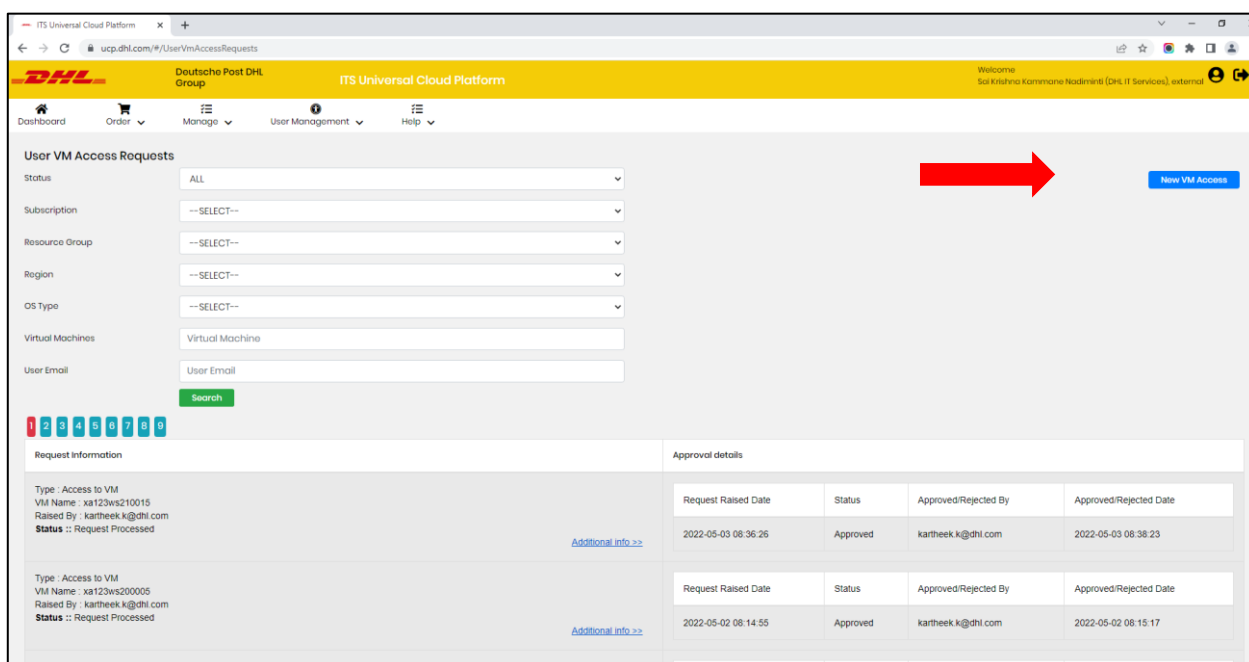Step 1.a – Enter your DHL email id AD Credentials

The user will be landing on the dashboard as shown hereunder

Step 3 – Navigate to Manage -> Azure -> User VM Access Requests.

b. Click on New VM Access request

A Pop-up screen will appear.

Step 2 : Select the Subscription, Resource Group, OS Type: Linux, Account Type

BU Sysadmin – A Business user Admin who needs temporary access to all the virtual machines in the resource Group

BU Application Admin – A Business user Admin who needs temporary access to all the virtual machines of different application types such as Apache, Tomcat, JBOSS, Weblogic and Oracle Database, within the resource Group.

Select the email in the "Provide Access to" Dropdown list.

Note: If an email id is not visible in the dropdown list, then please refer to "AAD User Onboarding - UCP User guide v 1.0" to onboard the email id to UDLDHL-PVWA Group first. After 45-60 minutes the email id will appear in the dropdown list below.

Select the desired duration and click on "Submit"

The request then goes for an approval to the Resource Group Owner / Team Manager

Click on Approve -> Proceed

The requestor will receive an acknowledgement

Request Information			Approval details			
Type : Access to VM Safe Name : SADMIN_EU_-dhl-testing, SADMIN_AP_-dhl-testing, SADMIN_US_-dhl-testing Raised By : s.kammane_nadiminti@dhl.com **Status ::** Request Processed		Additional info >>	Request Raised Date	Status	Approved/Rejected By	Approved/Rejected Date
			2022-05-03 05:28:15	Approved	s.kammane_nadiminti@dhl.com	2022-05-03 05:28:35

Request Details ✕

Subscription	7e8e1e96-c128-42b8-a445-d18281754604 / ITS-SPCS-Azure-Managed-VM-PROD-122
Resource Group	rg-dhl-testing
OS Type	Linux
Application Type	ALL
Duration	0 Days 1 Hours
Provide Access To	heena.rawal@dhl.com
Safe Name	SADMIN_EU_-dhl-testing, SADMIN_AP_-dhl-testing, SADMIN_US_-dhl-testing
Server Response Message	heena.rawal@dhl.com added to safe SADMIN_AP_-dhl-testing of resource group rg-dhl-testing in AP heena.rawal@dhl.com added to safe SADMIN_EU_-dhl-testing of resource group rg-dhl-testing in EU heena.rawal@dhl.com added to safe SADMIN_US_-dhl-testing of resource group rg-dhl-testing in US

The user who needs the access to the Virtual Machine will receive an acknowledgement email with the steps to login to the requested machine.

Below are the steps

Step1: Login into DHL network (VDI/VPN) and access the below PAM URL based on Region.

Region	URL
SEA	https://pvwa-sea.dhl.com
West EU	https://pvwa-weu.dhl.com
East U.S	https://pvwa-eus.dhl.com

Figure-1: SEA PAM URL

CLOUD4C SERVICES PVT LTD

CLOUD4C
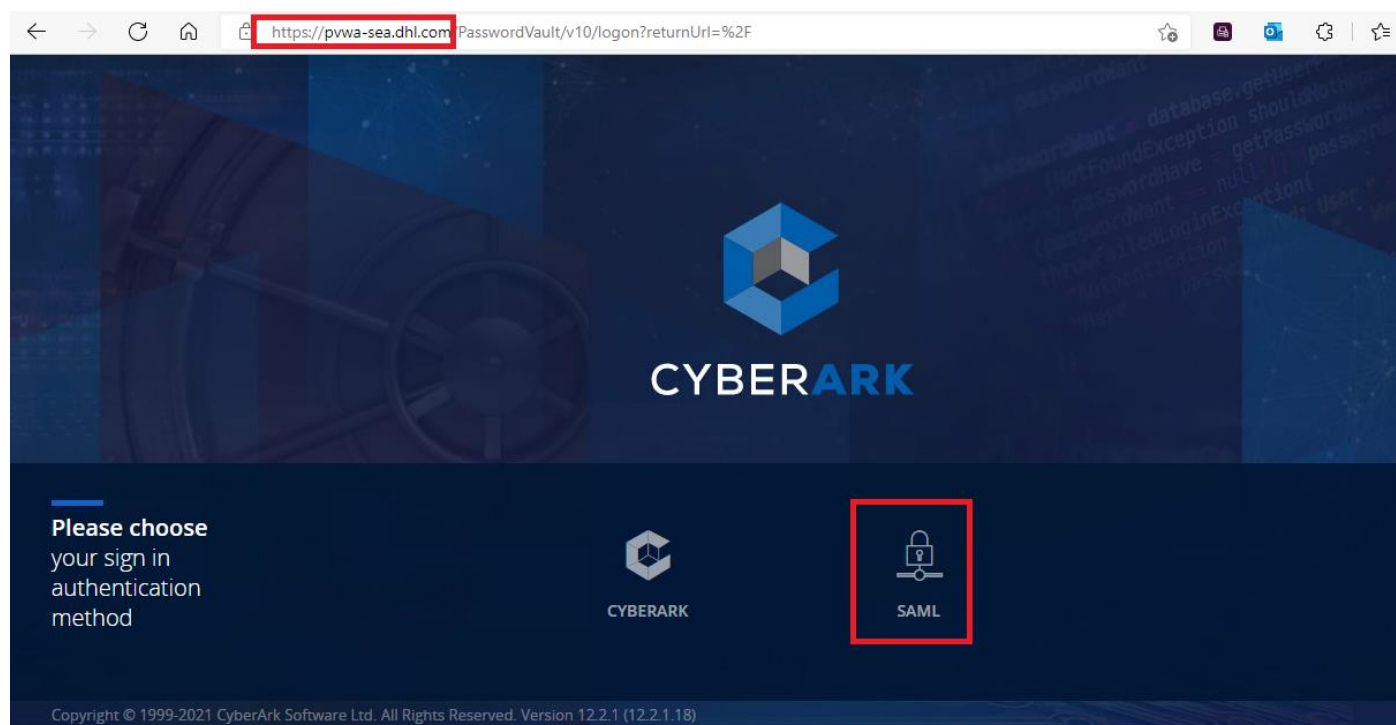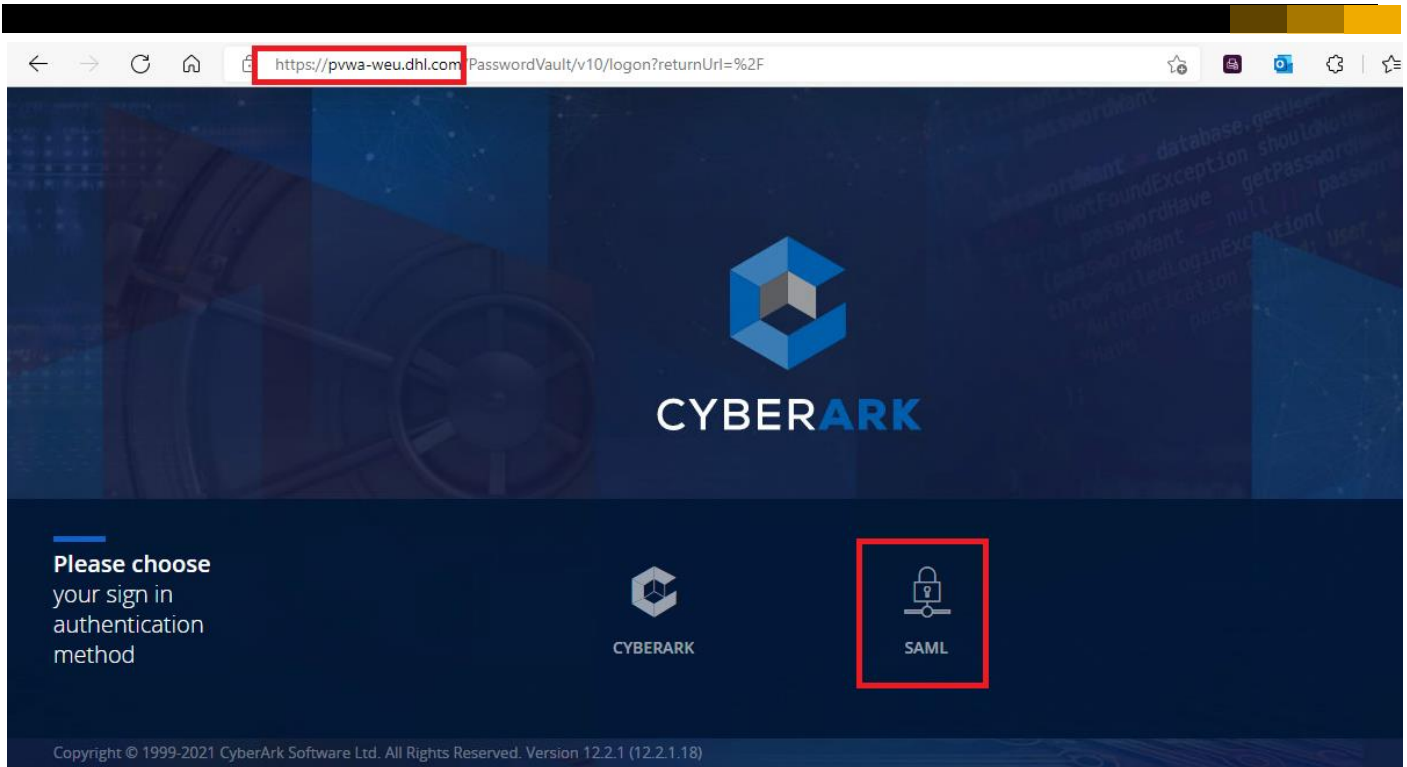

Figure-2: WEU PAM URL
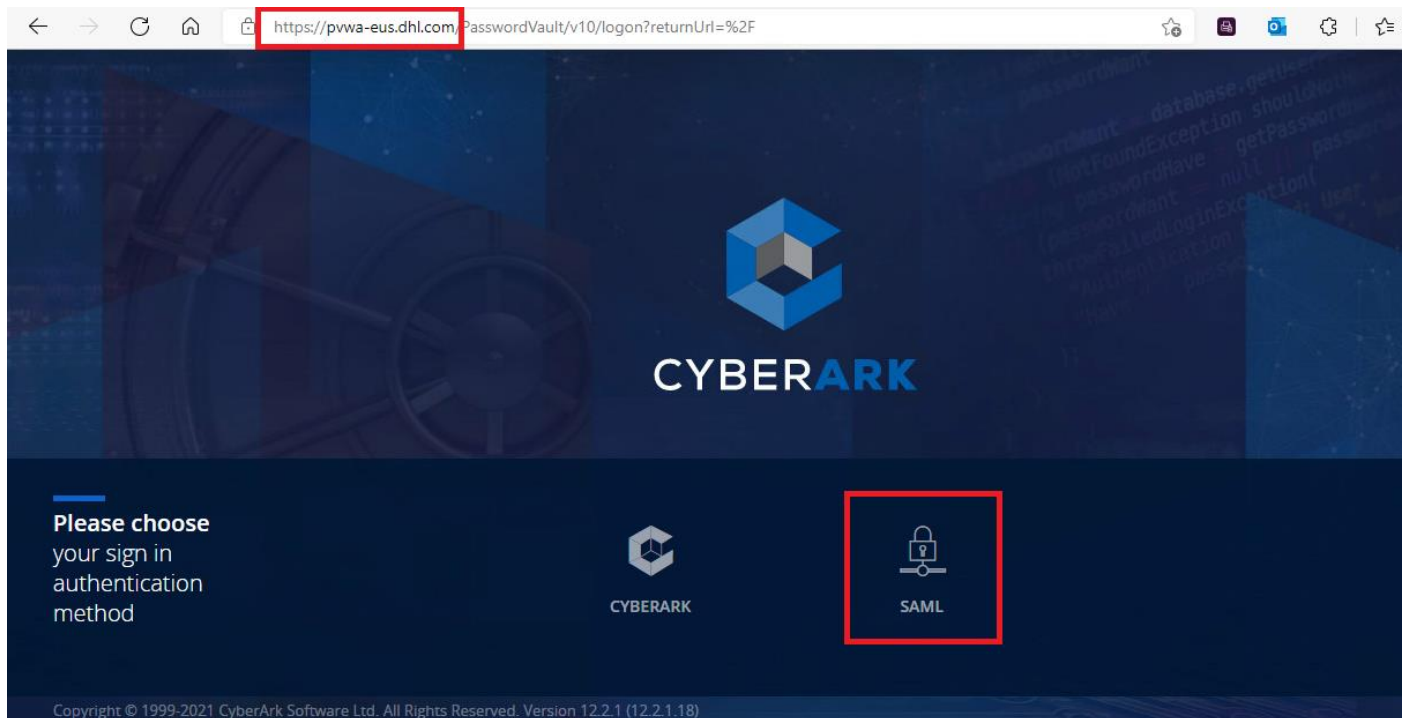

Figure-3: EU.S PAM URL

Step2: Click on SAML authentication for login and then it will login directly to CyberArk Console using Azure AD credentials.

Figure-4: On Login End User Dashboard.

Step3: Navigate (On Left Pane) select Accounts → PSM for SSH MFA Caching.

Figure-5: Navigating to PSM for SSH MFA Caching Tab.

Step 4: Click on Generate and Download PPK private key from CyberArk portal (Which is valid for 60 minutes) from PSM for SSH MFA Caching window.
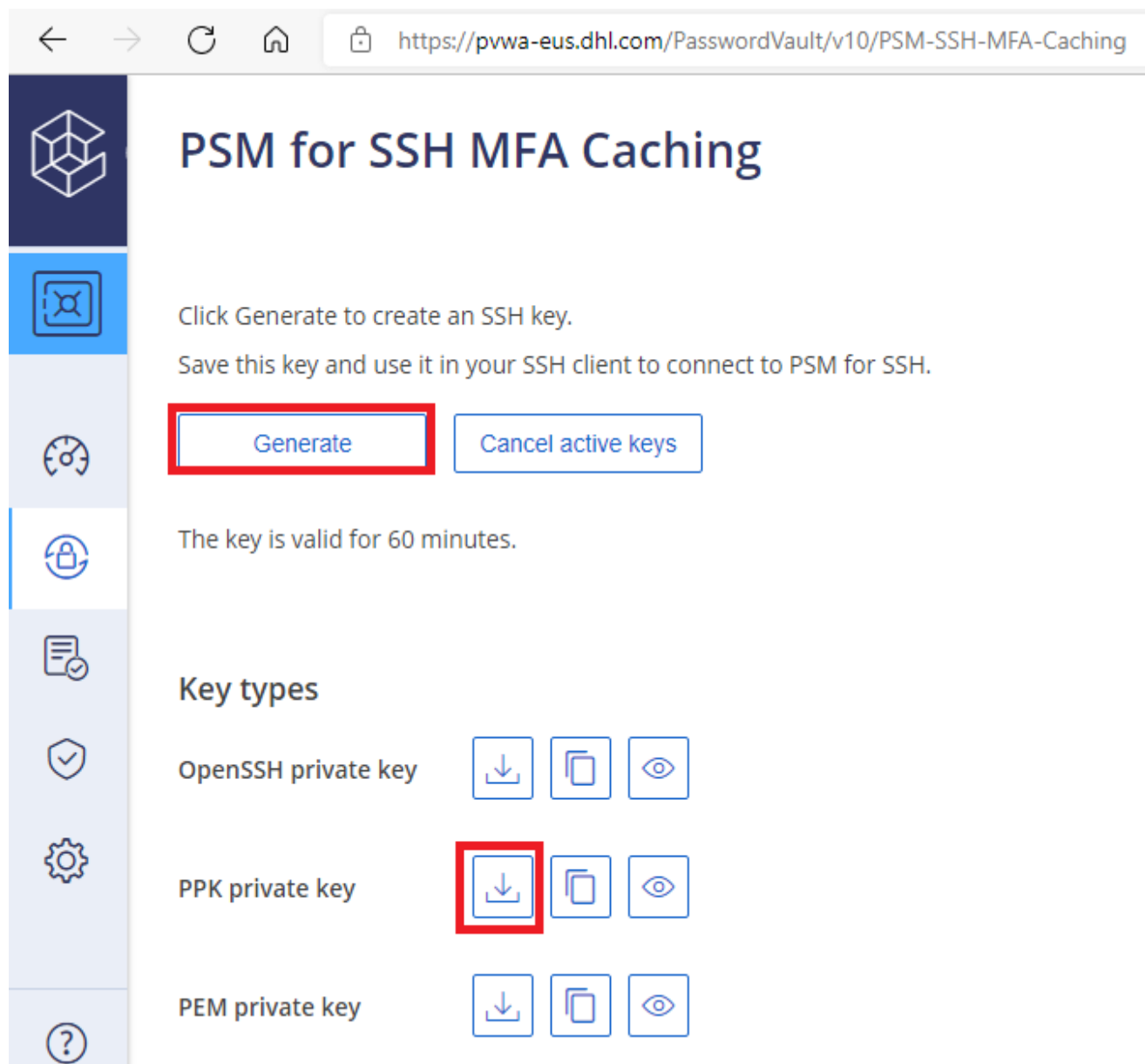

Figure-6: Generating Private Keys

Step4: Import the private key into putty (On Putty Application left pane select Connection → SSH → Auth → Private key file for authentication)
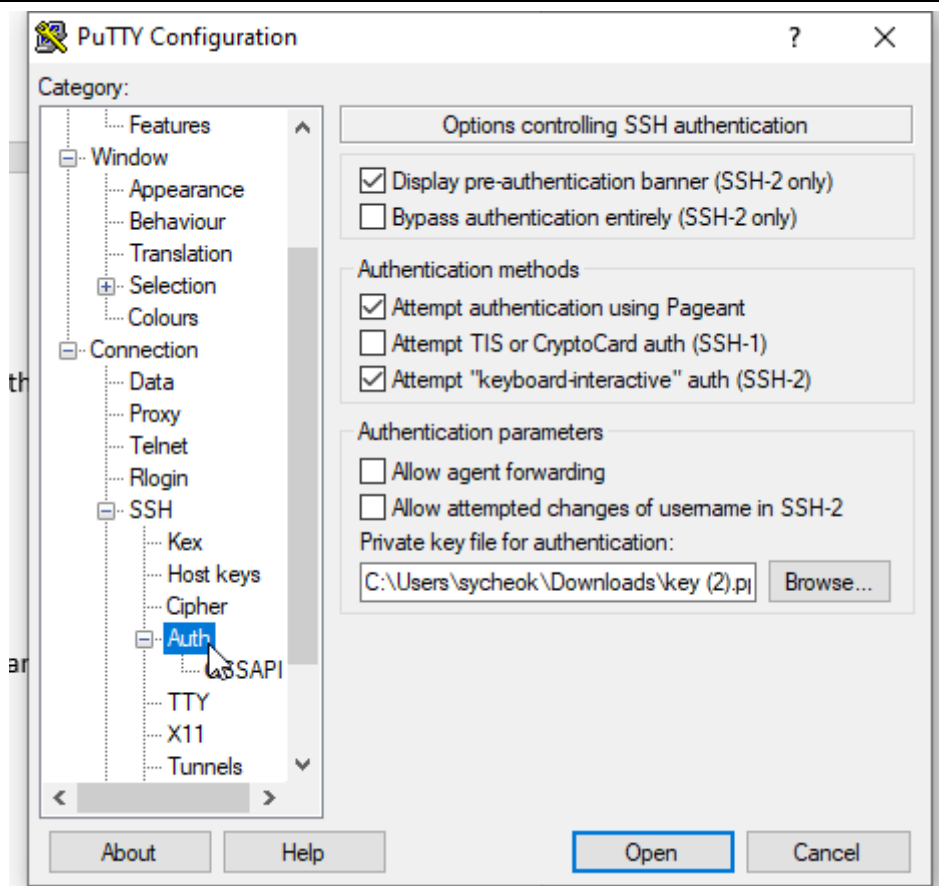
Figure-7: Connection through Putty Private Key

Step5: Prepare the connection string and put it into the hostname. (Session → Hostname)

Connection String: <CyberArkUserID>%<TargetAccountName>%<TargetServerIP>@<RegionSpecificPSM-SSHServerLoadBalancerIP>

Example: keerthana.ch@dhl.com%sadminits%10.224.174.4@10.224.18.42

East US PSM-SSH Load Balancer IP: 10.224.18.42

West Europe PSM-SSH Load Balancer IP: 10.156.9.145
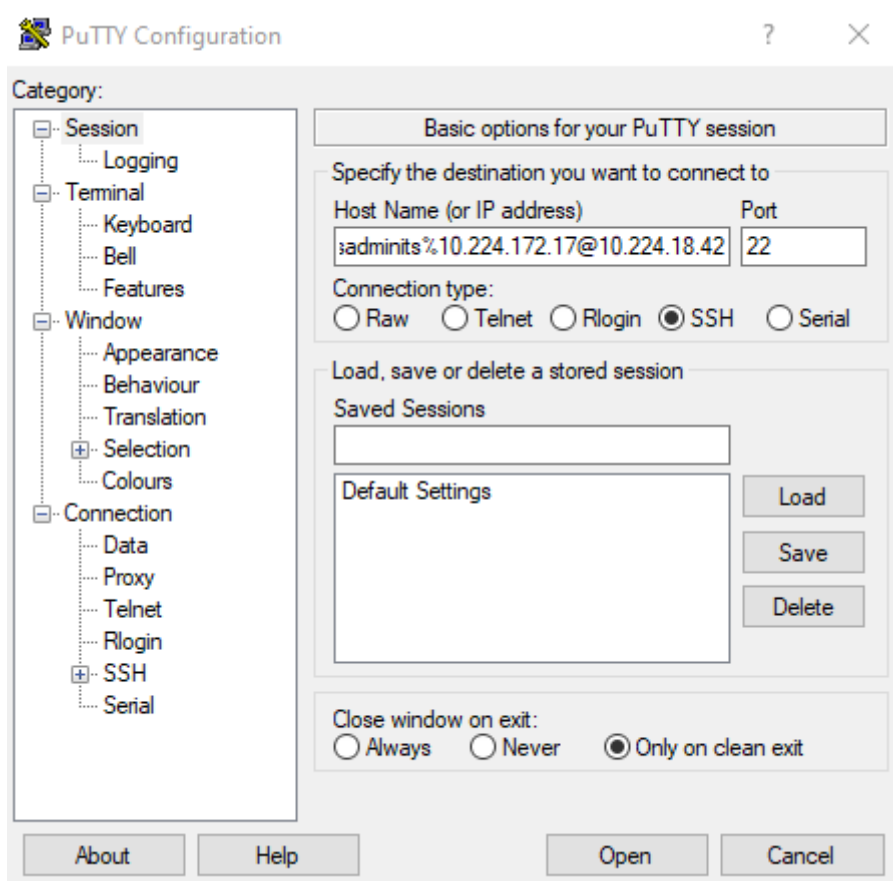
SEA PSM-SSH Load Balancer IP: 10.234.1.72

Figure-7: Connection to Target server using MFA Cache

Step 6: Specify the reason for accessing the target server and continue accessing the server.
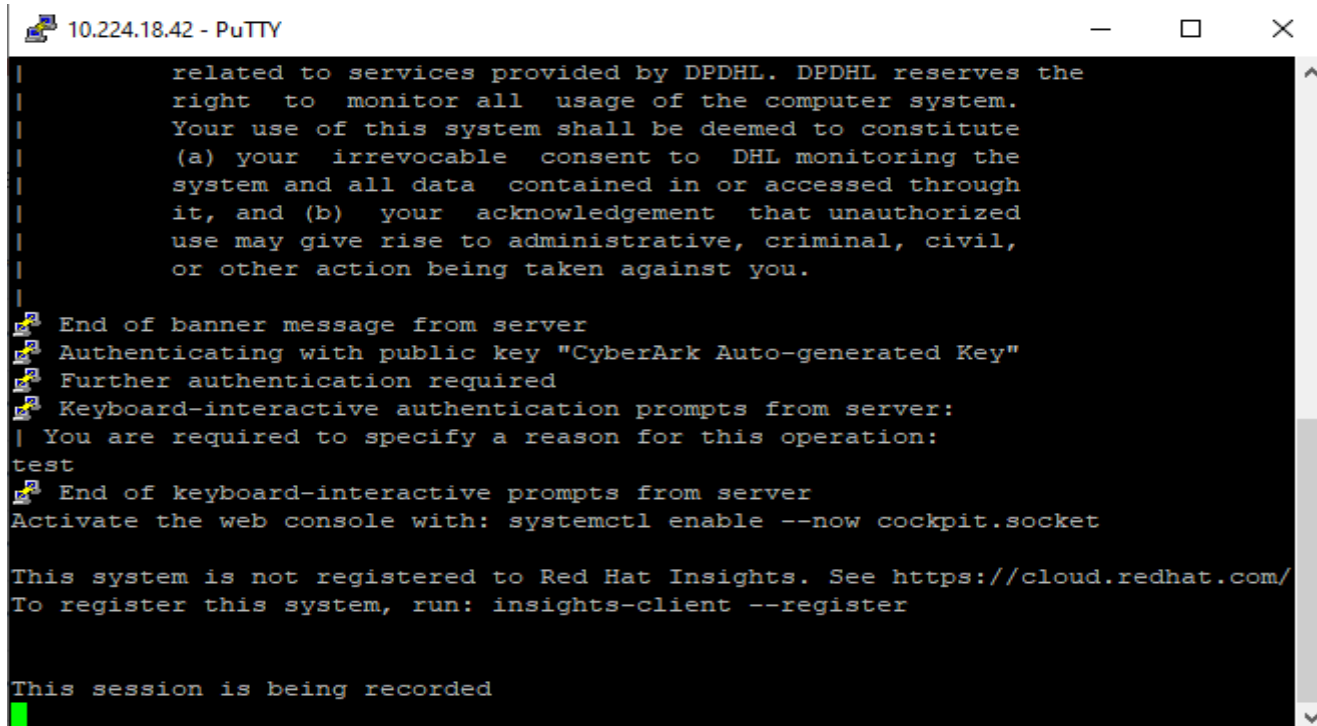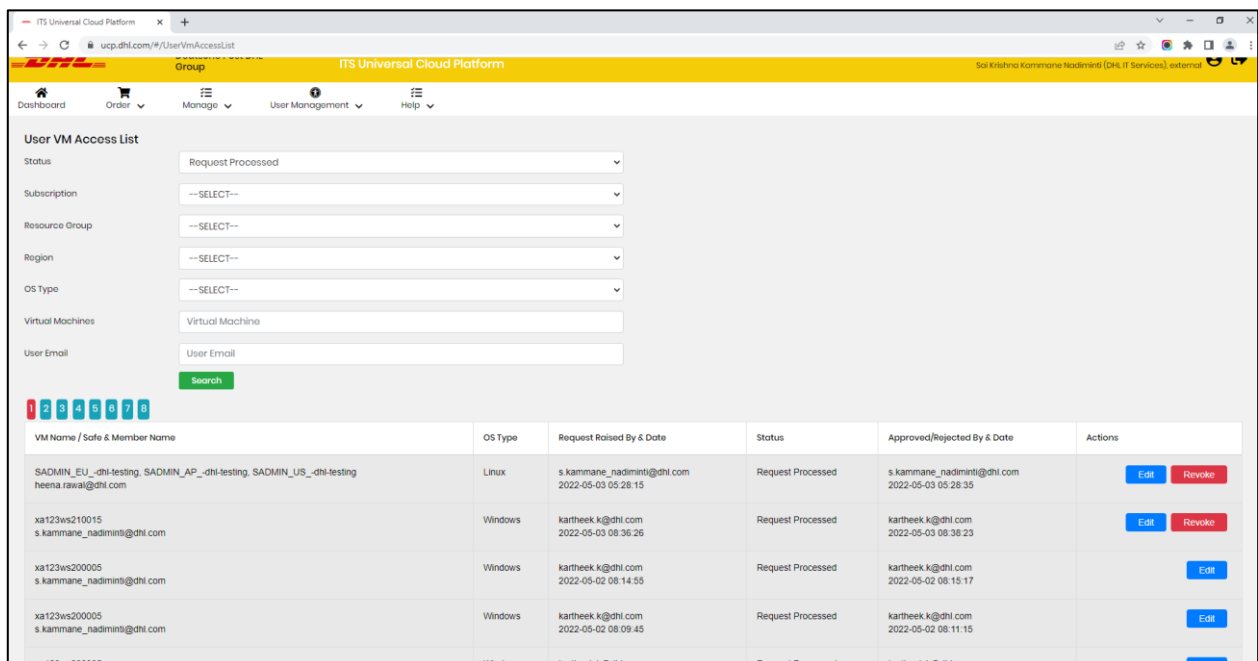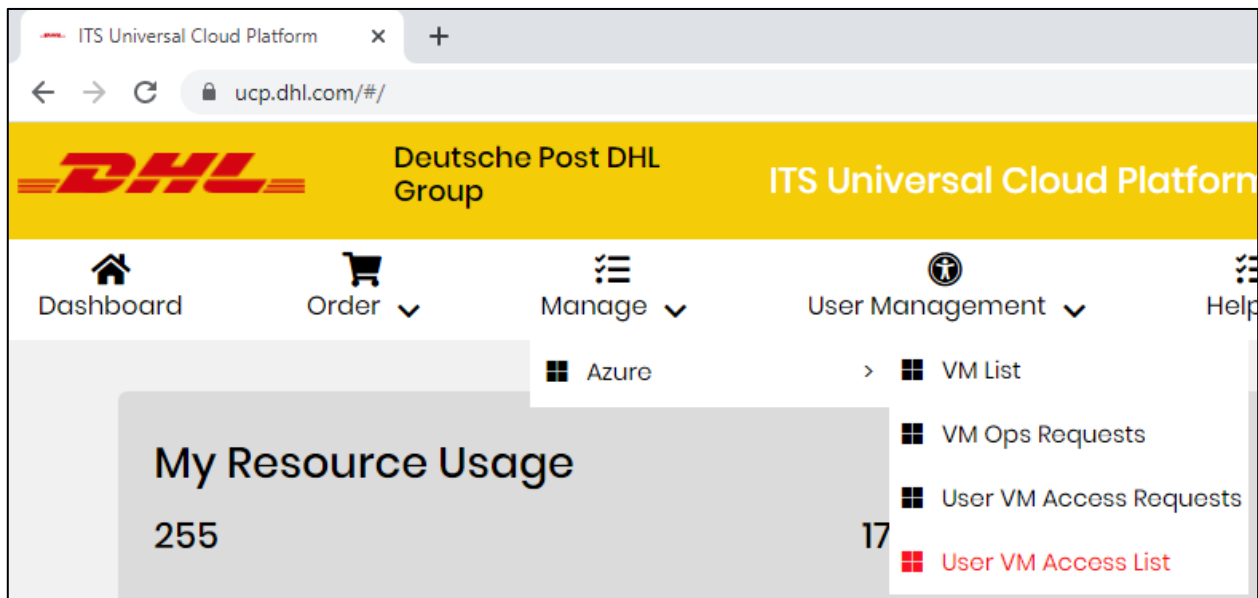

Figure-8: Access to target server

Step 2 : Extending the duration of the access.

Navigate to Manage -> Azure -> User VM Access List

The user can modify the duration of the by clicking on the edit button as shown below.

Click on "Update" for the duration to be updated.

The requestor will receive an acknowledgement email with the information about extended duration.

Step 3 – Revoke Access

The Resource group Owner can request to revoke the access of the virtual machines in the resource group at any time, so the business user is not allowed to access them at anytime.

Clicking on OK, will revoke the access of the servers to the business user.

3. Glossary

3.1 Definition

Terms	Abbreviation
VM	Virtual Machine
UCP	Universal Cloud Platform