



Identity Workshop



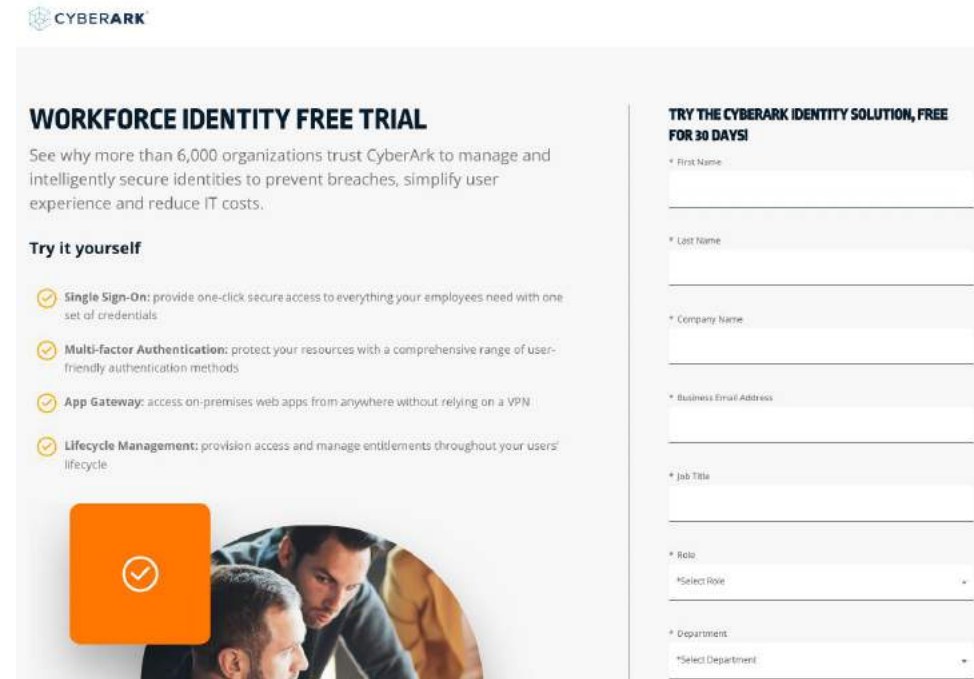
CyberArk Workforce Identity

In this workshop we will configure Single Sign On (SSO) authentication, which allows users to access all published applications with a single set of credentials. Then, we'll enable multi-factor authentication (MFA) to add a layer of security control in verifying users' identity. Finally, we will review Workforce Password Management (WPM) and browser extension to capture username/password fields on login pages automatically.

1. Start by signing up for a 30-day trial of CyberArk Workforce Identity at this url:
<https://www.cyberark.com/try-buy/workforce-identity-trial/>
2. Continue the process by confirming the code received via email (check spam folder)

CYBERARK IDENTITY FREE TRIAL REQUEST CONFIRMATION

👉 Your trial tenant has been successfully created. Instructions will be sent to your registration email.



The image shows a registration form for the CyberArk Workforce Identity Free Trial. The form is titled "WORKFORCE IDENTITY FREE TRIAL" and includes a sub-header "TRY THE CYBERARK IDENTITY SOLUTION, FREE FOR 30 DAYS!". Below the title, there is a paragraph explaining the benefits of the trial. The form is divided into two main sections: "Try it yourself" and "TRY THE CYBERARK IDENTITY SOLUTION, FREE FOR 30 DAYS!". The "Try it yourself" section lists four key features: Single Sign-On, Multi-factor Authentication, App Gateway, and Lifecycle Management. The "TRY THE CYBERARK IDENTITY SOLUTION, FREE FOR 30 DAYS!" section contains a series of input fields for user information: First Name, Last Name, Company Name, Business Email Address, Job Title, Role (with a dropdown menu), and Department (with a dropdown menu). An orange square with a white checkmark is overlaid on the bottom left of the form, indicating successful registration.

CYBERARK

WORKFORCE IDENTITY FREE TRIAL

See why more than 6,000 organizations trust CyberArk to manage and intelligently secure identities to prevent breaches, simplify user experience and reduce IT costs.

Try it yourself

- 👉 **Single Sign-On:** provide one-click secure access to everything your employees need with one set of credentials
- 👉 **Multi-factor Authentication:** protect your resources with a comprehensive range of user-friendly authentication methods
- 👉 **App Gateway:** access on-premises web apps from anywhere without relying on a VPN
- 👉 **Lifecycle Management:** provision access and manage entitlements throughout your users' lifecycle

TRY THE CYBERARK IDENTITY SOLUTION, FREE FOR 30 DAYS!

* First Name:

* Last Name:

* Company Name:

* Business Email Address:

* Job Title:

* Role:

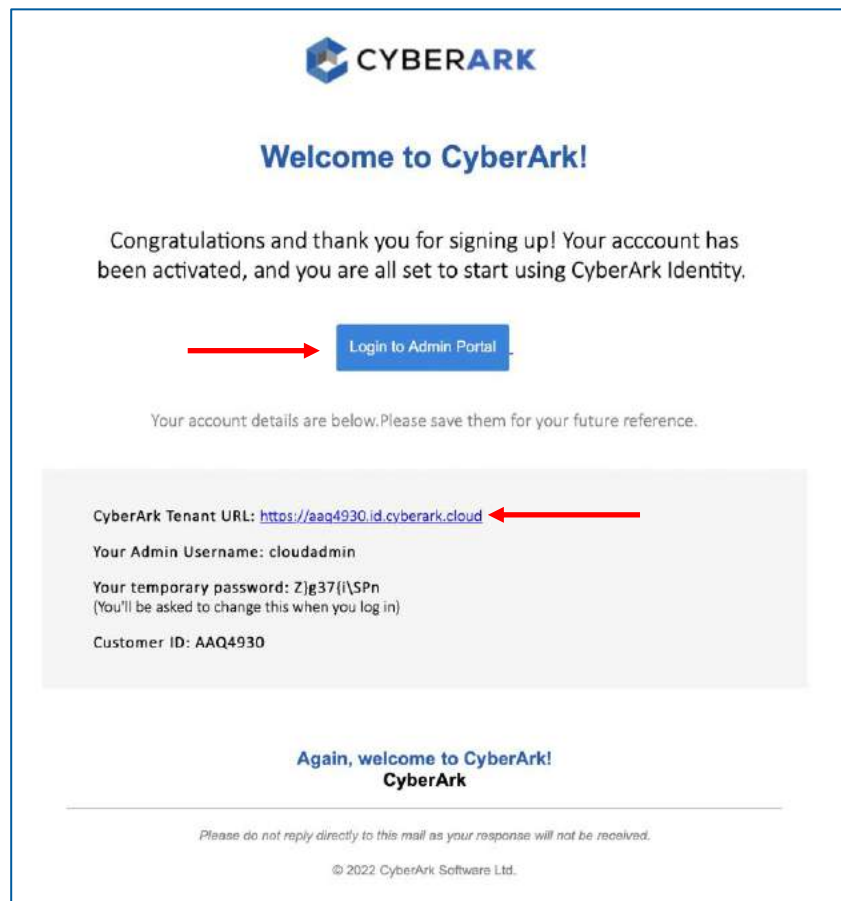
* Select Role:

* Department:

* Select Department:

CyberArk Workforce Identity

3. Once registration is complete, you will receive an additional email with instructions to access the Identity administrative portal. When entering for the first time, a password change will be requested, you must comply with the established policy:



The screenshot shows a "Change Your Password" form. It has two input fields: "New Password" and "Confirm New Password". Both fields have a red asterisk and an information icon. Below the fields is a green "Save" button.

Password Requirements: Must be at least 8 characters long. Must be less than 64 characters long. Must include at least one digit. Must include at least one upper case and one lower case letter. Cannot be the same as any of the last 3 password(s).

4. Ingresar al Admin Portal:



CyberArk Workforce Identity

Tenant Customization

1. In the **Admin Portal**, main menu, go to **Settings | Customization** and customize to your liking the **General Options** (Colors, Portal Images) and **Login** (wallpaper and logo in login view). In the **User Name Hint Text at Login option**, specify **user@cybr.com** (we will integrate the AD from our Skytap lab into our Identity service)

Account Customization

Use these settings to customize the look and feel of CyberArk Identity with your organization's color scheme, logo, and text.

[Learn more](#)

General Options

Portal Ribbon Account Color

Portal Ribbon Color

Company Name

Company Support Link

Portal Image



Short Portal Image



Login Customization

☒ [Back to Identity.com URL Forwarding](#)

User Name Hint Text at Login

☐ Remember last signed in username

Login Image



Login Background Image

2. In the **Login** submenu | **Suffix**, add a new suffix to the environment. The value must be globally unique. Once the suffix is defined, for future authentications with the cloudadmin user we must add it, e.g. **cloudadmin@kbcorp.biz**



Add Login Suffix

Enter a unique login suffix in the field below. The suffix will be validated to ensure it is not already in use before being saved.

Login Suffix (what users type to login)

username @

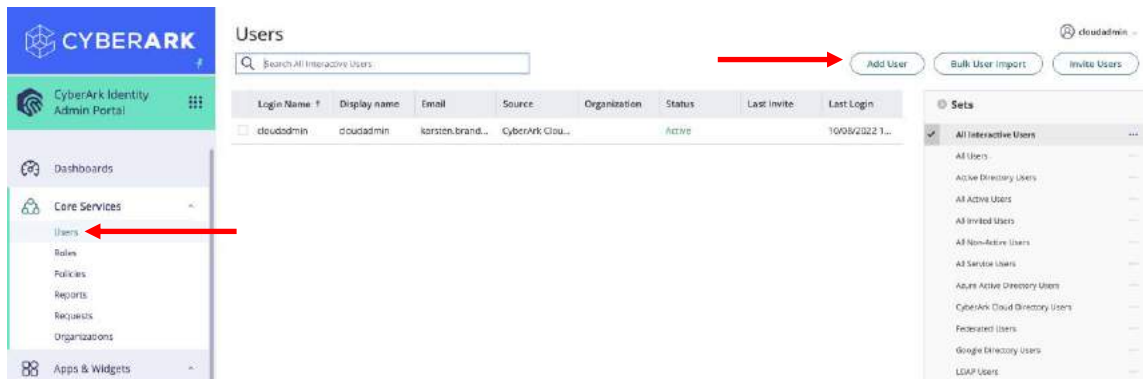
> Advanced

CyberArk Workforce Identity

Tenant Customization

3. For best practices, add a new tenant administrator from the **Core Services** menu | **Users** | **Add**. The **cloudadmin** user will be stored in a sealed envelope and no multi-factor policies will be applied.

4. In the new user creation form, be sure to add your **corporate email address** and **cell phone**, so that you can then perform MFA tests. **Assign a password manually** and disable the **Require Password change at next login** option.



The screenshot shows the 'Create CyberArk Cloud Directory User' form. The form is divided into several sections: 'Account', 'Password Type', 'Status', and 'Notifications'. Red arrows point to the following fields: 'Login name' (containing 'demouser'), 'Email address' (containing 'karsten.brandes@cyberark.com'), 'Display name' (containing 'Usuario Demo'), 'Manual' radio button under 'Password Type', and the 'Require password change at next login (recommended)' checkbox under 'Status'.

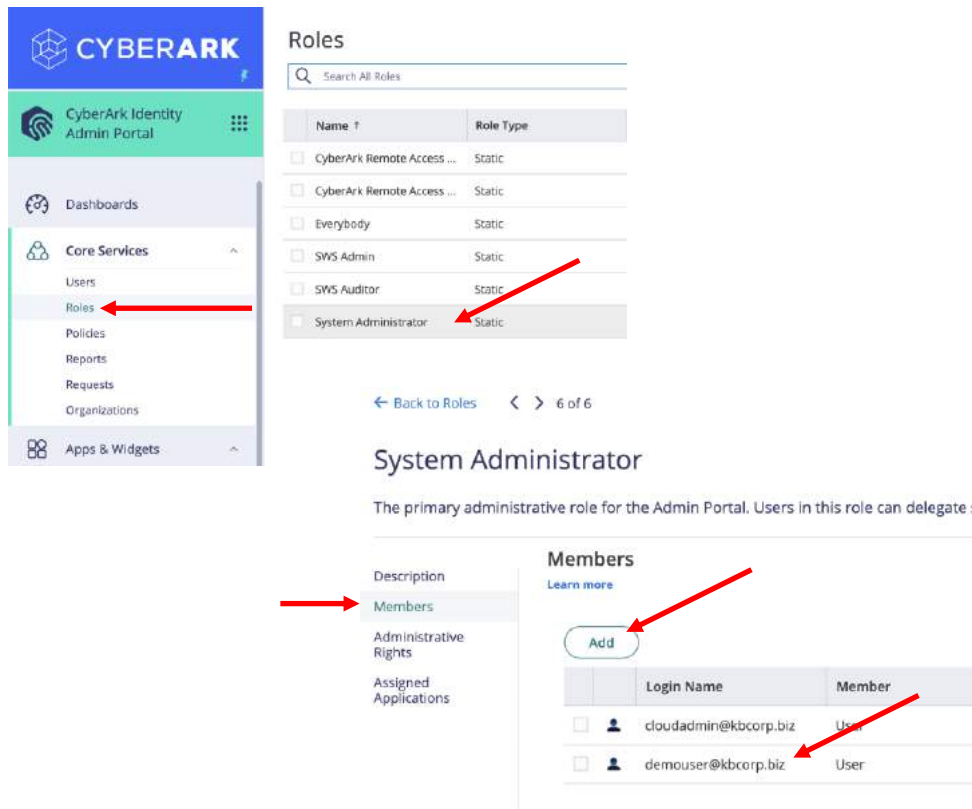
The screenshot shows the 'Create CyberArk Cloud Directory User' form, specifically the 'Account' section. Red arrows point to the 'Mobile number' field (containing '+51997577230') and the 'Organization' dropdown menu (currently set to 'Unassigned').

CyberArk Workforce Identity

Tenant Customization

5. To add the new user as a **tenant administrator**, go to **Core Services | Roles** and select the **System Administrator** role. Add the new account.

6. Go to **Settings | Authentication | Security Questions** and add a security question that we will then ask for as part of our users' registration.



Roles

Name ↑	Role Type
<input type="checkbox"/> CyberArk Remote Access ...	Static
<input type="checkbox"/> CyberArk Remote Access ...	Static
<input type="checkbox"/> Everybody	Static
<input type="checkbox"/> SWS Admin	Static
<input type="checkbox"/> SWS Auditor	Static
<input checked="" type="checkbox"/> System Administrator	Static

[Back to Roles](#) < > 6 of 6

System Administrator

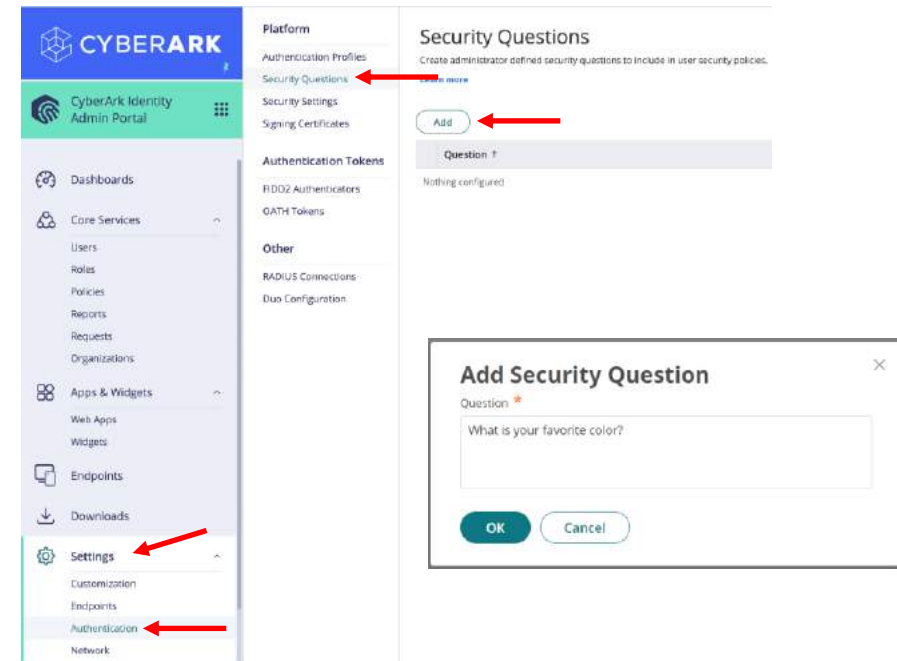
The primary administrative role for the Admin Portal. Users in this role can delegate:

Members

[Learn more](#)

[Add](#)

	Login Name	Member
<input type="checkbox"/>	cloudadmin@kbcorp.biz	User
<input type="checkbox"/>	demouser@kbcorp.biz	User



CYBERARK

CyberArk Identity Admin Portal

Platform

- Authentication Profiles
- Security Questions
- Security Settings
- Signing Certificates

Authentication Tokens

- FIDO2 Authenticators
- OATH Tokens

Other

- RADIUS Connections
- Duo Configuration

Security Questions

Create administrator defined security questions to include in user security policies.

[Add](#)

Question ↑

Nothing configured.

Add Security Question

Question *

What is your favorite color?

[OK](#) [Cancel](#)

CyberArk Workforce Identity

Tenant Customization

7. In **Security Settings**, review and enable the following options, finally click **Save**:

Security Settings
Use these settings to define security related settings.
[Learn more](#)

Authentication Options

- ☒ Enable QR code based user identification on login screen
- ☒ Enable anti-phishing security image ⓘ
- ☐ Securely capture users passwords at login ⓘ
- ☐ Enable forgot username self-service at login ⓘ
- ☐ Send email notification to users when password is changed
- ☐ Disable the force authentication at the Identity Provider for SAML login ⓘ
- ☒ Don't use certificates for authentication on Android if prompt is required ⓘ

8 Email and SMS passcode length ⓘ

Additional Attributes for MFA ⓘ

[Add](#)

Attribute	Type
No attributes specified	

CAPTCHA Settings

2 Number of consecutive failed login attempts allowed before showing a CAPTCHA (default Off)

8. Authenticate to the portal with the newly created user. Note that we have enabled the QR code on the authentication screen, and also text help for our end users of the cybr.com

CYBERARK

Sign In

Scan QR Code with the CyberArk Identity app.

QR

Enter your username (usuario@cybr.com)

demouser@kbcorp.biz

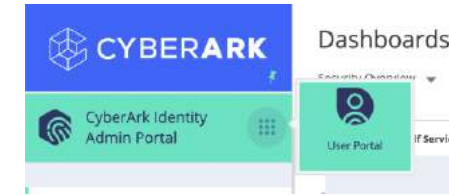
Next

CyberArk Workforce Identity

Tenant Customization

9. We have not yet applied multi-factor authentication policies or defined our answers, note that it only asks us for the password.

10. In the **User Portal**, select **Account | Authentication Factors** and add a security question.

A screenshot of the CyberArk authentication interface. At the top, it says 'Authenticate to the Platform' for the user 'demouser@kbcorp.biz'. Below this, it prompts the user to 'Enter the password associated with your username'. There is a password input field with a red arrow pointing to it. A 'Next' button is at the bottom. A 'Forgot your password?' link is also present.A screenshot of the CyberArk User Portal 'Account | Authentication Factors' screen. The left sidebar shows the 'Account' menu item selected. The main area is titled 'Authentication Factors' and lists 'Password' and 'Security Question'. A red arrow points to the 'Set' button next to the 'Security Question' entry. Below this, a 'Security Questions' modal is open, showing a table with one question: 'Cual es mi color favorito?' with the answer '*****'. A red arrow points to the 'Save' button at the bottom of the modal.

CyberArk Workforce Identity

Tenant Customization

11. Finally we will create a URL to access the Tenant that is more friendly for our organization. In the **Admin Portal**, go to **Settings > Customization > Tenant URLs** menu and select the **Add Tenant URL** button. Specify a unique name for your Tenant. The new URL may be used by our end users to access the service:

The screenshot displays the CyberArk Identity Admin Portal interface. On the left, a sidebar menu shows the navigation path: **Settings** > **Customization** > **Tenant URLs**, with red arrows indicating the selection sequence. The main content area is titled "Tenant URLs" and includes a description: "Use these settings to define a CyberArk Identity URL that is more specific to your organization." Below this, a table lists existing tenant URLs with columns for "Name" and "Default URL". A red arrow points to the "Add Tenant URL" button in the top right corner of the main area. A modal dialog titled "Create Tenant URL" is open, showing a text input field for the "Name" (63 characters max) with "kbcorp" entered. A red arrow points to this field. Below the input, the "Complete URL will be:" is shown as "https://kbcorp.id.cyberark.cloud". At the bottom of the modal, red arrows point to the "Save" and "Cancel" buttons.

Name	Default URL
aaq4930.id.cyberark.cloud	

Create Tenant URL

Enter a name in the field below to create a tenant specific URL. The URL will be validated during save to ensure it is not already in use (note: please allow up to 20 minutes for DNS replication).

Name (63 characters max) *

kbcorp

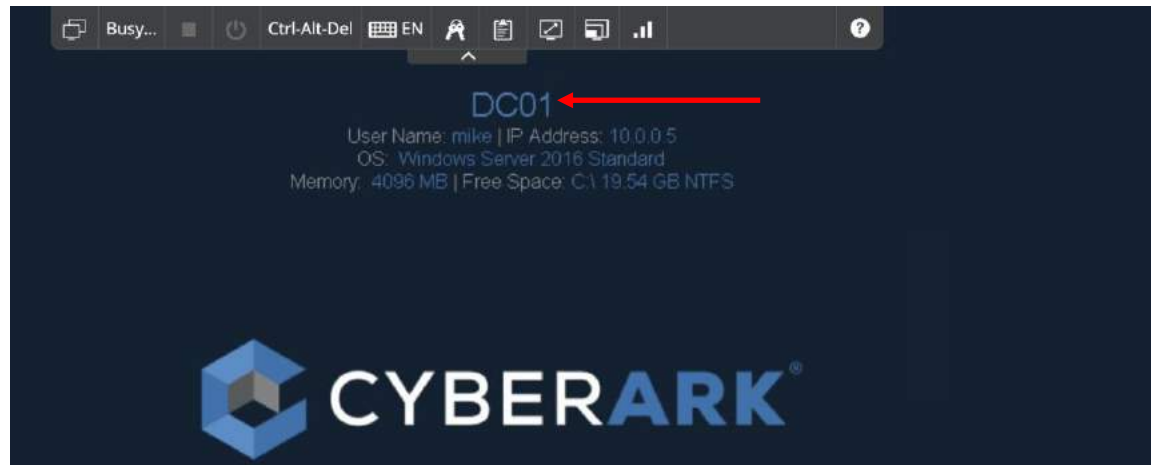
Complete URL will be:
https://kbcorp.id.cyberark.cloud

Save Cancel

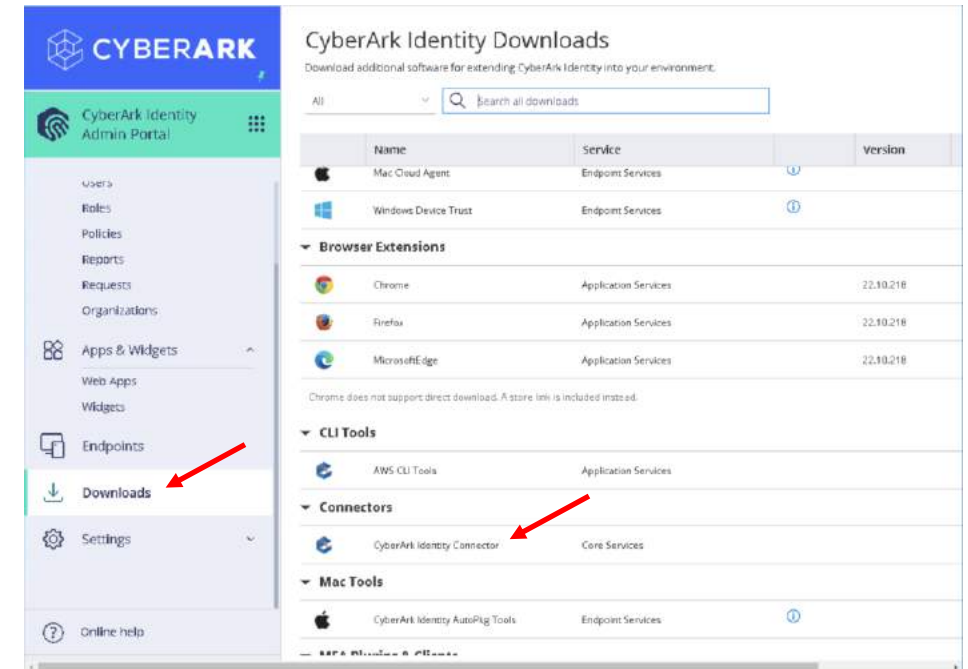
CyberArk Workforce Identity

Installing the Identity Connector

1. We will install the Identity connector in our Skytap environment to be able to integrate the Active Directory of the organization so that our corporate users can take advantage of the features of SSO/MFA/WPM/App Gateway. In Skytap, login to the **DC01** server using Mike's credentials (Cyberark1)



2. Open Chrome and authenticate to the Identity **Admin Portal** with the newly created user (system administrator role). Select the **Downloads** menu and download the **CyberArk Identity Connector**



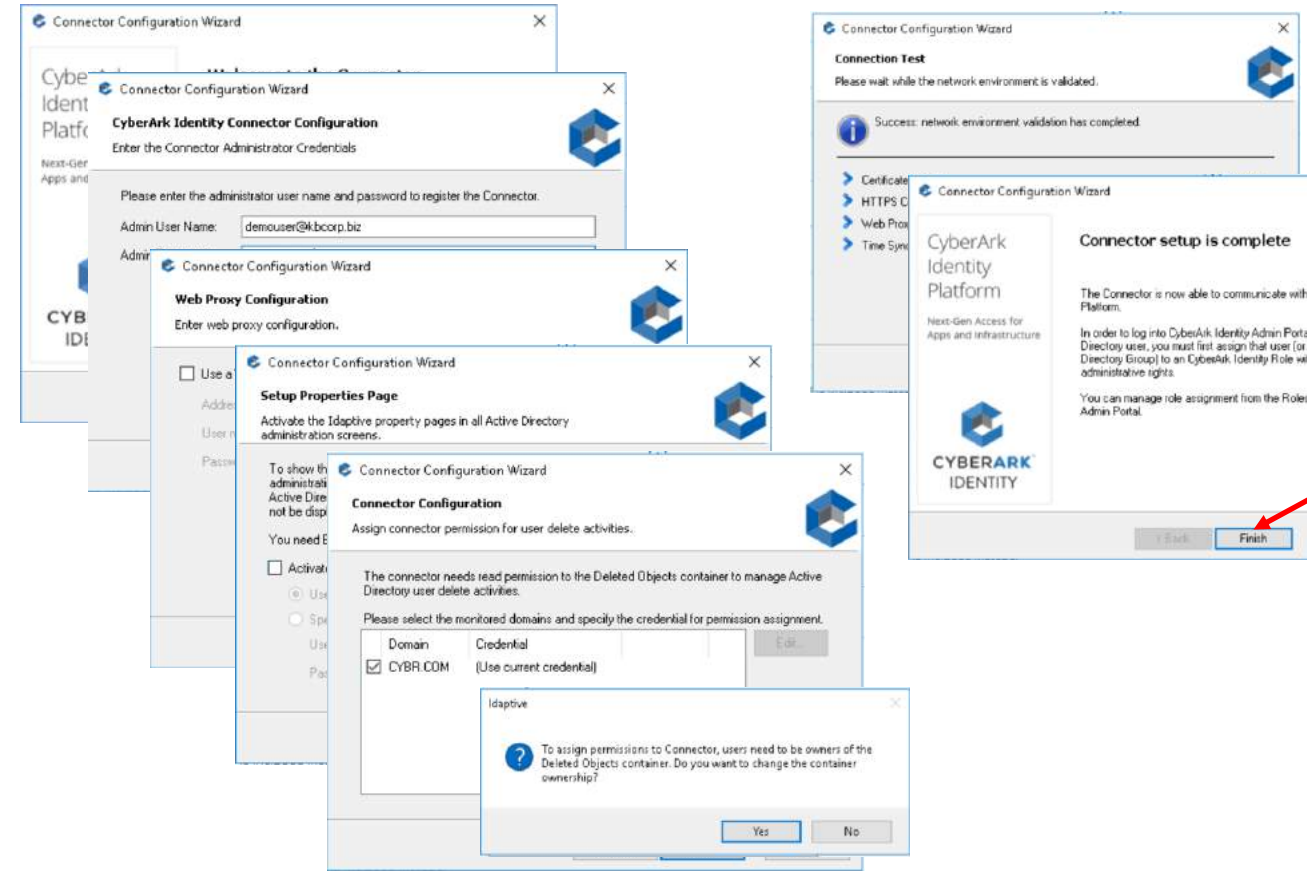
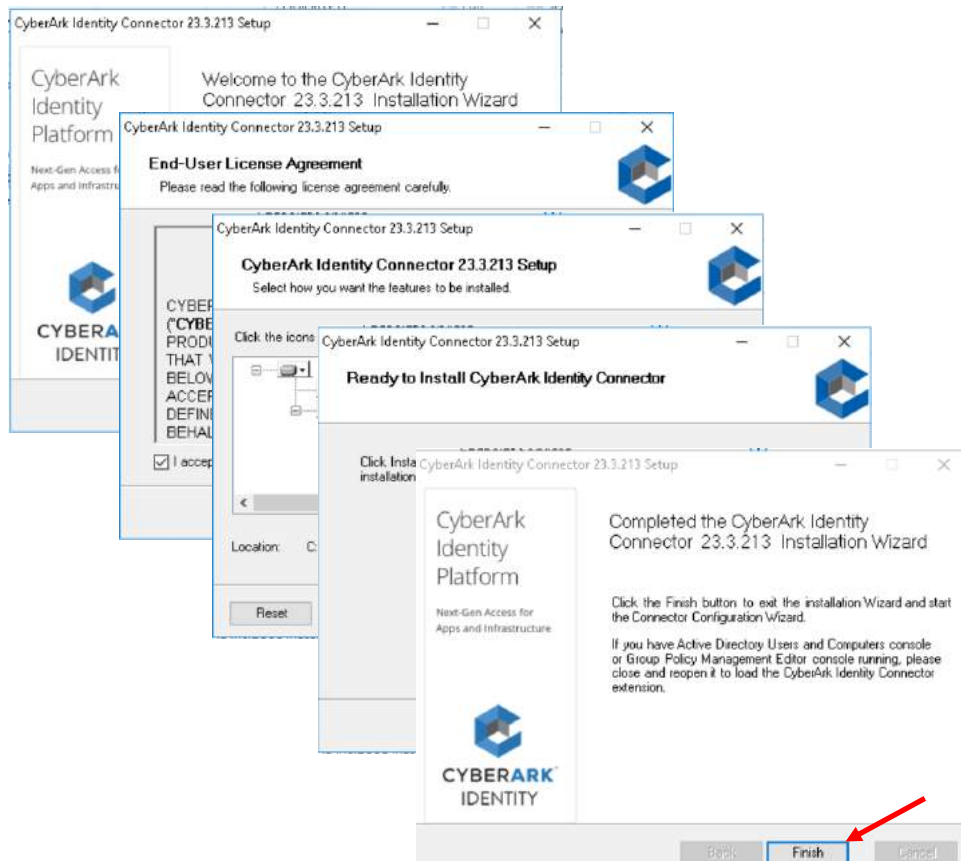
Note: In production environments, installing the connector on Domain Controllers is **not recommended**.

CyberArk Workforce Identity

Installing the Identity Connector

3. After downloading the file, unzip it and run the Connector installer. Accept the terms of service, enable all options, and select the Install option

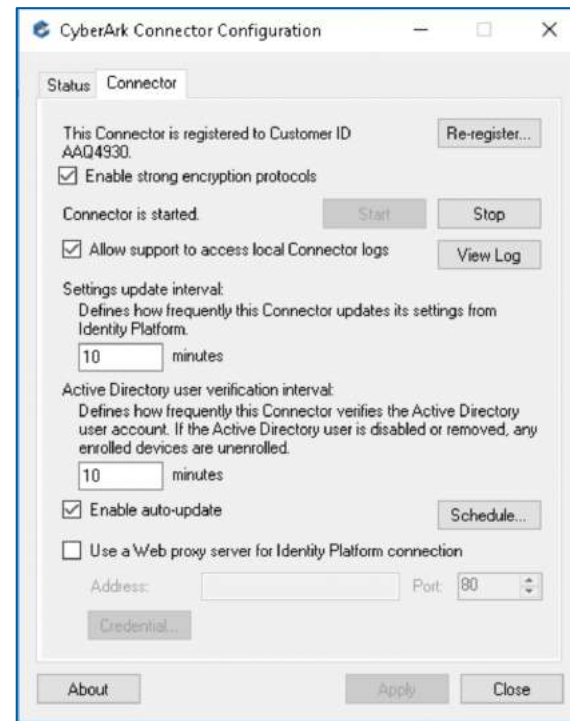
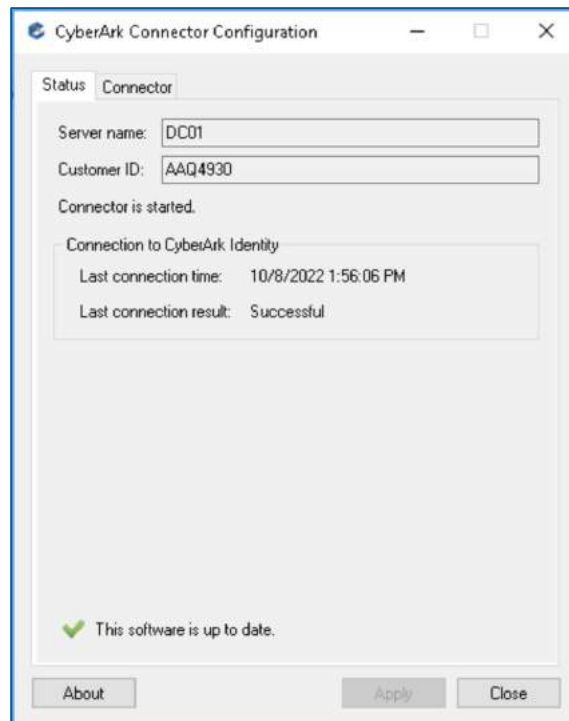
4. In the Configuration Wizard, specify the newly created admin user, we need to get 4 successes and then verify the successful completion of the install.



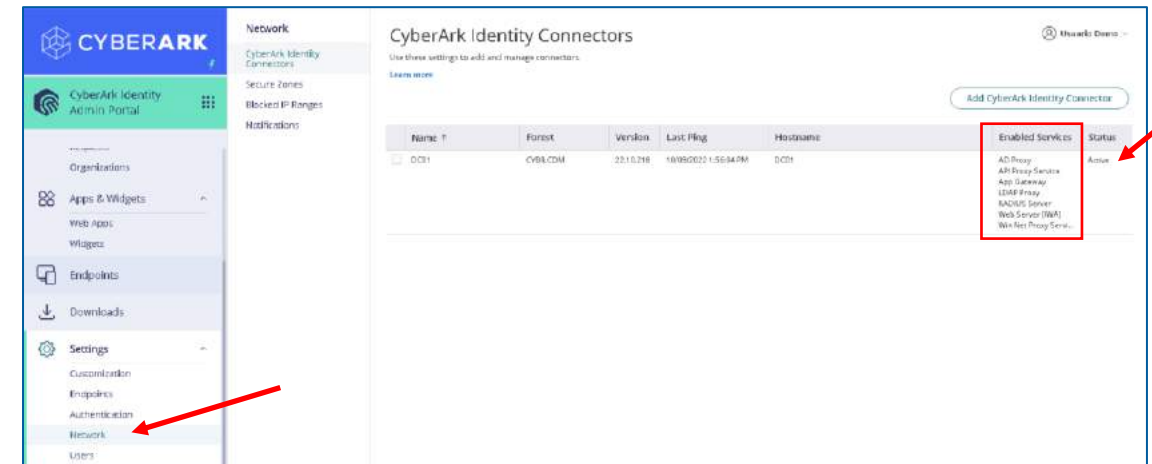
CyberArk Workforce Identity

Installing the Identity Connector

5. In the **CyberArk Connector Configuration** window, verify the time of the last connection, server name, and customer ID. Review the options available on the **Connector** tab.



6. In the **Admin Portal**, go to **Settings | Network | CyberArk Identity Connectors** and verify that the connector is listed as **Active**. Review the services that are enabled by default.



IWA Service: Integrated Windows Authentication, allows users already authenticated on their workstations to access the Identity portal automatically without the need for re-authenticate.

App Gateway: Access internal web applications from the SSO portal without the need to connect via a VPN

CyberArk Workforce Identity

Creating Roles and Policies

Policy-based access control, also known as Attribute-based Access Control (ABAC) is a strategy for managing user access to one or more systems, where users' business roles are combined with policies to determine the access and privileges that users in each role must have. The **Default Policy** is the policy that is configured by default in our tenant. In this lab we will create a new policy that will be assigned to users of the **CYBR.COM** domain.

1. In the **Admin Portal**, go to **Core Services | Roles**. We will create a new role for users in our organization's Active Directory.
2. On the **Description** menu, specify a **name** for the new role, and under **Members**, add the **Domain Users** group of the active directory **CYBR.COM**

The image displays three screenshots from the CyberArk Admin Portal illustrating the steps to create a new role.

Top Screenshot: Roles List
The 'Roles' page shows a list of existing roles. A red arrow points to the 'Add Role' button in the top right corner. The user 'Usuario Demo' is logged in.

Name	Role Type	Description	Organization
CyberArk Remote Access ...	Static	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Members of ...	
CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by CyberArk.	
Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Directory or a...	
SWS Admin	Static	Secure Web Sessions administrative role.	
SWS Auditor	Static	Secure Web Sessions auditor role.	
System Administrator	Static	The primary administrative role for the Admin Portal. Users in this role can delegate specific administrative righ...	

Bottom Left Screenshot: Add Role - Description
The 'Add Role' form shows the 'Description' tab selected. The 'Name' field is populated with 'Usuarios CYBR'.

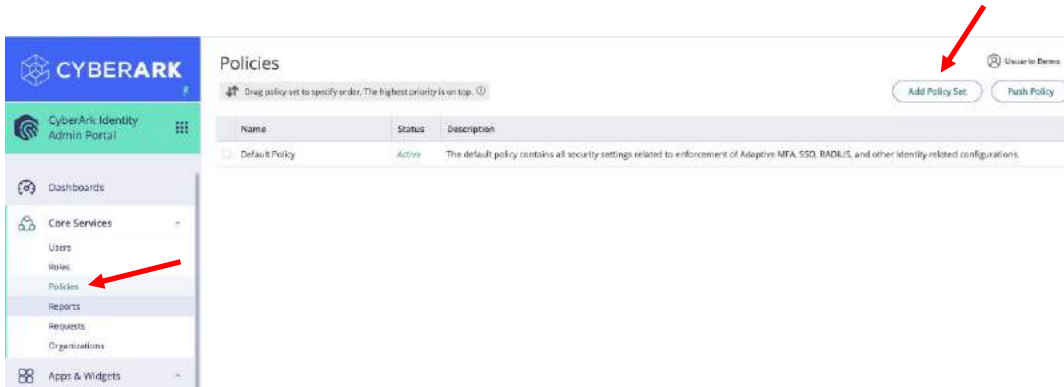
Bottom Right Screenshot: Add Role - Members
The 'Add Role' form shows the 'Members' tab selected. The 'Add' button is visible. Below it, a table lists the members to be added:

Login Name	Member
Domain Users@cybr.com	Group

CyberArk Workforce Identity

Creating Roles and Policies

3. In the **Admin Portal**, go to **Core Services | Policies** and review the properties of the **Default Policy**. Then, add a new policy.



4. In the **Policy Settings** menu, specify a name for the new policy and assign it to the newly created role:

The screenshot shows the 'Add Policy Set' form. The form has a search bar at the top. Below it is a 'Policy Settings' section with a list of expandable categories: 'Application Policies', 'Endpoint Policies', 'Authentication Policies', 'User Security Policies', and 'Third Party Integration'. The 'Summary' section is currently expanded. In the 'Summary' section, there is a 'Name' field with the value 'CYBR Policy' and a 'Description' field. Below these fields are 'Policy Setting' checkboxes for 'Set policy to active' (checked) and 'Verify compliance on Android and iOS devices' (checked). The 'Policy Assignment' section has three radio buttons: 'All users and Devices' (selected), 'Specified Roles', and 'Sets'. An 'Add' button is located below the 'Policy Assignment' section. At the bottom of the form, there is a table with columns 'Name' and 'Status'. The table contains one entry: 'Usuarios CYBR' with status 'Active'.

CyberArk Workforce Identity

Creating Roles and Policies

5. Go to **Application Policies | User Settings** and enable the following options:

Add Policy Set

Search

Policy Settings

- Application Policies
 - User Settings
 - Application Restrictions
- Endpoint Policies
- Authentication Policies
- User Security Policies
- Third Party Integration
- Summary

User Settings

Yes	Allow users to add personal apps ⓘ		
--	Allow users to customize user added apps ⓘ		
<input checked="" type="checkbox"/>	Name	<input checked="" type="checkbox"/>	Description
<input checked="" type="checkbox"/>	Logo	<input checked="" type="checkbox"/>	Url
--	Allow users to view/copy personal passwords ⓘ		
60	Clear clipboard after the configured time (in seconds)		
Yes	Enable Browser Extension Land & Catch ⓘ		
--	Enable WS-Trust protocol ⓘ		
<input checked="" type="checkbox"/>	Enforce application challenge with WS-Trust ⓘ		

Allow users to add personal apps: Allow the end user to add new applications to his/her Single Sign On (SSO) portal

Enable Browser Extension Land & Catch: Option to use the browser extension to capture username/password when authenticating to web pages

6. Go to **Endpoint policies | Common Settings | Mobile Settings | Security Settings**, enable the following options:

CYBR Policy

Status: Active

Search

Policy Settings

- Application Policies
- Endpoint Policies
 - Device Management Settings
 - Device Enrollment Settings
 - Common Settings
 - Mobile Settings
 - Common
 - Restrictions Settings
 - Security Settings

Security Settings

Yes	Show Mobile Authenticator by default ⓘ
--	Enable auto-login to Identity portal from Android browser with Android app unlock ⓘ
--	Require authentication to open CyberArk Identity app ⓘ
Yes	Require biometric authentication for Passcodes and QR code authenticator ⓘ
Yes	Use App PIN as fallback mechanism to biometric ⓘ
<input checked="" type="checkbox"/>	Enable Mobile authenticator and Passcodes on Apple watch ⓘ

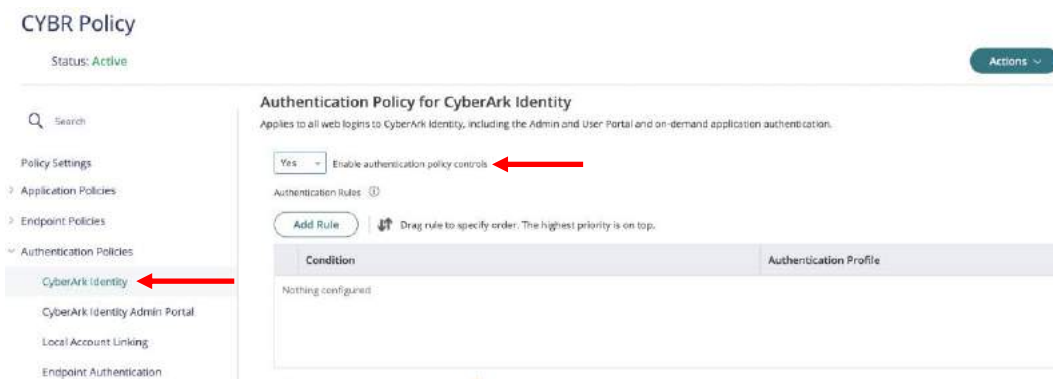
Show Mobile Authenticator by Default: show the mobile authenticator in the Identity app (OATH OTP)

Require Biometric authentication for Passcodes and QR code authenticator: use biometric scanning to access passcodes or QR code scans for authentication.

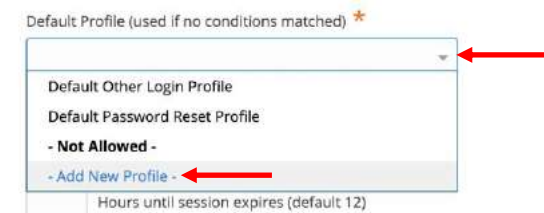
CyberArk Workforce Identity

Creating Roles and Policies

7. We will now secure user console access with MFA. Expand **Authentication Policies | CyberArk Identity** and enable **Enable Authentication Policy Controls**:



8. Expand **Default Profile (used if no conditions matched)**, and select the **Add New Profile** option:



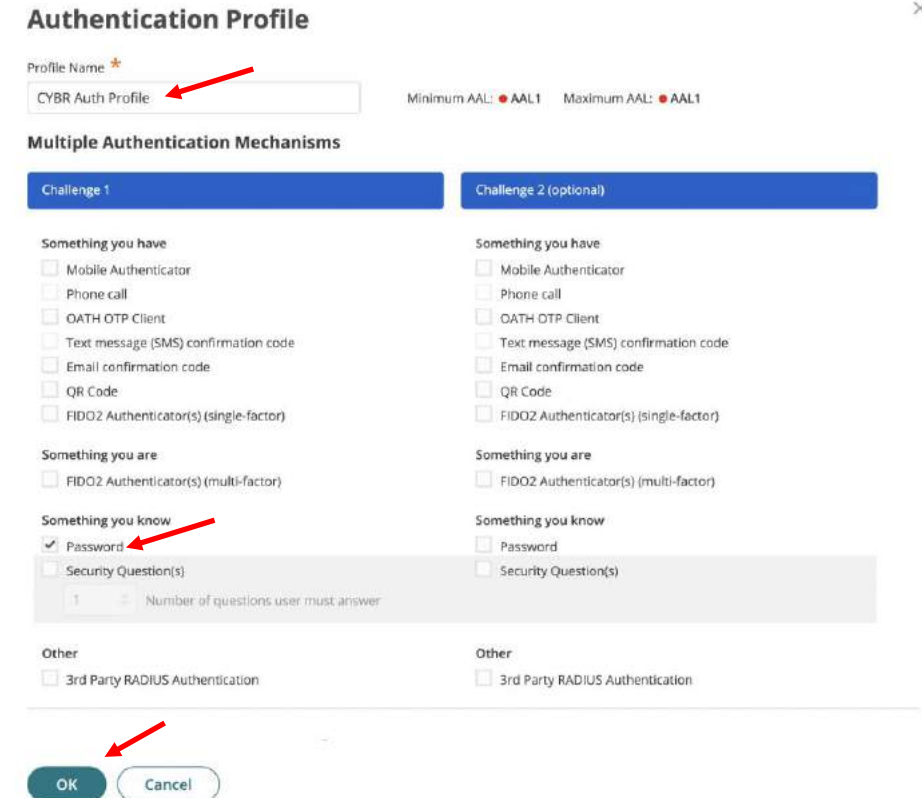
CyberArk Workforce Identity

Creating Roles and Policies

9. The authentication profile is where the required authentication mechanisms are defined, such as password, email confirmation code, mobile authenticator, etc. Define a name for the policy and enable the following options:

First challenge: Password

Second challenge: none (we will show the behavior when enabling second challenges later)



Authentication Profile

Profile Name *
CYBR Auth Profile

Minimum AAL: ● AAL1 Maximum AAL: ● AAL1

Multiple Authentication Mechanisms

Challenge 1

Something you have

- ☐ Mobile Authenticator
- ☐ Phone call
- ☐ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Email confirmation code
- ☐ QR Code
- ☐ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

- ☒ Password
- ☐ Security Question(s)

1 Number of questions user must answer

Other

- ☐ 3rd Party RADIUS Authentication

Challenge 2 (optional)

Something you have

- ☐ Mobile Authenticator
- ☐ Phone call
- ☐ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Email confirmation code
- ☐ QR Code
- ☐ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

- ☐ Password
- ☐ Security Question(s)

Other

- ☐ 3rd Party RADIUS Authentication

OK **Cancel**

CyberArk Workforce Identity

Creating Roles and Policies

10. Now we will enable the possibility that our users can reset their password in case they forget it. Still in the policy properties, go to **User Security Policies | Self Service**, enable **Enable Account Self Service Controls** and create a new authentication profile:

The screenshot shows the 'CYBR Policy' console with the 'Self Service' section expanded. A red arrow points to the 'Enable account self service controls' toggle, which is set to 'Yes'. Another red arrow points to the 'Password Reset' section, which is expanded. A third red arrow points to the 'Add New Profile' button in the dropdown menu for 'Password Reset Authentication Profile'. The dropdown menu shows several profiles, including 'CYBR Auth Profile', 'Default Other Login Profile', 'Default Password Reset Profile', and '- Not Allowed -'.

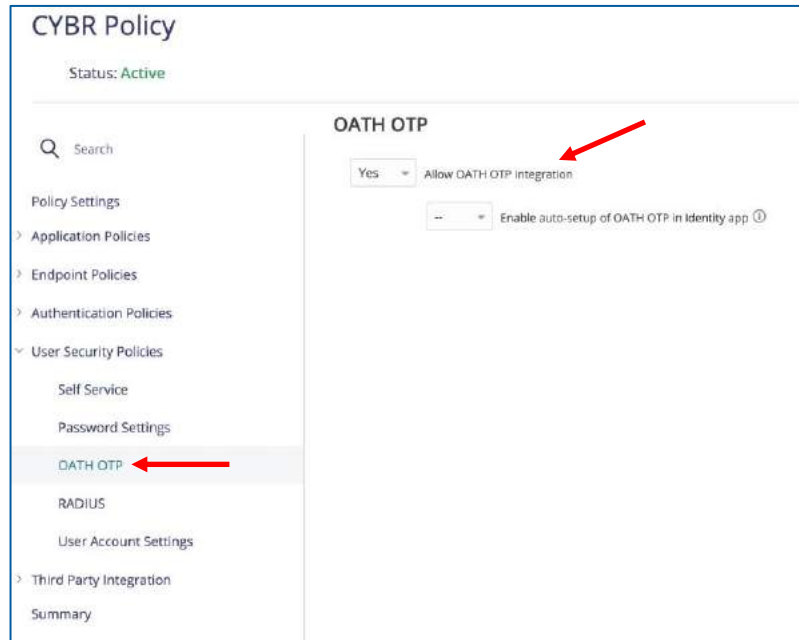
11. Specify a name for the new policy, and enable only the following mechanisms in the first challenge column:

The screenshot shows the 'Authentication Profile' configuration window. A red arrow points to the 'Profile Name' field, which contains 'Password Reset Auth Profile'. Another red arrow points to the 'Mobile Authenticator' checkbox in the 'Challenge 1' column. A third red arrow points to the 'OATH OTP Client' checkbox in the 'Challenge 1' column. A fourth red arrow points to the 'Security Question(s)' checkbox in the 'Challenge 1' column. The 'Challenge 2 (optional)' column is empty. The 'Other' section is also empty. The 'OK' and 'Cancel' buttons are at the bottom.

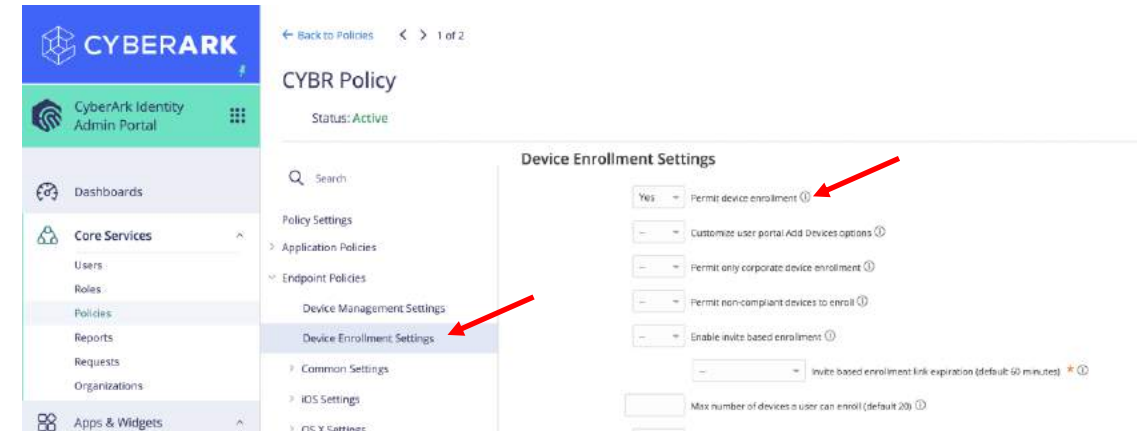
CyberArk Workforce Identity

Creating Roles and Policies

12. We will also allow our users to integrate with an OATH OTP (Identity Authenticator / Google Authenticator / MS Authenticator, etc). Go to **User Security Policies | OATH OTP**, and enable **Allow OATH OTP Integration**:



13. Expand **Endpoint Policies | Device Enrollment Settings** and enable **Permit device Enrollment**. Finally save (click on **SAVE** button) the policy that will apply to the users of the CYBR domain.

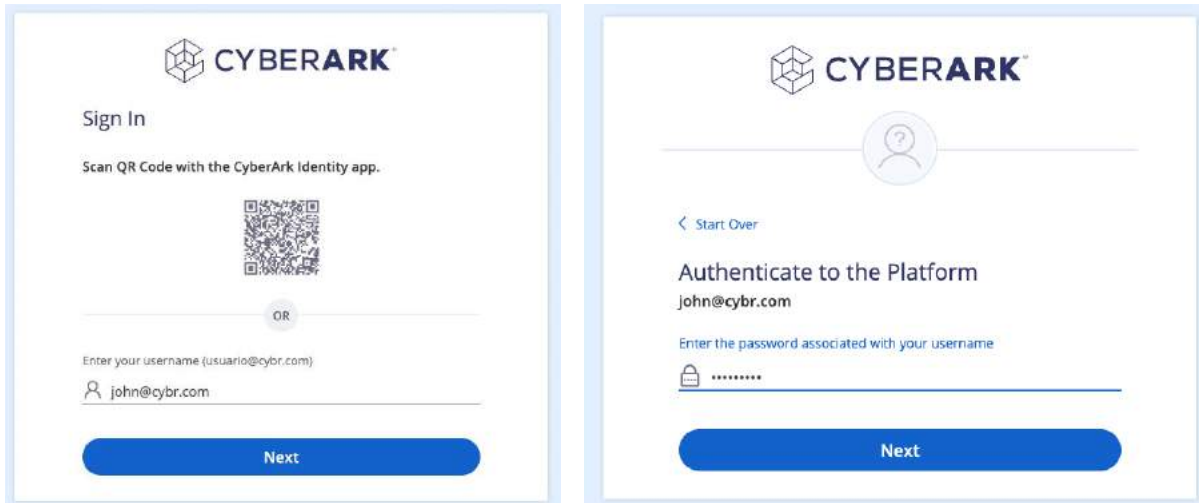


CyberArk Workforce Identity

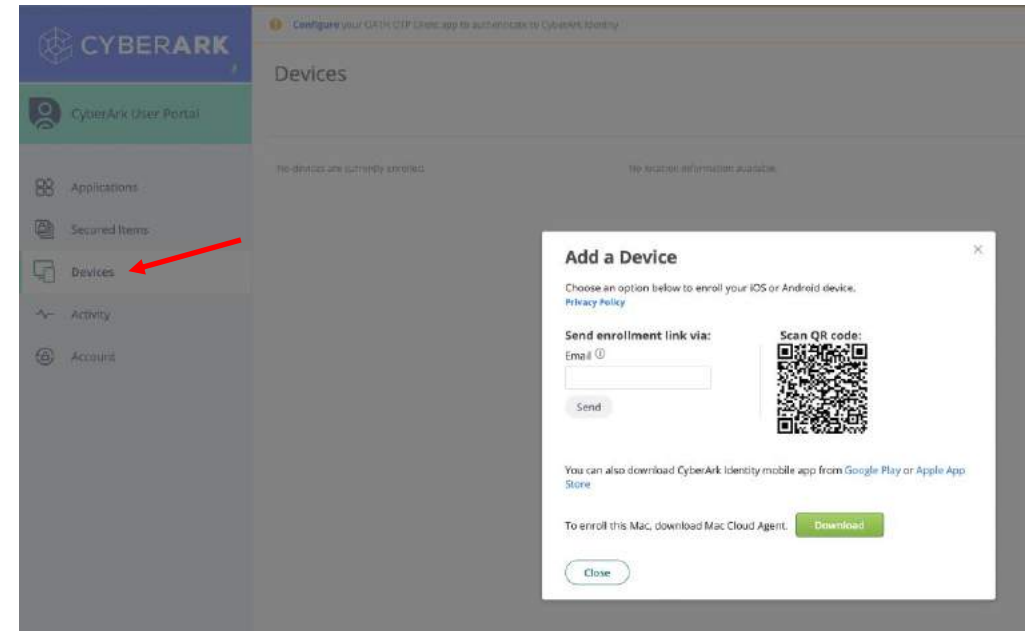
CyberArk Identity Mobile App

1. Login to the User Portal with **john@cybr.com**
(Cyberark1) – <https://xxxxxxxxx.id.cyberark.cloud>

2. Go to the **Devices** menu:



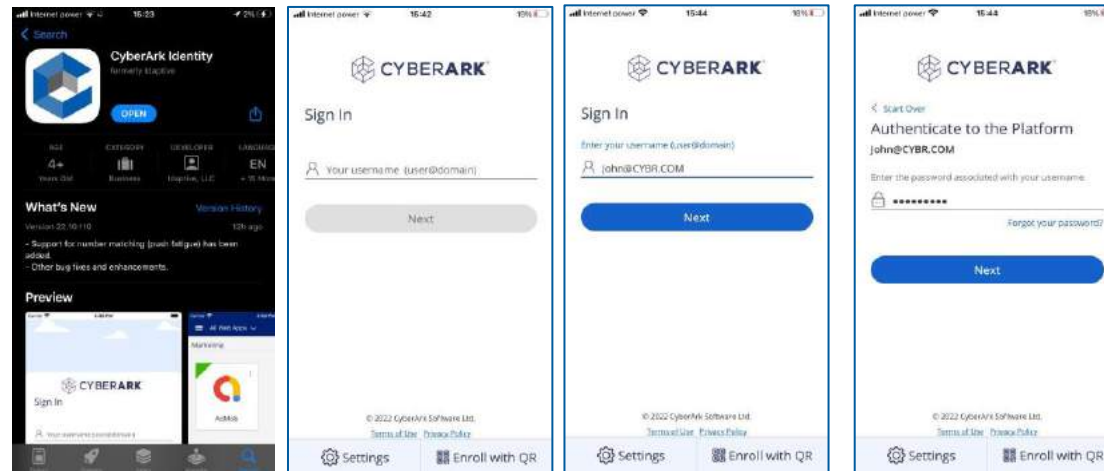
The first screenshot shows the 'Sign In' screen of the CyberArk Identity mobile app. It features the CyberArk logo, a QR code, and a 'Next' button. The second screenshot shows the 'Authenticate to the Platform' screen, where the user enters their username (john@cybr.com) and password, followed by a 'Next' button.



CyberArk Workforce Identity

CyberArk Identity Mobile App

3. Download the CyberArk Identity app on your phone. Once installed, run the app and select the **Enroll with QR** option. Scan the QR code displayed in the **User Portal**.



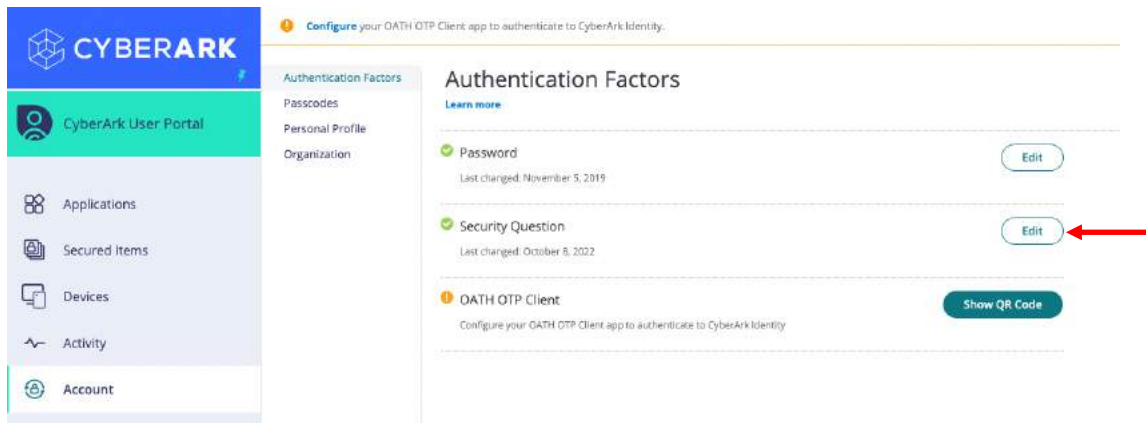
4. Complete the registration process with user **John** (note that the username field is populated by default). Once the new device is registered, it will appear in the list:



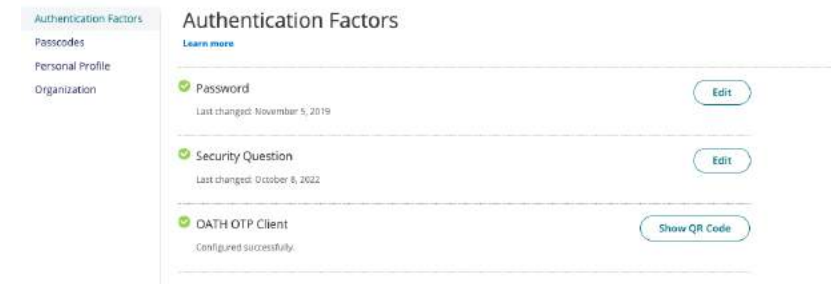
CyberArk Workforce Identity

CyberArk Identity Mobile App

5. Go to **Account | Authentication Factors** and add a security question:



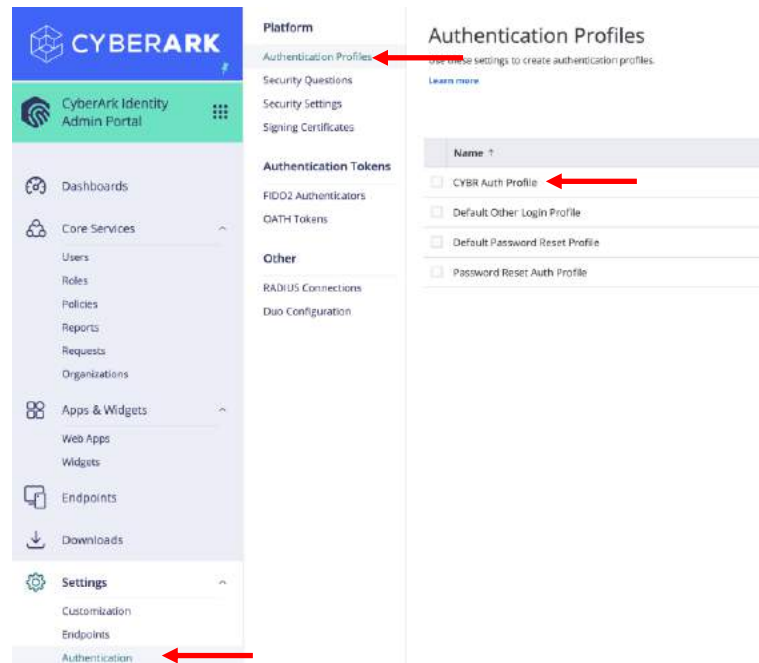
6. In the **OATH OTP Client** option, click **Show QR Code** and register your favorite OATH OTP client application (MS Authenticator, Google Authenticator, etc.)



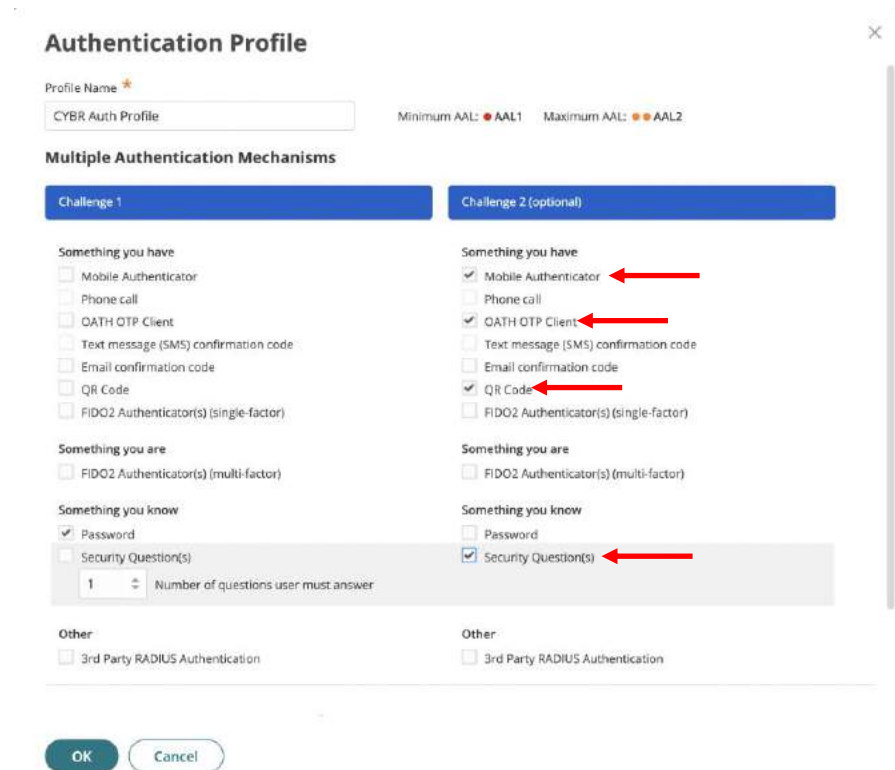
CyberArk Workforce Identity

CyberArk Identity Mobile App

7. We will modify the authentication policy to add new mechanisms in the second challenge. In the **Admin Portal**, select **Settings | Authentication | Authentication Profiles** and edit the profile we created for users in the CYBR domain:



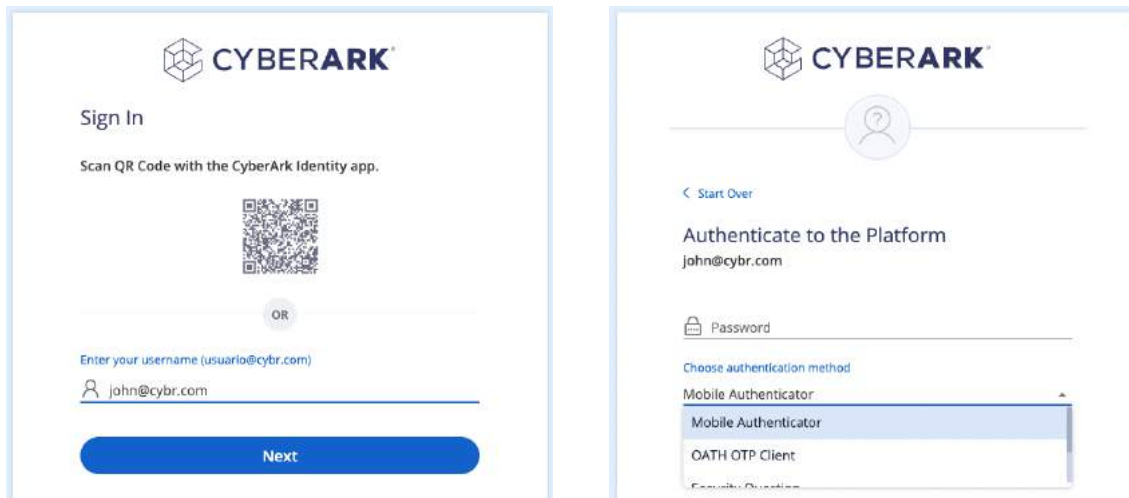
8. Add the following mechanisms in the Challenge 2 column:



CyberArk Workforce Identity

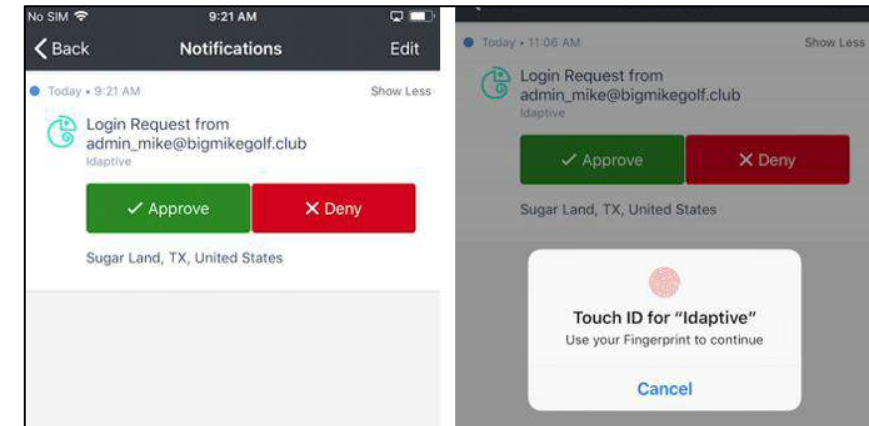
Multifactor Authentication

9. Authenticate to the **User Portal** with User **john@cybr.com**. Note that the first challenge is the password, and then we must select some mechanism as the second challenge. The list is updated depending on the mechanisms that we have available according to the registrations made in previous steps.



The image shows two screenshots of the CyberArk User Portal. The left screenshot is the 'Sign In' screen, featuring the CyberArk logo, a QR code, and a username field with 'john@cybr.com'. The right screenshot is the 'Authenticate to the Platform' screen, showing a password field and a dropdown menu for 'Choose authentication method' with options 'Mobile Authenticator' and 'OATH OTP Client'.

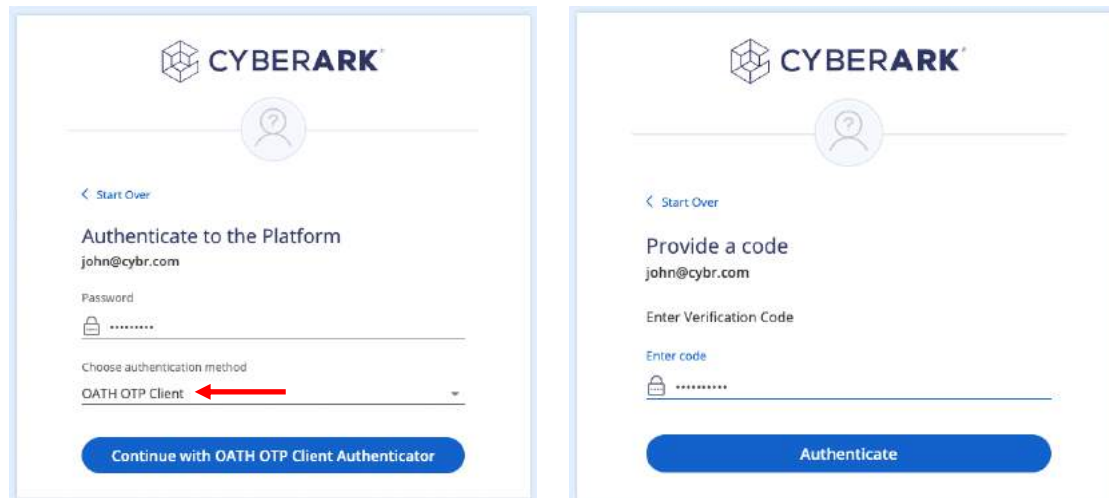
10. Try password and Mobile Authenticator. This will send a push to the mobile device Identity App:



CyberArk Workforce Identity

Multifactor Authentication

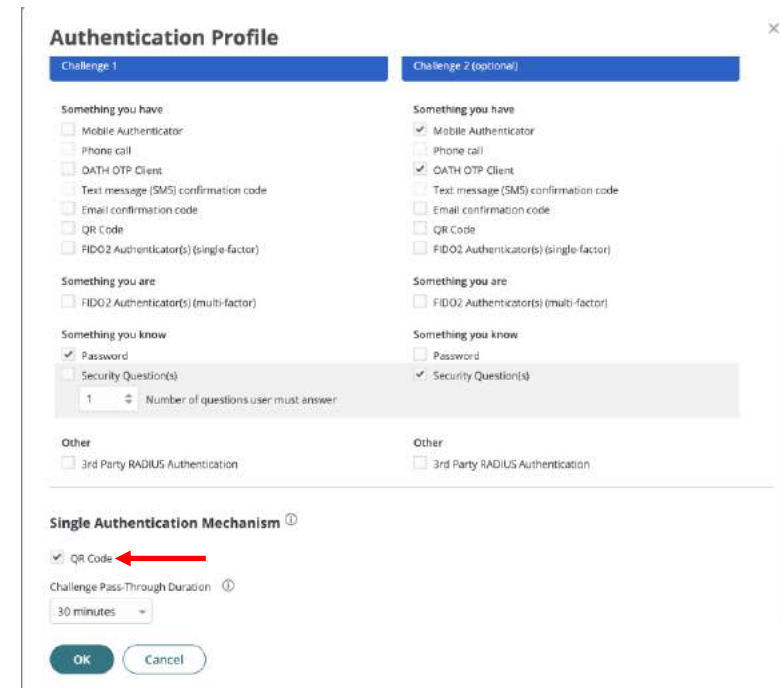
11. Now try with password and OATH OTP code



The left screenshot shows the CyberArk login page. The user is john@cybr.com. The password field is masked. Under 'Choose authentication method', 'OATH OTP Client' is selected, indicated by a red arrow. A button at the bottom says 'Continue with OATH OTP Client Authenticator'.

The right screenshot shows the 'Provide a code' screen. The user is asked to 'Enter Verification Code'. A button at the bottom says 'Authenticate'.

12. Now let's try a Passwordless authentication, authenticating with only QR code. Let's edit the authentication policy again in the **Admin Portal, Settings | Authentication** by selecting the policy for the CYBR domain. Enable **QR Code** under the **Single Authentication Mechanism** section:

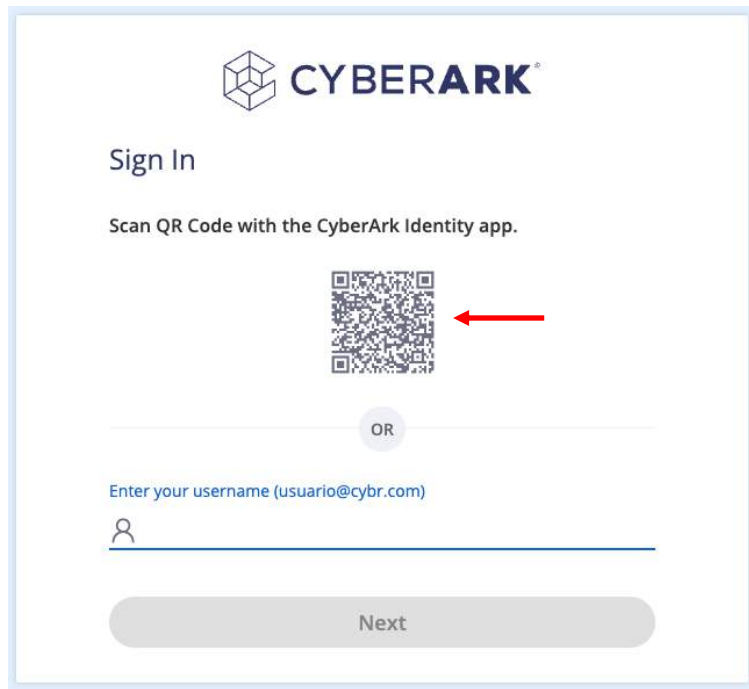


The 'Authentication Profile' window shows two challenges. Challenge 1 is active. Under 'Something you have', 'Mobile Authenticator' is checked. Under 'Something you are', 'FIDO2 Authenticator(s) (multi-factor)' is checked. Under 'Something you know', 'Password' is checked. In the 'Single Authentication Mechanism' section, 'QR Code' is checked, indicated by a red arrow. The 'Challenge Pass-Through Duration' is set to 30 minutes. 'OK' and 'Cancel' buttons are at the bottom.

CyberArk Workforce Identity

Multifactor Authentication

13. Now try to authenticate by simply scanning the QR code using the CyberArk Identity app:



The image shows a screenshot of the CyberArk Sign In interface. At the top, the CyberArk logo is displayed. Below it, the text "Sign In" is shown. The instruction "Scan QR Code with the CyberArk Identity app." is followed by a QR code. A red arrow points to the QR code. Below the QR code, there is a horizontal line with a circle containing the text "OR" in the center. Underneath this, the text "Enter your username (usuario@cybr.com)" is displayed above a text input field with a person icon. At the bottom, there is a "Next" button.

CyberArk Workforce Identity

Application Management – SAML

The CyberArk Identity App Catalog contains thousands of integrations available. Administrators can provide SSO access to on-premises, cloud, and mobile applications. Once applications are configured, end users can authenticate to Identity and run any of your web applications without needing to re-enter their credentials. The following basic use cases show how to configure SAML, bookmark, and user/password applications.

1. Authenticate to the **Admin Portal** and navigate to the **Apps & Widgets** menu | **Web Apps**. Add a new Web App.

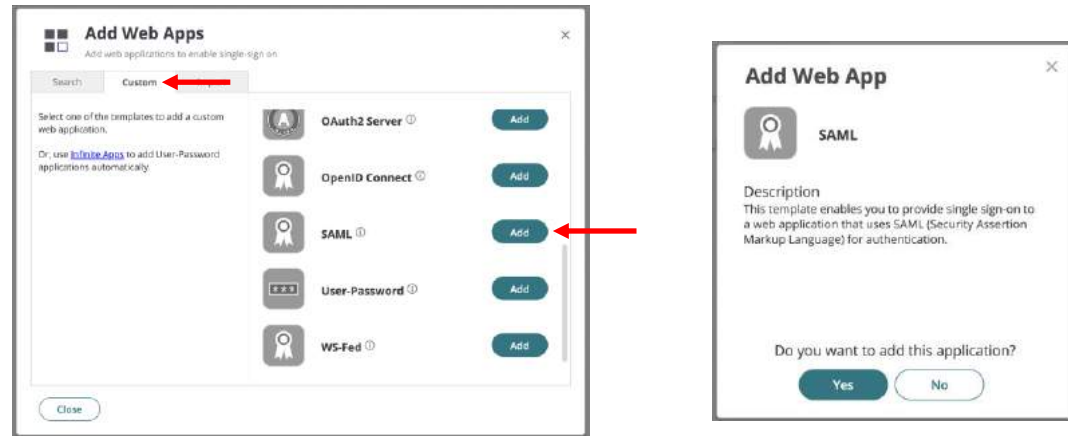
The screenshot displays the CyberArk Identity Admin Portal interface. On the left, a sidebar menu shows 'Apps & Widgets' selected, with a red arrow pointing to the 'Web Apps' sub-item. The main content area is titled 'Web Apps' and features a search bar and a table of existing web applications. A red arrow points to the 'Add Web Apps' button in the top right corner. Below the table, a 'Sets' sidebar is visible, showing 'All Web Applications' as the selected set.

Name	Type	Description	Provisioning	App Gateway	Organization	Status
CyberArk Remote Access ...	Web - SAML	Remote Access is a CyberArk compon...				Deployed
CyberArk Secure Web Ses...	Web - SAML	CyberArk Secure Web Sessions Portal.				Deployed
User Portal	Web - Portal	The User Portal is your interface to th...				Deployed

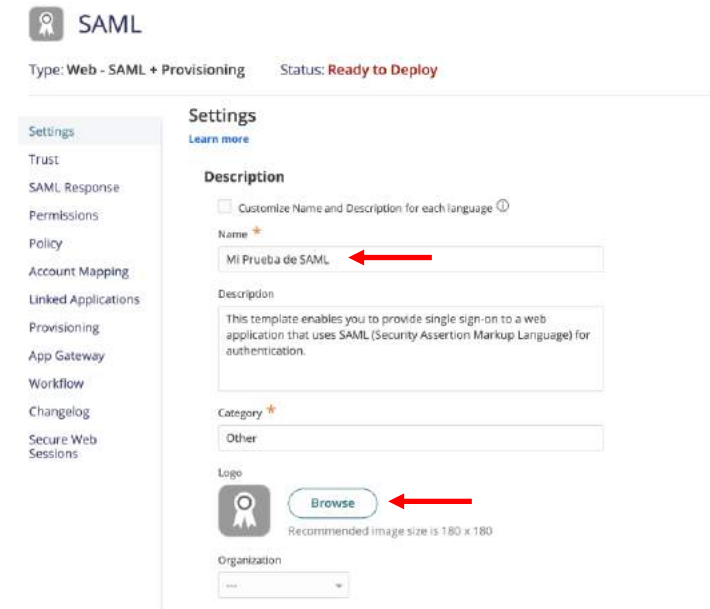
CyberArk Workforce Identity

Application Management - SAML

2. In the **Add Web Apps** window, on the **Custom** tab, add **SAML**:



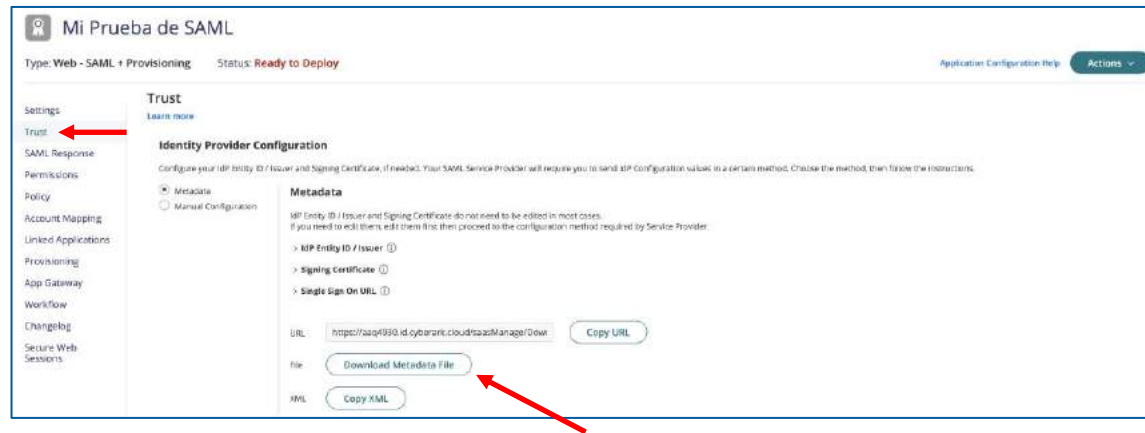
3. In the **Settings** section, name the SAML app and add a custom logo image if you like.



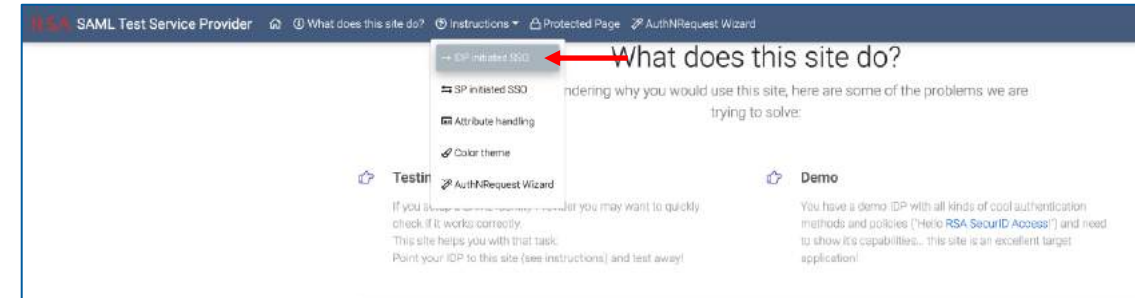
CyberArk Workforce Identity

Application Management - SAML

4. In the **Trust > Identity Provider Configuration > Metadata** section, select the **Download Metadata File** option



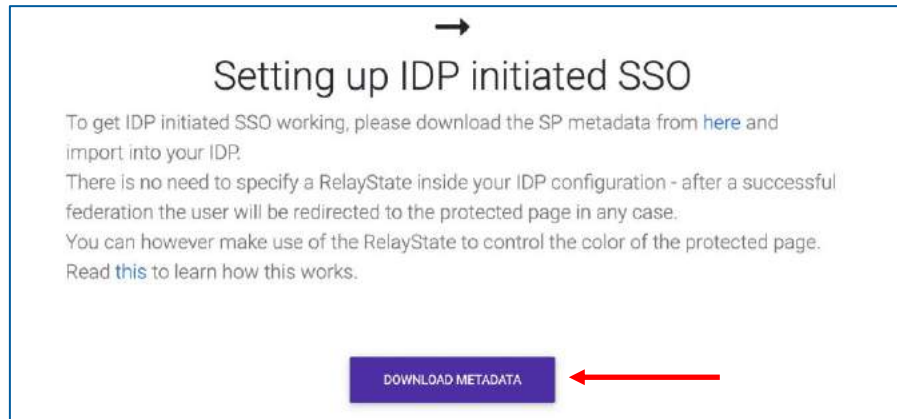
5. In a new Chrome Browser tab, navigate to <https://sptest.iamshowcase.com/index#start> then select **Instructions** and then **IDP initiated SSO**



CyberArk Workforce Identity

Application Management - SAML

6. Click on **Download Metadata**. This will load our metadata in a new browser tab.



7. We need the URL of our metadata found in the address bar of the browser. Copy the URL into memory.

A screenshot of a browser address bar. The address bar shows a lock icon followed by the URL "sptest.iamshowcase.com/testsp_metadata.xml". A red arrow points from the right towards the end of the URL.

CyberArk Workforce Identity

Application Management - SAML

8. Go back to the **Admin Portal**, we will add the URL in the SAML Service Provider settings. In the properties of our SAML App, select the **Trust** menu in the **Service Provider Configuration** section, under **Metadata**, paste the URL from the previous step, and then click **Load**. This will popularize the XML portion of the metadata section:

Service Provider Configuration

Select the configuration method specified by Service Provider, and then follow the instructions.

☒ Metadata
☐ Manual Configuration

Metadata

Use one of the following methods to import SP Metadata given by your Service Provider.

URL: **Load**

File:

XML:

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="IAMShowcase" validUntil="2025-12-09T09:13:31.006Z">
<md:SPSSODescriptor AuthnRequestsSigned="false"
```

9. On the **Permissions** menu, click **Add** and add **John's** account:

Permissions

[Learn more](#)

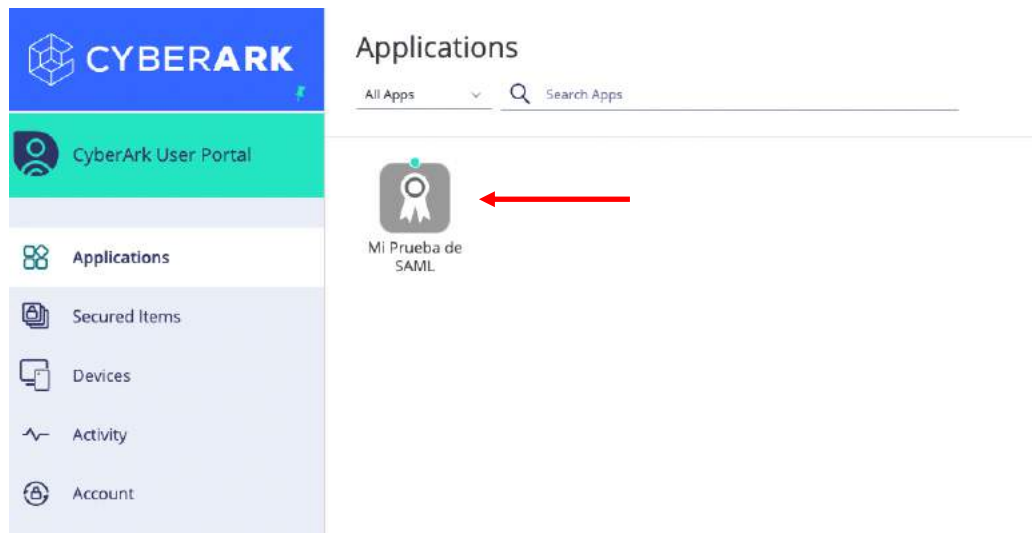
Add

Name	Grant	View	Manage	Delete	Run	Automatically D...	Starts	Expires	Inherited From
alicia-integration-user@S...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Administrat...
carol-integration-user@S...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Administrat...
System Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			Systemadm...
john@CYBR.COM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			

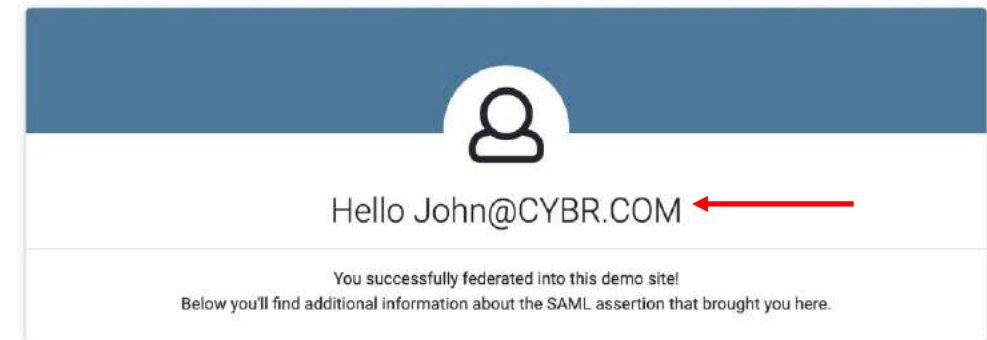
CyberArk Workforce Identity

Application Management - SAML

10. Authenticate with **John** in the **User Portal** and run the new SAML App. If the app does not appear, select the **Reload Rights** option by clicking on the menu for user John (upper right corner)



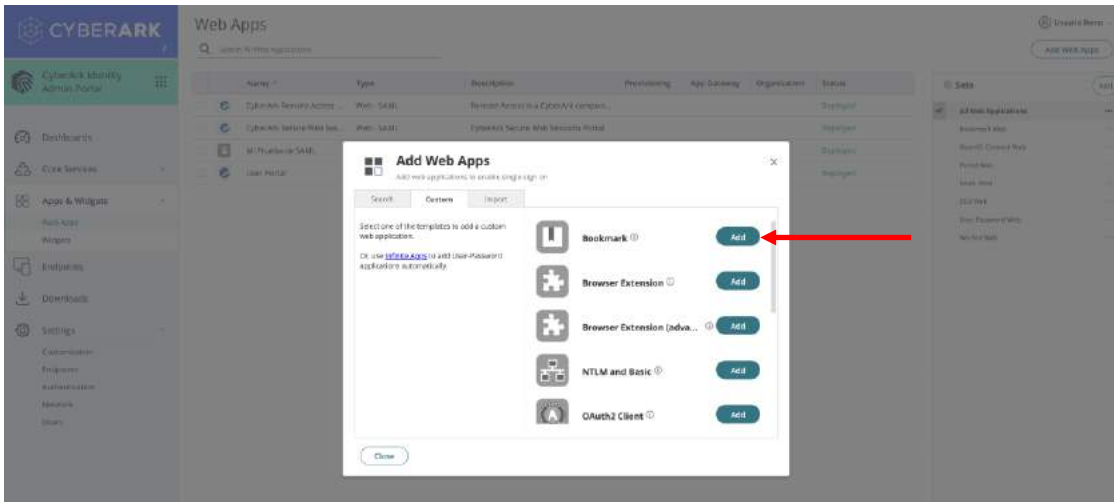
11. Clicking on the SAML App will open the **RSA SAML test** application, indicating successful federation for user John:



CyberArk Workforce Identity

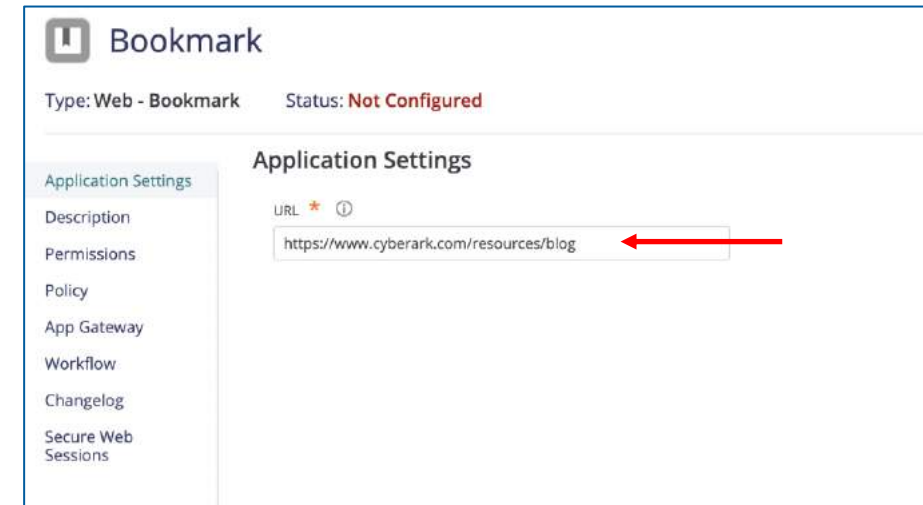
Application Management - Bookmark

1. Use Bookmark-type applications when you want to provide a link to the URL of a web application. This link does not provide any authentication mechanism. In the **Admin Portal**, in the **Apps & Widgets** menu, add a new Web App of type **Bookmark**:



2. Add the URL:

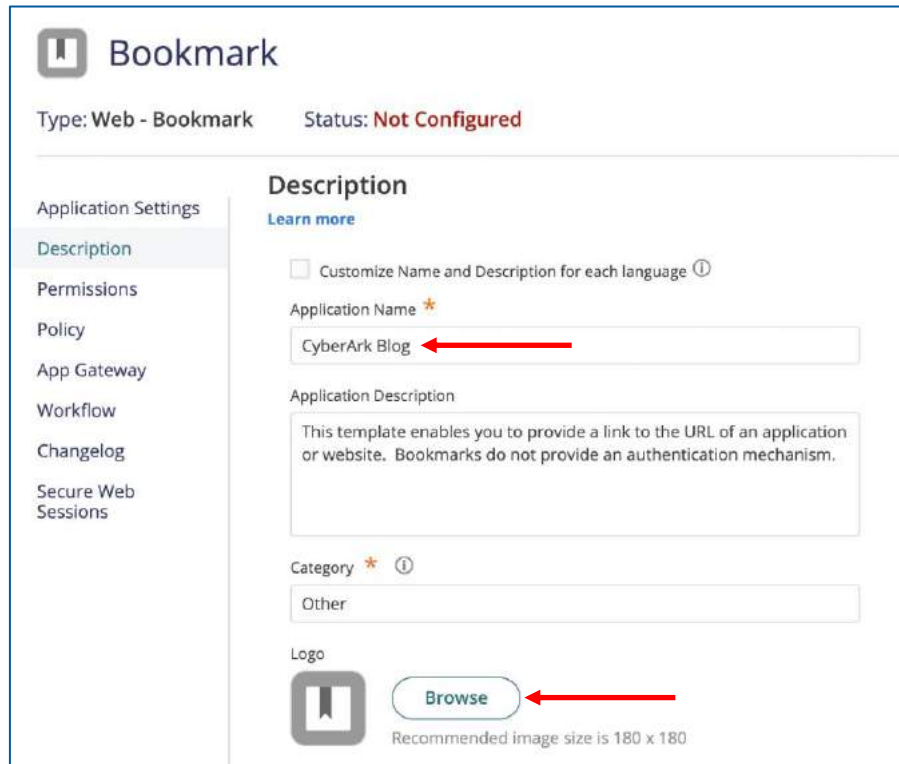
<https://www.cyberark.com/resources/blog>



CyberArk Workforce Identity

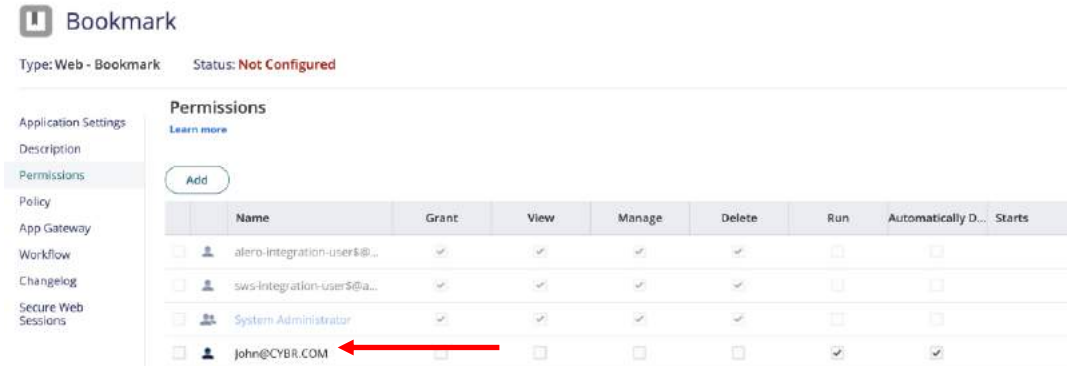
Application Management - Bookmark

3. In the **Description** menu, specify a name for the new app: **CyberArk Blog**. Change the logo if desired.



The screenshot shows the 'Bookmark' configuration page in the 'Description' tab. The left sidebar lists 'Application Settings', 'Description', 'Permissions', 'Policy', 'App Gateway', 'Workflow', 'Changelog', and 'Secure Web Sessions'. The main content area includes a 'Type: Web - Bookmark' and 'Status: Not Configured' header. Below is a 'Description' section with a 'Learn more' link and a checkbox for 'Customize Name and Description for each language'. The 'Application Name' field is set to 'CyberArk Blog' with a red arrow pointing to it. The 'Application Description' field contains a template text. The 'Category' is set to 'Other'. At the bottom, there is a 'Logo' section with a 'Browse' button and a red arrow pointing to it, and a note 'Recommended image size is 180 x 180'.

4. On the **Permissions** menu, add **John's** account:



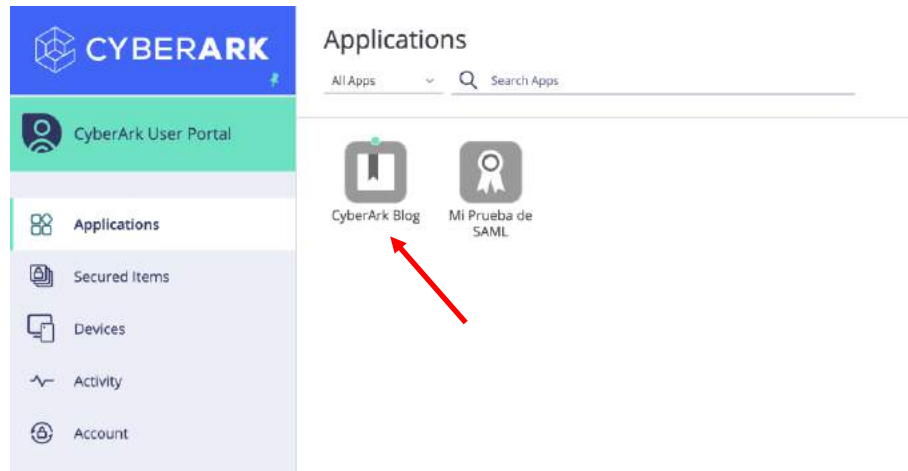
The screenshot shows the 'Bookmark' configuration page in the 'Permissions' tab. The left sidebar lists 'Application Settings', 'Description', 'Permissions', 'Policy', 'App Gateway', 'Workflow', 'Changelog', and 'Secure Web Sessions'. The main content area includes a 'Type: Web - Bookmark' and 'Status: Not Configured' header. Below is a 'Permissions' section with an 'Add' button and a table of permissions.

	Name	Grant	View	Manage	Delete	Run	Automatically D...	Starts
<input type="checkbox"/>	alero-integration-user\$@...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	sws-integration-user\$@a...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	System Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	john@CYBR.COM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

CyberArk Workforce Identity

Application Management - Bookmark

5. Authenticate to the **User Portal** as **John** and run the newly created App:

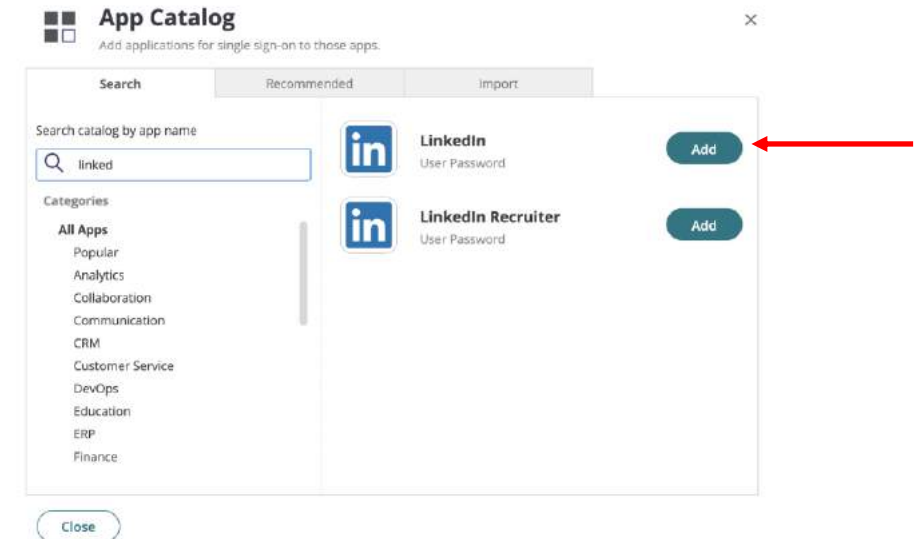
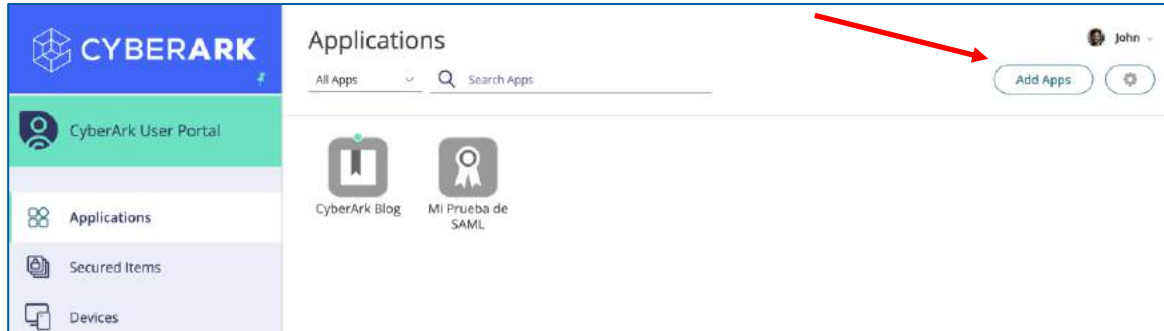


CyberArk Workforce Identity

Application Management – User/Password App

1. In the **User Portal**, click the **Add Apps** button to add a new application from the CyberArk Catalog.

2. In the catalog, find and add the **LinkedIn** app:



CyberArk Workforce Identity

Application Management – User/Password App

3. In the application properties, specify the following options:

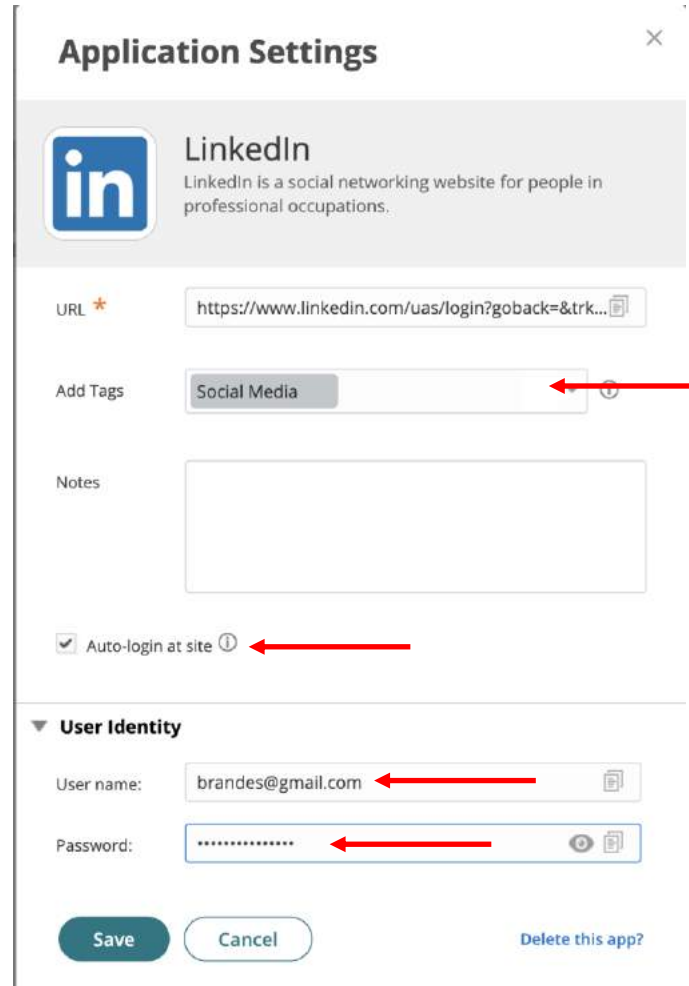
Add Tags: Social Media

Enable the Auto-Login at site option

Specify the **username**

Specify your **password**


Click in **Save**




The screenshot shows the 'Application Settings' dialog for a LinkedIn application. The dialog has a title bar with a close button. Below the title bar, there is a header section with the LinkedIn logo and the text 'LinkedIn' and 'LinkedIn is a social networking website for people in professional occupations.' Below this, there are several fields: 'URL' with a star icon and a text box containing 'https://www.linkedin.com/uas/login?goback=&trk...'; 'Add Tags' with a dropdown menu showing 'Social Media' and a red arrow pointing to it; 'Notes' with a text area; 'Auto-login at site' with a checked checkbox and a red arrow pointing to it. Below these fields is a section titled 'User Identity' with a dropdown arrow. It contains 'User name' with a text box containing 'brandes@gmail.com' and a red arrow pointing to it, and 'Password' with a text box containing '.....' and a red arrow pointing to it. At the bottom, there are three buttons: 'Save', 'Cancel', and 'Delete this app?'.


Application Settings

LinkedIn
LinkedIn is a social networking website for people in professional occupations.


URL 


Add Tags 

Notes

☒ Auto-login at site 

User Identity

User name: 

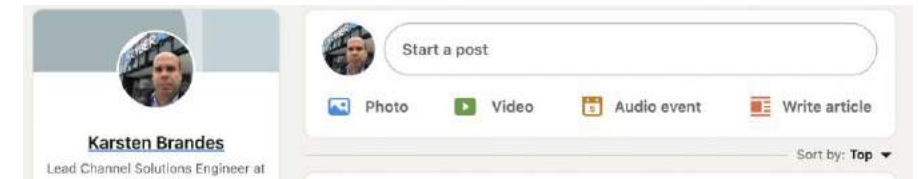
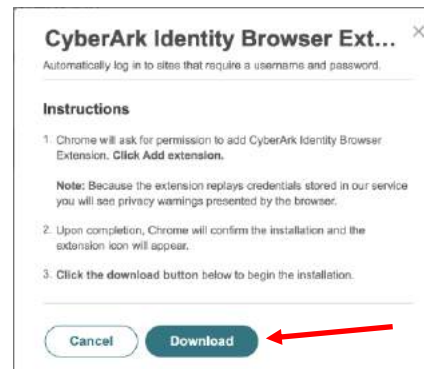
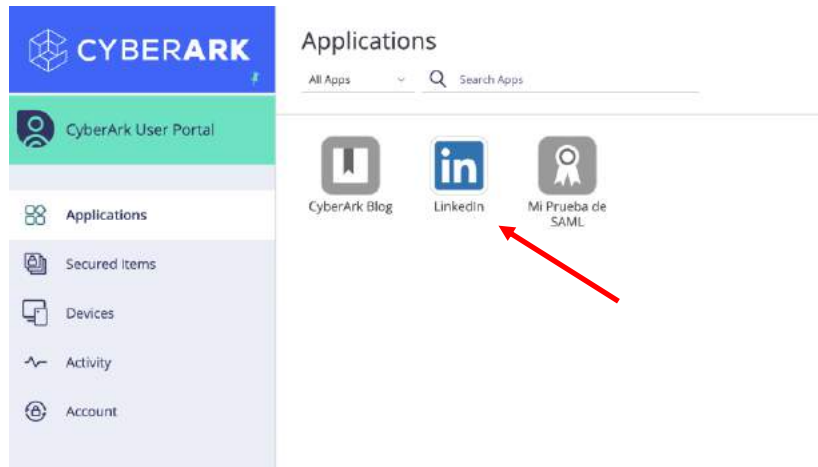
Password: 

Save **Cancel** [Delete this app?](#)

CyberArk Workforce Identity

Application Management – User/Password App

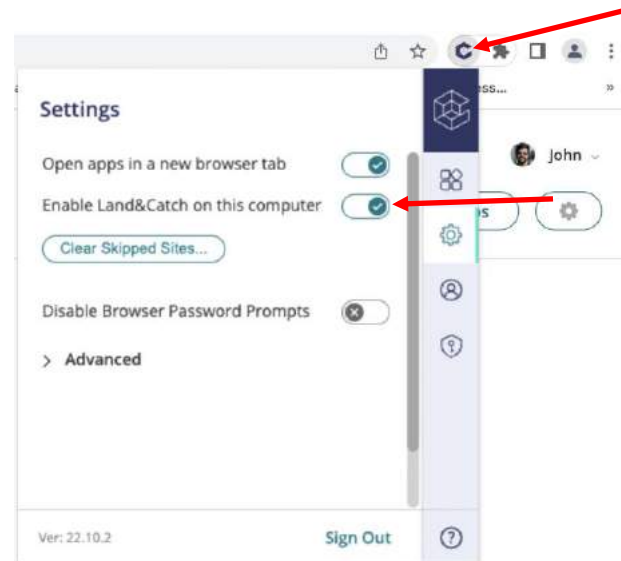
4. Run the **LinkedIn** app from the SSO portal. This will prompt for installation of the browser extension, click **Install**, **Download** and then add it in Chrome. The browser extension is an addon required for SSO to certain web applications. The extension is required by any application that has a puzzle piece icon in the user portal.



CyberArk Workforce Identity

Application Management – Land & Catch

1. Apps can also be added to the User Portal using the Land&Catch feature of the browser extension. This feature detects when you enter credentials on a web page and then adds the site to your user portal. Land & Catch must be enabled by your system administrator and then enabled on your computer. In your browser, click on the **Identity extension** and verify that the **Enable Land&Catch on this computer** option is enabled.



CyberArk Workforce Identity

Application Management – Land & Catch

2. In your browser, enter the web application you want to add to the User Portal and authenticate with your own credentials. The browser extension will detect this action and will add the site to the **User Portal**. In this example, I'll use the **Udemy** app. Once the new application is added, try to login through the User Portal, notice that the credentials are injected automatically:

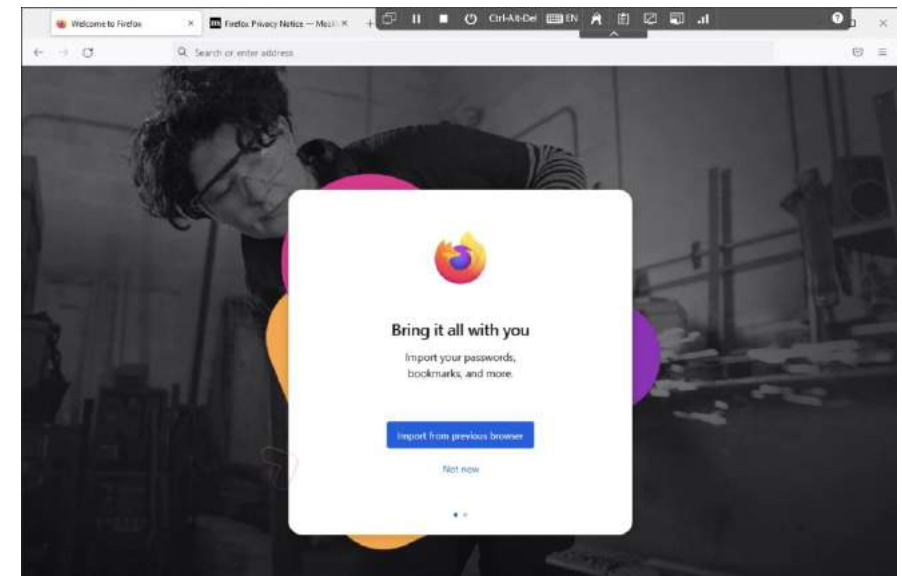
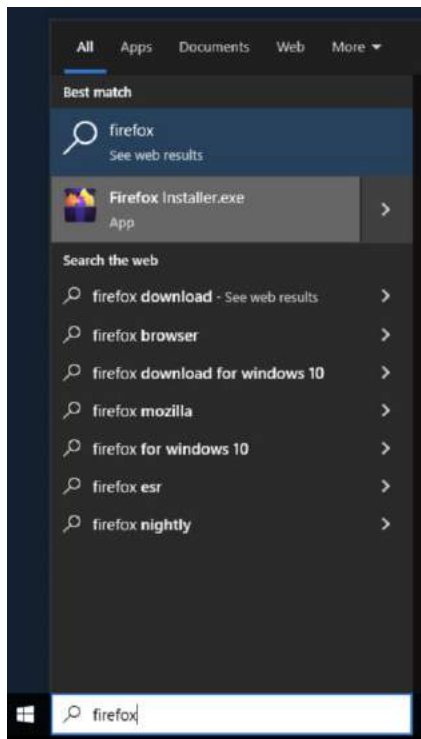
The image displays a sequence of four screenshots illustrating the 'Land & Catch' process in CyberArk Workforce Identity:

- Udemy Login Page:** A screenshot of the Udemy login page. It features options to 'Continue with Facebook', 'Continue with Google', and 'Continue with Apple'. Below these is a text input field for the email address 'brandes@gmail.com' and a password field. A prominent purple 'Log In' button is at the bottom. Links for 'or Forgot Password' and 'Don't have an account? Sign up' are also visible.
- Browser Extension Popup:** A screenshot of a browser extension popup titled 'Add this site to your User Portal?'. It shows the detected site 'Udemy - brandes' and provides a text area to 'Add a description...'. At the bottom, there are 'Yes', 'No', and 'Never' buttons, along with an 'Upload' button and a small Udemy logo.
- CyberArk User Portal:** A screenshot of the CyberArk User Portal interface. The left sidebar shows navigation options: Applications, Secured Items, Devices, Activity, and Account. The main content area, titled 'Applications', displays a list of added applications including 'CyberArk Blog', 'LinkedIn', 'Mi Prueba de SAML', and 'Udemy - brandes'.
- Signing In Dialog:** A screenshot of a 'Signing In...' dialog box. It features a loading spinner and the text 'Please wait while you are signed in.', indicating that the system is automatically injecting credentials for the selected application.

CyberArk Workforce Identity

Application Management – Infinite Apps

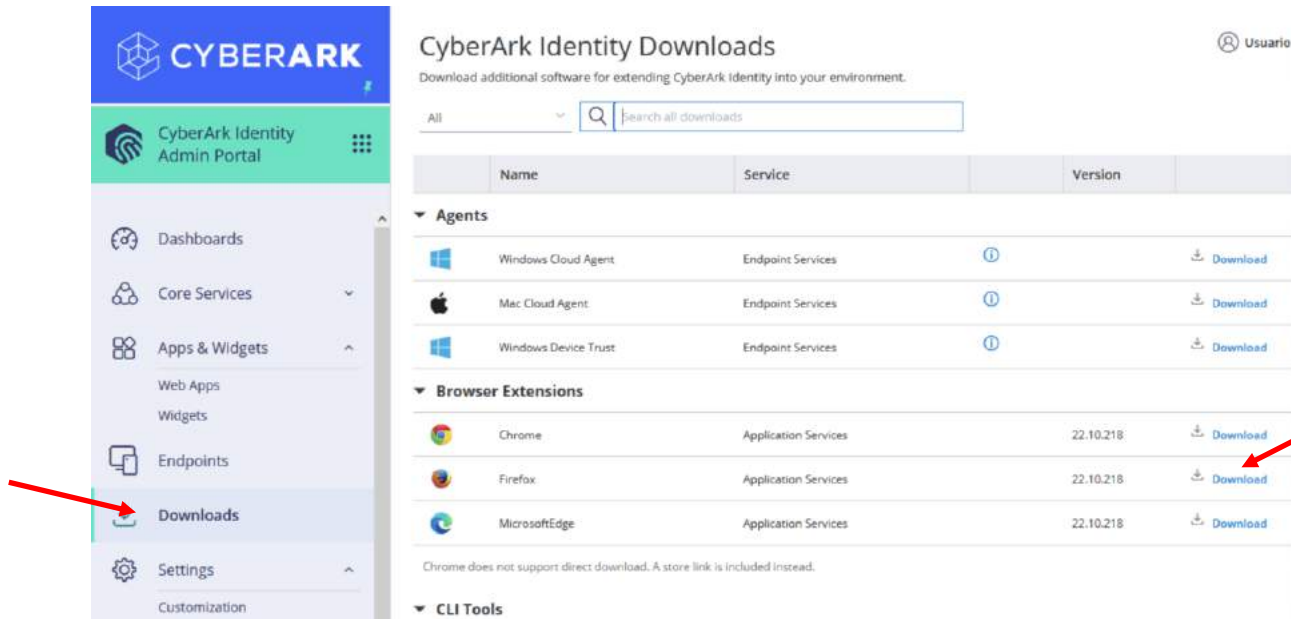
1. **Infinite Apps** is a browser extension feature that simplifies the creation of username/password applications that are not available in the catalog. Infinite Apps captures the **username** and **password** fields of the web application and adds the application to the Web Apps page of the **Admin Portal**, from where you can configure additional options, add authentication mechanisms and deploy the app to user portals and mobile devices. Infinite Apps is available for **Firefox browsers only**. On the **CLIENT01** workstation, locate the Firefox installer and run it with the **CYBR\Mike** account:



CyberArk Workforce Identity

Application Management – Infinite Apps

2. In Firefox, authenticate to the **Admin Portal** and then enter the **Downloads** menu to download the browser extension:



CYBERARK CyberArk Identity Admin Portal

CyberArk Identity Downloads
Download additional software for extending CyberArk Identity into your environment.

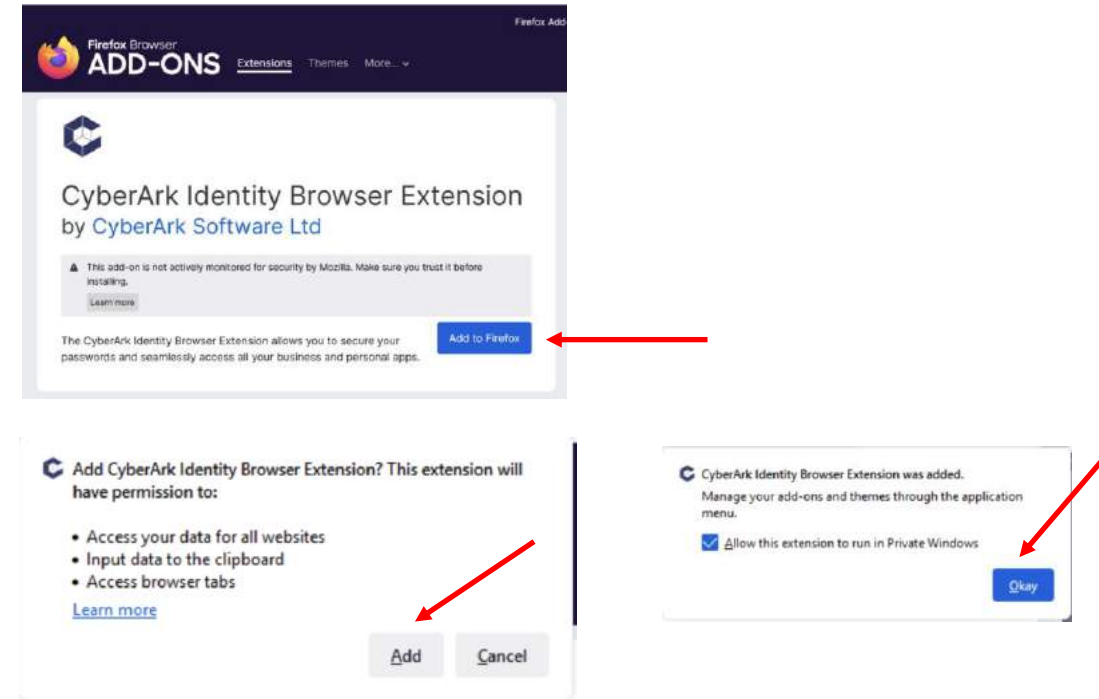
All

Name	Service	Version	
Agents			
Windows Cloud Agent	Endpoint Services	22.10.218	Download
Mac Cloud Agent	Endpoint Services	22.10.218	Download
Windows Device Trust	Endpoint Services	22.10.218	Download
Browser Extensions			
Chrome	Application Services	22.10.218	Download
Firefox	Application Services	22.10.218	Download
MicrosoftEdge	Application Services	22.10.218	Download

Chrome does not support direct download. A store link is included instead.

CLI Tools

3. Add the extension:



Firefox Browser ADD-ONS Extensions Themes More...

CyberArk Identity Browser Extension
by CyberArk Software Ltd

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.
[Learn more](#)

The CyberArk Identity Browser Extension allows you to secure your passwords and seamlessly access all your business and personal apps. [Add to Firefox](#)

Add CyberArk Identity Browser Extension? This extension will have permission to:

- Access your data for all websites
- Input data to the clipboard
- Access browser tabs

[Learn more](#) [Add](#) [Cancel](#)

CyberArk Identity Browser Extension was added.
Manage your add-ons and themes through the application menu.
☒ Allow this extension to run in Private Windows [Okay](#)

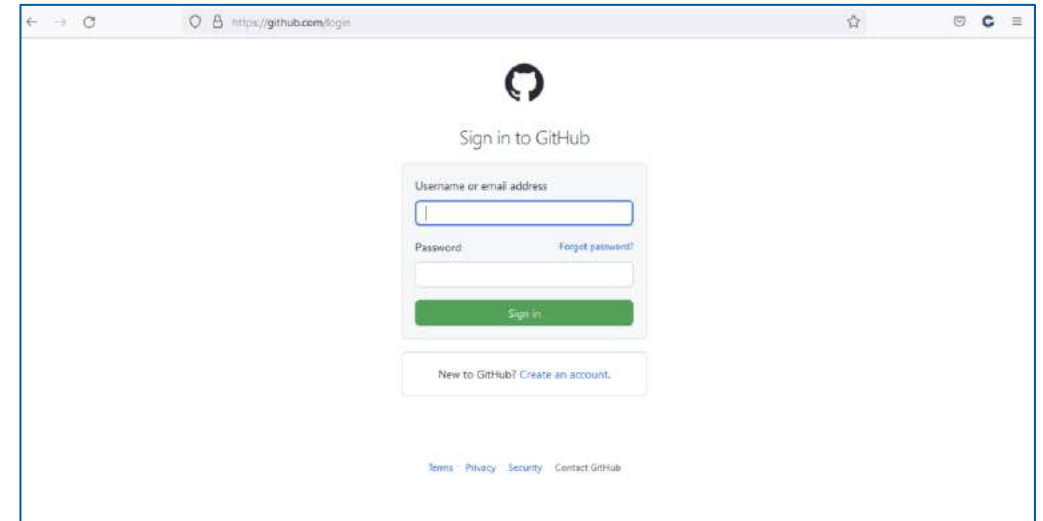
CyberArk Workforce Identity

Application Management – Infinite Apps

4. Authenticate to the browser extension:



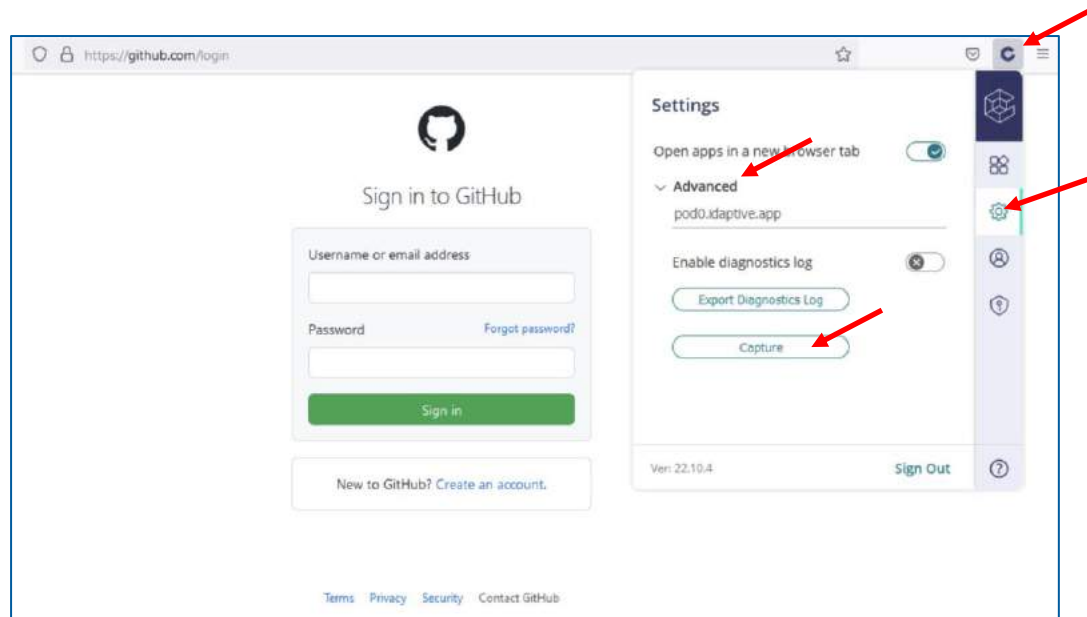
5. In Firefox, go to a web application that you want to capture, in this example, I will use **Github**:



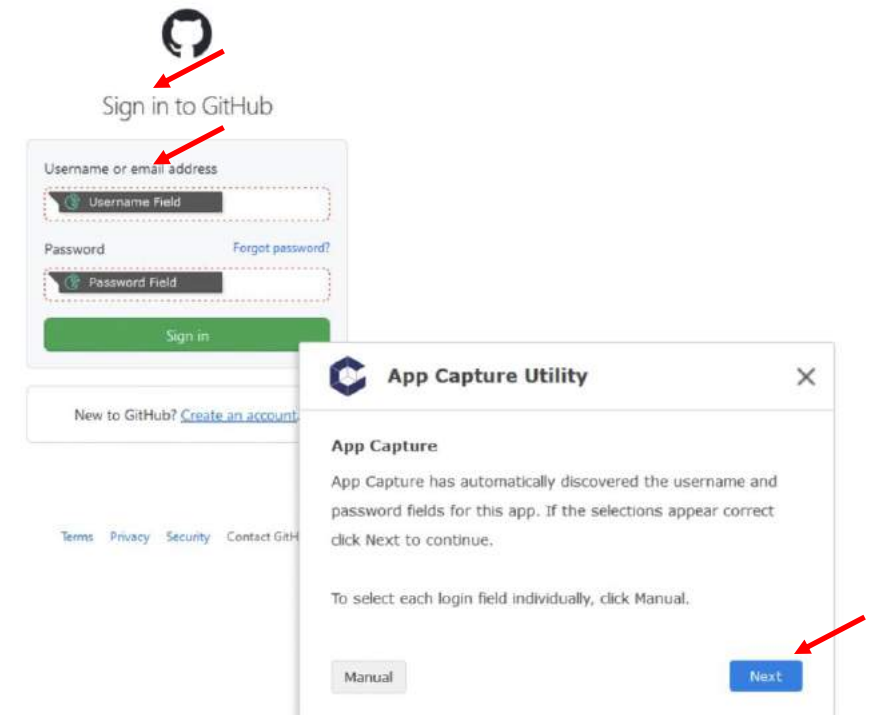
CyberArk Workforce Identity

Application Management – Infinite Apps

6. In the browser extension, click **Settings – Advanced** and then click the **Capture** button:



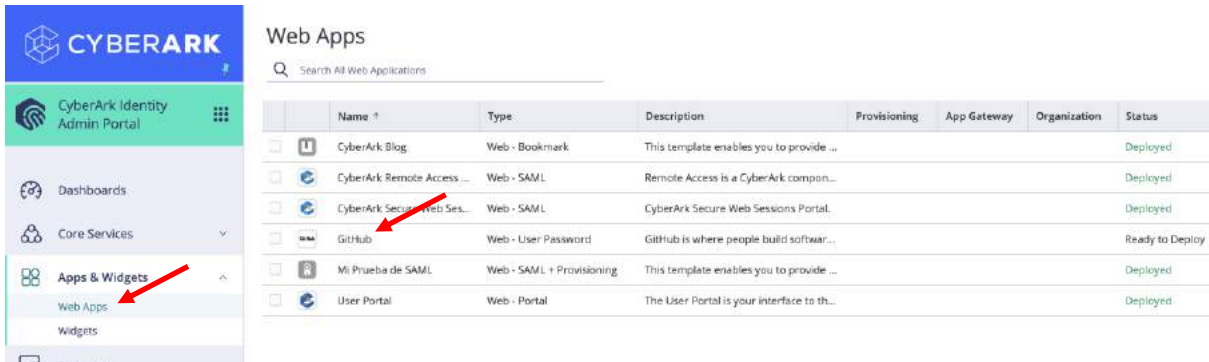
7. The fields will be captured automatically. In the wizard, specify that no additional values are required and leave the other options by default. Add the application to the **Admin Portal**.



CyberArk Workforce Identity

Application Management – Infinite Apps

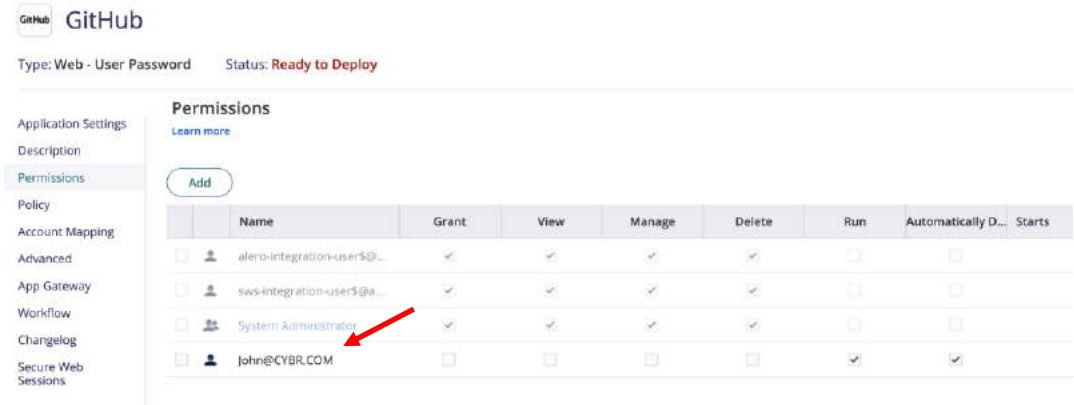
8. In the **Admin Portal**, in the **Apps & Widgets** menu | **Web Apps**, note that the **GitHub** app was added, select it to edit its properties:



The screenshot shows the CyberArk Admin Portal interface. On the left, the 'Apps & Widgets' menu is expanded, and 'Web Apps' is selected. The main area displays a table of 'Web Apps' with columns: Name, Type, Description, Provisioning, App Gateway, Organization, and Status. The 'GitHub' app is highlighted with a red arrow.

	Name ↑	Type	Description	Provisioning	App Gateway	Organization	Status
<input type="checkbox"/>	CyberArk Blog	Web - Bookmark	This template enables you to provide ...				Deployed
<input type="checkbox"/>	CyberArk Remote Access ...	Web - SAML	Remote Access is a CyberArk compon...				Deployed
<input type="checkbox"/>	CyberArk Secure Web Ses...	Web - SAML	CyberArk Secure Web Sessions Portal.				Deployed
<input type="checkbox"/>	GitHub	Web - User Password	GitHub is where people build softwar...				Ready to Deploy
<input type="checkbox"/>	Mi Prueba de SAML	Web - SAML + Provisioning	This template enables you to provide ...				Deployed
<input type="checkbox"/>	User Portal	Web - Portal	The User Portal is your interface to th...				Deployed

9. In the **Permissions** menu, add **John**:



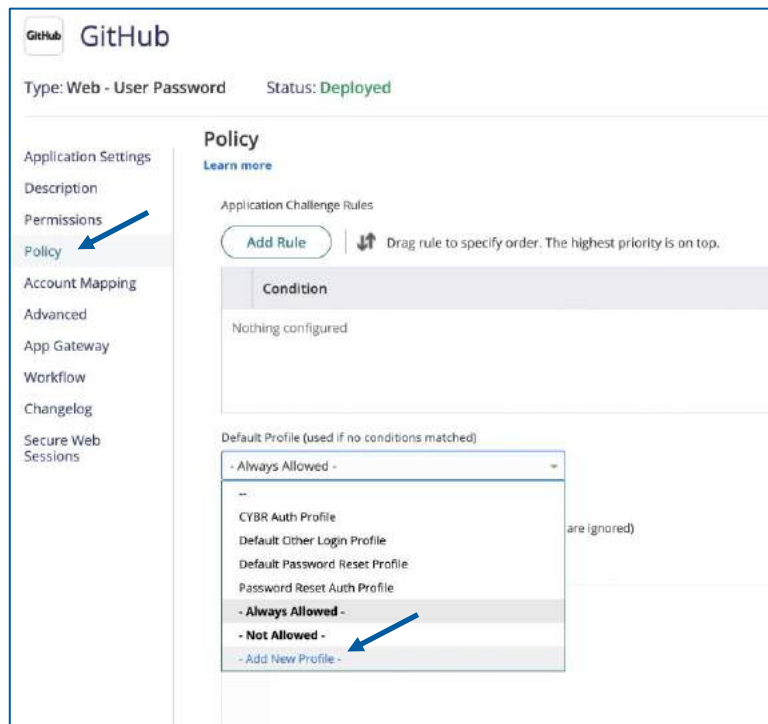
The screenshot shows the 'GitHub' app configuration page. The 'Permissions' section is active, and a table lists the permissions for various users. The 'John@CYBR.COM' user is highlighted with a red arrow.

	Name	Grant	View	Manage	Delete	Run	Automatically D...	Starts
<input type="checkbox"/>	alero-integration-user@...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	sws-integration-user@...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	System Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	John@CYBR.COM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

CyberArk Workforce Identity

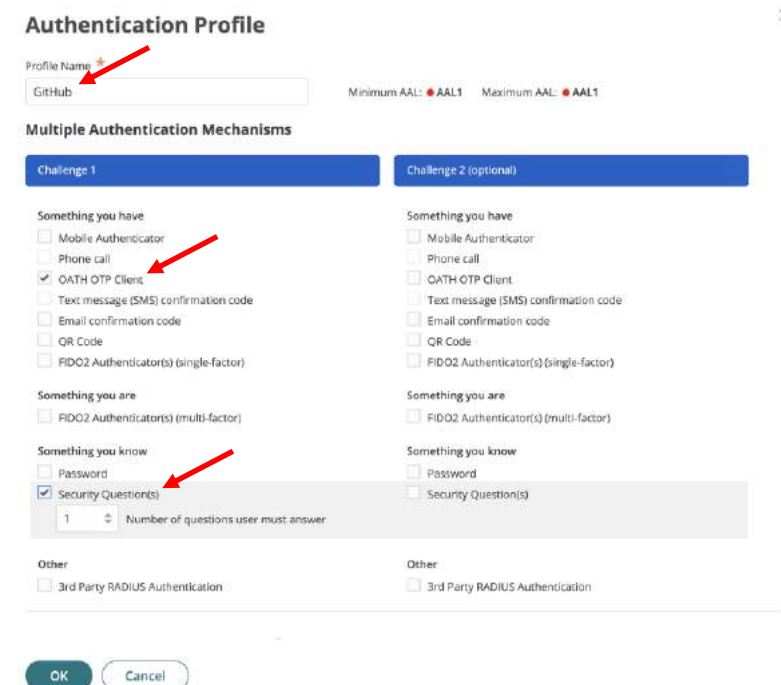
Application Management – Infinite Apps

10. In the **Policy** menu, we'll add an additional authentication mechanism to verify the user's identity every time they try to log in to the **github** portal. In the **Default Profile** section, select the **Add New Profile** option:



The screenshot shows the 'GitHub' application settings. The 'Policy' tab is active in the left sidebar. Under the 'Default Profile' section, a dropdown menu is open, and the 'Add New Profile' option is highlighted with a blue arrow.

11. Specify **GitHub** as the name for the profile, and enable **OATH OTP Client** and **Security Questions** as authentication mechanisms in the first challenge:

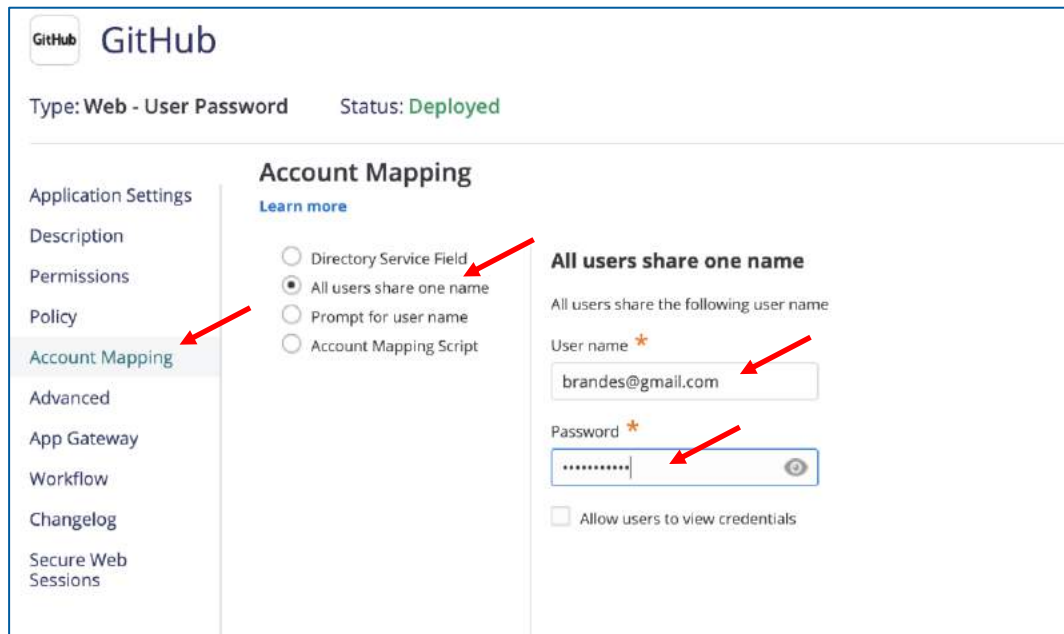


The screenshot shows the 'Authentication Profile' configuration window. The 'Profile Name' is set to 'GitHub'. In the 'Multiple Authentication Mechanisms' section, 'OATH OTP Client' and 'Security Questions' are selected for 'Challenge 1'.

CyberArk Workforce Identity

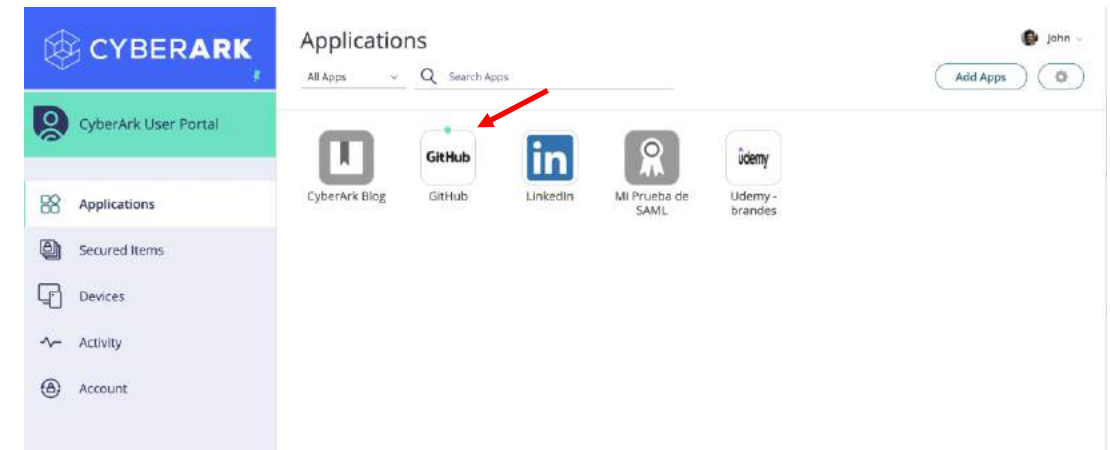
Application Management – Infinite Apps

12. Go to the **Account Mapping** menu, select the **All Users share one name** option, and add the username/password for the GitHub portal. Note that a single set of credentials could be shared by an entire development team. Finally click on **Save**:



The screenshot shows the 'GitHub' application configuration page. The 'Account Mapping' section is active, showing the 'All users share one name' option selected. The 'User name' field is populated with 'brandes@gmail.com' and the 'Password' field is masked with dots. Red arrows point to the 'Account Mapping' menu item in the left sidebar, the 'All users share one name' radio button, and the 'User name' and 'Password' input fields.

13. In the **User Portal**, authenticated with John, go to the Github portal. Note that John does not have access to credentials, we have only published the app on his SSO portal.



CyberArk Workforce Identity

Application Management – Infinite Apps

14. Note that when you have configured MFA, an additional authentication method is requested, select **OATH OTP Client** and then specify the verification code obtained from your OATH client app. If the code is correct, the portal will open and the browser extension will inject the credentials into the GitHub portal:

CYBERARK

< Start Over

Additional authentication required to continue with this action.
John@CYBR.COM

Choose authentication method

OATH OTP Client

Continue with OATH OTP Client Authenticator

CYBERARK

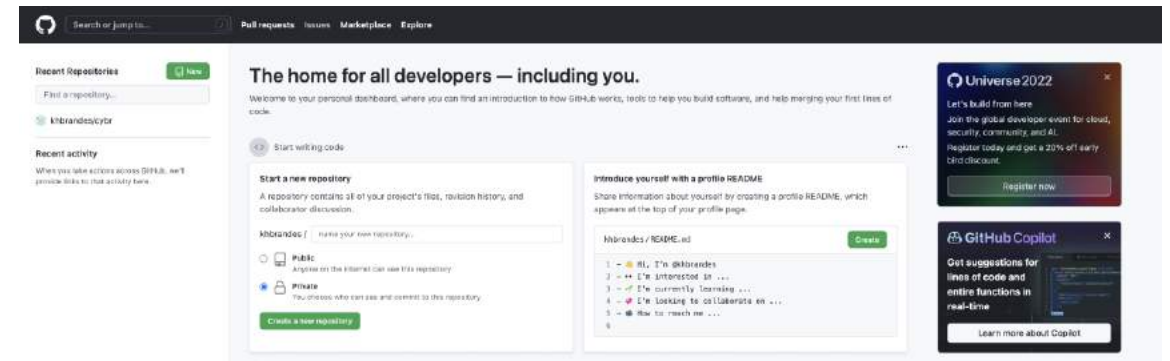
< Start Over

Provide a code
John@CYBR.COM

Enter Verification Code

Enter code

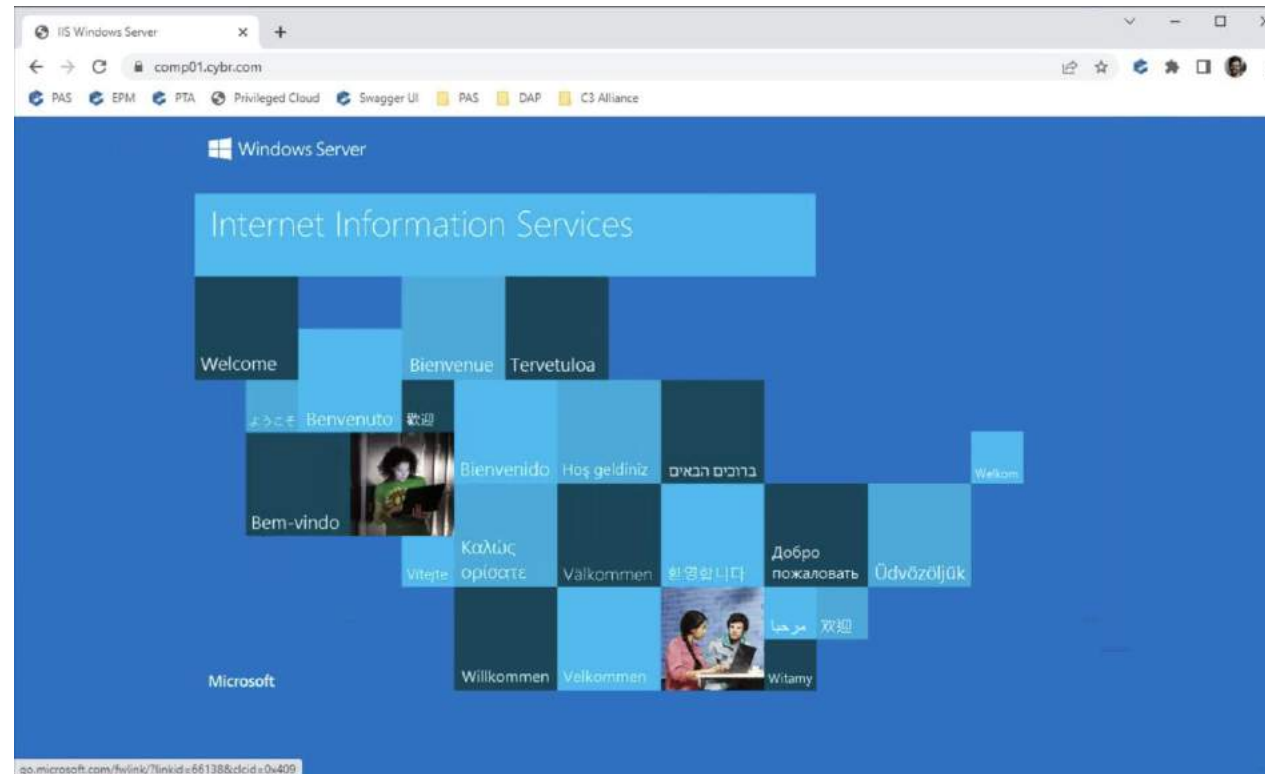
Authenticate



CyberArk Workforce Identity

Application Management – Application Gateway

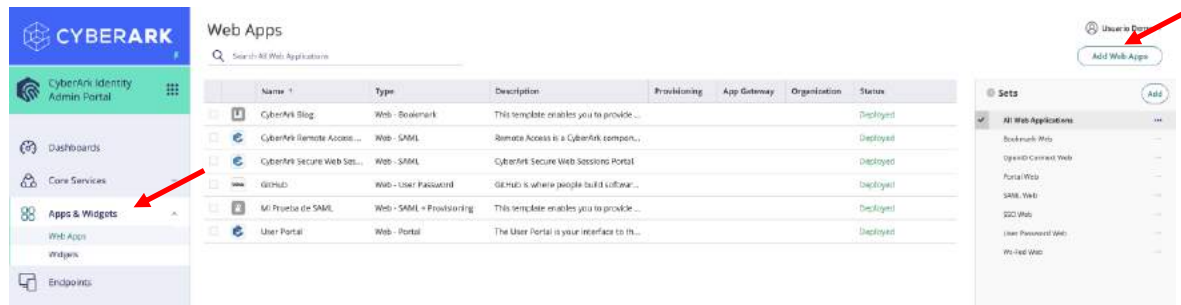
1. The Identity connector provides an **Application Gateway** functionality that allows end users to remotely access VPN-free web applications that are available on the organization's internal network. In this example, we'll add the IIS Web portal (<https://comp01.cybr.com>).



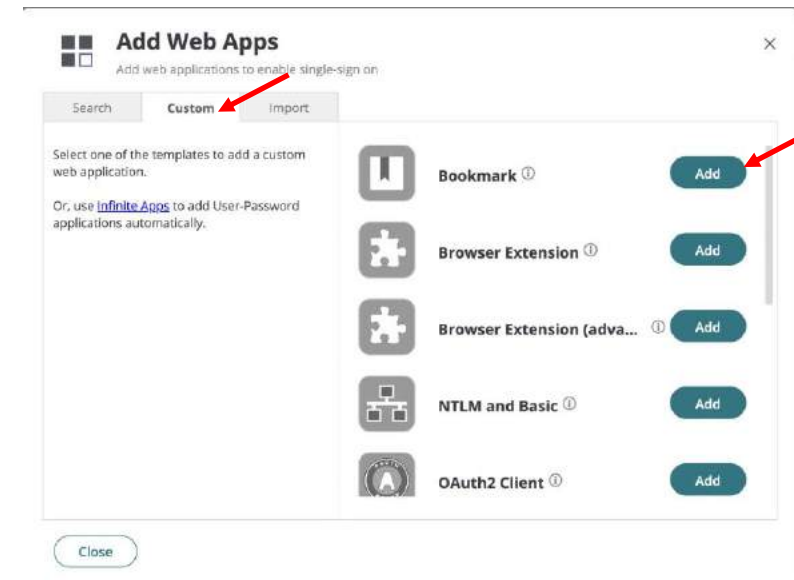
CyberArk Workforce Identity

Application Management – Application Gateway

2. In the **Admin Portal**, add a new Web App from the **Apps & Widgets** menu | **Web Apps**:



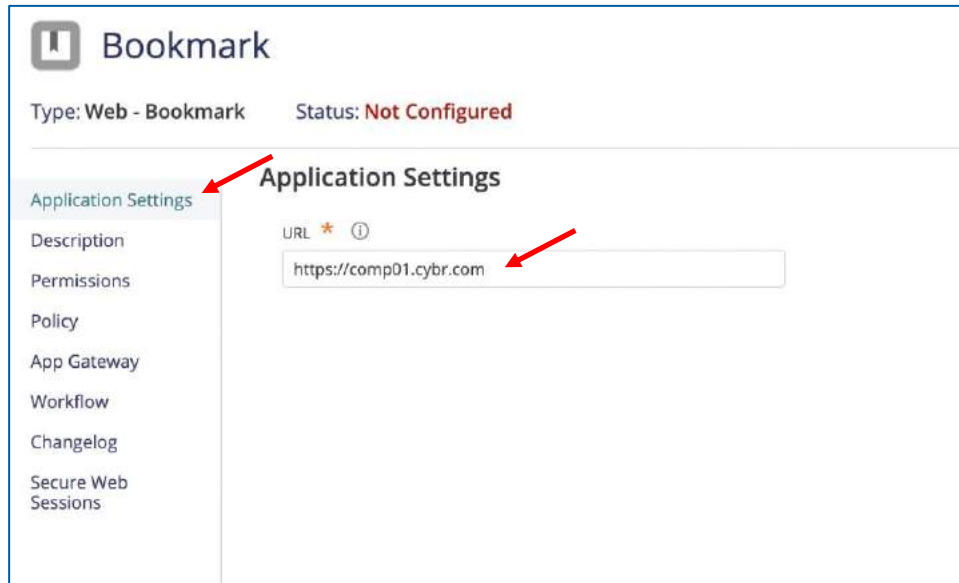
3. In the **Add Web Apps** window, on the **Custom** tab, add an app of type **Bookmark**:



CyberArk Workforce Identity

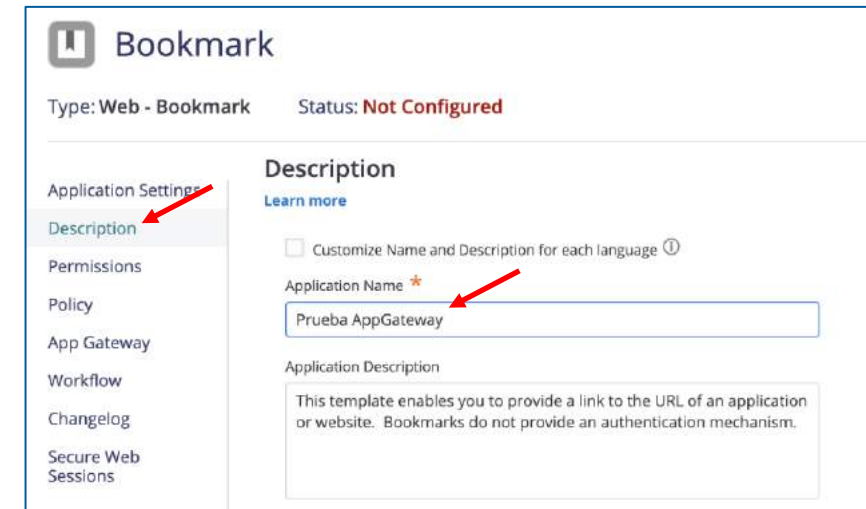
Application Management – Application Gateway

4. In the **Application Settings** menu, add the URL **https://comp01.cybr.com**:



The screenshot shows the 'Bookmark' configuration page in the CyberArk Application Gateway. The page has a header with a bookmark icon and the title 'Bookmark'. Below the header, it shows 'Type: Web - Bookmark' and 'Status: Not Configured'. A left sidebar contains a list of tabs: 'Application Settings', 'Description', 'Permissions', 'Policy', 'App Gateway', 'Workflow', 'Changelog', and 'Secure Web Sessions'. The 'Application Settings' tab is selected and highlighted. In the main content area, there is a 'URL' field with a star icon and an information icon. The URL 'https://comp01.cybr.com' is entered in the field. Two red arrows point to the 'Application Settings' tab and the URL input field.

5. On the **Description** menu, specify a new name for the app:

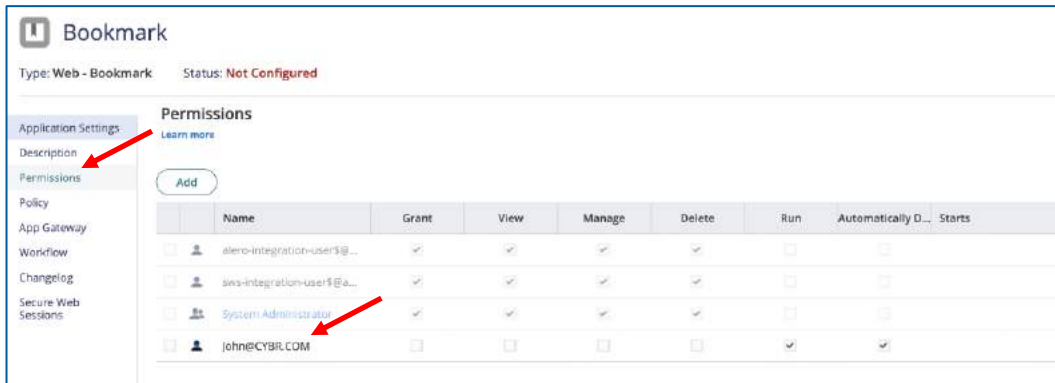


The screenshot shows the 'Bookmark' configuration page in the CyberArk Application Gateway, specifically the 'Description' tab. The page has a header with a bookmark icon and the title 'Bookmark'. Below the header, it shows 'Type: Web - Bookmark' and 'Status: Not Configured'. A left sidebar contains a list of tabs: 'Application Settings', 'Description', 'Permissions', 'Policy', 'App Gateway', 'Workflow', 'Changelog', and 'Secure Web Sessions'. The 'Description' tab is selected and highlighted. In the main content area, there is a 'Description' section with a 'Learn more' link. Below the link, there is a checkbox labeled 'Customize Name and Description for each language' with an information icon. Below the checkbox, there is an 'Application Name' field with a star icon. The name 'Prueba AppGateway' is entered in the field. Below the name field, there is an 'Application Description' section with a text area containing the text: 'This template enables you to provide a link to the URL of an application or website. Bookmarks do not provide an authentication mechanism.' Two red arrows point to the 'Description' tab and the 'Application Name' input field.

CyberArk Workforce Identity

Application Management – Application Gateway

6. On the **Permissions** menu, add **John's** account:



Bookmark

Type: Web - Bookmark Status: Not Configured

Application Settings

Description

Permissions

Policy

App Gateway

Workflow

Changelog

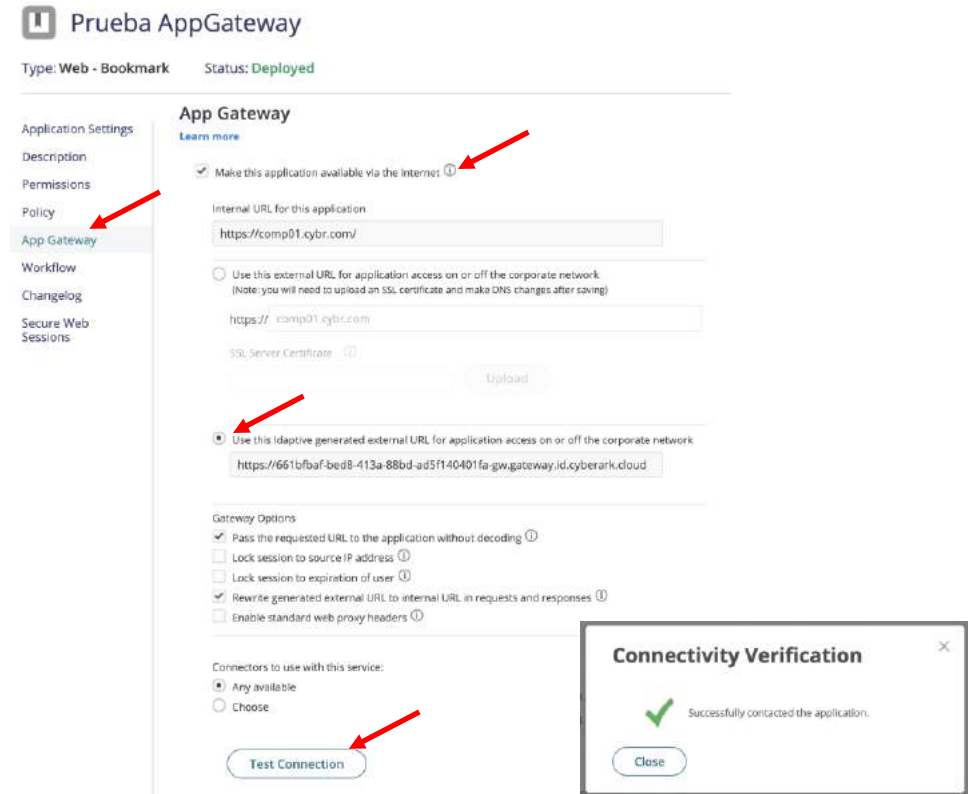
Secure Web Sessions

Permissions

Add

	Name	Grant	View	Manage	Delete	Run	Automatically D...	Starts
<input type="checkbox"/>	alero-integration-user\$@...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	sis-integration-user\$@a...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	System Administrator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	john@CYBR.COM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

7. From the **App Gateway** menu, enable the **Make this app available via the internet** option, and select the **Use this Idaptive generated external URL....** option. Then click on **Test Connection**:



Prueba AppGateway

Type: Web - Bookmark Status: Deployed

Application Settings

Description

Permissions

Policy

App Gateway

Workflow

Changelog

Secure Web Sessions

App Gateway

Learn more

☒ Make this application available via the internet

Internal URL for this application

https://comp01.cybr.com/

☐ Use this external URL for application access on or off the corporate network.
(Note: you will need to upload an SSL certificate and make DNS changes after saving)

https://comp01.cybr.com

SSL Server Certificate

Upload

☒ Use this Idaptive generated external URL for application access on or off the corporate network

https://661bf0af-bed8-413a-88bd-ad5f140401fa-gw.gateway.id.cyberark.cloud

Gateway Options

☒ Pass the requested URL to the application without decoding

☐ Lock session to source IP address

☐ Lock session to expiration of user

☒ Rewrite generated external URL to internal URL in requests and responses

☐ Enable standard web proxy headers

Connectors to use with this service:

☒ Any available

☐ Choose

Test Connection

Connectivity Verification

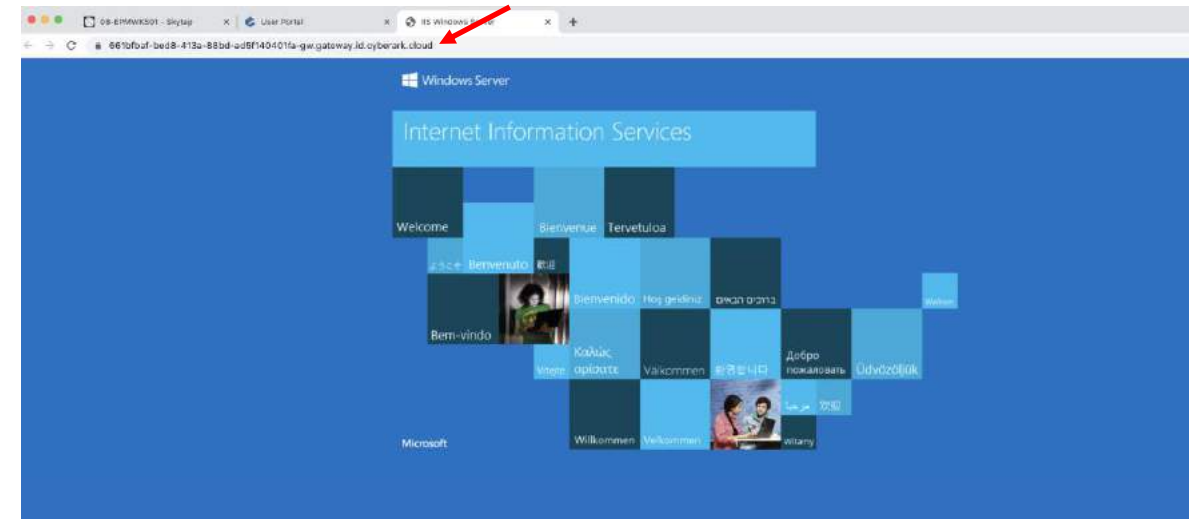
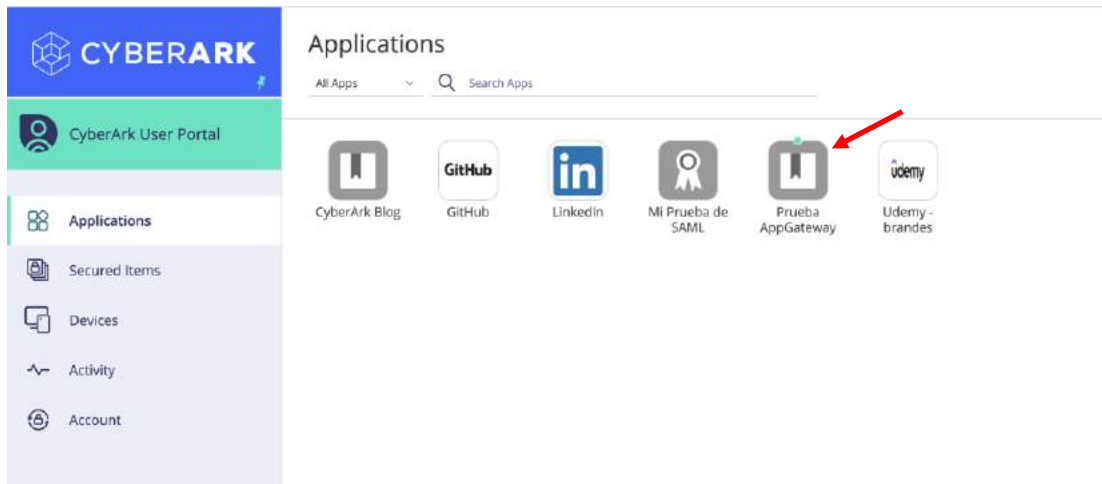
Successfully contacted the application.

Close

CyberArk Workforce Identity

Application Management – Application Gateway

8. Authenticate to the **User Portal** as **John** and run the newly added application. If you get the error "**This site cant be reached**" wait a few minutes and try again. Note the URL generated by Identity.

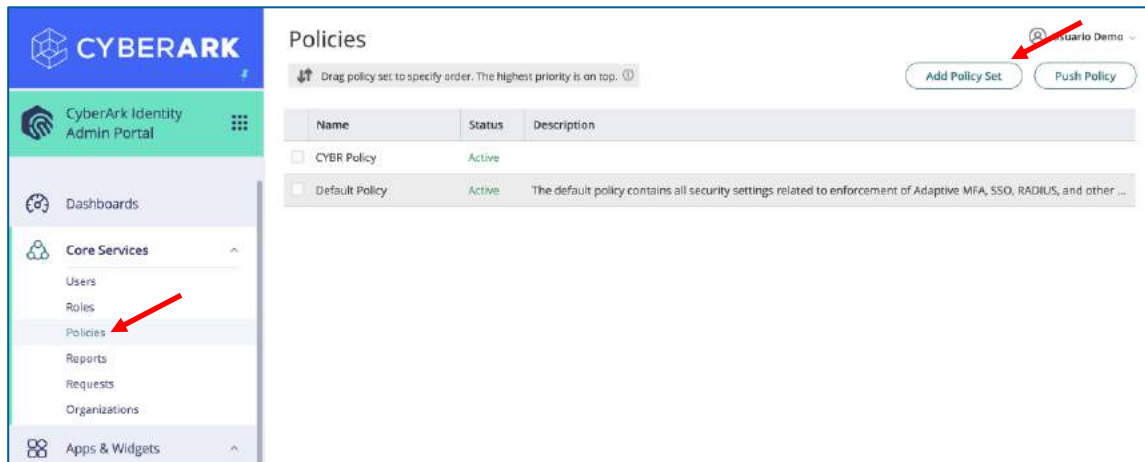


CyberArk Workforce Identity

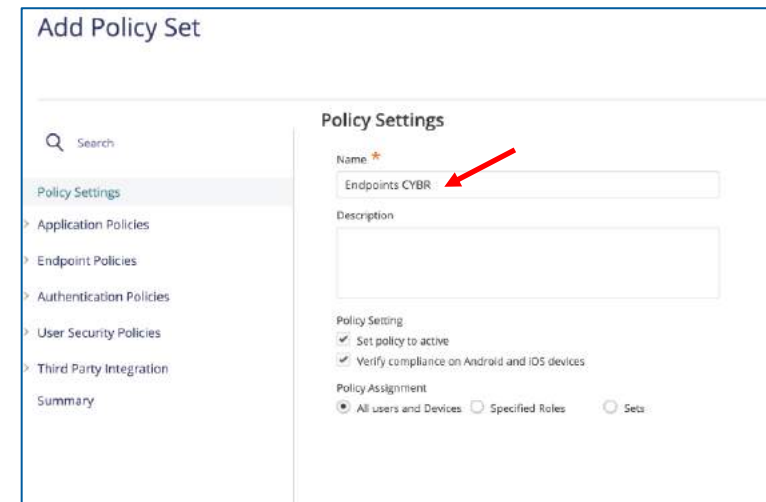
Endpoint Authentication

In this use case, we will install the **CyberArk Identity Agent** on the **CLIENT01** workstation to demonstrate MFA authentication to the OS. We will test John's passwordless authentication with Mobile Authentication.

1. In the **Admin Portal**, in the **Core Services** menu | **Policies**, add a new policy for our Endpoints:



2. In the **Policy Settings** menu, name the policy (CYBR Endpoints):



CyberArk Workforce Identity

Endpoint Authentication

3. On the **Authentication Policies** menu | **Endpoint Authentication**, enable the **Enable authentication policy controls** option, and in the **Default Profile** section add a new profile:

Add Policy Set

Search

Policy Settings

- Application Policies
- Endpoint Policies
- Authentication Policies
 - CyberArk Identity
 - CyberArk Identity Admin Portal
 - Local Account Linking
 - Endpoint Authentication**
- User Security Policies
- Third Party Integration
- Summary

Endpoint Authentication

Yes ☐ Enable authentication policy controls

Authentication Rules ⓘ

Add Rule ⬆️ Drag rule to specify order. The highest priority is on top.

Condition	Authentication Profile
Nothing configured	

Default Profile (used if no conditions matched) ⭐

- CYBR Auth Profile
- Default Other Login Profile
- Default Password Reset Profile
- GitHub
- Password Reset Auth Profile
- Always Allowed -
- Not Allowed -
- Add New Profile -

4. Specify a name for the new profile (Endpoints Profile) and define the following authentication mechanisms. Finally **save** the new policy.

Authentication Profile

Profile Name ⭐

Endpoints Profile Minimum AAL: AAL2 Maximum AAL: AAL2

Multiple Authentication Mechanisms

Challenge 1

Something you have

- ☐ Mobile Authenticator
- ☐ Phone call
- ☐ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Email confirmation code
- ☐ QR Code
- ☐ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

- ☒ Password
- ☐ Security Question(s)

1 Number of questions user must answer

Other

- ☐ 3rd Party RADIUS Authentication

Challenge 2 (optional)

Something you have

- ☒ Mobile Authenticator
- ☐ Phone call
- ☒ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Email confirmation code
- ☐ QR Code
- ☐ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

- ☐ Password
- ☐ Security Question(s)

Other

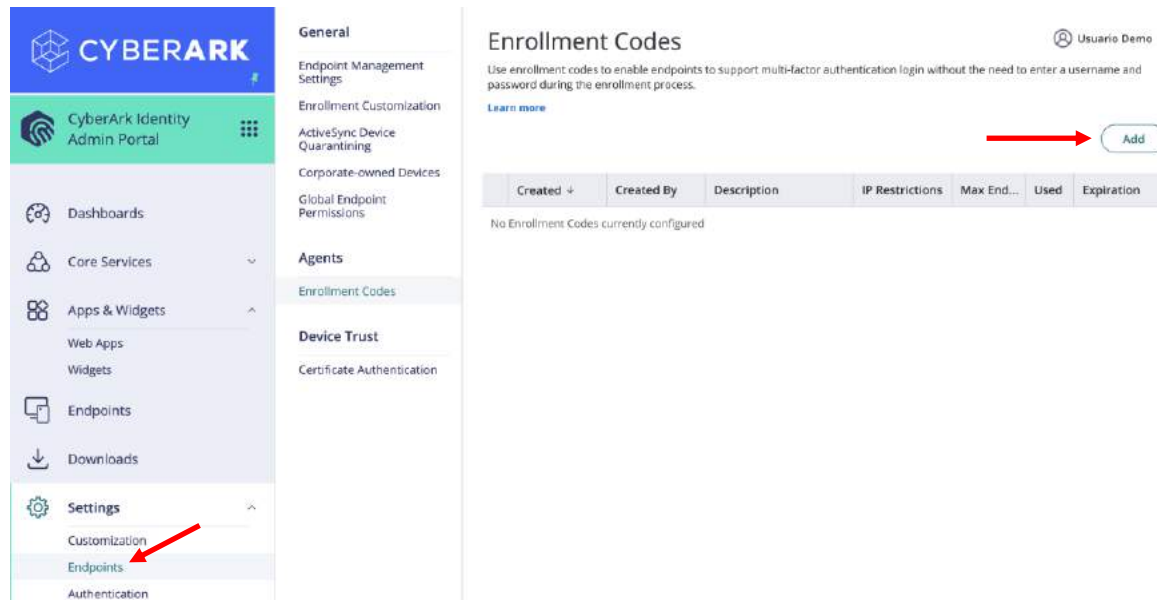
- ☐ 3rd Party RADIUS Authentication

OK Cancel

CyberArk Workforce Identity

Endpoint Authentication

5. Now we will generate a security code to enroll agents in our environment. Go to the **Settings** menu | **Endpoints** | **Enrollment Codes** and select the **Add** button:



6. In the **Generate Bulk Enrollment Codes** window, specify an expiration date and the maximum number of endpoints that can be enrolled with the code. Best security practices do NOT recommend to configure the code without an expiration date. **COPY** the code to a Notepad, you will not have access to the code later.

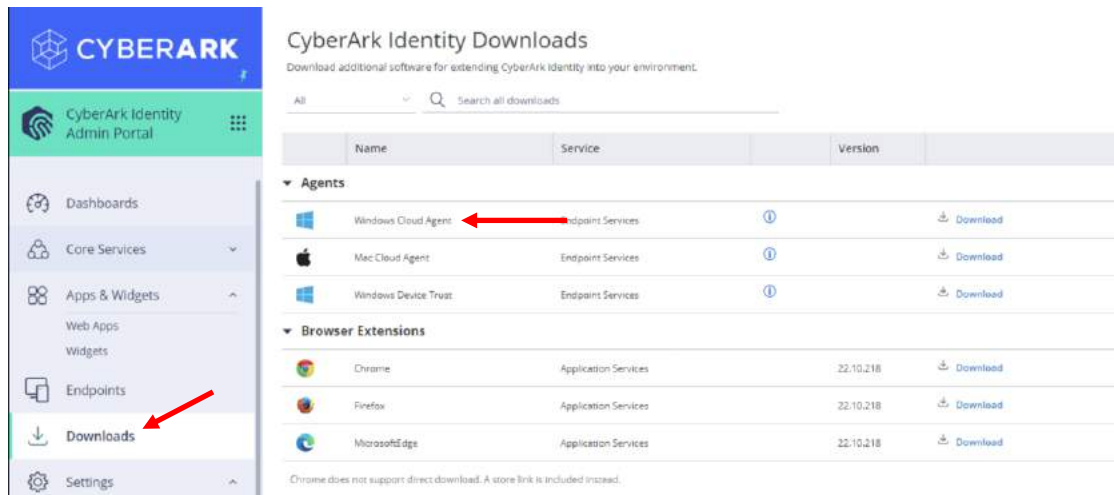
The screenshot shows the 'Generate Bulk Enrollment Codes' window. It has a 'Settings' sidebar on the left. The main area contains the following fields:

- Enrollment Code Expiration**: A dropdown menu with 'Never' and 'Specify Date' options. 'Specify Date' is selected, and a date '10/10/2022' is entered. A red arrow points to the date field.
- Max Joinable Endpoints**: A dropdown menu with 'Unlimited' and 'Specify Max' options. 'Specify Max' is selected, and the value '5' is entered. A red arrow points to the input field.
- Description**: A text input field.
- Save** and **Cancel** buttons at the bottom. A red arrow points to the 'Save' button.

CyberArk Workforce Identity

Endpoint Authentication

7. Go to the **Admin Portal** from the **CLIENT01** workstation and in the **Downloads** menu, download the **Windows Cloud Agent**:



8. Run the installer. On the **Enter Enrollment parameters** screen, specify the following options:

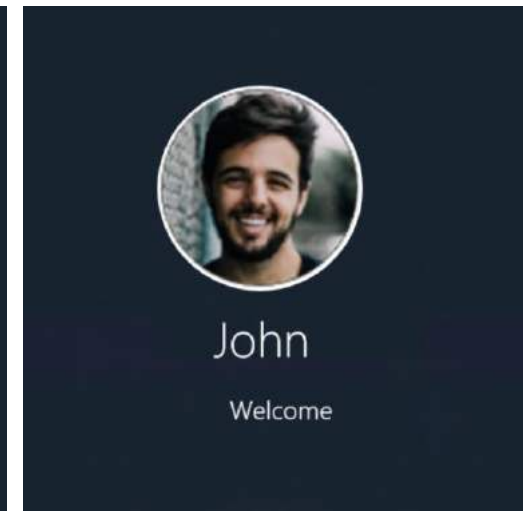
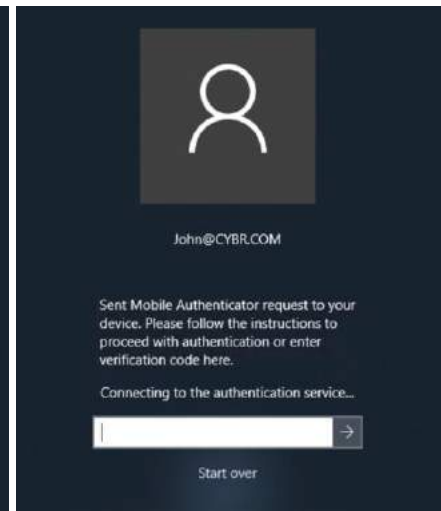
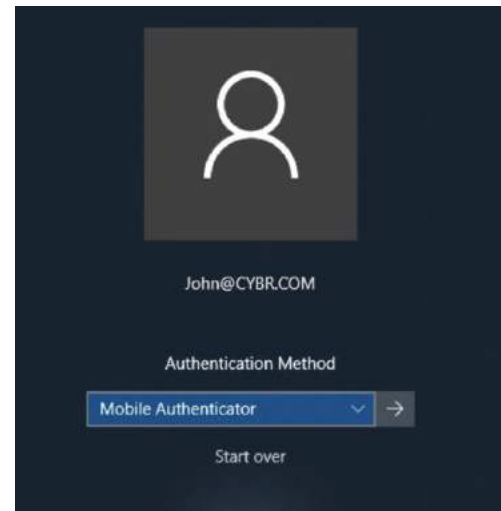
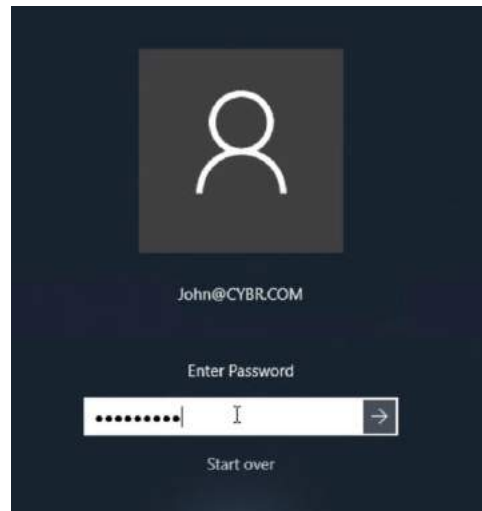
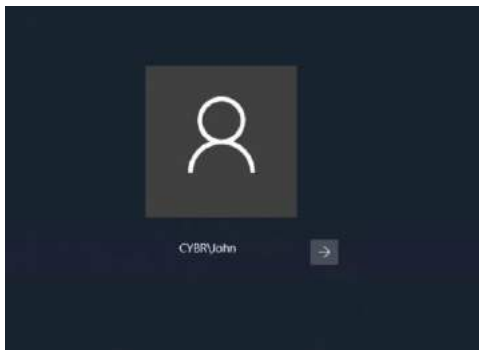
- **Tenant URL:** url of your Identity Tenant
- **Enrollment Code:** The enrollment code copied in previous steps.
- **Optional Parameters:**
 - **-l "Usuarios CYBR"** : The role that contains the users allowed to authenticate to the machine.



CyberArk Workforce Identity

Endpoint Authentication

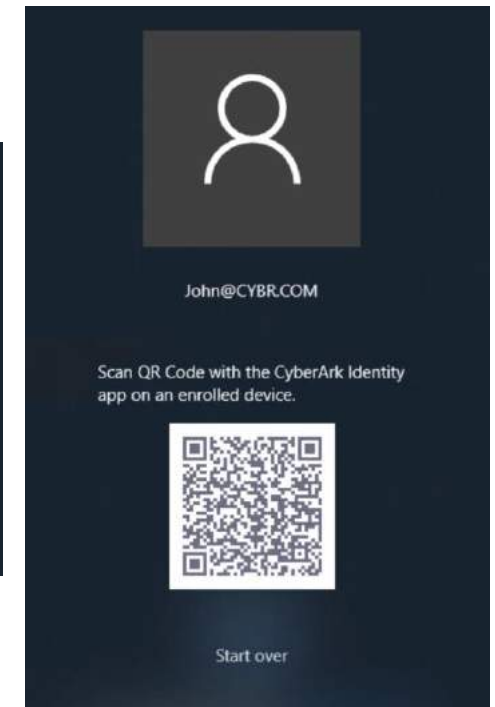
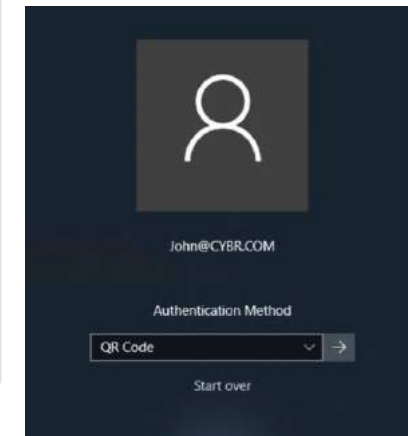
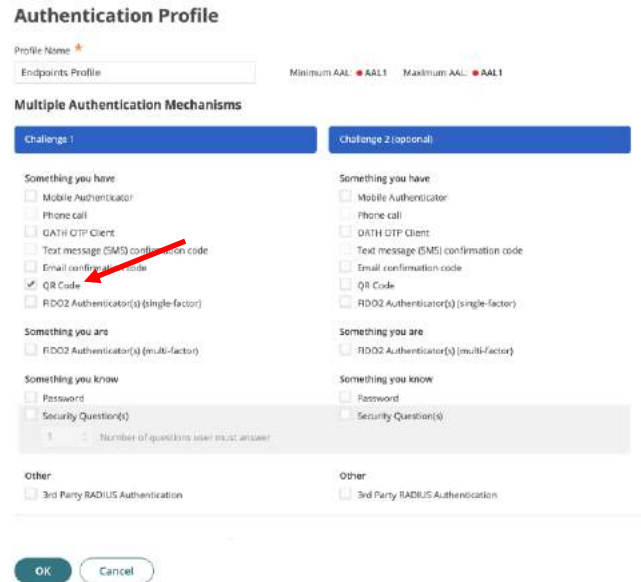
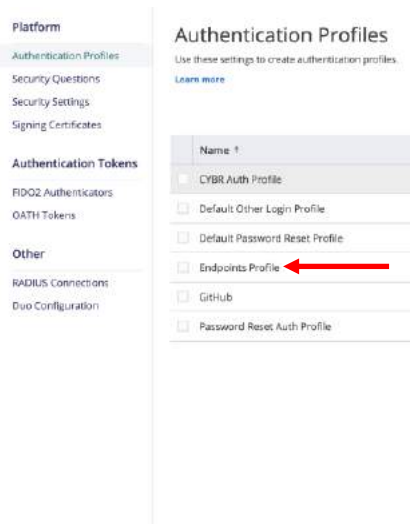
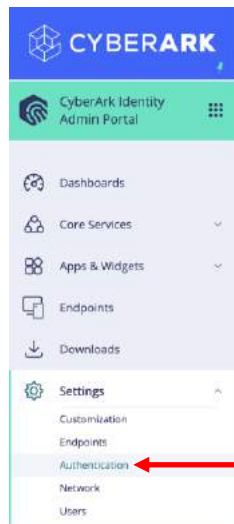
9. Restart the **CLIENT01** machine and attempt to authenticate with the user **CYBR\John**, following the authentication flow and selecting the **Mobile Authenticator** option as a second challenge.



CyberArk Workforce Identity

Endpoint Authentication

10. Now modify the authentication mechanism for the Endpoints and enable **QR Code** as the first and only challenge (Passwordless Authentication). Then restart the machine again and try to authenticate with the user **CYBR\John**.



CyberArk Workforce Identity

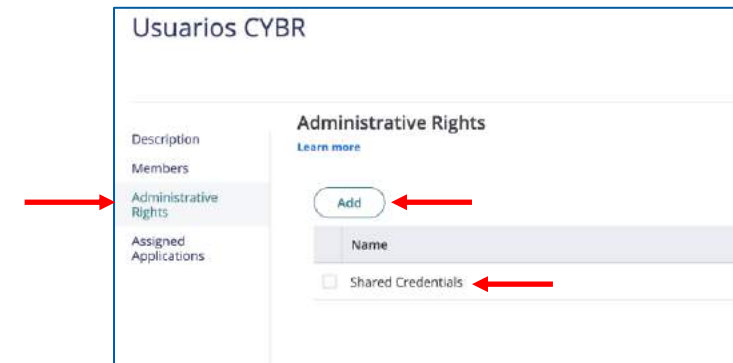
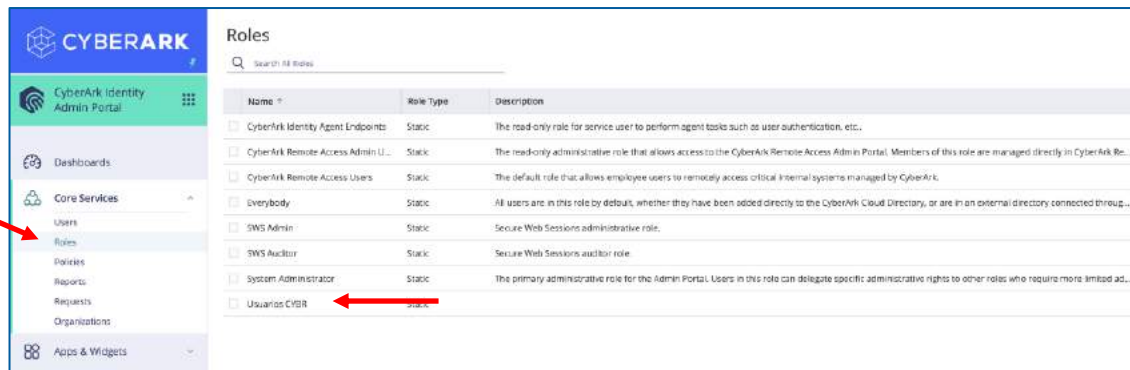
Secured Items

With CyberArk Workforce Password Management, we can allow our users to store personal confidential information on their **User Portal**, and also allow them to share those secure items with other users. CyberArk Identity stores:

- **Passwords**: Non-web application/service credentials
- **Secured Notes**: Credentials or secrets for use cases other than application access. For example: licenses, Access tokens, encryption keys, security questions, among others.

1. We will first hand over the right to share secure items to our users in the CYBR domain. For this, in the **Admin Portal**, go to the **Core Services** menu | **Roles** and edit the **CYBR Users** role:

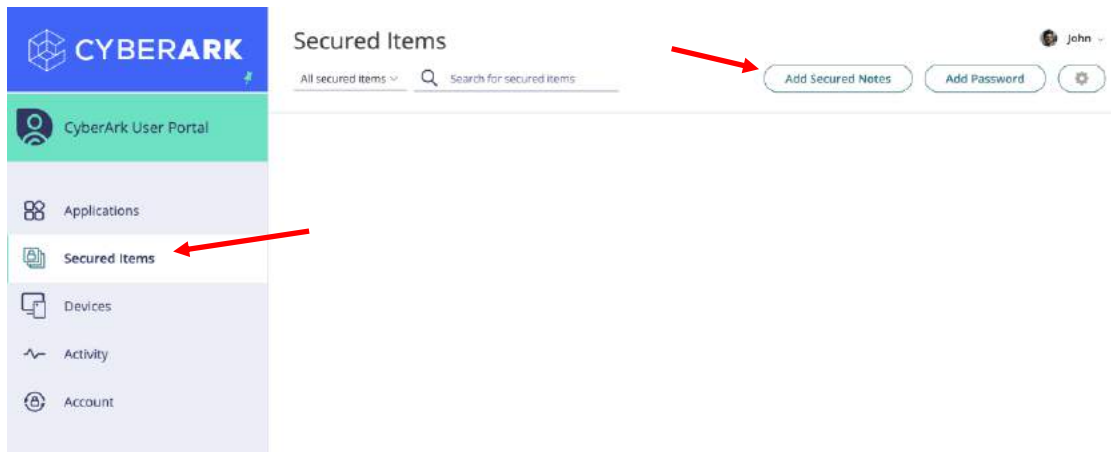
2. Go to the **Administrative Rights** menu and add the **shared credentials** right, finally **save** your changes:



CyberArk Workforce Identity

Secured Items

1. Authenticate with User **John** in the **User Portal** and select the **Secured Items** menu. Then click **Add Secured Notes**



2. In the **Secure Notes** window, specify the requested values (Name, tag (for quick search), Notes, custom fields):

The screenshot shows the 'Secure Notes' window. It has a 'Settings' title bar and a close button. The window is divided into two tabs: 'General' (selected) and 'Sharing'. Under the 'General' tab, there are three fields: 'Name' (labeled 'Llave Licencia Office'), 'Add Tags' (labeled 'Licencias Mic...'), and 'Notes' (labeled 'xxeds-sdvds-htrff-s332f'). At the bottom, there are 'Save' and 'Cancel' buttons.

CyberArk Workforce Identity

Secured Items

3. On the **Sharing** tab, click **Add** and add the Identity admin user. We are going to share the note with him. Save your changes.

Settings

Llave Licencia Office

Specify description for Secure Notes type...

General Sharing

Add

Name	Permissions	Start Time	End Time
<input type="checkbox"/> demouser@kbcorp.biz	View notes		

Save Cancel

Delete this item?

4. Now add a password with the **Add Password** button and fill in the corresponding options:

Settings

Password

Specify description for Password type...

General Sharing

Name RRHH App Creds

Add Tags

User name rrhuser1

Password

Add custom field

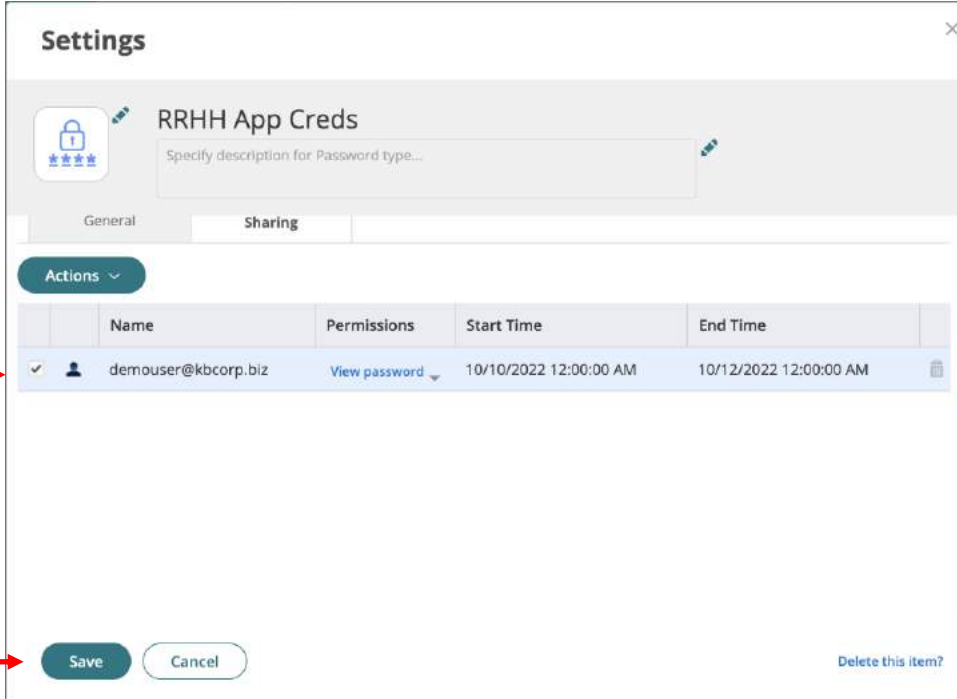
Name	Value	Hidden
------	-------	--------

Save Cancel

CyberArk Workforce Identity

Secured Items

5. On the **Sharing** tab, click **Add** and add the Identity admin user. We are going to share our password for the HR app with him. We will only allow you to view the password (not edit it) and only for a specified period of time:



The screenshot shows the 'Settings' dialog for 'RRHH App Creds'. The 'Sharing' tab is active, displaying a table of permissions. A red arrow points to the 'Add' button (a plus icon) in the top left corner of the dialog. Another red arrow points to the 'Save' button at the bottom left. The table lists a single permission for the user 'demouser@kbcorp.biz' with 'View password' permissions, valid from '10/10/2022 12:00:00 AM' to '10/12/2022 12:00:00 AM'.

	Name	Permissions	Start Time	End Time
<input checked="" type="checkbox"/>	demouser@kbcorp.biz	View password	10/10/2022 12:00:00 AM	10/12/2022 12:00:00 AM

CyberArk Workforce Identity

Secured Items

6. Do you remember that we added our personal LinkedIn account as an SSO portal app? We need to give HR staff access to our account, so we will share access to the user. In the **User Portal**, in the **Applications** menu, edit the properties of the LinkedIn app and in the **Sharing** tab add the administrative user, without being able to see the password, and specify an access period of time:

The image shows the CyberArk interface. On the left is the sidebar with the 'Applications' menu selected. The main area displays a list of applications, with the 'LinkedIn' app highlighted by a red arrow pointing to its settings icon. To the right, the 'Application Settings' dialog for LinkedIn is open. A red arrow points to the 'Sharing' tab, and another red arrow points to the 'Save' button at the bottom. The 'Sharing' tab shows a table with user access details.

	Name	Password Permis...	Start Time	End Time	
✓	demouser@kbcorp.biz	None	10/09/2022 12:00:00 AM	10/10/2022 12:00:00 AM	

CyberArk Workforce Identity

Secured Items

7. Now authenticate to the **User Portal** with the administrative user. Note that we have the LinkedIn application published in our profile. Review the properties of the application and then execute it. Finally enter the **Secured Items** menu and check if the shared items are listed.

The image displays three screenshots from the CyberArk Workforce Identity interface, illustrating the steps to verify the LinkedIn application and its secured items.

Left Screenshot: Applications List
The CyberArk User Portal sidebar is visible on the left. The main content area shows the "Applications" section. A red arrow points to the LinkedIn application icon in the list.

Middle Screenshot: Application Settings
The "Application Settings" modal for the LinkedIn application is shown. A red arrow points to the "Until" date field, which is set to "10/10/2022 12:00:00 AM". The URL field contains "https://www.linkedin.com/uas/login?goback=&trk...".

Right Screenshot: User Portal Profile
The CyberArk User Portal profile page is shown. The profile owner is Karsten Brandes, Lead Channel Solutions Engineer at CyberArk. The "Secured Items" menu item is highlighted in the sidebar. The main content area shows the "Secured Items" section, which lists "Llave Licencia Office".