



CYBERARK IDENTITY

(Adaptive Single Sign-On)

CYBERARK IDENTITY - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Beyond Identity

Website: <https://www.beyondidentity.com/>

Name of Product: Secure Work

Version: v1

Date: February 24, 2022

PARTNER SOLUTION OVERVIEW

Beyond Identity

Beyond Identity is fundamentally changing how the world logs in with a groundbreaking invisible, un-phishable MFA platform that provides the most secure and frictionless authentication on the planet. We stop ransomware and account takeover attacks in their tracks and dramatically improve the user experience.

Beyond Identity's state-of-the-art platform eliminates passwords and other phishable factors, enabling organizations to confidently validate users' identities. The solution ensures users log in from authorized devices, and that the device meets the security policy requirements during login and continuously after that. Our revolutionary approach empowers zero trust by cryptographically binding the user's identity to their device and analyzing hundreds of risk signals on an ongoing basis. The company's advanced risk policy engine enables organizations to implement foundationally secure authentication and utilize risk signals for protection, rather than just for detection and response.

Beyond Identity and CyberArk

Beyond Identity and CyberArk partner to provide the strongest level of authentication possible by enabling CyberArk Single Sign-On customers to leverage Beyond Identity's passwordless authentication and continuous risk-based authorization integrated seamlessly into CyberArk Single Sign-On.

Beyond Identity integrates seamlessly into CyberArk Single Sign-On via OIDC, providing strong integration without any disruption to your CyberArk identity infrastructure. Beyond Identity is a cloud-native solution that requires only a few minor configuration settings within CyberArk, and does not require any coding. To get started, simply configure Beyond Identity as a delegated identity provider in your CyberArk SSO environment.

When an end-user requests access to an enterprise application, the application calls CyberArk SSO, which subsequently redirects to Beyond Identity as a delegated identity provider.

Beyond Identity acts as a true platform authenticator, issuing public keys from the Beyond Identity cloud service in order to validate identity and device. Additionally, Beyond Identity authenticator captures device security posture in order to make policy-based authentication decisions, which then get sent back to CyberArk as a JWT to allow or deny authentication. This enables CyberArk Single Sign-On customers to add additional risk signals to be analyzed regarding the security posture of the device at the point of authentication.

Version: v1

Platform components:

- Beyond Identity Admin Console
- Beyond Identity User Console with SCIM provisioning
- Beyond Identity as the external identity provider

KEY BENEFITS

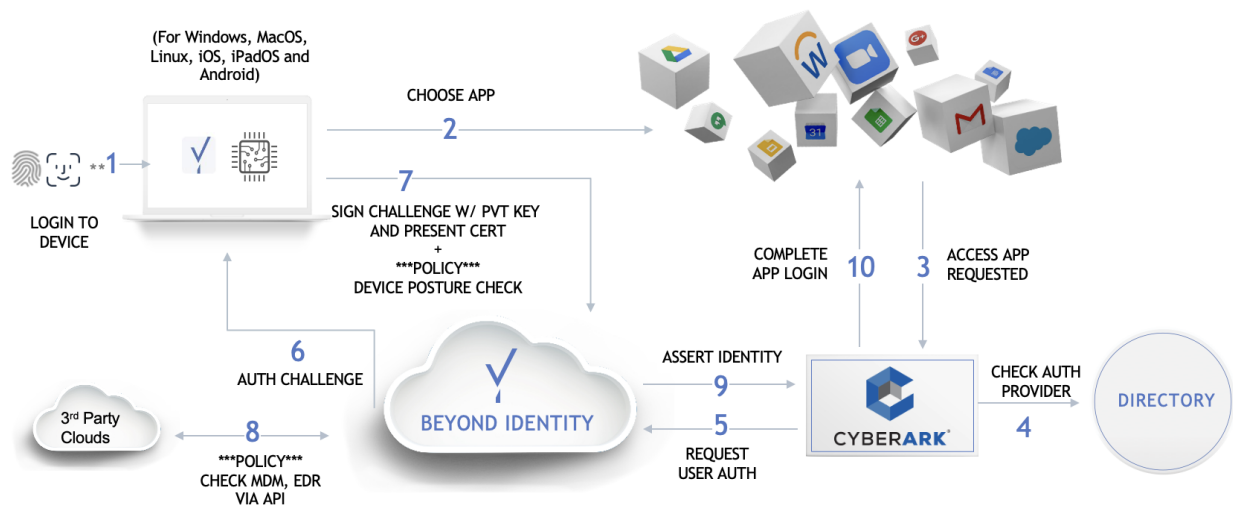
Benefits of Beyond Identity Secure Work:

- **No More Password Liabilities:** Replace passwords with the same proven and scalable cryptography that you trust to protect online transactions every day and remove the most significant threat to digital security, obviating password use across your organization.
- **MFA Users Love:** Implement the AAL3 MFA and a streamlined authentication experience that does not require users to pick up a second device or type in a one-time code at each authentication event.
- **Ensure Compliance:** Enforce and prove compliance to regulations by capturing immutable records of device security metadata at the exact time of authentication for every user and every device requesting access to your resources.
- **Tie Identity to Device:** Always know the person and device requesting access with identity bound to devices using private keys created and stored in the device's Trusted Platform Module (TPM).

Benefits of integrating Beyond Identity Secure Work with CyberArk AAM:

- **Trust Your Endpoints:** Verify device trustworthiness of managed and unmanaged devices across operating platforms and inform granular level policies that protect your resources from unauthorized access by unsecured devices.
- **Continuous Risk-Based Access Controls:** Employ rule-based access via customizable policies and constantly evaluate the risk and trustworthiness of each user and the device requesting access to your SaaS resources.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



CYBERARK IDENTITY INTEGRATION

Beyond Identity acts as a delegate identity provider within the authentication flow for CyberArk SSO, integrating via OIDC protocol. In this way when an end-user requests access to an enterprise application, the application calls to CyberArk SSO, which subsequently redirects to Beyond Identity (Steps 2-5).

In order to authenticate a user, Beyond Identity issues a challenge to the requesting device's authenticator (Step 6). The authenticator then signs the challenge with the corresponding private key, which is stored on the TPM. Because the authenticator exists on the device, additional device security

posture information can be included in the response packet, which allows for fine-grained device authentication policies to be written (Step 7). These policies can be augmented by additional API calls to 3P endpoint security products' clouds- such as MDM and EDR software- to ensure the security software is registered and active on the device (Step 8). Finally, once the challenge is correctly signed by the private key, and the authenticating device passes all policy checks, Beyond Identity cloud asserts the identity to CyberArk SSO as a JWT to allow or deny authentication (Step 9).

REQUIREMENTS

- Windows 10, MacOS, Android, iOS, and Linux (Ubuntu and CentOS)

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

INTRODUCTION

This guide provides information on how to:

- Set up Beyond Identity as a passwordless authentication solution for your CyberArk SSO (Idaptive) environment.
- Set up CyberArk SSO (Idaptive) to use Beyond Identity as an Identity IDP to federate authentication.
- Set up CyberArk SSO (Idaptive) as the source of truth for user identities.
 - o Users will be created in CyberArk SSO (Idaptive) and as part of application provisioning SCIM provisioned to Beyond Identity tenant

PREREQUISITES

Ensure that you have a CyberArk Identity SSO account with system admin privileges to:

- Create/Modify/Delete users in CyberArk Identity tenant.
- Create/Configure tenant.
- Create/Configure OpenID Connect Web applications.
- Create/Configure Federation Partner.

BEYOND IDENTITY CONFIGURATION

Information to provide to the Beyond Identity Field Team:

Your Company Name	
Your CyberArk Identity tenant URL e.g., <a href="https://<customer_id>.my.idaptive.app/">https://<customer_id>.my.idaptive.app/	
Beyond Identity Admin Portal Application credentials	

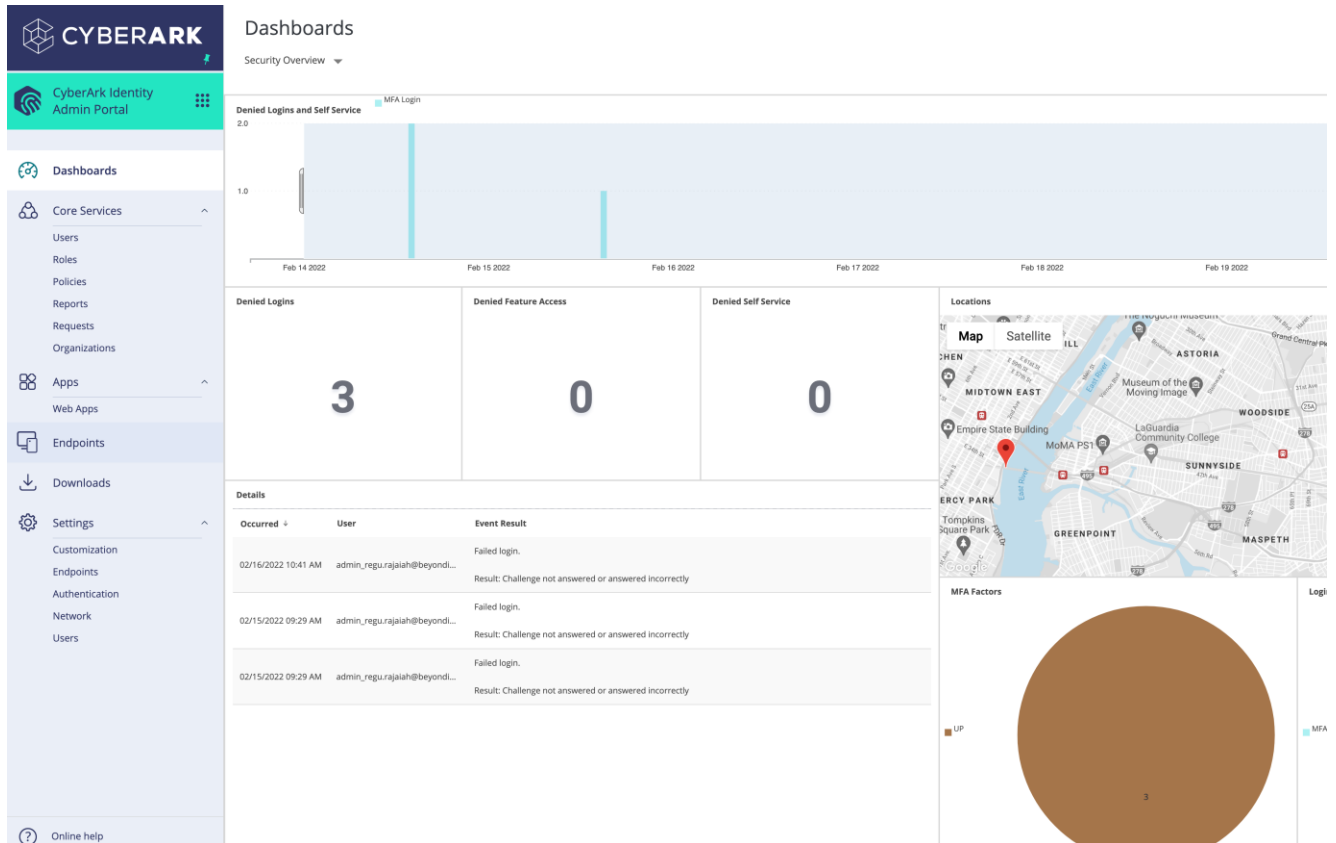
SSO Client Id	
SSO Client Secret	
Beyond Identity User Portal Application credentials	
SSO Client Id	<i>This will be updated by customer directly in Beyond Identity Admin UI.</i>
SSO Client Secret	
(Optional) A logo for your corporation	
Logo requirements:	
- 300 x 150 pixels or less - File size of 10kb or less - File types accepted: SVG, PNG, JPG, or GIF	

Information you will receive from the Beyond Identity Field Team

Beyond Identity IdP endpoint URLs:	
Issuer	https://auth.byndid.com/v2
Authorization endpoint	https://auth.byndid.com/v2/authorize
Token endpoint	https://auth.byndid.com/v2/token
JWKS endpoint	https://auth.byndid.com/v2/.well-known/jwks.json
Client ID	[From Beyond Identity Console]
Client Secret	[From Beyond Identity Console]
Tenant API Bearer Token for SCIM	[From Beyond Identity SE]
Beyond Identity Org ID	[From Beyond Identity SE]
SCIM API endpoint	https://api.byndid.com/scim/v2/Users https://api.byndid.com/scim/v2/Groups

Step 1: Sign in as an administrator to CyberArk Identity tenant

Sign into your tenant with the admin identity and password. The admin portal looks as below:

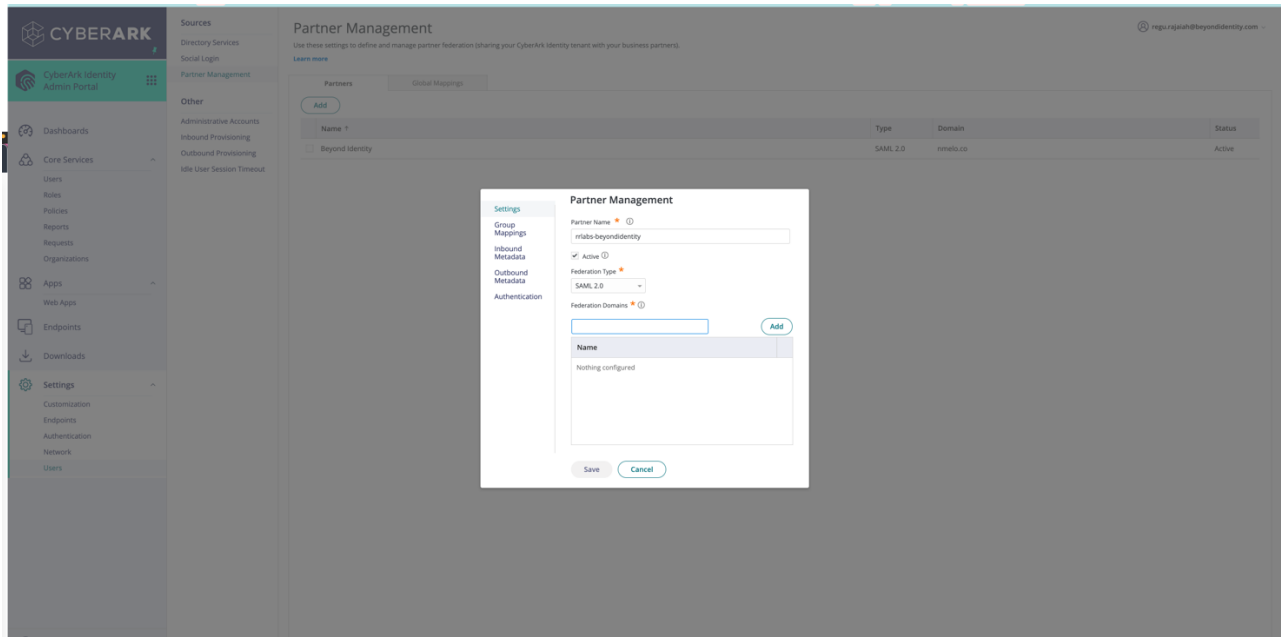


Step 2: Create and Configure a partner

Business Partner Federation establishes a trust relationship between the Service Provider (SP) and Identity Provider (IDP) using SAML tokens.

To add a partner:

Navigate to Settings=>Users=>Partner Management=>Add.



Set up the partner with the following settings:

Settings panel

- Partner Name: Beyond Identity
- Federation Type: SAML 2.0
- Federation Domain: <your_domain> e.g acme.com

Group Mappings panel

- Leave as default

Inbound Metadata panel

- Before filling this panel, set up in BI Admin Console a SAML connection that looks like the below
 - SP Single Sign on URL: your Idaptive tenant,
https://<customer_id>.my.idaptive.app/my
 - SP Audience URI: CN=Idaptive:Customer:<customer_id>
 - <customer_id> is your Idaptive customer ID
 - Attribute Statements (optional)
 - UserPrincipalname, value:{{ExternalId}}
 - EmailAddress, value:{{Email}}
 - DisplayName, value:{{UserName}}

Edit SAML Connection

Import SP Metadata File (optional) No file selected

ID

Name

SP Single Sign On URL

SP Audience URI

Name ID Format

Subject User Attribute

Request Binding

Signed Response ☒ SIGNED ☐ Unsigned

X509 Signing Certificate (optional) 1 file selected
Valid Certificate Expires Fri Dec 31 2038

Attribute Statements (optional)

Name	Name format	Value	Remove
UserPrincipalName	unspecified	(ExternalId)	Remove
EmailAddress	unspecified	(Email)	Remove
DisplayName	unspecified	(UserName)	Remove

[+ Add](#) [Delete This Connection](#) [Cancel](#) [Save Changes](#)

- Download this metadata from BI Admin Console

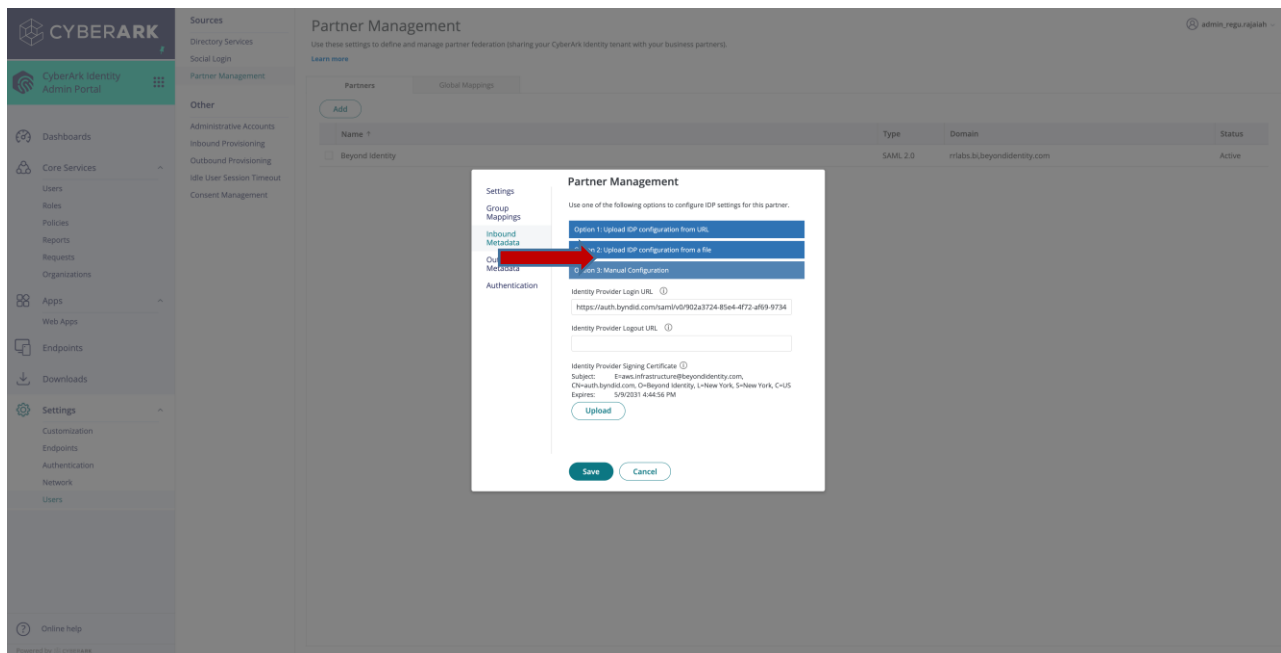
Integrations

OIDC **SAML** ENDPOINT MANAGEMENT OKTA

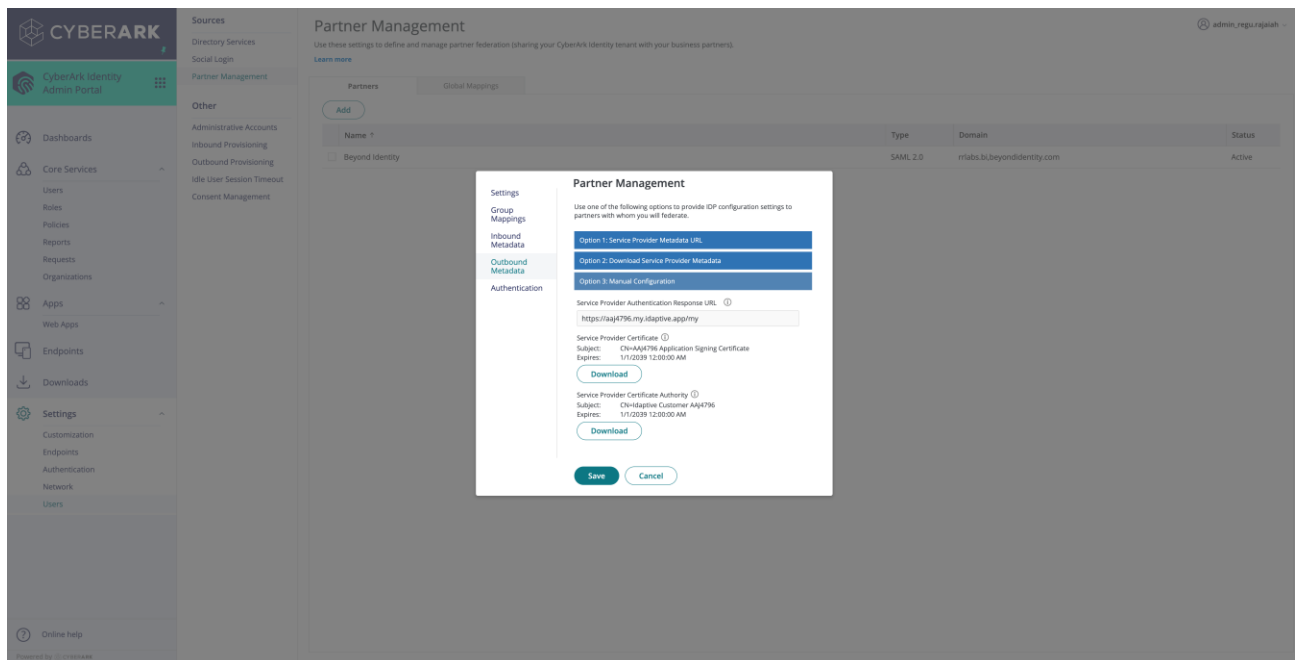
SAML Connections

Connection Name	IDP ID	IDP SSO URL	IDP Issuer	Actions
rnlabs-identity-asaj4796-saml-federation	902a3724-85e...	https://auth.by...	https://auth.by...	Download Metadata

- Import this metadata using “Option 2: Upload IDP configuration from a file”



Outbound Metadata panel



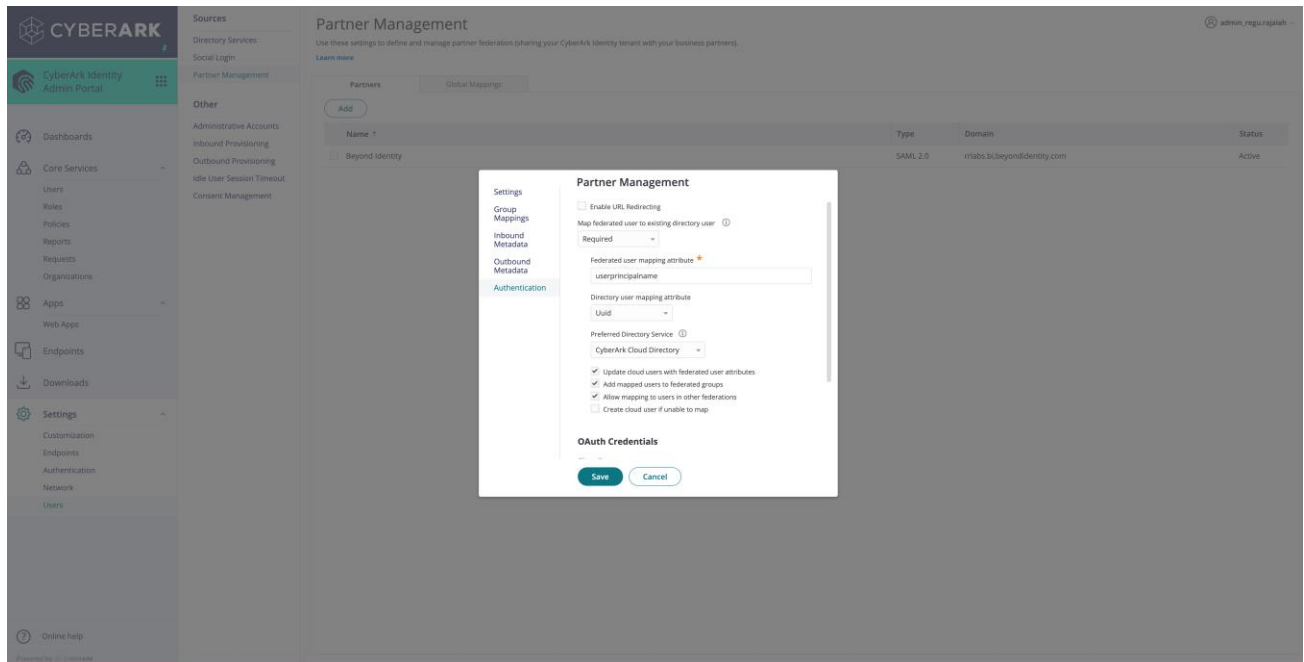
Authentication panel

Map federated user to existing directory user: Required

Federated user mapping attribute: userprincipalname

Directory user mapping attribute: Uuid

Preferred Directory Service: CyberArk Cloud Directory



Step 3: Create roles for BI Admin Console and BI User Console in CyberArk Identity

CyberArk Identity provisions users per application. The applications are mapped to roles and users are added to the roles. Idaptive do not recommend a user added to more than one role.

Navigate to Core Services=>Roles and click “Add Role” to create roles.

CYBERARK
CyberArk Identity Admin Portal

Roles

Search All Roles

admin_regu.rajiah Add Role

Name	Role Type	Description	Organization
Clam Ninjas	Static		
CyberArk Remote Access ...	Static	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Members of this role are managed directly in CyberArk Remote Access and synced to enable single sign on acc...	
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 are in an external directory connected through a CyberArk Identity Connector.	
rr_test_dynamic_role	Dynamic	rrlabs testing	
Run_BI_Admin_Console	Static	Members of this role can run BI admin console	
Run_BI_User_Console	Static	Role used in BI user console app provisioning	
scim_task_admins	Static		
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 rights to other roles who require more limited administrative access.	

Online help
Powered by CYBERARK

Create Run_BI_Admin_Console and Run_BI_User_Console roles for BI Admin Console and BI User Console applications respectively.

Use the Members panel=>Add button to add users to the role. Use “Assigned Applications” panel=>Add button to assign applications to the role. For the Run_BI_Admin_Console role, the assigned application is “Beyond Identity Admin Console”

CYBERARK
CyberArk Identity Admin Portal

Run_BI_Admin_Console

Members of this role can run BI admin console

Assigned Applications

Assign existing applications to this role.

Add

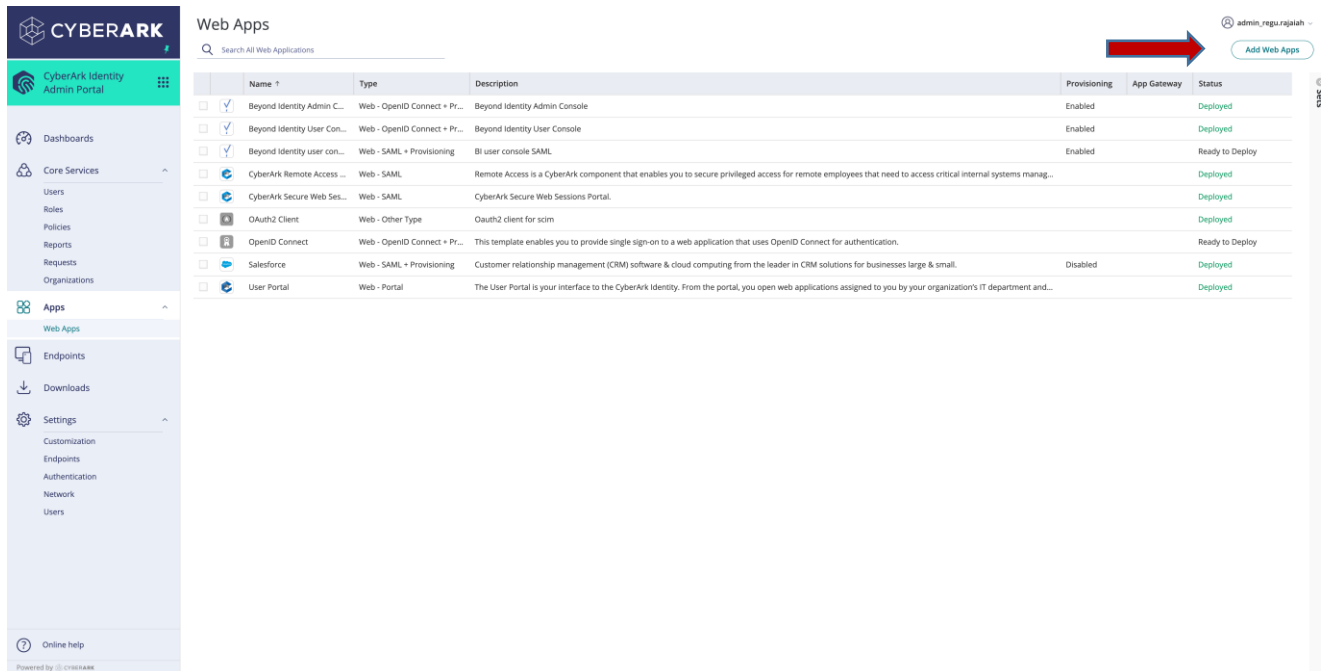
Name	Type	Description
Beyond Identity Admin Console	Web - OpenID Connect + Prov...	Beyond Identity Admin Console

Save Cancel

Online help
Powered by CYBERARK

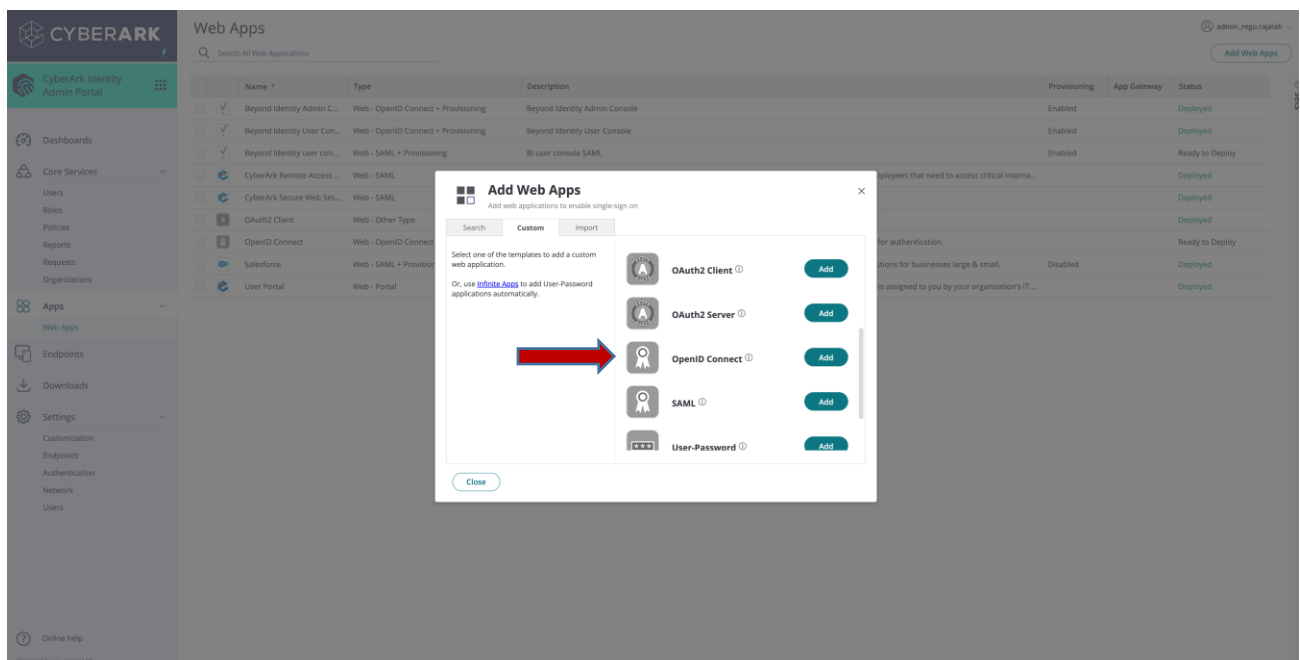
Step 4: Setup Beyond Identity Admin Application in CyberArk Identity

Sign in as administrator and Navigate to Settings=>Web Apps=>Add Web Apps.



The screenshot shows the CyberArk Identity Admin Portal interface. On the left is a sidebar with navigation options: Dashboards, Core Services (Users, Roles, Policies, Reports, Requests, Organizations), Apps (Web Apps, Endpoints, Downloads), Settings (Customization, Endpoints, Authentication, Network, Users), and Online help. The main area is titled 'Web Apps' and contains a table of existing web applications. A red arrow points from the top right of the page to the 'Add Web Apps' button.

	Name ↑	Type	Description	Provisioning	App Gateway	Status
☐	Beyond Identity Admin C...	Web - OpenID Connect + Pr...	Beyond Identity Admin Console	Enabled		Deployed
☐	Beyond Identity User Con...	Web - OpenID Connect + Pr...	Beyond Identity User Console	Enabled		Deployed
☐	Beyond Identity user con...	Web - SAML + Provisioning	BI user console SAML	Enabled		Ready to Deploy
☐	CyberArk Remote Access ...	Web - SAML	Remote Access is a CyberArk component that enables you to secure privileged access for remote employees that need to access critical internal systems manag...			Deployed
☐	CyberArk Secure Web Ses...	Web - SAML	CyberArk Secure Web Sessions Portal.			Deployed
☐	OAuth2 Client	Web - Other Type	OAuth2 client for scim			Deployed
☐	OpenID Connect	Web - OpenID Connect + Pr...	This template enables you to provide single sign-on to a web application that uses OpenID Connect for authentication.			Ready to Deploy
☐	Salesforce	Web - SAML + Provisioning	Customer relationship management (CRM) software & cloud computing from the leader in CRM solutions for businesses large & small.	Disabled		Deployed
☐	User Portal	Web - Portal	The User Portal is your interface to the CyberArk Identity. From the portal, you open web applications assigned to you by your organization's IT department and...			Deployed



The screenshot shows the 'Add Web Apps' dialog box open over the Web Apps list. The dialog has tabs for 'Search', 'Custom', and 'Import'. It prompts the user to 'Select one of the templates to add a custom web application.' or to 'use [Inline Apps](#) to add User-Password applications automatically.' A red arrow points to the 'OpenID Connect' option in the list of templates.

Name ↑	Type	Description	Provisioning	App Gateway	Status
☐	Beyond Identity Admin C...	Web - OpenID Connect + Provisioning	Enabled		Deployed
☐	Beyond Identity User Con...	Web - OpenID Connect + Provisioning	Enabled		Deployed
☐	Beyond Identity user con...	Web - SAML + Provisioning	Enabled		Ready to Deploy
☐	CyberArk Remote Access ...	Web - SAML			Deployed
☐	CyberArk Secure Web Ses...	Web - SAML			Deployed
☐	OAuth2 Client	Web - Other Type			Deployed
☐	OpenID Connect	Web - OpenID Connect			Ready to Deploy
☐	Salesforce	Web - SAML + Provisioning	Disabled		Deployed
☐	User Portal	Web - Portal			Deployed

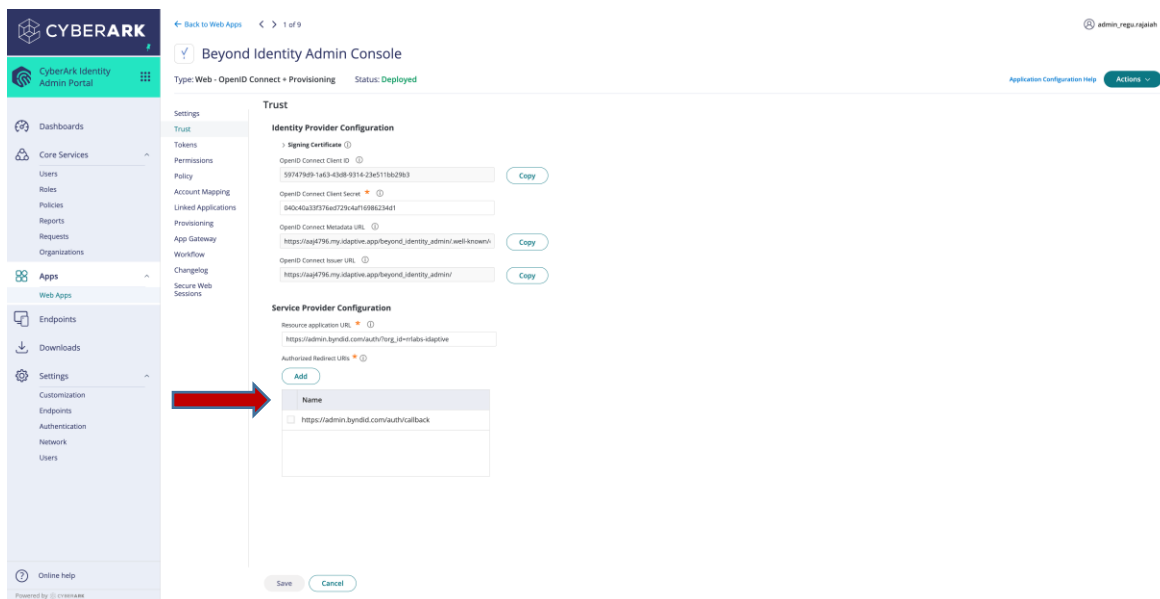
Choose “custom” and “OpenId connect” Click Add

Settings panel

- Under Logo, click browser to upload Beyond Identity logo

Trust panel

- IDP configuration
 - o Copy the client ID. You need this in setting up Admin Console SSO in BI.
 - o OpenID connect client secret: Enter a secret value, you can generate your own. Copy the client secret, you need this in setting up Admin Console SSO in BI.
- Service Provider configuration
 - o Resource application URL: BI Admin Console URL for example https://admin.byndid.com/auth/?org_id=rrlabs-idaptive
- Click Add under “Authorized redirect URL” and enter <https://admin.byndid.com/auth/callback>



Tokens panel

- Under custom logic script, add “setClaim(“idaptiveextid”,LoginUser.Uuid);”

Policy panel, Account mapping panel, App Gateway panel, Linked applications panel, Workflow panel and secure Web sessions panel

- Leave as defaults

Provisioning panel

- Check Enable provisioning for this application
 - o Select Live Mode
- SCIM service url: <https://api.byndid.com/scim>
- Authorization Type:
 - o Select Authorization header
 - o Header type: Bearer Token
 - o Bearer Token: Get this token from BI SME

- Click verify. This should connect to SCIM endpoint and gather configuration information to populate sync and deprovisioning options
- Role Mappings: Click “Add” and add Run_BI_Admin_Console role
- Expand the “Provisioning script” and the below script

```

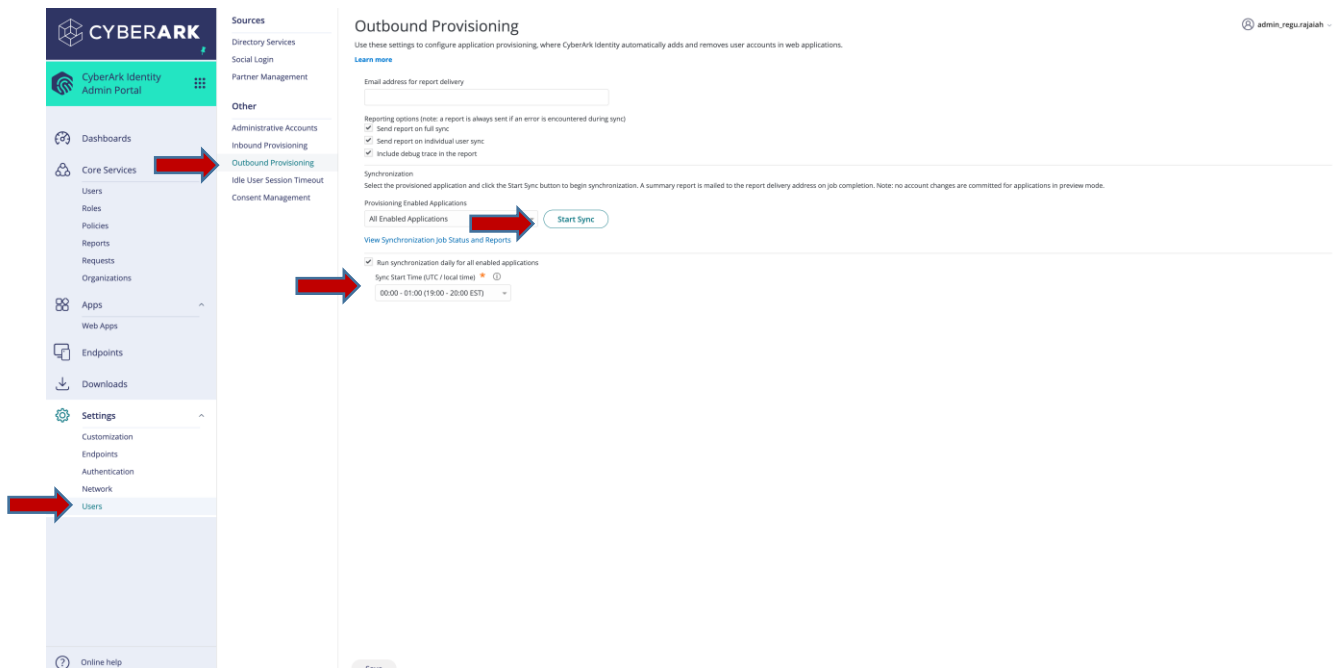
if (source.Classification == 'User') {
    var nameBits = source.DisplayName.split(' ');
    destination.active = source.Status;
destination.externalId = source.Uuid;

    destination.userName = source.Email;
    destination.displayName = source.DisplayName;
    destination.name = {
        'familyName': nameBits[nameBits.length - 1],
        'givenName': nameBits[0]
    };
    destination.emails = [{
        'type': 'work',
        'value': source.Email
    }];
}

if (source.Classification == 'Group') {
    var propArr = getSourcePropertyByName('name');
    if (propArr && propArr.Length) {
        destination.displayName = propArr[0];
    }
    destination.members = GetMemberList();
    // destination.id = "";
}

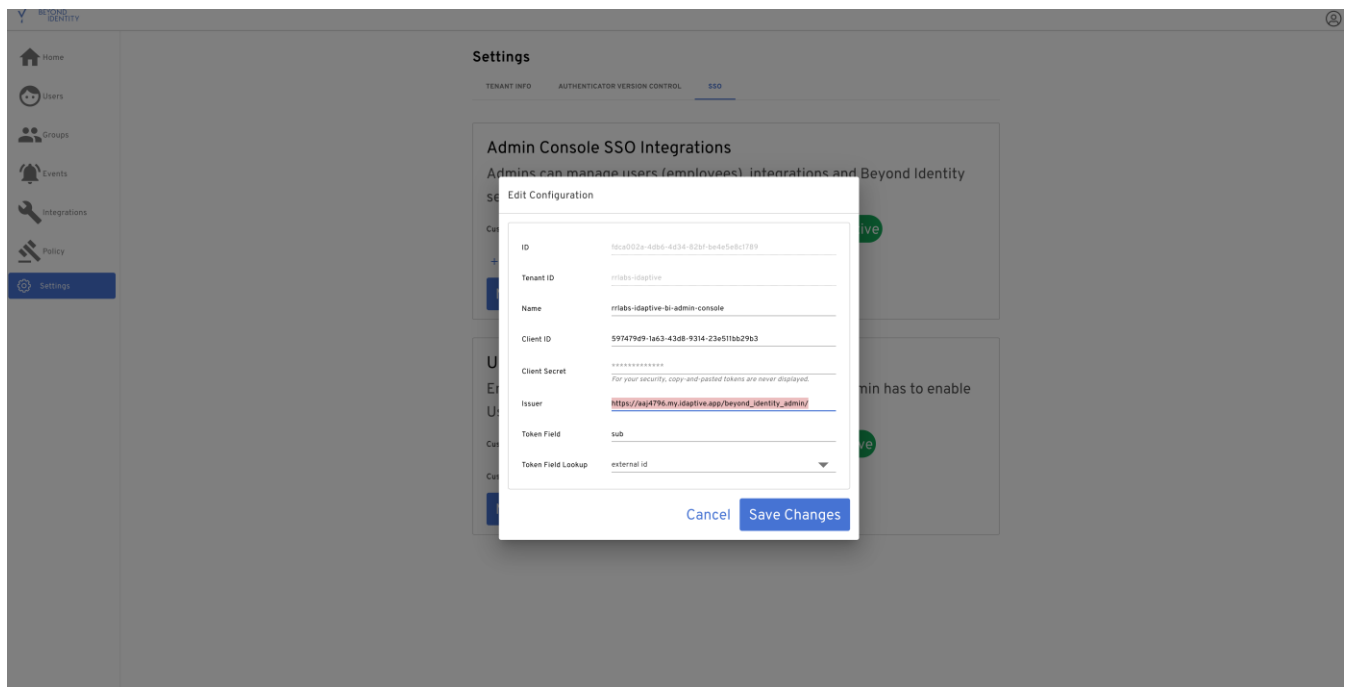
```

- On demand application provisioning, can be triggered by navigating to Settings=>Users=>Other=>Outbound provisioning. Under “Provisioning enabled applications”, choose “All enabled applications” or a specific application. Click “Start Sync” button.
- You can also schedule synchronization daily for all enabled applications by specifying a start sync time.



Step 5: Setup Beyond Identity Admin Console SSO in BI

1. Provide "Client ID" and "Client Secret" assigned to Admin console setup in Step 5, under Trust panel configuration to Beyond Identity SE. The Beyond Identity team will collect and configure this value.
2. Beyond Identity Field Team: Please configure following fields through Beyond Identity Support Console while updating Admin Console Configuration.
 - a. Name: rrlabs-idaptive-bi-admin-console
 - b. Client ID: <Use the value recorded in Step 5>
 - c. Client Secret: <Use the value recorded in Step 5>
 - d. Issuer: https://<customer_id>.my.idaptive.app/beyond_identity_admin/
 - e. Token Field: sub
 - f. Token Field Lookup: external_id
3. After these values are provisioned, customer should login and confirm that admin has access to Beyond Identity Console.



Step 6: Setup Beyond Identity User Console Application in CyberArk Identity

This is similar to setting up beyond identity Admin Console. The differences in this configuration are:

- Application name: Beyond Identity User Console
- Role Mapping: Run_BI_User_Console
- Different client ID and secret. Note these down for later use in BI User Console
- Resource Application URL
 - o https://user.byndid.com/auth-user/?org_id=rrlabs-idaptive
- Authorized Redirect URIs: <https://user.byndid.com/auth-user/callback>

Step 7: Setup Beyond Identity User Console SSO in BI

1. Once logged into Beyond Identity Admin UI, click on Settings -> SSO -> User Console SSO Integration and click on Edit.
2. Please configure the following fields for User Console SSO Integration.
 - a. Name: rrlabs-idaptive-bi-user-console
 - b. Client ID: <Use the value recorded in step 7>
 - c. Client Secret: Use the value recorded in step 7>
 - d. Issuer: https://<customer_id>.my.idaptive.app/beyond_identity_user_console/
 - e. Token Field: idaptiveextid
 - f. Token Field Lookup: external_id
3. Click on Save Changes.

SETTING UP TEST USERS

User Enrollment

1. To enroll a user in the Beyond Identity experience
 - a. Create a user using Idaptive admin console
 - b. Add the user to Run_BI_User_console role for assigning BI User Console or add to Run_BI_Admin_Console for assigning BI Admin Console.
 - c. The application provisioning should provision the user to BI tenant
 - d. Provisioned users will get an enrollment mail from BI
2. Enrolled users will receive an email from Beyond Identity welcoming them to the new Identity Provider.
 - a. See image below for reference



Your organization is using Beyond Identity, a new sign-in experience for you to securely sign into your corporate applications without passwords. Follow the steps below to get started.

Step 1: Get Authenticator

Download and install the Beyond Identity Authenticator for your device. Go to Step 2 if this device already has the Authenticator installed.

[View Download Options](#)

Step 2: Register credential

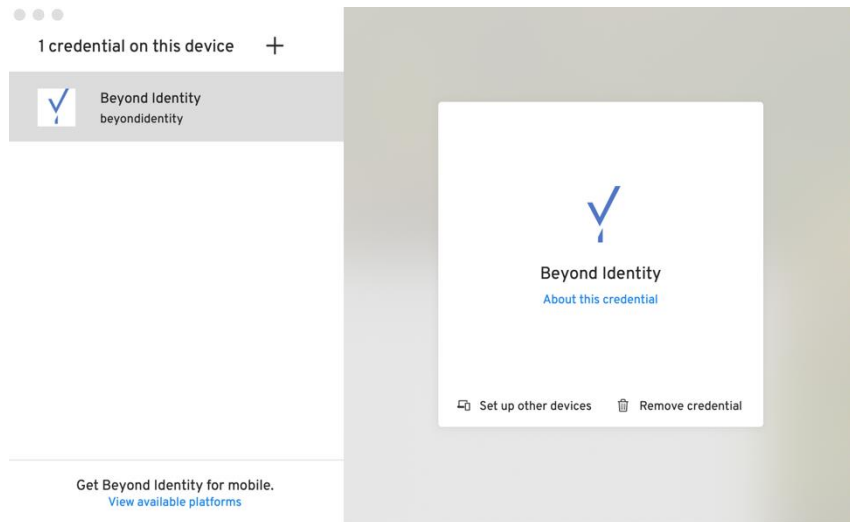
Use the link below to register your new credential to this device. Don't wait long - **this link expires in 7 days.**

[Register New Credential](#)

Once registered, your credential can be set up on other devices with the Authenticator installed.

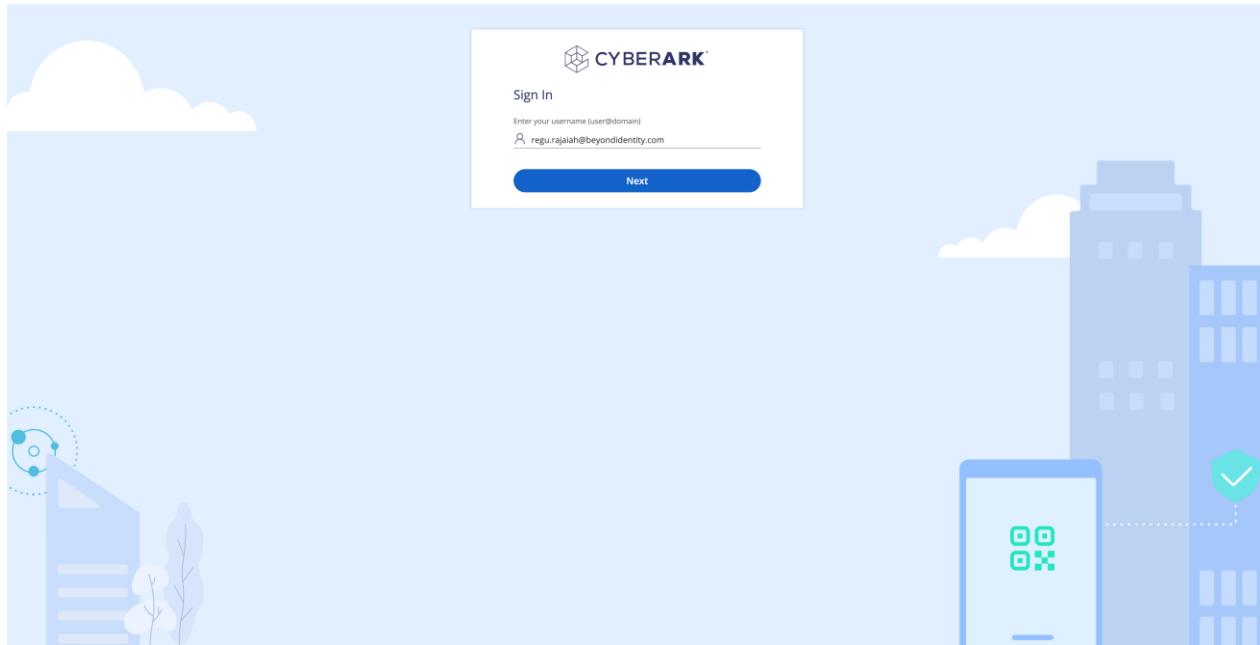
3. Each enrolled user will be asked to follow the two steps below:
 - a. Step 1: Download the Beyond Identity Authenticator to their device.
 - i. When the user clicks "View Download Options", the Beyond Identity Authenticator downloads page will open in a browser with all supported platforms displayed. The user should download and install the Beyond Identity Authenticator on their device if they have not already.
 - ii. Now that the user has the Authenticator installed on their device, they should proceed to Step 2 as there is not, yet a user credential associated with the Authenticator on that device.
 - b. Step 2: Register their Credential in the Beyond Identity IdP.

- i. By clicking on Step 2 “Register New Credential”, the user’s credential will get enrolled in the Beyond Identity service on the back end. On the front end, users who click Step 2 will be taken to the Beyond Identity Authenticator where they will see the progress of their credential registration. Once completed, the user will see the credentials in the Authenticator.
- ii. See example image below:

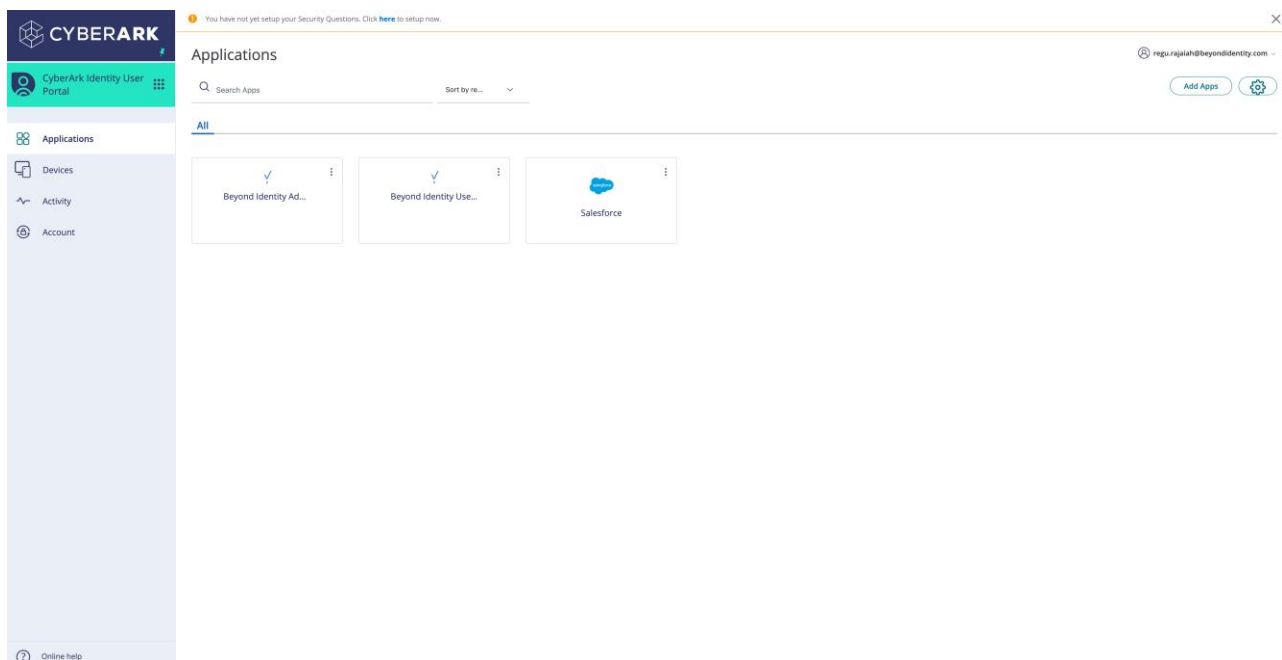


User Authentication (Signing in)

- Access Idaptive tenant URL for example, https://<customer_id>.my.idaptive.app/my
- Login with the federated user suffix, for example user@acme.com, click next



- This will trigger the passwordless experience with BI authenticator and show CyberArk Identity user portal listing the assigned applications for the user



User Deprovisioning

To deprovision a user from the Beyond Identity experience, remove the user from the appropriate role in CyberArk Identity.

PARTNER CONTACT INFO

Business Contact	Name	John Caldwell
	Email	John.caldwell@beyondidentity.com
	Tel	(212) 653-0847
Technical Contact	Name	Suresh Bhandarkar
	Email	Suresh.bhandarkar@beyondidentity.com
	Tel	(212) 653-0847
Support Contact	Name	Support
	Email	support@beyondidentity.com
	Tel	(212) 653-0847