

CODE42 INCYDR FLOWS

Products: CyberArk Identity, CyberArk Privilege Cloud, CyberArk Identity Flows and Code42.

Solution Overview:

The solution streamlines the management of identities flagged by Code42 for unauthorized access, modifications, or transfers of sensitive and critical data. By utilizing Watch List rules and risk scores, the solution enhances security by blocking access to privileged organizational resources and improving overall identity protection.

REQUIREMENTS

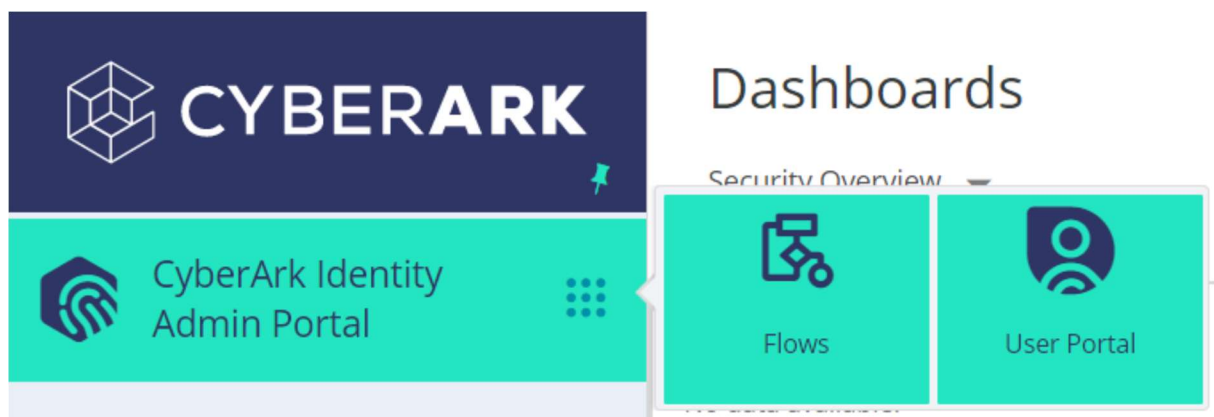
List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs.

- CyberArk Identity tenant
- CyberArk Privilege Cloud
- CyberArk Flows tenant
- Code42

FLOWS TEMPLATE INSTALLATION

The Marketplace contains four files: This integration guide and an Identity Flows 3 JSON file that includes the template for this integration. Once you have the JSON file, you can import it into your Identity Flows tenant.

Login to your CyberArk Identity tenant and Launch Flows from the waffle menu.



The CyberArk Identity Flows builder will launch in a new tab.

Flow-20230221090557

Save

Run

Export

Clone

Import

Delete

Once the Flows Builder loads, On the Action Menu at the top of the screen **Click** on the **Import** button.

Upload From Computer

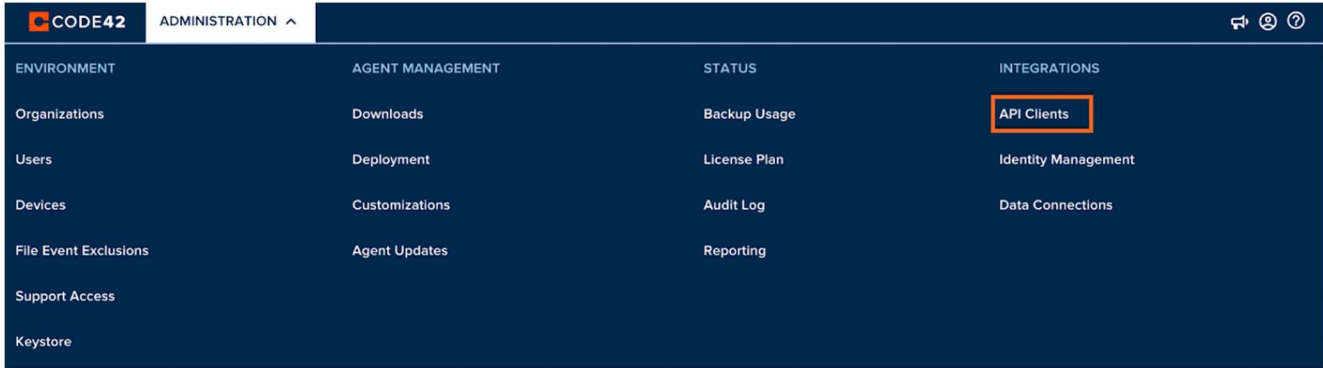
Drop or upload

The Upload dialog box will launch after Clicking the Import button. Either drag the **.Json** onto the Upload dialog or **Click the Cloud with the Up Arrow** to select the file.

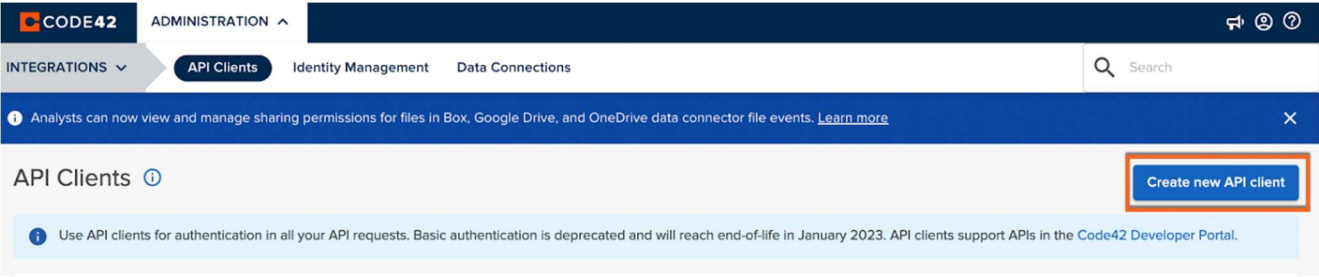
Code42 API KEY

To create the API client, follow the steps below:

1. Log in to your Code42 console.
2. Navigate to **Administration > Integrations > API Clients**.



3. Click **Create new API client**. When you click this button, the **Create new API client** pop-up window will open.



4. In the **Client name** field, enter a name for your new API client.

Create new API client

Client name

Test Integration

50 character limit

Description (optional)

250 character limit

API Permissions

API	Read	Write
Alert Rules	☐	☐
Alerts	☒	☐
Audit Log	☐	—
Cases	☐	☐
Data Preferences	☐	☐
Detection Lists	☐	☐
Device	☐	☐
File Events	☐	—

Cancel

Save

5. Select the **Read** option for all the required events(**Alerts**).
6. Click **Save** to create your new API client.
7. Copy and save the **Client ID**, **Secret**, and **Base URL** somewhere that you can easily access.

Create new API client

?

×

Copy this information to a secure place. This is the only time we'll display your secret.

Client ID

key-3a5f23c0ee-47646-4f4c2-58077-ee-44-30000774c2

Secret

88a3b1105a10f3b493c75a07d9a9f8b179a677a9b4c0ee

Base URL

https://api.us.code42.com

API Permissions

API	Read	Write
Alerts	✓	—

Done

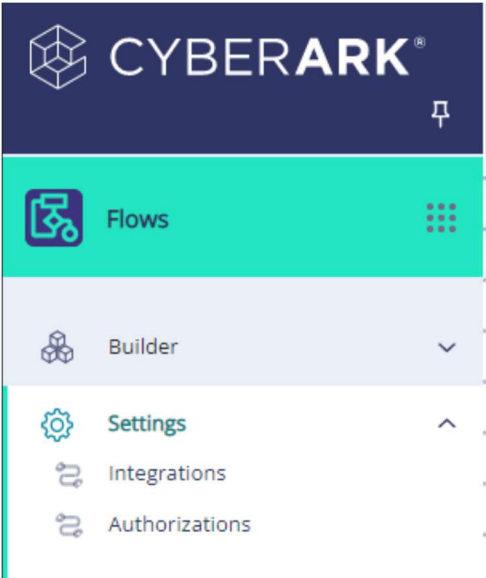
FLOWS CONFIGURATION

- To configure the flow for your tenants the following Items must be changed:
- Configure Authorizations for Code42.

- Configure CyberArk Identity OAuth2 Client.
- Configure Authorizations for CyberArk Identity.
- Configure the Hostname on all connectors.

CONFIGURING SENTINELONE AUTHORIZATION

To define configure the authorization for Code42 go into the **Settings** section in the Flows Builder menu on the **Left-hand** side of the builder.



Click on the **Authorizations**. This will launch the **Manage Authorizations** dialog box where you can configure all the Authorizations needed for the **Code42** Flow.

Manage Authorizations

New Authorizations X

Q Search Authorizations

Auth Name	Auth Type	Actions
Code42 Authz	oauth2	 
APIAuthK	oauth2	 
ApiAuthzContainer	oauth2	 
APIAuthS	oauth2	 
ApiAuthz	oauth2	 

Type*
OAuth2

Flow
Client Credentials

Content Type
application/json

Client ID*
.....

Client Secret*
.....

Auth Token
.....

Refresh Token

Token URL*
https://api.us.code42.com/v1/oauth

Audience
Typically not used

Scopes

☐ Scopes

To configure an Authorization for **Code42**. For the **Name** enter **Code42 Authz**. On the **Type**, Select **OAuth2**. For the **Flow Type** select **“Client Credentials”**. In the **ClientID** input **“clientId”**. In the **Client Secret** enter the **Client Secret** generated in the previous step.

CYBERARK IDENTITY OAUTH2 CLIENT

There are several steps in creating an OAuth2 Client inside of CyberArk Identity:

- Create a User to use as the ClientID and Client Secret.
- Create a OAuth2 Client Web App

CREATE A USER

Login to the CyberArk Identity Admin Portal, go to **Core Services->Users** and click **Add User**. Set up an API Service User like this, using your own domain instead of greentech.com.

apiuser@greentech.com

Type: CyberArk Cloud Directory User Last Login: 12/09/2021 3:31:48 PM Status: Active

- Account
- Activity
- Application Settings
- Assigned Applications
- Endpoints
- Roles
- Provisioned Applications
- Additional Attributes
- Policy Summary
- Identity Verification Details

Account

[Learn more](#)

Login Name *

apiuser

Suffix

@ greentech.com

Email Address

apiuser@greentech.com

Display Name *

API User

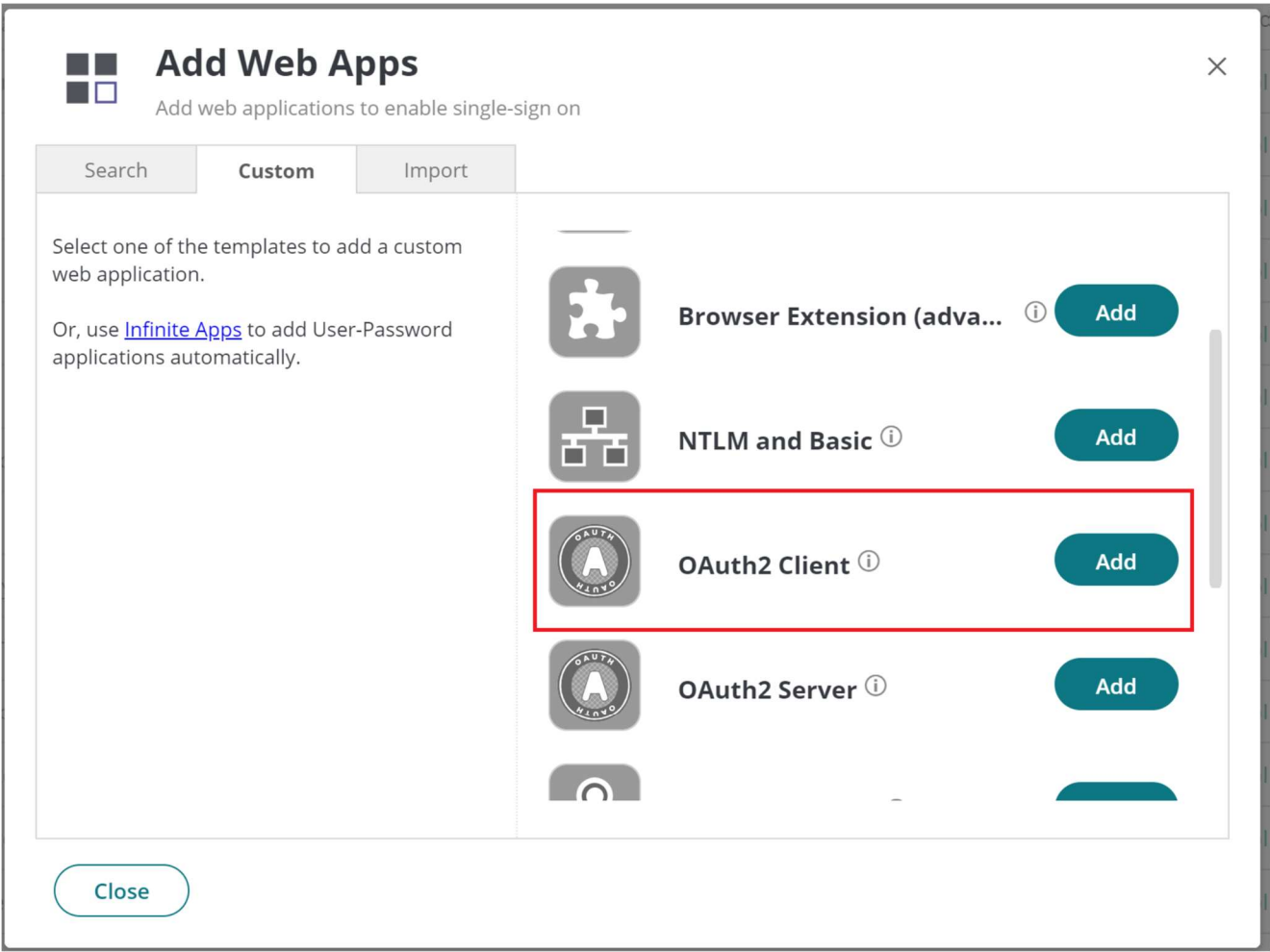
Status

- ☐ Locked
- ☒ Password never expires
- ☐ Require password change at next login
- ☒ Is Service User
- ☒ Is OAuth confidential client
- ☐ Send email invite for user portal setup
- ☐ Send SMS invite for device enrollment

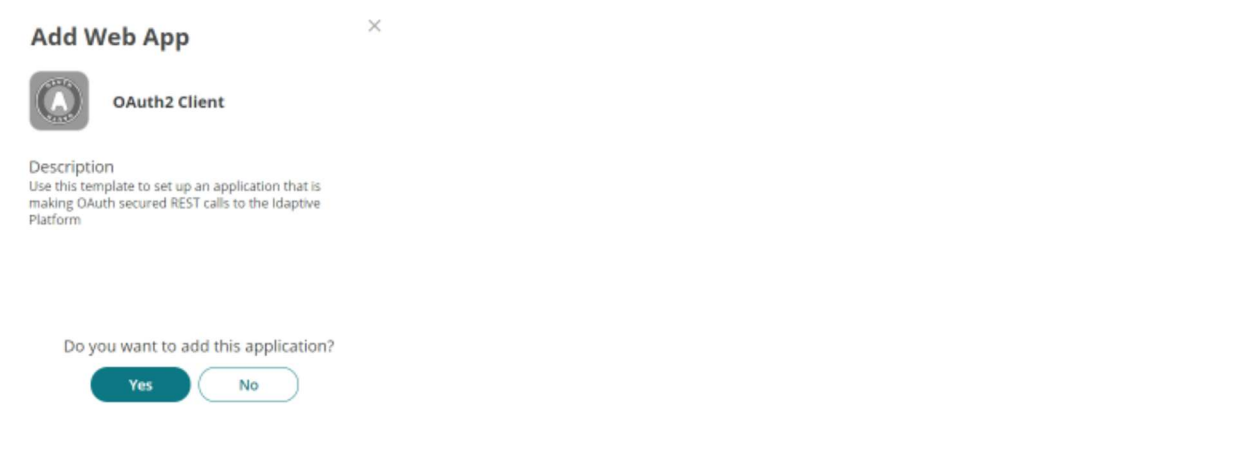
Next go to **Roles**, click **System Administrator**, and add the **apiuser** to that Role.

CREATE AN OAUTH2 CLIENT WEB APP

To create a new OAuth2 Client go to **Apps->Web Apps** and click **Add App**. This will launch the Web App selection page.



Click the **Custom Tab** up top and select the **OAuth2 Client**.



Click **Yes** to add a new OAuth2 Client.

Add Web Apps

Add web applications to enable single-sign on

Search

Custom

Import

Select one of the templates to add a custom web application.

Or, use [Infinite Apps](#) to add User-Password applications automatically.



Bookmark ⓘ

Add



Browser Extension ⓘ

Add



Browser Extension (advan... ⓘ

Add



NTLM and Basic ⓘ

Add



OAuth2 Client ⓘ

Add

Close

Then select **Close** down at the bottom. This will launch the Configuration Wizard.



CyberArk Identity API

Type: Web - Other Type

Status: Deployed

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web Sessions

Settings

[Learn more](#)

Application ID  

IdentityAPI

Description

☐ Customize Name and Description for each language 

Name 

CyberArk Identity API

Description

OAuth2 Client for Identity API

Category 

Other

Logo



[Browse](#)

Recommended image size is 180 x 180

On the **Settings** Tab, Enter the Following information. Enter the **Application ID** and **Name** of the WebApp. If you do not name your **Application ID** as **IdentityAPI** please note it down including the Case used. Since this ID is case sensitive. You will need this ID in later configuration of Flows Authorization.



CyberArk Identity API

Type: **Web - Other Type** Status: **Deployed**

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

General Usage

Client ID Type

☐ Anything

☐ List

☒ Confidential

☒ Must be OAuth Client

Confidential client is an CyberArk Cloud Directory user. [Click here to create one.](#)

Issuer

https://aae4199.my.idaptive.app

Allowed Redirects

Add

Redirect destinations

https://oauth.pstmn.io/v1/callback



Select on the **General Usage** Tab. In this screen you will need to add a call back URL in the **Redirect destinations**: **Select** the **Add** button. You will need to add the following URL replacing the TENANT section in the URL with your Tenant ID:

[https:// TENANT.flows.cyberark.cloud/gateway/callback](https://TENANT.flows.cyberark.cloud/gateway/callback)



CyberArk Identity API

Type: Web - Other Type

Status: **Deployed**

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

Tokens

Token Type *

JwtRS256

Auth methods *

☐ Auth Code

☐ Implicit

☒ Client Creds

☐ Resource Owner

Token Lifetime *

5

hours

☒ Issue refresh tokens

Refresh token lifetime *

365

days

Select the **Tokens** Tab. Confirm that the **Token Type** is **JwtRS256** next select the Auth Methods of **Auth Code** and **Client Creds**. Check the **Issue refresh tokens** and leave the default of 365 Days.



Status: **Deployed**

☐ User must confirm authorization request

☐ Allow scope selection

Add

Name	Description	Filters	
all		.*	

Select the **Scope** Tab, then **Click Add** and give it a Name of **all** and a filter of **.*** as you see above. Note the name of the scope is case sensitive. Under Permissions, add your **apiuser** and give that user all rights.



Status: **Deployed**

[Learn more](#)

Add

[illegible]

Select the **Permissions** tab, add your **apiuser** that you created in the first steps and give that user **View** and **Run** rights.

CYBERARK IDENTITY FLOWS AUTHORIZATION

In Flows on the Builder Menu **Select** on **Settings** then **Authorizations**. This will launch the **Manage Authorizations** page.

Manage Authorizations

New Authentication X

Search Authorizations

Auth Name	Auth Type	Actions
Slack E3	oauth2	 
Duo	hmac	 
Cyberark Identity AAH4087	oauth2	 
Bamboo HR	basic	 
Slack Bot E3	apiKey	 
Cyberark Identity - AAS4010	oauth2	 

Settings

Name*

Type*
OAuth2

Flow
Authorization Code

Content Type
application/json

Client ID

Client Secret

Auth Token

Reset

Authorize

Save

Once the Manage Authorization screen loads. Select **OAuth2** as the **Type** and give it a descriptive name such as **Product – Tenant ID**. Next, select the OAuth **Flow** that you will be using. Setup of the OAuth2 Client will support both the **Auth Code** and **Client Creds** flows. If you use the **Client Creds** flow you will need to change the Content-Type to be **application/x-www-form-urlencoded**. Next, fill in the **Client ID** with the **Username** that you created in the first step. Set the **Client Secret** to be the **Password** you set on that user. Next, scroll down on the Authorization configuration screen to get to the remaining configuration settings. So the **Authorization URL**, **Token URL** have some Tenant specific settings. For the **Authorization URL** specify it in this format:
<https://TENANT.id.cyberark.cloud/oauth2/authorize/APPLICATION ID>

The **Application ID** can be obtained from the OAuth2 Client configuration we completed before. It should be set to **IdentityAPI** if you followed these instructions. For the Token URL specify in this format:
<https://TENANT.id.cyberark.cloud/oauth2/token/APPLICATION ID>

Note: If you had Flows enabled on an older tenant you will need to use the host name format of **TENANT.my.idaptive.app** instead of **TENANT.id.cyberark.cloud**.

Manage Authorizations

New Authentication X

Search Authorizations

Auth Name	Auth Type	Actions
Cyberark Identity - AAS4010	oauth2	 
Microsoft Dev	oauth2	 
Proofpoint VAP	basic	 
Gurukul	apiKey	 
CorePAS	basic	 
Gurukul Dummy	apiKey	 

Refresh Token

.....

Authorization URL *

https://aas4010.id.cyberark.cloud/oauth2/authorize/identityapi

Token URL *

https://aas4010.id.cyberark.cloud/oauth2/token/identityapi

Redirect URL[Set this as the Redirect URL in your app settings page]

https://aal7307.cybrflows.com/gateway/callback

Scopes

☒ Scopes

☒ Scope

all

Description

all



+Add

Reset

Reauthorize

Update

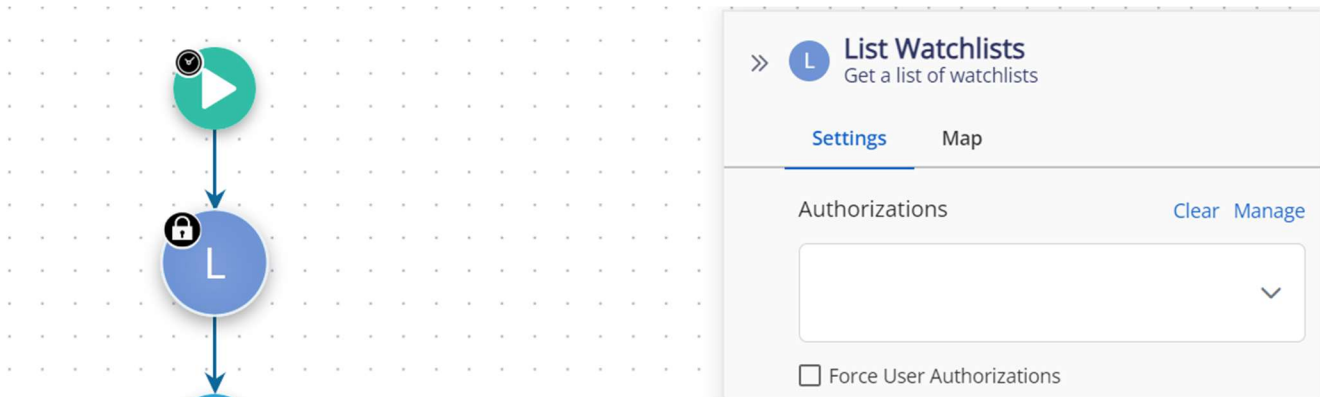
Finally, we need to do is set the **Scopes**. Click on the **Add** button and set the **Scopes** to **All** and the **description** to **All**. At this point the configuration is done. Click **Save** or **Update**. Now you are ready to test the Authorization. Click the Authorize/Reauthorize button. This will kick off the OAuth2 flow and try to obtain an **Access Token** and a **Refresh Token**.

If there are any errors here are the following things to check:

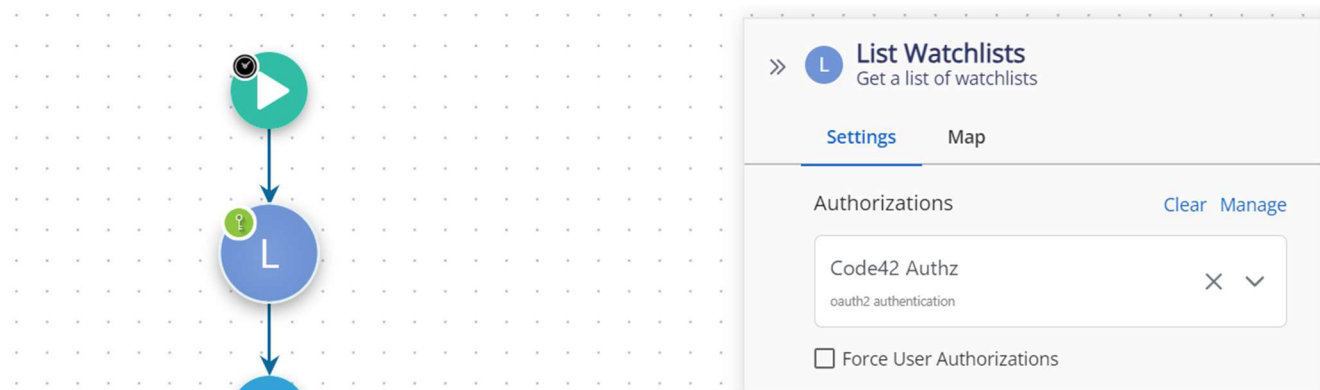
- Is your Application ID and Tenant ID correct in your Token and Authorize URLs? Case Sensitive!
- Is your Scope set correctly? Case Sensitive!
- Are your Client ID an Client Secret Correct?
- Does the user we created in the first step in Identity have View and Run permissions to the OAuth2 Client?
- Is the user created in the first step in a Role that gives them admin permissions in Identity?
- Once you have your Authorization configured and returning Tokens you can proceed to the next section.

CONFIGURING FLOW CONNECTORS

Now that we have all of the needed Authorizations configured for the Flow, we need to configure each connector to use the proper Authorization.



Select the Code42 connector in the Flow. This will open the **Connector Menu** on the right-hand side of the Builder. Click the **Down Arrow** on the **Authorizations** and Select the **Code42 Authz** Authorization you setup in the previous step. Set the code42 host to api.us.code42.com for the code42 connectors.



Next, Select the **Cyberark** connector in the Flow. This will open the **Connector Menu** on the right-hand side of the Builder. Click the **Down Arrow** on the **Authorizations** and Select the **CyberArk Identity** Authorization you setup in the previous step.

We need to change the hostname to your CyberArk Identity Tenant. If you have an older CyberArk Identity tenant, your hostname format will be: **tenant.my.idaptive.app**. Newer CyberArk Identity or ISPSS tenants will have the following formant: **tenant.id.cyberark.cloud**. Where “tenant” is replaced with your **Tenant ID**.

Repeat this step for every CyberArk connector in the Flow.

At this point you should be able to Run flow. Once you are happy you can configure the Flow to run on a schedule.

Setup needs the following steps to be completed to get the current flow working.

Authorization

- Add authorization (oauth2) in the authorization modal window for your CyberArk identity user account and Code42.
- Following API nodes are used and enable authorization as per the manage authorization dropdown menu.
 - CyberArk API: Get SCIM Users
 - CyberArk API: Get SCIM Container Permissions
 - CyberArk API: Patch SCIM Group (ID)
 - CyberArk API: Delete SCIM Container Permissions
 - Code42 API: Get Watchlists
 - Code42 API: Get Watchlist Members
 - Code42 API: Get User Risk Profiles

Other information

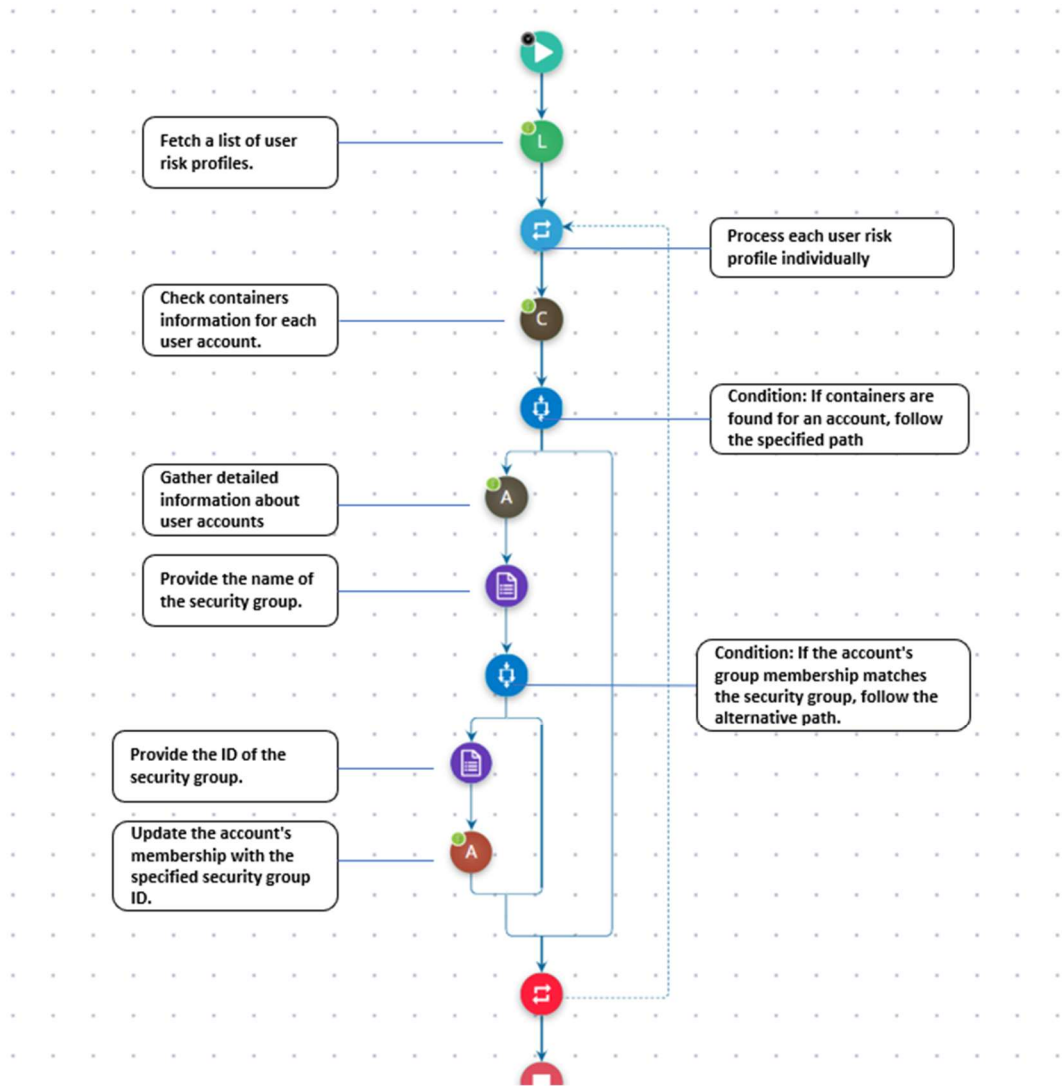
Hosts Accessed

- {tenantid}.id.cyberark.cloud
- api.us.code42.com

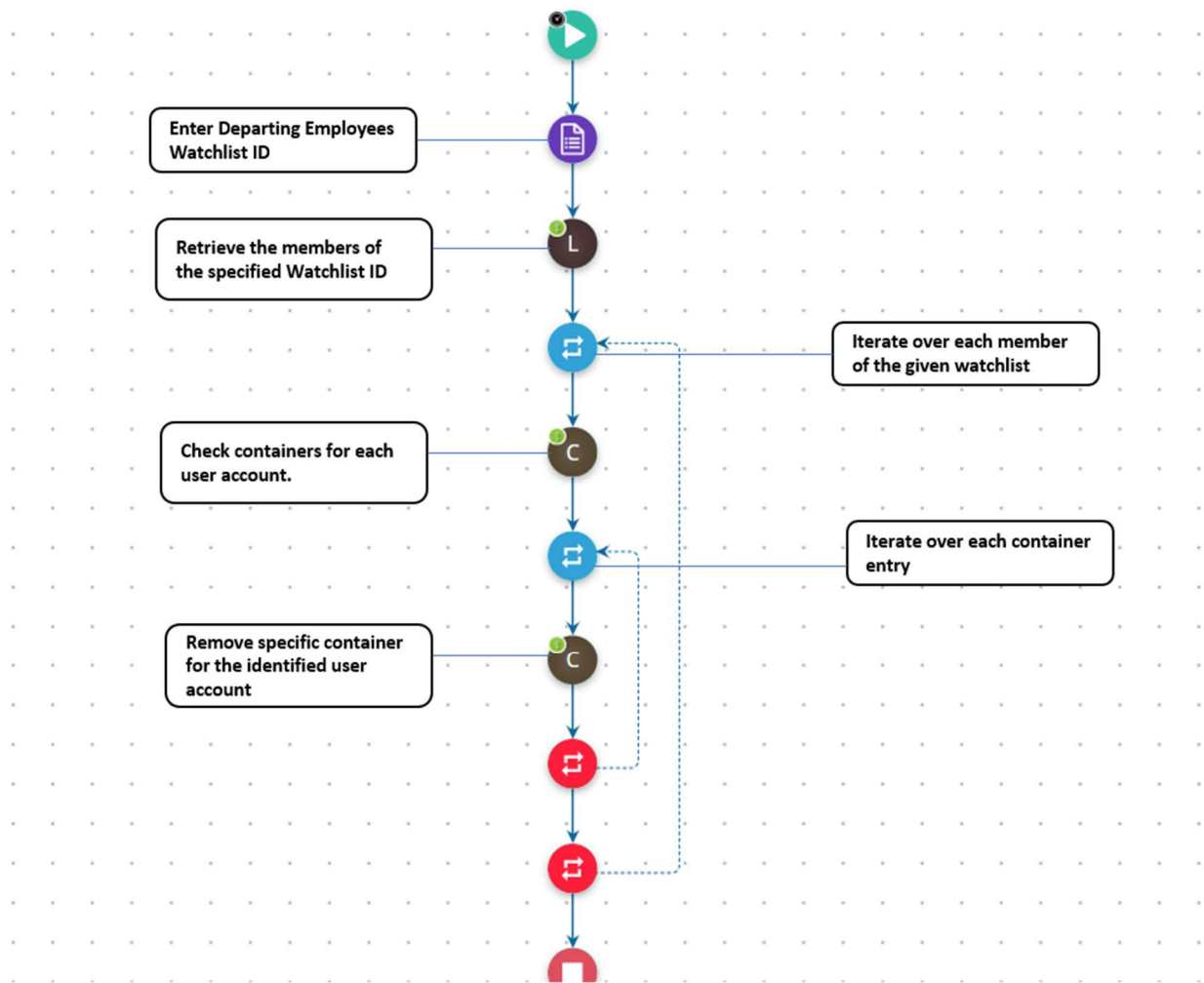
If you wish to change the hostname or use a different identity account, update the hostname in all Api nodes mentioned above in the authorization section.

Flows Diagram

USER RISK PROFILES:



DEPARTING EMPLOYEES:



WATCHLIST USERS:

