

Step-by-Step Guide: Using Identity Verification by Transmit Security in CyberArk Identity Flows

Integrating Transmit Security's Identity Verification (IDV) service with CyberArk identity flows significantly enhances security by ensuring that only verified users can access sensitive systems and data. This seamless integration offers a user-friendly verification process, reducing friction for legitimate users while maintaining robust security measures. Additionally, it helps organizations comply with regulatory requirements and reduces the risk of identity fraud by confirming user identities before granting access to critical resources.

The reason for these security improvements lies in Transmit Security's advanced IDV capabilities, which verify identities using methods like document scanning and analysis, biometrics, liveness checks and face matching. Our document scanning system leverages OCR and machine learning (ML) to authenticate and validate government-issued IDs, while biometric verification uses unique biological characteristics, such as fingerprints and facial recognition, to ensure users are who they claim to be. This approach provides fast, accurate identity verification, further enhancing overall security.

Practical use cases for this integration include verifying identities during password resets, accessing highly sensitive applications, performing high-risk transactions, onboarding new employees and verifying remote work access. By embedding IDV steps in these scenarios, organizations can enhance security, ensure compliance and prevent unauthorized access, ultimately protecting sensitive information and maintaining a secure environment.

Benefits

With Transmit Security's IDV, companies are able to improve security while maintaining the best UX to their final users. Here are the key benefits of this integration:

1. **Enhanced Security:** Ensures that only verified users can access critical resources.
2. **Compliance:** Helps meet regulatory requirements for identity verification.
3. **User Experience:** Provides a seamless and secure user verification process.
4. **Fraud Prevention:** Reduces the risk of identity fraud and unauthorized access.

Business Use Cases

Discover key business use cases that illustrate how integrating Transmit Security's IDV in Cyberark identity flows enhances overall security and compliance within organizations. Each use case demonstrates how IDV improves security in various scenarios that require identity verification.

1. **Enhanced Security:**
 - **Benefit:** Verifying users' identities through advanced methods like biometrics and document scanning significantly reduces the risk of unauthorized access to sensitive systems and data.

- **Use Case:** When an employee needs to reset their password, IDV ensures that only the legitimate user can perform this action, effectively preventing potential account takeovers.
- 2. **Compliance:**
 - **Benefit:** Many industries face regulatory requirements that mandate strict identity verification processes. Utilizing IDV enables organizations to meet these regulations effectively.
 - **Use Case:** Financial institutions can leverage IDV to comply with KYC (Know Your Customer) regulations, ensuring that only verified individuals gain access to financial services.
- 3. **User Experience:**
 - **Benefit:** A seamless and secure verification process enhances the overall user experience by reducing friction and frustration for legitimate users while upholding high security standards.
 - **Use Case:** Employees accessing highly sensitive applications can undergo a quick and efficient verification process without encountering inconvenient security checks that could interfere with their productivity.
- 4. **Fraud Prevention:**
 - **Benefit:** By verifying identities before granting access, organizations can prevent identity fraud and unauthorized access, protecting both the organization and its users.
 - **Use Case:** During a step-up authentication process — such as when accessing sensitive HR data or financial records — IDV makes sure that only authorized personnel can access this information.

Tactical Use Cases

Specific scenarios where IDV can be implemented to improve security and streamline processes. These practical examples highlight how organizations can integrate IDV into their workflows effectively.

1. **Password reset verification:**
 - **Scenario:** An employee forgets their password and requests a reset.
 - **Process:** The employee is prompted to undergo an IDV process, such as facial recognition or document scanning.
 - **Benefit:** This ensures that only the legitimate account owner can reset the password, effectively preventing unauthorized access.
2. **Access to highly sensitive applications:**
 - **Scenario:** An employee needs to access a highly sensitive application, such as a financial system or a critical infrastructure control panel.
 - **Process:** Before granting access, the system requires the employee to verify their identity through biometrics or a multi-factor authentication method that includes verifying their ID.
 - **Benefit:** This adds an extra layer of security, ensuring that only verified individuals can access sensitive applications, which reduces the risk of breaches.
3. **Step-up authentication for high-risk transactions:**

- **Scenario:** An employee is performing a high-risk transaction, such as approving a large financial transfer or accessing critical company data.
 - **Process:** The system triggers a step-up authentication process, requiring an additional verification to confirm the user's identity.
 - **Benefit:** This ensures that high-risk actions are thoroughly verified for authenticity, minimizing the risk of fraud or unauthorized activities.
4. **Onboarding new employees:**
- **Scenario:** A new employee is going through the onboarding process, which requires access to various internal systems.
 - **Process:** The onboarding process includes IDV to confirm the new hire's identity before granting access to any corporate resources.
 - **Benefit:** This ensures that only verified employees are onboarded, reducing the risk of insider threats and ensuring compliance with hiring policies.
5. **Remote access for employees:**
- **Scenario:** An employee working remotely needs to access corporate resources.
 - **Process:** Before accessing the company's network, the remote employee is required to verify their identity using IDV methods.
 - **Benefit:** This adds an extra layer of security for remote access, ensuring that only authorized employees can connect to the corporate network.

Step-by-Step Integration Guide

Prerequisites

For integrating Transmit Security's IDV into CyberArk identity flow, you will need:

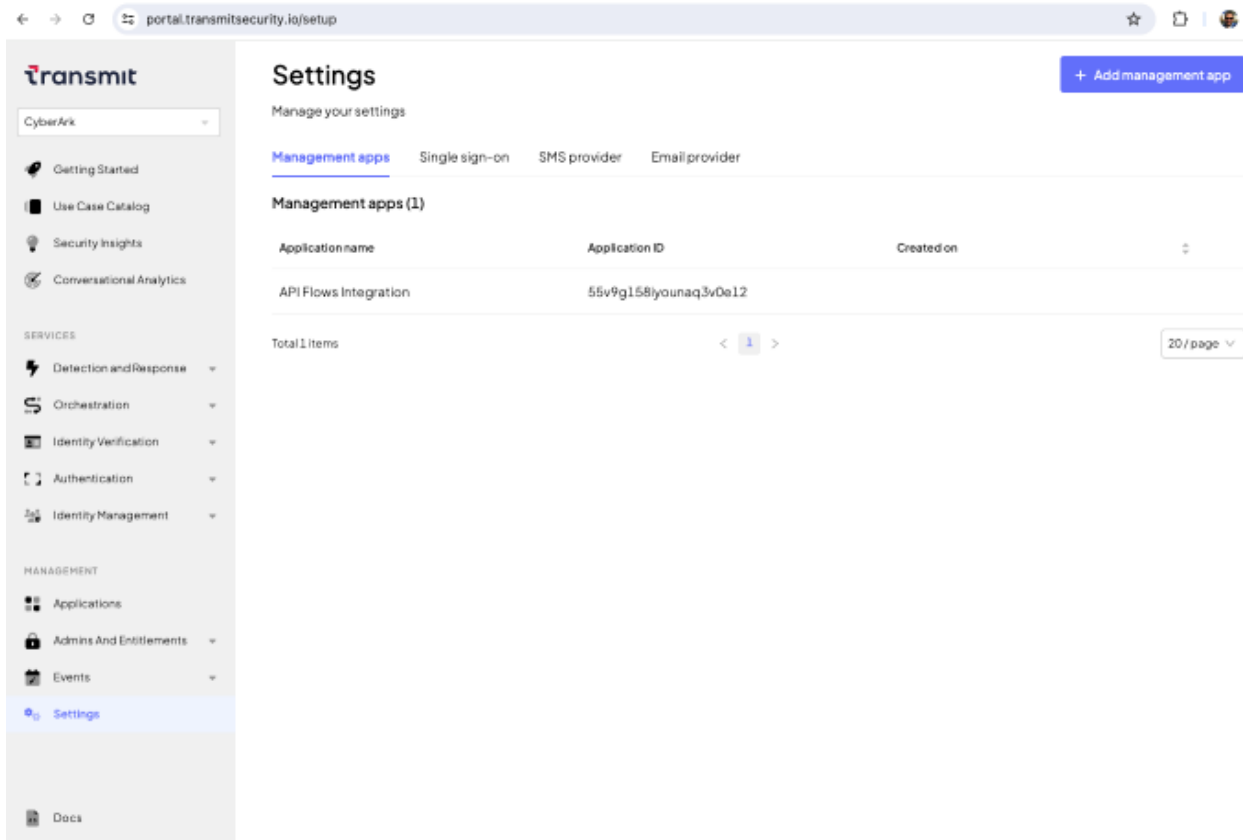
1. A Transmit Security account.
2. A CyberArk account with appropriate administrative privileges.
3. API credentials for both Transmit Security and CyberArk.

Step 1: Obtain API Credentials

1. Transmit Security setup

- **Log in to your Transmit Security account.**
 - Open your web browser and go to the Transmit Security login page.
 - Enter your credentials and log in.
- **Navigate to the “Settings” page and click on “Add management app”.**
 - Once logged in, locate the sidebar menu.
 - Click on "Settings" from the sidebar.
 - In the Settings page, go to the "Management apps" tab.
 - Click on the “Add management app” button.
- **Add Application Details**
 - **Application Name:** Enter a name for your application.
 - **Application Description:** Provide a brief description of the application.
- **Generate and save your API key and secret.**

- After adding the application details, generate the API credentials.
- Copy and securely save the API key and secret as they will be required later.



Step 2: Initial setting for IDV flow

- **On the side menu, click Experience Management under Identity Verification**
 - **Flow configuration:** Set the IDV flow (document only, full IDV, etc.), language, time period permissions for images retention and session token.
 - **Terms & Conditions (T&C):** To collect and process employee Personally Identifiable Information (PII) and biometric data, obtaining employee consent is essential before proceeding with the flow. The client can incorporate a customized disclaimer alongside our T&C to ensure clarity and compliance.
 - **Branding configuration:** Organizations are able to customize the logo and primary color of the application as well as some other additional settings.

Step 3: Set Restriction Criteria

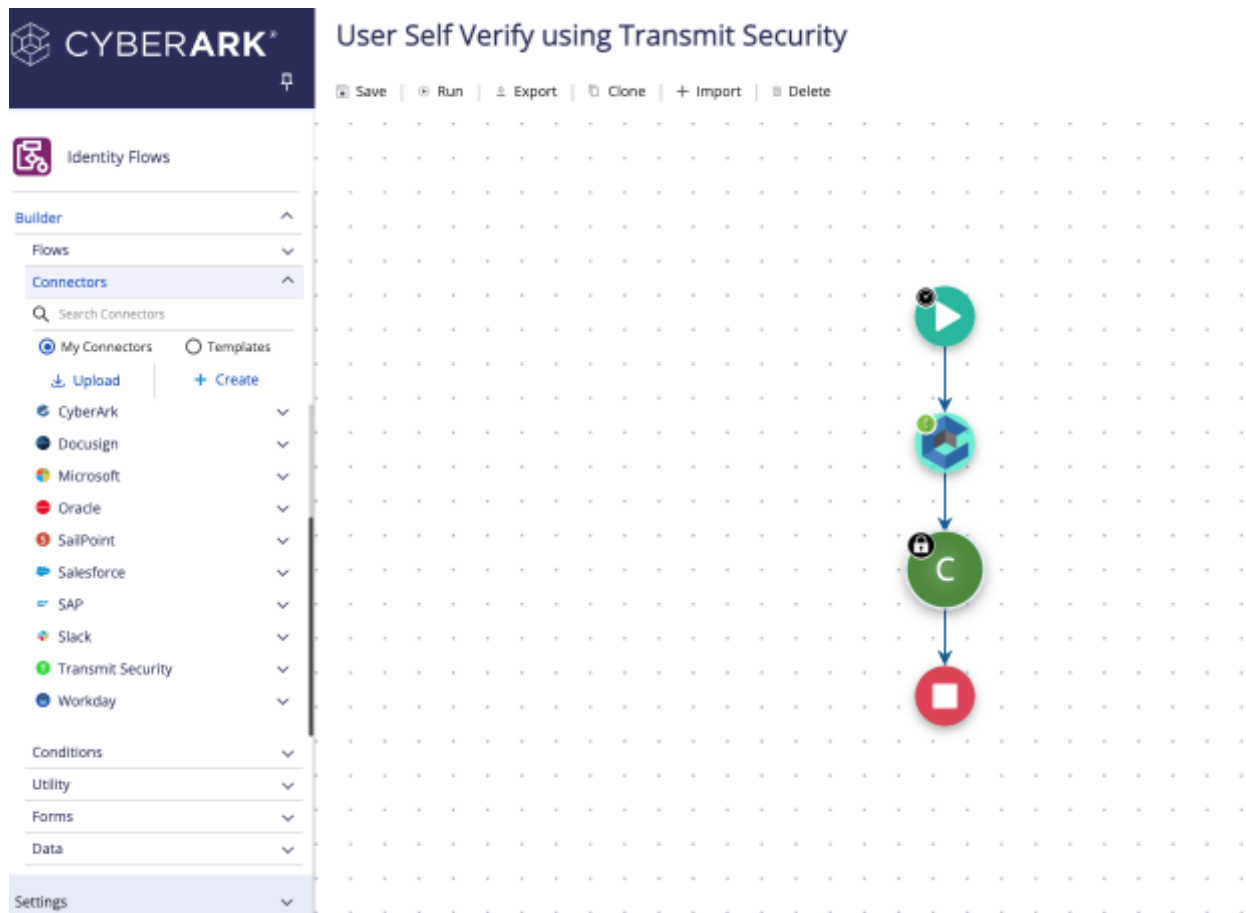
- **You can set restrictions based on document types and countries, on the side menu, by clicking Restriction Criteria.**
 - **Create rule:** Set restrictions based on country and document type, with the option to include state-level granularity if needed. For instance, if the customer's policy permits only U.S. driver's licenses due to their high security standards, they can

configure the restriction criteria to block all other document types and restrict access to countries outside of the U.S.

- **Customized message:** Customers can provide specific instructions to their end users, detailing which documents are required for the process. When a rule is triggered, users will receive a prompt that communicates the restrictions in place. This message guides the end user in instances where the customer's policy prohibits certain document types, ensuring a smoother experience and fostering clear communication throughout the process.

CyberArk Flows Setup

- **Log in to your CyberArk account.**
 - Open your web browser and go to the CyberArk login page.
 - Enter your credentials and log in.
- **Navigate to CyberArk Flows.**
 - Locate and click on the "CyberArk Flows" option from the main menu.
- **Import flows**
 - Import both the "Self Verification Flow" and the "ID Verification Complete Flow".
 - Follow the prompts to import these flows into your CyberArk account.



- **Authorization Setup**

- Ensure you have the Authorization Setup for both CyberArk Identity and Transmit Security.
- Enter the API credentials obtained from Transmit Security in the appropriate fields.
- Ensure the Hostname is also updated in the CyberArk steps to match your setup.

Manage Authorizations

New Authorizations

Search Authorizations

Auth Name	Auth Type	Actions
Transmit Security	oauth2	  
S1 API	apiKey	  
CyberArk API	oauth2	  

Settings

Name*

Transmit Security

Type*

OAuth2

▼

Flow

Client Credentials

▼

Content Type

application/x-www-form-urlencoded

▼

Client ID*

.....

Client Secret*

.....

Auth Token

.....

Refresh Token

.....

Token URL*

Reset

Reauthorize

Update

Update & Use

Step 4: Create and Map Fields in CyberArk Identity

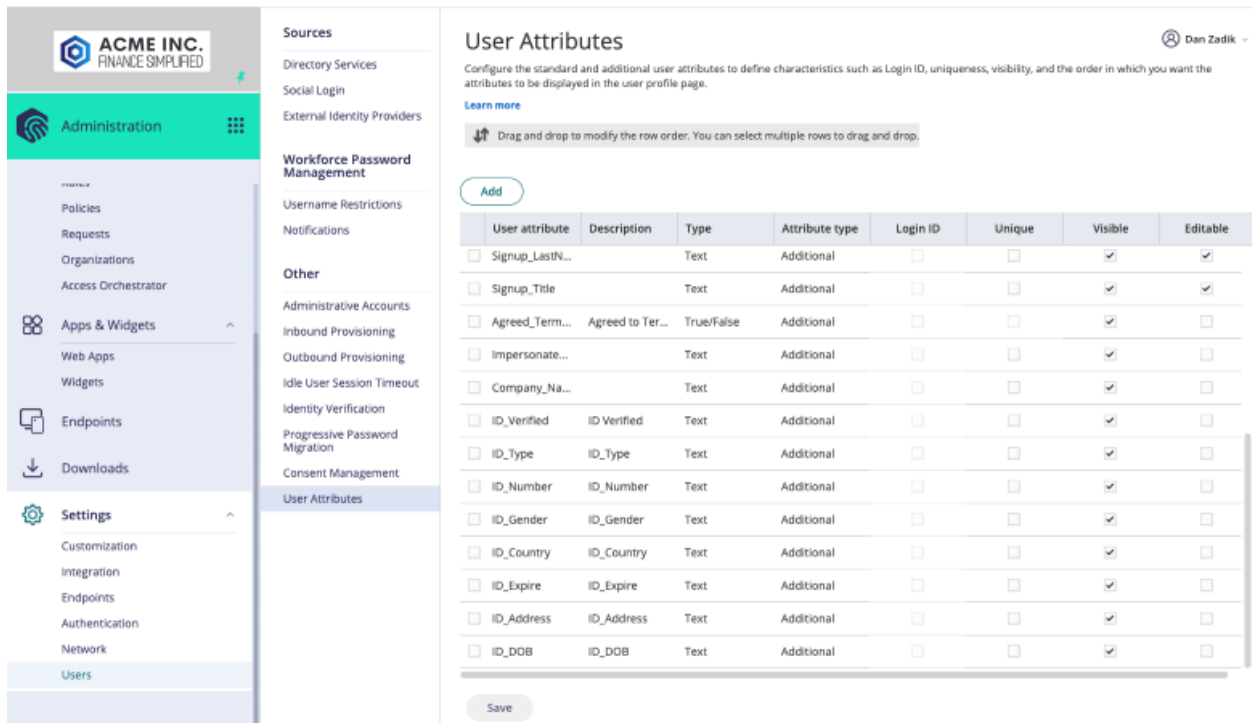
1. Transmit IDV fields

- Ensure the following fields are included for IDV:
 - full_address, biometric_liveness, biometric_matching, document_authentication, document_liveness, document_validation, flagged_identity, risk_recommendation, recommendation, country,

expiration_date, issue_date, number, region, serial_number, type, age, date_of_birth, full_name, gender, given_name, surname, session_id, status.

2. Create custom fields in CyberArk Identity for mapping

- **Go to Settings and click on Users**
 - Navigate to the "Settings" section.
 - Click on "Users".
- **Select User Attributes**
 - In the user settings, locate and select "User Attributes".
- **Add Corresponding Fields**
 - Add any of the fields listed above that you would like to include in the user profile.

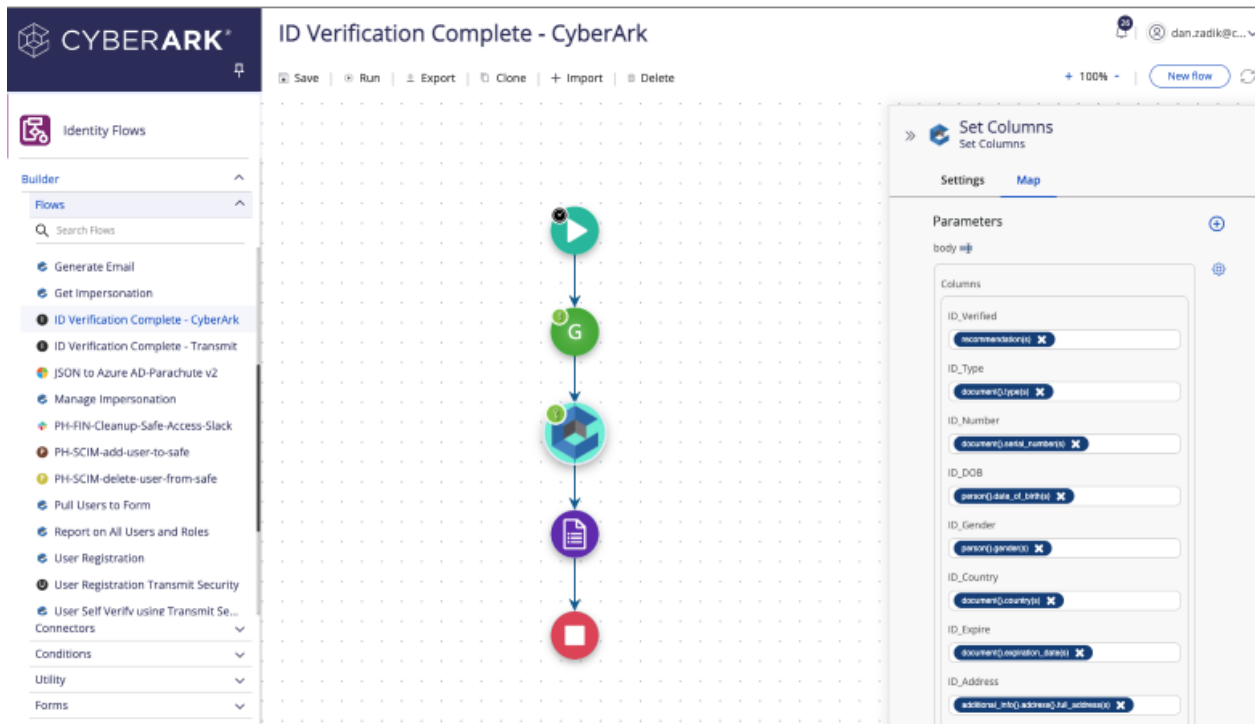


The screenshot shows the 'User Attributes' configuration page in the CyberArk Identity console. The left sidebar contains the navigation menu with 'Settings' and 'Users' highlighted. The main content area is titled 'User Attributes' and contains a table of attributes to be configured. The table has columns for 'User attribute', 'Description', 'Type', 'Attribute type', 'Login ID', 'Unique', 'Visible', and 'Editable'. The table lists various attributes such as 'Signup_LastN...', 'Signup_Title', 'Agreed_Term...', 'Impersonate...', 'Company_Na...', 'ID_Verified', 'ID_Type', 'ID_Number', 'ID_Gender', 'ID_Country', 'ID_Expire', 'ID_Address', and 'ID_DOB'. Each attribute has a checkbox for selection and a 'Save' button at the bottom.

User attribute	Description	Type	Attribute type	Login ID	Unique	Visible	Editable
☐ Signup_LastN...		Text	Additional	☐	☐	☒	☒
☐ Signup_Title		Text	Additional	☐	☐	☒	☒
☐ Agreed_Term...	Agreed to Ter...	True/False	Additional	☐	☐	☒	☐
☐ Impersonate...		Text	Additional	☐	☐	☒	☐
☐ Company_Na...		Text	Additional	☐	☐	☒	☐
☐ ID_Verified	ID Verified	Text	Additional	☐	☐	☒	☐
☐ ID_Type	ID_Type	Text	Additional	☐	☐	☒	☐
☐ ID_Number	ID_Number	Text	Additional	☐	☐	☒	☐
☐ ID_Gender	ID_Gender	Text	Additional	☐	☐	☒	☐
☐ ID_Country	ID_Country	Text	Additional	☐	☐	☒	☐
☐ ID_Expire	ID_Expire	Text	Additional	☐	☐	☒	☐
☐ ID_Address	ID_Address	Text	Additional	☐	☐	☒	☐
☐ ID_DOB	ID_DOB	Text	Additional	☐	☐	☒	☐

3. Map fields in CyberArk Flows

- **Open CyberArk Flow and open ID Verification Complete Flow**
 - Navigate to the "CyberArk Flow" section.
 - Open the "ID Verification Complete Flow".
- **Map fields**
 - Select the specific flow step and choose the "Map" option.
 - Edit the body to include the necessary data mappings to CyberArk Identity.



Step 5: Deploy Integration

1. Setup flow completion

- **Open the ID Verification Complete Flow**
 - Navigate to the "ID Verification Complete Flow".
- **Play the Flow**
 - Click the "Play" button.
 - Select the Flow Type – "Standard Flow".
 - Copy the Browser URL generated by this step.

ID Verification Complete - CyberArk

Save | Run | Export | Clone | Import | Delete

+ 100% | New flow

ID Verification Complete - CyberArk
Runtime Settings

Info | Schedule | Settings

Flow type
Flow type
Standard flow x v

External access controls
☒ User access
☒ Builder authentication
☐ Flow OIDC authentication

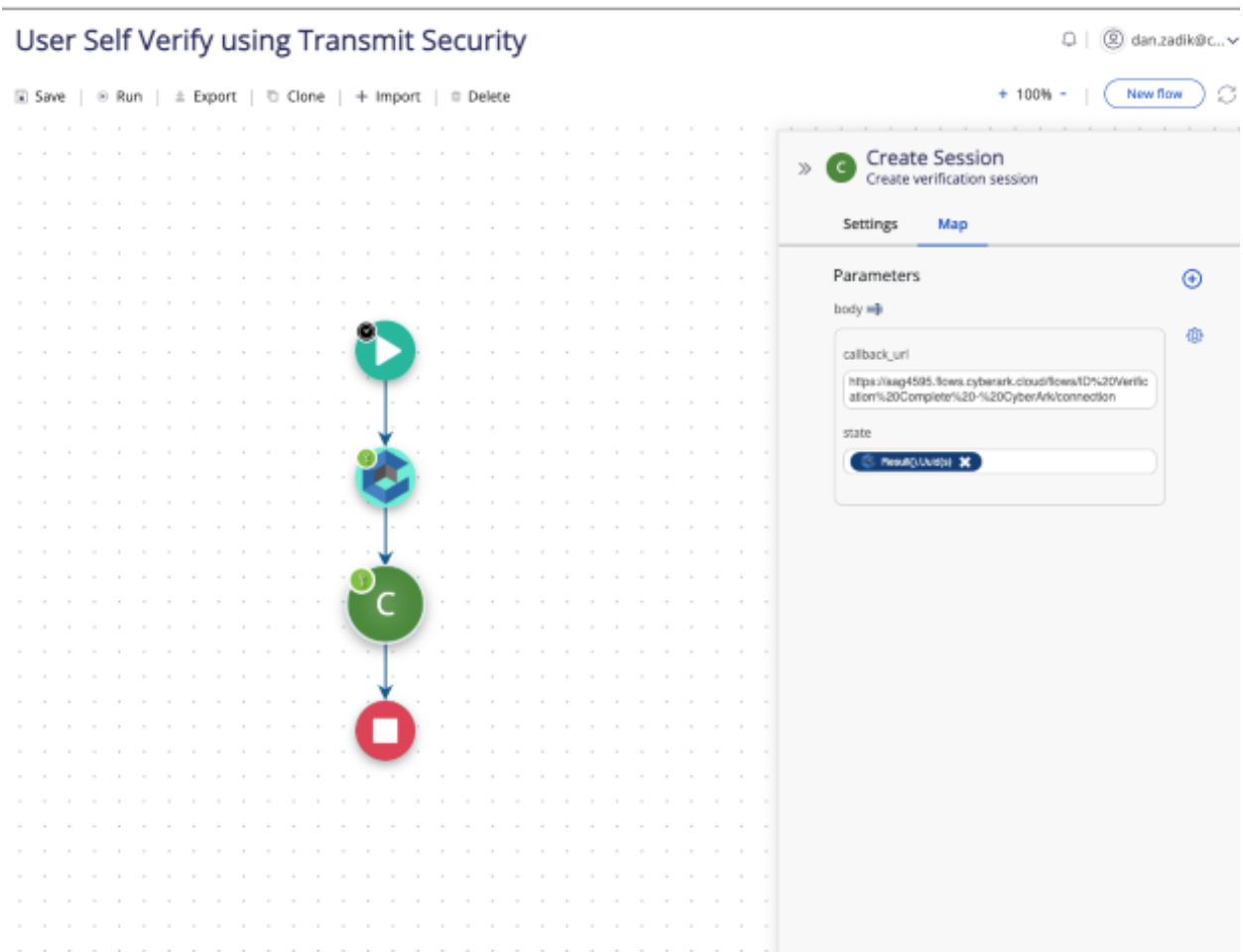
Browser URL
https://aag4595.flows.cyberark.cloud/flows/ID%20Verific

☐ API access

Publish as
Select API Access & save the flow to view the options

2. Connect to Self Verification Flow

- **Open Self Verification Flow**
 - Navigate to the "Self Verification Flow".
- **Create a session for Transmit Security.**
 - Click on the "Create Session" step for Transmit Security.
 - Click on "Map".
 - Paste the URL from the previous step into the `callback_url` field.



Step 6: Deploy to CyberArk Identity

1. Deploy the Flow

- **Open User Self Verify Flow**
 - Navigate to the "User Self Verify Flow".
- **Play the flow.**
 - Click the "Play" button.
 - Select the Flow Type – "Standard Flow".
 - Copy the Browser URL generated by this step.

User Self Verify using Transmit Security

Save | Run | Export | Clone | Import | Delete

+ 100% | New flow

User Self Verify using Transmit Security
Runtime Settings

Info Schedule Settings

Flow type
Flow type
Standard flow x v

External access controls

☒ User access
☒ Builder authentication
☐ Flow OIDC authentication

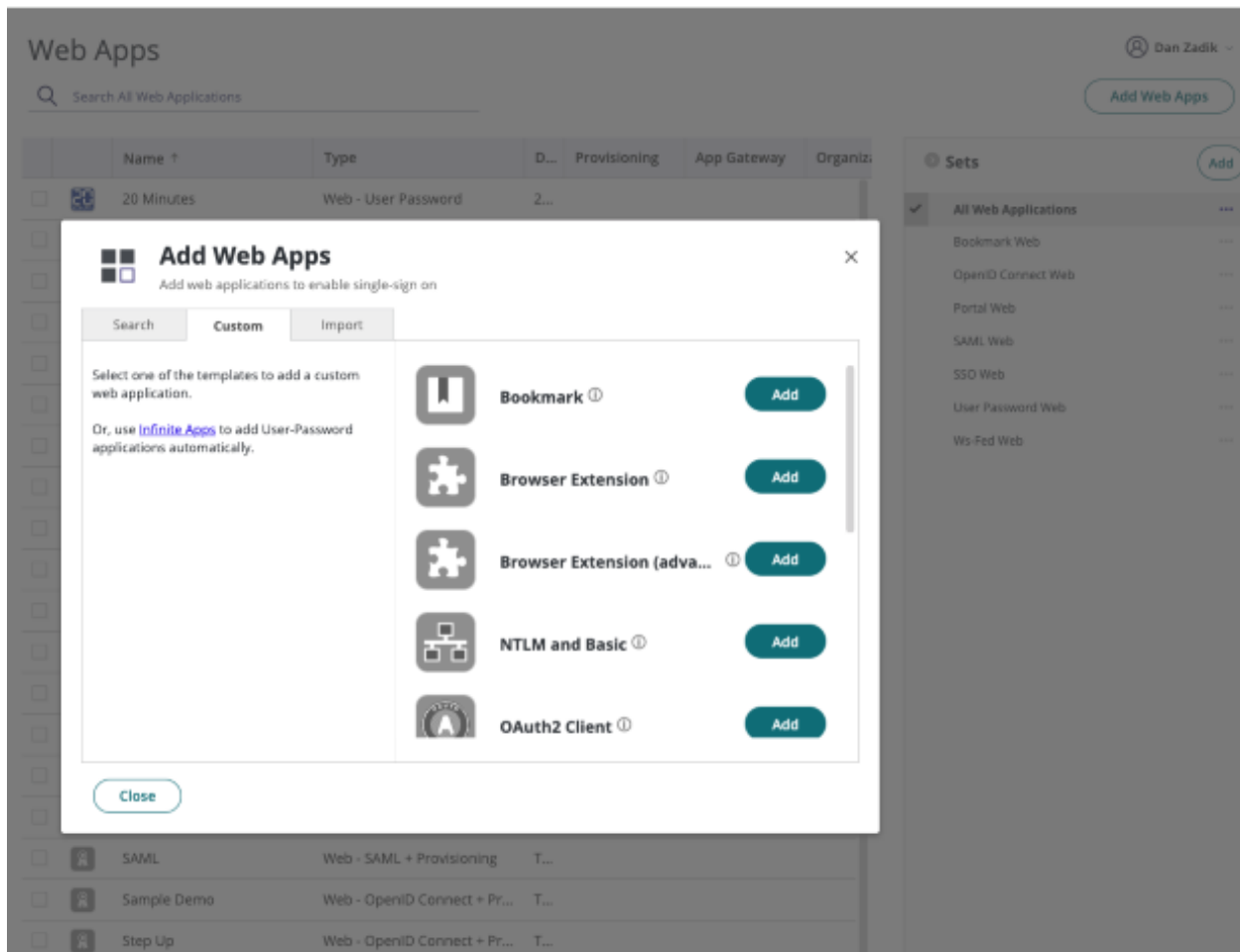
Browser URL
https://aag4595.flows.cyberark.cloud/flows/User%20Self

☐ API access

Publish as
Select API Access & save the flow to view the options

2. Create Web App in CyberArk Identity

- **Select Apps & Widget and click on Web Apps.**
 - Navigate to the "Apps & Widget" section.
 - Click on "Web Apps".
- **Add Web App.**
 - Select "Add Web Apps".
 - Click on the "Custom" tab.
 - Add a Bookmark.



- **Configure Web App**
 - Add any logo and the URL from the steps above.

Bookmark

Type: Web - Bookmark

Status: **Not Configured**

[Application Configuration Help](#)

Actions

Application Settings

Description

Permissions

Policy

App Gateway

Workflow

Changelog

Secure Web
Sessions

Additional Attributes

Application Settings

URL  

`https://aag4595.flows.cyberark.cloud/flows/User%20Self%20Ve`

3. Enable access

- **Select the Permissions tab.**
 - Navigate to the "Permissions" tab in the Web App settings.
- **Add roles.**
 - Click "Add" and select the corresponding roles that should have access to this app.

Bookmark

Type: Web - Bookmark

Status: **Not Configured**[Application Configuration Help](#)

Actions ▾

Application Settings

Description

Permissions

Policy

App Gateway

Workflow

Changelog

Secure Web

Sessions

Additional Attributes

Permissions

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

	Name	Grant	View	Manage	Delete	Run	Automatically D...	Star
☐	 Acme Austin Admin	☒	☒	☒	☒	☐	☐	
☐	 Acme Austin Admin	☐	☒	☐	☐	☐	☐	
☐	 alero-integration-user\$@...	☒	☒	☒	☒	☐	☐	
☐	 ANALYTICS_OAUTH_USER	☒	☒	☒	☒	☐	☐	
☐	 FLOWS-PORTAL-ADMIN\$	☒	☒	☒	☒	☐	☐	
☐	 sws-integration-user\$@cy...	☒	☒	☒	☒	☐	☐	
☐	 System Administrator	☒	☒	☒	☒	☐	☐	

Step 7: Run a test

1. Open the User Portal

- **Open the User Portal**
 - Navigate to the User Portal in CyberArk.
- **Select the ID Verification App.**
 - Locate and select the "ID Verification App".

All Items

View in classic UI

Dan Zadik

All Applications Secured Items

+ Add

Sort Custom

Group by None

Search


ID Verification


Salesforce


Healthcare Demo


SAML


TESTY-XYZ-22


MySecretToKeep


name


TESTY-XYZ-20


Building Access Code


test


20 Minutes

Folders

2. Follow the Verification Step

- **Complete verification process.**
 - Using your phone, go through the verification process as prompted.



Verify your identity

Scan the QR code using your mobile device to get started



Or use URL on a mobile device

https://api.transmitsecurity.io/verify/app/5pYd_2Q3dZN01Fc0IkZIILeXlp?startedOnDesktop=true

3. Validate mapped data

- **In CyberArk Identity:**
 - Navigate to "Core Services".
 - Open the "User" section.
 - Select the specific user designated for testing.
 - Validate the data to ensure it is mapped correctly.

By following these steps, you should be able to successfully integrate and test the Transmit Security with CyberArk Identity.

Account

Activity

Application Settings

Assigned
Applications

Endpoints

Roles

Provisioned
Applications

Additional Attributes

Policy Summary

Additional Attributes

Name	Value	Description
Company_Name		
ID_Verified	 ALLOW	ID Verified
ID_Type	 drivers_license	ID_Type
ID_Number	 64654654	ID_Number
ID_Gender	 male	ID_Gender
ID_Country	 US	ID_Country
ID_Expire	 2025-12-13	ID_Expire
ID_Address	 654 Main Street	ID_Address
ID_DOB	 1999-11-28	ID_DOB

Troubleshooting

- **API Errors:** Check the API endpoint, credentials, and request format.
- **Verification Failures:** Review the verification methods and user data accuracy.
- **Flow Issues:** Ensure all steps in the CyberArk flow are correctly configured and linked.

Mosaic by Transmit Security Admin Portal Tools

The following investigation and troubleshooting tools are available in the Admin Portal:

- **Verification Report:** Enable fraud administrators to obtain a comprehensive overview of each session, enhancing understanding of the IDV process. Administrators can easily identify actions taken and the reasons for any failures. For approved requests, the report

provides insights into the model's results and outcomes, promoting transparency and building confidence in the verification process.

- **IDV Analytics Dashboard:** Designed to offer a comprehensive, high-level overview of the performance of the IDV process, ensuring optimal functionality and facilitating continuous improvement.
- **Conversational Analytics:** Create customized dashboards using the graphs and visuals generated for deeper analytical insights.

Conclusion

Integrating ID Verification with CyberArk flows greatly strengthens security by validating user identities before granting access to critical resources. By following this guide, organizations can establish a robust and compliant identity verification process that not only enhances security but also optimizes the user experience. Embrace these advancements to foster a safer and more efficient environment for your organization.