

Connectors

July 1, 2025



CONNECTORS

Copyright

All product technical documentation is
Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Refer to <https://docs.pingidentity.com> for the most current product documentation.

Trademark

Ping Identity, the Ping Identity logo, PingAccess, PingFederate, PingID, PingDirectory, PingDataGovernance, PingIntelligence, and PingOne are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in Ping Identity product documentation is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Table of Contents

A-C	5
AuthenticID Connector	8
Azure AD User Management Connector	70
Azure AD User Management Connector Release Notes	90
Castle Connector	90
Challenge Connector	92
Challenge Connector Release Notes	101
Code Snippet Connector	102
Cookie Connector	110
CrowdStrike Connector	118
CrowdStrike Connector Release Notes	128
D-F	128
Daon Connector	132
Device Policy Connector	158
Duo Connector	165
Entrust Connector	177
Error Message Connector	181
FingerprintJS Connector	183
Flow Analytics Connector	190
Flow Analytics Connector Release Notes	193
Flow Conductor Connector	193
Flow Conductor Connector Release Notes	203
Functions Connector	204
Functions Connector Release Notes	218
G-I	219
Google Workspace Admin Connector	221
HTTP Connector	264
HTTP Connector Release Notes	285
HYPR Connector	287
ID DataWeb Connector	293
J-L	302
Jira Connector	304
LDAP Connector	316
LexisNexis Connector	321
LexisNexis Connector Release Notes	420
Location Policy Connector	421
Location Policy Connector Release Notes	423
M-O	423
Marketo Connector	426
Microsoft Edge for Business Connector	438

Microsoft Teams Connector	444
OIDC and OAuth IdP Connector	478
OneTrust Connector	482
P-R	495
PingFederate Connector	500
PingID Connector	511
PingID Connector Release Notes	526
PingOne Connector	528
PingOne Connector Release Notes	662
PingOne Advanced Identity Cloud Access Request Connector	667
PingOne Advanced Identity Cloud Access Request Connector Release Notes	701
PingOne Advanced Identity Cloud Login Connector	702
PingOne Advanced Identity Cloud Login Connector Release Notes	705
PingOne Authentication Connector	705
PingOne Authentication Connector Release Notes	730
PingOne Authorize Connector	731
PingOne Credentials Connector	739
PingOne Forms Connector	779
PingOne Forms Connector Release Notes	788
PingOne MFA Connector	789
PingOne MFA Connector Release Notes	901
PingOne Notifications Connector	902
PingOne Protect Connector	912
PingOne RADIUS Gateway Connector	942
PingOne RADIUS Gateway Connector Release Notes	947
PingOne Scope Consent Connector	948
PingOne Scope Consent Connector Release Notes	962
PingOne Verify Connector	962
S-U	1011
Salesforce Connector	1015
SAML IdP Connector	1070
Screen Connector	1079
SecurID Connector	1081
SEON Connector	1093
ServiceNow Connector	1114
Socure Connector	1145
Splunk Connector	1166
Splunk Connector Release Notes	1171
String Connector	1172
Teleport Connector	1189
Token Management Connector	1192
Token Management Connector Release Notes	1197
TransUnion TLOxp Connector	1197

V-Z 1275

Variable Connector 1277

Veriff Connector 1283

Yoti Connector 1291

A-C



AuthenticID Connector

This connector lets you use AuthenticID for identity proofing in your PingOne DaVinci flow.



Microsoft Teams

Azure AD User Management Connector

The Azure AD User Management connector lets you manage users, groups, and software licenses in your PingOne DaVinci flow.



Castle Connector

The Castle connector lets you add additional risk signals with Castle's fraud and risk management platform in your PingOne DaVinci flow.



Challenge Connector

The Challenge connector allows you to branch your PingOne DaVinci flow to handle an external event, such as an MFA step.



Code Snippet Connector

The Code Snippet connector lets you create custom JavaScript code that you can reuse across multiple PingOne DaVinci flows.



Cookie Connector

The Cookie connector lets you set and retrieve session cookies in your PingOne DaVinci flow.



CrowdStrike Connector

The CrowdStrike connector lets you use CrowdStrike improve authentication security in your PingOne DaVinci flow.

AuthenticID Connector

The AuthenticID connector lets you use AuthenticID for identity verification in your PingOne DaVinci flow.

The connector supports the AuthenticID CFAir and CFWeb services.

For CFAir, the connector can upload a previously captured identity document and selfie images to AuthenticID.

For CFWeb, the connector allows you to direct users to a unique verification URL where they will submit their driver license or passport along with a selfie photo. After AuthenticID verifies the user's identity, it sends the results to DaVinci where you can branch your flow accordingly.

To make sure a camera is available to scan the documents and take photos, the user typically completes the verification process on a mobile device, either in a web browser or using a mobile app:

- Mobile web browser

With this approach, the connector generates a unique verification URL and lets you provide it to the user in a few ways:

- The connector makes the URL available as a variable in your flow.

In the **Using the connector in a flow** section below, we use this URL to show a QR code in the web browser, which makes it easy to open the link on the mobile device.

- The connector sends the URL directly to the customer as an SMS message.
- The connector sends the URL directly to the customer as an email message.

- Mobile app

- The connector starts the verification process directly in an Android or iOS app that you built using the AuthenticID mobile SDK.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- Your AuthenticID application programming interface (API) access credentials (provided by an AuthenticID representative)
- Your SMTP email server credentials, if you want to send verification URLs by email
- A Twilio account, if you want to send verification URLs by SMS

Configuring the AuthenticID connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

To get the following information, speak to an AuthenticID representative.

Base URL

The API URL provided by AuthenticID. Change this URL to target the AuthenticID sandbox or production environment.

REST API URL

The REST API URL provided by AuthenticID. Change this URL to target the AuthenticID sandbox or production environment.

Account Access Key

The account access key provided to you by AuthenticID.

Secret Token

The secret token provided to you by AuthenticID.

Client Certificate

The client certificate provided to you by AuthenticID.

Client Key

The client key provided to you by AuthenticID.

Certificate Passphrase

The certificate passphrase, if AuthenticID provided you with one.

iOS SDK License Key

The iOS SDK license key provided to you by AuthenticID. This is only required if you built an iOS app with the AuthenticID mobile SDK.

Android SDK License Key

The Android SDK license key provided to you by AuthenticID. This is only required if you built an Android app with the AuthenticID mobile SDK.

Using the connector in a flow

Verifying identities with CFAir

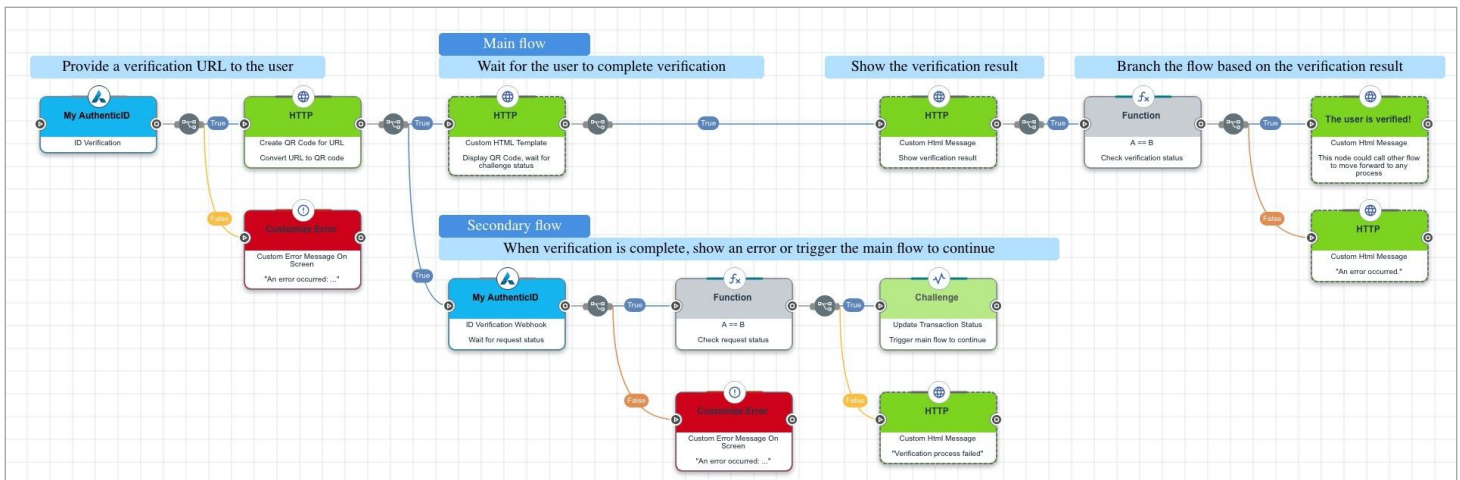


If you're satisfied with your existing document and selfie image capture experience, this flow shows how you can send the resulting images to AuthenticID for identity verification.

Both capabilities allow you to associate the images with an existing AuthenticID transaction ID to build a profile.

Download the [Identity verification with AuthenticID CFAir](#) flow template. For help, see [Using DaVinci flow templates](#).

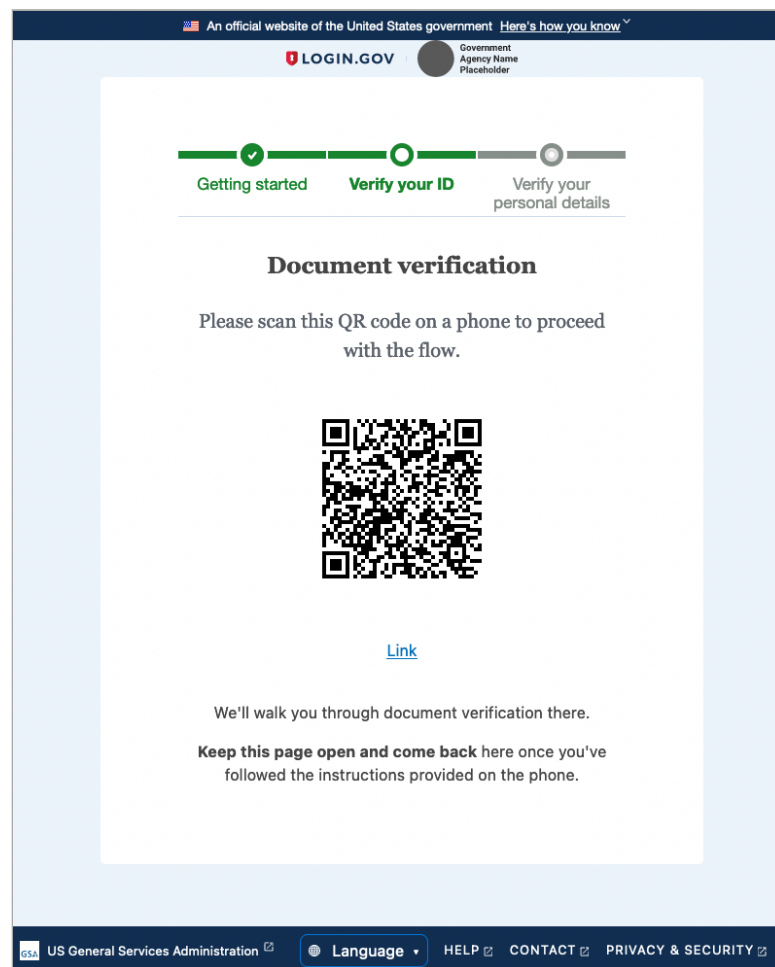
Verifying identities with CFWeb



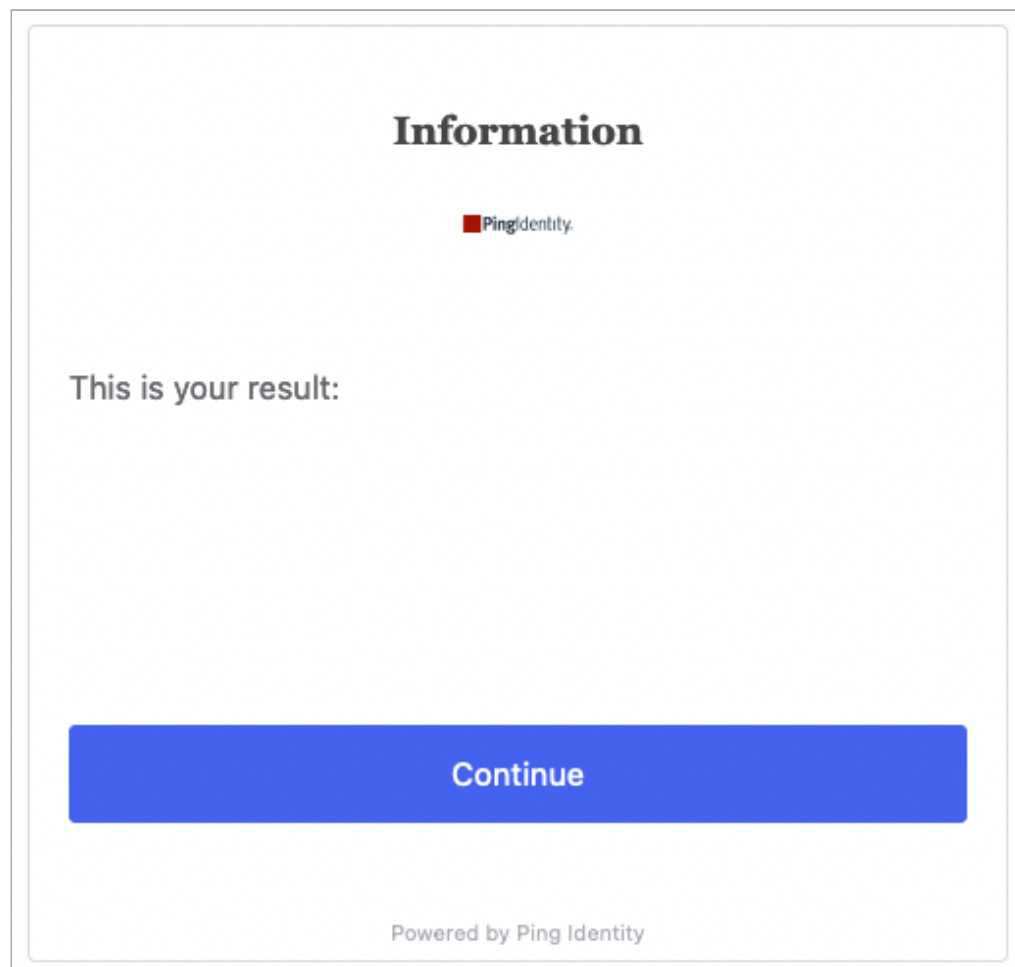
In this flow, you use AuthenticID to generate a unique verification URL and show it as a QR code in the user's web browser. When the user opens the QR code link with their mobile device, they're guided through the process of taking photos of their identification card (either a driver license or passport), then instructed to take a selfie photo. After the documents and photos are accepted, the flow continues where it started in the web browser.

This flow uses the **AuthenticID** connector to create a "challenge". This lets you pause the main flow on the QR code while a secondary flow continues the verification process. When the verification process is complete, you use a **Challenge** connector to trigger the main flow to continue. To learn more about this technique, see the **Challenge** connector.

1. Download the [AuthenticID Identity verification with CFWeb](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the document verification QR code prompt:



1. Select the **Custom HTML Template** node in the **Wait for the user to complete verification** section.
2. In the **HTML Template** field, customize the HTML.
3. Click **Apply**.
3. (Optional) Customize the result page:



1. Select the **Custom HTML Message** node in the **Show the verification result** section.
2. In the **Message** field, customize the message.
3. Click **Apply**.

Note

The flow template shows the user the result of the verification process. In a product environment, this is where you should redirect the user to their account page, another step in the registration process, or similar.

4. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

Capabilities

Verify ID with CFWeb

Verify the authenticity of an identity document with the AuthenticID hosted solution, CFWeb.

Properties

channel dropDown

Phone Number textField

Phone number to which the link is to be sent for ID Verification. (Required if channel is PHONE)

Email textField

Email address to which the link is to be sent for ID Verification. (Required if channel is EMAIL)

Mail Host textField

Contains the email server hostname.

Mail Port textField

Contains the email server port number.

Mail Username textField

Contains the email server login username.

Mail Password textField

Contains the email server login password.

Mail SMTP Auth toggleSwitch

If true, attempt to authenticate the user using the AUTH command. Defaults to false.

Mail SMTP Start TLS Enable toggleSwitch

If true, enables the use of the STARTTLS command.

Email Subject textField

Contains the subject line of the email sent to the customer. Please make sure no new lines characters are in this string.

Email Content textField

This variable provides the email content that will be sent to your customer. Use '%URL%' in your content template as a placeholder for the verification link. Please make sure no new lines characters are in this string.

Email From textField

Contains the email from which the verification email will be sent to the customer.

Twilio Account String Identifier (SID) textField

Contains Twilio account accountSid.

Twilio Authorization Token textField

Contains Twilio account authToken.

Twilio From Number textField

Contains the phone number from which the SMS will be sent.

Twilio SMS Content textField

Contains the structure of the SMS message to be sent to the customer. Use '%URL%' in your message as a placeholder for the verification link. Please make sure no new lines characters are in this string.

channelResponse dropDownMultiSelect***Request Expiry Time in Minutes textField***

This value dictates the expiry time of the verify request's token. Default: 4320

Transaction Expiry Time in Minutes textField

This value dictates the expiry time of the transaction. Default: 60

Transaction Attempts textField

This value specifies the number of transaction a user can attempt before the request is marked as failures.
Default: 4

Front Capture Attempt textField

This value specifies the number of front capture attempts the user is allowed to use to capture a good image, after this threshold the last image is used. Default: 4

Back Capture Attempt textField

This value specifies the number of back capture attempts the user is allowed to use to capture a good image, after this threshold the last image is used. Default: 4

Selfie Capture Attempt textField

This value specifies the number of selfies capture attempts the user can use to capture a good image, after this threshold the last image is used. Default: 4

Enable Selfie Capture toggleSwitch

Setting this value to true lets the application request for a near selfie to be captured. Default: true

Enable Far Selfie toggleSwitch

Setting this value to true lets the application request for a far selfie to be captured. Default: true

Focus Front textField

Specifies the front images focus threshold, any image which does not have a focus value greater than this value will be rejected by the application. Default: 30

Focus Back textField

Specifies the back images focus threshold, any image which does not have a focus value greater than this value will be rejected by the application. Default: 30

Glare Front textField

Specifies the front images glare threshold, any image which does not have a glare value less than this value will be rejected by the application. Default: 2.5

Glare Back textField

Specifies the front images glare threshold, any image which does not have a glare value less than this value will be rejected by the application. Default: 2.5

Review Screen Front toggleSwitch

If this flag is set to true, Front review screen is shown once front image is captured. Default: true

Review Screen Back toggleSwitch

If this flag is set to true, Back review screen is shown once back image is captured. Default: true

Logo (Base64 image) textField

This value is used to show the logo at the welcome screen. The value in this field should be Base64 encoded image file.

Home Screen (Base64 image) textField

This value is used to show the background image in the welcome and consent screen. The value in this field should be a Base64 encoded image file.

frontCaptureMode dropDown***Front Overlay Text Manual textField***

This message is shown on top of the front capture screen when the frontCaptureMode is set to Manual

Default:

Align ID and tap
 to capture.

Front Overlay Text Auto textField

This message is shown on top of the front capture screen when the frontCaptureMode is set to Auto

Default:

Align ID within box and capture

Front Overlay Color textField

This value is used to color the text shown on the front capture screen. The value should be in CSS3 Hex format.

Front Enable Face Detection toggleSwitch

This flag specifies if the face detection should be enabled when the front image is captured.

Front Set Manual Timeout in Seconds textField

This value specifies after how many seconds to pass before the capture mode is switched from Auto to Manual

backCaptureMode dropDown**Back Overlay Text Manual textField**

This message is shown on top of the back capture screen when the backCaptureMode is set to Manual

Default:

Align ID and tap
 to capture.

Back Overlay Text Auto textField

This message is shown on top of the back capture screen when the backCaptureMode is set to Auto

Default:

Align ID within box and capture

Back Overlay Color textField

This value is used to color the text shown on the back capture screen. The value should be in CSS3 Hex format.

Back is Barcode Detected toggleSwitch

This flag specifies if the face detection should be enabled when the back image is captured.

Back Set Manual Timeout in Seconds textField

This value specifies after how many seconds to pass before the capture mode is switched from Auto to Manual

selfieCaptureMode dropDown**Selfie Use Back Camera textField**

This value specifies if the back camera should be used instead of the front facing camera

Selfie Overlay Text Manual textField

This message is shown on top of the selfie capture screen when the selfieCaptureMode is set to Manual

Default:

Align face and tap button</br> to capture.

Selfie Overlay Text Auto textField

This message is shown on top of the selfie capture screen when the selfieCaptureMode is set to Auto

Default:

Align face and capture

Selfie Overlay Color textField

This value is used to color the text shown on the selfie capture screen. The value should be in CSS3 Hex format.

Selfie Enable Face Detection toggleSwitch

This flag specifies if the face detection should be enabled when the selfie image is captured.

Selfie Orientation Error Text textField

This value is used when the mobile device is oriented incorrectly when selfie is being captured. The correct orientation is Portrait.

Selfie Set Manual Timeout in Seconds textField

This value specifies after how many seconds to pass before the capture mode is switched from Auto to Manual

Custom Color textField

This value is used to color all the buttons in the application. The value should in CSS3 Hex format.

Retry Count textField

Number of retries

Enable Location Detection toggleSwitch

This value specifies if GPS location should be captured and embedded in the front and back image.

Show Consent toggleSwitch

If this value is set to true then the consent screen will be shown.

Call Post Back Securely toggleSwitch

If this value is set to true then the results will be returned to the customer using a secure postback call. The postback URL should be passed in the verify request.

Transaction Expired Message textArea

Message to display when the transaction has expired

Default:

Your verification request has expired. Please contact support to start a new verification request.

Redirect URL textField

This is the url where the Digital Mobile Application will be redirected once the identity verification is completed

authenticIdDocumentType dropDown

Account Code textField required

Your AuthenticID account code.

Input Schema

- default object
 - properties object
 - baseUrl string required
 - clientCertificate string required
 - clientKey string required
 - passphrase string
 - channel string required
 - phone string
 - email string
 - channelResponse array
 - requestExpiryTimeInMin string
 - transactionExpiryTimeInMin string
 - transactionAttempts string
 - frontCaptureAttempt string
 - backCaptureAttempt string
 - selfieCaptureAttempt string
 - enableSelfieCapture boolean
 - enableFarSelfie boolean
 - focusFront string
 - focusBack string
 - glareFront string
 - glareBack string
 - reviewScreenFront boolean
 - reviewScreenBack boolean
 - logo string
 - homeScreen string
 - frontCaptureMode string
 - frontOverlayTextManual string
 - frontOverlayTextAuto string

- frontOverlayColor string
- frontEnableFaceDetection boolean
- frontSetManualTimeout string
- backCaptureMode string
- backOverlayTextManual string
- backOverlayTextAuto string
- backOverlayColor string
- backIsBarcodeDetectedEnable boolean
- backSetManualTimeout string
- selfieCaptureMode string
- selfieUseBackCamera string
- selfieOverlayTextManual string
- selfieOverlayTextAuto string
- selfieOverlayColor string
- selfieEnableFaceDetection boolean
- selfieOrientationErrorText string
- selfieSetManualTimeout string
- mailHost string
- mailPort number/string
- mailUsername string
- mailPassword string
- mailSmtpAuth boolean
- mailSmtpStarttlsEnable boolean
- emailSubject string
- emailContent string
- emailFrom string
- twilioAccountSid string
- twilioAuthToken string
- twilioFromNumber string
- twilioSmsContent string

- customColor string
- retryCount string
- enableLocationDetection boolean
- showConsent boolean
- callPostbackSecurely boolean
- transactionExpiredMessage string
- redirectURL string
- authenticIdDocumentType number/string
- accountCode number/string

Output Schema

- output object
 - challenge string
 - rawResponse object
 - url string
 - requestID string

Output Example

```
{ "challenge" : "7f83-b0c4-90e0-90b3-11e1",  
  "rawResponse" :  
    { "requestID" : "a1743e9b-bc46-4b46-9238-f950c14905de",  
      "url" : "https://cfweb.amalgam.ascendant.cloud/MWA/index.html?token=c9c11bd1-5cdd-48d9-993a-fa061e050380" } }
```

Verify Document with CFAir

Verify the authenticity of an identity document with the AuthenticID API solution, CFAir.

Properties

Account Code textField required

Your AuthenticID account code.

Document Type dropDown required

The type of identity document.

- License
- Passport

Front Image textField required

Image of the front side of the identity document, encoded as Base64 data.

Back Image textField required

Image of the back side of the identity document, encoded as Base64 data.

Transaction ID textField required

Transaction ID obtained from Authenticate Document response.

Input Schema

- default object
 - properties object
 - apiUri string required
 - accountAccessKey string required
 - secretToken string required
 - transactionID string
 - frontImageData string required
 - backImageData string
 - authenticIdDocumentTypeV2 string required
 - accountCode number/string required

Output Schema

- output object
 - rawResponse object
 - systemId string
 - ApiRequestHeaders object
 - DOCUMENTTYPE string
 - HOST string
 - RAW-REQUEST-URI string
 - TRANSFER-ENCODING string
 - USER-AGENT string
 - X-B3-TRACEID string
 - X-REQUEST-ID string
 - TransactionDate string
 - TransactionId string
 - ApiVersion integer
 - AccessKey string
 - MerchantId string
 - LocationCode string
 - DocumentImageAnalysis object
 - Front object
 - ColorSpace string
 - DPI integer
 - Back object
 - ColorSpace string
 - DPI integer
 - Result string
 - DocumentId string
 - DocumentCharacteristics object
 - Classification object
 - state string

- type string
- year string
- country string
- IssuerCode string
- IssuerCountry string
- IssuerContinent string
- IssuerRegion string
- DocumentClassName string
- Authentication object
 - imagery number
- Pass1 object
 - result_inlier object
 - angle number
 - country string
 - inliers string
 - state string
 - type string
 - year string
 - rotation integer
- Pass2 object
 - result_inlier object
 - angle integer
 - country string
 - inliers string
 - state string
 - type string
 - year string
 - rotation integer
- DocumentEncoding object
 - Label_29 string

- Label_27 string
- Label_28 string
- GivenName string
- EyeColor string
- Version string
- Label_21 string
- Label_22 string
- Label_20 string
- Label_25 string
- Label_26 string
- Label_23 string
- Label_24 string
- Label_38 string
- processed_image_height string
- Label_39 string
- Label_32 string
- Label_33 string
- processed_image_width string
- Label_30 string
- Label_31 string
- Label_36 string
- Label_37 string
- Label_34 string
- BirthDate string
- Label_35 string
- Sex string
- Height string
- Label_18 string
- Label_19 string
- Label_16 string

- Label_17 string
- Address2 string
- IssueDate string
- Address1 string
- DocumentNumber string
- Label_2 string
- Label_10 string
- Label_7 string
- Label_11 string
- Label_8 string
- Label_9 string
- Label_14 string
- Label_3 string
- Surname string
- Label_15 string
- Label_4 string
- Label_12 string
- Label_5 string
- Label_13 string
- Label_6 string
- FullName string
- DocumentMaterialAnalysis object
- DocumentImageIntegrityAnalysis object
 - PaperSplice object
 - Front object
 - Tampered number
 - IDSaturation object
 - Front object
 - Tampered number

- PrintDetector object
 - Front object
 - Tampered number
 - Natural number
- Glare object
 - Front object
 - Tampered integer
 - Back object
 - Tampered integer
- Focus object
 - Front object
 - Tampered integer
- BiometricTamper object
 - Front object
 - Tampered number
- PhotoBorderDetector object
 - Front object
 - Tampered integer
- PaperDetector object
 - Front object
 - Tampered number
- ScreenPhotoDetector object
 - Front object
 - Tampered integer
 - Back object
 - Tampered number
- PhotoSplice object
 - Front object
 - Tampered number

- CredentialDetector object
 - Front object
 - Tampered number
- PhotoStitch object
 - Front object
 - Tampered number
- DocumentImages object
 - HeadShot string
- CatfishNetUsed boolean
- DocumentFields object
 - Fused object
 - VizNative object
 - 2DBarcode object
 - Custom2DBarcode object
 - error string
 - transactionId string
- DocumentRiskVectorData object
 - Front object
 - Exif object
 - MobileSDK object
 - Back object
 - Exif object
 - MobileSDK object
- DocumentRiskConditions object
 - DQL_Default_Results object
- SegmentName string
- SegmentUiSettings string
- MatchedSegmentAlgorithms array
 - Array Item Schema string
 - Array Item Schema string

- Array Item Schema string
- Array Item Schema string
- ErrorCodes object
- ActionCodes object
 - code integer
 - actionMessage string
 - cat string
- DocumentRiskVectorAnalysis object
 - CaptureTime object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
 - FrontAndBack object
 - Result string
 - Display string
 - LocationAnalysis object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
 - FrontAndBack object
 - Result string
 - Display string

- CameraUsed object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
- DeviceOrientation object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
- CaptureMethod object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
- CaptureType object
 - Front object
 - Result string
 - Display string
 - Back object
 - Result string
 - Display string
- Result string
- ProcessingTimeInMilliseconds integer

- statusCode number
- headers object

Match Selfie to Document with CFAir

Match selfie to document with CFAir.

Properties

Transaction ID textField required

Transaction ID obtained from Authenticate Document response.

Account Code textField required

Your AuthenticID account code.

Selfie Image textField required

Selfie photo of the user, encoded as Base64 data.

Use Selfie for Liveness Check toggleSwitch

When selected, the selfie image is used to fulfill the "liveness" check instead of the regular selfie image.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - accountAccessKey string required
 - secretToken string required
 - transactionID string required
 - selfieImageData string required
 - livenessSelfie boolean required
 - accountCode number/string required

Output Schema

- output object
 - rawResponse object
 - systemId string
 - TransactionDate string
 - ApiRequestHeaders object
 - CONTENT-LENGTH string
 - HOST string
 - LOCATION string
 - RAW-REQUEST-URI string
 - REMOTE-ADDRESS string
 - TIMEOUT-ACCESS string
 - TLS-SESSION-INFO string
 - USER-AGENT string
 - X-B3-PARENTSPANID string
 - X-B3-SAMPLED string
 - X-B3-SPANID string
 - X-B3-TRACEID string
 - X-ENVOY-ATTEMPT-COUNT string
 - X-ENVOY-EXTERNAL-ADDRESS string
 - X-FORWARDED-CLIENT-CERT string
 - X-FORWARDED-FOR string
 - X-FORWARDED-PROTO string
 - X-REQUEST-ID string
 - TransactionId string
 - ApiVersion integer
 - AccessKey string
 - MerchantId string
 - ProcessingTimeInMilliseconds integer
 - LivenessSelfie boolean

- SelfieRiskVectorAnalysis object
 - CaptureTime object
 - Selfie object
 - Result string
 - Display string
 - LocationAnalysis object
 - Selfie object
 - Result string
 - Display string
 - CameraUsed object
 - Selfie object
 - Result string
 - Display string
 - DeviceOrientation object
 - Selfie object
 - Result string
 - Display string
 - CaptureMethod object
 - Selfie object
 - Result string
 - Display string
 - CaptureType object
 - Selfie object
 - ExifData null
 - Result string
 - Display string
 - AuthenticityAnalysis object
 - Selfie object
 - Result string
 - Display string

- Result string
- SelfieImageAnalysis object
 - Selfie object
 - ColorSpace string
 - Width integer
 - Height integer
 - NumFaces integer
 - Result string
- SelfieScores array
 - Array Item Schema object
 - Name string
 - VerificationScore number
- LivenessSelfieScores array
- SelfieImageIntegrityAnalysis object
 - Result string
 - PaperSplice object
 - Selfie object
 - Threshold integer
 - Result string
 - Natural number
 - Tampered number
 - PrintDetector object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered integer
 - Natural integer
 - Glare object
 - Selfie object
 - Threshold integer

- Result string
- Tampered number
- Natural number
- Focus object
 - Selfie object
 - Threshold integer
 - Result string
 - Natural number
 - Tampered number
- BiometricTamper object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered number
 - Natural number
- PhotoBorderDetector object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered integer
 - Natural integer
- NaturalCapture object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered integer
 - Natural integer
- PhotoSplice object
 - Selfie object
 - Threshold integer

- Result string
- Tampered number
- Natural number
- CredentialDetector object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered integer
 - Natural integer
 - PhotoStitch object
 - Selfie object
 - Threshold integer
 - Result string
 - Tampered number
 - Natural number
- SelfieRiskVectorData object
 - Selfie object
 - Exif object
 - Width integer
 - Height integer
 - Orientation integer
 - MobileSDK object
- SelfieDemographicData object
 - HeadShot object
 - leftEyeX integer
 - leftEyeY integer
 - rightEyeX integer
 - rightEyeY integer
 - faceScore number
 - chinX integer

- chinY integer
- yaw integer
- pitch integer
- roll integer
- iod integer
- gender string
- age integer
- ethnicity string
- glasses string
- spoof integer
- lips string
- Selfie object
 - leftEyeX integer
 - leftEyeY integer
 - rightEyeX integer
 - rightEyeY integer
 - faceScore number
 - chinX integer
 - chinY integer
 - yaw integer
 - pitch integer
 - roll integer
 - iod integer
 - gender string
 - age integer
 - ethnicity string
 - glasses string
 - spoof integer
 - lips string

- SelfieRiskConditions object
 - DQL_Default_Results object
 - DQL_Series_9000_Result string
 - DQL_FRScore1_Final_Result_Reason string
 - DQL_FRScore1_Final_Result string
 - DQL_Selfie1_Score_Result string
 - DQL_Series_9200_Result string
 - DQL_FRScore_Final_Result string
 - DQL_FarSelfie_Usable_Result_Reason string
 - DQL_Selfie1_Usable_Result_Reason string
 - DQL_Selfie1Liveness_Result string
 - DQL_FarSelfie_Liveness_Result_Reason null
 - DQL_FarSelfie_Liveness_Result string
 - DQL_Version string
 - DQL_Series_9100_Result string
 - DQL_Selfie1_Score_Result_Reason string
 - DQL_Series_9500_Result string
 - DQL_Headshot_Usable_Result string
 - DQL_Final_EnrollFace_Result null
 - DQL_FarSelfie_Usable_Result string
 - DQL_Headshot_Usable_Result_Reason string
 - DQL_Final_EnrollFace_Which_Result string
 - DQL_Series_9400_Result string
 - DQL_Selfie2Liveness_Result string
 - DQL_Selfie1_Usable_Result string
 - DQL_Selfie1Liveness_Result_Reason string
- SegmentName string
- SegmentUiSettings string
- MatchedSegmentAlgorithms array
- ErrorCodes object

- ActionCodes object
 - code integer
 - actionMessage string
 - cat string
- FRVerifications integer
- statusCode number
- headers object

Verify Identity with Mobile SDK

Verify the authenticity of an identity document with an app powered by the AuthenticID mobile SDK.

Properties

title textField

Default:

ID Verification

bodyHeaderText textField

authenticIdDocumentType dropDown

Input Schema

- default object
 - properties object
 - apiUrl string required
 - accountAccessKey string required
 - secretToken string required
 - authenticIdDocumentType number/string

Output Schema

- output object
 - challenge string
 - userReference string

Output Example

```
{ "challenge" : "7f83-b0c4-90e0-90b3-11e1",  
  "userReference" : " a1743e9b-bc46-4b46-9238-f950c14905de" }
```

Get Result from CFWeb

Get the result of an ID verification check from CFWeb.

Output Schema

- output object
 - challenge string
 - rawResponse object
 - requestID string
 - requestStatus string
 - uid string
 - transactions array

Output Example


```

{ "challenge" : "80a6e8b8-5522-416f-9f97-473e4c3c5657",
  "rawResponse" :
  { "requestID" : "95cd0d82-5e91-4b07-8006-537b0be89b57",
    "requestStatus" : "SUCCESS",
    "uid" : "001a33d6-ca1a-4fe6-a66e-3eff243f8cc8",
    "transactions" :
    [
      { "transactionID" : "Zt6ae_scvDvV0576",
        "transactionStatus" : "COMPLETED",
        "transactionSubStatus" : "COMPLETED",
        "executedDeletionRule" : false,
        "sequenceNumber" : 0,
        "statusColor" : "color:#FFFFFF;background:#008000;",
        "segmentName" : "Verified",
        "transactionDetails" :
        { "documentType" : "11",
          "homeScreen" : " ",
          "focusFront" : "30.0",
          "reviewScreenFront" : "true",
          "reviewScreenBack" : "true",
          "enableSelfieCapture" : "true",
          "enableFarSelfie" : "true",
          "transactionAttempts" : "4",
          "requestExpiryTimeInMin" : "4320",
          "transactionExpiryTimeInMin" : "60",
          "enableLocationDetection" : "true",
          "showConsent" : "true",
          "callPostbackSecurely" : "false",
          "frontEnableFaceDetection" : "true",
          "selfieEnableFaceDetection" : "true",
          "mailSmtplibAuth" : "true",
          "mailSmtplibStarttlsEnable" : "true" },
        "actionCodes" :
        { "code" : 99,
          "actionMessage" : "Please click to Continue.",
          "cat" : "Environment" },
        "pii" :
        { "Address" : "",
          "AddressCity" : "",
          "AddressPostalCode" : "",
          "AddressLine1" : "",
          "AddressLine2" : "",
          "AddressLine3" : "",
          "AddressState" : "",
          "BirthDate" : "21/May/1987",
          "BirthPlace" : "Cape Town",
          "DocumentNumber" : "234230432",
          "ExpirationDate" : "09/Jun/2028",
          "EyeColor" : "",
          "FullName" : "John Doe",
          "GivenName" : "John",
          "FirstName" : "Doe",
          "MiddleName" : "",
          "Height" : "",
          "IssueDate" : "10/Jun/2018",
          "LicenseClass" : "",
          "LicenseRestrictions" : "",
          "Sex" : "M",
          "Surname" : "Doe",
          "Weight" : ""
        }
      }
    ]
  }
}

```

```

"ClassName" : "Passport",
"DocumentName" : "Passport",
"IssuerName" : "South Africa",
"IssuerCode" : "SAF",
"DocumentIssueDate" : "2015",
"SystemDate" : "26/Feb/2021" },
"passIDThreshold" :
[
{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_General_Data_Analysis_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Generalized Data Analysis" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_SubmissionDocumentType_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Wrong ID Type Submitted" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Allowable_Doc_Type_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "On Approved List" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "EXISTS",
  "FailThreshold" : "NOTEXISTS",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "",
  "Name" : "ID - System Processing Failure" },

{ "Category" : "DATE ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Min_Age_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Minimum Age Requirement" },

{ "Category" : "ID INTEGRITY ANALYSIS",

```

```

    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Materials_Replica_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Materials Analysis" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "SelfieRiskConditions",
      "DQL_Default_Results",
      "DQL_Selfie1Liveness_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Liveness Assessment 1" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "SelfieRiskConditions",
      "DQL_Default_Results",
      "DQL_Selfie1_Score_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Selfie - Facial Recognition Matching" },

  { "Category" : "FRAUD SHIELD",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Data_Source1_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Data Matching" },

  { "Category" : "DATE ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_ID_About_To_Expire_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Expiring Soon" },

  { "Category" : "MINIMUM PII EXTRACTED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Final_Minimum_PII_Result" ],
    "ScoreSegmentResult" : "PASS",

```

```

    "IDESystemScore" : "Passed",
    "Name" : "Final PII - minimum extracted" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_HeadshotExtracted_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "ID Headshot Extracted" },

{ "Category" : "ID INTEGRITY ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Front_Color_Analysis_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Color Analysis" },

{ "Category" : "DATE ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_ID_Expired_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Already Expired" },

{ "Category" : "SELFIE AND LIVENESS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FarSelfie_Liveness_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Liveness Assessment 2" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_Selfie1_Usable_Result" ],
  "ScoreSegmentResult" : "PASS",
  "IDESystemScore" : "Passed",
  "Name" : "Selfie Usable" },

{ "Category" : "ID INTEGRITY ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :

```

```

    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Pattern_Analysis_Result" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : "Passed",
    "Name" : "Visual Pattern Assessment" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : ">=250",
    "FailThreshold" : "<250",
    "CatFishReferenceField" :
    [ "DocumentImageAnalysis",
      "Front",
      "DPI" ],
    "ScoreSegmentResult" : "PASS",
    "IDESystemScore" : 295,
    "Name" : "Minimum DPI Requirements" } ],
  "failIDThreshold" :
  [ ],
  "uncertainIDThreshold" :
  [
    { "Category" : "PII DATA ANALYSIS",
      "PassThreshold" : "Passed",
      "FailThreshold" : "Failed",
      "CatFishReferenceField" :
      [ "DocumentRiskConditions",
        "DQL_Default_Results",
        "DQL_FTB_ExpirationDate_Result" ],
      "ScoreSegmentResult" : "N/A",
      "IDESystemScore" : "Disabled",
      "Name" : "Expiration Date - Front-To-Back Analysis" },

    { "Category" : "PII DATA ANALYSIS",
      "PassThreshold" : "Passed",
      "FailThreshold" : "Failed",
      "CatFishReferenceField" :
      [ "DocumentRiskConditions",
        "DQL_Default_Results",
        "DQL_Street_Front_To_Back_Result" ],
      "ScoreSegmentResult" : "N/A",
      "IDESystemScore" : "Disabled",
      "Name" : "Street Address - Front to Back" },

    { "Category" : "PII DATA ANALYSIS",
      "PassThreshold" : "Passed",
      "FailThreshold" : "Failed",
      "CatFishReferenceField" :
      [ "DocumentRiskConditions",
        "DQL_Default_Results",
        "DQL_City_Front_To_Back_Result" ],
      "ScoreSegmentResult" : "N/A",
      "IDESystemScore" : "Disabled",
      "Name" : "City - Front to Back" },

    { "Category" : "SELFIE AND LIVENESS",
      "PassThreshold" : "EXISTS",
      "FailThreshold" : "NOTEXISTS",
      "CatFishReferenceField" :
      [ "SelfieScores",
        "VerificationScore" ],
      "ScoreSegmentResult" : "N/A",
      "IDESystemScore" : "Disabled",

```

```

    "Name" : "Selfie Received" },

{ "Category" : "SELFIE AND LIVENESS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_PassiveSelfie_LIFO_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Passive Selfie - LIFO" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_LastName_SpecialCharacter_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Last Name - Special Characters" },

{ "Category" : "MINIMUM PII EXTRACTED",
  "PassThreshold" : "<90",
  "FailThreshold" : ">=98",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "BiometricTamper",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Biometric Tamper (Replaced)" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "<90",
  "FailThreshold" : ">99",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "Focus",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Focus - Front (Info Only)" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : ">=75",
  "FailThreshold" : "<75",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "BiographicSplice",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Biographic Splice" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "Passed",

```

```

    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Useful_Output_Result2" ],
    "ScoreSegmentResult" : "INFO ONLY",
    "IDESystemScore" : "Info Only",
    "Name" : "Information - Address" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_ID_Cropping_Exception_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Cropping and Capture Issues" },

  { "Category" : "SELFIE AND LIVENESS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "SelfieRiskConditions",
      "DQL_Default_Results",
      "DQL_Overall_Liveness_Conclusion_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Liveness 1 and 2 Fused Conclusion" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : ">=250",
    "FailThreshold" : "<250",
    "CatFishReferenceField" :
    [ "DocumentImageAnalysis",
      "Back",
      "DPI" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "DPI Resolution - Back" },

  { "Category" : "UNUSED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskVectorAnalysis",
      "CaptureTime",
      "Back",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Capture Time - Back" },

  { "Category" : "ID INTEGRITY ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Headshot_Modification_Result" ],
    "ScoreSegmentResult" : "N/A",

```

```

    "IDESystemScore" : "Disabled",
    "Name" : "Headshot Integrity Analysis" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_State_SpecialCharacter_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "State - Special Characters" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Useful_Output_Result1" ],
  "ScoreSegmentResult" : "INFO ONLY",
  "IDESystemScore" : "Info Only",
  "Name" : "Information - Name and Dates" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FR_LIFO_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Fused FR - LIFO" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FR_BestCase_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Fused FR - Best Case" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_PostalCode_SpecialCharacter_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Postal Code - Special Characters" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :

```



```

[ "DocumentRiskVectorAnalysis",
  "DeviceOrientation",
  "Front",
  "Result" ],
"ScoreSegmentResult" : "N/A",
"IDESystemScore" : "Disabled",
"Name" : "Device Orientation - Front" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "<100",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "TextBlurOcclusion",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Blur or Occlusion" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskVectorAnalysis",
    "DeviceOrientation",
    "Selfie",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Orientation Analysis - Selfie" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Speciality_Document_Analysis_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Speciality Document Analysis" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL-Allowable_Doc_Type_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Allowable Document Type" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_GPS_Low_Result" ],
  "ScoreSegmentResult" : "N/A",

```

```

    "IDESystemScore" : "Disabled",
    "Name" : "GPS Risk - Low" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_UsableSelfie_Fused_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Headshot Usable" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskVectorAnalysis",
    "CaptureTime",
    "Front",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Capture Time - Front" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_IdentityDocumentType_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Unused" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_FTB_BirthDate_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Birth Date - Front-To-Back Analysis" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskVectorAnalysis",
    "CaptureTime",
    "Selfie",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Capture Time - Selfie" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",

```

```

    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_GPS_Restricted_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "GPS Risk - Restricted" },

  { "Category" : "UNUSED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskVectorAnalysis",
      "CaptureType",
      "Front",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Capture Type - Front" },

  { "Category" : "USEFUL INFORMATION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Compromised_Document_Analysis_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Compromised Document Analysis" },

  { "Category" : "PII DATA ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_DocumentNumber_Analysis_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Document Number Integrity Analysis" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "SelfieRiskVectorAnalysis",
      "CameraUsed",
      "Selfie",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Camera Used - Selfie" },

  { "Category" : "PII DATA ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Gender_Result" ],

```

```

    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Missing Fullname Data" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "<95",
  "FailThreshold" : ">99",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "Glare",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Glare - Front (Info Only)" },

{ "Category" : "UNUSED",
  "PassThreshold" : "<=99",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "PaperDetector",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Advanced Paper Detection" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Biographic_Fused_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Biographic Tamper Conclusion" },

{ "Category" : "FRAUD SHIELD",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Face_Source1_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Headshot Matching" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "<50",
  "FailThreshold" : ">50",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "TinyOcclusion",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Tiny Occlusion" },

```

```

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "<100",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "MachineReadable",
    "Back",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Machine Readable" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FR_Avg_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Fused FR - Average Score" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_FTB_FullName_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "FullName - Front-To-Back Analysis" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Image_EXIF_Issue_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Manipulated During Transmission" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_PostalCode_Front_To_Back_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Postal Code - Front to Back" },

{ "Category" : "FRAUD SHIELD",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",

```

```

    "DQL_Velocity_Source1_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Velocity Analysis" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_State_Front_To_Back_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "State - Front to Back" },

{ "Category" : "MINIMUM PII EXTRACTED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_2D_Minimum_PII_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Barcode Data - minimum extracted" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "EXISTS",
  "FailThreshold" : "NOTEXISTS",
  "CatFishReferenceField" :
  [ "SelfieScores" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "ID Photo Usable" },

{ "Category" : "DATE ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_ExpirationDate_Info_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "ID Expiration" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "Personal_Info_Analysis" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Personal Information Analysis" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :

```

```

[ "DocumentRiskConditions",
  "DQL_Default_Results",
  "DQL_Allowable_GPS_Result" ],
"ScoreSegmentResult" : "N/A",
"IDSystemScore" : "Disabled",
"Name" : "Allowable GPS Location" },

{ "Category" : "ID INTEGRITY ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Visual_Image_Analysis_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDSystemScore" : "Disabled",
  "Name" : "Visual Image Analysis" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_CheckDigit_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDSystemScore" : "Disabled",
  "Name" : "Check Digit Assessment" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_FTB_DocumentNumber_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDSystemScore" : "Disabled",
  "Name" : "Document Number - Front-To-Back Analysis" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskVectorAnalysis",
    "DeviceOrientation",
    "Back",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDSystemScore" : "Disabled",
  "Name" : "Device Orientation - Back" },

{ "Category" : "MINIMUM PII EXTRACTED",
  "PassThreshold" : "<90",
  "FailThreshold" : ">=100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "PhotoSplice",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDSystemScore" : "Disabled",

```

```

    "Name" : "Biometric Splice (Replaced)" },

{ "Category" : "MINIMUM PII EXTRACTED",
  "PassThreshold" : "<95",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "PhotoStitch",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Photo Stitch (Replaced)" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Allowable_State_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Allowable State" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_LastName_Front_To_Back_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Last Name - Front to Back" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_MiddleName_Front_To_Back_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Middle Name - Front to Back" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_Overall_FR_Conclusion_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "FR Conclusion" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :

```



```

    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Dates_Validity_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Are the ID Dates Valid" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "<=30",
    "FailThreshold" : ">40",
    "CatFishReferenceField" :
    [ "SelfieImageIntegrityAnalysis",
      "PhotoBorderDetector",
      "Selfie",
      "Tampered" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Photo Integrity - Selfie" },

  { "Category" : "UNUSED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskVectorAnalysis",
      "CaptureType",
      "Back",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Capture Type - Back" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "<=30",
    "FailThreshold" : ">40",
    "CatFishReferenceField" :
    [ "SelfieImageIntegrityAnalysis",
      "CredentialDetector",
      "Selfie",
      "Tampered" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Credential Integrity - Selfie" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Back_Color_Analysis_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "ColorSpace Analysis - Back" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : ">=40",
    "FailThreshold" : "<30",
    "CatFishReferenceField" :
    [ "SelfieRiskConditions",
      "DQL_Default_Results",
      "DQL_FRScore_Final_Result" ],
    "ScoreSegmentResult" : "N/A",

```

```

    "IDESystemScore" : "Disabled",
    "Name" : "Facial Recognition #1" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : ">=40",
  "FailThreshold" : "<=39",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FR_Score2_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Facial Recognition #2" },

{ "Category" : "UNUSED",
  "PassThreshold" : "<=94",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentMaterialAnalysis",
    "PolyCarbonate",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Advanced Polycarbonate Materials Detection" },

{ "Category" : "ID INTEGRITY ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Doc_Classified_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Document Classified" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskVectorAnalysis",
    "AuthenticityAnalysis",
    "Selfie",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Authenticity Capture - Selfie" },

{ "Category" : "ID IMAGE USABLE",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_2D_Usable_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Barcode Integrity" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : ">=40",

```

```

    "FailThreshold" : "<=39",
    "CatFishReferenceField" :
    [ "SelfieRiskConditions",
      "DQL_Default_Results",
      "DQL_FR_Score3_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Facial Recognition #3" },

  { "Category" : "ALLOWABLE ID",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Type_Allowed_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "DL Type Allowed" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "SelfieRiskVectorAnalysis",
      "CaptureType",
      "Selfie",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Capture Type - Selfie" },

  { "Category" : "UNUSED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskVectorAnalysis",
      "LocationAnalysis",
      "FrontAndBack",
      "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Location Analysis - Front And Back" },

  { "Category" : "ALLOWABLE ID",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_GPS_Med_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "GPS Risk - Med" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Environment_Impact_Result" ],

```

```

    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Environment Condition Analysis" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_FTB_Address_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Full Address - Front-To-Back Analysis" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_FirstName_SpecialCharacter_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "First Name - Special Characters" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_BirthDate_Info_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Birth Date Integrity" },

{ "Category" : "UNUSED",
  "PassThreshold" : "<99",
  "FailThreshold" : ">=99",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "ScreenPhotoDetector",
    "Back",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Screen Photo Detector - Back" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "<100",
  "FailThreshold" : ">100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "TinyText",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Tiny Text" },

{ "Category" : "ALLOWABLE ID",

```

```

    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Temporary_PaperID_Override_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Temporary DMV ID Submission" },

  { "Category" : "USEFUL INFORMATION",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Useful_Output_Result3" ],
    "ScoreSegmentResult" : "INFO ONLY",
    "IDESystemScore" : "Info Only",
    "Name" : "Information - Classification and Scores" },

  { "Category" : "ID INTEGRITY ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Layout_Analysis_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Layout Analysis" },

  { "Category" : "PII DATA ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_FTB_IssueDate_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Issue Date - Front-To-Back Analysis" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Customer_Declined_ID_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Customer Declined ID Verification" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "<90",
    "FailThreshold" : ">99",
    "CatFishReferenceField" :
    [ "DocumentImageIntegrityAnalysis",
      "Focus",
      "Back",
      "Tampered" ],

```

```

    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Focus - Back (Info Only)" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_IssueDate_Info_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Issue Date Integrity" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskVectorAnalysis",
    "CaptureTime",
    "FrontAndBack",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Capture Time - Front and Back" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskVectorAnalysis",
    "CameraUsed",
    "Front",
    "Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Camera Used - Front" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_GPS_High_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "GPS Risk - High" },

{ "Category" : "MINIMUM PII EXTRACTED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_VIZ_Minimum_PII_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "OCR - minimum extracted" },

{ "Category" : "ID IMAGE USABLE",

```

```

    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Overall_ID_Conclusion_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "ID Usable Image Conclusion" },

  { "Category" : "ALLOWABLE ID",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_Overall_IDAllowable_Conclusion_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Allowable ID Conclusion" },

  { "Category" : "PII DATA ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_City_SpecialCharacter_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "City - Special Characters" },

  { "Category" : "ID INTEGRITY ANALYSIS",
    "PassThreshold" : "<99",
    "FailThreshold" : ">=99",
    "CatFishReferenceField" :
    [ "DocumentImageIntegrityAnalysis",
      "DigitalReproduction",
      "Front",
      "Tampered" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Digital Reproduction (Replaced)" },

  { "Category" : "MINIMUM PII EXTRACTED",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_MRZ_Minimum_PII_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "MRZ Data - minimum extracted" },

  { "Category" : "ID IMAGE USABLE",
    "PassThreshold" : "<95",
    "FailThreshold" : ">99",
    "CatFishReferenceField" :
    [ "DocumentImageIntegrityAnalysis",
      "Glare",
      "Back",

```

```

    "Tampered" ],
    "ScoreSegmentResult" : "N/A",
    "IDESystemScore" : "Disabled",
    "Name" : "Glare - Back (Info Only)" },

{ "Category" : "FRAUD SHIELD",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Face_Source2_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "3rd Party - Headshot Matching" },

{ "Category" : "ID INTEGRITY ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Structural_Image_Assessment_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Digital Reproduction Assessment" },

{ "Category" : "UNUSED",
  "PassThreshold" : "<100",
  "FailThreshold" : ">=100",
  "CatFishReferenceField" :
  [ "DocumentImageIntegrityAnalysis",
    "ScreenPhotoDetector",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Screen Photo Detector - Front" },

{ "Category" : "UNUSED",
  "PassThreshold" : ">50",
  "FailThreshold" : "<=50",
  "CatFishReferenceField" :
  [ "DocumentMaterialAnalysis",
    "IDSaturation",
    "Front",
    "Tampered" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Paper Analysis" },

{ "Category" : "FACIAL RECOGNITION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "SelfieRiskConditions",
    "DQL_Default_Results",
    "DQL_FR_WorstCase_Result_Reason" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Fused FR - Worst Case" },

```



```

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_DOBsymbol_Analysis_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "HKID DOB Symbol Analysis" },

{ "Category" : "USEFUL INFORMATION",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Useful_Output_Result4" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Information - MRZ" },

{ "Category" : "FRAUD SHIELD",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_Data_Source2_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "3rd Party - Data Matching" },

{ "Category" : "ALLOWABLE ID",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_GPS_Usable_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "GPS Is Usable ( Usable GPS )" },

{ "Category" : "PII DATA ANALYSIS",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskConditions",
    "DQL_Default_Results",
    "DQL_SpecialCharacter_Analysis_Result" ],
  "ScoreSegmentResult" : "N/A",
  "IDESystemScore" : "Disabled",
  "Name" : "Potentially Incomplete Fullname" },

{ "Category" : "UNUSED",
  "PassThreshold" : "Passed",
  "FailThreshold" : "Failed",
  "CatFishReferenceField" :
  [ "DocumentRiskVectorAnalysis",
    "CameraUsed",
    "Back",

```

```

    "Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDSystemScore" : "Disabled",
    "Name" : "Camera Used - Back" },

  { "Category" : "PII DATA ANALYSIS",
    "PassThreshold" : "Passed",
    "FailThreshold" : "Failed",
    "CatFishReferenceField" :
    [ "DocumentRiskConditions",
      "DQL_Default_Results",
      "DQL_ExpirationDate_Info_Result" ],
    "ScoreSegmentResult" : "N/A",
    "IDSystemScore" : "Disabled",
    "Name" : "Expiration Date Integrity" },

  { "Category" : "FACIAL RECOGNITION",
    "PassThreshold" : "<=30",
    "FailThreshold" : ">40",
    "CatFishReferenceField" :
    [ "SelfieImageIntegrityAnalysis",
      "NaturalCapture",
      "Selfie",
      "Tampered" ],
    "ScoreSegmentResult" : "N/A",
    "IDSystemScore" : "Disabled",
    "Name" : "Natural Capture - Selfie" } ] ] ] } }

```

Azure AD User Management Connector

The Azure AD User Management connector lets you manage users, groups, and software licenses in your PingOne DaVinci flow.

You can use the Azure AD User Management connector to:

- Query user information
- Create, update, and delete users
- List the users in a group
- Add and remove group members
- Add and remove software licenses and disable plans

Setup

Resources

For information and setup help, see the following:

- Microsoft documentation:
 - [Register an application with the Microsoft identity platform](#)

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need administrator access to Microsoft Azure.

Setting up Azure AD

1. Sign on to the [Azure portal](#).
2. Create the application:
 1. Search for and select **Azure Active Directory**.
 2. Under **Manage**, select **App registrations** → **New registration**.
 3. On the **Register an Application** page, for **Supported account types**, select **Accounts in any organizational directory and personal Microsoft accounts**.
 4. Leave the **Redirect URI** field blank.
 5. Click **Register**.

[Home](#) > [Ping Identity | App registrations](#) >

Register an application ...

*** Name**

The user-facing display name for this application (this can be changed later).

PingOne DaVinci 

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Ping Identity only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☒ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform 

3. On your app's **Overview** page, note the **Application (client) ID** and **Directory (tenant) ID**. You'll use these in the connector configuration.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb navigation shows 'Home > Ping Identity | App registrations >'. The main heading is 'PingOne DaVinci'. Below this, there are three tabs: 'Delete', 'Endpoints', and 'Preview features'. A message banner says 'Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer).'. Under the 'Essentials' section, the following details are listed:

- Display name: [PingOne DaVinci](#)
- Application (client) ID: **5db65414-a030-4082-852c-213aef4329f2**
- Object ID: **e4ba22d4-7815-4239-9d12-93ec4efd943**
- Directory (tenant) ID: **07ec9af2-7ce5-4ab7-8638-115736bbf990**
- Supported account types: [All Microsoft account users](#)

4. Create a client secret:

1. Under **Manage**, click **Certificates & secrets**. On the **Client secrets** tab, click **New client secret**.
2. Enter a name and select an expiry time. Click **Add**.
3. Note the **Value** of the secret. You'll use this in the connector configuration.

The screenshot shows the 'Client secrets' tab in the Azure portal. It has three tabs: 'Certificates (0)', 'Client secrets (1)', and 'Federated credentials (0)'. Below the tabs, there's a description: 'A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.' There's a '+ New client secret' button. Below that is a table with the following columns: 'Description', 'Expires', 'Value', and 'Secret ID'.

Description	Expires	Value	Secret ID
DaVinci	8/10/2024	jMD8Q~GwvnrWLnj~p30nc0N ...	5c0e4e15-a241-4e12-860c-cb ...

5. Give the connector permission to manage users and send messages:

1. Under **Manage**, click **API permissions**.
2. Click **Add a permission** and add the following Microsoft Graph API permissions:

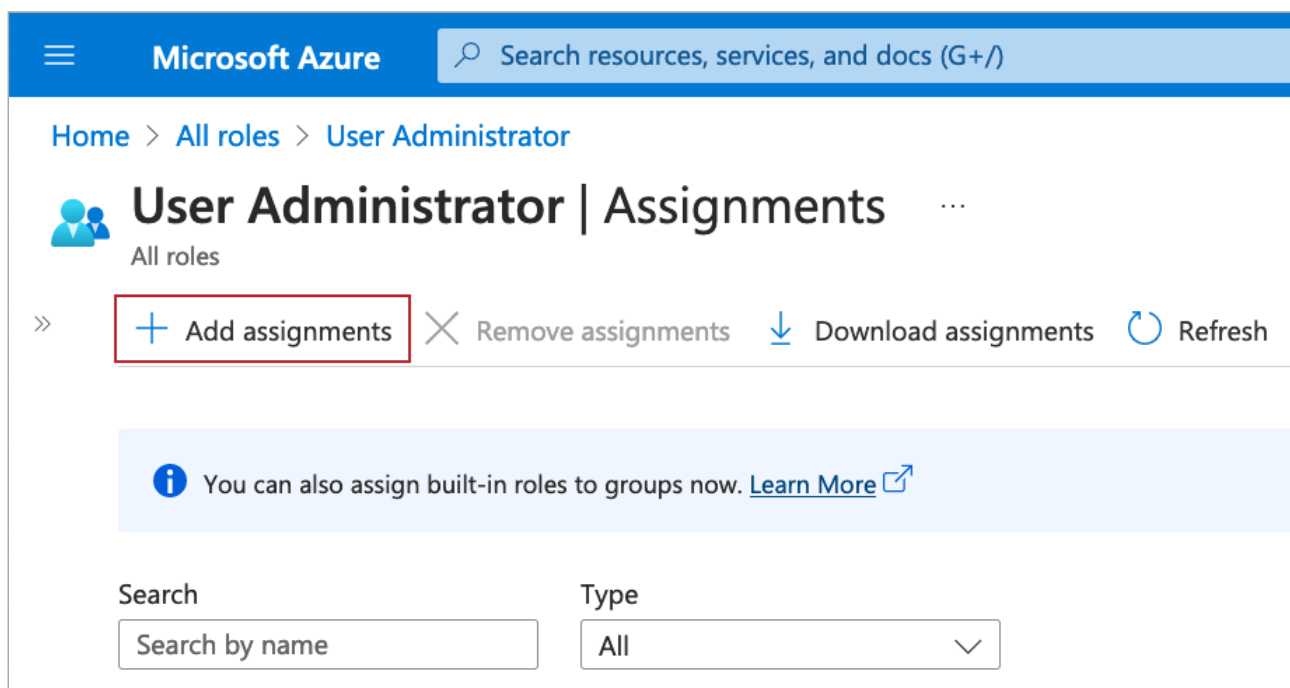
Application permissions

Permission	Type
Directory.Read.All	Application
Directory.ReadWrite.All	Application
Group.Read.All	Application
Group.ReadWrite.All	Application
GroupMember.Read.All	Application
GroupMember.ReadWrite.All	Application
User.EnableDisableAccount.All	Application
User.ManageIdentities.All	Application
User.Read.All	Application
User.ReadWrite.All	Application

3. Click **Grant admin consent for <your organization>**.

6. Grant your application the User Administrator role:

1. In the Azure portal, search for and select **Azure AD roles and administrators**.
2. On the **All Roles** list, search for and select **User Administrator**.
3. On the **User Administrator > Assignments** page, click **Add assignments**.



4. Search for and select your application. Click **Add**.

Configuring the Azure AD User Management connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Client ID

The **Application (client) ID** that you noted in [Setting up Azure AD](#).

Client Secret

The client secret **Value** that you noted in [Setting up Azure AD](#).

Tenant ID

The **Directory (tenant) ID** that you noted in [Setting up Azure AD](#).

Using the connector in a flow

Get user attributes based on a query

The **Query Users** capability allows you to get information about one or more users based on a query function.

This capability queries the Azure AD **users** endpoint. You can select certain user attributes, and filter, order, or format the results. For help creating a query, see [Use query parameters](#) and [Advanced query capabilities](#) in the Microsoft documentation.

Enter queries in the **Query Parameters** field. See the following table for examples.

Example queries

Description	Query Parameters
List users whose given name starts with J.	<code>\$filter=startswith(givenName, 'J')</code>
Get users' given name and surname only.	<code>\$select=givenName,surname</code>
Combined query: List users whose given name starts with J and get their given name and surname only.	<code>\$filter=startswith(givenName%2C+'J')&\$select=givenName,surname</code>

List changes to users since a previous query

The **Query User Changes** capability allows you to get information about one or more users based on a query function, then repeat the same query one or more times and only receive the information that has changed since the previous query. This includes data that has been created, modified, or deleted. Because only changes are included, the query runs more quickly and can provide valuable or actionable results. For more information about this function, see [Get delta](#) in the Graph API documentation.

In your initial request, you can specify a set of query parameters. You'll receive the requested information, as well as a **deltaLink** URL, which includes a delta token. In subsequent requests, you only need to provide the delta token as a parameter. The results include any changed data that matches the original query parameters.

Microsoft provides a limited query options for this function. For details, see the [Query parameters](#) section of the [Get delta](#) topic in the Graph API documentation.

1. Define and test your query parameters:

1. Create a flow and add an **Azure AD User Management** with the **Query User Changes** capability.
2. In the **Query Parameters** field, enter your initial query parameters to define the user information you want to track. For example:

```
$select=givenName,surname
```

3. Add an HTTP connector with the **Custom HTML Message** and use it to display the *output* variable from the **Query User Changes** node. Click **Apply**.

The image shows a configuration panel for a message node. It has a light gray background and a dark gray border on the right. There are three main sections, each with a title and a text input field:

- Message**: The first section has a title "Message" in bold. Below it is a large, empty text input field. To the right of the field is a circular icon containing a lock symbol.
- Message CSS**: The second section has a title "Message CSS" in bold. Below it is a large, empty text input field. To the right of the field is a circular icon containing a document/copy symbol.
- Message Icon URL**: The third section has a title "Message Icon URL" in bold. Below it is a large, empty text input field. To the right of the field is a circular icon containing a lock symbol.

4. Click **Save**, **Deploy**, and **Try Flow**.

5. In the output, check that your queries return the information that you want.

2. Get the delta token:

1. Open the **Query User Changes** node for editing.

2. In the **Query Parameters** field, add the parameter to get the delta token. For example:

```
$deltaToken=latest&$select=givenName,surname
```

3. In the **Custom HTML Message** node, remove the *output* variable and add the *deltaToken* variable.

4. Click **Save**, **Deploy**, and **Try Flow**.

5. In the output, copy the delta token parameter. For example:

```
$deltatoken=slyJnDHUp6df3Y...nT1LF0VXPjexmCk2a
```

3. Use the delta token to make subsequent requests:

1. Create a new flow and add an **Azure AD User Management** with the **Query User Changes** capability.

2. In the **Query Parameters** field, enter your delta token parameter only. For example:

```
$deltaToken=slyJnDHUp6df3Y...nTlLF0VXPjexmCk2a
```

3. Add an HTTP connector with the **Custom HTML Message** and use it to display the *output* variable from the **Query User Changes** node. Click **Apply**.
4. Click **Save**, **Deploy**, and **Try Flow**.
5. In the output, see the list of user attributes that have been created, modified, or deleted since you generated the delta token.

User management

The connector has several capabilities that allow you to manage users:

- Read User
- Create User
- Update User
- Delete User

No special configuration is needed. Add the capability and populate its properties according to the help text.

Group membership management

The connector has several capabilities that allow you to manage the groups that a user is part of:

- List User's Groups
- Add User to Group
- Remove User From Group

No special configuration is needed. Add the capability and populate its properties according to the help text.

Manage user licenses

The **Manage User License** capability lets you select a user and define one or more licenses to add, remove, or disable for that user.

For more information, see [user: assignLicense](#) in the Graph API documentation.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Query Users

Get user attributes based on a custom query.

Properties

Query Parameters `textField`

Customize your request with a user filter or query, such as "\$select=displayName,givenName,postalCode". See 'User Query' in the Graph API documentation for help. This field is optional.

Input Schema

default object

clientId string

clientSecret string

tenantId string

userQuery string

Output Schema

output object

rawResponse object

properties object

@odata.context string

@odata.nextLink string

value array

items array

type object

properties

statusCode integer

Query User Changes

Get user attributes based on an initial query, then run subsequent queries to get a list of attributes that have been created, modified, or deleted since the initial query. See 'user: Delta' in the Graph API documentation for help.

Properties

Query Parameters `textField`

Customize your request with a user filter or query, such as "\$select=displayName,givenName,postalCode". See 'User Query' in the Graph API documentation for help. This field is optional.

Input Schema**default** object**clientId** string**clientSecret** string**tenantId** string**userQuery** string**Output Schema****output** object**rawResponse** object**properties** object**@odata.context** string**@odata.nextLink** string**@odata.deltaLink** string**skiptoken** string**deltatoken** string**value** array**items** array**type** object**properties****statusCode** integer**Read User**

Select a single user to get all of their attributes.

Properties**User dropDown required**

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's principal name, such as "[jsmith@example.com](#)" or "144c6d7e-ef33-46b8-847a-7021943e9900".

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

Output Schema

output object

rawResponse object

properties object

businessPhones array

displayName string

givenName string

jobTitle string

mail string

mobilePhone string

officeLocation string

preferredLanguage string

surname string

userPrincipalName string

id string

statusCode integer

Create User

Create a new user account

Properties

***Account Enabled* toggleSwitch required**

When enabled, the new account is enabled and ready to use.

***Display Name* textField required**

The name to display in the address book for the user.

***Mail Nickname* textField required**

The mail alias for the user, such as "jsmith".

***Principal Name* textField required**

The user's principal name, such as "[jsmith@example.com](#)".

***Password* textField required**

The user's password

Force Change Password toggleSwitch

When enabled, the user must set a new password the next time they sign on.

Force Change Password with MFA toggleSwitch

When enabled, the user must authenticate with MFA then set a new password the next time they sign on.

Other Attributes variableInputList

Define additional attributes to add to the user account.

Input Schema

default object

clientId string

clientSecret string

tenantId string

createUserAccountEnabled boolean

createUserDisplayName string

createUserMailNickname string

createUserPrincipalName string

forceChangePasswordNextSignIn boolean

forceChangePasswordNextSignInWithMfa boolean

createUserPassword string

Output Schema

output object

rawResponse object

properties object

@odata.context string

id string

businessPhones array

displayName string

givenName string

jobTitle string

mail string

mobilePhone string

officeLocation string

preferredLanguage string

surname string

userPrincipalName string

statusCode integer

Update User

Update information about a user.

Properties

User dropdown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's principal name, such as "jsmith@example.com" or "144c6d7e-ef33-46b8-847a-7021943e9900".

Given Name textField

The given name (first name) of the user

Surname textField

The user's surname (family name or last name).

Display Name textField

The name to display in the address book for the user.

Password textField

The user's password.

Force Change Password toggleSwitch

When enabled, the user must set a new password the next time they sign on.

Force Change Password with MFA toggleSwitch

When enabled, the user must authenticate with MFA then set a new password the next time they sign on.

Country textField

The user's country, in ISO 3166-1 alpha-2 format, such as "US".

State or Province textField

The user's state or province, such as "WA".

City textField

The user's city, such as "Seattle".

Department textField

The user's department, such as "Accounting".

Employee ID textField

The user's employee identifier, such as "A2304884". Maximum length is 16 digits.

Mail textField

The user's SMTP address, such as "jsmith@example.com". Changes to this property will also update the user's proxyAddresses collection to include the value as an SMTP address.

Other Attributes variableInputList

Define additional attributes to add to the user account.

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

displayName string

accountEnabled boolean

password string

forceChangePasswordNextSignIn boolean

forceChangePasswordNextSignInWithMfa boolean

givenName string

surname string

country string

state string

city string

department string

employeeId string

mail string

Output Schema

output object

rawResponse object

properties object

ok

statusCode integer

Delete User

Delete a user account

Properties

User dropdown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's principal name, such as "[jsmith@example.com](#)" or "144c6d7e-ef33-46b8-847a-7021943e9900".

Input Schema

default object

userId string

clientId string

clientSecret string

tenantId string

Output Schema

output object

rawResponse object

properties object

ok

statusCode integer

Manage User License

Manage a user's access to products by adding, removing, or disabling licenses.

Properties

User dropdown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's principal name, such as "[jsmith@example.com](#)" or "144c6d7e-ef33-46b8-847a-7021943e9900".

Remove License textField

The ID for the license that you want to revoke, such as ["bea13e0c-3828-4daa-a392-28af7ff61a0f"]. Separate multiple IDs with a comma.

Default:

[" "]

Add License textField

The SKU ID for the license that you want to grant, such as "45715bb8-13f9-4bf6-927f-ef96c102d394".

Disable Plan textField

The ID of a plan associated with the new license, such as ["11b0131d-43c8-4bbb-b2c8-e80f9a50834a"]. Separate multiple IDs with a comma.

Default:

```
[ " " ]
```

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

removeLicenses array

skuld string

disabledPlans array

Output Schema

output object

rawResponse object

properties object

accountEnabled boolean

assignedLicenses array

items array

type object

properties

assignedPlans array

items array

type object

properties

businessPhones array

items array

type string

city string

companyName string

statusCode integer

headers object

List User's Groups

Get a list of groups that a user belongs to.

Properties

User dropdown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's principal name, such as "[jsmith@example.com](#)" or "144c6d7e-ef33-46b8-847a-7021943e9900".

Limit to Security Groups toggleSwitch required

When enabled, the request only lists the user's security groups.

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

Output Schema

output object

rawResponse object

properties object

@odata.context string

value array

items array

type string

statusCode integer

Add User to Group

Add a member to a security or Microsoft 365 group.

Properties

User dropdown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's ID such as "144c6d7e-ef33-46b8-847a-7021943e9900".

Group dropDown required

The group to target. For a dynamic value, select Use Group ID and enter a value in the Use Group ID field.

- Use Group ID

Group textField

The id of the group, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

groupId string

Output Schema

output object

rawResponse object

properties object

ok

statusCode integer

Remove User From Group

Remove a user from a group.

Properties

Group dropDown required

The group to target. For a dynamic value, select Use Group ID and enter a value in the Use Group ID field.

- Use Group ID

Group textField

The id of the group, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

User dropDown required

The user to target. For a dynamic value, select Use User ID and enter a value in the User ID field.

- Use User ID

User ID textField

The user's ID such as "144c6d7e-ef33-46b8-847a-7021943e9900".

Input Schema

default object

clientId string

clientSecret string

tenantId string

userId string

groupId string

Output Schema

output object

rawResponse object

properties object

ok

statusCode integer

Make a Custom API Call

Define and use your own call to the Microsoft Graph API

Properties

Endpoint textField required

The Microsoft Graph API endpoint, such as "/user". This endpoint is added to the base API URL selected in the connector configuration.

HTTP Method dropDown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE
- PATCH

Body codeEditor

The body of the API call.

Input Schema

default object

clientId string

clientSecret string

tenantId string

endpoint string

method string

customQueryParams array

headers array

bodyData object

Output Schema

output object

rawResponse object

statusCode integer

headers object

Azure AD User Management Connector Release Notes

New features and improvements in the Azure AD User Management connector.

March 2023

The Azure AD User Management connector is now available

New

You can use the Azure AD User Management connector to:

- Query user information
- Create, update, and delete users
- List the users in a group
- Add and remove group members
- Add and remove software licenses and disable plans

Castle Connector

The Castle connector lets you add additional risk signals with Castle's fraud and risk management platform in your PingOne DaVinci flow.

You can use the Castle connector to:

- Filter registration and login traffic to block bots and bad traffic

- Request a risk evaluation from Castle's API

Setup

Resources

For information and setup help, see the following:

- Castle documentation:
 - [Introduction to Castle](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A Castle license
- Your Castle credentials

Setting up Castle

Follow the instructions in the [Castle documentation](#).

Configuring the Castle connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

API Secret

Your 32-character Castle API secret, for example, `01c3...YIBF`.

Using the connector in a flow

Registration and Login Traffic Filtration

You can use the **Filter Registration and Login Traffic** capability to block bots and bad traffic early in the request chain based on context and user information.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Risk evaluation

You can use the **Get Risk Evaluation** capability to request a risk evaluation from Castle's API.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Filter registration and login traffic

Used to block bots and bad traffic early in the request chain, typically at registration.

Properties

Body codeEditor required

The raw JSON body, such as "{ \"Username\": \"jsmith@example.com\", \"Session ID\": \"00e8a0000024zkjAAA\" }\".

Output Schema

output object

rawResponse object

statusCode number

headers object

status string

Risk Evaluation

Used to request a risk evaluation from Castle's API

Properties

Body codeEditor required

The raw JSON body, such as "{ \"Username\": \"jsmith@example.com\", \"Session ID\": \"00e8a0000024zkjAAA\" }\".

Output Schema

output object

rawResponse object

statusCode number

headers object

Challenge Connector

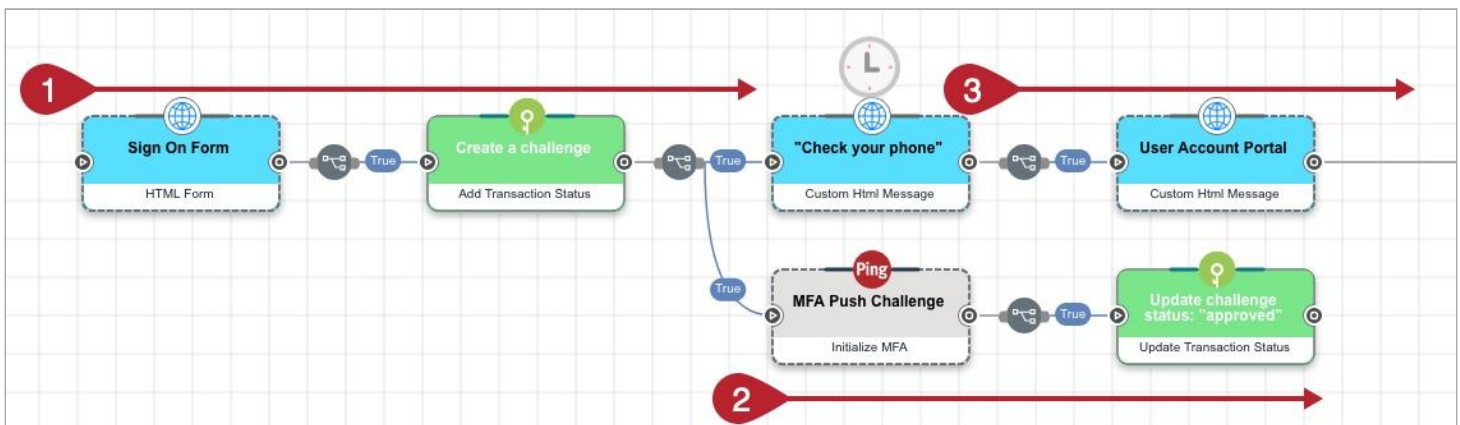
The Challenge connector allows you to branch your PingOne DaVinci flow to handle an external event, such as a multi-factor authentication (MFA) step.

By using the Challenge connector, you can show the user a message and “waiting” indicator in the main flow while a secondary flow interacts with the user elsewhere. When the secondary flow is done, the Challenge connector can trigger the main flow to continue.

The connector works by creating, updating, or checking the status of a “challenge” in your flow. Challenges are special variables that can be created by several connectors, including the Challenge connector, [Flow Conductor](#) and some authentication and verification connectors.

Other connectors, such as the [HTTP](#) connector, can pause the flow until the status of a challenge changes.

The Challenge connector updates the status of a challenge, which triggers the waiting HTTP connector to continue the flow.



Setup

Setting up the Challenge connector

In DaVinci, add a **Challenge** connection. For help, see [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

The Challenge connector supports a variety of use cases, such as:

Building an MFA sign-on flow

In this example, we want our user to complete an MFA challenge after entering their username and password. We'll show an HTML message in the browser telling the user to complete MFA. At the same time, we'll start the MFA connector in a secondary flow, which pushes a notification to the user's phone. When the user completes MFA on their phone, our secondary flow triggers the HTML message to continue the main flow.

Before you start, you'll need:

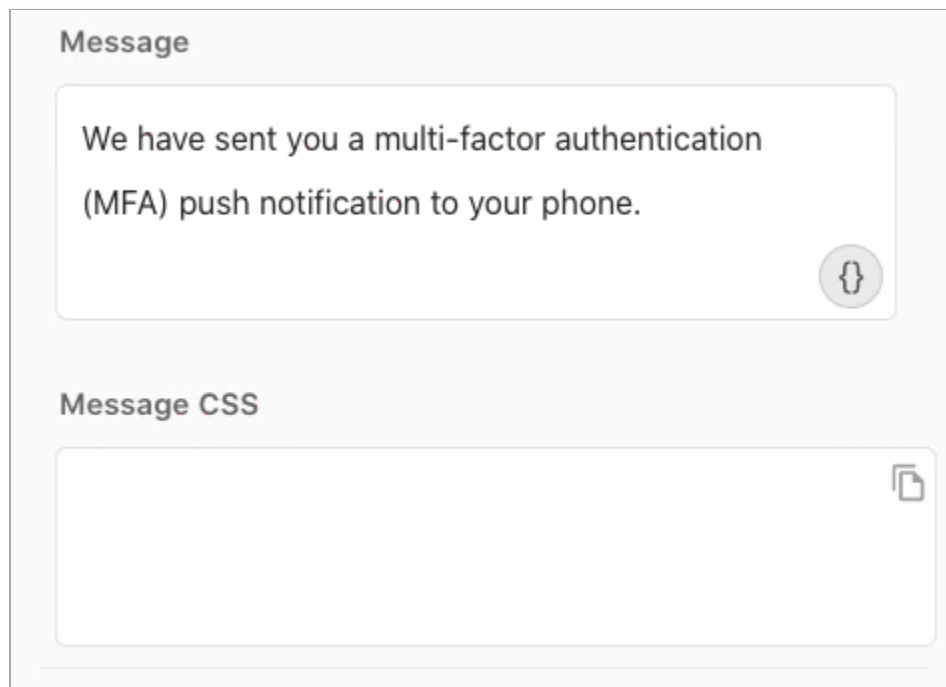
- A sign-on form. You can create one with the [HTTP](#) connector.
- An MFA connector, such as the [PingOne MFA](#) connector.

1. Create the challenge:

1. In your flow, following the sign-on form, add the **Challenge** connector and select the **Add Transaction Status** capability. Select the new node in your flow.
2. Turn off **Is challenge record complete**.
3. In the **Challenge Status** list, select **started**.

2. Show a page with a “waiting” animation until the user clicks the link:

1. Following your **Add Transaction Status** node, add an [HTTP](#) connector and select the **Custom HTML Message** capability. Select the new node in your flow.
2. Build your message in the **HTML Template** field. To show a “waiting” animation on the page, click {} and select the `skpolling` variable from SK-Component.



Message

We have sent you a multi-factor authentication (MFA) push notification to your phone.

Message CSS

3. In the **Challenge** field, click {} and select the `challenge` variable from your **Add Transaction Status** node. Turn on **Enable Polling**.

This pauses the main flow on this page until the challenge status changes. We'll update the challenge status in the secondary flow.

Note

Any change in the challenge status, regardless of the value, will cause this flow to continue.

3. Build a secondary flow that sends the MFA push and updates the challenge status:
 1. Following your **Add Transaction Status** node, parallel to your **Custom HTML Template** node, add an MFA node. In our example, we use the [PingOne MFA](#) connector. You can use your MFA service of choice or link to a subflow using the [Flow conductor](#) connector.
 2. Configure your MFA node by following its documentation. If you are using the **PingOne MFA** connector, see [PingOne MFA](#).
 3. Following your MFA node, add a **Challenge** connector and select the **Update Transaction Status** capability.
 4. In the **Challenge** field, click  and select the `challenge` variable from your **Add Transaction Status** node.
 5. Turn on **Is challenge record complete**. This indicates to DaVinci that our **Custom HTML Template** can stop polling for the status of this challenge.
 6. In the **Challenge Status** list, select **approved**.
4. Following your **Custom HTML Template** “waiting” page in the main flow, continue building the rest of your flow. For example, you could direct the user to their user account self-service portal.

Capabilities

Add Transaction Status

Add the transaction status challenge to the flow.

Properties

isChallengeComplete toggleSwitch
challengeStatus dropdownWithCreate

started:

This status signifies that the challenge has been created and can be polled until the status changes or times out

approved:

This status signifies that the challenge has been approved and should be treated as a success event

denied:

This status signifies that the challenge has been denied. This status will still be treated as a success event and the flow is expected to move forward to the true path. Flow can then decide what next to do with the denied status

Challenge Timeout in seconds (default 300secs) textField
updatedByFlowId textField
claimsNameValuePairs selectNameValueListColumn

Input Schema

- default object
 - parameters object
 - challengeStatus string
 - updatedByFlowId string

Output Schema

- output object
 - challenge string
 - challengeStatus string
 - updateByFlowId string

Output Example

```
{ "challenge" : "IXaa0MwwUFtrI4AJedpr4ha40wZmEe0isisRPFlnA0c",  
  "challengeStatus" : "started",  
  "updateByFlowId" : "MwwUFtrI4AJedpr4ha40wZmEe0" }
```

Update Transaction Status

Update the transaction status challenge in the flow.

Properties

Challenge textField

isChallengeComplete toggleSwitch

challengeStatus dropdownWithCreate

started:

This status signifies that the challenge has been created and can be polled until the status changes or times out

approved:

This status signifies that the challenge has been approved and should be treated as a success event

denied:

This status signifies that the challenge has been denied. This status will still be treated as a success event and the flow is expected to move forward to the true path. Flow can then decide what next to do with the denied status

updatedByFlowId textField

claimsNameValuePairs selectNameValueListColumn

Input Schema

- default object

- parameters object

- challenge string minLength: 1 maxLength: 100

- Unique string to identify the Transaction

- challengeStatus string minLength: 1 maxLength: 50

- Current status of the Transaction

- updatedByFlowId string minLength: 1 maxLength: 100

- Id of the flow updating the challenge

Output Schema

- output object
 - challenge string
 - challengeStatus string
 - updateByFlowId string

Output Example

```
{ "challenge" : "IXaa0MwwUFtrI4AJedpr4ha40wZmEe0isisRPFlNA0c",  
  "challengeStatus" : "approved",  
  "updateByFlowId" : "MwwUFtrI4AJedpr4ha40wZmEe0" }
```

Get Transaction Status

Retrieve transaction status information in the flow.

Properties

Challenge textField

Input Schema

- default object
 - parameters object
 - challenge string minLength: 1 maxLength: 100
Unique string to identify the Transaction

Output Schema

- output object
 - challenge string
 - challengeStatus string
 - updateByFlowId string

Output Example

```
{ "challenge" : "IXaa0MwwUFtrI4AJedpr4ha40wZmEe0isisRPFlnA0c",  
  "challengeStatus" : "approved",  
  "updateByFlowId" : "MwwUFtrI4AJedpr4ha40wZmEe0",  
  "createdDate" : 1.6353453453E10,  
  "statusUpdatedDate" : 1.6353453453E10 }
```

Poll for Transaction Status

Poll for transaction status information in the flow.

Properties

Challenge textField
pollInterval textField
pollRetries textField

Input Schema

- default object
 - parameters object
 - challenge string minLength: 1 maxLength: 100
Unique string to identify the Transaction
 - pollInterval number
Poll Interval in ms
 - pollRetries number
Number of Poll Retries

Output Schema

- output object
 - challenge string
 - challengeStatus string
 - updateByFlowId string

Output Example

```
{ "challenge" : "IXaa0MwwUFtrI4AJedpr4ha40wZmEe0isisRPFlnA0c",  
  "challengeStatus" : "approved",  
  "updateByFlowId" : "MwwUFtrI4AJedpr4ha40wZmEe0" }
```

Challenge Connector Release Notes

New features and improvements in the Challenge connector.

January 2023

Fixed the "poll is not defined" error

Fixed

Fixed an issue that caused the connector to report "poll is not defined" when using the **Poll for Transaction Status** capability.

October 2022

Get Transaction Status now outputs the complete transaction status details

Fixed

Previously, the **Get Transaction Status** capability would output a blank `details` object. It is now populated with the **Additional Fields** configured in the **Challenge** node that set the transaction status.

Code Snippet Connector

The Code Snippet connector lets you create custom JavaScript code that you can reuse across multiple PingOne DaVinci flows. You can use it to provide dynamic messages, get a specific attribute from a JavaScript Object Notation (JSON) payload, or insert any other custom behavior into your flow.

This piece of code is saved at the environment level, so you can use it multiple times in a flow, or reuse it in all of your flows. When you update the code, it affects every flow that you added it to. This is different from the [Function](#) connector's **Custom Function** capability, which only exists once in a single flow.

Because this code is reusable, it can help in the centralization or automation of your organization's common processes.



Important

For best practices to use custom code in your flows, see [Using custom code safely](#).



Note

The following libraries are available in custom functions:

- [File System](#) (non-functional mockup only)
- [Buffer](#)
- All JavaScript built-in objects

Setup

Configuring the Code Snippet connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

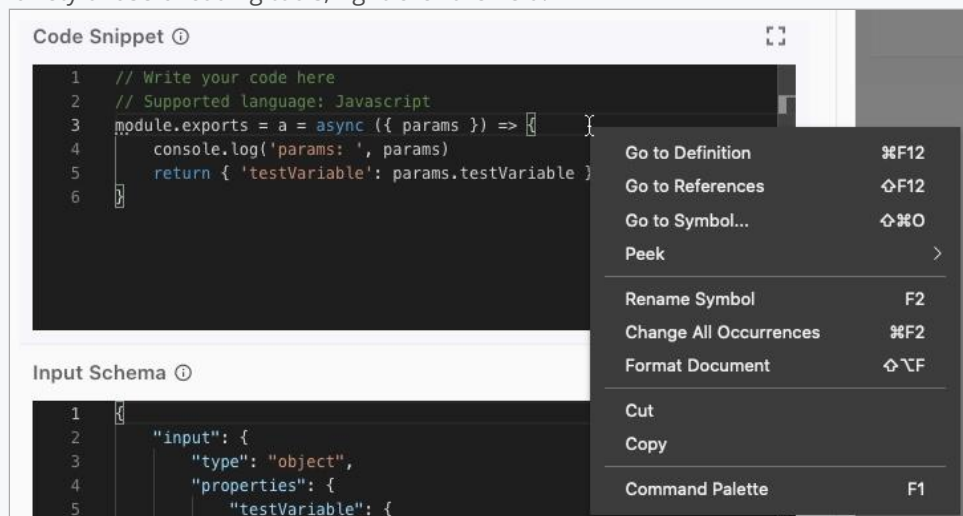
Connector configuration

Code Snippet

Enter your own JavaScript code within the default `module.exports`. This gives you access to the variables from your flow.

Tip

- To give yourself more room to work, click the Expand (⌵) button.
- To access a variety of useful coding tools, right-click the field.



Input Schema

This defines the structure of the data that your code receives from the flow. When you pass variables into your code from the flow, use this space to define whether it is a string, boolean, or other type. For help, see JSON-Schema.org.

Output Schema

This defines the structure of the data that your code returns to the flow. Use this space to define the type for any variable your code returns.

Get your output schema:

1. Copy your raw JSON output:
 1. Following your **Code Snippet** node, add an [HTTP](#) connector and select the **Custom HTML Message** capability. Click the new node in your flow.
 2. In the **Message** field, click **{}** and insert the **output (object)** variable from your **Code Snippet** node.
 3. Click **Apply**.
 4. Click **Save**, **Deploy**, and **Try Flow**.
 5. Copy the JSON payload that appears in your HTML message.
2. In a browser, open the [Online JSON Schema Validator and Generator](#) tool.
3. Paste the JSON response you copied into the **JSON** field. Click **Generate Schema From JSON**. Copy the output from the **JSON SCHEMA** field.

JSON

Generate Schema From JSON
Browse JSON file

```
1 {"img/QH.png","value":"QUEEN","suit":"HEARTS","remaining":47}}
```

JSON SCHEMA

Generate JSON from Schema
Browse JSON SCHEMA file

```
1 {
2   "definitions": {},
3   "$schema": "http://json-schema.org/draft-07/schema#",
4   "$id": "https://example.com/object1642544708.json",
5   "title": "Root",
6   "type": "object",
7   "required": [
8     "headers",
9     "statusCode",
10    "body"
11  ],
12  "properties": {
13    "headers": {
14      "$id": "#root/headers",
15      "title": "Headers",
16      "type": "object",
17    }
18  }
19 }
```

4. In your **Code Snippet** node, paste the JSON schema into the **Output Schema** field.

To edit your Code Snippet after adding it to a flow, come back to these details by clicking the **Edit** button.

My Code Snippet

id: cishgocfot
connectionId: 4e279336c06e4325d37ddf6512a16a28

TRIGGER:

Snippet

GENERAL **SETTINGS**

* indicates required

Function Argument List

**Caution**

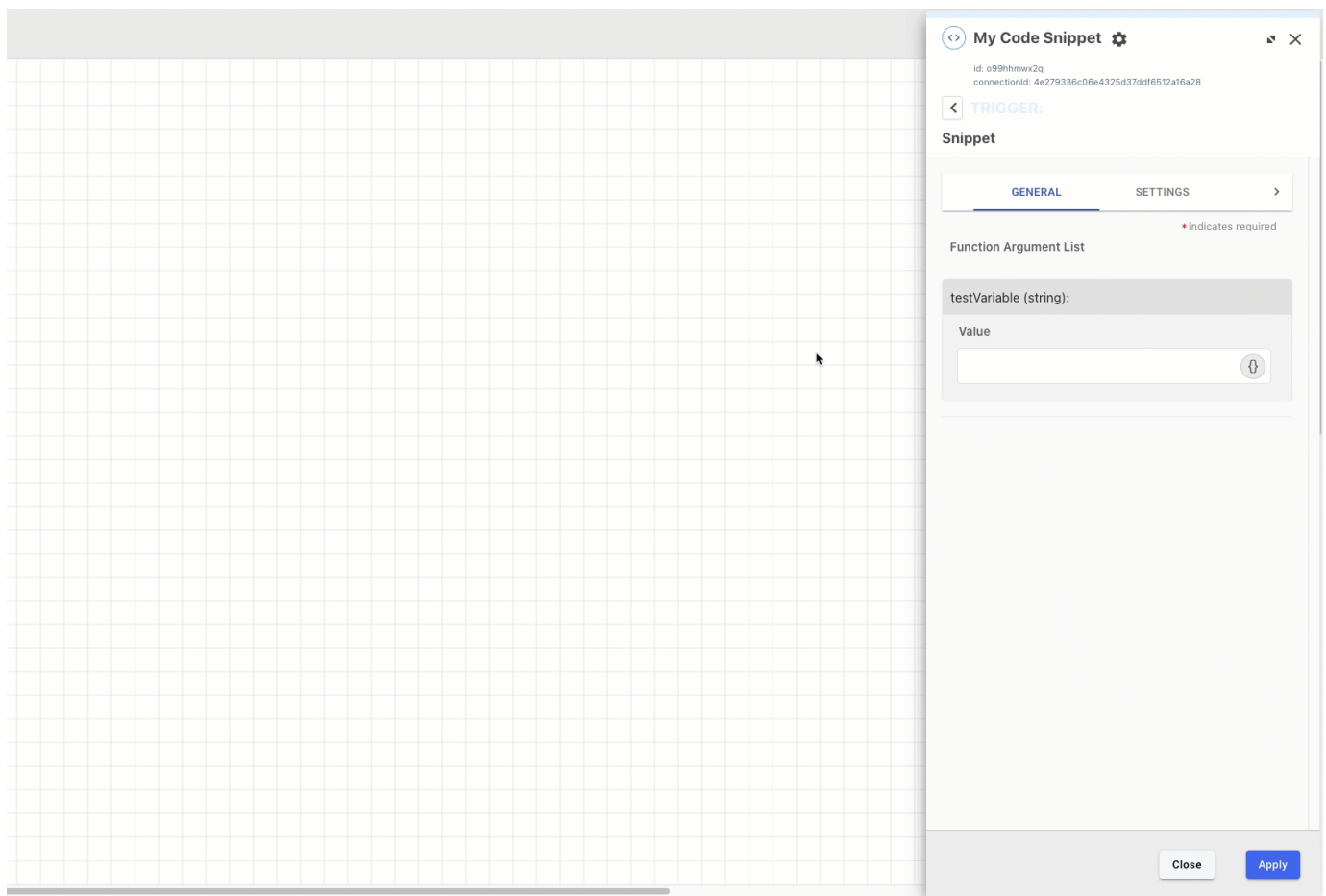
Any changes you make will affect every flow that uses this Code Snippet.

Using the connector in a flow

Showing a dynamic message with a switch

In this example, a user has selected a multi-factor authentication (MFA) method. Depending on which method they chose, we'll display a different message on the screen.

1. Add a **Code Snippet** connection to your environment. For help, refer to [Adding a connector](#).
2. Click the **Gear** icon to open the **Code Snippet Details** window.



3. In the **Code Snippet** field, enter the following switch code:

```
// Write your code here
// Supported language: Javascript
module.exports = a = async ({params}) => {
  switch (params.mfaMethod){
    case "SMS":
      return {'HTMLResult': "Enter your phone number"};
      break;

    case "EMAIL":
      return {'HTMLResult': "Please enter your email address"};
      break;

    default:
      return {'HTMLResult': "No MFA method selected."}
  }
}
```

4. This code takes the `mfaMethod` variable from earlier in our flow and checks the value. If it matches `SMS` or `EMAIL`, it returns the matching message. If the `mfaMethod` variable doesn't match one of the two options, the code returns the error "No MFA method selected".

5. We know that the `mfaMethod` variable in our flow contains text, so we define it as a string in the **Input Schema** field:

```
{
  "input": {
    "type": "object",
    "properties": {
      "mfaMethod": {
        "type": "string"
      }
    }
  }
}
```

6. Our example code always returns a message in the *HTMLResult* variable, so we define it as a string in the **Output Schema** field:

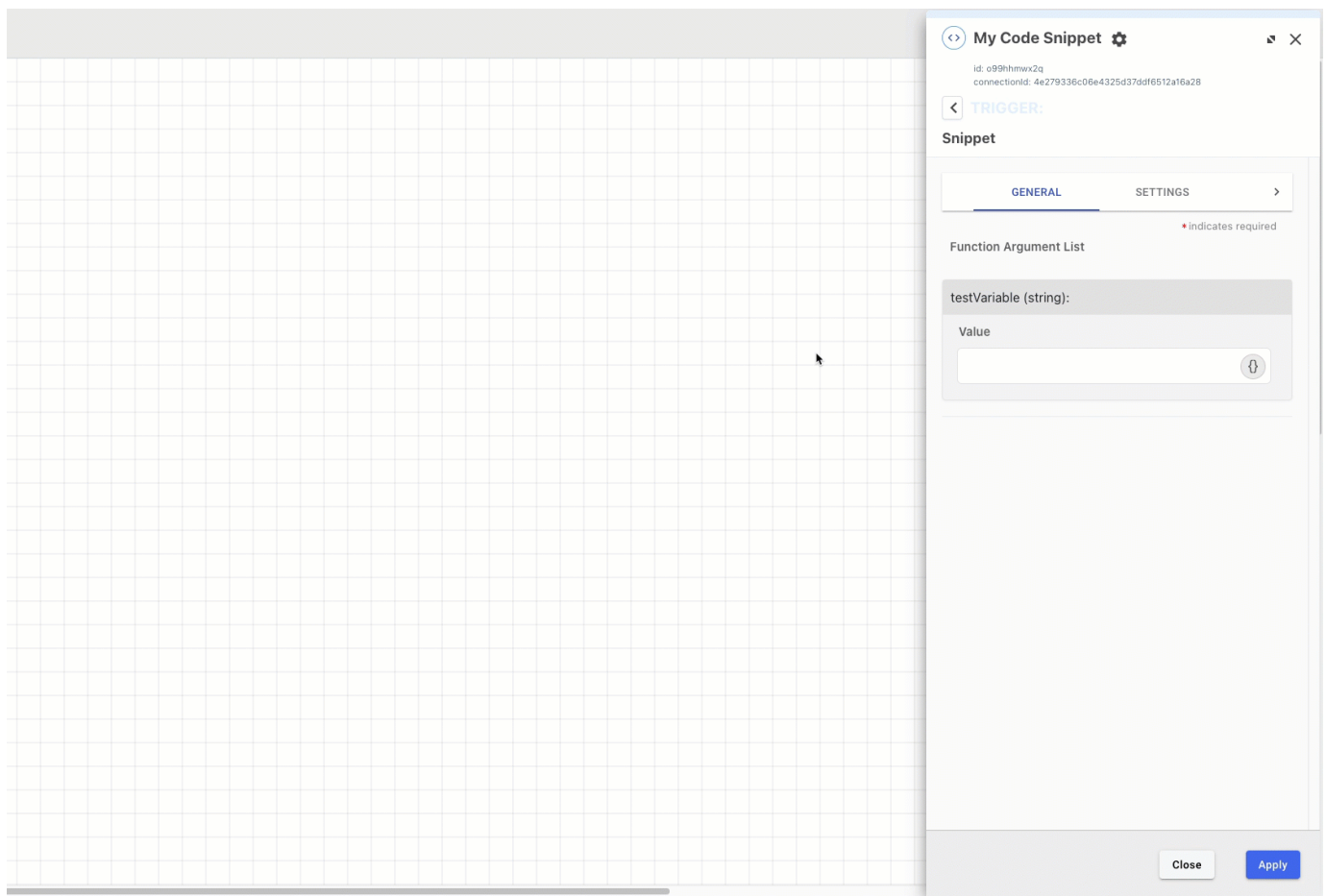
```
{
  "output": {
    "type": "object",
    "properties": {
      "HTMLResult": {
        "type": "string"
      }
    }
  }
}
```

7. In your flow, add the **Code Snippet** connection that you created and select the **Snippet** capability. No other setup is needed.

Getting a value from a JSON response

In this example, we retrieved information about a user from a directory, including the user's name, address, phone number, and more. To continue our flow, we need the user ID, which is buried somewhere in the response.

1. Add a **Code Snippet** connection to your environment. For help, see [Online JSON Schema Validator and Generator](#).
2. Click the **Gear** icon to open the **Code Snippet Details** window.



3. In the **Code Snippet** field, enter the following:

```
// Write your code here
// Supported language: Javascript
module.exports = a = async ({params}) => {
  console.log('params: ', params)
  const body = JSON.parse(params.body)
  return {
    'userId': body._embedded.users[0].id
  }
}
```

4. This code uses `JSON.parse` to put the usable data into the `body` object. This is a good starting point when you want to parse a JSON payload.
5. Next, the code returns a variable called password `userId`. In our case, the user ID is located at `__embedded.users[0].id` inside the `body` object we created. When creating your own code, look at the structure of the payload to determine the path you need.
6. We know that the `id` contains text, so we define it as a string in the **Input Schema** field:


```
{
  "input": {
    "type": "object",
    "properties": {
      "id": {
        "type": "string"
      }
    }
  }
}
```

7. Our user ID contains text, so we define it as a string in the **Output Schema** field:

```
{
  "output": {
    "type": "object",
    "properties": {
      "userId": {
        "type": "string"
      }
    }
  }
}
```

8. In your flow, add the **Code Snippet** connection that you created and select the **Snippet** capability. No other setup is needed.

Using variables in code snippets

You can create dynamic code by including variables in your code snippets. Variables are populated when the flows runs.

Global variables

For global variables, use the following syntax:

```
{{global.variables.variablename}}
```

For example, to include the following **username** variable, include the following:

```
{{global.variables.userInfo.username}}
```

Flow instance variables

For flow instance variables, use the following syntax:

```
{{local.nodeid.output.variablename}}
```

To find the value for any variable:

1. Open your flow.
2. Select a node that has access to the variable you want to use.
3. In any field, click `{}` and select the variable.
4. Use your mouse to hover over the inserted variable.

The image shows a light gray form with three sections, each with a title and an information icon (i):

- Error Message**: A text input field with a vertical cursor and a variable selector icon (a circle with curly braces) on the right.
- Error Description**: An empty text input field with a variable selector icon on the right.
- Error Code**: An empty text input field with a variable selector icon on the right.

Capabilities

Snippet

Properties

functionArgumentList functionArgumentList

Output Schema

• output object::

Cookie Connector

The Cookie connector lets you set and retrieve session cookies in your PingOne DaVinci flow.

Setup

Resources

For more information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Cookie connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

HMAC Signing Key

The Base64-encoded, 256-bit key that the connector uses to sign the session cookies. This prevents unauthorized agents from gaining access by guessing a session ID.

To use this, enable the **Sign Cookies with HMAC Key** option in the **Set a Session Cookie** capabilities.

Using the connector in a flow

Creating a session cookie

The connector has two capabilities that allow you to set session cookies:

- **Set a Session Cookie**
- **Set a Session Cookie (Non-User)**

These two capabilities are identical, except the **Non-User** variant doesn't require a user to already have been identified in the flow.

No special configuration is needed. Add the capability and populate its properties according to the help text.

You can include custom claims in the session cookie. In the **Session Cookie Custom Claims** section, click **+ Field**, select a claim from the list, and enter a value. To delete a custom claim from the list, click **Edit**.

Retrieving a session cookie

The connector has two capabilities that allow you to read existing session cookies:

- **Check a Session Cookie**
- **Check a Session Cookie (Non-User)**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Set Session Cookie

Sets an opaque session cookie so that the user is not asked to authenticate again during the flow.

Properties

cookieName textField

useSecureCookie toggleSwitch

useHttpOnlyCookie toggleSwitch

cookieExpiresInSeconds textField

cookieDomain textField

Cookie Path textField

The path where the cookie will be accessible

cookieSameSite dropDown

signCookie toggleSwitch

setCookieClientSide toggleSwitch

claimsNameValuePairsSessionCookie selectNameValueListColumn

useSessionTokenFlag toggleSwitch

sessionToken textField

Input Schema

- default object
 - userInfo object required
 - User with which the cookie is to be associated.
 - ip string minLength: 1 maxLength: 50
 - Ip address of the user in current session.
 - userAgent string minLength: 1 maxLength: 250
 - Information about browser, OS, etc. of user in current session.
 - skOpenId object
 - Object containing client id of user.
 - origin string minLength: 0 maxLength: 500
 - Origin
 - originCookies string minLength: 0 maxLength: 20000
 - OriginCookies

Check Session Cookie

Determine if a session cookie exists in the flow. If it exists, continue with the flow, or ask the user to provide additional authentication information.

Properties

***cookieName* textField**

***enforceClientIP* toggleSwitch**

***enforceFlowIdMatch* toggleSwitch**

***Resolve to User* toggleSwitch**

Attempt to resolve cookie to a user, which will then be available in `{{global.userInfo}}` parameter

Input Schema

- default object

- userAgent string minLength: 1 maxLength: 250

Information about browser, OS, etc. of user in current session.

- ip string minLength: 1 maxLength: 50

Ip address of the user in current session.

- cookies object

List of cookies associated with the user.

- skOpenId object

Object containing client id of user.

- origin string minLength: 0 maxLength: 500

Origin

- originCookies string minLength: 0 maxLength: 20000

OriginCookies

Output Schema

- output object
 - claims object
 - userId string
 - connectionId string
 - companyId string
 - ip string
 - userAgent number
 - flowId string
 - client_id string
 - signCookie boolean
 - createdAt number
 - cookieExpiresInSeconds number
 - loa number

Output Example

```
{ "userId" : "mzDcrsYnonx8S9JTyblHD0bHeE9quaZJ",  
  "connectionId" : "HVxcjWW8sBFrdue6vdryxUSInua51tK",  
  "companyId" : "mzDcrsYnonx8S9JTyblHD0bHeE9quaZJ",  
  "ip" : "192.168.0.4",  
  "userAgent" : "",  
  "flowId" : "mzDcrsYnonx8S9JTyblHD0bHeE9quaZJ",  
  "client_id" : "mzDcrsYnonx8S9JTyblHD0bHeE9quaZJ",  
  "signCookie" : true,  
  "createdAt" : 1.606535447E9,  
  "cookieExpiresInSeconds" : 1000,  
  "loa" : 1 }
```

Set Session Cookie (Non User)

Set an opaque session cookie with a set of custom claims.

Properties

cookieName textField

useSecureCookie toggleSwitch

useHttpOnlyCookie toggleSwitch

cookieExpiresInSeconds textField

cookieDomain textField

Cookie Path textField

The path where the cookie will be accessible

cookieSameSite dropDown

signCookie toggleSwitch

setCookieClientSide toggleSwitch

claimsNameValuePairsSessionCookie selectNameValueListColumn

useSessionTokenFlag toggleSwitch

sessionToken textField

Input Schema

- default object
 - ip string minLength: 1 maxLength: 50
Ip address of the user in current session.
 - userAgent string minLength: 1 maxLength: 250
Information about browser, OS, etc. of user in current session.
 - skOpenId object
Object containing client id of user.
 - origin string minLength: 0 maxLength: 500
Origin
 - originCookies string minLength: 0 maxLength: 20000
OriginCookies

Check Session Cookie (Non User)

Check if a specific session cookie exists and retrieve the custom claims for decision-making purposes.

Properties

***cookieName* textField**
***enforceClientIP* toggleSwitch**
***enforceFlowIdMatch* toggleSwitch**

Input Schema

- default object
 - userAgent string minLength: 1 maxLength: 250
Information about browser, OS, etc. of user in current session.
 - ip string minLength: 1 maxLength: 50
Ip address of the user in current session.
 - cookies object
List of cookies associated with the user.
 - skOpenId object
Object containing client id of user.
 - origin string minLength: 0 maxLength: 500
Origin
 - originCookies string minLength: 0 maxLength: 20000
OriginCookies

Output Schema

- output object
 - claims object
 - ip string
 - userAgent number
 - flowId string
 - client_id string
 - signCookie boolean
 - createdAt number
 - cookieExpiresInSeconds number
 - loa number

Output Example

```
{ "ip" : "192.168.0.4",  
  "userAgent" : "",  
  "flowId" : "mzDcrsYnonx8S9JTyb1HD0bHeE9quaZJ",  
  "client_id" : "mzDcrsYnonx8S9JTyb1HD0bHeE9quaZJ",  
  "signCookie" : true,  
  "createdAt" : 1.606535447E9,  
  "cookieExpiresInSeconds" : 1000,  
  "loa" : 1 }
```

CrowdStrike Connector

The CrowdStrike connector lets you use CrowdStrike improve authentication security in your PingOne DaVinci flow.

CrowdStrike protects the people, processes and technologies that drive modern enterprise. A single agent solution to stop breaches, ransomware, and cyberattacks powered by world-class security expertise and deep industry experience.

You can use the CrowdStrike connector to:

- Check whether a device is managed by CrowdStrike
- List the devices associated with a username or IP address
- Get the incident scores for a device
- Get the CrowdStrike scores from multiple incidents
- Get the CrowdStrike Zero Trust Assessment scores for a device

- Get the CrowdScore for an environment
- Managed quarantined devices

Setup

Resources

For information and setup help, see the following:

- CrowdStrike documentation
 - [CrowdStrike OAuth2-Based APIs](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a CrowdStrike license.

Setting up CrowdStrike

Follow the steps in [Creating an API client](#).

- Select the following API scopes:

Scope	Permissions
Hosts	Read, Write
Falcon Discover	Read
Incidents	Read
Zero Trust Assessment	Read

- Record your client ID and secret. You'll use them in the connector configuration.

Configuring the CrowdStrike connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

CrowdStrike Base URL

The base URL for your CrowdStrike environment.

Client ID

The client ID you created in Setting up CrowdStrike.

Client Secret

The client secret you created in Setting up CrowdStrike.

Using the connector in a flow

Getting device details

The **Get Device Details** capability allows you to get detailed information about one or more devices.

In the **Device IDs** field, you can click {} and select the `deviceIds` variable from a **Get Devices from Logins** node.

Getting device management status

The **Check Device Status by Device ID** and **Check Device Status by IP** capabilities identify if a device is managed by CrowdStrike.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Quarantining devices

You can quarantine a device by applying CrowdStrike Network Containment on the device ID with the **Set Containment on Devices** capability.

When you determine a device is safe, you can remove the quarantine with the **Lift Containment on Devices** capability.

In the **Device IDs** field, you can click {} and select the `deviceIds` variable from a **Get Devices from Logins** node.

Getting incident scores

The **Get Incident Scores** lets you find out the highest incident score from a list of incident IDs. In the **Incident IDs** field, you can click {} and select the `incidentIds` variable from a **Get Incidents from Logins** node.

The **Get Incident Scores by Device ID** capability lets you find out the highest incident score for a particular device. In the **Device ID** field, you can click  and select a variable from your flow that includes the device ID.

Capabilities

Get Incident Score by Device ID

Get the maximum incident score from a single CrowdStrike device ID.

Properties

Device ID `textField`

The CrowdStrike device ID (also known as agent ID), such as "f69915c8a8b244a1a7c4e4a4d7870e2f".

Input Schema

default `object`

deviceIdIncidentScore `string` required

A CrowdStrike device ID.

Output Schema

output `object`

rawResponse `object`

statusCode `number`

maxIncidentScore `number`

incidentsOnDevice `boolean`

Get Zero Trust Assessment Scores from Devices

Use a list of device IDs to get the most recent Zero Trust Assessment scores.

Properties

Device IDs `textField` required

List of Device IDs (JSON Array formatted)

Input Schema

default `object`

deviceIds `string` required

List of Device IDs

Output Schema

output `object`

rawResponse `object`

statusCode `number`

maxOverallScore `number`

Maximum Overall Score from Devices

***maxOSScore* number**

Maximum Operating System Score from Devices

Get Environment CrowdScore

Get the most recent CrowdScore for the CrowdStrike environment.

Output Schema

***output* object**

***rawResponse* object**

***statusCode* number**

***score* number**

***adjustedScore* number**

Check Device Status by Device ID

Use the CrowdStrike Device ID to check whether a device is managed by CrowdStrike.

Properties

***Device ID* textField**

The CrowdStrike device ID (also known as agent ID), such as "f69915c8a8b244a1a7c4e4a4d7870e2f".

Input Schema

***default* object**

***deviceIdDeviceManaged* string required**

The CrowdStrike Device Id.

Output Schema

***output* object**

***rawResponse* object**

***statusCode* number**

***deviceManaged* boolean**

***deviceDetails* object**

Check Device Status by IP

Use an IP address to check whether a device is managed by CrowdStrike.

Properties

***IP* textField**

The user's IP address

***Username* textField**

The username associated with the device.

***Last Seen Number of Days* textField**

The number of days to search back in time for a managed device.

Default:

365

Input Schema

***default* object**

***ip* string required**

The IP address of the device

***username* string**

The username associated with the device

***lastSeenDays* string/number required**

The number of days to search back in time for a managed device

Output Schema

***output* object**

***rawResponse* object**

***statusCode* number**

***deviceManaged* boolean**

***foundLoginMatch* boolean**

Get Devices from Logins

Get a list of device IDs from CrowdStrike Logins that match a username, email address, or IP address.

Properties

***Username* textField**

The username associated with the device.

***Email* textField**

The email of the user associated with the device.

***IP* textField**

The user's IP address

***Search Back Number of Days* textField**

The number of days to search back in time for a login

Default:

365

Input Schema**default object****username string**

The username associated with the device

email string

The email of the user associated with the device

ip string

The user's IP address

searchLoginDays string/number required

The number of days to search back in time for a login

Output Schema**output object****rawResponse object****statusCode number****deviceIds array****Get Device Details**

Get device details from a list of devices.

Properties**Device IDs textField required**

List of Device IDs (JSON Array formatted)

Input Schema**default object****deviceIds string required**

List of Device IDs (JSON Array formatted)

Output Schema

output object

rawResponse object

statusCode number

devices array

Get Incidents by IP

Use an IP address to get a list of incidents associated with the device.

Properties

IP textField

The user's IP address

Last Seen Number of Days textField

The number of days to search back in time for a managed device.

Default:

365

Input Schema

default object

ip string required

The IP address of the device

lastSeenDays string/number required

The number of days to search back in time for a managed device

Output Schema

output object

rawResponse object

statusCode number

incidentsOnDevice boolean

incidentIds array

Get Incidents from Logins

Get a list of incidents from CrowdStrike Logins that match a username, email address, or IP address.

Properties

Username textField

The username associated with the device.

Email textField

The email of the user associated with the device.

IP textField

The user's IP address

Search Back Number of Days textField

The number of days to search back in time for a login

Default:

365

Input Schema

default object

username string

The username associated with the device

email string

The email of the user associated with the device

ip string

The user's IP address

searchLoginDays string/number required

The number of days to search back in time for a login

Output Schema

output object

rawResponse object

statusCode number

loginsWithIncidents boolean

incidentIds array

Get Incident Scores

Get the maximum incident score from a list of incident IDs.

Properties

Incident IDs textField

List of Incident IDs (JSON Array formatted)

Input Schema

default object

incidentIds string required

List of Incident IDs

Output Schema

output object

rawResponse object

statusCode number

maxIncidentScore number

incidents array

Set Containment on Devices

Apply CrowdStrike Network Containment on the Device IDs.

Properties

Device IDs textField required

List of Device IDs (JSON Array formatted)

Input Schema

default object

deviceIds string required

List of Device IDs

Output Schema

output object

rawResponse object

statusCode number

Lift Containment on Devices

Remove CrowdStrike Network Containment on the Device IDs.

Properties

Device IDs textField required

List of Device IDs (JSON Array formatted)

Input Schema

default object

deviceIds string required

List of Device IDs

Output Schema

output object

rawResponse object

statusCode number

CrowdStrike Connector Release Notes

New features and improvements in the CrowdStrike connector.

March 2023

New capabilities for getting information by device ID

New

We have added the following capabilities:

- **Check Device Status by Device ID**
- **Get Incident Scores by Device ID**

These allow you to create more granular policies by targeting a specific device.

June 2022

The CrowdStrike connector is now available

New

You can use the CrowdStrike connector to:

- Check whether a device is managed by CrowdStrike
- List the devices associated a username or IP address
- Get the incident scores for devices
- Get the CrowdStrike scores from multiple incidents
- Get the CrowdStrike Zero Trust Assessment scores for a device
- Get the CrowdScore for an environment
- Managed quarantined devices

D-F



Daon Connector

The Daon connector lets you use Daon IdentityX for MFA in your PingOne DaVinci flow.



Device Policy Connector

The Device Policy connector lets you check the user agent, browser information, and operating system version in your PingOne DaVinci flow.



Duo Connector

The Duo connector lets you use Duo for MFA in your PingOne DaVinci flow.



Entrust Connector

The Entrust connector lets you use Entrust adaptive authentication in your PingOne DaVinci flow.



Error Message Connector

The Error Message connector lets you create and customize the error messages that appear in your PingOne DaVinci flow.



FingerprintJS Connector

The FingerprintJS connector lets you create a unique visitor ID based on browser attributes for use in fraud and analytics in your PingOne DaVinci flow.



Flow Analytics Connector

The Flow Analytics connector lets you log details about flow outcomes that you can review in flow analytics.



Flow Conductor Connector

The Flow Conductor connector lets your PingOne DaVinci flow initiate asynchronous events in external systems. It also allows you to use another flow as a subflow.



Functions Connector

The Functions connector lets you branch your PingOne DaVinci flow using logical conditions or based on the result of custom JavaScript code.

Daon Connector

The Daon connector lets you use Daon IdentityX for multi-factor authentication (MFA) in your PingOne DaVinci flow.

The connector triggers authentication on a user's mobile device using an app that was built with the Daon mobile SDK. DaVinci can get the result of the authentication process by polling Daon or by listening for a webhook response.

Setup

Resources

For more information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirement

To use the connector, you'll need:

- An existing integration between your mobile app and Daon IdentityX
- Your Daon access information, including:
 - Admin credentials
 - The URL for your IdentityX application programming interface (API) service

Configuring the Daon connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

API Base URL

The URL for your Daon IdentityX API. For example, <https://api.identityx-cloud.com/>[yourcompany/IdentityXServices/rest/v1](#)

Admin Username

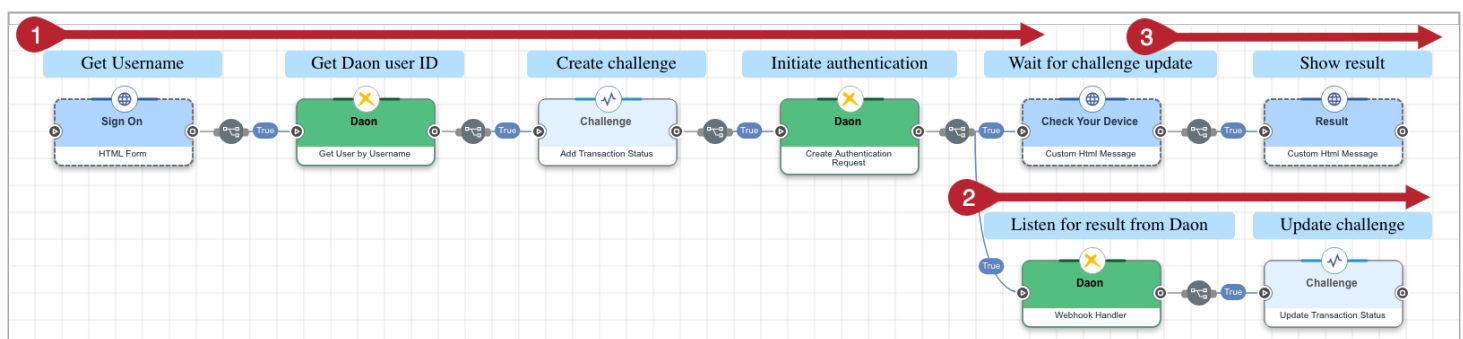
The username for your Daon administrator account.

Admin Password

The password for your Daon administrator account.

Using the connector in a flow

Authenticating users with results via webhook



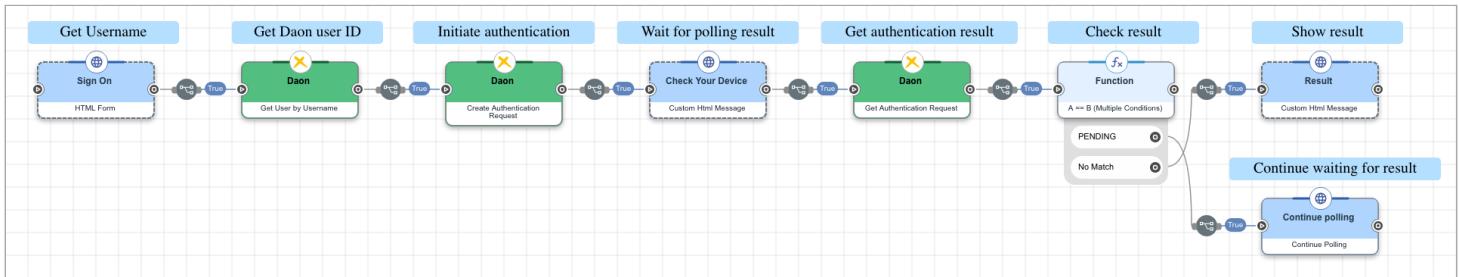
This flow asks the user to enter their username in an HTML form. The connector gets their Daon user ID and initiates the authentication process on the user's mobile device.

The user sees a "Check your device" message that stays on screen until as long as the flow challenge remains unresolved.

In a secondary branch, the connector listens for a transaction result that Daon sends using a webhook. When DaVinci receives the result, the flow challenge is updated and the waiting message changes to show the result of the authentication process.

1. Download the [Daon - Authentication with results via webhook](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Configure the **Create Authentication Request** node by adding your Daon authentication policy in the **Policy URL** field.
3. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

Authenticating users with results via polling



This flow asks the user to enter their username in an HTML form. The connector gets their Daon user ID and initiates the authentication process on the user's mobile device.

The user sees a "Check your device" message, and the flow begins polling Daon until the authentication result is available. When DaVinci gets the result, the flow updates the waiting message to show the result of the authentication process.

1. Download the [Daon - Authentication with results via webhook](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Configure the **Create Authentication Request** node by adding your Daon authentication policy in the **Policy URL** field.
3. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

Capabilities

Get User by Username

Retrieve a user record with the user's login

Properties

User Login textField

The userId of the user you want to retrieve. E.g. `user@example.com`

Input Schema

- default object
 - properties object
 - apiUrl string required
 - username string required
 - password string required
 - userLogin string required

Output Schema

- output object
 - rawResponse object
 - userId string

Output Example

```

{ "metadata" :
  { "limit" : 1,
    "page" : 1,
    "totalCount" : 1 },
  "paging" :
  { "first" : null,
    "previous" : null,
    "next" : null,
    "last" : null },
  "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users?
userId=akennedy%2Batu001%40pingidentity.com&status=ACTIVE&limit=1",
  "items" :
  [
    { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w",
      "id" : "QTAzs3wrZYvmxdu0LQ13r8z75w",
      "userId" : "akennedy+atu001@pingidentity.com",
      "created" : "2022-04-26T14:35:04.399+0000",
      "updated" : "2022-04-26T14:35:04.399+0000",
      "nextPossibleDirectOtpDtm" : "2022-04-26T15:56:28.103+0000",
      "pinEnrolled" : false,
      "faceEnrolled" : false,
      "voiceEnrolled" : false,
      "keystrokesEnrolled" : false,
      "failedVerificationCount" : 0,
      "accountUnlockedCount" : 0,
      "status" : "ACTIVE",
      "tenant" :
      { "href" : "https://api.identityx-cloud.com/IdentityXServices/rest/v1/tenants/r4SWIoHpn0fmXw4pkQhAbw" },
      "applications" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/applications" },
      "registrations" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/registrations" },
      "authenticators" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/authenticators" },
      "authenticationRequests" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/authenticationRequests" },
      "sponsorships" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/sponsorships" },
      "registrationChallenges" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/registrationChallenges" },
      "enrollments" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/enrollments" },
      "samples" :
      { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w/samples" } } ] }

```

Create Authentication Request

Create an authentication request on the Identity X server for a user

Properties

User ID textField

The ID of the user.

Authentication Description textField

A description of the authentication request - if using the IdentityX Authenticator, this will be provided to the user.

Authentication Type dropDown

Specifies the protocol type of the authentication request.

- Fido 1 (Default)
- Fido Offline
- IdX
- REST
- OTP
- Fido 2 W3C

Policy URL textField

The policy associated with the authentication request.

Push Notification Type dropDown

Provides operation instructions to the mobile application how to behave when a push notification is received.

- Refresh
- Verify Without Confirmation
- Verify With Confirmation (Default)

Secure Transaction Content Type dropDown

Describes the value of the secureTransactionContent and secureTextTransactionContent property.

- text/plain (Default)
- image/png
- text/plain;image/png

Secure Text Transaction Content textField

Text to be displayed securely to a user. The secureTransactionContentType property must be "text/plain" or "text/plain;image/png".

Secure Image Transaction Content textField

Image to be displayed securely to a user. The secureTransactionContentType property must be "image/png" or "text/plain;image/png".

Input Schema

- default object
 - properties object
 - apiUrl string required
 - username string required
 - password string required
 - userId string required
 - description string required
 - type string required
 - pushNotificationType string required
 - secureTextTransactionContent string
 - secureTransactionContent string required
 - secureTransactionContentType string required
 - policyUrl string required

Output Schema

- output object
 - rawResponse object
 - status string
 - id string

Output Example

```
{
  "href": "https://api.identityx-cloud.com/pingdavoinci/IdentityXServices/prost/v1/users/QTAzw8gbbh6Z777TpHz3pkXERiW/authenticationRequests/QTAzAFVl0lrFXPHCidlov4Yt6Q",
  "id": "QTAzAFVl0lrFXPHCidlov4Yt6Q",
  "authenticationRequestId": "postman-27b76ffa-6c2f-4359-bdec-0f7a1199c86c",
  "description": "FIDO - OOB Auth Request",
  "expiration": "2022-04-25T12:42:31.141+0000",
  "availableRetries": 5,
  "totalRetriesAllowed": 5,
  "oneTimePasswordEnabled": false,
  "created": "2022-04-25T12:27:31.835+0000",
  "type": "FI",
  "fidoChallenge": "TuA-su0iHlpEwcdGR-xxZQ",
  "secureTextTransactionContent": "secure transaction details from postman",
  "secureTransactionContentType": "text/plain",
  "fidoAuthenticationRequest": "[{\\"header\\":{\\"upv\\":{\\"major\\":1,\\"minor\\":0},\\"op\\":\\"Auth\\",\\"appID\\":\\"https://example.com\\",\\"exts\\":[{\\"id\\":\\"com.daon.sdk.ados.decChain\\",\\"data\\":\\"\\\\"MIIE6TCCAT0gAwIBAgIRAJEmGK-0XEGFin4brMpnidIwCwYJKoZIhvcNAQELMecxFTATBgNVBAMDElkZW50aXR5WCBDQ TENMA sGA1UECgw ERGFvbjESMBAGAIUECwwJSWRlbnRpdHlYMQswCQYDVQGEwJRTAEFw0xNzA2MTUwOTQ3NTFaFw0xOTA2MTUwOTQ3NTFaMFoxDTALBgNVBAoM BERhb24xeJABGbnVBAsMCUlkZW50aXR5WDELMAKGA1UEBhMCSUUXKDA MBgNVBAMMH0RFX0RBT05fQVVUVEUVOVElDQVRJT05fREFUQV9LRUswg gEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXrHT7hGCZR4KzlwawZl3yefpUov44BWoFCNnuGh3RoaQ63vXX6jSrfoCVJdto5a38ND 7ckQzjhtuoAfLeUT3sbm7uhXCCOC5xJ_B96G6LeTvY6yZ2Zs03K8d0l8epKOI7e2Xh_3WQg0xa21QmJxnTcMSMj0TMHrXlB66nh-CoTbAcKopm0xbrPfOMLOz1xGk7i0VxSY_TRjep6tn4Z7t7r-bsJnDjJtctto4gYXk7mDkwdAMfBpoq1Jp0nGbv8TCMySAjOUsS9pte7pRl5No6iF4QYNDUUhI9q7MAcpSgEYLaPzhDzdZnmDfwW0IPCiss0 qKV9L3H6wh-NLQ_r7AgMBAAGjcAwgb0wfgYDVR0jBHcWdYAUZpISSlDw67i7wEa-1wVzqvZdL5ahS6RJMEcxFTATBgNVBAMDElkZW50aXR5WCBDQ TENMA sGA1UECgw ERGFvbjESMBAGAIUECwwJSWRlbnRpdHlYMQswCQYDVQGEwJRRYIQUhll9ePQGSsywpeleVwvazAdBgNVHQ4EFgQUyeJ8CGmnhFk5Cs0c6TEEG2GrL08wDAYDVROTAQH_BAIwADA0BgNVHQ8BAf8EBAMCBLAwCwYJKoZIhvcNAQELA4ICAQA-CspJue0Az96VXYHqIS_yRkltsSkLvmgquwux2fShZJQ1pawRf8qWH9takyyBzAPNVMySxIc4eMF4qRhExtADB5EQBFF-DWVmoLymYOLMDHii9lnuYdsV08B82eYsU7SecuDH3fFN01VJq2NS8jHUFm7GxUF3606BdojT3vXgHmH_d03GzGCRDpKkt_gUA01aj2Ga1YmLcd2ptA60A1S1lW0eWS5yb_KNscCVVQke2gvJkAChrSiel7AxBGukWlTANCrgH2U0hhhXl0mu3RR0xhUL8Ya5V7qSdiVZzmFMzWRpyX92FbGU Ib_lL9nIfs3iGtE9gXE-DVTNs93jn_XIK0Q8D6lcvpVtI4bJQhUJ7u78MeoSPuYx-9SX4ioiNmVVC6fdAieSG1ggEiIhw0U81-4u1pItyPIqwt_OijaEl0ouTWzeBa3AJA7Cqas0ZomX6BXJE5dLcILbpyDaU0vSc3em6cr-LJgRr7uuvQCJ-3pGX_gipMyailXYd2S985PQXsyKEW5AegBcEgNX3MivNPUhb2eS-Ab_JIZbQGAUGTT_HwQXFB08pMXJ-UK_FwdphXVGMJy9jmyvwLLBFXyYGrAiq0pLlkHexCqHcYjYbchgf1IDIwp0yQ3KcoA42w555djBN7hFHTa9dfAdTOHRKLIcG_PhsmUdhZ_T7oQ==\\\\"}\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.sdk.ados.dekId\\",\\"data\\":\\"1000090661\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.authRequest.retriesRemaining\\",\\"data\\":\\"5\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.authRequest.maxAttempts\\",\\"data\\":\\"5\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.user.retriesRemaining\\",\\"data\\":\\"10\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.user.maxAttempts\\",\\"data\\":\\"10\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.face.retriesRemaining\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.face.maxAttempts\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.voice.retriesRemaining\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.voice.maxAttempts\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.passcode.retriesRemaining\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.passcode.maxAttempts\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.otp.retriesRemaining\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.otp.maxAttempts\\",\\"data\\":\\"3\\",\\"fail_if_unknown\\":false},{\\"id\\":\\"com.daon.identityx.version\\",\\"data\\":\\"5.2.4.0\\",\\"fail_if_unknown\\":false}},\\"challenge\\":\\"TuA-su0iHlpEwcdGR-xxZQ\\",\\"policy\\":{\\"accepted\\":[[{\\"aaid\\":[\\\"D409#2601\\\"],\\"keyIDs\\":[\\\"RKE4NDhFQ0ItMjI5Ri0tM0kU2LUeZnkytNUiZqJAzMTBCRkQw\\\"]}]]},\\"transaction\\":[{\\"contentType\\":\\"text/plain\\",\\"content\\":\\"c2VjdXJlIHRyYW5zYWN0aW9uIGRldGFpbHMgZnJvbSBwb3N0bWFu\\",{\\"tcDisplayPNGCharacteristics\\":{\\"width\\":320,\\"height\\":240,\\"bitDepth\\":16,\\"colorType\\":2,\\"compression\\":0,\\"filter\\":0,\\"interlace\\":0},\\"contentType\\":\\"image/png\\",\\"content\\":\\\"iVBORw0KGGoAAAANSUHEuGAAUAAADwCAYAAABxLb1rAAA0QkLEQVR4Xu2dCdGxVfXhrZASTDY3yAdQSQG1FE0UBaEC0cAtFSRks8VE0wxSQFv00VRScwEUQUQVE3mREwCFXNJuxAEeVMDQ0RLSuta5v985u-83t-ZOudd37b0-fzP0cpee_c-dZ09-Ze-6952zlkYqiFJst5D8oiqIUBRVARVEkiwggooiiFRQVQUZTCogKoKEphUQUFUkWWqAAqilJYVAARSRksKoCKohQWUFBUFUqLcQcKiKIVFBVRlMKiAqgoSmFRAVQUppbCoAcQKUIhUABVFKSwggIqiFJZUAvjhxx96c-f0X74wx96X_61719993X23XXXb3ddtvtN23vvvb3evXt7w4cP9372s5958-fP99555x1Zhr0bN2_27r__fu-0007zDj_8cK9Hjx7--fbbbz_v3_84x97v_9771_vf8tBG0Tsfeuhgb_z48d43vvEnR2fPnt7uu-}
```

_uffGLX_T2339_75vf_Kb305_-1HvkkUe8f_3rX_LwEI8__rj_OwN78803ZZFE_va3v5XUkabDK1euLCm_bNmykr__73__8_993Lhx_v3s1q2
b161TJ-9LX_qSd_7555eUjaNa901R8iJWAD_44ANvwoQJ3uc__3lvq622Sm2f-
cxnvK997WveK6-8IquMZdOmTb7Ifvaznw3VabPOnTt7t912m_9ANwbOe-6553otW7YmNspKtt12W--
UU06JbW07du1KjrnghhhtkUQEHlURDGOB33rWyX1EFOARYsW-
S8tWWdgCFcS1bpPipI3kQL417_8xdtjz1CndnFhn74YVltJPfdd5_XqlWrUB1p7KijjvK_3rJw9913e9ttt12ozrR2zTXXyCobqDUBvPzyy7
1PfepToFPMGzBggKitlGrdJ0UpB1YB_Oc__-ntueeeoQ6M8dZnyMSw1-ETw8QUxbr4X32ybFoBvPbaa71Pf_rToeOxFi1a-EJ84IEH-
v_bvHnzUBns4IMPdn64fvGLX0QKAv_eoUMH78tf_rI__GVo16xZs1C5ehHam266KVRPYGa7-
vfvL6troFr3SVHKHvUAL7roolDHPeSQQ7zf_va3kb4vRP0pp57yfWTBECuNAN57772hc_GQnXjiid6SJUu8LVu21JTH78RwCtGVx33ve98rKR
vHrFmzQsdj1ItQ_fwvf5WH-A8ufj18W_jMKF8PARjPPvuUDO-7du3qTZkyvVuzZo330Ucf-
UPTt956y_vNb37jXLJJBIn6n2rdJ0UpJ1YB1F9_Rx99tPef__xHFouFiQIESdhef_11r02bNiXnQjSYiEGc_-
SgQYNCd9fChQt10RAvvvii_8Uij2VsqD7IUfz3v__1br_9dv-
1EEWtCGDWNgZU6z4pSrkJCSAObt1zmVUsB_JB_dznPuc98cQTS1gkfHUYc2nWweRLEviiZBtdZj_TUmsCOHbsWfK0FbK-
St0nRSk3IQHk68jsqAxzyjF7xyTL11tvXXIuhs-
uMPySD_qKFStksQb4m_T79erVy_kLNw21JIAd03b0v8ZcqdZ9UPRKEBLAVatWhTpqlvVrSbBm0DwHQ1L8RlnAx2XWddVVV8kiDTAE101DZMpB
LQngxRdfLIu1olr3SVEqUGa6dxytnP06NGyWKPp06dPyTlYJyVM888s6SuE044QRZp4IADDigpi7-
zXNSACb5Y60o1n1S1EoQEKcQnR7j33D457Gqn51LH_Ehm_Zdeeqks1hqWZ5h18aVh4_333w8t1zn11FNlsdyoFQFs3bq1LJJKat0nRakUVgF8
8MEHQw9dYG3btvWGDnB1L6N4_vnnM_n0XnrppVC9bKWbPHlyiV122WUNxoNnGss1Ahs6dGhJXV_4whfkKX2WL18eOu_MmTn1sdyoFQFkHMMWq
nWfFKVSWAUQMbwVnd9m7AoYPHiw_3bfuHGjrMYKa-
1kPXnaNttsI0_ps3jx41BZ9i6Xi1oRwK9-9auySCqddZ8UPVJECiDceutXvv27UMdN8rwHfKWZyIljnnz5oW0zdMY5tqwLeZdunSpLJYbtSK
A515gF6p1nxS1UsQKILB0YsaMGV6_fv0itdzJY7vc1K1TZVUN2IRo--2393baaadclGpoZXugH330UVksN-
pdAkt1nxS1UikQoAliyPY21kawkDUpesrs2bN1FT6IjizLcKvc2IZ0hHMqF3kiINFb5G-
ulABW6z4pSqWvEKAJW6rY0vTtb3_burUMAWDMVcICWFn21ltukcVyx-
bUx3dZLVhaMs81ffp0WSQR21dYpQSwWvdJUSpFowTQZN26dX4kEPnAzJkzRxb1gwrIWHJnnHGGLJY7CLYU6pNPP1kWy40gYEJgV1xxhSySyLR
p00LXtFICWK37pCiViJcBhNdeey0ULonFrzb69u1Bu05wU5WAobt53p133tk50EBA5P7Xc845RxZJZMSIESV1YJUSQKjWfVKUSpCrAikMnjxs
2DBZxMcWcqcuc_rgAYgDK895xxx2yWC4cccQRJecZOHCGLBILQQR22GGH00-tpABW6z4pSiXIXQAJIGo-LFE7LYg_J4ej3bt3z7Rb3wXWKRl-
zDwvXz02X2VjmTrPUs152FXx3nvvyWKRXHn1SHxwSogpNW6T4pSCUIC-Oqrr3p__vf5T-ngqAJch8x0wWiIK-
EfLjZa9qYIe1zzz0n_ykESXzyPq8N246atJFU_vSnP4WE0rBKCIbu6z4pSrkJCSBLNuiC9KMf_ShxQbMJX1CsFZQPytq1a2XRBniQybgmjyE8
lcvmfajUMyxjxwNfWUmQtY7wUPK8hIMn-Gca1q9f75199t1-
qPko2CYoF5kz1pK8GnGw55r9u_L3BVZpAazWfVKUcmMVQL0T48hnKmdDyySHGRIFhXvFkVjVWNQqH5CRI0d-
UnEELLUgw5o81l0Cxx9_vHfzzTd7q1ev9oe0xCX8xz_-4c84P_bYY344JXaemEmNmLVmwx_-8IdQnLvgeJb18KASC4_2EGCCoTnr4BiW8gAHk
z1xIFgb_bDyHMQjP0mkk_wQ9LwgEFP2VbNMRk7SjBkzJnR8pQUQnWfFKWcJAqgzRiaRQ3PAsMXmPsgBpBLxCagWczlwVqwYIFzyk9pSQKIEJ
IvVx6Xxs4666yq7gSRV0s-
KUq5yCSASubIeVc_4oYNG0KzplmMp00uvPDCC6FAnS6WZiE1CZZcz0HipcSBufxbtQQQqnWfFKUchASQYS1DM2ZvbX6fKGNISJpMjm0MDE0RU
BmHLS722msv3x_3zDPpyOpSQYtjdjjIdXtRxtCZYTDIBqKy5EkYGiJqSe3iy91MN1RrAhhqJfukKHkTEKDJ22-_7Tv18eMwJGNhLj0A-
HRIb8i-YLZr8WWQJwgxmexwLzILGZwXvyK7EUjyze-ypa9sDPj9brzxRm_ixIned77zHd-
_haB8__vf92e0W0djlswghHfddZcvhqNGjflRx8-
Hr7AehaFa901R8iBRABVFUzoqKoCKohQWfUBFUQLCqCiKIVFBVBRlMKiAqgoSmFRAVQUpbCoACqKAywAZ81jYFnSHCi1gwqgojggA-
ruueesohSR6gAKooDKoBNi0gBnDlzp-
HNDc2wS1KPZJnX1YBfPEciABUC0bvf_-8siilIX5NmXVQCbfqAsPmNZ75M0AQcWAZGhBulflEBVJo82peVKFQA1SaP9mUlChVApcmjfVmJ
QgVQafJoX1aiKBHAZcuW-SHYsRNPLGk0-yxxx4Nf4uyF1980ayugZurV5aU4zwmQe6LcePG-WH1u3Xr5nXq1mKpUX_--
eeX1JUQzv7Z75_1I1YToBpv375-_o30nTv79RxyyCheCSec4Gdza0wu2qQ2ABnQCP1-2GGH-ekEdt99d--
ggw7yM8CRNS0plH0SH374oTd371w_8jLXibwaJHXfbbfdvL333tvr3bu3N3z4cD9K9_z58_30n65U6nrGQTtJCzB-
_Hh_2UrPnj39a8k1RbyIOE1-ZSJRR6UkKFdfJm2qWY5EUvng0r0r5Cc_-Yk3aNaG78ADD_TvI9eazIBkjrzzzjudc-
uY1EKfrXVKBJD0ZnYUV6Nj2ojLUbFo0SL_4ZV1BXb44YcbNf0_ZFoj9wgPe1z-XJsdFPDBfsJyV-
LaQEpL0o0817R27dp5U6ZMMWpNxcwff0BNmDDB0YMDs5Q8TK-88oqssorQXE8bmzZt8s4991yvZcuWofNEGak6Tzn1lFaby9WX81gW0sMoZH
ntBnZ83gRZBHCavbZeqGqaki-CHLkynpMGzBggKjN83MRy3KuxtcmicvTetWGO-64w--
ksv440_PMM0Xt0ZcjH8WWYelPfzww7LaEqpxPSV33313Sd5gV5PpScvVlxsjgORkpVLIIPnSmM77LCD9-STT8oqY61Wn60nqiaAN910U-
j4wJo1a9bw__v37y-
r13xg0S4Y0jNs6tq1a2zWMP2lpMXWhgceeMD_yjL_HUHnrnblLrvEdrIZM2bIU4Qg4RAPmDwWo26GpAx7GQ7T3i5duor-
D5ZVAMt5PU0QlAgXIIf_eoUMHP1sew1-G_Gb_CKzWBfDdd9_1h7nyPIGRb5n2MQyNusZ8GS9cuFBWHUk1-my9USKAjPfJ3oWRBc1sPB0w-
FuURfkL5I3Az2EOc3iw-Mxes2AN99FHH_k-wbfeessf11lyySWyuoYH1lSc-KSuu0IKP6OazR_E8A5fy-jRo_3y8qbSIdIg28D1MIeL-
Mruv_9-_y0fwLkZ4vp0yd0Xo7loYjjoosuCh1He8myZmsrIJr4pFCRBa6FtAJYyesZMGvWrFadGGJ0jmbpNj18hI8__rifWQ-
BprwUwHL15awCin9UthEhpw1r164tKUsfIuVq0DbT2rRp448K01CNPltvVGQWWN4I0xg6bdmyRR4Sy4oVK_yU1QimC48--
mjIx5U2QXDUG3ibXnfddbJ4CTi8cSrLY50Sqsuvv60PPt5mM1EqdJ1qsb1BCYaWrRoEbouLn2Ca3v77bf7L4Uo8uzLWQQMQMZNtbNWqVeIECu
1X8eHKY81JnYZqN16o6oCOHbsWfM07PA1JH8HXnJRLVBfn1EQWfееedS47t1auXLYAEwLyXMzq1RpZryeQWF0emzTrn4U8-7KrADKAyVh
rHsOQk6-
sNGzevNnr3r176DotXrxYfG1R6T5bj1RNAdt270jPb1YDZpbN33LeeefJIiFsbcd_5gIzn0bx22yzTeQXHV9HZlmgmxMtUiW681Xp_T78XBF
XY_GkGdfdhVavkzN8hiz1i4glrK04447ThYLUek-
W49UTQAvvvhWaxi8AY0fwuTCEnY2nDffffJYrGwFkvWEfVvt2rVq1DZN998UxarCbJcT4a5sn1cn3KQZ192FcARI0aE2unqagC5ZAX_YdIHR
KX7bD1SNQHMOgnygskV87e0b99eFgkh25CmA0o2btwYug5LliyRxXwY-
sjZTiYeapEs1_OAAw4o0SJSBPdnn3ZVQD18JfZ9CzgezPrwZKGwZXus_VIVQQX3neMHv8wgsV-
A5nQhYxDGPtEn5Gacccc0zJ72HZQRKyDcywusLQQXamefPmyWIN2Gbi-

DeGVczWlZNYXk98S3IpxqmnniqL5Uaefd1FANmJI-8fvYULLFyWdfFb4qhGn603qiKAjaLsmDBAm_o0KF0uwsdZlvyYSLbwBKCLMh1Vr_-9a
9lkQbYYSF_Z2Bt27b1hgwZ4i8f4uHIyy9Tieu5fPnyUHmiNpeLPPuyiwDa1lf0nj1bFksFs-
Jbb711SV0s74mjGn223qikAKadxo_jjTfe8AY0HFHsb2MsaauRbIO5rcgF2ZlYwEHs6Lyt9qMZRWDBw_2h0oMW1yp5PVk6CbLs3e5X0TZl10
E0DZ5wQsmKzvuuGNJXbyo4qhWn60nqiKAww9EwKuvvmpdJGoagsB-Syl28tNs20ti1r4GpBXG7J0Joah-
NXkb44yfD08HEykpKHS1_Pee-8NlV-6dKkslht59mUXAbznntC7XziiSdksdRif6Jtn7xJNftsvVB3AshSEBzJZn0YW6TYOcGDZK5st2Gb2Y
p7YCGvNmTtTDiv2YrUr18_r3nz5qHfbzPONXXqVF1VCdW4nviQZHkVWZeLPPuyiwCyy0K2k-
grWSFajFkX-4rjqHafrQfqTgDnJlTUhdG2CaXSQHbAxAj3wEJebcijMyGGLEAm7BU7BZL8dXF-
p2pcTxZKy_KIRbnIsy-7CCCiLtvZmKE--3XNuuiTcdRSn61V6k4A2Q4mf5frBABxsw6sLgHFvJqQzk6Ew5yNskTQ862tYwHh5lXG9W4ni-99
FKofDm3W0XZl10E0DbZc_3118tiqeC1J_den3766bJYCbXcZ2uFuhNAFFmXV1l1RFQ1KwDi3tgIa82lLszrVu3zhp1hC89G9W4ngi2F0qTTz
5ZFsuNPPuyiwAiWnItZ9LMBRT4DuU1Tnpp1EufrSaRAkiUCrPRPXr0kEVSk9eNINKJ7Arp91Sa8ADIEuIeWmirDZXoTK-99lroa8EWz62a11N
u8mfPadoACK7k2ZddBBA4l0v5KC688MLQNSZydxz11GerRaQAXnDBBSWNJmRVVvK6EYITikp3A1Xl0GHdZB5b0w0bVhkp1Jh1le9iwYbJiVa-
nFBKMQJ3lIM--
LH93kqD94Ac_CLXz6aeflSvViYaJKzrQTHtZJT1tvfbYaRArg1VdfXdJoovVmJa8bwReCWQ82ffp0WSyWqIi8SQ9sXm2oVGci9pt5Htt0i2peT
9YqsrHePIaZ5yhFZWPIsy-7CqBtMXTS8hWJzceaJpJSvfXZahApgLYwRzh1s5DXjQC5FICcFGkh0KdsU2BJD2xebUjbmVibF7eY0A6CJkjf0-
TJk2Uxn2pdTzjttNNCxxGJOe-hcJ592VUAgSCz8vwEe00D_YBw-
OaxRNfHiImJSvfZeiRSAIn8Kh8iwtOn6diSvG4E2B6aiRMnymIlMKtpi65sWlK78mpD2s7EA8IwBwd-2gXNWbcUawVl-2TU4YBqXU9gryxh0e
Sx9D0yr6Vh_fr1f1YzLixEkWdfziKATGDIvc_8d1KIEUKiZ2In2b7mbV6z9YjKQIicokExrCFFHpcXOKamTZt2jRZhU9eNwJwr14d6kwY2-
uIShIMoYhoy_YuhnTktDDLsodWHP_0M0TVhrSdCQE0y9GGSZmm-
eGMm0Qw99oymcFQ4ieT3BKybSNHjvykYkG1rmcA4fXlHleM68SyHtYHEgKe9uLzYujM0kLScvIbg8mepCCfefXl1AlI3Dt5fozJIPbWmMTP-7
huCCa-
Q9lXMHYBaS06VLrP1i0xAkjQSumnib0oRDJ53YiApP2x_GbbQ42NGjXKeecC5NWGtJ1JCqDNaGfS_cEXmNS2a1xPE_bHuqb8lJYkgHn15awCy
FfzmdFjQudxMdwVMv1nHJXus_ViRAACndv2VWGzqE6T140YIFZMjrPjYzi06YhZhti82pC2M6URwCQj5HwaP2I1rqeE0Fsky5L1pLWkNXGQR1
_0KoABJEK3ffEmGX5EW4Ko0CrDZ-uRRAEEhh98pv0232-
__XynrC11X1SnyetGSPhNcnmAzVgYbEbhyPLA5tWGtJ2JYS1DUPw9chN8nDEkJCIZx7pSyetpg2H2LbfcEhpiRxlCwjCYyBFx4bdMGtuXGyuA
8PLLL_tZ4mRfsBnLmbIuD6p0n61HUglgLCNDg08IpyZzY4__ng_Ego-FAIBpJktqwfefvttPxDqVvdd5Z11111-
qHuEutrK3l32BRNlZcOGDfJQJ2rleuL3u_HGG_0JmeB38EDzpcqMNTeiHEtmKlB1JvDpksKUdp144om-
MLNwGx8kM8BKea17AVQURcmKcQCiKIVFBVBRlMKiAqgoSmfRAVQUpbCoACqKULhUABVFKSx1FUBWrrNw1LR6X7tVq7Cn1rzOacNaZT2uHqE_P
vDAA_4um1_-8pc17WbNoVI8yiaQzzzTGHlOwtclfzJukMh63H1BDspDjggFBFNI0900rxUAFsImQVsqzH1QPscWZnheyDNlMBLCYqgB8zc-
ZMf69kYgW3qyeyClnW4-qBSY65JNT_okwFsJioAH5MnnpDqkFWIct6XK3DPtVrWuXtI3AB0Sx_uMf_-jHVKqVbKz-FKV4qAB-
TL0L4KWXUrH7Atr732kkWsNFUBx09ntosw8oTcUhQTFcCPqXcBzEpTFUCZq9g114lSHFQAP0YFsGkJ4LHHHlVsLsLcK4pEBfBjVACblgASK
NVsF_EMFUWIAvgxKoBNSwBlKsozzzxTF1EUNwEk3-yvfvUrP8MWC0s7d-7sh-
weNGiQH0F4Zzo1JeXzFMDNmzf7GcJI40hi6R49eviJtAlrzn8TRZF7Q6TWSuyZcv8YzCi8Zq_k9Dwwd-ijLSFSRBh-
dlnn_UjOR05uW_fvn7uC65dt27d_AeV80hk0XvuuefK4akhjaT525566ilZxExpjBfDDdz_05s6d6_vcCMW_7777-
veFBD70jd69e3vDhw_3I1bPnz_ft4VZDsikZrafc5vtInq2-
XfTbPdx5cqvJWx0KyasMeTfx40b57ebe9mpUyc_nD9JptJA32AnDn1CeIZInC81o3-QLY6seHfeeWeqvC42ktrA-YmszTNFP-
zSpYufhv0ggw7y_23JkiU15W1Qx0MPPEsdfvrp3qGHuqnb8D4_3x1p6mjmqSQMTnjDP0aEhBGGX8nbDlHg-
HPARw06ZN_sM18xJEGcJy2223-
R00Cdb7yeNdLCpVBCJMTg4eflKUI8lW1j_44IOyykSyClnW40jN0GHCB0dsbsxQ83C7ZDdLQ9pkRzaz3ce4fBqLFi0KCaxpvJCT4KVhy_lRM_
R--PHjnYUwQq3ca3kuaYh71DNLwnvnu3buHjpE2c0DayDqQtaIAs16Kt5JsVJwhQuSbbawAki-hVatWoTrSGBNr-DqJo1wCSI5eWdbV-
LIg41pasgpZlu04h2mSJ8UZD0-
eVeOAL7_8cn9JjazDtAEDBojaPoH1iUceeWTomDTG0sYnn3xSVh1JVBtIIZr0MWWMa1YdMKHfJF0H09AQ12e_UsQK4Pr16yPfUuRY5V0DIR1v
AZnqjwbzaSyPS3sRSHMYdZNatGjhp4AMGfjf5s2bh8pgfE3FiWC1BBzS2YNw6SePXt6Xbt2tWYkC4yv7rRkETJwPY5sdVFfDnypMBRk2MuXA
21kWGLKvYpAnjTTTEfjg2Mexv8__79-8vqfN59912_z8pjA6MN-
J4ZQkb1i5YtW3oLFy6UVVuxtWHOnDmhOn1203To4AatslKjhagpeyLwE5N9pf_v27b0dd9wx8r1lWJxmZFZJYgWQoYpsBBEJyBm8yUzw7bDKft
ttt20oa8vzmKYaYw4mj-
0i4qfDp7Bly5a8gzRGfbysMnj8LtFQepGIoRgMi8uW60Cv0VZV0rHQAD5zfhwuC58DdtSNzJcxg80evRoa8chekkaXIUsWPU4fL3yN9JGfEm
29gGiiU-S7GfB0DFvAdy4cWPJvZFCQ2Y5ef_i7qMUD_oy4hP8Ny-vKV0m-H7vjz76Yh-
w2U2C64MteDbw9cprh3Dgv167dm1JWZ4v0n3ywpThTgnTjTvtJnVai9d0WZBpD9-
g6TfHfUV_tbk2rrvu0j9joP1C45mUdeC2iqqDtKe1RKQA2t52f0k1bRmiQ_AmkMcGlnTjC0Zzg81j2rVr539NJoFfCmeyPGean2aes8ArVqzw
Hzg5KZTEo48-GvIZMZmqQBlchC3A9Tn79MSHmM1SHRxs55xPnauNLyWWApHqbhnpAv4SQQM1kP7p2kySrCx9k-RFjmk0RUGxgxMbkSB0Nt-
RXKvQ98FvwnF1UcTExJ332vXr1ksapiFUBmduSbh5v1xhtvyKJW-AKQ-
LAKgRQ3jQuNBcyLXxtMTadKak8hTAXsCXkxbxmwHWTcBWYAJfjePL38ZMYy1SLgEc03asLoIX4cyuT1DTSYi0sAIxzbZsHjxYlM0hKg2zJo
1Sxa1cs4554S0DYzk8mk4--yzQ8fykVMrWAWQUWj5oxn3uyC3IgUWJ4D8TQonwyZXGCB18_JVFketCCAwi2j-
1vP0008WCeEiZCYux7FxcZLkL3WfDoB5RDAjh07-qMMV3APyLpcd6YglrK04447ThYrwdYGfLNP4StdHo-
Zs8lJvPTSS6Hj77rrLlmsalGf80STTy75wfg-pM8vCb4WbQ7VOAFkrZhZlsk03n5ZkP5H1uHFUUsCyCyd-
VvSdFoXITN0W7Vq1U1ZTHWhtYi5RDAiy--
WBZLYgRI0J1ZXEBsD7PrAP_YZwg29qAj9IFJkdkHWlCsiZmJjJhs-6xVrAKoJxMGDJKiCyScmYD5cWLE8A-
ffqU1LXnzqWFDm_WhQM6jloSQDqp-VvwqSbhImQmLsfmXjJn0zEmb2QrcghGfTEC0fxldjwLrIyQvyluGCzbw0gqb1WEjX79-pXUgU-
PSR8XpA6ceupskjVCAkgU_XyIrNLIQss3pR1RQkgF1U6XQnxlBXZWfgiJkPcAkj7CMeEM5x2MazlocSnJ02YY44p-
S1c1yRchMzE9Tj5ksL4N4Z5Lrtwyk3eAsjkVBZYHSGv30tC88__3yoLu5fFLINsc-
ADRIUguUwrgwePLikjpN00kkWqRohAWTb1rzIv_vd72SxVmyePTtUV5QA2nwF7KSYPHlyiV122WUNhpcYxvKdWIOHVpSF2us4iiXAC5YsMD_
LeYSiwwtCqKwFXIALyPs_mHA2vbtq0_WmB5CA-r6-

xwnuQtgFn7g21NKM9FFph5l1j5ylm9FIdivA15wrs06oNY5x0CfM0njB1wohAWSJgrxhd0Ys2B6WKAfKp10WzdNYuB1H3gKID5QtQPJ3ZLWkbVC
uQhaQ5Tj2usrfZzNWDvD252ucdXqVJG8BTLPSxIZt8oKXYlakP42XaxSyDS6TFwGyDpY9uSIFMEsd5SIkgPfccc0_ohr366quyWcPvYiLrihLA
efPmhcrmaSzeJcNPAeR6yWVE0hAhdtkQuZlzmWbbZmZbrGuSRcgg63EM5ePWe0rDd8jDyKRKJchbAL0IB9ieJ5d1XRLPT4zbd5xHG2QdWcSrr
gSQxY3yhmV1_rkWV9YVJYC23R_bb7-9t9N00-VilRoCsywEJ7dsCxFS2EWxd0nSxBl1VtBL42tNAIEZyBkzZvhDq6jtiNjwok-
d01VW1Tu1IoEBMFLX4LHHHPFUiP35b0v0Io82iDryCJedSWAzCrJG4ZfMATyNh0LEKCbWKZZAJwXeQmgbas12_FcJghsX801KIAMIcGLuFnK
xMLZJJ9nVj9YWmpFAG39mrBgWWFX1fKXvz0KPNog68giXnU1gMxUyhvmunYoYPr06aG6ogSQhcqybCX3DeYlgnXcWY_rZMDNN98cuha1LoASH
PasFyOmHes5Zxt4kNnmVS5qRQCXL18eavv1118vi6WCL4zcl04cvijyaIo0sI4t41ZUAsk5IrvVi6JYf1nSY9WBRash55b5B12gojSUVAZThu5
gRdcW2i6beBNBk3bp1oeAEGF_L5aJWBBDRks9T3MxtHDaf0hNMUeTRB1lHFvGqKwEENuCbPzguv1kctqCRUQIIhNyy-
I3qxRE5DDPTcRpV9iHLNubdr-
nCeIr66lnAQTIycmvf1dRcqFWBBDoS3lc4wsvvLckHiz0PZVHG2QdWcSr7gSQLy_zBz0DumHDB1ksFttQGoSTQFuoJZzIleCCCy4o0S_hjlwh
Uo78_fiAXCAsvqWdQ3cBBPLCHDZsmCySG7UkgISGN-vCnn76aVksFibX50aAwk3F-ZbzaIo0sI4t41Z0A2hZDu3YgrtHJ0rA4AURApL-1KBhx-
x3z4uqrry4573bbbSeLJILfS7YXP6gLUdGcm4IAEmPRPfc5t0TVkgDaFkPHLV-
xYfMLJ0WmyaMNs04s41V3AghyGIYfgYUcabj77rtDNyuw0AEEm_8LMXWNv2aSJtmQLQwVDMxX5DIF14TcBJGUvyGwWhBA1jcmLci0gqAJ0hfG
zp5yUUSCCPL3YDfccIMsZoXrTiBi81gCjbB7Ko482iDryCJedSmArEWT0VzY6kT04jhYwiH39JqWJIA86HKxJ0YGRzf1iGwdY_jmCv40e2nZA
y0fULb9JAmPhGxa8rdPnDhRfUbuWWLb8N-0pN_hImQmLsfWDLsYsLIZUEzs71yUz0moyDnIRScagsgExgyNQD_zTRKOAhBZktLkebr0Y82yD
qyIfddCiCwhEFeeG4a69oQwiCyBFFC2C8s99_ahnNJAggsiTfD65vnJow3wwGSLr333nu-
b4SFxcw0ssCUsFf8DoawwXhMLqdBmHB2EJ32GGH-R2BGG6mTZs2TVbh_y7Z0TGE0VEwdIPgs6yXY4hsgzgKjsMVisCaJbld0-
aNMlFPM8kh7lfmQkhhn7Ub8vXMXLkyE8qLg01JoDatZLXAWPdJAFG6cP49lJXCcA-Q7kyAsMXmMYt1EcBZB1ZxEv25yx11ItYAaQT8-
DKG2AaAiH_DUM0bNP2aQQQCBVue3CyWFOBRHiJ2mOzqHBDsXt10YdNJLFR0bV7E4QKYA2021J1xBfYFJ7GkstCiBf-
mPGjAlDdxFdXZI2pWgebZB1ZBGvuhVayJLGj-
EOvqLGpsVksvmII44I1eFqafNqAOKTVniJBJCvUp1kKY3h10YhQcBTDLs1Wb1I7pQiwIYQEBQdUljDEmkjilJY82yDqyIfddC2AAw05Cgsu
bYhQrKNDkBsZfGiuAAQy3eXDiFivSCDJAPgJ-gysM5RiS8DVG_DmC0LZzRwlgAHXIPqs2Y5GwGSGkVgWQEQHDePXPJ9t1LH-
j6jWWXcuZaGwBRBefv1lP0ibvYgrjeVDd9xxh6wikTzaIoVil15NQgCBLxvWtF385z_3vvvd7_r-0MJ9k7eDB9g1UqwrPICE6-KhZbaYcyNC-
JNYu0jeEgJzurwlyw2-
PvY0M81BpjuiGT5K_DsEBuiayat1SKHI9cbvetZZZxcD9qHn5h9wQS5cF1DWiQYYeFD5Rli1ECaSV68LMzHx5w1Ep0SDicBVBRFaUqoACqKU
1hUABVFKSwggIqiFBYVQVEVRCosKoKIohUUFUGUwqICqChKYVEVBs1sKgAKopSWFQAK8jMmTP9_ZiBsX1MUZTqoQJYqFLKPKcoSj6oAFYQFU
bFNd931Z4476KCDvC5duvjh1EmIRmh0IjcTDTkPqTew-ORSGDRokB9CnuQw--yzj59Ri99w55135pZrgmx3c-
f09aNOE8qdnCK77rqrF07Ck_fu3dsbPny4H_F4_vz53jvvvC0raIDrFlxDov2aAki4fPMa24y0iDaS7g_XjGjNp0kkPDz3h_SK3Cv-
bcmSJSX1bVDHQw895J1--
uneoYce6ofBx_j_RLROU0cc1P_ss8_6EaWJIN23b1__nnbu3Nnr1q2b_7sJG3_1lVemyu0cR9L1ArIKkkaBhF60M7heJ510kp8SIktgVJ_RA
qgzAVg5hMgP0GHdh1K_m4z0tHixYUNWt1BiGx5UW1GfoXx48dnFkJSDU6YMMHPfSvrjMyvCHetmxXDdZ3sWi8o7E3Z9Fixb5LYNZlZTEPSP
HC4niu3fvHjpG2sCBAYPrsEHAR3KD8AJp3bp1qL44I8n8gw8-KKtMRdz1ev75532hk-
eT1q5d02_K1C1GrUq94yyA5557bqhjxBnJ1S-88EJRezJZstEFRHkJ598U1YZCw9xmRGcYZoSCotgNdcc42fHejWE2VkwC0nrwk5V7hvsmy
U8WWcVgtJFSyPd7Vx48Y1JN5KS9T14mWeJjGRaa4JlpTaxUkAyfgm00P79u39N30vXr1i00leem18hSRvPvuu_4wV9YRG0fBf8YXpi1bG9ay
ZUtv4cKfsmorJfUk-mLi4WA4xrCXL6aePXv6w01bXt9qC-Cc0XNCx5N-
ka91XgpRokbmu0BQSCw1_96sWTP_PpP1L0pcGRATNCuJKAHkHJ06dfKTRX0Nu3btGnlvMZJguWC7Xg888EDoPnKN-
NLBZZddYoVxxowZ8hRKHZJaAPK6at68ecN_H3744davLHw1x57bKjD0LHIKJcG_D7yeB4QMmWtXbu2pCxfirfeeqv_8Mhj2rRpk-
rLhIXt81j8t_jQSJfPA9EkeTvzPALcoxNAPEbkaU0k7mCSRAe_C3Kovx08v4gH0bQnexz-
LoYcgaQxY2XmG2If9111_nZ60xBwGcp69i0aVNkhbfcckDuSgCAURIucbURPES23XmvPh-R48ebRVEBCwt8npx7c0h0P7H---
_3-9PAZwfd0KfPn1C5-
ZYXtRKfZNaAE0777zzZPEQ112Weg4vrJsHd0EMZPHtWrVyheb0N5__33fDyePZVImCfn1R95S1yEWkz5r1qyR_1xCnrPAUfeH1xQTQnHw4pJ
fv1yDw0fH30jVGMCTTzwR-kJiFJDEihUr_PSGSddKwstT-
gxdt5HXS8EH_GPg8kaJkLksdde60sqTQZzgJIR0iL_0LBbrzXRlmsAYZQMue2X468hdOwefNmQ-M-
biKGLxpZnhnDc1AJAZw1a5YsauWcc84JHRsYCd3TwIypPPb111-
XxXKDL2x5Pr5a0B1vfCZp0EX7M4771xybBrBV2obJwFk200SdJzZWHxPZh3MtKXBkF0e85RTTPHFYkEsZR3HHXecLNYAy0zMsy10viys1Bu
AcRHmRa-w0TxdmK7mgRJ3eXxLi0qJ7hezP0lGY2A7Xrh13VBtGBus802ziMFpbZwEkDwarki0w0Wle1-
xIgRobKuYyQsXrwh7LExcaqVatC53zzdTlSvwtwCyyMQF21KmtBNHAUyMmMezVrOc8MVmni-
t6NuuV9IwX4I_VNZRrtGCUhmctBJA04MoLL7wQqofZShty-MtsYBbwzchzRg2DGTyjkGZZn07loJwCyGwvC7hd6NevX0kd-
PRY404CX1FmHSyCLyeIvHk-
ZqfTIK9X3EsxioBn5bUgTV2MbshXVILiENDc4YsLtIQWZJi1mULBMpuCtm5EIwssLBV1sXatihss3z8G0Nycwa0sZRTAN1B4YqcrWc5jCuDB
w8uqcPFRxyA6PKiZAKM5VIMA1lrN3bs2JAdc8wxJedjwiYN8n0xc-8Kw12zDmzevHmyfJHpbZA1r51Ra7pY5ZVY1sfNnv2bFksFVU2bPG_iM
y6mJCJgt0F8tyBtW3b1hsyZii_AwBhbYzPp5wCyNecK7K0_v37yyKJcG3M0hCotCyxSMAb0nRo6AXpakkRc0C21WUvWZAz32knjJTaJLUAXk1
eJCEXA_N1JbFNXvCAZEX6pnjQ4jj__PND57cZS3L46mGYzZDIhXIKoMvkRYCsw_ZiSkIKYJo63njJDX8Lnby2WS3N1kfZ1izXC6QA3n777bKI
UkekFsABAwBiIqkZnmXYSV0s2pXcc889oY7NWR0sSH8is4dJMATDpyR_R5ThR0JYmUhJgwqg50-A2Ratm8ZLhv3fe-2113-
NTLntV4xaLG4i25rleoEKYnmItCQyyDgrMgpKjx49ZBF_Fb7s2ETnyAr7U8262FecBhzjbHnISGnufIkzHoqpU6fKqkIUQXBZXSTe1rx-
RNphN87SpUsT_cy2mVgVQCUrQXwK1_5iisGjncse30YKW_7NiEmsoK-
znNumiPK4ghi28Je8ULIM1XleSLLoA2vYqs7TKZaKJSQdZhwgqkXUAsjm8Kww5DXrsm3wX758eahjX3_99bJYKhAuuXeUmHaNhckV1skrf7
Bfixah34vosmMgiqILIH-T7XedVCIun1kHpgKoZCW1AGJxgT-
jsM3ITpo0SRbrRUuux4ubuY0D36H87Xnv21y3b11odhuLWuMIRRDafHtm2Syx9QhSa9aBqQAqWXESQCYqXGEBsqwHf58NfINm0TboZ4H4g_Kc
RB7OG-
LoyS_NuFhXRLMxy9p8oWmR9yflay3riB0vKNiKINFzZHY2j3eJrw0ZD0qgEpWnASQEEuuEPnDrIPoG1HLRwizLs_59NNPy2Kx4GiXM4XsYXb


```
xM7kQhMIKjBnvKC644IKSssS8y4q8P1keaFlHlHjFkVYA33rrrJyWNrwaAGEWpN1YCqASlacBBDxwleXlJ__-c-
hsEtHHXWULNaAbTF0muUrJjYfETsIygVx5cxzxW0Fu_rqq0vKbrfddrJIauT9yfJAyzqixCuOtAKIK8Qsh02fP10WiyUqQrgKoJIVJwHECAGU
ZuU9X1ysH2THJ83sEiRTHnPDDTfIYlZYyajzxBOi6glUXBMmoW0NgiaIP2WkydPlsUasIVzcnmhmMj7k-
WBlnVEiVccaQUQ5NIkIomnxRanPDVAVQCUrzgKI0cnjZjvZlC8XP2025S8SJbkmHL-
OykEOWGtbMmT4r7IAHfliMwERdoFzUD7ZTABTEasNiGcsBRMtp-
leYAl8v5keaBlHXHiFYWLAJKNtL6viRMnymI1MEtsi9htWpr rJ9ua5XqBCmDTIrUAMuNprq3r2LGjP6RjWxMBD_C9rV-_3o-
uK3dhYMR0SxvaillieTzGWjz2XjIDyxcMHR_BxHco0yaGLzAp4gcCaB7Dkh30T6gkJjnMr10c-
QzTCaxgy38ycuTITyqQC4Fwb2pGLkmhP_0LRp06bJKnzK_cnyQMS64sQrChcBXL16dejlhvFiJmPL8FK1P9GvGCLLJVtyfJgKoJKV1AJIh6
GT2jowXzVyyqYtp_M0lVh1v_TFjxoTqTGGW7Y0lRlpgDZDoDD576bhC0zzIBISPqku02xrJsF2f1yRdcSJvXRSkJLqSNpzzbWx9TFs1KhRuhN
EyRUnAQs-wGQniDPWfrkGngwguGacsEYZfsS0kavTCGCSMBhj4kfkIbZ9QdqsQkgIwVbqoQkYyKLF6MKoJInzgIIfMXI7W3S-
CpkDzDD4sbw8ssv-1niZMezGutSyPPqAsNavk7xFdqG7LHG-j-
iEbt82ZowtOZlwlcnCfiYvJEz5lhTE8AA2i6XK9K14sZfUGFUMmTTAIYwAwqPirezjwITHyQtJqvKliw5gmb5PmSJA0lXxCiK-LB4mJ-
Q1SYfVf43QRCveqqq_zArYtPr4SI-sK-VfYF33vvvd6GDRvkoYoj-PpIasQkB-
tFWWfKdcanS3CJuNl7RcmDRgmgoihKPaMCqChKYVEBVBSlsKgAKopSWFQAFUUpLcQAiqIUfHVARVEKiwqgoiiFJVIAWQDMnszA4uL4KYqi1CO
RAqgoitLUUQFUFKWwqAAqilJYVAAVRSksKoCKohQWFUBFUqLcQAiqIUfHVARVEKiwqgoiiFRQVQUZTCogKoKEphUQFUFKWwqAAqilJYVAAVR
CosKoKiOhUUFUFUqLcQAiqIUfHVARVEKiwqgoiiFRQVQUZTCogKoKEphUQFUFKWwqAAqilJYVAAVR
SksKoCKohQWFUBFUqLcQAiqIUfHVARVEKiwqgoiiFRQVQUZTCogKoKEphUQFUFKWwqAAqilJYVAAVR
SlsKgAKopSWFQAFUUpLcQAiqIUfHVARVEKiwqgoiiFRQVQUZTCogKoKEphUQFUFKWw_B9FTUKADrx2aAAAAABJRu5ErkJggg\"}]]",
  "status" : "PENDING",
  "policy" :
  { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/policies/
QTazCPHRfwCBXcI1Rm9-FiDR1g" },
  "application" :
  { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/applications/
QTazdui396GxUj_w7N2Khr1edg" },
  "user" :
  { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTazw8gbh6Z777TpHz3pkXErIw",
    "userId" : "jbeloncik@daon.com" },
  "tenant" :
  { "href" : "https://api.identityx-cloud.com/IdentityXServices/rest/v1/tenants/r4SWIoHpn0fmXw4pkQhAbw" } }
```

Get Authentication Request

Retrieve an authentication request

Properties

Authentication Request Id textField

The identifier of the authentication request to be retrieved.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - username string required
 - password string required
 - authId string required

Output Schema

- output object
 - rawResponse object
 - complete boolean
 - verificationResult string
 - fidoResponseCode number
 - fidoResponseMessage string
 - status string

Output Example

```

{ "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/authenticationRequests/
QTazqDIl7wrj-v_gtombS9f_tw",
  "id" : "QTazqDIl7wrj-v_gtombS9f_tw",
  "complete" : true,
  "authenticationRequestId" : "8bAHBTRJ06N8vbLncP-Irg",
  "description" : "FIDO - 00B Auth Request",
  "verificationResult" : "Y",
  "expiration" : "2022-04-27T11:37:07.476+0000",
  "availableRetries" : 5,
  "totalRetriesAllowed" : 5,
  "processed" : "2022-04-27T11:24:51.484+0000",
  "oneTimePasswordEnabled" : false,
  "created" : "2022-04-27T11:22:08.033+0000",
  "type" : "FI",
  "fidoChallenge" : "Kcd2xYLyd1hwPwRwdrohcw",
  "secureTextTransactionContent" : "secure transaction details from postman",
  "secureTransactionContentType" : "text/plain",
  "fidoAuthenticationRequest" : "[{"header":{"upv":{"major":1,"minor":0},"op":{"Auth"},"appID":{"
  "https://example.com"},"exts":{"id":{"com.daon.sdk.envCheck"},"data":{"true"},"
  "fail_if_unknown":false},"id":{"com.daon.sdk.deviceInfo"},"data":{"true"},"fail_if_unknown":false},
  {"id":{"com.daon.sdk.location"},"data":{"true"},"fail_if_unknown":false}, {"id":{"
  "com.daon.sdk.authenticatorMetadata"},"data":{"true"},"fail_if_unknown":false}, {"id":{"
  "com.daon.sdk.healthCheck"},"data":{"true"},"fail_if_unknown":false}, {"id":{"fido.uaf.safetynet"},
  "data":{""},"fail_if_unknown":false}, {"id":{"com.daon.sdk.ados.decChain"},"data":{"
  "MIIIE6TCCAt0gAwIBAgIRAJEmGK-0XEGFin4brMpnidIwCwYJKoZIhvcNAQELMEcxFTATBgNVBAMMDElkZW50aXR5WCBDQTENMASGA1UECgw
  ERGFvbjESMBAGA1UECwwJSWRlbnRpdHlYMQswCQYDVQGEwJRTAeFw0xNzA2MTUwOTQ3NTFaFw0xOTA2MTUwOTQ3NTFaMFoxDTALBgNVBAoM
  BERhb24xZjEjBQBgNVBAsMCUlkZW50aXR5WDELMAkGA1UEBhMCUUxKDAwBgNVBAMMH0RFX0RBT05fQVVUSEV0VElDQVRJT05fREFUQV9LRUsWg
  gEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXrHT7hGCZR4KzlwawZl3yefpUov44BWofCNnuGh3RoaQ63vXX6jsrfoCVJdto5a38Nd
  7ckQzjhtuoAfLeUT3sbm7uhXCCoC5xJ_B96G6LeTvY6yZ2Zs03K8d018epK0I7e2Xh_3WQg0xa21QmJxnTcMSMj0TMhrXl66nh-
  CoTbAcKopm0xbrPFOmLoZ1xGk7i0VxSY_TRjep6tn4Z7t7r-
  bsJnDjJtcctto4gYXk7mDkdwAMfBpoq1Jp0nGbv8TCMySAjOUsS9ptE7pR15No6iF4QYNDUUhI9q7MAcpSgEYLaAPzhZdzZnmDfwwOIPCiss0
  qKV9L3H6wh-
  NLQ_r7AgMBAAGjcAgwb0wfgYDVR0jBHcwYAUZp1SSlDw67i7wEa-1wVzqzvdL5ahS6RJMEcxFTATBgNVBAMMDElkZW50aXR5WCBDQTENMAS
  GA1UECgwERGFvbjESMBAGA1UECwwJSWRlbnRpdHlYMQswCQYDVQGEwJRTAeFw0xNzA2MTUwOTQ3NTFaFw0xOTA2MTUwOTQ3NTFaMFoxDTALBgNVBAoM
  Cs0c6TEEG2GrL08wDAYDVR0TAQH_BAIwADA0BgNVHQ8BAf8EBAMCBLAwCwYJKoZIhvcNAQELA4ICAQA-
  cpJUe0Az96VXYHqIS_yRkltsSkLvmgquwux2fShZJQ1pawarF8qWH9takyyBzAPNVMySxIc4eMF4qRhExtADB5EQBFF-
  DWVMoLymYOLMDHi9lInuYdsV0B82EsQu5U7ScuDH3ffN01VJq2NS8jHUFm7GxF3606BdojT3vXgHmH_dZo3GzGCRDpkKt_gUA01aj2Ga1YmL
  cd2ptA60A1S1lW0eWS5yb_KNscCVVQke2gvJkACHrsIe17AxNBgukW1TANCrgH2U0hHhX10mu3RR0xhUL8Ya5V7qSdiVZzmFmZWryX92FbGU
  Ib_1L9n1Fs3iGtE9gXE-
  DVTNs93jn_XIK0Q8D6lcvpVtI4bJqHJ7u78MeoSPuYx-9SX4ioiNmVvYC6fdAieSG1ggEiIhw0U8l-4u1pItyPIqwt_OijaElOouTWzeBa3A
  JA7CqasOZ0mX6BXJE5dLcILbpYduA0vSc3em6cr-LJGrR7uuvQCJ-3p6X_gipMyailXYd2S985PQXsyKEW5AegBcEGNX3MIvNPuHb2eS-
  Ab_JIZbQGAUGTT_HwQXFB08pMXJ-
  UK_FwdphXVGMJy9jmyvwWLLBFXYGrAiq0pLlkHexCqHcjYbchgf1DIWp0yQ3KcoA42w555djBN7hFHTa9dfAdTOHRK1ICG_PhsmUdhZ_T7o
  Q==\\\"}\\\", \"fail_if_unknown\":false}, {\"id\": \"com.daon.sdk.ados.dekId\", \"data\": \"1000090661\",
  \"fail_if_unknown\":false}, {\"id\": \"com.daon.authRequest.retriesRemaining\", \"data\": \"5\",
  \"fail_if_unknown\":false}, {\"id\": \"com.daon.authRequest.maxAttempts\", \"data\": \"5\",
  \"fail_if_unknown\":false}, {\"id\": \"com.daon.user.retriesRemaining\", \"data\": \"10\",
  \"fail_if_unknown\":false}, {\"id\": \"com.daon.user.maxAttempts\", \"data\": \"10\", \"fail_if_unknown\":false},
  {\"id\": \"com.daon.face.retriesRemaining\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.face.maxAttempts\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.voice.retriesRemaining\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.voice.maxAttempts\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.passcode.retriesRemaining\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.passcode.maxAttempts\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.otp.retriesRemaining\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.otp.maxAttempts\", \"data\": \"3\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.identityx.version\", \"data\": \"5.2.4.0\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.D409#8201.ados.mode\", \"data\": \"enrol\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.D409#9201.ados.mode\", \"data\": \"enrol\", \"fail_if_unknown\":false}, {\"id\":
  \"com.daon.D409#8401.ados.mode\", \"data\": \"enrol\", \"fail_if_unknown\":false}, {\"id\":

```

```

\ "com.daon.D409#9401.ados.mode\","data\":"enrol\","fail_if_unknown\":false},{\"id\":"
\ "com.daon.D409#8201.recognition.timeout\","data\":"7000\","fail_if_unknown\":false},{\"id\":"
\ "com.daon.D409#9201.recognition.timeout\","data\":"7000\","fail_if_unknown\":false},{\"id\":"
\ "com.daon.D409#8401.recognition.timeout\","data\":"30000\","fail_if_unknown\":false},{\"id\":"
\ "com.daon.D409#9401.recognition.timeout\","data\":"30000\","fail_if_unknown\":false},{\"challenge\":"
\ "Kcd2xYLyd1hwPwRWDrohcw\","policy\":"{\"accepted\":[[{\\"aaid\":[\ "D409#2204\"],\"keyIDs\":"
[\"NDRBQj1GQzQtNUYyNC00QTA0LTk0NjMtMURFNEI5MTBEQ0Y1\"]]}}],\"transaction\":[{\\"contentType\":"text/plain\",
\ "content\":"c2VjdXJlIHRyYW5zYWN0aW9uIGRldGFpbHMgZnJvbSBwb3N0bWFu\"},{\"tcDisplayPNGCharacteristics\":"
{\\ \"width\\ \":320,\"height\\ \":240,\"bitDepth\\ \":16,\"colorType\\ \":2,\"compression\\ \":0,\"filter\\ \":0,\"interlace\\ \":
0},{\"contentType\\ \":\"image/png\", \"content\\ \":
\ "iVBORw0KGgoAAAANSUHuEUGAAUAAADwCAYAAABxLb1rAAAOQk1EQVR4Xu2dCdGxVfXhrZASTDY3yAdQSQG1FE0UBaEC0cAtFSRks8VE0wx
SQFv00VRSwEUQUQVE3eMREwCFXNJUAEEVMDQ0RLSuta5v985u-83t-Z08udd37b0-fzP0cpee_c-d2Z09-
Ze-6952z1KYqifJSt5D8oiqIUBRVARVEKiwwgoiiFRQVQUZTCogKoKEphUQUFUFWwQAAqilJYVAVRsksKoCKohQWFUBFUQQLCqCiKIVFBVBR
lMKiAqgoSmFRAVQUpbCoACqKULhUABVFKSwgqIqiFJZUAvjhxx96c-
f09X74wx96X_61719993X23XXb3ddtVN23vvvb3evXt7w4cP9372s5958-fP99555x1ZhR0bN2_27r__fu-0007zDj_8cK9Hjx7--
fbbbz__v3_84x97v__9771__vf8tBGQTSfeughb_z48d43vvEnr2fPnt7uu-
_uffGLX_T2339_75vf_Kb305_-1HvkkUe8f_3rX_LwEI8__rj_OwN78803ZZFE_v3v5XUkabdK1euLCm_bNmykr__73__8_993Lhx_v3s1q2
b161TJ-9LX_qSd_7555eUjaNa90lR8iJWAD_44ANvwoQJ3uc__3lvq622Sm2f-
cxnvK997WveK6-8IquMZdOmTb7Ifvaznw3VabP0nTt7t912m_9ANwb0e-6553otW7YmNpSKtt12W--
UU06JbW07du1KjrnhhhtkkUQEHlURDGOB33rWyXlEfOARYsW-
S8tWWdGcFcS1bpPipI3kQL417_8xdtjz1CndnFHn74YVltJPfdd5_XqlWRUB1p7KijjvK_3rJw9913e9ttt12ozrR2zTXXyCobqDUBvPzyy7
1PfepTofPMGzBgqKitlGrdJ0UpB1YB_Oc__-ntueeeoQ6M8dZnyMSwl-ETw8QuXbr4X32ybFoBvPbaa71Pf_rToeOxFi1a-EJ84IEH-
v_bvHnzUBns4IMPdn64fvGLX0QKAv_eoUMH78tf_rI__GVo16xZs1C5ehHam266KVRPYGa7-
vfvL6troFr3SVHKHvUAL7roolDHPeSQZ7zf_v3kb4vRP0pp57yfwTBECuNAN57772hc_GQnXjiid6SJUu8LVu2lJTH78RwCtGVx33ve98KR
vHrFmzQsdj1ItQ_fwvf5WH-A8ufj18W_jMKF8PARjPPvuUDO-7du3qTZkyxVuzZo330Ucf-
UPTt956y_vNb37jXXLJJB6n2rdJ0UpJ1YBlF9_Rx99tPef__xHFouFiQIESDhef_11r02bNiXnQjSYiEgC_-
SgQVNCd9fChQt10RAvvvii_8Uij2VSQD7IUfz3v__1br_9dv-
lEEWtCGDWNqZU6z4pSrkJCSAObt1ZmVUsB_JB_dznPuc98cQTslgkfhUyc2nWweRLEviiZBtdZj_TUmsCOHbsWFk0FbK-
St0nRSk3IQHk68jsqAxzyJf7xyTL1ltvXXIuhs-
uMPySD_qKFStksQb4m_T79erVy_kLNw21JIA03b0v8Zcqdz9UPRKEBLAVatWhTpqlvVrSbBm0DwHQ1L8RlnAx2XWddVVV8kiDTAE10lDZMPB
LQngxRdflIuolr3SVEqQUgA6dxytnP06NGyWKPp06dPyTlYJyVM888s6SuE044QRZp4IADDigpi7-
zXNSsACb5Y60o1n1S1EoQEKcQnR7j33D457Gqn5lH_Ehm_ZdeeqslhQWZ5h18aVh4_333w8t1zn11FNlsdyoFQFs3bq1LJJKat0nRakUVgF8
8MEHQw9dYG3btvWGDnbiL6N4_vnnM_n0XnrppVC9bKwBPHlyiV122WUNxoNnGss1Ahs6dGhJXV_4whfKX2WL18eOu_MmTNlsdyoFQFKHMMWq
nWfFKVSWAUQmBWVnd9m7AoYPHiw_3bfuHGjrMYKa-
lkPXnaTtsI0_ps3jx4lBZ9i6Xi1oRwK9-9aaySCqddZ8UpVJECiDceutXvv27UMdN8rwHfKWZyIljnnz5oW0zdMY5tqwLeZdunSpLJYbtSK
A5l5gF6p1nxS1UsQKILB0YsaMGV6_fv0itdzJY7vc1KlTZVUN2IRo--2393baaadclGpoZXugH330UVksN-
pdAkt1nxSLiUkQoAliyPY2lKawKDUPesrs2bNlFT6IjizLcKvc2IZ0HMQf3kIINFb5G-
ulABW6z4pSqVwEkAJW6ry0vTtb3_burUMAWDMVcICWFN2l1tukeVyx-
bUX3dZLVhams81ffp0WSQR21dYpQSWvdJUSpFowTQZN26dX4kEPnAZJkzRxb1gwrIWHJnnHGLJY7CLYU6pNPP1kWy40gYEJgV1xxhSySyLR
p00LxtFICWk37pCiViJcBhNdeey0ULonFrzb69u1bUo5wU5Aobt53p133tk50EBa5P7Xc845RxZJMSIESV1YJUSQKjWfVKUSpCAlKMnjxs
2DBZxMcWcquc_rgAYgDK895xxx2yWC4cccQRJecZ0HCgLBILQQR22GGH00-tpABW6z4pSiIXQAJIgo-LFE7LYg_J4ej3bt3z7R3wXWKRl-
zDwvXzU2X2vjmtRPUsl52FXx3nvvyWKRXHnllSHxwSopgNW6T4pSCUIC-Oqrr3p___vf5T-ngqAJch8x0wWiIK-
EfLjZa9qYIelzzz0n_ykESXzyPq8N246atJFU_vSnP4WE0rBKCIbU6z4pSrkJCSBLNUiC9KMf_ShxQbMJX1CsFZQPyqtq1a2XRbniQybgmjyE8
lcvmfaJUMyxjxwNfWUmQtY7wUPK8hIMn-Gca1q9f75199t1-
qPko2CYoF5KzlpK8GnGw55r9u_L3BVZpAazWfVKUcmMVQL0T48hnKMDyysHGRIHxvFvKjvJWNQqH5CRI0d-
UnEELLUgW5o8l1l0Cxx9_vHfzzTd7q1ev9oe0xCX8xz_-4c84P_bYY344JXaemEmNmLVmwx_-8IdQnLvgeJb18KASC4_2EgCCoTnr4BiW8gAHk
z1xIfGb_bDyHMQjP0mkk_wQ9LwgFEP2VbNMRk7SjBkzJnR8pQUQnWfFKWcJAqgzRiaRQ3PAsMXmPSgBpBLxCagWczlwVqwYIFzyk9pSQKIEJ
IvVx6Xxs4666yq7gSRV0s-
KUq5yCSASUBIEvc_4oYNG0KzplmMp00uvPDCC6FAnS6WZiE1CZZcz0HipSCBufxbtQQQnWfFKUchASQYS1DM2ZvbX6fKGNISJpMjm0MDE0RU
BmHLS722msv3x_3zDPPyOpSQYIjdjjIdXtRxtCZYTDBIqKy5EkYGiJqSe3iy9lMNLrAhHqJfukKHkTEKDJ22-_7Tv18eMwJGNhLj0A-
HRIB8i-YLZr8WWQJwgxmexLzILGzwXvyK7EUjyze-ypa9sDPj9brzxRm_ixIned77zHd-
_haB8__vf92e00Wdj1slwghHfddZcvhqNGjflRx8-
Hr7AehaFa90lR8iBRABVFUzoqKoCKohQWFUBFUQQLCqCiKIVFBVBRlMKiAqgoSmFRAVQUpbCoACqKAyWAZ81jYFnSHCi1gwqogjggA-
ruueeesohSR6gAKooDKoBni0gBnDlZpr-
HNDC2wSlKPZJnX1YBfPECIABUC0bvfv__8siilIX5NmXVQCbfFiqASpmnz75M0AqCwAZGhBulflEBVJo82peVKFQA1SaP9mU1ChVApcmjfvMj
QgVQafJoX1a1KBHAZcuW-SHYSRNPLGk0-yxxx4Nf4uyF1980ayugZurV5aU4zwmQe6LcePG-WH1u3Xr5nXq1MkPUX__-
eeX1JUQzv7ZZ5_1I1YToBpv375-_o30nTv79RxyyCheCSec4Gdza0wu2qQ2ABnQCP1-2GGH-ekEdt99d--
ggw7yM8CRNS0p1H0SH374oTd371w_8jLXibwaJHXfbbfdvL333tvr3bu3N3z4cD9K9_z58_30n65U6nrGQTtJCzB-
_Hh_2UrPnj39a8k1RbyIOE1-ZSJRR6UkKFdfJm2qWY5EUvng0rOr5Cc_-Yk3aNaG78ADD_TvI9eazIBkjrzzzjudc-
uY1EKfrXVKBJD0ZnYUV6Nj2ojLubFo0SL_4ZV1BXb44YcbNf0_ZFoJ9wgPe1z-XJsdFPDBfsJyV-
LaQEpL0o0817R27dp5U6ZMMWpNxcwff0BNmDDBOYMDs5Q8TK-88oqssorQqX8bmzT8s4991yvZcuWofNEGak6Tzn1lFaby9WX81gGw0sMoZH
ntBnZ83gRZBHCavbZeqGqAki-CHLkynpMgzBgqKjN83MRY3KuxtcmicvTETWGO-64w--

```

ksv440_PMM0Xt0ZCjhC8WWYELPfzww7LaEqpxPSV33313Sd5gV5PpScvVlxsjg0RKpVLIi0PnSmM77LCD9-STT8oqY6lWn60nqiaAN910U-j4wJo1a9bw__v37y-
ri3xg0S4Y0jNs6tq1a2zWmPL2pMXWhgceeMD_yjL_HUHNrbnLLrvEdrIZM2bIU4Qg4RAPmDwWo26GpAx7GQ7T3i5duoR-
D5ZVAMt5PU0QlagXIf_eoUMHP1sew1-G_Gb_CKzWBfDdd9_1h7nyPIGRb5n2MQyNusZ8GS9cuFBWHUK1-my9USKAjPfJ3oWRBc1sPB0w-
FuUrfkL5I3Az2E0c3iw-Mxes2aN99FHH_k-wbfeessfll1yySWyuoYHl1Sc-KSuu0IKP6OazR_E8A5fy-jRo_3y8qbSidIg28D1MIeL-
Mruv_9-_y0fwLkZ4vfp0yd0Xo7loYjjoosuCh1He8myZmsrIJr4pfCRBa6FtAJYyesZMGvWrFAdGGJ0jmbpNj18hI8__rifWQ-
BprwUwHL15awCiN9UthEhpw1r164tKUsfIuVq0DbT2rRp448K0lCNPltvVQGWNN4I0xg6bdmyRR4Sy4oVK_yU1QimC48--
mjIx5U2QXDUG3ibXnfdDbJ4CTi8cSrLY50Sqsuvv60PPtp5mMlEqdJ1qsb1BCYaWrRoEbouLn2Ca3v77bf7L4Uo8uzLWQQQMZNtbnWQVeIECu
1X8eHKY8lJnYZqN16o6oCOHbsWFm07PA1JH8HXxNJRLVBfnlEQWfееееdS47t1auXLNYAEwLyXMzq1RpZryeQWF0emzTrn4U8-7KrADKAyVh
rHsOQk6-
sNGzevNnr3r176DotXrxYfg1R6T5bj1RNADt270jPbLYDZpbN33LeeefJIiFsbcd_5gIzn0bx22yzTeQXHV9HZlmgmxMtUiW68lXp_T78XBF
XY_GkGdfdhVavkzN8hiz1i4glrK04447ThYLUek-
W49UTQAvvvhWaxi8AY0fwuTCEnY2ndffffJYrGwFkvWEfVvt2rVqLDZN998UxarCbJcT4a5sn1cn3KQZ192FcARI0aE2unqagC5ZAX_YdIHR
KX7bD1SNQHMOgnygskV87e0b99eFgkh25CmA0o2btwYug5LliyRxXwY-
sjZTiYeapEs1_OAAw4o0SJSBpDnn3ZVQDl8JfZ9CzgezPrwZKGwZXus_VIVQQQx3neMHv8wgsV-
A5nQhYxDGPtEn5Gaccc0zJ72HZQRKyDcywusLQQXamefPmyWIN2Gbi-
DeGVczWlZNYXk98S3IpxqmnniqL5UaeFDlFANmJI-8fyvULLfYWdfFb4qhGn603qiKajaLsmDBAm_o0KF0uwsZlvyYSLbwBKCLMh1Vr_-9a
9lkQbYYSF_Z2Bt27b1hgwZ4i8f4uHiyy9Tieu5fPnyUHmiNpeLPPuyiwDa1lf0nj1bFksFs-
Jbb711SV0s74mjGn223qikAKadxo_jjTfe8AY0HFhSb2MsaauRbIO5rcgF2ZlYwhEHs6Lyt9qMZRWDBw_2h0oMW1yp5PVk6CbLs3e5X0TZl10
E0DZ5wQsmKzvuuGNJXbyo4qhWn60nqiKAww9EwKuvvmpdJGoggsB-Syl28ttNs20ti1r4GpBXG7J0Joah-
NXkb44yfD08HEykpKHS1_Pee-8NlV-6dKkslht59mUXAbznntC7XziiSdksdRI6Jtn7xJNftsvVB3AshSEBzJzn0YW6TYocGDZK5st2Gb2Y
p7YCGvNmTtDiv2YrUr18_r3nz5qHfbzPONXXqVF1VCdW4nviQZHkVWZelPPuyiwCyy0K2k-
grWsfajFkX-4rjgHafqFqTgDznJlTUhdG2CaXSQHbAxj3wEJebciJmyGGLEAm7BU7BZL8dXF-
p2pcTxZKy_KIRbnIsy-7CCCilTvmZKE--3XNuuiTcdRSn61V6k4A2Q4mf5fRBABxzw6sLgHFvJqQzk6Ew5yNskTQ862tYwHh5lXG9W4ni-99
FKofDm3W0XZl10E0DbZc_3118tiqeClJ_den3766bJYCbXcZ2uFuhNAFFmXVli1RFQ1KwDi3tgIa82lLszrVu3zhp1hC89G9W4ngi2F0qTTz
5ZFsuNPPuyiwAiWnItZ9LMBRT4DuU1Tnpp1EufrSaRAkiUCrPRPxr0KEVSK9eNINKJ7Arp91Sa8ADIEuIeWmirDZXoTK-99lroa8EWz62a11N
u8mfPadoACK7k2ZddBBA4l0v5KC688MLQNSZydxz11GerRaQAXnDBBSWNJmRVVvK6EYTIkp3A1X10GHdZB5b0wObVhkp1Jh1le9iwYbJIVa-
nFBKMJQJ3lIM--
LH93kqD94Ac_CLXz6aeflsviYajKzrQTHtZJT1tvfbYaRArg1VdfXJoovVmJa8bwReCWQ82ffp0WSyWqIi8SQ9sXm2oVGci9pt5Htt0i2peT
9YqsrHePIaZ5yhFZWPIsy-7CqBtMXTS8hWJzceaJpJSvfXZahApgLYwRzh1s5DXjQC5FICcFGkh0KdsU2BJD2xebUjbmVibF7eY0A6CJkjf0-
TJk2Uxn2pdTztjttNNCxxGJOe-hcJ592VUAgSCz8vweE00D_YBw-
OaxRNfHiImJSvfZeiRSAIn8Kh8iwtOn6diSvG4E2B6aiRMnymIlMKtpi65sWlK78mpD2s7EA8IwBwd-2gXNwBcUawVl-2TU4YBqXU9gryxh0e
Sx9D0yr6Vh_fr1f1YzUixEkWdfziKATGDIVc_8d1KIeUKi2ZIn2b7mbVS6z9YjkQIIcokExrCFFHpcXOKamTzt2jRZHu9eNwJwR14d6kwY2-
uIShIMoYhoy_YuhnTktDDLSodWHp_0M0TVhrSdCQ0y9GGSZMm-
eGmM0Qw99oymcFQi4eT3BKbySNHjvykYg1rmcA4fXlHlEm68SyHtYHEgKe9uLzYujM0kLScvIbg8mepCCfexfXlLAII3Dt5fozJIPbWMntP-7
huCCa-
Q9lXMHYBaS06VLrP1i0xAKjQSumnib0oRDJ53YiApP2x_GbbQ42NGjXKeecC5NWGtJ1JCqDNaGfS_cEXmNS2a1xPE_bHuqb8lJYkgHn15awCy
FfzmDFjQudxMdwVMv1nHJXus_ViRAACndv2VWGzqE6T140IYFZMJrpyJzi06YhZhti82pC2M6URwCQj5HwaP2I1rqeE0fSky5L1pLWkNXGQR1
_0KoABJEK3ffEmGX5Ew4KioOCrdZ-uRRAEEhh98pv0232-
__XynrC11X1SnyetGSPHncmAZvgYbEbhyPLA5tWgtJ2JYS1DUPw9chN8nDeKJCIZx7pSyetpg2H2LbfcEhpiRxlCwjCYBYFx4bdMGtuXGyuA
8PLLL_tZ4mRfsBnLmbIuD6p0n61HUglgLcNDg08IpyZzY4__ng_Ego-FAIBpJktqwfefvttPxDqVvdd5Z1111l-
qHuEutrK3132BRNlZcOGdfJQJ2rleuL3u_HGG_0JmeB38EDzpcqMnteiHEtmKlBjVdPkSkUdp144om-
MLNwGx8kM8BKeal7AVQURcmKcQcKiKIVFBVBRlMKiAqgoSmFRAVQUpbCoACqKulhUABVFKSx1FUBWrrNw1LR6X7tVq7Cn1rzOacNaZT2uHqE_P
vDAA_4um1_-8pc17WbNoVI8yiaqAzzzzTghl0wtclfzJukMh63H1BDspDjjggfBFbNI0900rxUAFsImQVsqzH1QpScWZnheyDN1MBLCYqgB8zc-
ZMf69kYgW3qyeyClnW4-qBSy65JNT_okwFsJioAH5MnnpDqkFWIct6XK3DPtvWrVuXtI3AB0Sx_umf_-jHVkQvBkZ-FKv4qAB-
TL0L4KWXurH7Atsr732kkWsNFUBx09ntosw8oTcUhQTFcCPqXcBzEpTFUCZq9g141SHFQAP0YfSgKJ4LHHHlVSLsLcK4pEBfBjVACblgASK
NVsF_EMFUWiAvgxKoBNSwBlKsozzzTFLEUNwEk3-yvfvUrP8MWC0s7d-7sh-
weNGiQH0F4Zzo1JeXzFMDNmzf7GcJI40hi6R49eviJtAlrzn8TRZfQ7GTWSuyZcv8YzCi8Zq_k9Dwwd-ijLSFSRBh-
dlnn_UjOR05uW_fvn7u6C5dt27d-AeV80hk0Xvuuefk4akhjaT525566ilZxExpjBfDDdz_05s6d6_vcCMW_7777-
veFBD70jd69e3vDhw_3I1bPnz_ft4VZDsikZrafcs5vtInq2-
XfTbPdx5cQJWxOKyasMeTfx40b57ebe9mpUyc_nd9JptJA32AnDn1CeIZInCB1o3-QLY6seHfeeWeqvC42ktrA-YmszTNFP-
zSpYufhv0ggw7y_23JkiU15W1Qx0MPPEsdfvrp3qGHHuqnb8D4_3x1p6mjmqQSQTnjDPoAEhBGGX8nbDlHg-
HPARw06ZN_sM18xJEGcJy2223-
R00Cdb7yeNdLCpvBCJMTg4efLkUI8lw1j_44I0yykSyClnW40jNOGHCBOdsbsxQ83C7ZDdLQ9pkRzaz3ce4fBqLFi0KcaxpvJCT4KVhy_lrM_
r--PHjnYUwqQ3ca3kuaYh71DNLwvnu3buHjpe2c0DAYdDqTaIAsl6Kt5JsVJwhQuSbbawAki-hVatWoTrSGBNr-DqJo1wCSI5eWdbV-
LIg41pasgpZlU04h2mSJ8UZD0-
eVEoAL7_8cn9JjazDtAEDBojaPoH1iUceeWTomDTG0sYnn3xSVh1JVBTiIZr0MWMa1xYdMKHfJF0H09AQ12e_UsQK4Pr16yPfUuRY5V0DIR1v
AZnqjwbzaSyPS3sRSHMYdZNatGjhP4AMGfjf5s2bh8pgfE3FiWClBbZs2YNw6SePXt6Xbt2tWYkC4yv7rRkETJwPY5sdVfFDnypMBRk2MuXA
21kWGXLKVyPanjTTTEfjg2Mexv8__79-8vqfN59912_z8pjA6MN-
J4ZQkb1i5YtW3oLFy6UVVuxtWHOnDmhOn1203To4Ats1KjhaagepyLwE5N9pf_v27b0dd9wx8r1lWJxmZFZJYgWQoYpsBBEJyBm8yUzw7bDKft
ttt20oa8vzmkyAYw4mj-
Oi4qfDp7Bly5a8gzRcfbysMnj8LtFQepGIoRgMi8uW60Cv0VZVORHQAD5zfHwUc58DdtSNzJcxg80evRoa8chekkaXIUsWPU4fL3yN9JGfEm

29gGiIU-S7GfB0DFvAdy4cWPJvZFCQ2Y5ef_i7qMUD_oy4hP8Ny-vKV0m-H7vjz76yH-
w2U2C64MteDbw9cprh3Dgv167dm1JWZ4v0n3ywpThTgnTJtVzJNVai9d0WZBpD9-
g6TfHfUV_tbk2rrvu0j9joP1C45mUdeC2iqdQtKe1RKQA2t52f0k1bRmiQ_AmkMcGlnTjc0Zzg81j2rVr539NJoFfCmeyPGeaN2aes8ArVqzw
Hzg5KZTEo48-GvIZmqMB1chC3A9Tn79MSHmM1SHRx55xPnaULYWWApHqbhnpAv4SQQM1kP7p2kySrCx9k-RFjmk0RUGxgxMbkSB0Nt-
RXKvQ98fvwNF1UcTExJ332vXr1ksapiFUBmduSbh5v1xhtvyKJW-AKsq-
LAKgRQ3jQuNBcylXxtyMTadKak8hTAXsCXkxbmvHWTcBWyAJfjeLPL38ZMYy1SLgEc03asLJoIX4cyuT1DTSYi0sAIXzbZsHjxYlM0hKg2zJo
1Sxa1cs4554S0DYzk8mk4--yzQ8fykVMrWAWQWUj5oxn3uyC3IgUWJ4D8TQonwyZXGCB18_JVfketCCAwi2j-
lvP0008WceEiZCYux7FcxZLkL3WfDoB5RDAjh07-qMMV3APyLpcd6YglrK04447ThYrwdYGfLNP4StdHo-
Zs81JvPTSS6Hj77rrLlmsalgF80STTy75wfg-pM8vCb4WbQ7V0AFkrZhZlSk03n5ZkP5H1uHFUUsCyCyd-
VvSdFoXITNx0W7Vq1U1ZTHWhtYi5RDAiy--
WBZLxYgRI0J1ZXEBsD7PrAp_YZwg29qAj9IFJkdKHWlCsiZmJjJHs-6xVrAKoJxMGDJkiCySCmYD5cWLE8A-
ffqU1LXNZqWFDm_WhQM6j1oSQDqp-VvwqSbhImQmLsfMxJn0zEmb2QrcghgFtEC0fxldjwLrIyQvyluGCzbw0gqb1WEjX79-pXUgU-
PSR8XpA6ceuqpskjVCAkgU_XyIrNLIQss3pR1RQkgF1U6XQnx1BXZWfgiJkPcAkj7CMeEM5x2MazlocSnJ02YY44p-
S1c1yRchMzE9Tj5ksL4N4Z5Lrtwyk3eAsjkVBZYHSGvF30tC88__3yoLu5fFLINsc-
ADRLUguUwrgwePLikjpN00kKwqRohAWTb1rzIv_vd72SxVMyePTtUV5QA2nwF7KSYPHlyiV122WUNhpCYxvKdWIOHVpSF2us4iiXAC5YsMD_
LeYSiiWtCqKwFXIALyPs_mHA2vbtq0_WmB5CA-r6-
xwnuQgtgFn7g21NKM9FFph51j5ylm9FIdvA15wrs06oNY5x0CFm0njB1wohAWSJgrxhd0Ys2B6WKAfKp10WzdNYuB1H3gKID5QtQPJ3ZLWkbVC
uQhaQ5Tj2usrfZzNWDvD252ucdXqVJG8BTLpsxIZt8oKXYlakP42XaxSySD6TFWgyDpY9uSIFMEsd5SIkgPfcc0_ohr366quyWCPYvILrihLA
efPmhcrmaSzeJCNPAAeR6yWVE0hAHdtKQuZlzmWbbZmZbrGuSRcgg63EM5ePwe0rDd8jDyKRKJchbAL0IB9ieJ5d1XRLpT4zbd5xHG2QdWcSrr
gSQxY3yhmV1_rKwV9YVJYC23R_bb7-9t9N00-VilRoCsyeJ7dsCxFS2EWd0nSxB11VtBL42tNAIEZyBkzZvhDq6jtiNJwok-
d01VW1Tu1IoBEMJLX4LHHHPFUip35b0v0Io82iDryCJedSWAZCrJG4ZfMatyNh0LEkCbWKZZAJwXeQmgbal2_FcJghsX801KIAmiCGLuFnK
xMLzJJ9nVj9YWmpFAG39mrBgWwFX1FkXvz0KPNog68giXnUlgMxUyhvmunYoYPr06aG6ogSQhcqybCX3DeYlgNxcWY_rZMDNN98cuha1LoASH
PasFyOmHesSZxt4kNnmVS5gRQCXL18eavv1118vi6WC14zcl04cviyaIoSI4t41ZUAsk5IrvVi6JYfInSY9WBRASH55b5B12gojSuvAZThu5
gRdcW2i6beBNBk3bp1oeAEGF_L5aJWBBDRks9T3MxtHdAf0hNMUeTRB1lHFvGqKwEENuCbPzguvlktctqCRUQIIhNyyy-
I3qxRE5DDPTcRpV9iHLNubdr-
nCeIr66lnAQTIycmvF1dRcqFWBBD0S3lc4wsvvLckHiz0PZVHG2QdWcSr7gSQLy_zBz0DumHDB1ksFttQGosTQFuoJZzIleCCCy4o0S_hjlwh
Uo78_fiAXCAsvqWdQ3cBPP1CHDZsmCySG7UkgISGN-vCnn76aVksFibX50oAwk3F-ZbzaIoSI4t41Z0A2hZDu3YgtrHJ0rA4AURApL-1KBhx-
x3z4uqrry4573bbbSeLJILfS7YXP6gLUdGcm4IAEmPRPfc5t0TVkgDaFkPHLV-
xYfMLJ0WmyaMNso4s41V3AgHyGIYfgyUcabj77rtDNyu0AEEm_8LMXWNv2aSJtmQLQvDmxX5DIF14TcBJGUvyGwWhBA1jcmLci0gqAJ0hfG
zp5yUUsCCPL3YDfccIMsZoXrTiBi81gCjbb7Ko482iDryCJedSmArEWT0VzY6kT04jhYwiH39JqWJIA86HKxJ0YgRZF1iGwdY_jMcV40e2nZA
y0fULb9JAmPhGxa8rdPnDhRFiuBWWLb8N-0pN_hImQmLsfwxDLsYsLIZUEzs71yUz0moyDniRScagsgExgyNQD_zTRK0AhBZktLkebr0Y82yD
qyiFddCiCwhEFeeG4a69oQwiCyBFFC2C8s99_ahnNJAgsiTFD65vnJow3wwGSLr333nu-
b4SFxcw0ssCUsFf8DoawwXHMLqdBLmHB2EJ32GGH-R2B6G6mTZs2TVbh_y7Z0TGEm0VEwdIPgs6yXY4hsgzgKjsMVisCaJbld0-
aNM1fPM8kh71fmQkhhn7Ub8vXMXLkyE8qLg01JoDAtZLXAWPdJAFG6cP49lJXCcA-Q7kyAsMXmMYt1ECbZB1ZxEv25yx11ItYAAQT8-
DKG2AaAiH_DUM0bNP2aQQCBVue3CyWf0BRHiJ2mOzqHBDStx10yDNJLFR0bV7E4QKYA2o21J1xBfYFJ7GkstCiBf-
mPGjAlDxDxZi2pWgebZB1ZBGvuhVayJLgJ-
EOvqLGpsVksVmII44I1eFqafNqAOKTVniJBJCvUp1kKY3h10YhqWcBTDLS1Wb1I7pQiwIYQEBQGdU1jdEmkjilJY82yDqyiFddC2AAw05Cgsu
bYhqRKNdkBzsfGiuAAQy3eXDiFiVSCDJAPgJ-gysM5RiS8DVG_DmC0LzZrWlgAHXIPqs2Y5GwSGKvGwQEQHDePXPnj9t1LH-
j6jWWXcUZAqGWBRebFv1lP0ibvYgrjeVDd9xxh6wikTzaIOvI15NqgCBLxvWtf385z_3vvvd7_r-OMJ9k7eDB9g1UqwrPICE6-KhZbaYcyNC-
JNYu0jeEgJzurwlyw2-
PvY0M81BpjjuGT5K_DsEBUiyat1SKHI9cbvetZZZxXd9qHn5h9wQS5cF1DWiQYyFeFD5Rli1ECaSV68LMzHx5w1Ep0SDicBVBReFaUqoAcqKU
1hUABVFKSwggIqiFBYVQEVRCosKoKIohUUFUGUwqICqChKYVEVBs1sKgAKopSWFQAK8jMmTP9_ZiBsX1MUZTqoQJYQfLKPkcSj6oAFYQFU
BFqS1UACuICqCi1BYqgBVEVBVRagsVwAqiAqgotYUKYAVRAVSU2iJSAFeuX0mHZg9s2bJLJX8n-
vNdd931Z4476KCDvC5dvvjh1EmiRMh0IjcTDTkPqIew-ORSgDRokB9CnuQw--yzj59Ri99w55135pZrgmx3c-
f09aNOE8qdnCK77rqrF07Ck_fu3dsbPny4H_F4_vz53jvvvC0raIDrFlxDov2aAki4fPma24y0iDaS7g_XjGjNp0kkPDz3h_SK3Cv-
bcmSJSX1bVDHQw895J1--
uneoYce6ofBx_j_RLROU0cc1P_ss8_6EaWJIN23b1__nnbu3Nnr1q2b_7sJG3_1lVemyu0cR9L1ArIKkkaBhF60M7heJ510kp8SIktgVJ_RA
qgzAVg5hMgP0GHDh1K_m4z0tHixYUNWt1BiGx5UW1GfoXx48dnFKJSDU6YMMHPfSvrjjMyvCHETmxdXdDz3sWi8o7E3Z9Fixb5LYNZlzTEPSP
HC4niu3fvHjpG2sCBAYPrSEHaR3KD8AJp3bp1qL44I8n8gw8-KKtMRdz1ev75532hk-
eT1q5d02_K1C1GrUq94yyA5557bqhjxBnJ1S-88EJRezJZstEFRhKjJ598U1YZCw9xmgRGcYZoScotgNdcc42fhEjWE2VkwC0nrwk5V7hvsmy
U8WWcVgtJfJSyPd7Vx48Y1JN5KS9T14mWeJjGraa4JlpTaxUkAyfgm00P79u39N30vXr1i00leeum18hSrvPvuU_4wV9YRG0fBf8YXpi1bG9ay
ZUtv4cKfsmorJfUk-mLi4WA4xrCXL6aePXv6w01bXt9qC-CcOXNcX5N-
ka91XgpRokbmu0BQSCw1_96sWTP_PpP1L0pcGRATNCuJKAHKHJ06dfKTRX0Nu3btGnlvMZJguWC7Xg888EDoPnKN-
NLbZddYoVxxowZ8hrKHZJaAPK6at68ecN_H3744davLHw1xx57bKjD0LHIKJcG_D7yeB4QMmWtXbu2pCxfirfeeqv_8Mhj2rRpk-
rLhIxt81j8T_jQSJfPA9EkeTvZvPALcoxNAPEbkaU0k7mCSRAe_C3Kovx08v4gH0bQnexz-
LoYcgaQxY2XmG2If9111_nZ60xBwGcp69i0aVnKhBfccktdUSgCAURiucbURepS23XmvPh-R48ebRVEBCwt8npx7c0h0P7H---
_3-9PAZwfd0KfPn1C5-
ZYXtRKfZNaAE0777zzZPEQ1112Weg4vrJsHd0EMZPHtWrVyheb0N5__33fDyePZVImCfn1R95S1yEWkz5r1qyR_1xCnrPAUfeH1xQTQnHw4pJ
fv1yDw0FH30jVGMCTTzwr-kJiFJDEihUr_PSGSddKwstT-
gxdEt5HXS8EH_GPg8kaJkLksdde60sqTQZzgJIR0iL_OLBbrzxRlmsAYZQMUE2X468hdOwefNmQ-M-
biKGLxpZnhnDc1AJAZw1a5YsauWcc84JHRsYcd3TwIypPPb111-
XxXKDL2x5Pr5a0xB1rVcZp0EX7M4771xybBrBV2obJwFk200SDJzZWHxPZh3MtkXBkF0e85RTTPHFYkEsZR3HHXecLNYAy0zMsgy10viys1Bu


```

AcRhmRa-w0TxdMk7mgRJ3eXxLI0qJ7hezP0lGY2A7Xrh13VBtGBus802ziMFpbZwEkDWarkioW0Wle1-
xIgRobKuQyWQSxrwH7LExqaqVatC53zzzTdlsVwotwCyyMQF21KmtBNHAUyMmMezVrOc8MVmni-
t6NuuV9IwX4I_VNZRrtGCUhmCBAJ04MoLL7wQqofZShTy-MtsYBbwzchzRg2DGTyjkGZZn07loJwCyGwvC7hd6NevX0kd-
PRY404CX1FmHSyCLyEivHk-
ZqfTIK9X3Esxio0bN5bUgTV2MbhsXVILIENDc4YsLtIqWZJi1mULBMpuCtm5EIwssLBV1sXatihss3z8G0Nycwa0sZRTANlB4YqcrWc5jCuDB
w8uqcPFRxyA6PKiZAKM5VIMa1lrN3bs2JAdc8wxJedjwiYN8nox-8Kw12zDmzevHmyfJHpbZA1r5lRa7pY5ZVY1sfNnv2bFksFVu2bPG_iM
y6mJCJgt0F8tyBtW3b1hsyZii_AwBhbYzPp5wCyNecK7K0_v37yyKJcG3MOhCotCxYsMab0nRo6AXpakkrc0C2lWUvWZAz32knjJTaJLUAXk1
eJCEXA_N1JbFNxvCAZEX6pnjQ4jj_PND57cZS3L46mGYzZDIhXIKOMvKRYCsw_ZiSkIKYJo63njJDX8Lnby2WS3N1kfZ1izXC6QA3n777bKI
UkekFsABAWbIIqkZNmxYsV0s2pXcc889oY7NWr0sSH8is4dJMATDpyR_R5ThR0JYmUhJgwqg50-A2Ratm8ZLhv3fe-2113-
NTLntV4xaLG4i25rleoEKYNmitQCyyDgrMgpKjx49ZBF_Fb7s2ETnyAr7U8262FecBhzjbHnISGnufIkzHoqpU6fKqkIUXQBZxsTElrx-
RNphN87SpUsT_cy2mVgVQCURqQXwK1_5iisGjncse30YKW_7NiEmsoK-
znNumiPK4ghi28Je8ULIMlXleSLLoA2vYqs7TKZaKJSQdZhwqgkpXUAsjm8Kww5DXrsm3wX758eahjX3_99bJYKHauuXeuMHaNhckV1skrf7
BFixah34vosmMgiqILIH-T7XedVCIun1kHpgKoZCW1AGJxgT-
jsM3ITpo0SRbrRUuux4ubuY0D36H87Xnv21y3b11odhuLWuMIRRDafHtm2Syx9QhSa9aBqQAqWXESQCYqXGEBsqwHf58NfINm0TboZ4H4g_Kc
RB7OG-
LoyS_NuFhxRLMxy9p8oWmR9yflAy3riB0vKNiKINFzHJY2j3eJrw0ZD0qgEpWnASQEEuuEPnDrIPoG1HLRwizLs_59NNPy2Kx4GiXM4XsYXb
xM7KqHMKJjBnvKc644IKSssS8y4q8P1keaFlHlHjFkVYA33rrrZJyWNRwaAGEWpN1YcqASLacBBDxwleXlJ__-c-
hsEtHHXWULNaAbTF0muUrJjYfETsIygVx5cxzxW0Fu_rqq0vKbrfddrJIAuT9yfJAYzqixCu0tAKIK8Qsh02fP10WiyUqQrgKoJIVJWHECAGU
ZuU9X1ysHZTHJ83sEiRTHnPDDtFIY1ZYyYajzxBOi6glUXBMmoW0NgiaIP2WkydPlsUasIVzcnmhmMj7k-
WBlnVEiVccaQUQ5NikIomnxRaNPDAVQCURzgzKI0cnjZjvZlC8XP2025S8SJbKmhL-
OykEOWGtbMmT4r7IAHFliMwERdoFzUD7ZTABTEasNiGcsBRMtp-
leYA18v5keaBlHXHiFYWLAJKNtL6viRMnymILMEtsi9htWprJ9ua5XqBCmDTIrUAMuNprq3r2LgJP6RjWxMBD_C9rV-_3o-
uK3dhYMR0SxvailiieTzGwJz22jIDyxcMHR_BxHcoOyaGLzAp4gcCaB7Dkh30T6gkJjnMr10c-
QzTCaxgy38yCuTITyqQC4FwbG2pGLkmhP_0LRp06bJKnzK_cnyQMs64sQrChcBXL16dejlhvFiJmPL8FK1P9GvGCLLJVtyfJgKoJKV1AJIh6
GT2jowXzVyqYtp_M0lVh1v_TFjxoTqcTGGW7Y0lRipgDZDoDD576bhC0zzIBISpku02xrJsF2f1yRdcSJvXRSKJLqSNpzzbWx9TFs1KhRuhN
EyRUaQS-wGQniDPWfrkGngwguGacsEYzfsS0kavTCGCSMBHj4kfkIbZ9QdqsqQkIwVbqoQkYyKLF6MKoJInzgIIFMXI7W3S-
CpkDzDD4sbw8ssv-1niZMezGUtSyPPqAsNavk7xFdqG7LHG-j-
iEBt82ZowtOZlwcNcfiYvJez5lhtE8AA2i6KX9kM14szFUGFUMMTaiYwAwqPirezjwITHyQtJqvKlIw5gmb5PmSJA0lXxCiK-LB4mJ-
Q1SYfVf43QRCveqqq_zArYTPr4SI-sK-VfYF33vvvd6GDRvkoYoj-PpIasQkB-
tFWWfKdcans3CJuNl7RcmDRgmgoihKpAMCqChKYVEBVBSlsKgAKopSWFQAFUUpLCqAiQIUFhVARVEKiwggoiifJVIawQDMnszA4uL4KYqi1CO
RAqgoitLUUQFUFKwWqAAqilJYVAVRsksKoCKohQWFUBFUQlCqCiKiVFBVBRlMKiAqgoSmFRAVQUpbCoACqKUlhuABVFKSwqgIqiFBYVQVEVR
CosKoKiOhUUFUFGUwqICqChKYVEBVBSlsKgAKopSWFQAFUUpLCqAiQIUFhVARVEKiwggoiifRQVQUZTCogKoKEphUQFUFKwWqAAqilJYVAVR
SksKoCKohQWFUBFUQlCqCiKiVFBVBRlMKiAqgoSmFRAVQUpbCoACqKUlhuABVFKSwqgIqiFBYVQVEVRCosKoKiOhUUFUFGUwqICqChKYVEBVBS
SlsKgAKopSWFQAFUUpLCqAiQIUFhVARVEKiwggoiifRQVQUZTCogKoKEphUQFUFKwW_B9FTUKAdrx2aAAAAABJRUErKJggg\}}]]",
  "fidoAuthenticationResponse" : [{"header":{"upv":{"major":1,"minor":0},"op":{"Auth"},"appID":{"
"https://example.com"},"exts":{"id":{"com.daon.capture.edek"},"data":{"ALnaVOLAKy_woNCP-
DLwwrwGGKZJjahZ83gS-nw9S-i_RCWuKkzDebZIVavvTEAS9_s6dobKQkRSIuz8E5SXMKUGYfy8nYPvPZK_5xqHXdj0xFK6ffATgSnLXz-
HcmK3SEi6fV3N9LwAyU_Pg9NqoCnIWCAY9Y5kcC0q82YEEQJvhqu6jyGgqAbBPJREiGLFYfyLo0_arXTQPyz-xhNjuGpCcZIZhYi50QEdL3-
tV8NdLYAQDRPHnwWYheSATg4Q6rDzzC-QTdj7X60F1df-Z79H5yQQmKzH69pL8Uv2pCifo22u4f-
xeDlNwAbtqJ91HHbRnzkJyb3lGg4brj6Tg=="},"fail_if_unknown":false},"id":{"com.daon.capture.iv"},"data":
{"e3hxRsGyxR_wJfM-F94Mwg=="},"fail_if_unknown":false},"id":{"com.daon.capture.schemeId"},"data":
{"CDEM1"},"fail_if_unknown":false},"id":{"com.daon.D409#8201.ados.mode"},"data":{"enrol"},
{"fail_if_unknown":false},"id":{"com.daon.D409#8201.recognition.timeout"},"data":{"7000"},
{"fail_if_unknown":false},"id":{"com.daon.D409#8401.ados.mode"},"data":{"enrol"},
{"fail_if_unknown":false},"id":{"com.daon.D409#8401.recognition.timeout"},"data":{"30000"},
{"fail_if_unknown":false},"id":{"com.daon.D409#9201.ados.mode"},"data":{"enrol"},
{"fail_if_unknown":false},"id":{"com.daon.D409#9201.recognition.timeout"},"data":{"7000"},
{"fail_if_unknown":false},"id":{"com.daon.D409#9401.ados.mode"},"data":{"enrol"},
{"fail_if_unknown":false},"id":{"com.daon.D409#9401.recognition.timeout"},"data":{"30000"},
{"fail_if_unknown":false},"id":{"com.daon.face.authentication.reason"},"data":{"Authenticate with Face
ID"},"fail_if_unknown":false},"id":{"com.daon.face.embedded.ui.enabled"},"data":{"true"},
{"fail_if_unknown":false},"id":{"com.daon.face.liveness.active.type"},"data":{"blink"},
{"fail_if_unknown":false},"id":{"com.daon.face.liveness.enroll"},"data":{"true"},
{"fail_if_unknown":false},"id":{"com.daon.face.registration.reason"},"data":{"Register with Face ID"},
{"fail_if_unknown":false},"id":{"com.daon.finger.authentication.reason"},"data":{"Authenticate with
Touch ID"},"fail_if_unknown":false},"id":{"com.daon.finger.embedded.ui.enabled"},"data":{"true"},
{"fail_if_unknown":false},"id":{"com.daon.finger.embedded.ui.reason"},"data":{"ui-reason"},
{"fail_if_unknown":false},"id":{"com.daon.finger.registration.reason"},"data":{"Register with Touch
ID"},"fail_if_unknown":false},"id":{"com.daon.finger.sdk.locking"},"data":{"true"},
{"fail_if_unknown":false},"id":{"com.daon.identityx.version"},"data":{"5.2.4.0"},
{"fail_if_unknown":false},"id":{"com.daon.sdk.ados.decChain"},"data":{"\\
\\MIIIE6TCCAt0gAwIBAgIRAJEmGK-0XEGFin4brMpnidIwCwYJKoZIhvcNAQELMEcxFTATBgNVBAMMDElkZW50aXR5WCBDQTENMAsGA1UECgw

```

```

ERGFvbjESMBAGA1UECwwJSWRlbnRpdHlYMQswCQYDVQQGEwJRTAeFw0xNzA2MTUwOTQ3NTFaFw0xOTA2MTUwOTQ3NTFaMFoxDTALBgNVBAOM
BERhb24xZjAqBgNVBAsMCUk1ZW50aXR5WDELMAkGA1UEBhMCSUUxKDAmbG9NBAMMH0RFX0RBT05fQVVUeSVOVElDQVRJT05fREFUQV9LRUswg
gEiMA0GCSqSISB3DQEBAQUAA4IBDwAwggEKAoIBAQCXhR7H7GCR4KzLwawZl3yefpUov44BWofCNnuGh3RoaG63vXX6jsrfoCVJdto5a38Nd
7ckQzjhtuoAfLeUT3sbm7uhXCCoC5xJ_B96G6LeTvY6yZ2Zs03K8d018epK0I7e2Xh_3WQg0xa21QmJxnTcMSMj0TMhrX1b66nh-
CoTbAcKopm0xbrPf0MLoZ1xGk7i0VxSY_TRjep6tn4Z7t7r-
bsJnDjJtctto4gYXk7mDkdwAMFBoq1Jp0nGbv8TCMySAj0Uss9ptE7pRl5No6iF4QYNDUUhI9q7MAcpSgEYLAPzhZdzZnmDfw0IPCiss0
qKV9L3H6wh-
NLQ_r7AgMBAAGjgcAwgb0wfgYDVR0jBHcWdYAUZpISSlDw67i7wEa-1wVzqzvdL5ahS6RJMEcxFTATBgNVBAMMDElZW50aXR5WCBDBQDENMAs
GA1UECgwERGFvbjESMBAGA1UECwwJSWRlbnRpdHlYMQswCQYDVQQGEwJRTAeFw0xNzA2MTUwOTQ3NTFaFw0xOTA2MTUwOTQ3NTFaMFoxDTALBgNVBAOM
Cs0c6TEEG2GrL08wDAYDVDR0TAQH_BAIwADA0BgNVHQ8BAf8EBAMCBLAwCwYJKoZIhvcNAQELA4ICAQA-
cpJUE0A296VXYHqIS_yRk1tsSkLvmgqwuwx2fShZJQ1pawarF8qWH9takyyBzAPNVMYsxIc4eMF4qRhExtADB5EQBFF-
DWVMOlymYOLMDH3i9InuYdsV0B82EsQu5U7ScuDH3ffN01VJq2NS8jHuFm7GxF3606BdojT3vXgHmH_dZo3GzGCRDpkKt_gUA01aj2Ga1YmL
cd2ptA60A1S1lW0eWS5yb_KNscCVVQke2gvJkACHrsIe17AxNBgukWlTANCrgH2U0hHhXl0mu3RRoxhUL8Ya5V7qSdiVZzmFMZwRpyX92FbGU
Ib_1L9n1Fs3iGtE9gXE-
DVTNs93jn_XIK0Q8D6lcvpVtI4bJQH7u78MeoSpuYx-9SX4ioiNmVVC6fdAieSG1ggEiIhw0U8l-4u1pItyPIqwt_OijaEl0ouTWzeBa3A
JA7CqasOZ0xM6BXJE5dLcILbpYduA0vSc3em6cr-LJGrR7uuvQCJ-3pGX_gipMyailXYd2S985PQXsyKEW5AegBcEgNX3MIvNPUhb2eS-
Ab_JIZbQGAUGTT_HwQXFB08pMXJ-
UK_FwdphXVGMJy9jmyvWLLBFXYGrAiq0pLlkHexCqHcjYbchgf1IDWp0yQ3KcoA42w555djBN7hFHTa9dfAdToHRK1ICG_PhsmUdhZ_T7o
Q==\\\"\\\"\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":\\\"com.daon.sdk.ados.dekId\\\",\\\"data\\\":\\\"100090661\\\",
\\\"fail_if_unknown\\\":false},{\\\"id\\\":\\\"com.daon.sdk.authenticatorMetadata\\\",\\\"data\\\":\\\"true\\\",
\\\"fail_if_unknown\\\":false},{\\\"id\\\":\\\"com.daon.sdk.deviceInfo\\\",\\\"data\\\":\\\"true\\\",\\\"fail_if_unknown\\\":false},
{\\\"id\\\":\\\"com.daon.sdk.envCheck\\\",\\\"data\\\":\\\"true\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.healthCheck\\\",\\\"data\\\":\\\"true\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.keys.access.biometry\\\",\\\"data\\\":\\\"false\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.location\\\",\\\"data\\\":\\\"true\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.response.deviceInfo\\\",\\\"data\\\":\\\"{\\\"deviceId\\\":\\\"85F60EE0-E6B9-46EB-AD5A-A714AEFF3462\\\"
\\\",\\\"make\\\":\\\"Apple\\\",\\\"osVersion\\\":\\\"15.4.1\\\",\\\"model\\\":\\\"iPhone12,1\\\",\\\"name\\\":\\\"iPhone12,1\\\",
\\\"sdkVersion\\\":\\\"4.4.0.24\\\",\\\"appId\\\":\\\"6FE23CA3-9F8D-4BE5-AE59-8B4D5B10F81E\\\",\\\"name\\\":\\\"
\\\"seaPhone\\\",\\\"notificationToken\\\":\\\"
\\\"1976b4665f3b9bce4c4342999ec2acb290da4a3896d800a32b1232892863c084\\\"}\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.response.envCheck\\\",\\\"data\\\":\\\"Passed\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.response.healthCheck\\\",\\\"data\\\":\\\"true\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.sdk.response.location\\\",\\\"data\\\":\\\"44.667134,-63.567784,1651058684217.362793\\\",
\\\"fail_if_unknown\\\":false},{\\\"id\\\":\\\"com.daon.sdk.version\\\",\\\"data\\\":\\\"4.4.0.24\\\",\\\"fail_if_unknown\\\":false},
{\\\"id\\\":\\\"com.daon.status.D409#2204.NDRBQjLGQzQtNUYyNC00QTA0LTk0NjMtMURFNEI5MTBEQ0Y1.reenrolCounter\\\",
\\\"data\\\":\\\"0\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.status.D409#2204.NDRBQjLGQzQtNUYyNC00QTA0LTk0NjMtMURFNEI5MTBEQ0Y1.state\\\",\\\"data\\\":\\\"AVAIL\\\",
\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.status.D409#2204.NDRBQjLGQzQtNUYyNC00QTA0LTk0NjMtMURFNEI5MTBEQ0Y1.unlockCounter\\\",\\\"data\\\":\\\"0\\\",
\\\"fail_if_unknown\\\":false},{\\\"id\\\":\\\"fido.uaf.safetynet\\\",\\\"data\\\":\\\"null\\\",\\\"fail_if_unknown\\\":false},
{\\\"id\\\":\\\"com.daon.authRequest.retriesRemaining\\\",\\\"data\\\":\\\"5\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.authRequest.maxAttempts\\\",\\\"data\\\":\\\"5\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.user.retriesRemaining\\\",\\\"data\\\":\\\"10\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.user.maxAttempts\\\",\\\"data\\\":\\\"10\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.face.retriesRemaining\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.face.maxAttempts\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.voice.retriesRemaining\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.voice.maxAttempts\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.passcode.retriesRemaining\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.passcode.maxAttempts\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.otp.retriesRemaining\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.otp.maxAttempts\\\",\\\"data\\\":\\\"3\\\",\\\"fail_if_unknown\\\":false}}},\\\"fcParams\\\":
\\\"eyJhcHBjRCI6Imh0bDZ0lwvXC9leGFtcGx1LmNvbSIsImNoYXN0ZW5kaW5nIjpw7fSwiZmFjZXJRJC6Im1vczpidW5kbGUtaWQ6Y29
tLmRhbm24uZm1kby5zYW1wbGUucnAucHvZaCI5ImNoYXN0ZW5nZSI6IktjZDJ4UWUxZDZ0d1B3Uldkcm9oY3cifQ==\\\",\\\"assertions\\\":
[{\\\"assertionScheme\\\":\\\"UAFV1TLV\\\",\\\"assertion\\\":
\\\"Aj4pAAQ-4QALLgkARDQwOSMyMjA0Di4FAAQAAGADy4IAEy_Boox0eJBCi4gAJk_6zJweHGVDWIahD5EZYDetzyd82MedHvDFqFEtIE3EC4
gADK9b07JZ-
V1snweyNF3csizuEQayV3mdpcqwW8L_2kkCS4kADQ0QUI5RkM0LTVGMjQtNEEwNC05NDYzLTFERTCOTewRENGNQ0uBAAAAAAAEj5DABMuGwB
jb20uZGFvbi5zZGsuZXh0ZW5zaW9uc0hhc2gULiAARz18jrN1ZwiM9oxH7ziEhMPRzNh8NtLepJ4-
MThdWAEGLkAAEG3BBXGgWcPtanbkZ641WHOMfHFLC7hFJxvqrmc-0-bhVraMqgynDSX-Rt85E1v2_qIxY0ze4AL-QX9kYvbw==\\\",
\\\"exts\\\":[{\\\"id\\\":\\\"com.daon.dataStoreType\\\",\\\"data\\\":\\\"OS\\\",\\\"fail_if_unknown\\\":false},{\\\"id\\\":
\\\"com.daon.embedded.ui.reason\\\",\\\"data\\\":\\\"Verify your face to continue authentication.\\\",

```



```

{"fail_if_unknown":false}, {"id":"com.daon.info.time","data":{"3000"},"fail_if_unknown":false},
{"id":"com.daon.keyStoreType","data":{"HardwareOS"},"fail_if_unknown":false}, {"id":
"com.daon.token","data":{"1651058688715"},"fail_if_unknown":false}}]]],
  "fidoResponseCode" : 1200,
  "fidoResponseMsg" : "Successfully Validated Authentication",
  "status" : "COMPLETED_SUCCESSFUL",
  "deviceStatus" : "{ \"version\":\"1.0\", \"authenticatorInfo\":{\"D409#2204\":{\"registrationInfo\":
{ \"deviceInfo\":{\"appId\":\"6FE23CA3-9F8D-4BE5-AE59-8B4D5B10F81E\", \"deviceId\":\"85F60EE0-E6B9-46EB-AD5A-
A714AEFF3462\", \"make\":\"Apple\", \"model\":\"iPhone 12 Mini\", \"osVersion\":\"15.4.1\", \"sdkVersion\":
\"4.4.0.24\", \"name\":\"seaPhone\", \"notificationToken\":
\"1976b4665f3b9bce4c4342999ec2acb290da4a3896d800a32b1232892863c084\", \"location\":{\"longitude\":
\"-63.567784\", \"latitude\":\"44.667134\", \"captured\":\"2022-04-27T11:24:44.217+00:00\"},
\"healthCheckPassed\":true, \"environmentCheckResult\":\"Passed\"}, \"attestation\":{\"form\":
\"SURROGATE_BASIC\"}}, \"authenticationInfo\":{\"deviceInfo\":{\"appId\":\"6FE23CA3-9F8D-4BE5-
AE59-8B4D5B10F81E\", \"deviceId\":\"85F60EE0-E6B9-46EB-AD5A-A714AEFF3462\", \"make\":\"Apple\", \"model\":
\"iPhone 12 Mini\", \"osVersion\":\"15.4.1\", \"sdkVersion\":\"4.4.0.24\", \"name\":\"seaPhone\",
\"notificationToken\":\"1976b4665f3b9bce4c4342999ec2acb290da4a3896d800a32b1232892863c084\", \"location\":
{ \"longitude\":\"-63.567784\", \"latitude\":\"44.667134\", \"captured\":\"2022-04-27T11:24:44.217+00:00\"},
\"healthCheckPassed\":true, \"environmentCheckResult\":\"Passed\"}, \"attestation\":{\"form\":
\"SURROGATE_BASIC\"}}}}}",
  "authenticationAttempts" :
  [
    { "attemptId" : "1006700020:1006701019",
      "created" : "2022-04-27T11:24:51.446+0000",
      "decision" : "Y",
      "state" : "COMPLETED_SUCCESSFUL",
      "attributes" :
      { },
      "items" :
      [
        { "created" : "2022-04-27T11:24:51.446+0000",
          "authenticator" :
          { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/authenticators/
QTAzbtS4D4IA2RfWR1tpJiWfdg",
            "id" : "QTAzbtS4D4IA2RfWR1tpJiWfdg" },
          "type" : "Face",
          "result" : "MATCH",
          "authenticatorCounter" : 2,
          "aaid" : "D409#2204" } ] } ],
    "registration" :
    { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/registrations/
QTAzSjr1BHUwctCsDXZtGvVJ1Q" },
    "policy" :
    { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/policies/
QTAzCPHRfwbCBXcI1Rm9-FiDR1g" },
    "application" :
    { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/applications/
QTAzdui396GxUj_w7N2Khr1edg" },
    "user" :
    { "href" : "https://api.identityx-cloud.com/pingdavinci/IdentityXServices/rest/v1/users/
QTAzs3wrZYvmxdu0LQ13r8z75w" },
    "tenant" :
    { "href" : "https://api.identityx-cloud.com/IdentityXServices/rest/v1/tenants/r4SWIoHpn0fmXw4pkQhAbw" } }

```

Webhook Handler

Listen for an authentication response webhook

Output Schema

- output object
 - restId string
 - transactionIdentifier string
 - transactionStatus string

Device Policy Connector

The Device Policy connector lets you check the user agent, browser information, and operating system version in your PingOne DaVinci flow.

You can use the Device Policy connector to:

- Enable mobile device management.
 - Selected devices, browsers, and operating systems included in the allow list grants access to users.
 - Selected devices, browsers, and operating systems included in the deny list will prevent access to users.
- Implement risk intelligence by creating a device policy.

Note

This connector relies on information provided by the device's user agent. Because the implementation of user agent varies, the information might

Setup

Resources

For more information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Device Policy connector

In DaVinci, add a Device Policy connector. For help, see [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Allow requests from specified devices

The connector has several capabilities to select allowed devices:

- **Allow selected OS**
- **Allow selected user agent**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Deny requests from specified devices

The connector has several capabilities to select denied devices:

- **Deny selected OS**
- **Deny selected user agent**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Get information about a device

The connector has several capabilities to get information about a user's device:

- **Get operating system**
- **Get browser**
- **Get platform**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Trusted Device OS

Properties

deviceOSName dropDownMultiSelect

Input Schema

- default object
 - userAgent string required
 - properties object
 - deviceOSName array required

Output Schema

- output object
 - deviceOSName string

Output Example

```
{ "deviceOSName" : "MacOS" }
```

Blacklisted Device OS

Properties

deviceOSName dropDownMultiSelect

Input Schema

- default object
 - userAgent string required
 - properties object
 - deviceOSName array required

Output Schema

- output object
 - deviceOSName string

Output Example

```
{ "deviceOSName" : "MacOS" }
```

Trusted User Agent

Properties

browserNames dropDownMultiSelect

Input Schema

- default object
 - userAgent string required
 - properties object
 - browserNames array required

Output Schema

- output object
 - browserName string

Output Example

```
{ "browserName" : "chrome" }
```

Blacklisted User Agent

Properties

browserNames dropDownMultiSelect

Input Schema

- default object
 - userAgent string required
 - properties object
 - browserNames array required

Output Schema

- output object
 - browserName string

Output Example

```
{ "browserName" : "chrome" }
```

Get Device OS

Return the Device OS name

Input Schema

- default object
 - userAgent string required

Output Schema

- output object
 - deviceOSName string

Output Example

```
{ "deviceOSName" : "MacOS" }
```

Get Browser

Returns the Name of the Browser that is used.

Input Schema

- default object
 - userAgent string required

Output Schema

- output object
 - browserName string

Output Example

```
{ "browserName" : "Chrome" }
```

Get Platform

Returns whether the flow is running in mobile or desktop.

Input Schema

- default object
 - userAgent string required

Output Schema

- output object
 - platform string

Output Example

```
{ "platform" : "mobile" }
```

Duo Connector

The Duo connector lets you use Duo for multi-factor authentication (MFA) in your PingOne DaVinci flow.

Setup

Resources

For information and setup help, see the following documentation:

- Duo documentation
 - [Getting Started with Duo Security](#)
 - [Protect an Application](#)
 - [Policy & Control](#)
 - [What is the Duo Universal Prompt?](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A configured Duo environment
- A Duo user account to use for testing

Getting your application credentials

1. In Duo, add an application. For help, see [Protecting an application](#) in the Duo documentation.
2. Select **PingFederate** as the application type.
3. Note your **Client ID**, **Client secret**, and **API hostname**. You'll use these in the connector configuration.
4. Click **Save**.

Setting up the Duo connector configuration

In DaVinci, add a **Duo** connection. For help, see [Adding a connector](#).

Connector configuration

Client ID

The **Client ID** that you noted in **Getting your application credentials**.

Client secret

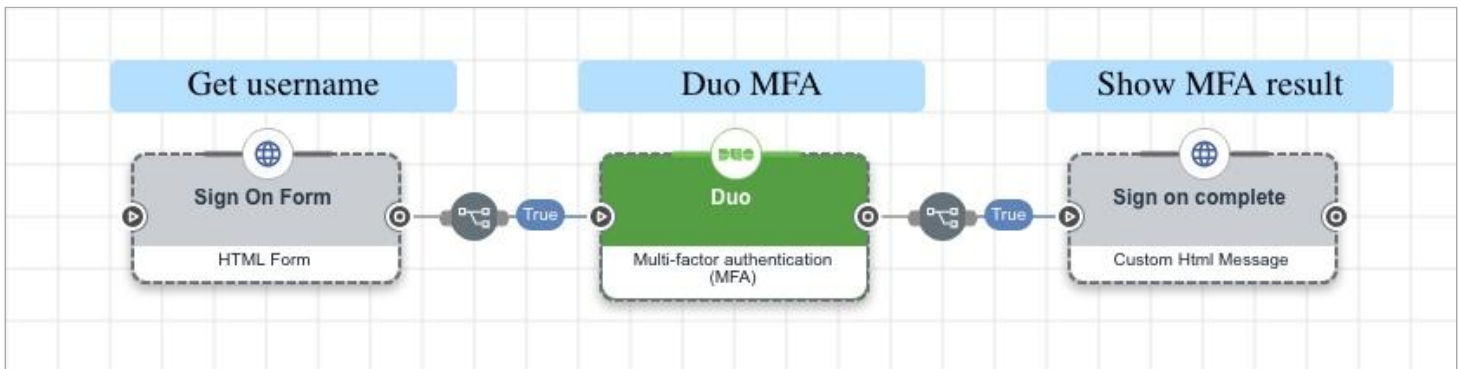
The **Client secret** that you noted in **Getting your application credentials**.

API Hostname

The **API hostname** that you noted in **Getting your application credentials**.

Using the connector in a flow

Authenticating users with Duo multi-factor authentication



Complete the steps below to create a flow that asks the user to enter their username in an HTML form, uses the connector to redirect them to Duo, then shows the results on an HTML page.

Note

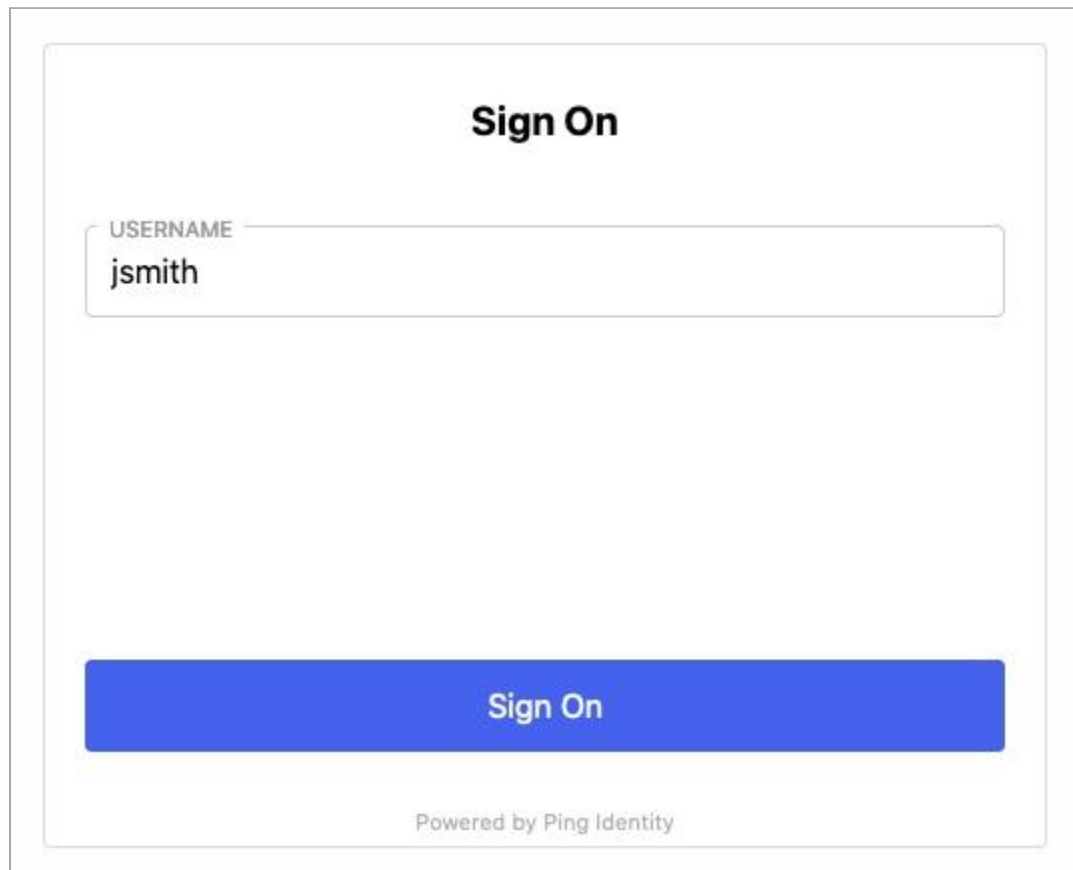
Duo's Universal Prompt experience doesn't provide a "Cancel" option that would let the user exit MFA and return to the DaVinci flow. Because of this, it's possible for Duo to become a dead end in the user experience if they can't successfully complete MFA.

1. Create a sign on form:

1. In a new flow, add the **HTTP** connector and select the **HTML Form** capability. Select the node that appears in your flow.

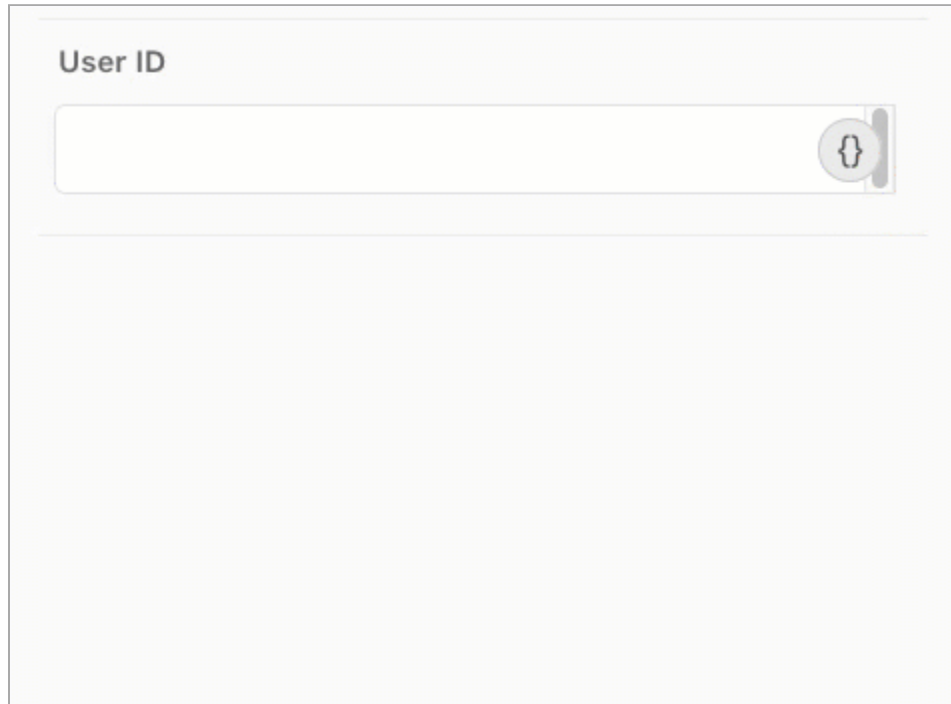
Note

In this example flow, we'll collect the username in a form. When you build your own flow, this is where you should add your first-factor authentication step.

 **Tip**

For help, see the [HTTP](#) connector.

2. In the **Title** field, enter a title, such as **Sign On**.
 3. In the **Fields List** section, click **Add**.
 4. In the **Property Name** field, enter **username**.
 5. In the **Display Name** field, enter **Username**.
 6. In the **Next Button Text** field, enter **Sign On**.
 7. Click **Apply**.
2. Redirect the user to Duo for MFA:
1. Following your **HTML Form** node in your flow, add the **Duo** connector and select the **Multi-factor authentication (MFA)** capability. Select the node that appears in your flow.
 2. In the **User ID** field, click **{}** and select the **username** variable from your **HTML Form** node.

A screenshot of a user interface element. It features a light gray rectangular container. Inside, at the top, is the text 'User ID' in a bold, dark gray font. Below this text is a white rectangular input field with a thin gray border. To the right of the input field is a circular icon containing a curly brace '{'.

3. (Optional) If you want the flow to show a Duo sign-on button rather than automatically redirecting the user to Duo, do the following:

Note

This lets you include a Duo sign-on button alongside other sign-on options in an **IDP Container** connector or as part of a custom HTML page using an [HTTP](#) connector.

1. Turn off **Skip Button Press**.
2. In the **Display Name** field, enter the button text, such as `Sign on with Duo`.
3. (Optional) In the **CSS** field, add CSS to customize the appearance of the prompt.
4. (Optional) Turn on **Show Powered By** to display **Powered by Ping Identity** at the bottom of the prompt page.

4. Click **Apply**.

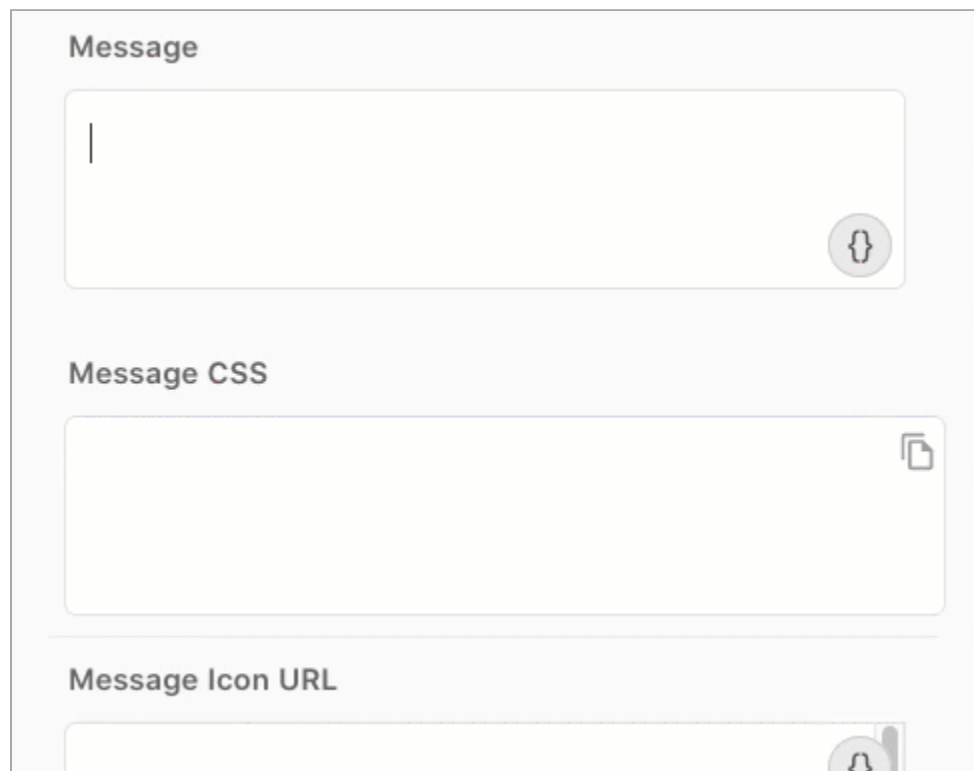
3. Show the response from Duo:

1. Following your **Multi-factor authentication (MFA)** node, add an **HTTP** connector and select the **Custom HTML Message** capability. Select the node that appears in your flow.

Note

In this example flow, we'll show the user the response from Duo. When you build your own flow, this is where you should redirect the user to the resource they originally wanted to access.

2. In the **Title** field, enter `Sign on complete`.
3. In the **Message** field, click `{}` and select the **rawResponse** variable from your **Multi-factor authentication (MFA)** node.



Message

Message CSS

Message Icon URL

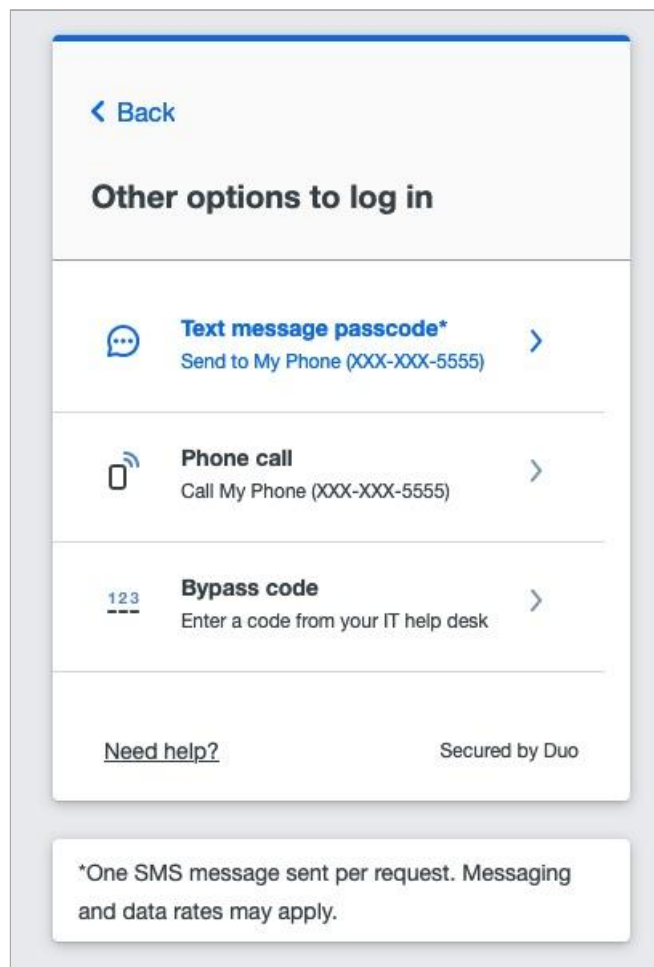
4. Click **Apply**.

4. Test the flow.

1. Click **Save, Deploy**, then **Run**.

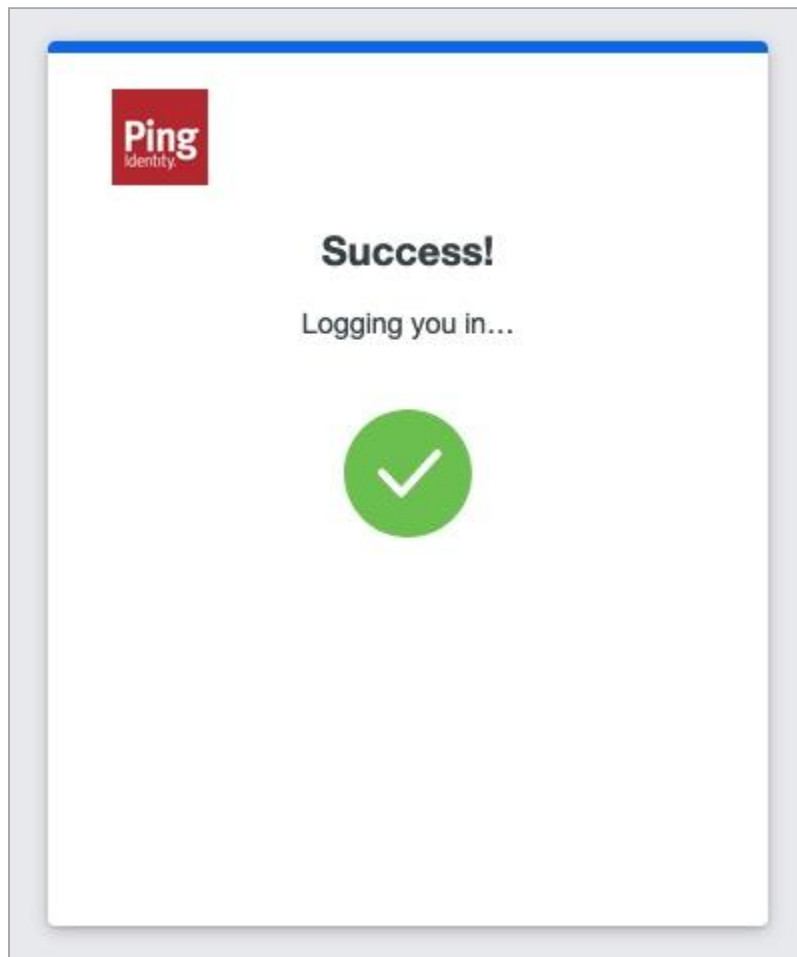
2. On the **Sign On** page, enter the username for your Duo test user account. Click **Sign On**.

Result: The browser redirects to the Duo MFA experience, such as Universal Prompt.



3. Complete the MFA process with Duo.

Duo shows a success message, then redirects the browser back to DaVinci.



Your **Custom HTML Message** shows the complete response from Duo.



For help, see the [Creating an authentication flow](#) guide.

Capabilities

Multi-factor authentication (MFA)

Redirect to Duo for multi-factor authentication.

Properties

Username textField required
Display Name button
showPoweredBy toggleSwitch
skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - username string required
Username
 - clientSecret string required
 - clientId string required
 - apiHostname string required
API Hostname

Output Schema

- output object
 - rawResponse object
 - access_token string
 - id_token string
 - expires_in integer
 - token_type string
 - statusCode integer
 - headers object
 - server string
 - date string
 - content-type string
 - content-length string
 - connection string
 - cache-control string
 - pragma string
 - strict-transport-security string
 - content-security-policy string
 - tokens object
 - access_token string
 - id_token string
 - expires_in integer
 - token_type string
 - iss string
 - sub string
 - aud string
 - exp integer
 - iat integer
 - auth_time integer

- auth_result object
 - result string
 - status string
 - status_msg string
- auth_context object
 - txid string
 - timestamp integer
 - user object
 - name string
 - key string
 - groups array
 - application object
 - name string
 - key string
 - auth_device object
 - ip string
 - location object
 - city string
 - state string
 - country string
 - name string
 - access_device object
 - ip string
 - location object
 - city string
 - state string
 - country string
 - hostname null
 - epkey string
 - factor string

- event_type string
- result string
- reason string
- alias string
- isotime string
- email string
- ood_software null
- preferred_username string
- nonce string

Entrust Connector

The Entrust connector lets you use Entrust adaptive authentication in your PingOne DaVinci flow.

You can use the Entrust connector to:

- Profile a user's device and perform multi-factor authentication (MFA) using:
 - A one-time passcode (OTP) through SMS or email
 - A time-based one-time passcode (TOTP) through a hardware or software token

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need an Entrust license.

Adding an application in Entrust

The connector needs an application ID to communicate with Entrust.

To get the application ID, complete the steps in "Integrate Authentication API with Identity as a Service" in the Entrust administrator documentation.

For a direct link to the documentation, modify the following URL: https://<your Entrust domain>/documentation/help/admin/index.htm#t=Resources%2FAdd_Authentication_API.htm

1. For **Source of Client IP Address for Risk Conditions**, select **From the incoming HTTP connection**.
2. Copy the **Application ID**. You'll use it when you set up the connector configuration.
3. Configure a resource rule as described in the Entrust documentation.

Configuring the Entrust connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Service Domain

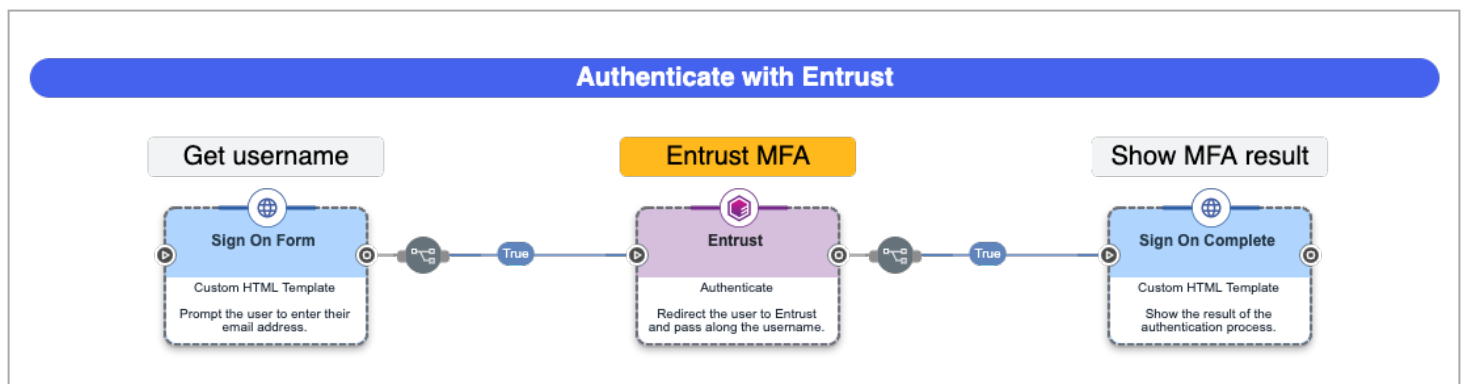
Your Entrust domain. For example, "company.us.trustedauth.com".

Application ID

The ID of your Entrust application.

Using the connector in a flow

Authentication



This flow asks a user to authenticate with Entrust. It asks the user to enter their user ID in an HTML form, prompts them to select and complete a Entrust authentication method, then shows the results on an HTML page.

1. Download the [Entrust Authentication](#) flow template. For help, see [Using DaVinci flow templates](#).

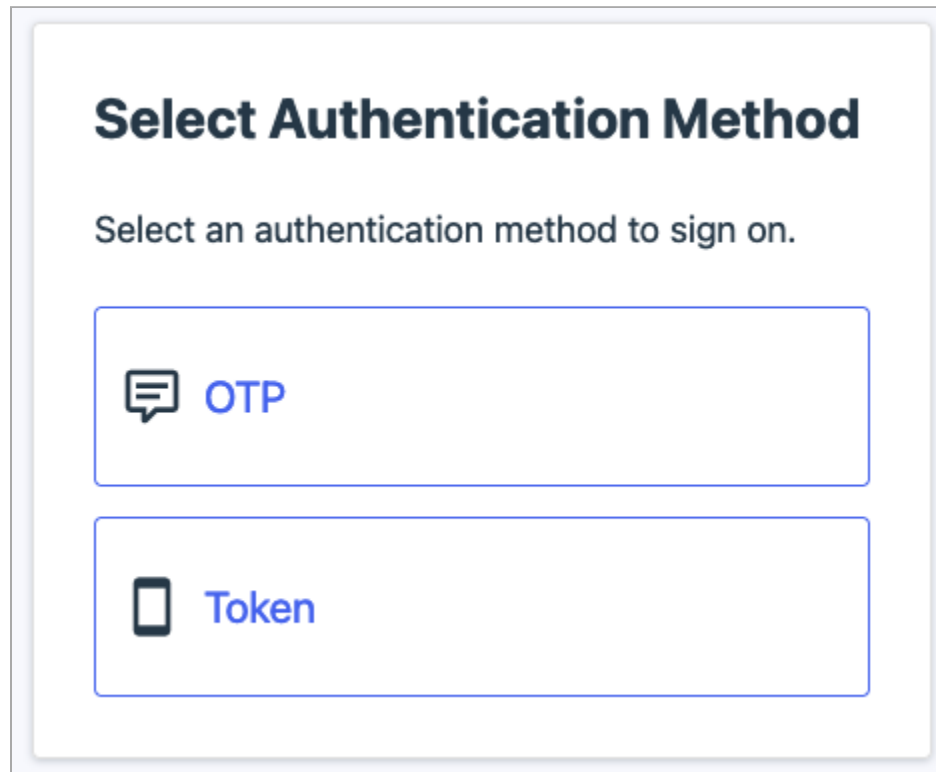
2. (Optional) Add transaction details:

1. On the flow canvas, select the **Authenticate (Entrust)** node.
2. On the **General** tab, in the **Transaction Details** section, add attributes as key-value pairs. These are sent to Entrust as part of the authentication process.

 Tip

You can dynamically populate values by clicking `{}` and selecting a variable from elsewhere in your flow.

3. (Optional) Customize the default **Authenticator Selection** interface.

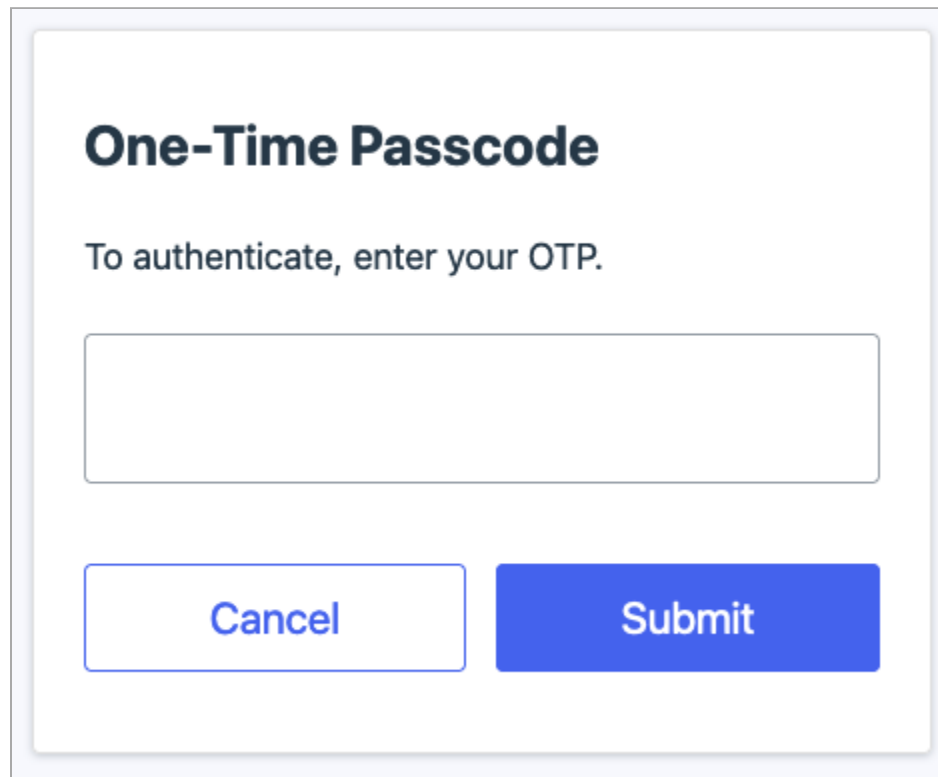


1. On the flow canvas, select the **Authenticate (Entrust)** node.
2. On the **Custom** tab, in the **Select Authenticator** section, modify the **HTML Template**, **CSS**, and **Script** fields.

 Tip

- Click **Switch View** to see the HTML formatted with syntax highlighting.
- Click the **Maximize**  icon to give yourself more room to work.
- To access a variety of useful tools, right-click the field when you're in syntax highlighting mode (dark background).

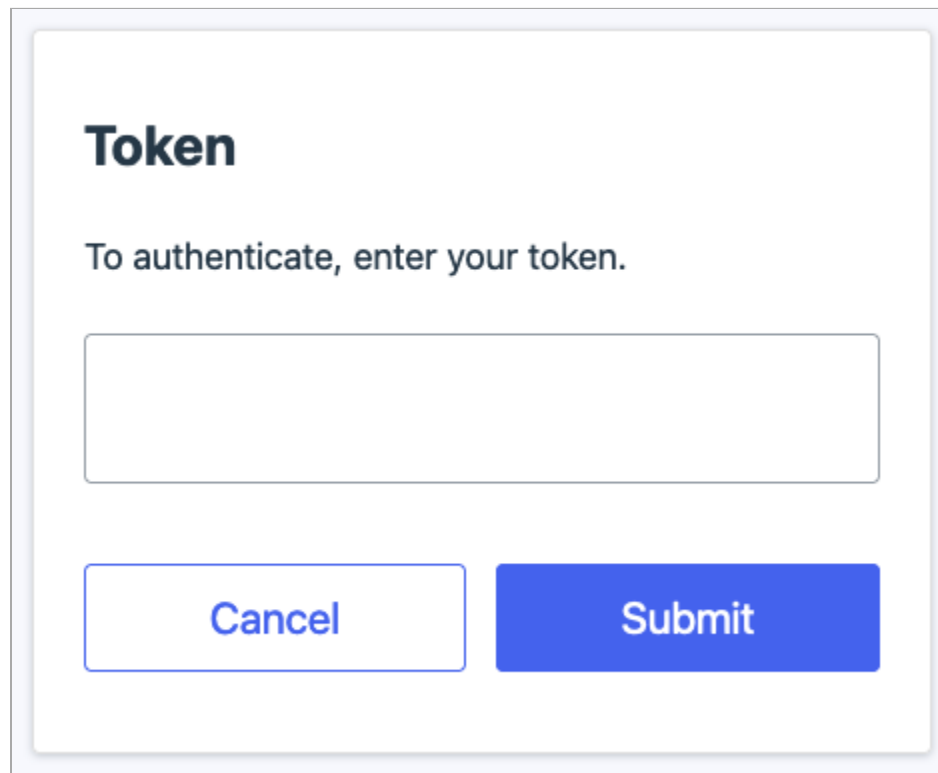
4. (Optional) Modify the default **OTP Input** interface on the **Custom** tab.



One-Time Passcode

To authenticate, enter your OTP.

5. (Optional) Modify the default **Token Input** interface on the **Custom** tab.



Token

To authenticate, enter your token.

6. Test the flow.

1. Click **Save**, **Deploy**, then **Try Flow**.

2. On the **Sign On** page, enter your Entrust user ID, such as `jsmith@example.com`.
3. Select your authentication method and complete the authentication process.
4. See the result of the authentication process.

Capabilities

Authenticate

Authenticate users with Entrust.

Properties

User ID textField required

The unique ID of the user you want to authenticate.

Transaction Details keyValuePairList

Additional transaction details to send to Entrust.

Input Schema

- default object
 - properties object
 - serviceDomain string required
 - applicationId string required
 - userId string required

Output Schema

- output object
 - statusCode integer
 - rawResponse object

Error Message Connector

The Error Message connector lets you create and customize the error messages that appear in your PingOne DaVinci flow.

You can use the Error Message connector to customize an error message shown in the user interface.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Error Message connector

In DaVinci, add an Error Message connector. For more information, see [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Custom error message creation

You can use the **Custom error message on screen** capability to create a custom error message and set when that error appears on screen.

To use the connector in the flow, you must add the `skerror` component to an HTTP connector node in your flow.

Note

You can add the component to the **Custom HTML Template** of the HTTP connector in your flow, formatted as `<div data-skcomponent="skerror"></div>`. For more information, see [SK-Components reference](#).

Capabilities

Custom Error Message On Screen

Customize Error message shown on UI/Screen

Properties

errorMessage textField

Custom Error Message

errorDescription textField

Custom Error Description

Error Code dropDown

Custom Error Code

- 400
- 403
- 404
- 405
- 429
- 500

errorReason textField

Custom Error Reason

errorCallbackSuppress toggleSwitch

Input Schema

- default object

FingerprintJS Connector

The FingerprintJS connector lets you create a unique visitor ID based on browser attributes for use in fraud and analytics in your PingOne DaVinci flow.

This connector enables browser fingerprinting to stop fraud, spam, and account takeovers.

You can use the FingerprintJS connector to:

- Provide a single sign-on (SSO)-like experience across multiple nodes in a flow.

- Implement risk intelligence through browser fingerprinting.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A configured FingerprintJS environment
- Your FingerprintJS API keys

Configuring the FingerprintJS connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Fingerprint Subscription Browser Token

A public API key from FingerprintJS. This key can be found in your FingerprintJS environment under **App Settings > API Keys**.

Fingerprint Subscription API Token

TA secret API key from FingerprintJS. This key can be found in your FingerprintJS environment under **App Settings > API Keys**.

JavaScript CDN URL

A CDN URL for the FingerprintJS element.

Using the connector in a flow

Visitor ID creation

You can use the **Get a visitor's ID** capability to create a unique ID for a user. No special flow configuration is needed. Add the capability and populate its properties according to the help text.

Information through visitor's ID

You can use the **Get visitor's info based on ID** capability to get visitor information, such as their ID, IP address, browser, and whether incognito mode is being used. No special flow configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Get Visitor's ID

Input Schema

- default object
 - properties object
 - token string required minLength: 0 maxLength: 100
Fingerprint JS Subscriber Token
 - javascriptCdnUrl string required
Fingerprint JS javascript URL

Input Example

```
{ "properties" :  
  { } }
```

Output Schema

- output object
 - requestId string required
 - visitorId string required
 - visitorFound boolean required
 - meta null required

Output Example

```
{ "requestId" : "1619596982579.qsyv0p",  
  "visitorId" : "oUT1HXUBaQZ9RwdF5xCX",  
  "visitorFound" : true,  
  "meta" : null }
```

Get Visitor's Info based on ID

Get Visitor information such as ID, incognito mode, IP, browser, etc.

Properties

Visitor ID textField required

Input Schema

- default object
 - properties object
 - apiToken string required minLength: 0 maxLength: 100
Fingerprint JS Subscriber API Token
 - visitorId string required minLength: 0 maxLength: 100
Fingerprint JS visitor id

Input Example

```
{ "properties" :  
  { "visitorId" : "visitor-id" } }
```

Output Schema

- output object
 - visitorId string required
 - visits array required
 - Array Item Schema object
 - requestId string required
 - incognito boolean required
 - linkedId string required
 - time string required
 - timestamp integer required
 - url string required
 - ip string required
 - ipLocation object required
 - accuracyRadius integer required
 - latitude number required
 - longitude number required
 - postalCode string required
 - timezone string required
 - city object required
 - name string required
 - continent object required
 - code string required
 - name string required
 - country object required
 - code string required
 - name string required
 - subdivisions array required
 - Array Item Schema object
 - isoCode string required
 - name string required

- browserDetails object required
 - browserName string required
 - browserMajorVersion string required
 - browserFullVersion string required
 - os string required
 - osVersion string required
 - device string required
 - userAgent string required

- lastTimestamp integer required

Output Example

```
{ "visitorId" : "Ibk1527CUFmcnjLwIs4A9",
  "visits" :
  [
    { "requestId" : "0KSh65EnVoB85JBmloQK",
      "incognito" : true,
      "linkedId" : "somelinkedId",
      "time" : "2019-05-21T16:40:13Z",
      "timestamp" : 1.582299576512E12,
      "url" : "https://www.example.com/login",
      "ip" : "61.127.217.15",
      "ipLocation" :
      { "accuracyRadius" : 10,
        "latitude" : 49.982,
        "longitude" : 36.2566,
        "postalCode" : "61202",
        "timezone" : "Europe/Dusseldorf",
        "city" :
        { "name" : "Dusseldorf" },
        "continent" :
        { "code" : "EU",
          "name" : "Europe" },
        "country" :
        { "code" : "DE",
          "name" : "Germany" },
        "subdivisions" :
        [
          { "isoCode" : "63",
            "name" : "North Rhine-Westphalia" } ] },
      "browserDetails" :
      { "browserName" : "Chrome",
        "browserMajorVersion" : "74",
        "browserFullVersion" : "74.0.3729",
        "os" : "Windows",
        "osVersion" : "7",
        "device" : "Other",
        "userAgent" : "Mozilla/5.0 (Windows NT 6.1; Win64; x64) ...." } } ],
    "lastTimestamp" : 1.582299576512E12 }
```

Flow Analytics Connector

The Flow Analytics connector lets you log details about flow outcomes that you can review in flow analytics.

You can use the Flow Analytics connector to:

- Track analytics based on different flow outcomes.
- Create a policy for running flows if logging errors occur.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the FingerprintJS connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Capture flow information

You can use the **Log flow outcomes** capability to log details about flow outcomes based on outcome type and outcome status.



Important

The **Outcome Status Detail** field is limited to 250 characters and the **Outcome Description/Comment** field is limited to 1000 characters. While these limits can be exceeded, the system will automatically trim the data during flow execution.

No special flow configuration is needed. Add the capability and populate its properties according to the help text.



Tip

To view flow analytics from the flow canvas, go to **More Options (⋮) > Analytics**.

Capabilities

Log Flow Outcomes

Log custom flow outcomes.

Properties

outcomeType dropdownWithCreate required
outcomeStatus dropdownWithCreate required
outcomeStatusDetail dropdownWithCreate
outcomeDescription textArea
customTimestamp textField
shouldContinueOnError toggleSwitch

Input Schema

- default object
 - properties object
 - outcomeType string required minLength: 2 maxLength: 75
Type of outcome from flow (e.g. login, enrollment, etc.)
 - outcomeStatus string required minLength: 2 maxLength: 75
Status of the outcome from the flow (e.g. success, error, denied, fraud, approved, etc.)
 - outcomeStatusDetail string minLength: 2 maxLength: 250
Details about status of the outcome
 - outcomeDescription string minLength: 2 maxLength: 1000
Description of the outcome
 - customTimestamp string minLength: 2 maxLength: 75
Custom timestamp to be logged along with the outcome
 - shouldContinueOnError boolean
true if flow should continue if an error is encountered in logging

Input Example

```
{ "properties" :  
  { "outcomeType" : "login",  
    "outcomeStatus" : "success" } }
```

Output Schema

Flow Analytics Connector Release Notes

New features and improvements in the Flow Analytics connector. Updated October 18, 2024.

October 2024

Expanded Data Sent to Webhooks

Fixed

The Flow Analytics Connector now sends the contents of the **Outcome Status Detail** and **Outcome Description/Comment** fields to webhooks, providing external logging systems with more thorough information about flow errors. You can also populate these fields with variables or data from preview nodes using the `{ }` icon.

Flow Conductor Connector

The Flow Conductor connector lets your PingOne DaVinci flow initiate asynchronous events in external systems. It also allows you to use another flow as a subflow.

Interacting with external systems

Some authentication workflows require the user to do something in another system, such as clicking a magic link in their email or verifying a document in a mobile app. The Flow Conductor connector simplifies these cases by allowing you to generate the magic link and create a challenge variable that's resolved when the link is clicked. Learn more about challenges in the [Challenge connector documentation](#).

The Flow Conductor also allows you to create a secondary path in your flow that's triggered when the magic link is clicked:

1. In your main flow, a Flow Conductor **Out-of-Band Start (Links Only)** node generates a magic link or QR code. You can send this link to the user by email, SMS, or another method of your choice. This node also creates the challenge, which gives an [HTTP](#) connector the ability to pause the flow until the status of the challenge changes.
2. When the user clicks the magic link, an **Out-of-Band Continue** node starts a secondary flow. You can use this flow to show a confirmation message, and to trigger the main flow to continue by updating the status of the challenge.

The Start and Continue nodes work as a pair, and they are always attached to the same parent node. DaVinci automatically follows the Start node first and activates the Continue node when the user clicks the magic link that contains the matching challenge ID.

Links to subflows

By linking to subflows, you can simplify visually complex flows by breaking them into smaller components. You can also link to a subflow from as many main flows as you want, so this is a powerful way to centralize your maintenance work.

Subflows are best used for frequently-used groups of nodes that serve a specific purpose. For example, you might create a subflow for registering a multi-factor authentication (MFA) device or letting a user reset their password. Then you could include these in several of your main flows, such as your registration, authentication, and user self-service portal experiences.

Setup

Setting up the Flow Conductor connector configuration

In DaVinci, add a **Flow Conductor** connection. For help, see [Adding a connector](#).

Connector configuration

Input Schema

When you call on this subflow, it will receive information from your main flow. The input schema defines the structure of that information. For help, see [JSON-Schema.org](#).

Public Key

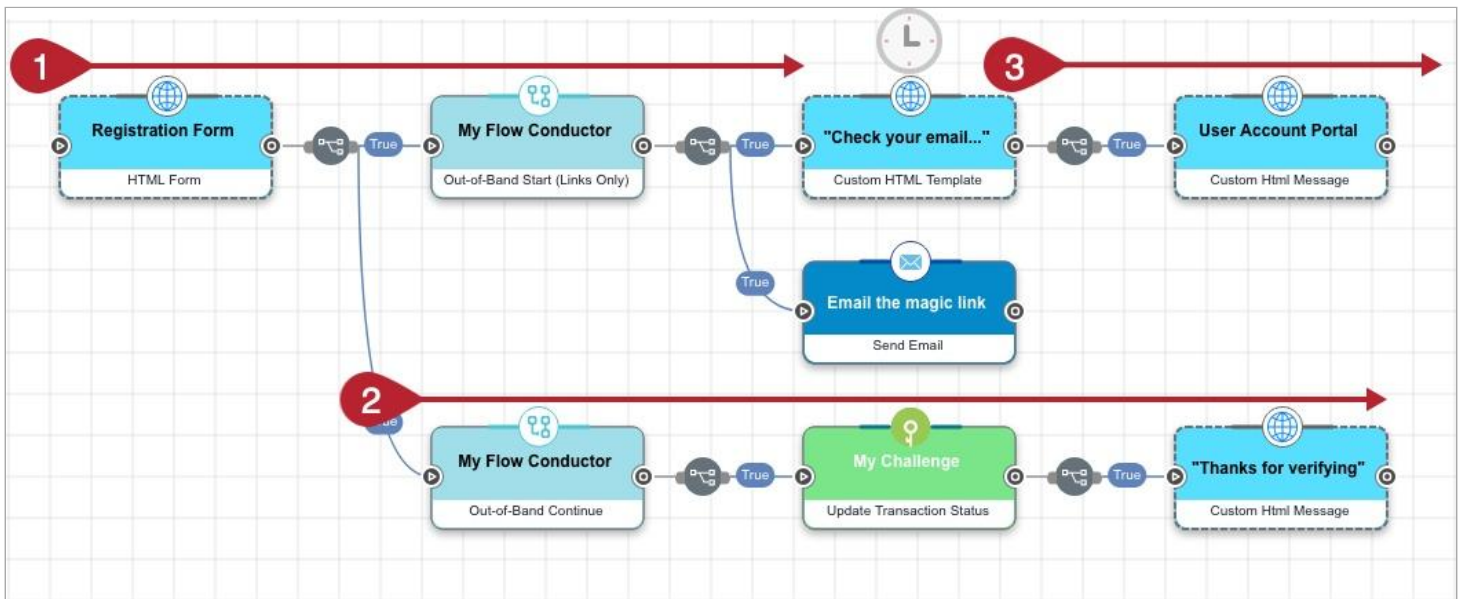
To make sure the flow is only called by an authorized source, enter your public encryption key here.

Enforce Signed Token

Turn this on to require that the token is signed.

Using the connector in a flow

Emailing a magic link to a user, then continuing the flow



When a guest registers a new user account, you can verify that they own the email address that they entered. We want to pause our main flow until the user clicks the link in their email inbox. We also want to show them a confirmation message in a new browser tab when they click the link. After they click the magic link, our secondary flow will trigger our main flow to bring the user to the User Account Portal.

For this flow, you'll need:

- A registration form in your flow, made using the [HTTP](#) connector.
- A way to send an email to the user, such as the SMTP connector.
- A [Challenge](#) connector available in your environment.

1. Generate the magic link and the challenge:

1. In your flow, following the registration form, add the **Flow Conductor** connector, and select the **Out-of-Band Start (Links only)** capability. Select the node that appears in your flow.
2. In our case, we want to send a text link rather than a QR code, so we'll leave **Generate QR Code** turned off.
3. In the **Challenge Length** field, you can customize the length of the challenge ID. This is a number that DaVinci generates to keep track of this challenge. We'll refer to this ID elsewhere in our flow, but we don't need to know the number. Leave it as the default of 32.
4. In the **Challenge Expiry** field, specify how long you want the flow to wait before timing out.
5. It won't take the user long to click a magic link, but if your flow has the user taking photos of their drivers license for identity verification, you should give them more time.
6. We're sending a normal link to the user, so we'll leave **Use Custom Link** turned off.

7. You can turn this on in your own flow if you need to customize the URL to point to a mobile app. To customize the URL, point to your equivalent of `com.myApp://skSKD?challenge=`.

2. Send the magic link to the user:

1. Following your **Out-of-Band Start** node, add an **SMTP** connector and select the **Send Email** capability. Select the node that appears in your flow.
2. In the **To Email Address** field, select the email address variable from your registration form.
3. In the **HTML Message** field, include a hyperlink. For the **href** part of the link, click `{}` and select the `continueLink` variable from your Flow Conductor node.

The screenshot shows the configuration for an SMTP connector. The 'HTML Message' field is populated with the following text: 'Welcome, {username}! Click here to verify your account.' The 'href' attribute is highlighted with red dots, and a variable selection icon (a circle with curly braces) is visible to its right. Below this, there is a 'Send Test Email?' section with a toggle switch that is currently turned off.

This inserts the magic link with the unique challenge ID associated with our flow.

3. Show a page with a “waiting” animation until the user clicks the link:

1. Parallel to your SMTP node, add an **HTTP** connector and select the **Custom HTML Template** capability. Select the node that appears in your flow.
2. Build your message in the **HTML Template** field. To show a “waiting” animation on the page, click `{}` and select the `skpolling` variable from **SK-Component**.
3. In the **Challenge** field, click `{}` and select the `challenge` variable from your Flow Conductor node.

The screenshot shows a configuration window for an HTML Template. At the top, there's a title 'HTML Template' and a 'Switch View' toggle which is currently turned off. Below the title is a large text area containing the following HTML code:

```
<div>
  <p>Go to your email and click the verification
  link.</p>
  <p>|</p>
</div>
```

To the right of the text area is a circular icon containing a curly brace. Below the text area, there's a section titled 'Use Recaptcha Verification' with an information icon and a toggle switch that is currently turned off. At the bottom, there's a section titled 'Form validation rules' with an information icon.

This pauses the main flow on this page until the challenge status changes. We'll update the challenge status in the secondary flow. Any change in the challenge status, regardless of the value, will cause this flow to continue.

4. Build a secondary flow that thanks the user for clicking the link and signals the main flow to continue by resolving the challenge:

1. Following your registration form, add another **Flow Conductor** connector parallel to the first one. Select the **Out-of-Band Continue** capability, and click **Apply**.

Note

You don't need to configure this node. It starts automatically when the user clicks the magic link.

2. Following your **Out-of-Band Continue** node, add a **Challenge** connector and select the **Update Transaction Status** capability.
3. In the **Challenge** field, click `{}` and select the `challenge` variable from your **Out-of-Band Continue** node.
4. In the **Challenge Status** list, select **approved**. Click **Apply**.

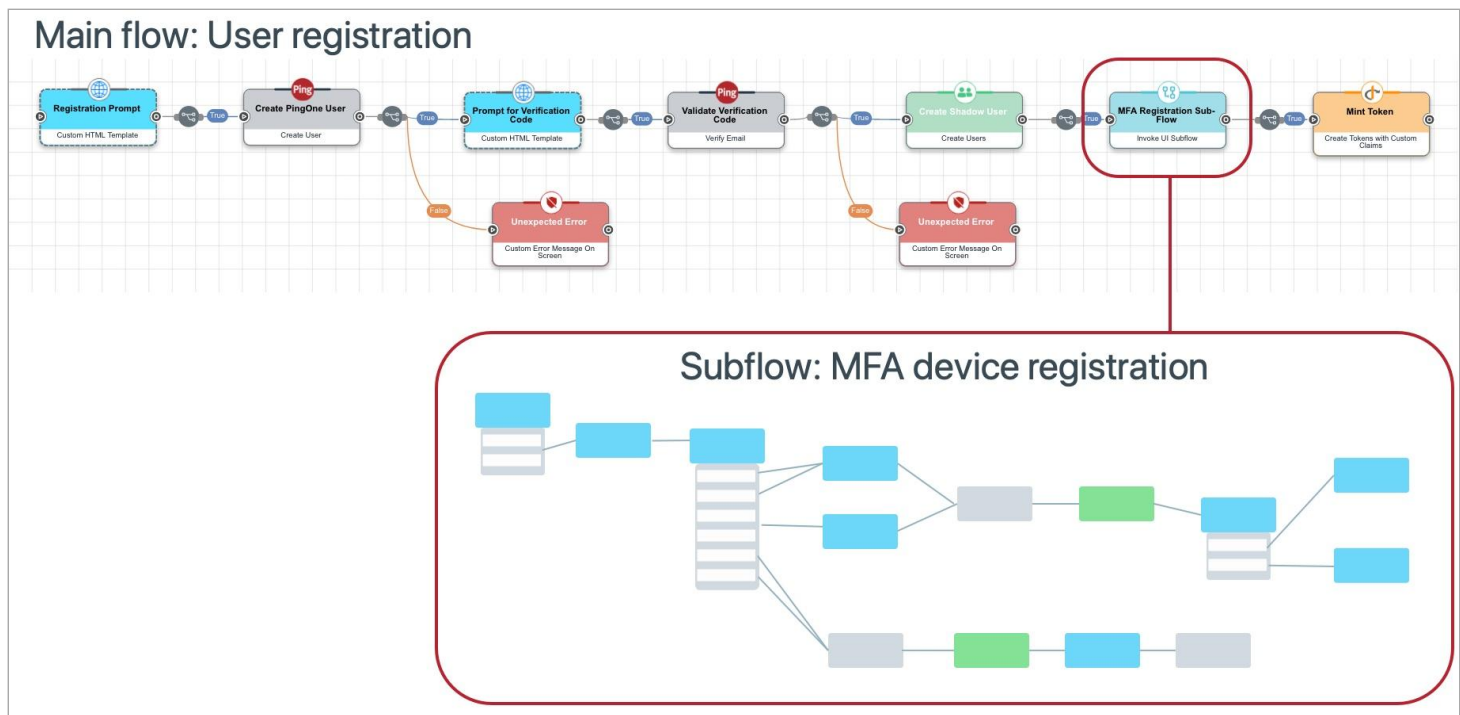
Because our **Custom HTML Template** page in the main flow is waiting for this challenge status to change, this update will trigger the flow to continue.

5. Add a "Thanks for verifying" page after your **Out-of-Band Continue** node. This page will appear when the user clicks the magic link.

5. Following your **Custom HTML Template** "waiting" page in the main flow, continue building the rest of your flow.

For example, you could direct the user to their user account self-service portal.

Linking to a subflow



Using subflows lets you organize large flows into smaller pieces that are more manageable and modular. This approach includes a main flow and one or more subflows.

In the example scenario below, the main flow allows guests to register a new user account. As part of the process, the user is prompted to add a multi-factor authentication (MFA) device.

This example organization created a subflow for MFA device management so it can be reused in an authentication flow and a user self-service portal flow.

Before you start, you need a main flow and a subflow. You can create these yourself, or import the **PingOne - Register with verify email and MFA enrollment** and **PingOne - Device registration sub-flow** flows in the [Flow Library](#).

1. In your main flow, create a link to your subflow:

1. Add the Flow Conductor connector and select the **Invoke UI Subflow** capability. Select the node that appears in your flow.

Note

We need this capability because there is a user interface component to our MFA setup experience. If your own flow doesn't have a UI component, select the **Invoke Subflow** capability instead.

2. In the **Flow** list, select the flow that you want to invoke. You can choose any flow in your environment, but you should only choose a flow that would work well in the middle of your main flow.
3. In the **Flow Version Id** field, enter a version number.

 Note

If you want to link to the latest version of the subflow, enter `-1`.

If you want to use a specific version, click **Edit Subflow** to open the **Flow Studio** in a new tab. Open the subflow and click **More Options (⋮) > Flow Versions** to see the list of versions.

4. Click **Apply** to save your changes.
2. Configure the input schema to pass properties from your main flow to your subflow:
 1. Click the **Edit Subflow** link to open the **Flow Studio** in a new tab.
 2. Open your subflow. In the example scenario, this is the MFA device registration flow.
 3. Click **More Options (⋮) > Input Schema**
 4. Click **Add**.
 5. In the **Property Name** field, enter the attribute that your subflow needs. In our example case, it's `pingone_userId`.
 6. In the **Data Type** list, we'll select **String** because it matches the data for the PingOne user ID.
 7. (Optional) Click **Add** to any more properties that your subflow needs.
 8. Click **Save** to save your changes.
 9. Click **Save** to save your flow.
3. Configure the output schema to pass properties from your subflow to back to your main flow. To determine the output schema, you can get an example payload and convert it in using an online tool.
 1. Copy your raw JSON output:
 1. At the end of your subflow, add an [HTTP](#) connector and select the **Custom HTML Message** capability. Click the new node in your flow.
 2. In the **Message** field, click `{}` and insert the **output (object)** variable from your the node immediately preceding the HTTP node you're editing.
 3. Click **Apply**, save, deploy, and run your changes.
 4. Copy the JSON payload that appears in your HTML message.
 5. Remove the **Custom HTML Message** node from your flow.
 2. In a browser, open the [Online JSON Schema Validator and Generator](#) tool.
 3. Paste the JSON response you copied into the **JSON** field. Click **Generate Schema From JSON**. Copy the output from the **JSON SCHEMA** field.

JSON	JSON SCHEMA
Generate Schema From JSON Browse JSON file	Generate JSON from Schema Browse JSON SCHEMA file
<pre data-bbox="290 298 875 312">1tatic/img/QH.png"},"value":"QUEEN","suit":"HEARTS"}],"remaining":47}}</pre>	<pre data-bbox="924 298 1422 604">1 { 2 "definitions": {}, 3 "\$schema": "http://json-schema.org/draft-07/schema#", 4 "\$id": "https://example.com/object1642544708.json", 5 "title": "Root", 6 "type": "object", 7 "required": [8 "headers", 9 "statusCode", 10 "body" 11], 12 "properties": { 13 "headers": { 14 "\$id": "#root/headers", 15 "title": "Headers", 16 "type": "object", 17</pre>

4. In your subflow, click **More Options (:)** > **Output Schema**.
 5. In the **Output Schema** field, paste the output schema that you copied.
 6. Click **Save** to save your changes.
 7. Click **Save** to save your flow.
4. Run your main flow to test it.

When your main flow reaches the Flow Conductor node, it jumps over to the MFA setup subflow and passes the necessary properties. When that flow completes, properties from the subflow are carried over and the main flow continues.

Capabilities

Receive Start Flow Redirect

Receive the redirect URI to start the flow.

Details

Properties

authenticatedRequest dropDown

tokenSigningMethod dropDown

clientId textField

clientSecret textField

issuerUrl textField

jwksKeys textArea

tokenHint textField

connectionId dropDown

claimsMapping mapping

Default:

```
[
  {
    "value1": "username",
    "value2": "sub",
    "deleteAllowed": false
  },
  {
    "value1": "name",
    "value2": "name",
    "deleteAllowed": false
  },
  {
    "value1": "email",
    "value2": "email",
    "deleteAllowed": false
  }
]
```

Out-of-Band Start (Links Only)

Receive links through email, SMS, or push notifications to continue the flow outside of the typical path.

Details

Properties

generateQr toggleSwitch
challengeLength textField
challengeExpiry textField
useCustomLink toggleSwitch
customLink textField

Output Schema

output object
challenge string
continueLink string
continueQr string

Out-of-Band Continue

Continue the flow in the out-of-band path.

Details

Properties

Node ID when this OOB link expires textField

Select Node ID when this OOB link expires

Output Schema

output object

status string

detailStatus string

rawStatus string

challenge string

credId string

Invoke Subflow

Invoke API-based subflows.

Details

Properties

subFlowId dropdownAsync

subFlowVersionId textField

Input Schema

default object

cookies object

List of cookies associated with the user.

ip string minLength: 1 maxLength: 255

Ip address of the user in current session.

userAgent string minLength: 1 maxLength: 250

Information about browser, OS, etc. of user in current session.

skOpenId object

Object containing client id of user.

origin string minLength: 0 maxLength: 500

Origin

originCookies string minLength: 0 maxLength: 5000

OriginCookies

Invoke UI Subflow

Invoke UI-based subflows.

Details

Properties

subFlowId dropdownAsync

subFlowVersionId textField

Input Schema

default object

cookies object

List of cookies associated with the user.

ip string minLength: 1 maxLength: 255

Ip address of the user in current session.

userAgent string minLength: 1 maxLength: 250

Information about browser, OS, etc. of user in current session.

skOpenId object

Object containing client id of user.

origin string minLength: 0 maxLength: 500

Origin

originCookies string minLength: 0 maxLength: 5000

OriginCookies

Flow Conductor Connector Release Notes

New features and improvements in the Flow Conductor connector.

November 2023

Updated Error Mappings

Fixed

The error mappings for the OOB Continue and OOB Start capabilities have been updated.

The following error mappings were removed from the OOB Continue capability:

```
'missingQueryData': 'The request did not include query data',  
'missingTokenData': 'The request was missing token data',  
'jwtError': 'There was a problem parsing the JWT',  
'validationError': 'There was a problem validating the JWT contents',  
'challengeRefExpired': 'The challenge reference has expired',  
'challengeRefNotFound': 'The challenge reference was not found',  
'challengeExpired': 'The challenge has expired',  
'challengeNotFound': 'The challenge could not be found',  
'challengeRefError': 'The challenge reference is invalid',  
'challengeAlreadyApproved': 'The challenge has already been approved'
```

If you modified any of these error messages, the modified version will remain. You can delete and recreate the node to remove the older mapping.

The following error mappings were added to the OOB Start capability:

```
'challengeExpired': 'The challenge has expired',  
'challengeAlreadyApproved': 'The challenge has already been approved',  
'unexpectedError': 'An unexpected error occurred'
```

The OOB Start capacity also includes a non-customizable error message displayed for some backend issues: **An internal error has occurred.** Contact support if you see this error message or `unexpectedError`.

Functions Connector

The Functions connector lets you branch your PingOne DaVinci flow using logical conditions or based on the result of custom JavaScript code.

You can use the Functions connector to:

- Compare the value of variables in your flow, such as $A > B$
- Perform calculations
- Run custom JavaScript



Important

For best practices to use custom code in your flows, see [Using custom code safely](#).

Setup

Setting up the Functions connector

In DaVinci, add a **Functions** connection. For help, see [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

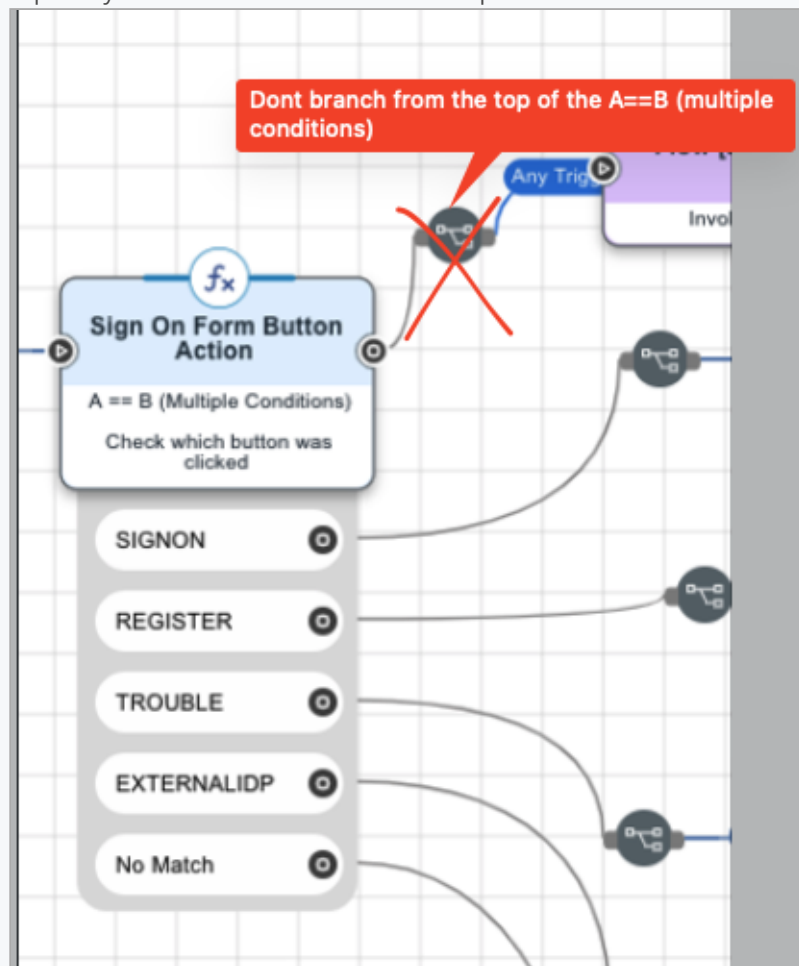
Using the connector in a flow

Comparing values

You can compare values using a variety of comparison capabilities, such as $A == B$, $A != B$, and $A < B < C$.

Important

A node with the $A == B$ capability cannot be branched from the top:



For example, we can check whether a user is eligible for a senior's discount based on their age:

1. In your flow, add the **Functions** connector and select the $A >= B$ capability. Select the node that appears in your flow.
2. In the **Value A** field, click {}, then select the attribute that holds the user's current age.

3. In the **Value B** field, enter 65.

A >= B

GENERAL **SETTINGS** >

* indicates required

Value A

Value B

Type:

String ▼

4. After applying your changes, you can add a True branch from your node for seniors, and a False branch for those who aren't.

Adding a custom function to your flow

You can make your flows more powerful and flexible by adding your own custom code. This capability lets you take inputs from your flow, work with them in JavaScript, and make the results available in your flow.

The JavaScript in a custom function runs on the server, not the client. These functions stay with your flow if you export it to another DaVinci environment.

For example, we want to know how long until a user turns 65 and gets a senior's discount. We already know their age from earlier in the flow and that they're younger than 65. Our code will subtract their current age from 65 and make the result available in the flow.

 Note

The following libraries are available in custom functions:

- [File System](#) (non-functional mockup only)
- [Buffer](#)
- All JavaScript built-in objects

 Note

All code for custom functions must comply with JavaScript's strict mode. For more information, see [Strict Mode](#).

1. In your flow, add the **Functions** connector and select the **Custom Function** capability.
2. Select the node that appears in your flow.
3. Make the variable with their current age available in your function:
 1. In the **Variable Input List**, click **Add**.
 2. In the **Variable Name** field, enter `currentAge`. Our code will call the variable by this name.
 3. In the **Value** field, click the input button and select the variable from your flow that you want as the value of `currentAge` in your function.
 4. In the **Data Type** list, select the type that best suits the value your variable holds.
 5. (Optional) To bring in more variables, click **Add** again.

 Tip

To remove an extra variable, click **Edit**, then click the remove button.

4. In the **Code** field, enter your JavaScript custom code.

 Tip

To give yourself more room to work, click the **Expand** (⌵) icon. This lets you use your browser zoom to enlarge the code.

Our code creates a variable called `ageDelta` that holds the difference between the user's current age and 65:

```
// How long until eligible for a senior's discount?
module.exports = a = async ({params}) => {
  Let ageDelta = 65 - params.currentAge
  return {'yearsUntilDiscount': ageDelta}
}
```

Our code returns a variable called `yearsUntilDiscount`.

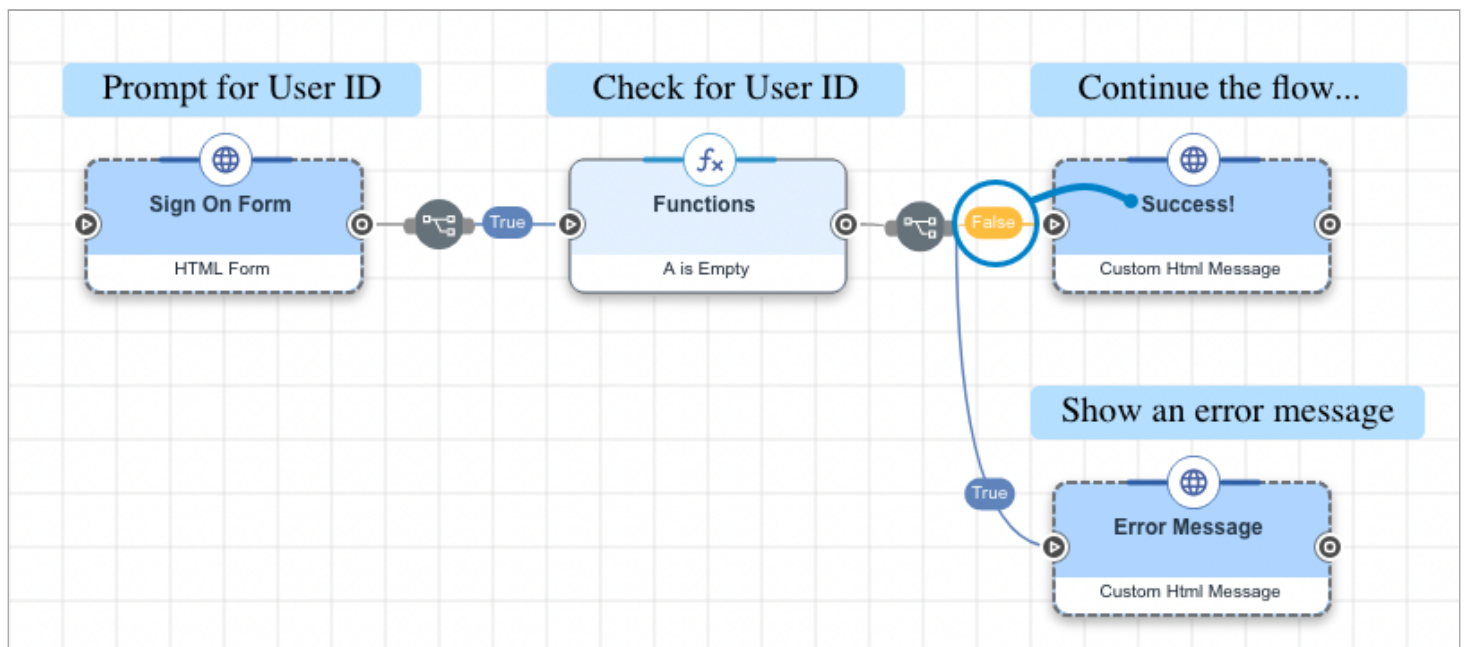
5. In the **Output Schema** field, capture the return variables from your code and make them available elsewhere in your flow.

```
{
  "output": {
    "type": "object",
    "properties": {
      "yearsUntilDiscount": {
        "type": "integer"
      }
    }
  }
}
```

Now, `yearsUntilDiscount` is available to use elsewhere in your flow.

Checking whether a variable has a value

When building a flow, it can be useful to check whether a variable contains a value. For example, testing whether the expected user ID or token has actually been provided earlier in the flow.



1. Check whether the variable is empty:

1. In your flow, add a **Functions** connector with the **A is Empty** capability.
2. In the **Value A** field, click `{}` and select the variable that you want to check.
3. Enable **Check undefined/null**.
4. In the **Type** list, select the type of data that the variable should contain.

A is Empty

GENERAL

SETTINGS

S >

* indicates required

Value A

UserID

✕

{ }

Check undefined/null ⓘ

☒

Type:

String ▼

5. Click **Apply**.

2. Add a success path by following the **A is Empty** node using the **Any Trigger False** condition.



Note

The **A is Empty** capability returns "false" when the expected User ID, token, or other value is provided. As a result, the success path for your flow follows branches from the "false" result.

3. Add an error message or failure path by following the **A is Empty** node using the **All Triggers True** condition.

Hashing a value

You can use the **Create a Hash** capability to hash the value provided by another node in your flow. Hashing transforms an input value into a fixed-length string or number for secure verification.

To hash a value:

1. In your flow, add a **Functions** connector with the **Create a Hash** capability.
2. In the **Input Value** field, enter the value or select the variable containing the value to hash.
3. Select a **Hash Algorithm** to use.
4. Select a **Salt Mode** to determine whether to add a salt value to make the hash value more unique and difficult to guess.

**Note**

To use a custom value, you can select **Use Custom Salt Value** and define your own in the **Custom Salt Value** field.

5. Select the **Output Encoding Format** for the resulting hash value.

**Note**

Binary encoding produces raw binary, which does not render meaningfully when the hashed value outputs to the screen in plain text.

Capabilities

A == B

If A equals B

Properties

leftValueA textField
rightValueB textField
type dropDown
Case Sensitive toggleSwitch

When enabled, the values are considered a match only if the case is the same.

A != B

If A is not equal to B

Properties

leftValueA textField
rightValueB textField
type dropDown
Case Sensitive toggleSwitch

When enabled, the values are considered a match only if the case is the same.

A < B

If A is less than B

Properties

leftValueA textField
rightValueB textField
type dropDown

A ≤ B

If A is less than or equal to B

Properties

leftValueA textField
rightValueB textField
type dropDown

A > B

If A is greater than B

Properties

leftValueA textField
rightValueB textField
type dropDown

A ≥ B

If A is greater than or equal to B

Properties

leftValueA textField
rightValueB textField
type dropDown

$B < A < C$

If A is between B and C

Properties

leftValueA textField
rightValueB textField
rightValueC textField
type dropDown

$B \Leftarrow A \Leftarrow C$

If A is between B and C or equal to B or C

Properties

leftValueA textField
rightValueB textField
rightValueC textField
type dropDown

$B \Leftarrow A < C$

If A is between B and C or equal to B

Properties

leftValueA textField
rightValueB textField
rightValueC textField
type dropDown

$B < A \Leftarrow C$

If A is between B and C or equal to C

Properties

leftValueA textField
rightValueB textField
rightValueC textField
type dropDown

A is Empty

If A is Empty

Properties

leftValueA *textField*

Check undefined/null *toggleSwitch*

Check undefined/null

type *dropDown*

If Array A includes B

Properties

leftValueA *textField*

rightValueB *textField*

type *dropDown*

inputContains *dropDown*

Case Sensitive *toggleSwitch*

When enabled, the values are considered a match only if the case is the same.

If String A includes B

Properties

leftValueA *textField*

rightValueB *textField*

Case Sensitive *toggleSwitch*

When enabled, the values are considered a match only if the case is the same.

Custom Function

Properties

variableInputList *variableInputList* *code* *codeEditor*

Follow example for code. Caution: Custom code is for advanced users only. Before using custom code, review the security risks in the DaVinci documentation by searching for "Using custom code safely".

Default:

```
// Write your code here
// Supported language: Javascript
module.exports = a = async ({params}) => {
  console.log('params: ', params)
  return {'testVariable': params.testVariable}
}
```

outputSchema *codeEditor*

Follow example for JSON schema.

Default:

```
{
  "output": {
    "type": "object",
    "properties": {
      "testVariable": {
        "type": "string"
      }
    }
  }
}
```

Output Schema

- output object::

Create a Hash

Hash a value using the selected algorithm

Properties

Input Value textField

The value to hash, such as "myPa55woRd123#".

Hash Algorithm dropDown

The hash algorithm to use.

- SHA-1
- SHA-256 (Default)
- SHA-384
- SHA-512

Salt Mode dropDown required

Determines whether to add a salt value to make the hashed value unique and more difficult to guess. For a custom value, select Use Custom Salt Value and enter the value in Custom Salt Value.

- Off (Default)
- Generate random salt
- Use Custom Salt Value

Custom Salt Value textField required

Enter the salt value to use when hashing, such as "mySaltu7v8w9x0".

Output Encoding Format dropDown required

The encoding method for the resulting hashed value.

- Base64
- Binary
- Hexadecimal (Default)

Input Schema

- default object
 - properties object
 - message string required

The input value to hash, such as "myPa55woRd123#".
 - digestAlgorithm string required

The hash algorithm to use.
 - saltMode string

Determines whether to add a salt value to make the hashed value unique. For useCustomSaltValue, provide the customSaltValue.
 - customSaltValue string

The salt value to use when hashing, such as "mySaltu7v8w9x0".
 - outputEncodingFormat string

The encoding method for the resulting hashed value.

Input Example

```
{ "properties" :  
  { "message" : "mysecretpassword",  
    "digestAlgorithm" : "sha256",  
    "saltMode" : "useCustomSaltValue",  
    "customSaltValue" : "mySaltu7v8w9x0",  
    "outputEncodingFormat" : "base64" } }
```

Output Schema

- output object

- hash string

The hashed value.

- salt string

The salt value used in the hash.

- length number

The length of the hashed value.

Output Example

```
{ "hash" : "NJM86MstFd2CZ04M5nMR4HvJdUaf0wpeSL5aFgS+r9A=",
  "salt" : "mySaltu7v8w9x0",
  "length" : 44 }
```

A == B (Multiple Conditions)

If A equals B or A equals to C ...

Properties

*leftValue*A *textField*

*rightValue*Multiple *multipleTextFields*

type *dropDown*

Case Sensitive *toggleSwitch*

When enabled, the values are considered a match only if the case is the same.

Functions Connector Release Notes

New features and improvements in the Functions connector. Updated December 4, 2024.

December 2024

New hashing options in the Functions connector

Updated

fx

Functions

id: 4t10rz8m3g

connectionId: de650ca45593b82c49064ead10b9fe17

<

TRIGGER:

Create a Hash

GENERAL

SETTINGS

S >

Input Value * ⓘ

* indicates required

myinputvalue

Hash Algorithm * ⓘ

SHA-512

Salt Mode * ⓘ

Use Custom Salt Value

Custom Salt Value * ⓘ

uniquesaltvalue

Output Encoding Format * ⓘ

Hexadecimal

Close

Apply

Hashing a value is an effective way to verify data in your flow while keeping it secure. To make this easier, we've added new configuration options to the **Create a Hash** capability in the Functions connector. Select the hashing algorithm, use a generated salt value or provide your own, and choose the final encoding method.

G-I



Google Workspace Admin Connector

The Google Workspace Admin connector lets you manage Google Workspace users, groups, and application licenses in your PingOne DaVinci flow.



HTTP Connector

This powerful and versatile connector lets you show custom HTML pages, make REST API calls, and more in your DaVinci orchestration flow.



HYPR Connector

The HYPR connector lets you use HYPR for passwordless authentication in your PingOne DaVinci flow.



ID DataWeb Connector

The ID DataWeb connector lets you use ID DataWeb for identity verification in your PingOne DaVinci flow.

Google Workspace Admin Connector

The Google Workspace Admin connector lets you manage Google Workspace users, groups, and application licenses in your PingOne DaVinci flow.

Setup

Resources

For information and setup help, see the following documentation:

- Google Workspace documentation:
 - [Using OAuth 2.0 for Server to Server Applications](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need administrator access for your Google organization.

Setting up Google Workspace Admin

Follow the instructions in [Using OAuth 2.0 for Server to Server Applications](#) to do the following:

1. Create a service account.
2. Delegate domain-wide authority to the service account and authorize it with the following scopes:

```
https://www.googleapis.com/auth/admin.directory.user,  
https://www.googleapis.com/auth/admin.directory.group,  
https://www.googleapis.com/auth/admin.directory.device.chromeos,  
https://www.googleapis.com/auth/admin.directory.device.mobile,  
https://www.googleapis.com/auth/apps.licensing
```

Setting up the Google Workspace Admin connector configuration

In DaVinci, add a **Google Workspace Admin** connection. For help, see [Adding a connector](#).

Connector configuration

Service Account Email Address

The email address associated with the Google Workspace service, such as `google-workspace-admin@xenon-set-123456.iam.gserviceaccount.com`. You can find this on the [Service Accounts](#) page.

Filter Enter property name or value			
☐	Email	Status	Name ↑
☐	 google-workspace-admin@xenon-set-123456.iam.gserviceaccount.com	✓	davinci-workspace-service

Admin Email Address

The email address you use to sign on to Workspace as an administrator.

Private Key

The private key associated with the public key that you added to the Google Workspace Admin service.

If you allowed Workspace to generate the key pair, open the downloaded `.json` file and copy the private key value.

```
{
  "type": "service_account",
  "project_id": "genial-upgrade-123456",
  "private_key_id": "4657e3d54657e3d54657e3d54657e3d54657e3d5",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAcwggSjAgEAAoIBAQDgp27nqx5Ai40L\n87ktfYrLnb2m8aKMiBgo
ZbT5QIrbYGpVztIC0UFcUtZMj1ZQaMECHbKH+p/
...
EF8w90SMcG9lM\nA88aLUHVExRIoAYmiCzVB9uQQeasZKVT0srmPjFmnWaB7J4czwRifuvCc3QSlldch\nnwMX7uHe
puCTQAI9/SPHdhVs=\n-----END PRIVATE KEY-----\n",
  "client_email": "google-workspace-admin@xenon-set-123456.iam.gserviceaccount.com",
  "client_id": "112711271127112711271",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://oauth2.googleapis.com/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/google-workspace-admin%40xenon-set-123456.iam.gserviceaccount.com"
}
```

Using the connector in a flow

Managing users

The connector has several capabilities that allow you to manage users in Workspace:

- **Create a User**
- **Delete a User**
- **Update a User**
- **Get User Information**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing group memberships

The connector has several capabilities that allow you to manage the users that belong to each group in Workspace:

- **Add a User to a Group**
- **Remove a User from a Group**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing user devices

The connector has several capabilities that allow you to list and take administrative action on the mobile devices associated with users in Workspace:

- **List a User's Devices**
- **Manage a Device**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing application licenses

The connector has several capabilities that allow you to manage the applications that each user can access in Workspace:

- **Assign a License to a User**
- **Revoke a User's License**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make Custom API Call** capability to define your own action.

This capability uses the credentials from your connection to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Create a User

Create a new user account

Properties

Primary Email textField

The user's primary email address.

Password textField

The password to assign to the user account.

Family Name textField

The user's last name.

Given Name textField

The user's given name.

Other User Attributes variableInputList

Define additional attributes to add to the user account. For help, see the User Accounts section of the Google Workspace SDK documentation.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - primaryEmail string required
 - password string required
 - familyName string required
 - givenName string required

Output Schema

- output object
 - rawResponse object
 - id string
 - primaryEmail string
 - password string
 - hashFunction string
 - isAdmin boolean
 - isDelegatedAdmin boolean
 - agreedToTerms boolean
 - suspended boolean
 - changePasswordAtNextLogin boolean
 - ipWhitelisted boolean
 - name object
 - givenName string
 - familyName string
 - fullName string
 - kind string
 - etag string
 - emails array
 - Array Item Schema object
 - address string
 - customType string
 - type string
 - primary boolean
 - externalIds array
 - Array Item Schema object
 - customType string
 - type string
 - value string

- relations array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- aliases array
 - Array Item Schema string
- isMailboxSetup boolean
- customerId string
- addresses array
 - Array Item Schema object
 - country string
 - countryCode string
 - customType string
 - extendedAddress string
 - formatted string
 - locality string
 - poBox string
 - postalCode string
 - primary boolean
 - region string
 - sourceStructured boolean
 - streetAddress string
 - type string
- organizations array
 - Array Item Schema object
 - costCenter string
 - customType string
 - department string
 - description string

- domain string
- fullTimeEquivalent integer
- location string
- name string
- primary boolean
- symbol string
- title string
- type string
- lastLoginTime string
- phones array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- suspensionReason string
- thumbnailPhotoUrl string
- languages array
 - Array Item Schema object
 - customLanguage string
 - languageCode string
 - preference string
- posixAccounts array
 - Array Item Schema object
 - accountId string
 - gecos string
 - gid integer
 - homeDirectory string
 - operatingSystemType string
 - primary boolean

- shell string
- systemId string
- uid integer
- username string
- creationTime string
- nonEditableAliases array
 - Array Item Schema string
- sshPublicKeys array
 - Array Item Schema object
 - expirationTimeUsec integer
 - fingerprint string
 - key string
- notes object
 - contentType string
 - value string
- websites array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- locations array
 - Array Item Schema object
 - area string
 - buildingId string
 - customType string
 - deskCode string
 - floorName string
 - floorSection string
 - type string

- includeInGlobalAddressList boolean
- keywords array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- deletionTime string
- gender object
 - addressMeAs string
 - customGender string
 - type string
- thumbnailPhotoEtag string
- ims array
 - Array Item Schema object
 - customProtocol string
 - customType string
 - im string
 - primary boolean
 - protocol string
 - type string
- customSchemas object
 - somefield string
- isEnrolledIn2Sv boolean
- isEnforcedIn2Sv boolean
- archived boolean
- orgUnitPath string
- recoveryEmail string
- recoveryPhone string
- statusCode integer

- headers object

- etag string
- content-type string
- vary string
- date string
- server string
- content-length string
- x-xss-protection string
- x-frame-options string
- x-content-type-options string
- alt-svc string
- connection string

Delete a User

Delete a user account

Properties

User Identifier textField

The user's primary email address, unique user id, or one of the user's alias email addresses.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - userKey string required

Output Schema

- output object
 - rawResponse string
 - statusCode integer
 - headers object
 - etag string
 - vary string
 - date string
 - content-type string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

Get User Information

Get information about a user

Properties

User Identifier textField

The user's primary email address, unique user id, or one of the user's alias email addresses.

Requested Fields dropDown

The level of information to request about the user. "Basic" returns a standard set of fields. "Full" returns all fields. "Use Custom Field Schemas" returns the Basic fields as well as specific fields associated with the schemas you enter in "Custom Field Schemas".

- BASIC
- CUSTOM
- FULL

View Type dropDown

The type of fields to request. "Admin View" returns publicly visible and administrator-only fields. "Public View" only returns publicly visible fields.

- Admin View
- Domain Public

Output Filter textFieldArrayView

The list of fields for the connector to output to the flow, such as "emails" or "emails.address". Instead of outputting all of the results from the "Requested Attributes", you can filter the results to a list of specific fields. Type a field name and press Enter to add it. Leave this field blank to include all requested fields in the connector output.

Custom Field Schemas textFieldArrayView

The list of schemas to request. This returns all fields associated with the listed schemas. Type a schema name and press Enter to add it.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - userKey string required

Output Schema

- output object
 - rawResponse object
 - id string
 - primaryEmail string
 - password string
 - hashFunction string
 - isAdmin boolean
 - isDelegatedAdmin boolean
 - agreedToTerms boolean
 - suspended boolean
 - changePasswordAtNextLogin boolean
 - ipWhitelisted boolean
 - name object
 - givenName string
 - familyName string
 - fullName string
 - kind string
 - etag string
 - emails array
 - Array Item Schema object
 - address string
 - customType string
 - type string
 - primary boolean
 - externalIds array
 - Array Item Schema object
 - customType string
 - type string
 - value string

- relations array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- aliases array
 - Array Item Schema string
- isMailboxSetup boolean
- customerId string
- addresses array
 - Array Item Schema object
 - country string
 - countryCode string
 - customType string
 - extendedAddress string
 - formatted string
 - locality string
 - poBox string
 - postalCode string
 - primary boolean
 - region string
 - sourceStructured boolean
 - streetAddress string
 - type string
- organizations array
 - Array Item Schema object
 - costCenter string
 - customType string
 - department string
 - description string

- domain string
- fullTimeEquivalent integer
- location string
- name string
- primary boolean
- symbol string
- title string
- type string
- lastLoginTime string
- phones array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- suspensionReason string
- thumbnailPhotoUrl string
- languages array
 - Array Item Schema object
 - customLanguage string
 - languageCode string
 - preference string
- posixAccounts array
 - Array Item Schema object
 - accountId string
 - gecos string
 - gid integer
 - homeDirectory string
 - operatingSystemType string
 - primary boolean

- shell string
- systemId string
- uid integer
- username string
- creationTime string
- nonEditableAliases array
 - Array Item Schema string
- sshPublicKeys array
 - Array Item Schema object
 - expirationTimeUsec integer
 - fingerprint string
 - key string
- notes object
 - contentType string
 - value string
- websites array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- locations array
 - Array Item Schema object
 - area string
 - buildingId string
 - customType string
 - deskCode string
 - floorName string
 - floorSection string
 - type string

- includeInGlobalAddressList boolean
- keywords array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- deletionTime string
- gender object
 - addressMeAs string
 - customGender string
 - type string
- thumbnailPhotoEtag string
- ims array
 - Array Item Schema object
 - customProtocol string
 - customType string
 - im string
 - primary boolean
 - protocol string
 - type string
- customSchemas object
 - somefield string
- isEnrolledIn2Sv boolean
- isEnforcedIn2Sv boolean
- archived boolean
- orgUnitPath string
- recoveryEmail string
- recoveryPhone string
- statusCode integer

- headers object

- etag string
- content-type string
- vary string
- date string
- server string
- content-length string
- x-xss-protection string
- x-frame-options string
- x-content-type-options string
- alt-svc string
- connection string

Update a User

Update information about a user

Properties

User Identifier textField

The user's primary email address, unique user id, or one of the user's alias email addresses.

Other User Attributes variableInputList

Define additional attributes to add to the user account. For help, see the User Accounts section of the Google Workspace SDK documentation.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - userKey string required

Output Schema

- output object
 - rawResponse object
 - id string
 - primaryEmail string
 - password string
 - hashFunction string
 - isAdmin boolean
 - isDelegatedAdmin boolean
 - agreedToTerms boolean
 - suspended boolean
 - changePasswordAtNextLogin boolean
 - ipWhitelisted boolean
 - name object
 - givenName string
 - familyName string
 - fullName string
 - kind string
 - etag string
 - emails array
 - Array Item Schema object
 - address string
 - customType string
 - type string
 - primary boolean
 - externalIds array
 - Array Item Schema object
 - customType string
 - type string
 - value string

- relations array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- aliases array
 - Array Item Schema string
- isMailboxSetup boolean
- customerId string
- addresses array
 - Array Item Schema object
 - country string
 - countryCode string
 - customType string
 - extendedAddress string
 - formatted string
 - locality string
 - poBox string
 - postalCode string
 - primary boolean
 - region string
 - sourceStructured boolean
 - streetAddress string
 - type string
- organizations array
 - Array Item Schema object
 - costCenter string
 - customType string
 - department string
 - description string

- domain string
- fullTimeEquivalent integer
- location string
- name string
- primary boolean
- symbol string
- title string
- type string
- lastLoginTime string
- phones array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- suspensionReason string
- thumbnailPhotoUrl string
- languages array
 - Array Item Schema object
 - customLanguage string
 - languageCode string
 - preference string
- posixAccounts array
 - Array Item Schema object
 - accountId string
 - gecos string
 - gid integer
 - homeDirectory string
 - operatingSystemType string
 - primary boolean

- shell string
- systemId string
- uid integer
- username string
- creationTime string
- nonEditableAliases array
 - Array Item Schema string
- sshPublicKeys array
 - Array Item Schema object
 - expirationTimeUsec integer
 - fingerprint string
 - key string
- notes object
 - contentType string
 - value string
- websites array
 - Array Item Schema object
 - customType string
 - primary boolean
 - type string
 - value string
- locations array
 - Array Item Schema object
 - area string
 - buildingId string
 - customType string
 - deskCode string
 - floorName string
 - floorSection string
 - type string

- includeInGlobalAddressList boolean
- keywords array
 - Array Item Schema object
 - customType string
 - type string
 - value string
- deletionTime string
- gender object
 - addressMeAs string
 - customGender string
 - type string
- thumbnailPhotoEtag string
- ims array
 - Array Item Schema object
 - customProtocol string
 - customType string
 - im string
 - primary boolean
 - protocol string
 - type string
- customSchemas object
 - somefield string
- isEnrolledIn2Sv boolean
- isEnforcedIn2Sv boolean
- archived boolean
- orgUnitPath string
- recoveryEmail string
- recoveryPhone string
- statusCode integer

- headers object

- etag string
- content-type string
- vary string
- date string
- server string
- content-length string
- x-xss-protection string
- x-frame-options string
- x-content-type-options string
- alt-svc string
- connection string

Add a User to a Group

Add a user to a group

Properties

Group Identifier textField

The group's primary email address, unique group id, or alias.

Member Email textField

The member's email address. The member can be a user or another group.

Member Role dropDown

The role to assign the member in the group.

- Manager
- Member
- Owner

Member Type dropDown

The type of member in the group.

- Customer
- External
- Group
- User

Member Email Delivery Settings dropDown

The member's email delivery frequency.

- ALL_MAIL
- DAILY
- DIGEST
- DISABLED
- NONE

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - groupKey string required
 - memberEmail string required

Output Schema

- output object
 - rawResponse object
 - id string
 - email string
 - name string
 - description string
 - adminCreated boolean
 - directMembersCount string
 - kind string
 - etag string
 - aliases array
 - nonEditableAliases array
 - statusCode integer
 - headers object
 - etag string
 - content-type string
 - vary string
 - date string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

Remove a User from a Group

Remove a user from a group

Properties

Member Key textField

Identifies the group member in the API request.

Group Identifier textField

The group's primary email address, unique group id, or alias.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - groupKey string required
 - memberKey string required

Output Schema

- output object
 - statusCode integer
 - headers object
 - vary string
 - date string
 - content-type string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

List a User's Devices

Query Google Workspace for a list of devices associated with a user account

Properties

Customer ID textField

The unique ID for the customer's Google Workspace account, such as "C123abc4d". This ID is available from the "Get User Information" capability.

Maximum Number of Results textField

The maximum number of results to return from the query, up to 100.

Device Order dropDown

The device property to use for sorting results.

- DEVICE_ID
- EMAIL
- LAST_SYNC
- MODEL
- NAME
- OS
- STATUS
- TYPE

Requested Device Fields dropDown

The level of information to request about the device. "Basic" returns a standard set of fields. "Full" returns all fields.

- BASIC
- FULL

Query String textField

The query used to search for devices, such as "status:approved" or "os:Android". For help, see documentation for "Mobile device search fields" section of the Google Workspace SDK Directory API documentation.

Sort Order dropDown

The sort order for the list of devices. This is required if you have selected a "Device Order" option.

- ASCENDING
- DESCENDING

Page Token textField

The token used to specify the next page in the results, such as "3". Use this to get pages of results for queries that return more than the maximum number of results.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - customerId string required
 - maxResults number
 - orderBy string
 - deviceProjection string
 - query string
 - sortOrder string

Output Schema

- output object
 - kind string
 - etag string
 - mobiledevices array
 - Array Item Schema object
 - kind string
 - etag string
 - resourceId string
 - deviceId string
 - name array
 - Array Item Schema string
 - email array
 - Array Item Schema string
 - model string
 - os string
 - type string
 - status string
 - hardwareId string
 - firstSync string
 - lastSync string
 - userAgent string
 - serialNumber string
 - imei string
 - meid string
 - wifiMacAddress string
 - networkOperator string
 - defaultLanguage string
 - managedAccountIsOnOwnerProfile boolean
 - deviceCompromisedStatus string

- buildNumber string
- kernelVersion string
- basebandVersion string
- unknownSourcesStatus boolean
- developerOptionsStatus boolean
- otherAccountsInfo array
 - Array Item Schema string
- adbStatus boolean
- supportsWorkProfile boolean
- manufacturer string
- releaseVersion string
- securityPatchLevel string
- brand string
- bootloaderVersion string
- hardware string
- encryptionStatus string
- devicePasswordStatus string
- privilege string
- applications array
 - Array Item Schema object
 - packageName string
 - displayName string
 - versionName string
 - versionCode string
 - permission array
 - Array Item Schema string
- nextPageToken string

Manage a Device

Take administrative action on a device, such as approving, blocking, or wiping data

Properties

Customer ID textField

The unique ID for the customer's Google Workspace account, such as "C123abc4d". This ID is available from the "Get User Information" capability.

Device ID textField

The device ID, such as "AFiQxQ-WO...YM-hf080OZy".

Action dropDown

The administrative action to take on the device.

- Admin remote wipe
- Admin account wipe
- Approve
- Block
- Cancel remote wipe then activate
- Cancel remote wipe then block

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - customerId string required
 - resourceId string required
 - action string required

Output Schema

- output object
 - rawResponse string
 - statusCode integer
 - headers object
 - etag string
 - vary string
 - date string
 - content-type string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

Assign a License to a User

Grant a user access to a product by assigning a license

Properties

Product ID textField

The product ID, such as "Google-Apps".

SKU ID textField

The SKU ID, such as "Google-Apps-For-Business".

User ID textField

The user's primary email address.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - productId string required
 - skuld string required
 - licenseUserId string required

Output Schema

- output object
 - rawResponse object
 - userId string
 - statusCode integer
 - headers object
 - etag string
 - content-type string
 - vary string
 - date string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

Revoke a User's License

Remove a user's access to a product by revoking a license

Properties

Product ID textField

The product ID, such as "Google-Apps".

SKU ID textField

The SKU ID, such as "Google-Apps-For-Business".

User ID textField

The user's primary email address.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - productId string required
 - skuld string required
 - licenseUserId string required

Output Schema

- output object
 - statusCode integer
 - headers object
 - etag string
 - content-type string
 - vary string
 - date string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

Make a Custom API Call

Define and use your own call to the Google Workspace Admin REST API

Properties

Endpoint textField required

The Workspace API endpoint, such as "https://admin.googleapis.com/admin/directory/v1/users/user@example.com".

HTTP Method dropdown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE

Query Parameters keyValueList

Query parameters for the request.

Additional Headers keyValueList

Define additional headers to send to Workspace. For help, see the Google Workspace API documentation.

Body codeEditor

The body of the API call.

Input Schema

- default object
 - properties object
 - privateKey string required
 - iss string required
 - sub string required
 - endpoint string required
 - method string required

Output Schema

- output object
 - rawResponse object
 - statusCode integer
 - headers object
 - etag string
 - content-type string
 - vary string
 - date string
 - server string
 - content-length string
 - x-xss-protection string
 - x-frame-options string
 - x-content-type-options string
 - alt-svc string
 - connection string

HTTP Connector

This powerful and versatile connector lets you show custom HTML pages, make REST application programming interface (API) calls, and more in your DaVinci orchestration flow.

Use it to create a custom HTML message, show flow progress, or send custom responses in an API-triggered flow. You can use the messages as quick placeholders to help you sketch out a new flow. If you want to craft a memorable user experience, use the **Custom HTML Template** capability to create complete HTML pages with your own structure, style, and scripts.

Because this connector allows you to quickly add API calls and user interfaces, it can be a valuable sketching tool in your flow design process or to prove the design for a connector your organization might build.

Setup

Configuring the HTTP connector

In DaVinci, add an **HTTP** connection. Learn more in [Adding a connector](#).

Connector configuration

reCAPTCHA v2 Site Key

The site key provided in your reCAPTCHA dashboard. Learn more in [Creating reCAPTCHA keys](#) in the Google documentation.

This field is only needed for the connector's reCAPTCHA capability.

reCAPTCHA v2 Secret Key

The secret key provided in your reCAPTCHA dashboard. Learn more in [Creating reCAPTCHA keys](#) in the Google documentation.

This field is only needed for the connector's reCAPTCHA capability.

Select an OpenID token management connection for signed HTTP responses

To add a selection to this list, go to **Connections** and add a **Token Management** connector.

This selection is only needed if you want to sign HTTP responses.

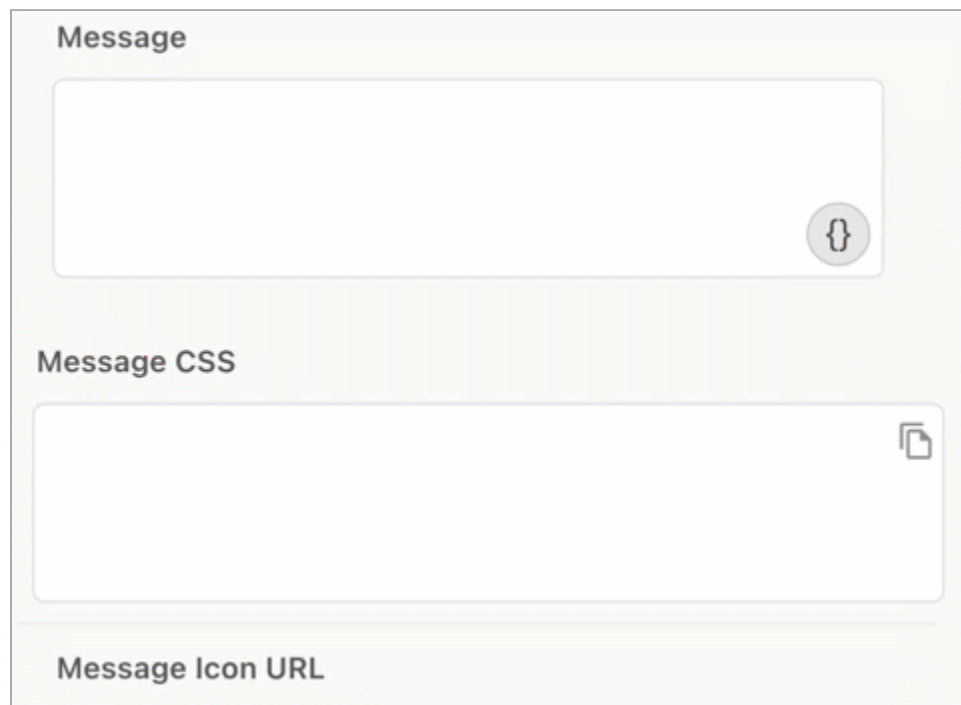
Using the connector in a flow

Showing simple messages

If you want to show information to the user, the **Custom HTML Message** capability gives you a premade page with a title, message, and button. You can't change the structure, but you can add an icon or style the message with your CSS. This is useful for error messages and confirmations, such as confirming a user's registration details.

1. In your flow, add the **HTTP** connector and select the **Custom HTML Message** capability.
2. Add a **Message Title**, such as "Welcome."
3. Add a **Message**. You can include values from elsewhere in your flow by clicking , then selecting the attribute that holds the value you want.

For this example, insert the username that the user entered into the registration form created by the PingOne Forms connector:



The image shows a configuration panel for a connector. It has three main sections: 'Message' with a large text input field and a JSON icon; 'Message CSS' with a text input field and a copy icon; and 'Message Icon URL' with a text input field.

4. If you don't want the flow to end here, turn on **Show Continue Button** and customize the button **Display Name**.

Building a custom page

The **Custom HTML Template** capability lets you include an HTML page in your flow. The structure, style, and behavior is entirely up to you.

Note

For creating forms, the PingOne Forms connector provides a drag-and-drop experience builder. Learn more in [PingOne Forms Connector](#) and [PingOne Forms](#).

Starting with a template from the UI Studio

To start your custom HTML page, you can autofill its settings from any template you created in the [UI Studio](#). This makes it easy to create several pages from the same template. Keep the following in mind:

- If you modify your HTML page in your flow, it won't affect your original template in the UI Studio.
- When you select a UI template from within an HTTP node, it overwrites any work you've done in that node. The UI templates are best used for newly-created HTTP nodes.

< **TRIGGER:**

Custom HTML Template

GENERAL SETTINGS >

* indicates required

Select UI Template

Registration ▾

HTML Template Switch View ☐

Use Recaptcha Verification ⓘ ☐

Adding your HTML, CSS, and scripts

Your custom page defines the look and behavior of a widget that is powered by React.

Adding custom HTML

The **HTML Template** field lets you see and modify the HTML for your page.

Tip

- Click **Switch View** to see the HTML formatted with syntax highlighting.
- Click the **Maximize** () icon to give yourself more room to work.
- To access a variety of useful tools, right-click the field when you're in syntax highlighting mode (dark background).

Important

For security reasons, the **HTML** field only allows certain HTML elements. You can find the elements on the allow list in the [DOMPurify allow list](#).

Note that custom HTML elements from the `svgDisallowed` and `mathMLDisallowed` lists are not allowed.

These restrictions apply to all custom HTML fields in DaVinci.

If you want your HTML to include values from elsewhere in your flow, switch back to the initial view (white background), click `{}`, and then select the variable that holds the value you want.

HTML Template

Switch View ☒

```

1 <div class="container" id="container">
2   <div class="form-container sign-in-container">
3     <form action="#">
4       <h1>
5         Sign in to
6       </h1>
7       <input type="email" placeholder="Email">
8       <input type="password" placeholder="Password">
9       <button>Sign In</button>
10    </form>
11  </div>
12  <div class="overlay-container">
13    <div class="overlay">
14      <div class="overlay-panel overlay-right">
15        <h1>Hello, Friend!</h1>
16        <p>Enter your personal details and</p>
17        <button class="ghost" id="signUp">Sign Up</button>
18      </div>
19    </div>
20  </div>
21 </div>
22

```

Important

The **HTML Template** field doesn't support inline events or script tags. Refer to the following script [Adding a custom script](#).

Adding custom CSS

The **CSS** field lets you add styles to the HTML page. The contents of the CSS field is appended to the body of the widget. You can use any standard CSS, including `@import`.



Adding a custom script

The **Script** field allows you to customize the behavior of your page. You can use any standard JavaScript in the **Script** field.



Important

The **HTML Template** field doesn't support inline events or script tags. Instead of triggering events with the HTML, such as with `<button onclick="myFunction()">Click me</button>`, use the **Script** field to listen for the event instead.

Example: Triggering a script with a button

In the **HTML Template** field, add a button.

```
<h2>JavaScript addEventListener()</h2>
```

```
<p>This example uses the addEventListener() method to attach a click event to a button.</p>
```

```
<button id="myButton">Try it</button>
```

```
<p id="demo"></p>
```

In the **Script** field, add an event listener and associate it with the button ID.

```
//Listen for a click event on 'myButton', then run myFunction
document.getElementById("myButton").addEventListener("click", myFunction);

function myFunction () {
  //Enter your code here, for example:
  document.getElementById("demo").innerHTML = Date();
}
```

Managing the widget's states and functions

By default, scripts can't access the state and functions of the widget that contains the HTML page. To access them, you can use event-based communication between the script and the widget by dispatching JavaScript custom events.

In the **Script** field, trigger a custom event using the following structure.

```
const event = new window.CustomEvent('skevent', {
  detail: {
    type: EVENT_TYPE,
    payload: PAYLOAD
  }
});

window.dispatchEvent(event);
```

The widget has an event listener for `skevent`, so the widget will catch and process this event. The detail object is designed to match syntax of a standard [Redux](#) action object. You can use the following event types:

- `SET_STATE` lets you set a value in the state of the widget:

```
const event = new window.CustomEvent('skevent', {
  detail: {
    type: 'SET_STATE',
    payload: {
      name: 'email',
      value: 'testuser@example.com'
    }
  }
});

window.dispatchEvent(event);
```

- `GET_STATE` lets you get a value from the current state of the widget:

```
const event = new window.CustomEvent('skevent', {
  detail: {
    type: 'GET_STATE',
    payload: 'email'
  }
});

window.dispatchEvent(event);
```

The `GET_STATE` event dispatches an event called `skeventresponse` with the `STATE` event type. To complete the process, add an event listener to listen for the `skeventresponse` event:

```
window.addEventListener('skeventresponse', e => {
  switch(e.detail.type) {
    case 'STATE':
      console.log(e.detail.payload);
      break;
  }
});
```

The event listener produces the result from the `GET_STATE` event:

```
{
  "name": "email",
  "value": "testuser@example.com"
}
```

Adding form validation rules

You can add one or more form validation rules. Enter the name of the field in the **Property Name** field, then select a validation rule in the **Rule Name** list. The options for validation rules are:

- **Required**
- **Email**
- **Length**
- **Format**
- **Equality**

For each rule, validation is checked, and a validation message is displayed based on the results.

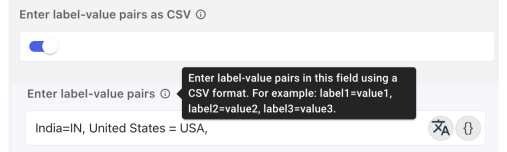
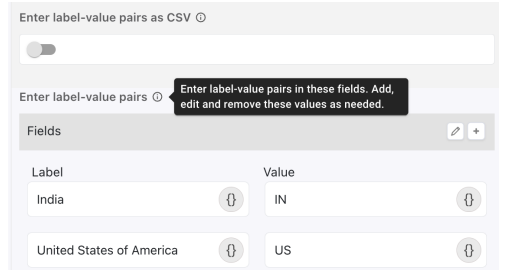
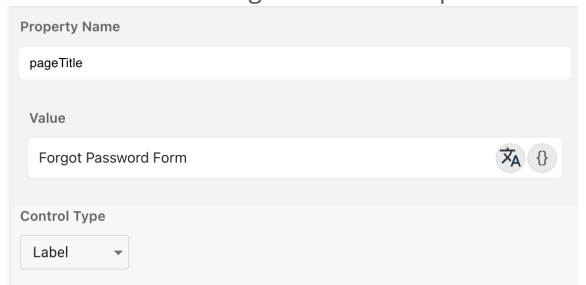
Adding output fields

You can add one or more output fields under **Output Fields List**. These fields outline the different outputs of the HTML form for use in Direct or SDK Flow Executions.

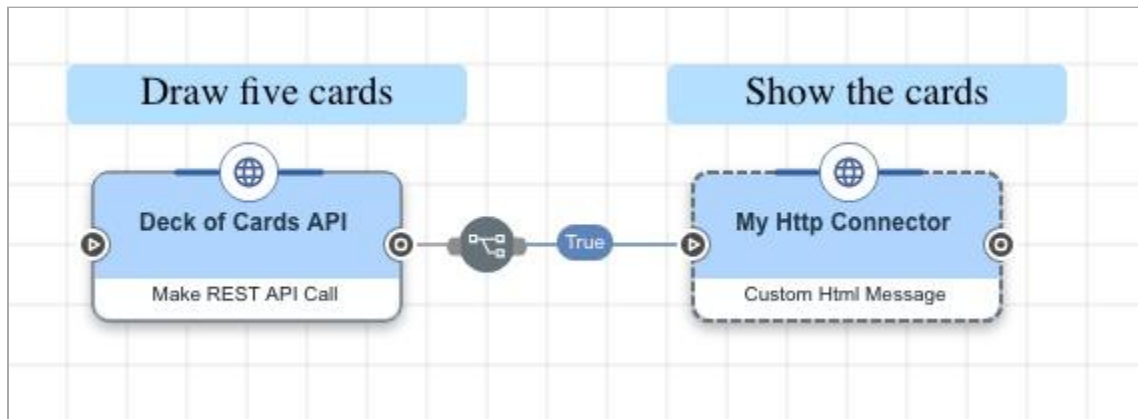
To configure an output field:

1. Enter a unique name for the property in the **Property Name** field. This name is assigned to the output in subsequent nodes when selecting the field as a variable.
2. Select a **Control Type** from the list and configure it based on the following table:

Control Type	Description	Configuration
Text Field	A field for users to input relevant information.	This control type is supported by both Direct and SDK Flow Executions with the following configuration: ◦ The Display Name provides text to help users understand the purpose of the text field. ◦ The Value represents a default text value that will be populated in the text field.
Secure Text Field / Password	A field to allow users to authenticate with a password.	This control type is supported by both Direct and SDK Flow Executions with the following configuration: ◦ The Control Type must be Text Field. ◦ The Display Name provides text to help users understand the purpose of the password field. ◦ Secure must be toggled on to make the text field a password field. ◦ The Value represents a default, pre-populated password. We recommend leaving this field empty.

Control Type	Description	Configuration
Dropdown	A dropdown list for uses such as providing country codes for phone numbers.	This component is supported only by SDK Flow Executions with the following configuration: ◦ The Display Name provides text to help users understand the purpose of the dropdown. ◦ You can enter label-value pairs to populate the dropdown options in two ways: ■ Toggle on Enter label-value pairs as CSV and enter pairs separated by commas:  ■ In Enter label-value pairs, click the + icon and enter the Label and Value. 
Radio Button List	A radio button component to provide a user with a small set of options.	This component is supported only by SDK Flow Executions with the following configuration: ◦ The Display Name provides text to help users understand the purpose of the radio button list. ◦ You can enter label-value pairs to populate the dropdown options in two ways: ■ Toggle on Enter label-value pairs as CSV and enter pairs separated by commas. ■ In Enter label-value pairs, click the + icon and enter the Label and Value.
Label	A label for the form that can be used as a form heading, such as "Welcome" or "Sign On."	This component is supported only by SDK Flow Executions with the following configuration: ◦ The Value is required to provide the content of the label in the user-facing form. For example: 

Making a REST API call



You can use the HTTP connector to make a call to any REST API. You can choose the call method (such as GET or POST) and configure query parameters, headers, body, and the responses. This is a flexible way to integrate your flow with external systems.

Important

Best practice is to use secret variables stored in **DaVinci > Variables**. Learn more in [Variables](#) and [Creating Variables](#).

The following example uses the <http://deckofcardsapi.com/> [Deck of Cards API] call to draw five cards, then make the cards available in the flow.

The Deck of Cards API documentation specifies the following URL to draw five cards:

<http://deckofcardsapi.com/api/deck/new/draw/?count=5>

Getting an API response

1. Making an API call

1. In your flow, add the **HTTP** connector and select the **Make REST API Call** capability.
2. In the **URL**, enter the API URL. In this example, this is `http://deckofcardsapi.com/api/deck/new/draw/`.
3. From the **HTTP Method** list, select the action to take, such as **GET**.
4. In the **Query Parameters** section, add each query parameter and its value. You can include values from elsewhere in your flow by clicking {}, then selecting the variable that holds the value you want. For this example, get five cards every time:

Query Parameters

Key	Value
count	5

5. In the **MTLS Support** list, select a key configured in PingOne to select the client certificate used in outbound mTLS connections.

 Note

Keys are configured in PingOne. To create a key in the PingOne admin console, click the **Certificates & Keypairs** link.

6. (Optional) In the **Timeout (ms)** field, enter a timeout for the API call.

 Note

To not have a timeout, leave the field blank. You can select any timeout value, but if the API call needs a response, there is a hard timeout at 30 seconds.

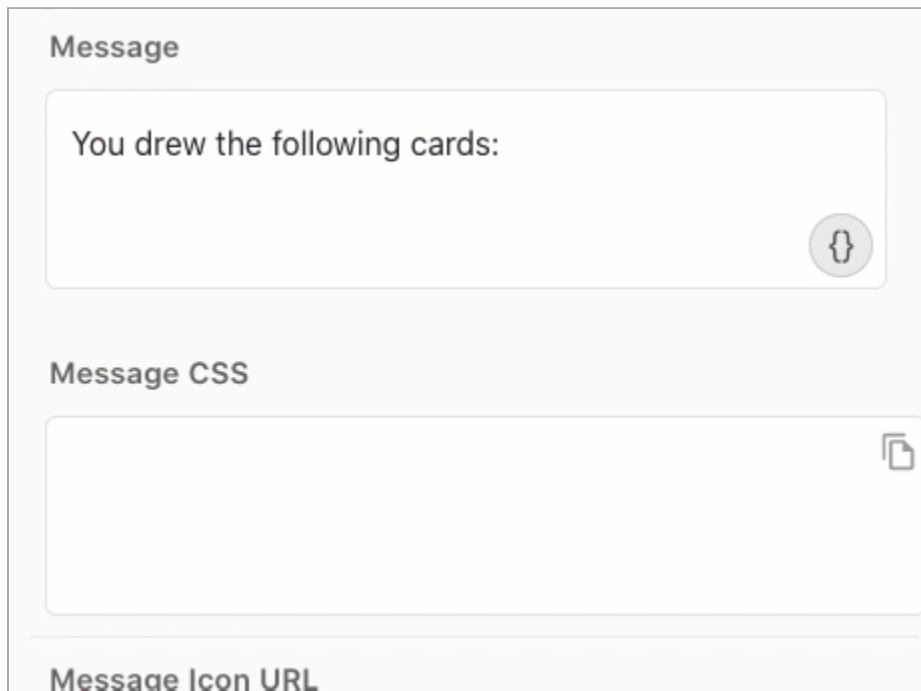
7. Click **Apply** to save your changes.

 Note

In your own flow, you can use the **Headers** and **Body Parameters** sections the same way to add any other parameters you need in your API call, and use the **Body** list, select the content type of the body data you're sending to the API.

2. Working with the API response

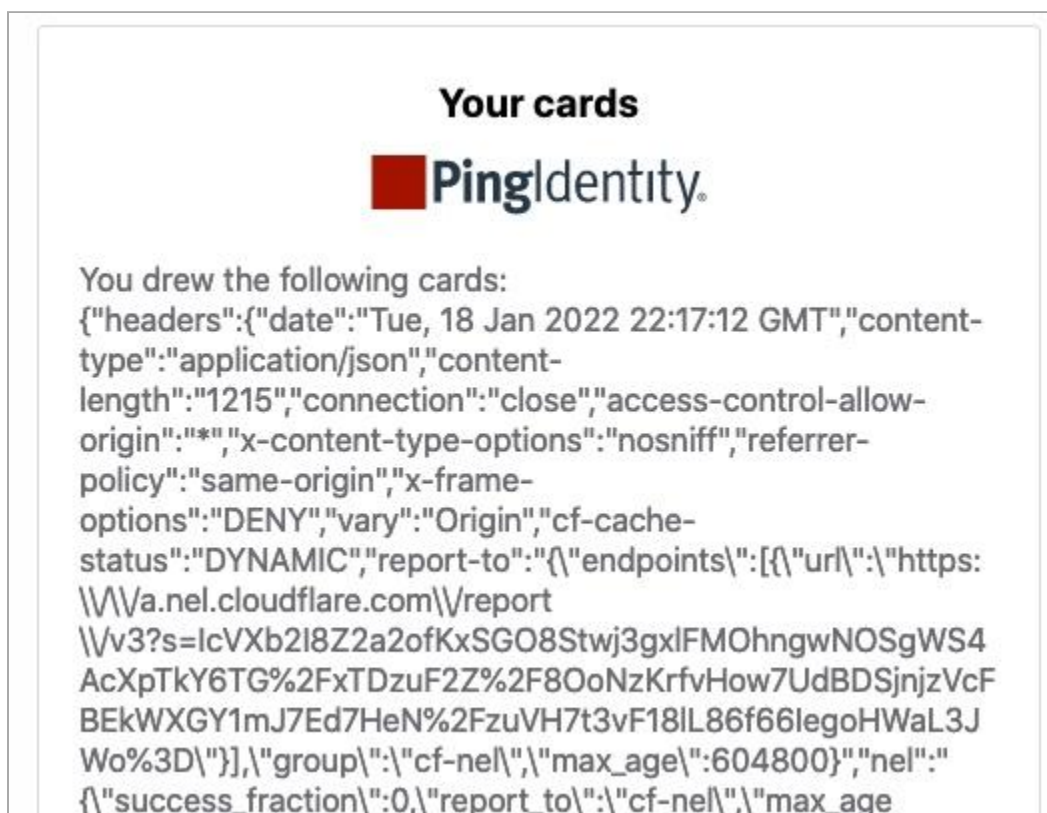
1. Following your **Make REST API Call** node, add an **HTTP** connector and select the **Custom HTML Message** capability.
2. In the **Message** field, click  and select the **rawResponse** variable from your **Make REST API Call** node by clicking **(+)**.



The screenshot shows a configuration window for a message. It has three main sections: 'Message', 'Message CSS', and 'Message Icon URL'. The 'Message' section contains a text area with the text 'You drew the following cards:' and a small icon button with a code symbol. The 'Message CSS' section contains an empty text area with a document icon button. The 'Message Icon URL' section is partially visible at the bottom.

3. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

The resulting message shows the card information, including the card value, suit, and an image. Copy this block of text, starting with `{"headers":`.... You'll use it in the next step.



3. Separate the raw response into usable values by defining a response schema:

1. In a browser, open the [Online JSON Schema Validator and Generator](#) tool. You'll use it to generate the JavaScript Object Notation (JSON) schema.
2. Paste the JSON response you copied into the **JSON** field. Click **Generate Schema From JSON**. Copy the output from the **JSON SCHEMA** field.



3. In your **Make REST API Call** node, paste the JSON schema into the **Success Response Schema** field.

Success Response Content Type ⓘ

Select or type your option and press enter... ▼

Success Response Schema ⓘ ⌵

```
1  {
2    "definitions": {},
3    "$schema": "http://json-schema.org/draft-07/schema#",
4    "$id": "https://example.com/object1642544708.json",
5    "title": "Root",
6    "type": "object",
7    "required": [
8      "headers",
9      "statusCode",
10     "body"
11   ],
```

4. Apply your changes, then go back to your **Custom HTML Message** node.
5. In your **Custom HTML Message** node, remove the **rawOutput** variable that you included in the **Message** field. Because you added a response schema, you can select specific parts of the JSON response to include in our message. Click **{}** and select the **cards** variable:

Message

You drew the following cards:

My Http Connector 

deck_id (string)

▼ cards (array of objects) ⓘ ⊕

code (string)

image (string)

▼ images (object) ⓘ ⊕

svg (string)

png (string)

Capabilities

Send Success JSON Response

Send a successful response.

Properties

returnRequestParameters toggleSwitch

Additional Fields in the Response selectNameValueListColumn

Use this section to add additional fields to the response

additionalFieldsName textField

Validate the additional properties toggleSwitch

The flow will fail if the validation is failed.

Signed Response toggleSwitch

Sign the response as JWT using your company's private keys. Signatures can be validated using JWKS public keys in the Company section.

Validity textField

Expiry time in milliseconds. Default is 86400000 (1 day).

Send Error JSON Response

Send an error response.

Properties

returnRequestParameters toggleSwitch

Additional Fields in the Response selectNameValueListColumn

Use this section to add additional fields to the response

additionalFieldsName textField

Signed Response toggleSwitch

Sign the response as JWT using your company's private keys. Signatures can be validated using JWKS public keys in the Company section.

Validity textField

Expiry time in milliseconds. Default is 86400000 (1 day).

Send Custom JSON Response

Send a custom response.

Properties

HTTP Body (JSON) textArea

This property needs to be a properly formatted JSON value. It can contain DaVinci parameters, which will be replaced at runtime. If you are using DaVinci parameters that are of type 'string', you will need to put string quotes around it.

httpStatusCode textField

httpHeaders textArea

Custom HTML Message

Creates a customizable HTML message.

Properties

messageTitle textField

Default: `Information`

message textArea

Message Icon URL textField

Message Icon Height (in pixels) textField

showFooter toggleSwitch

Display Name button

challenge textField

Enable Polling? toggleSwitch

pollInterval textField

Default: `2000`

pollRetries textField

Default: `60`

pollChallengeStatus toggleSwitch

showContinueButton toggleSwitch

reCAPTCHA v2 Verification

Verify that you are not a robot and proceed.

Properties

title textField

Form title.

bodyHeaderText textField

Form body title.

nextButtonText textField

Make REST API Call

Extend the functionality of the DaVinci platform by invoking any third party service.

Properties

URL textField required

HTTP Method dropDown required

Query Params keyValuePairList

Headers keyValuePairList

Body dropDown

Body Params keyValuePairList

raw codeEditor

Input your raw request body

Success Response Content Type dropdownWithCreate

Content Type of the response data. To apply output schema content type must be application/json

outputSchema codeEditor

Follow example for JSON schema.

Keep API output if the validation failed toggleSwitch

Error Response Content Type dropdownWithCreate

Content Type of the response data. To apply output schema content type must be application/json

outputSchemaError codeEditor

Follow example for JSON schema.

MTLS Support dropDown

Select the client certificate used to make outbound mTLS connections.

- None (Default)

Ignore TLS Errors toggleSwitch

When enabled, the connector ignores TLS errors. Use this for testing in non-production environments.

Timeout (ms) textField

Timeout for API call. Leave blank to not have timeout.

Output Schema

- output object
 - rawResponse object
 - statusCode integer
 - body array/object/number/string/boolean
 - headers array
 - item object

Custom HTML Template

Create an HTML page using this customizable template.

Properties

Content Source dropDown

Select the source of the HTML, CSS, & Script content

Template

HTML Template textArea

HTML CDN URL textField required

Enter the CDN URL that hosts the HTML you would like to use. The CDN hostname must be listed in the Trusted Sites under the connector settings.

CSS codeEditor

CSS CDN URL textField

Enter the CDN URL that hosts the CSS you would like to use. The CDN hostname must be listed in the Trusted Sites under the connector settings.

Script codeEditor

Write custom JavaScript. Caution: Custom code is for advanced users only. Before using custom code, review the security risks in the DaVinci documentation by searching for "Using custom code safely".

Script CDN URL textField

Enter the CDN URL that hosts the Javascript you would like to use. The CDN hostname must be listed in the Trusted Sites under the connector settings.

Use Recaptcha Verification toggleSwitch

Add sk-component skrecaptcha to use this feature.

Form validation rules validationRules

Rules to check to validate form inputs

inputSchema codeEditor

Follow example for JSON schema.

outputSchema codeEditor

Follow example for JSON schema.

formFieldsList formFieldsList challenge textField

Output Schema

- output object
 - formFieldsList object

Create QR Code for URL

Create a QR code that contains a URL.

Properties

URL textField required

Input Schema

- default object
 - properties object
 - customUrl string required minLength: 0 maxLength: 400
- Custom URL to create the QR Code

Input Example

```
{ "properties" :  
  { "customUrl" : "testurl.com" } }
```

Output Schema

- output object
 - generatedQr string

Continue Polling

Use this capability in conjunction with Polling in Custom HTTP capabilities.

Properties

Node ID of the UI node (Optional) textField

In advanced scenarios, it might be required to specify the Node ID of the UI node where polling in enabled. When a Node ID is not entered (default behavior), polling will continue on the current UI node.

Simulate Latency

Send a response with latency.

Properties

Delay Time (ms) textField

Time to wait for response to be sent in milliseconds. Default: 50

Default: 50

Return Success Response toggleSwitch

Return success or failure response

HTTP Body (JSON) textArea

This property needs to be a properly formatted JSON value. It can contain DaVinci parameters, which will be replaced at runtime. If you are using DaVinci parameters that are of type 'string', you will need to put string quotes around it.

Output Schema

- output object

HTTP Connector Release Notes

New features and improvements in the HTTP connector.

June 2023

The Make REST API Call capability now supports mTLS

New

The connector now supports mTLS. The **Make REST API Call** capability includes a new **MTLS Support** field to include keys configured in PingOne. You can view and create keys in PingOne by selecting the **Certificates and Keypairs** link under the field.

The default configuration is **None**, which will not use mTLS for API calls with the connector.

March 2023

Check boxes in HTML forms now return detailed values

Improved

The **Custom HTML Template** capability is often used to build a form, with check box elements such as the following:

```
<input type="checkbox" name="customerLocation" id ="customerLocation" value="loc256">
```

Previously, checkboxes would only return **true** or **false**, such as:

```
customerLocation=true
```

Now, when the checkbox is selected, it provides the **value** defined in the element properties, such as:

```
customerLocation=loc256
```

Other scenarios:

- When the checkbox is selected and a **value** isn't defined, it returns **true** or **on**, depending on the browser.
- When the checkbox is cleared, no value is returned.

 Note

This change could impact the function of your production flows.

Review any flows that use the **Custom HTML Template** capability to show a check box to the user. If so, check whether the flow relies on a **true** or **false** result from the check box and adapt it to accept **true** or **on**, a value string, or no value.

December 2022

"HTML Form" capabilities have been deprecated

Info

The following capabilities are not available on environments created after December 5, 2022:

- **HTML Form**
- **HTML Form with reCAPTCHA**

These capabilities are being replaced by a new drag-and-drop form builder in PingOne. In the PingOne admin console, navigate to **Experiences > Forms** to create forms that use your existing branding and themes.

The PingOne Forms connector lets you include these forms in your flows.

HYPR Connector

The HYPR connector lets you use HYPR for passwordless authentication in your PingOne DaVinci flow.

Setup

Resources

For more information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A configured HYPR environment
- A HYPR user account and mobile app to use for testing

Configuring the HYPR connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

To get your API URL and credentials, speak to a HYPR representative.

API URL

The API URL provided to you by HYPR.

Client ID

The client ID provided to you by HYPR.

Client secret

The client secret provided to you by HYPR.

Scope

The [OpenID Connect scopes](#) to send to HYPR to customize the verification process. Separate multiple scopes with a space, such as `openid email profile`.

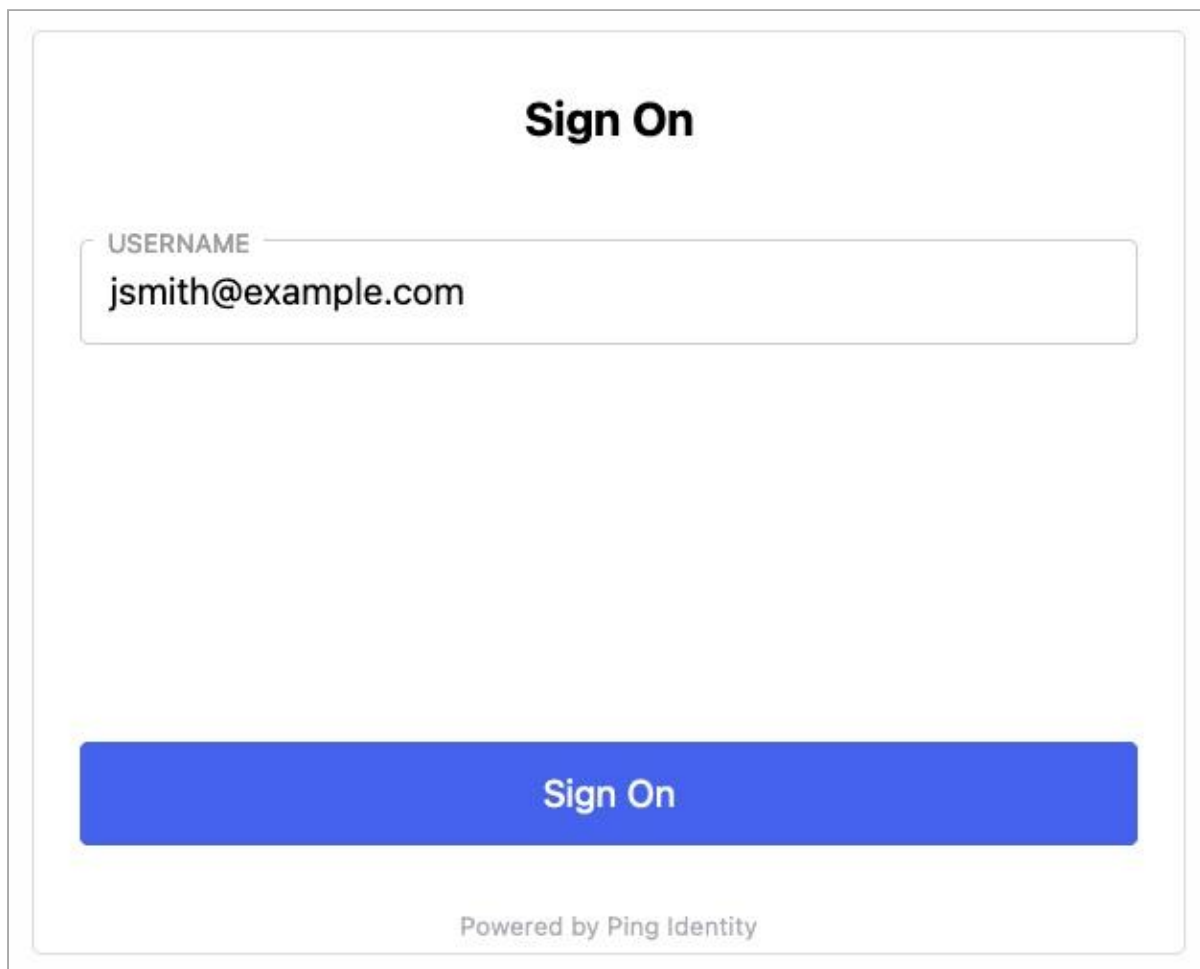
Using the connector in a flow

Authenticating users with HYPR



This flow asks the user to enter their username in an HTML form, redirects the user to HYPR for authentication, then shows the results on an HTML page.

1. Download the [HYPR Authentication](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the sign on form:



1. Select the **Sign On Form** node.
 2. (Optional) Customize the **Title** field.
 3. (Optional) Customize the **Next Button Text** field.
 4. Click **Apply**.
3. (Optional) Show a HYPR sign-on button rather than automatically redirecting the user to HYPR:

**Note**

This approach lets you include a HYPR sign-on button alongside other sign-on options in an **IDP Container** connector or as part of a custom HTML page using an [HTTP](#) connector.

1. Select the **HYPR** node.
2. Turn off **Skip Button Press**.
3. In the **Display Name** field, enter the button text, such as `Sign on with HYPR`.
4. (Optional) In the **CSS** field, add CSS to customize the appearance of the prompt.
5. (Optional) Turn on **Show Powered By** to display **Powered by Ping Identity** at the bottom of the prompt page.

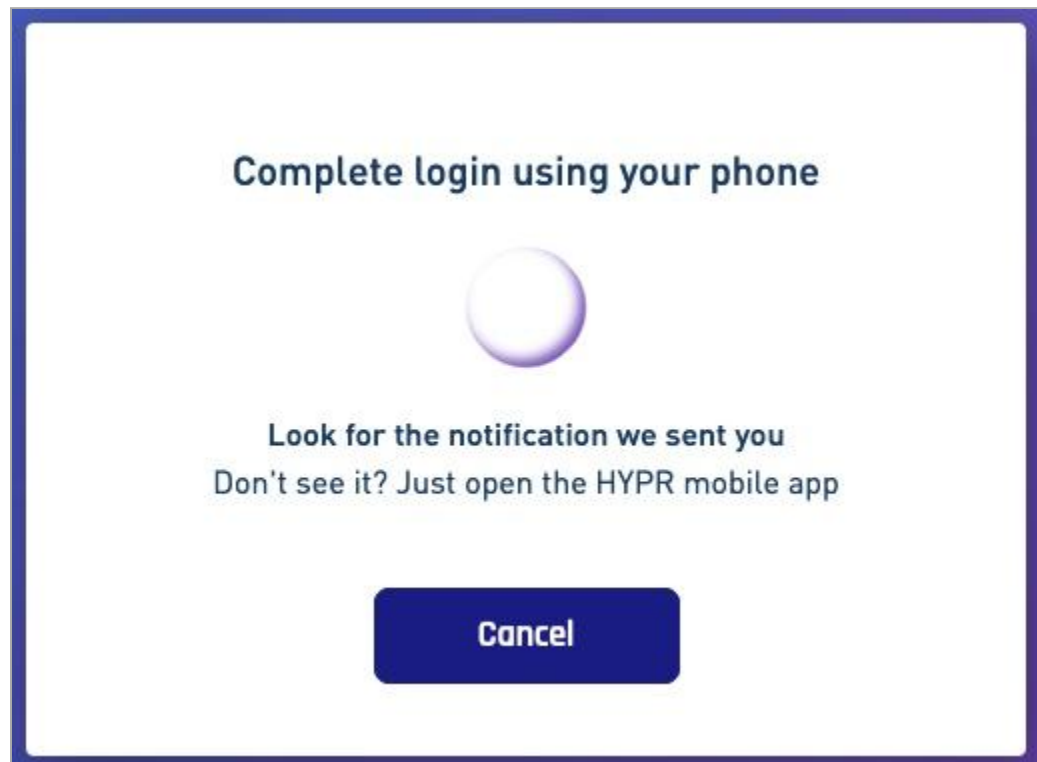
4. Test the flow:

1. Click **Save**, **Deploy**, then **Run**.
2. On the **Sign On** page, enter the username for your HYPR test user account. Click **Sign On**.

The browser redirects to the HYPR, which prompts you to authenticate.

A screenshot of the HYPR Sign In page. The page has a white background with a blue border. At the top center is the HYPR logo. Below the logo is a horizontal line. Underneath the line is a text input field containing the email address 'jsmith@example.com'. Below the input field is a blue rectangular button with the text 'Sign In' in white.

3. Complete the MFA process with HYPR.



HYPR shows a success message and then redirects the browser back to DaVinci.

Your **Custom HTML Message** shows the complete response from HYPR.



Capabilities

Authenticate

Properties

Username textField

The username of the authenticating user.

Display Name button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - username string
 - clientId string required
 - clientSecret string required
 - scope string required
 - apiUrl string required

Output Schema

- output object
 - statusCode integer
 - rawResponse object
 - tokenResponse object
 - id_token string
 - access_token string
 - token_type string
 - expires_in number

ID DataWeb Connector

The ID DataWeb connector lets you use ID DataWeb for identity verification in your PingOne DaVinci flow.

The connector allows you to direct users to ID DataWeb's AXN Verify service where they can enter their information for identity verification. By mapping attributes from your DaVinci flow, you can pre-populate some of the information requested in the identity verification process. After ID DataWeb verifies the user's identity, it sends the results to DaVinci where you can branch your flow accordingly.

Setup

Resources

For information and setup help, see the following:

- ID DataWeb documentation:
 - [Getting Started](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A configured ID DataWeb environment

- Your ID DataWeb client ID and secret

Configuring the ID DataWeb connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Redirect URL

This URL continues the DaVinci flow when ID DataWeb is finished. Add this URL to the **Redirect URL(s)** list on the **Basic Info** tab of your ID DataWeb verification service configuration. For help, ask an ID DataWeb representative.

Client ID

The client ID provided to you by ID DataWeb. This allows DaVinci to communicate with ID DataWeb.

Client Secret

The client secret provided to you by ID DataWeb.

Scope

Scopes customize the verification experience and determine the information provided by ID DataWeb. For help, see [Scopes](#) in the ID DataWeb documentation and speak to an ID DataWeb representative.

Separate multiple scopes with a space. For example, `openid country.US`.

AXN Federated Gateway Base URL

The ID DataWeb AXN Federated Gateway to use. Select the production or preproduction server, or use your custom base URL.

- Production
 - DaVinci uses the live Gateway.

- Preproduction
 - DaVinci uses the preproduction Gateway. Use this for testing.
- Custom Base URL

DaVinci uses the Gateway address that you enter in the **[.uicontrol]Custom Gateway Base URL**** field. Use this if your organization has a custom domain or vanity URL configured for ID DataWeb.

Custom Gateway Base URL

When **AXN Federated Gateway Base URL** is set to **Custom Gateway Base URL**, this field determines the AXN Federated Gateway address. Enter your custom Gateway URL, such as <https://mycompany.com/preprod-axn/axn/oauth2>.

Data protection

Determines how DaVinci protects the user data it sends to ID DataWeb.

- Signed
 - DaVinci sends user data in a signed JSON Web Token (JWT). ID DataWeb can detect whether the data was modified in transit.
- Encrypted
 - DaVinci sends the user data in an encrypted JWT. Only ID DataWeb can read the data. Select this if you want to use a public encryption key provided by ID DataWeb.

Public Encryption Key

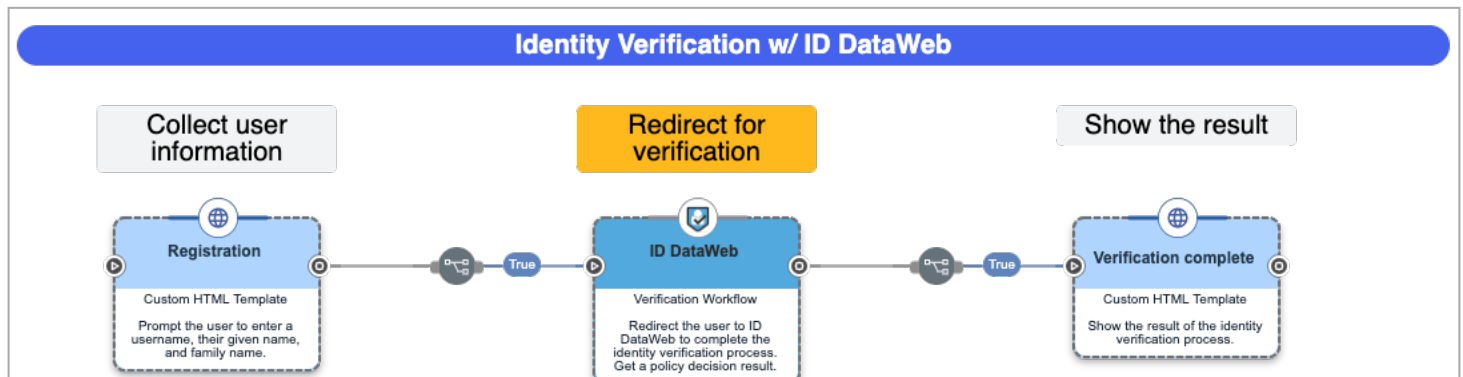
When **Data Protection** is set to **Encrypted**, DaVinci uses this key to encrypt the user data. Enter the a public encryption key provided by ID DataWeb.

Application Redirect URL

Your application's redirect URL, such as <http://app.yourorganization.com/>. Enter this URL if you embed the DaVinci widget in your application. This allows DaVinci to redirect the browser back to your application.

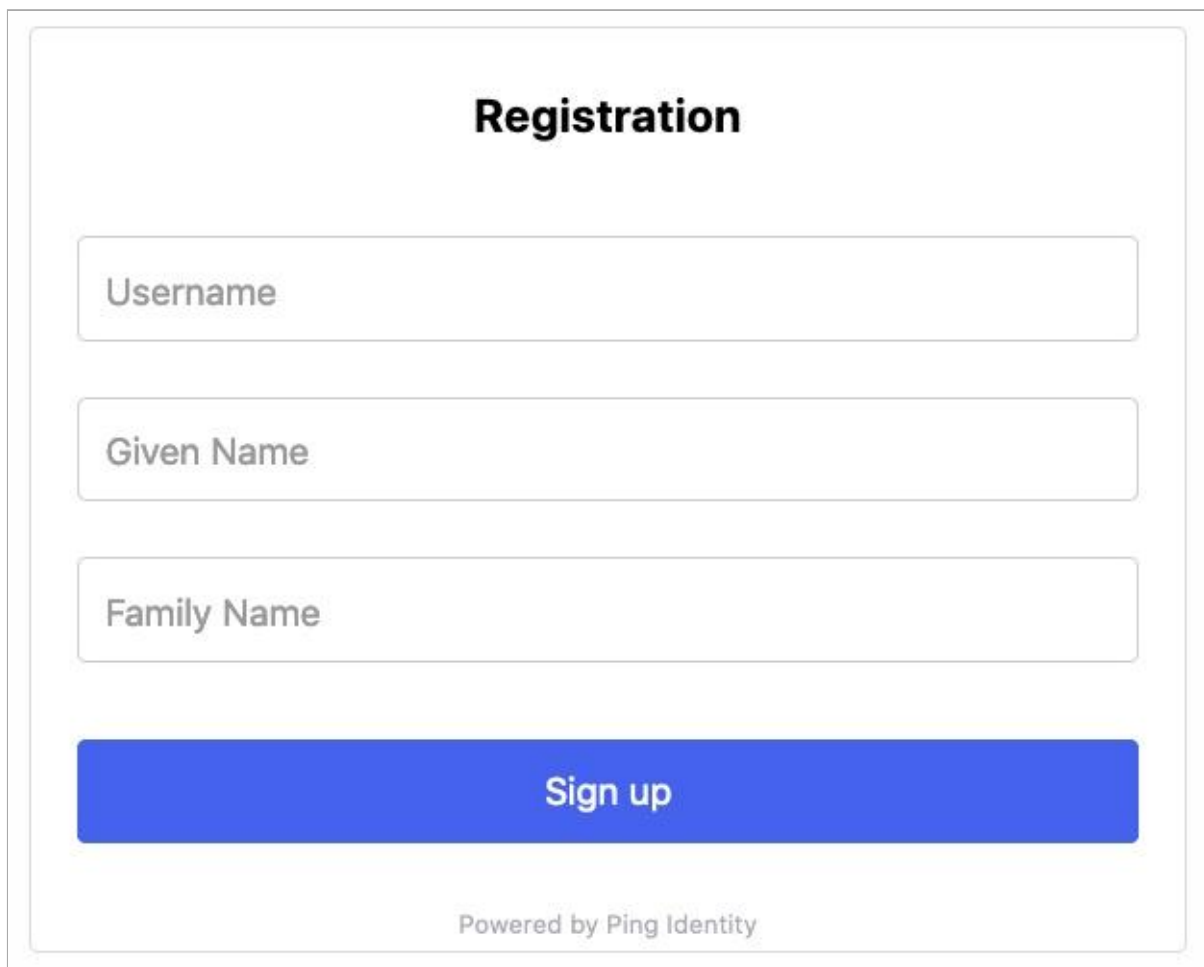
Using the connector in a flow

Verifying a user by redirecting them to ID DataWeb



In this flow, an HTML form gathers user data, then the connector directs the browser to ID DataWeb. When the user completes the identity verification process, a simple HTML message shows the result.

1. Download the [ID DataWeb Identity Verification](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Download the flow template and use it to create a new flow. For help, see [Using DaVinci flow templates](#).
3. (Optional) Customize the registration form:

A registration form titled "Registration" in bold black text. It contains three input fields: "Username", "Given Name", and "Family Name", each with a light gray border and rounded corners. Below these fields is a large blue button with the text "Sign up" in white. At the bottom of the form, it says "Powered by Ping Identity" in a smaller, gray font.

1. Select the **Registration** node.
 2. (Optional) Customize the **Title** field.
 3. (Optional) In the **Fields List** section, customize the user data fields by clicking **Add** to add a new field or clicking **Edit** to remove fields.
 4. (Optional) Customize the **Next Button Text** field.
 5. Click **Apply**.
4. If you customized the user data fields in the **Registration** node, update the attribute mappings for ID DataWeb:
1. Select the **ID DataWeb** node.
 2. In the **PII Parameters** section, find the ID DataWeb parameter in the **Key** column, then click **{}** in the **Value** column and select the related variable from your **HTML Form** node.

Subject ⓘ

PII Parameters ⓘ

Fields

Key	Value
fname	
mname	

3. Click **Apply**.

5. Test the flow:

1. Click **Save**, **Deploy**, then **Try Flow**.
2. On the **Registration** page, enter a username, given name, and family name. Click **Sign Up**.
3. Complete the ID DataWeb verification process.

Notice that some of the fields are already populated, such as first name and last name.



Identity Proofing

First, please fill out your personal mobile phone number (in your possession), and click confirm.

Full Name *

Address *

Enter address manually

4. On the **Verification complete** page, see the verification result.

Verification complete



Verification result: approve

Powered by Ping Identity

Capabilities

Verification Workflow

Properties

Subject textField required

Username/friendly reference to the transaction.

PII Parameters keyValuePairList

Provide ID DataWeb with user information for verification.

Display Name button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - subject string required
 - piiParams array
 - clientId string required
 - clientSecret string required
 - scope string required
 - gatewayBaseUrl string required
 - customGatewayBaseUrl string
 - dataProtection string required
 - publicEncryptionKey string

Output Schema

- output object
 - statusCode integer
 - rawResponse object
 - policyDecision string
 - tokenResponse object
 - id_token string
 - access_token string
 - token_type string
 - expires_in number

J-L



Jira Connector

The Jira connector lets you manage issues and trigger Jira workflows in your PingOne DaVinci flow.

LDAP

LDAP Connector

The LDAP connector for PingOne DaVinci lets you gain access to entries in an LDAP directory to be used in your PingOne DaVinci flow.



LexisNexis Connector

The LexisNexis connector lets you create a PingOne DaVinci flow that performs risk assessments with ThreatMetrix and other Dynamic Decision Platform services, sends an OTP, and prompts users with security questions.

The davincci logo, featuring a stylized orange and red graphic above the word "davincci" in a bold, dark blue sans-serif font.

davincci

Location Policy Connector

The Location Policy connector lets you check a user's IP and geographic location in your PingOne DaVinci flow.

Jira Connector

The Jira connector lets you manage issues and trigger Jira workflows in your PingOne DaVinci flow.

You can use the Jira connector to:

- Search for issues in the Jira workflow
- Receive information about new and updated issues by listening for a webhook
- Set up a custom application programming interface (API) call to suit your needs

Setup

Resources

For information and setup help, see the following documentation:

- Jira documentation:
 - [Create an API token](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a Jira license.

Setting up Jira

Follow the instructions in [Create an API token](#).

Setting up the Jira connector configuration

In DaVinci, add a **Jira** connection. For help, see [Adding a connector](#).

Connector configuration

Base URL

The base URL for your Jira Cloud API. For example, <https://id.atlassian.com>.

Email Address

Your Jira administrator email address.

Jira API token

The Jira API token that you created in [Setting up Jira](#), such as "bACbrdOf3q6vLCLGMSbxDDDD".

Using the connector in a flow

Managing Jira issues

The connector has several capabilities that allow you to manage issues in Jira:

- **Create an Issue**
- **Get Issue Details**
- **Delete an Issue**
- **Assign an Issue**
- **Update an Existing Issue**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

For capabilities that have a **Query Parameters** section, you can add any query parameters that are supported by the Jira API. For help, see the [Jira Cloud platform REST API documentation](#).

Searching for Jira issues

You can use the connector to search for Jira issues using the Jira Query Language (JQL).

The **JQL Query** field in the **Search for Issues Using JQL** capability accepts an advanced search string. For help, see [Use advanced search with Jira Query Language \(JQL\)](#) in the Jira documentation.

Other properties let you control the type of information you get about the issues.

If you expect to get more results than the **Maximum Number of Results** you define, you can run the query several times with a different **Starting Result Number** to paginate the results.

Creating a custom API call

If you want to do something not supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Create an Issue

Create an issue in JIRA.

Properties

Project dropDown required

The Jira project to create the issue in. For a dynamic value, select Use Project Key and enter a value in the Project Key field.

- Use Project Key (Default)

Project Key textField required

The Jira project to create the issue in, such as "PROJ".

Summary textField required

The issue summary, such as "Fix development workflow".

Issue Type dropDown required

The type of issue to create.

- Story
- Task
- Sub-task
- Bug
- Epic

Parent Issue ID textField

The ID of an existing issue, such as "PROJ-10". When this value is provided, the new issue will be created as a sub-task of the parent issue.

Components textFieldArrayView

The ID of the component to associate with the issue, such as "10000".

Description textField

The issue description, such as "Please fix the following development workflow issue..."

Reporter dropDown

The person reporting the issue. For a dynamic value, select Use Reporter ID and enter a value in the Reporter ID field.

- Leave Blank (Default)
- Use Reporter ID

Reporter ID textField required

The ID of the reporter, such as "5b10a2844c20165700ede21g".

Fix Versions textFieldArrayView

The ID of the fix version to associate with the issue, such as "10001". Type an ID and press Enter to add it.

Versions textFieldArrayView

The ID of the version to associate with the issue, such as "10001". Type an ID and press Enter to add it.

***Due Date* textField**

The due date for the issue, formatted as "2022-01-30".

***Assignee* dropDown**

The person to assign the issue to. For a dynamic value, select Use Assignee ID and enter a value in the Assignee ID field.

- Leave Blank (Default)
- Use Assignee ID

***Assignee ID* textField required**

The ID of the assignee, such as "5b10a2844c20165700ede21g".

***Priority* textField**

The priority for the issue, such as "3".

***Labels* textFieldArrayView**

The labels to associate with the issue. Type a label and press enter to add it.

***Query Parameters* keyValuePairList**

Define additional query parameters to send to Jira. For help, see the Jira Cloud platform REST API documentation.

***Other Attributes* variableInputList**

Add other attributes and their values. Will overwrite attributes in General tab if key is the same.

Input Schema

default object

apiUrl string required

email string required

apiKey string required

project string required

projectKey string

summary string required

issueType string required

parent string

components array

description string

reporter string

reporterId string

fixVersions array

versions array

dueDate string

assignee string

assigneeId string

priority string

labels array

items array

0 string

queryParams array

otherAttributes array

Output Schema

output object

headers object

statusCode integer

rawResponse object

Get Issue Details

Get details for an issue by providing the issue ID.

Properties

Issue ID textField required

The ID of the issue, such as "PROJ-1".

Query Parameters keyValuePairList

Define additional query parameters to send to Jira. For help, see the Jira Cloud platform REST API documentation.

Input Schema

default object

apiUrl string required

email string required

apiKey string required

issueld string required

queryParams array

Output Schema

output object

headers object

statusCode integer

rawResponse object

Update an Issue

Update an issue in JIRA.

Properties

Issue ID textField required

The ID of the issue, such as "PROJ-1".

Summary textField

The issue summary, such as "Fix development workflow".

Issue Type dropDown

The updated issue type.

- Story
- Task
- Sub-task
- Bug
- Epic

Parent Issue ID textField

The ID of an existing issue, such as "PROJ-10". When this value is provided, the new issue will be created as a sub-task of the parent issue.

Components textFieldArrayView

The ID of the component to associate with the issue, such as "10000".

Description textField

The issue description, such as "Please fix the following development workflow issue..."

Reporter dropDown

The person reporting the issue. For a dynamic value, select Use Reporter ID and enter a value in the Reporter ID field.

- Leave Blank (Default)
- Use Reporter ID

Reporter ID textField required

The ID of the reporter, such as "5b10a2844c20165700ede21g".

Fix Versions textFieldArrayView

The ID of the fix version to associate with the issue, such as "10001". Type an ID and press Enter to add it.

Versions textFieldArrayView

The ID of the version to associate with the issue, such as "10001". Type an ID and press Enter to add it.

Due Date textField

The due date for the issue, formatted as "2022-01-30".

Assignee dropDown

The person to assign the issue to. For a dynamic value, select Use Assignee ID and enter a value in the Assignee ID field.

- Leave Blank (Default)
- Use Assignee ID

Assignee ID textField required

The ID of the assignee, such as "5b10a2844c20165700ede21g".

Priority textField

The priority for the issue, such as "3".

Labels textFieldArrayView

The labels to associate with the issue. Type a label and press enter to add it.

Query Parameters keyValueList

Define additional query parameters to send to Jira. For help, see the Jira Cloud platform REST API documentation.

Other Attributes variableInputList

Add other attributes and their values. Will overwrite attributes in General tab if key is the same.

Input Schema

default object

apiUrl string required

email string required

apiKey string required

issueld string required

updateSummary string

parent string

components array

updateIssueType string

description string

reporter string

reporterId string

fixVersions array

versions array

dueDate string

assignee string

assigneeld string

priority string

labels array

items array

0 string

queryParams array

otherAttributes array

Output Schema

output object

headers object

statusCode integer

Delete an Issue

Delete an issue in the project.

Properties

Issue ID textField required

The ID of the issue, such as "PROJ-1".

Query Parameters keyValueList

Define additional query parameters to send to Jira. For help, see the Jira Cloud platform REST API documentation.

Input Schema

default object

apiUrl string required

email string required

apiKey string required

issueld string required

queryParams array

Output Schema

output object

headers object

statusCode integer

Assign an Issue

Assign an issue to an account.

Properties

Assignee dropDown

The person to assign the issue to. For a dynamic value, select Use Assignee ID and enter a value in the Assignee ID field.

- Leave Blank (Default)
- Use Assignee ID

Assignee ID textField required

The ID of the assignee, such as "5b10a2844c20165700ede21g".

Issue ID textField required

The ID of the issue, such as "PROJ-1".

Input Schema

default object

apiUrl string required

email string required

apiKey string required

assignee string

assigneeld string

issueld string required

Output Schema

output object

headers object

statusCode integer

Search for Issues Using JQL

Search for issues using Jira Query Language.

Properties

JQL Query textField

The JQL query used to search for issues, such as "project=SysAdmin AND assignee=jsmith". For help, see documentation for the Jira Query Language.

Starting Result Number textField

The index number of the first item to return in the results. For example, "101" will return the maximum number of results starting with result number 101. Use this to get pages of results for queries that return more than the maximum number of results.

Maximum Number of Results textField

The maximum number of results to return from the query. Use with Starting Result Number to get pages of results for queries that return more than the maximum number of results.

Fields textFieldArrayView

The fields to get for each issue returned in the results, such as "assignee" or "comment". Type a field name and press enter to add it.

Identify Fields with Keys toggleSwitch

Enable this when the "Fields" list uses keys, rather than IDs, to identify fields.

Query Validation dropDown

The method to use to validate the JQL query.

- Strict (Default)
- Warn

- None

***Expanded Information* textFieldArrayView**

Additional information to get for the issues returned in the results, such as "names", "schema", or "changelog". For help, see "Search for issues with JQL (POST)" in the Jira Cloud platform REST API documentation.

***Properties* textFieldArrayView**

The app or entity properties to get for each issue returned in the results. Type a property name and press enter to add it, to a maximum of five properties.

Input Schema

***default* object**

***apiUrl* string required**

***email* string required**

***apiKey* string required**

***jql* string required**

***startAt* string**

***maxResults* string**

***fields* array**

***validateQuery* string**

***expand* array**

***searchProperties* array maxItems: 5**

***fieldsByKeys* boolean**

Output Schema

***output* object**

***headers* object**

***statusCode* integer**

***rawResponse* object**

Make Custom API Call

Define and invoke custom call to the Atlassian Jira REST API.

Properties

***Endpoint* textField required**

The Jira API endpoint, such as /rest/api/3/search.

***HTTP Method* dropDown required**

The HTTP method of the API call.

- GET
- POST
- PUT

- DELETE

Query Parameters keyValuePairList

Define additional query parameters to send to Jira. For help, see the Jira Cloud platform REST API documentation.

Additional Headers keyValuePairList

Additional headers for the request, connector automatically adds 'Authorization' and 'Content-Type' headers.

Body codeEditor

The body of the API call.

Input Schema

default object

apiUrl string required

email string required

apiKey string required

endpoint string required

method string required

customQueryParams array

headers array

bodyData object

Output Schema

output object

headers object

statusCode integer

rawResponse object

LDAP Connector

The Lightweight Directory Access Protocol (LDAP) connector for PingOne DaVinci lets you gain access to entries in an LDAP directory to be used in your PingOne DaVinci flow.

You can use the LDAP connector to:

- Create a new entry in your LDAP store.
- Reset a user's password, including generating a new password.
- Update a user or group's profile.
- Delete an entry from your LDAP store.
- Search for and view a user's group membership.

Setup

Resources

For information and setup help, see the following documentation:

- PingOne Gateway documentation:
 - [Introduction to Gateways](#)
 - Documentation for your LDAP directory, such as PingDirectory:
 - [Introduction to PingDirectory Server](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- An LDAP directory store, such as PingDirectory:
 - For more information, see [Supported directories](#).
- Your LDAP directory store credentials
- A PingOne LDAP Gateway installation
- A worker application for userless administration:
 - For more information, see the [Worker application](#) documentation.

Setting up the LDAP connector

Review the prerequisites in [Before you begin](#), and then follow the gateway set up instructions in [Overview](#).

Setting up the connector configuration

In DaVinci, add an LDAP connector. For help, see [Adding a connector](#).

Connector settings

Environment ID

Your PingOne Environment ID. In PingOne, go to **Environment > Properties**.

Client ID

The **Client ID** for your PingOne Worker application. In PingOne, go to **Applications > Your application > Configuration**.

Client secret

The **Client secret** for your PingOne Worker application. In PingOne, go to **Applications > Your application > Configuration**.

Region

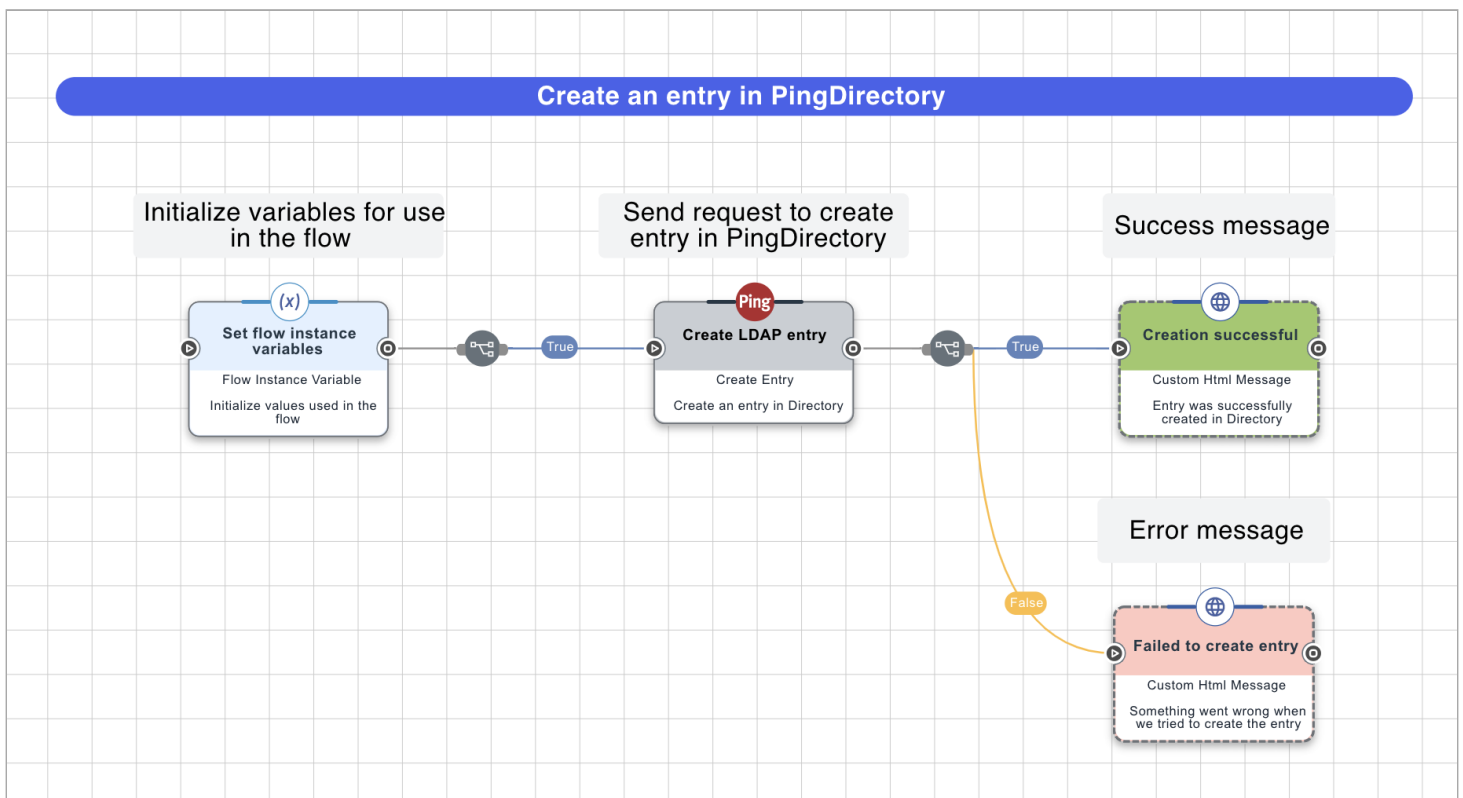
Your PingOne environment region. In PingOne, go to **Environment > Properties**.

Using the connector in a flow

Managing entries in an LDAP directory store

The connector has several capabilities that allow you to manage entries in your LDAP directory store:

- Create entry
- Modify DN
- Search entries
- Delete entry



This flow allows the user to create a new entry in any LDAP directory.

1. Customize the entry-creation parameters:

1. Select the **Create LDAP entry** node.
2. In the **DN** field, customize the distinguished name of the new entry.
3. In the **Attributes** section, click the **Add** button. In the **Variable Name** field, enter `objectClass`, and in the **Value** field, enter the name of the new entry's objectClass according to the directory schema.

Note

The objectClass attribute value differs depending on the directory. For example, a new PingDirectory entry is an instance of the `inetOrgPerson` objectClass, while a new Active Directory (AD) entry is an instance of the `user` objectClass.

4. In the **Attributes** section, click the **Add** button and populate the **Variable Name** and **Value** fields with information on the entry's username.

Note

The **Variable Name** differs depending on the directory. For example, a new PingDirectory entry's username requires a variable name of `uid`, while a new AD entry's username requires a variable name of `sAMAccountName`.

5. (Optional) In the **Attributes** section, add other attributes as permitted by the new entry's objectClass.
6. In the **Perform Operation As** list, select the user account performing the entry creation.

7. Click **Apply**.

Managing passwords in an LDAP directory store

The connector has several capabilities that allow you to manage different entries' passwords in your LDAP directory store:

- **Generate password**
- **Reset password**
- **Check password**

No special flow configuration is needed. Add the capability that you want and populate its properties according to the help text.

Managing attributes in an LDAP directory store

The connector has several capabilities that allow you to manage different entries' attributes in your LDAP directory store:

- **Modify attributes**
- **Replace attributes**

No special flow configuration is needed. Add the capability that you want and populate its properties according to the help text.

Capabilities

LDAP Search

Execute ldap/ad searches

Properties

baseDN textField
ldapScope dropDown
ldapFilter textField
ldapAttributes textFieldArrayView

Output Schema

- output object

LDAP Add

Add entry to your LDAP Directory

Properties

DN textField

New User Entry Fields selectNameValueListColumn

Use this section to add additional fields to the response

Output Schema

- output object

LDAP Delete

Delete entry from your LDAP Directory

Properties

DN textField

Output Schema

- output object

LexisNexis Connector

The LexisNexis connector lets you create a PingOne DaVinci flow that performs risk assessments with ThreatMetrix and other Dynamic Decision Platform services, sends a one-time passcode (OTP), and prompts users with security questions.

You can use the LexisNexis connector to:

- Get risk assessments from ThreatMetrix with the LexisNexis Dynamic Decision Platform
- Use the LexisNexis Dynamic Decision Platform to access services defined by your LexisNexis policy
- Get insights into identity data associated with phone numbers and email addresses
- Authenticate users with OTPs

- Authenticate users with security questions

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A LexisNexis account
- Credentials and access details for the LexisNexis services that you want to use

Configuring LexisNexis

To configure the LexisNexis connector in DaVinci, you will need to create an API Key in DaVinci.

To create an API Key:

1. From the **Applications** tab, click **Add Application**.
2. Enter a name for the application in the **Name** field, then click **Create**.
3. Find the application you created and click **Edit**.
4. From the **General** tab, copy the **API Key**.

Configuring the LexisNexis connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

API URL

The API URL to target. For a custom value, select **Use Custom API URL** and enter a value in the **Custom API URL** field.

Custom API URL

The API URL to target, such as <https://h.online-metrix.net>.

Organization ID

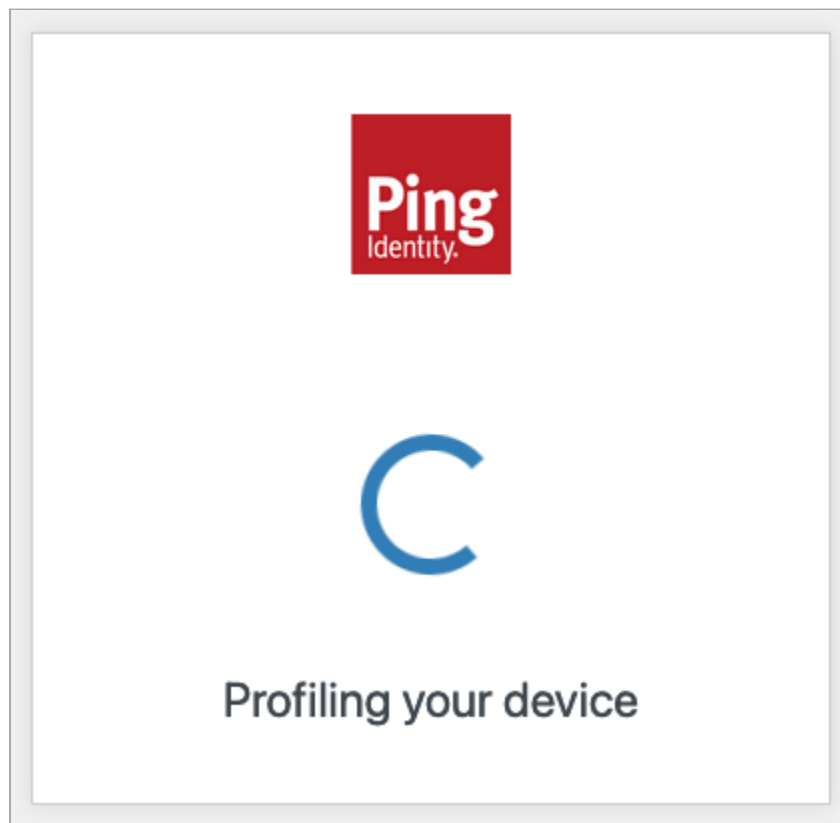
Your LexisNexis organization ID, such as `4en6112s`.

API Key

Your LexisNexis API key, such as `3x9ywfs26rm1zv1`.

Using the connector in a flow

Get a risk assessment for ThreatMetrix



Use the **Get Device Profile** capability followed by the **Dynamic Decision Platform (DDP)** capability to point to a ThreatMetrix policy name. Use the `review_status` and `risk_rating` results from the output to branch your flow.

The **Get Device Profile** capability presents an interim spinner page while gathering the device profile.

 Note

On the **UI** tab, you can customize the appearance of the spinner page with the **HTML**, **CSS**, and **Script** fields.

Dynamic Decision Platform (DDP)

You can use the **Dynamic Decision Platform (DDP)** to access services defined by your LexisNexis policy.

1. From the **General** tab, select a **Query Type**.

 Note

Session Query requires a session ID obtained through the **Get Device Profile** capability and is used for the device-centric operations. You must provide at least one **Additional Parameter**.

Attribute Query requires personally identifiable information (PII) to provide a risk rating and is used to trigger the DDP Rules Engine with a policy. You must provide at least one **Additional Parameter**.

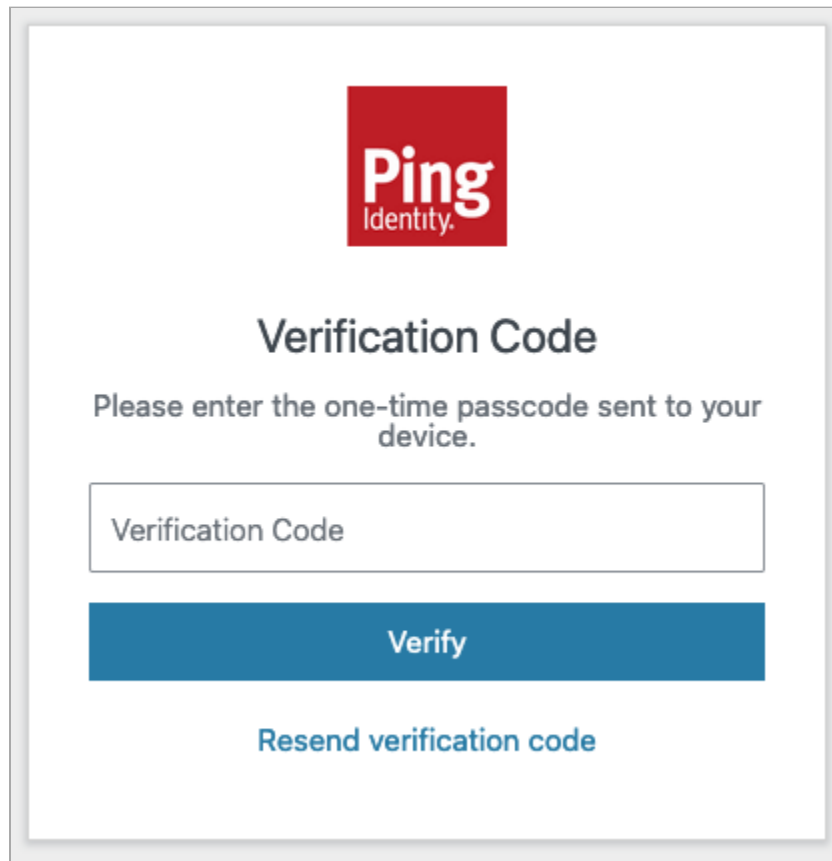
2. Select a **Service Type**.
3. (Optional) Select an **Event Type**.
4. In the **Policy** field, type the name of the Dynamic Decision Platform policy to use for this capability.

 Note

The policy name entered in the **Policy** field must match exactly with the policy name defined in LexisNexis. To modify a policy, reach out to LexisNexis support.

5. Define any additional parameters to send to LexisNexis, such as user attributes.
6. Click **Apply**.

Prompt a user for a one-time passcode

A screenshot of a web-based verification prompt from Ping Identity. At the top is the Ping Identity logo, which consists of a red square with the word "Ping" in white and "Identity." in smaller white text below it. Below the logo, the title "Verification Code" is centered in a large, bold, dark grey font. Underneath the title, a message in a smaller dark grey font reads "Please enter the one-time passcode sent to your device." Below this message is a white rectangular input field with a thin grey border, containing the placeholder text "Verification Code". Under the input field is a solid blue rectangular button with the word "Verify" in white text. At the bottom of the prompt, the text "Resend verification code" is displayed in a blue, clickable font.

You can use the **OTP Prompt** capability to prompt users for a one-time passcode. On the **UI** tab, you can customize the appearance of the prompt with the **HTML**, **CSS**, and **Script** fields.

Note

The **`\${ExpirePeriod}`** variable in the **Email Body** and **SMS Body** uses the policy default instead of the value from the **OTP Timeout** field.

Prompt a user with security questions



Identity Verification

Please select the correct responses to continue.

Which of the following street addresses in Chicago have you ever lived at or been associated with?

- ☐ 118 East 45th Street
- ☐ 3538 South Emerald Avenue
- ☐ 4832 West Saint Paul Avenue
- ☐ 837 North Leclaire Avenue
- ☐ None of the above or I am not familiar with this property

Which of the following professional licenses have you ever held?

- ☐ Acupuncturist
- ☐ Physical Therapist
- ☐ Prov. Marriage & Family Therap
- ☐ Speech-language Pathologist
- ☐ None of the above

Which of the following corporations have you ever been associated with?

- ☐ Audio Profiles
- ☐ Barefoot Realty Resort Properties
- ☐ C Stores
- ☐ Com Global Sys
- ☐ None of the above

Submit Answers

You can use the **InstantID Q&A** capability to prompt a user with security questions. On the **UI** tab, you can customize the appearance of the prompt with the **HTML**, **CSS**, and **Script** fields.

Handling unknown sessions

Unknown sessions occur when the **Get Device Profile** capability tries to get a risk evaluation due to a device profiling failure, therefore causing LexisNexis to not return a review status. Device profiling can be blocked for various reasons, including ad blockers and browsers (such as Firefox). DaVinci will attempt to fingerprint the user's device until the time limit defined by the **Timeout** property is reached.

The **Get Device Profile** capability allows the end user to continue through the flow whether the device profiling succeeded or failed. The **Review Status for Unknown Sessions** property in the **Dynamic Decision Policy** capability allows you to pre-define how unknown sessions are treated. With this property, you assign a static review status, such as **Pass**, **Review**, **Challenge**, or **Reject**, allowing users with unknown sessions to proceed through the flow following the same branching rules as users that received a realtime review status from LexisNexis.

Capabilities

ThreatMetrix: Send Device Profile

Run the device profiling script, submit the profile, and get a session ID.

Properties

Initialization Loading text textField

Input Schema

- default object
 - properties object
 - javascriptCdnUrl string required
 - orgId string required

Output Schema

- output object
 - sessionId string

ThreatMetrix: Get Profiling URL

Get a unique URL and session ID to use for device profiling in a custom page.

Input Schema

- default object
 - properties object
 - javascriptCdnUrl string required
 - orgId string required

Output Schema

- output object
 - cdnUrl string
 - sessionId string

Instant Verify International

Use LexisNexis DDP for multi-faceted fraud and risk assessment.

Properties

Policy textField required

The name of your policy in the Dynamic Decision Platform (DDP).

Service Type dropDown

Restricts which output fields are returned based on the level of access that a customer has. The service type is linked to your API key.

- Basic
- Session Policy
- Device
- DID
- IP
- Session
- All (Default)
- 3ds

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Account Email textField

The primary account holder's email address.

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

Account Work Phone textField

The primary account holder's work telephone number. This field is not an entity.

Date of Birth textField

The primary account holder's date of birth, formatted as YYYYMMDD.

Gender textField

The primary account holder's gender.

National ID Number textField***National ID Type dropDown***

The Type of National Id that will be used for verification.

- US_SSN
- US_SSN_HASH
- US_SSN4
- US_SSN_FIRST5
- BR_CPF
- MX_CURP
- CO_CEDULA

Driver License Number textField

The primary account holder's driver license number.

Driver License Issuer textField

Primary account driver license issuer

Routing Address textField

The primary account holder's routing address.

Routing Standard textField

The primary account holder's routing standard.

Account Number textField

The primary account holder's account number.

Passport Number textField

The primary account holder's passport number.

Passport machine Readable Line 1 textField

The primary account holder's passport information in machine-readable format, line 1.

Passport machine Readable Line 2 textField

The primary account holder's passport information in machine-readable format, line 2.

Passport Expiration Date textField

The primary account holder's passport expiration date, formatted as YYYY-MM-DD.

Passport Country textField

The primary account holder's passport country, in ISO 3166-1 alpha-2 format, such as "US".

Transaction ID textField

The identifier used by the merchant to identify the transaction, such as a purchase order number.

Credit Card Number textField

The credit card number used in the transaction.

Online TLD textField

The description of the online TLD handle source. Used to prevent collisions between different online TLD handles. For help determining the correct online TLD for the ID you wish to send with your query, speak to a LexisNexis representative. This field is required if the Online TLD Handle field is populated.

Online TLD Handle textField

A unique third-party identifier, such as a LexID or a DUNS Number. Used for rule creation and investigation. This field is required if the Online TLD field is populated.

Line of Business textField

The line of business specified by the customer.

Application Name textField

The name of the application sending the event.

Shipping Account Holder's Street Address 1 textField

The shipping account holder's street address, line 1.

Shipping Account Holder's Street Address 2 textField

The shipping account holder's street address, line 2.

Shipping Account Holder's City textField

The shipping account holder's city.

Shipping Account Holder's State textField

The shipping account holder's state.

Shipping Account Holder's ZIP or Postal Code textField

The shipping account holder's ZIP or postal code.

Shipping Account Holder's Country textField

The shipping account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Routing Number textField

The routing number for the account. When using this attribute in a Condition/Expression Condition rule or Expression variable, the value will be treated as a string if quotes are used to enclose it and as a number if no quotes are used.

Transaction Amount textField

The numeric currency amount. If a decimal is used, exactly two digits must follow it.

Transaction Currency textField

The currency used for the transaction, formatted in ISO 4217 currency code, such as "USD". This field is required when Transaction Amount is populated.

Account Login textField

A unique identifier for the customer, such as a username or account ID. Used to check whether the customer is on a watch list.

Password textField

The password associated with the Account Login. This is hashed and sent to LexisNexis. Used to check whether the customer is on a watch list.

Social Security Number textField

The customer's social security number.

Account Number (Hash) textField

The customer's account number. This is hashed and sent to LexisNexis.

Driver License Number (Hash) textField

The customer's driver license number. This is hashed and sent to LexisNexis.

IP Address textField

The customer's IP address as detected by a web server. This must be a valid external address.

Page FingerPrint textField

The page fingerprint. This is hashed and sent to LexisNexis.

Device ID textField

The ExactID persistent global identifier, which relies on a variety of persistent markers (browser cookies, Adobe Flash cookies, HTML 5 local storage) to allow ThreatMetrix to 100% accurately identify a device.

Fuzzy Device ID textField

The SmartID device identifier, which is cookieless, and is based exclusively on device attributes to improve detection of returning visitors, especially those trying to elude identification, and reduces false positives.

HTTP Referer Domain textField

For TD Cloud, the domain of the HTTP referrer detected during profiling. For TD Mobile, this field can be optionally populated by the 'Custom URL' option in the TrustDefender Mobile Library. This relates to the Profiled Domain property below but only includes the domain portion of the passed URL as opposed to the whole URL which is present in the Profiled Domain property. This is passed to the library by the customer's native application. Described in more detail in the TMX Knowledgebase, Article ID 378.

Profiled Domain textField

For TD Cloud, the URL (i.e. domain + path + querystring) of the referring page. For TD Mobile, the same as the HTTP Referer Domain property.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - apiKey string required
 - orgId string required
 - policy string required
 - service_type string required
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_email string
 - account_telephone string
 - account_work_phone string
 - account_date_of_birth string
 - account_gender string
 - national_id_number string
 - national_id_type string
 - account_drivers_license_number string
 - account_drivers_license_issuer string
 - account_routing_address string
 - account_routing_standard string
 - account_number string
 - account_passport_number string

- account_passport_machine_readable_line1 string
- account_passport_machine_readable_line2 string
- account_passport_expiration_date string
- account_passport_country string
- transaction_id string
- cc_number_hash string
- online_tld string
- online_tld_handle string
- line_of_business string
- application_name string
- shipping_account_address_street1 string
- shipping_account_address_street2 string
- shipping_account_address_city string
- shipping_account_address_state string
- shipping_account_address_zip string
- shipping_account_address_country string
- ach_routing_number string
- transaction_amount number
- transaction_currency string
- account_login string
- password_hash string
- ssn_hash string
- ach_account_hash string
- drivers_licence_number_hash string
- input_ip_address string
- page_fingerprint string
- device_id string
- fuzzy_device_id string
- http_referer_domain string
- profiled_domain string

Output Schema

- output object
 - rawResponse object
 - account_address_city string
 - account_address_state string
 - account_address_street1 string
 - account_address_zip string
 - account_date_of_birth string
 - account_first_name string
 - account_last_name string
 - account_telephone string
 - account_telephone_is_possible string
 - account_telephone_is_valid string
 - account_telephone_type string
 - api_call_datetime string
 - api_type string
 - api_version string
 - champion_request_duration string
 - custom_count_10 string
 - custom_count_12 string
 - custom_count_15 string
 - custom_count_8 string
 - custom_count_9 string
 - custom_output_11 array
 - custom_output_12 array
 - custom_output_13 array
 - custom_output_14 array
 - custom_output_15 array
 - custom_output_16 array
 - custom_output_7 array

- custom_output_9 array
 - event_datetime string
 - event_type string
 - integration_hub_results object
 - 3c8qvza7:DIIG Identity Verification object
 - Execute DIIG object
 - rule_id string
 - tps_datetime string
 - tps_duration string
 - tps_result string
 - tps_type string
 - tps_vendor string
 - tps_vendor_raw_response string
 - tps_was_timeout string
 - national_id_number string
 - national_id_type string
 - org_id string
 - policy string
 - policy_details_api object
 - policy_detail_api array
 - policy_engine_version string
 - policy_score string
 - reason_code array
 - request_id string
 - request_result string
 - review_status string
 - risk_rating string
 - service_type string
 - tps_was_timeout string
- transactionStatus string

Output Example

```

{ "rawResponse" :
  { "account_address_city" : "Los Angeles",
    "account_address_state" : "ca",
    "account_address_street1" : "123 san marino ave",
    "account_address_zip" : "95014",
    "account_date_of_birth" : "19890625",
    "account_first_name" : "John",
    "account_last_name" : "Doe",
    "account_telephone" : "+14579345754568",
    "account_telephone_is_possible" : "yes",
    "account_telephone_is_valid" : "yes",
    "account_telephone_type" : "FIXED_LINE_OR_MOBILE",
    "api_call_datetime" : "2021-08-18 10:34:31.214",
    "api_type" : "session-query",
    "api_version" : "12.3.2",
    "champion_request_duration" : "1380",
    "custom_count_10" : "8",
    "custom_count_12" : "0",
    "custom_count_15" : "1",
    "custom_count_8" : "40",
    "custom_count_9" : "8",
    "custom_output_11" :
      [ "1" ],
    "custom_output_12" :
      [ "1" ],
    "custom_output_13" :
      [ "1" ],
    "custom_output_14" :
      [ "1" ],
    "custom_output_15" :
      [ "1" ],
    "custom_output_16" :
      [ "1",
        "1" ],
    "custom_output_7" :
      [ "1" ],
    "custom_output_9" :
      [ "1" ],
    "event_datetime" : "2021-08-18 10:34:31.214",
    "event_type" : "payment",
    "integration_hub_results" :
      { "3c8qvza7:DIIG Identity Verification" :
        { "Execute DIIG" :
          { "rule_id" : "198399037",
            "tps_datetime" : "2021-08-18 10:34:31.225",
            "tps_duration" : "1372",
            "tps_result" : "ok",
            "tps_type" : "LexisNexis_DIIG",
            "tps_vendor" : "LexisNexis - Connectors",
            "tps_vendor_raw_response" : "<raw_response>",
            "tps_was_timeout" : "no" } } },
    "national_id_number" : "1234",
    "national_id_type" : "us-ssn4",
    "org_id" : "3c8qvza7",
    "policy" : "master",
    "policy_details_api" :
      { "policy_detail_api" :
        [
          { "type" : "champion",
            "id" : "0",

```

```

"customer" :
{ "score" : "8",
  "pvid" : "1493214",
  "review_status" : "reject",
  "risk_rating" : "high",
  "rules" :
  [
    { "rid" : "198140113",
      "reason_code" : "ThreatMetrix",
      "score" : "8",
      "pvid" : "1493221",
      "rules" :
      [
        { "rid" : "198140834",
          "reason_code" : "INPUT ERROR: NO WEB SESSION ID",
          "score" : "0" },

        { "rid" : "198140836",
          "reason_code" : "UNKNOWN SESSION",
          "score" : "0" },

        { "rid" : "198140859",
          "reason_code" : "Email Agt GT 3Months (Global)",
          "score" : "8" } ] },

    { "rid" : "198140114",
      "reason_code" : "Call DIIG",
      "score" : "0",
      "pvid" : "1493699",
      "rules" :
      [
        { "rid" : "198399037",
          "reason_code" : "Execute DIIG",
          "score" : "0" },

        { "rid" : "198399051",
          "reason_code" : "DIIG Fail",
          "score" : "0" },

        { "rid" : "198399053",
          "reason_code" : "IF DIIG Fails",
          "score" : "0" },

        { "rid" : "198399054",
          "reason_code" : "Terminate - Identity Verification Failed",
          "score" : "0" } ] } ] } ] } ] },
"policy_engine_version" : "12.3.1",
"policy_score" : "8",
"reason_code" :
[ "INPUT ERROR: NO WEB SESSION ID",
  "UNKNOWN SESSION",
  "Email Agt GT 3Months (Global)",
  "ThreatMetrix",
  "Execute DIIG",
  "DIIG Fail",
  "IF DIIG Fails",
  "Terminate - Identity Verification Failed",
  "Call DIIG" ],
"request_id" : "26895134-7b20-4c02-8d68-dfa76c7b32a1",

```



```
"request_result" : "success",  
"review_status" : "reject",  
"risk_rating" : "high",  
"service_type" : "basic",  
"tps_was_timeout" : "no" } }
```

ThreatMetrix: Get Risk Assessment

Get a risk assessment from ThreatMetrix using a session ID and optional attributes.

Properties

Service Type dropDown

Restricts which output fields are returned based on the level of access that a customer has. The service type is linked to your API key.

- Basic
- Session Policy
- Device
- DID
- IP
- Session
- All (Default)
- 3ds

Event Type dropDown

NOTE: If event_type is passed to attribute query, it WILL increment velocity counters etc just like a session query. if there is no event_type on attribute query, it will run but not increment velocity etc counters.

- Login
- Payment
- Account Creation (Default)
- Transfer
- Transaction Other
- Auction Bid
- Details Change
- Add Listing
- Account Balance
- Transaction History
- Digital Download
- Digital Stream

Session ID textField

LexisNexis Session ID.

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Account Email textField

The primary account holder's email address.

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

Account Work Phone textField

The primary account holder's work telephone number. This field is not an entity.

Date of Birth textField

The primary account holder's date of birth, formatted as YYYYMMDD.

Gender textField

The primary account holder's gender.

National ID Number textField

The primary account holder's national ID number. Used for identity verification.

National ID Type dropDown

The primary account holder's national ID type. Used for identity verification.

- US SSN
- US SSN HASH
- US SSN4
- US SSN FIRST5
- BR CPF
- MX CURP
- CO CEDULA

Driver License Number textField

The primary account holder's driver license number.

Driver License Issuer textField

Primary account driver license issuer

Routing Address textField

The primary account holder's routing address.

Routing Standard textField

The primary account holder's routing standard.

Account Number textField

The primary account holder's account number.

Passport Number textField

The primary account holder's passport number.

Passport machine Readable Line 1 textField

The primary account holder's passport information in machine-readable format, line 1.

Passport machine Readable Line 2 textField

The primary account holder's passport information in machine-readable format, line 2.

Passport Expiration Date textField

The primary account holder's passport expiration date, formatted as YYYY-MM-DD.

Passport Country textField

The primary account holder's passport country, in ISO 3166-1 alpha-2 format, such as "US".

Transaction ID textField

The identifier used by the merchant to identify the transaction, such as a purchase order number.

Credit Card Number textField

The credit card number used in the transaction.

Online TLD textField

The description of the online TLD handle source. Used to prevent collisions between different online TLD handles. For help determining the correct online TLD for the ID you wish to send with your query, speak to a LexisNexis representative. This field is required if the Online TLD Handle field is populated.

Online TLD Handle textField

A unique third-party identifier, such as a LexID or a DUNS Number. Used for rule creation and investigation. This field is required if the Online TLD field is populated.

Line of Business textField

The line of business specified by the customer.

Application Name textField

The name of the application sending the event.

Shipping Account Holder's Street Address 1 textField

The shipping account holder's street address, line 1.

Shipping Account Holder's Street Address 2 textField

The shipping account holder's street address, line 2.

Shipping Account Holder's City textField

The shipping account holder's city.

Shipping Account Holder's State textField

The shipping account holder's state.

Shipping Account Holder's ZIP or Postal Code textField

The shipping account holder's ZIP or postal code.

Shipping Account Holder's Country textField

The shipping account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Routing Number textField

The routing number for the account. When using this attribute in a Condition/Expression Condition rule or Expression variable, the value will be treated as a string if quotes are used to enclose it and as a number if no quotes are used.

Transaction Amount textField

The numeric currency amount. If a decimal is used, exactly two digits must follow it.

Transaction Currency textField

The currency used for the transaction, formatted in ISO 4217 currency code, such as "USD". This field is required when Transaction Amount is populated.

Account Login textField

A unique identifier for the customer, such as a username or account ID. Used to check whether the customer is on a watch list.

Password textField

The password associated with the Account Login. This is hashed and sent to LexisNexis. Used to check whether the customer is on a watch list.

Social Security Number textField

The customer's social security number.

Account Number (Hash) textField

The customer's account number. This is hashed and sent to LexisNexis.

Driver License Number (Hash) textField

The customer's driver license number. This is hashed and sent to LexisNexis.

IP Address textField

The customer's IP address as detected by a web server. This must be a valid external address.

Page FingerPrint textField

The page fingerprint. This is hashed and sent to LexisNexis.

Device ID textField

The ExactID persistent global identifier, which relies on a variety of persistent markers (browser cookies, Adobe Flash cookies, HTML 5 local storage) to allow ThreatMetrix to 100% accurately identify a device.

Fuzzy Device ID textField

The SmartID device identifier, which is cookieless, and is based exclusively on device attributes to improve detection of returning visitors, especially those trying to elude identification, and reduces false positives.

HTTP Referer Domain textField

For TD Cloud, the domain of the HTTP referrer detected during profiling. For TD Mobile, this field can be optionally populated by the 'Custom URL' option in the TrustDefender Mobile Library. This relates to the Profiled Domain property below but only includes the domain portion of the passed URL as opposed to the whole URL which is present in the Profiled Domain property. This is passed to the library by the customer's native application. Described in more detail in the TMX Knowledgebase, Article ID 378.

Profiled Domain textField

For TD Cloud, the URL (i.e. domain + path + querystring) of the referring page. For TD Mobile, the same as the HTTP Referer Domain property.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - apiKey string required
 - orgId string required
 - service_type string required
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_email string
 - account_telephone string
 - account_work_phone string
 - account_date_of_birth string
 - account_gender string
 - account_national_id_number string
 - account_national_id_type string
 - account_drivers_license_number string
 - account_drivers_license_issuer string
 - account_routing_address string
 - account_routing_standard string
 - account_number string
 - account_passport_number string
 - account_passport_machine_readable_line1 string

- account_passport_machine_readable_line2 string
- account_passport_expiration_date string
- account_passport_country string
- event_type string
- transaction_id string
- cc_number_hash string
- online_tld string
- online_tld_handle string
- line_of_business string
- application_name string
- shipping_account_address_street1 string
- shipping_account_address_street2 string
- shipping_account_address_city string
- shipping_account_address_state string
- shipping_account_address_zip string
- shipping_account_address_country string
- ach_routing_number string
- transaction_amount number
- transaction_currency string
- sessionId string
- account_login string
- password_hash string
- ssn_hash string
- ach_account_hash string
- drivers_licence_number_hash string
- input_ip_address string
- page_fingerprint string
- device_id string
- fuzzy_device_id string
- http_referer_domain string

■ profiled_domain string

Output Schema

- output object
 - rawResponse object
 - account_address_city string
 - account_address_state string
 - account_address_street1 string
 - account_address_zip string
 - account_date_of_birth string
 - account_first_name string
 - account_last_name string
 - account_telephone string
 - account_telephone_is_possible string
 - account_telephone_is_valid string
 - account_telephone_type string
 - api_call_datetime string
 - api_type string
 - api_version string
 - champion_request_duration string
 - custom_count_15 string
 - event_datetime string
 - event_type string
 - national_id_number string
 - national_id_type string
 - org_id string
 - policy string
 - policy_details_api object
 - policy_detail_api array
 - policy_engine_version string
 - policy_score string
 - reason_code array

- request_id string
- request_result string
- review_status string
- risk_rating string
- service_type string

Output Example

```

{ "rawResponse" :
  { "account_address_city" : "cupertino",
    "account_address_state" : "ca",
    "account_address_street1" : "1234 Example ave",
    "account_address_zip" : "84101",
    "account_date_of_birth" : "19850515",
    "account_first_name" : "John",
    "account_last_name" : "Doe",
    "account_telephone" : "+13684940396",
    "account_telephone_is_possible" : "yes",
    "account_telephone_is_valid" : "yes",
    "account_telephone_type" : "FIXED_LINE_OR_MOBILE",
    "api_call_datetime" : "2021-08-19 06:04:21.106",
    "api_type" : "session-query",
    "api_version" : "12.3.2",
    "champion_request_duration" : "5",
    "custom_count_15" : "1",
    "event_datetime" : "2021-08-19 06:04:21.106",
    "event_type" : "payment",
    "national_id_number" : "1234",
    "national_id_type" : "us_ssn4",
    "org_id" : "3c8qvza7",
    "policy" : "account_registration_v1",
    "policy_details_api" :
    { "policy_detail_api" :
      [
        { "type" : "champion",
          "id" : "0",
          "customer" :
            { "score" : "8",
              "pvid" : "1493221",
              "review_status" : "pass",
              "risk_rating" : "trusted",
              "rules" :
                [
                  { "rid" : "198140834",
                    "reason_code" : "INPUT ERROR: NO WEB SESSION ID",
                    "score" : "0" },

                  { "rid" : "198140836",
                    "reason_code" : "UNKNOWN SESSION",
                    "score" : "0" },

                  { "rid" : "198140859",
                    "reason_code" : "Email Agt GT 3Months (Global)",
                    "score" : "8" } ] } } ] },
          "policy_engine_version" : "12.3.1",
          "policy_score" : "8",
          "reason_code" :
            [ "INPUT ERROR: NO WEB SESSION ID",
              "UNKNOWN SESSION",
              "Email Agt GT 3Months (Global)" ],
          "request_id" : "85b47c80-0ac6-4fea-adb3-654677bdc30a",
          "request_result" : "success",
          "review_status" : "pass",
          "risk_rating" : "trusted",
          "service_type" : "basic" } }

```

Phone Finder

Search by phone number or identity to get ranked results with data insights like phone type, status, CallerID, and portability.

Properties

Service Type dropDown

Restricts which output fields are returned based on the level of access that a customer has. The service type is linked to your API key.

- Basic
- Session Policy
- Device
- DID
- IP
- Session
- All (Default)
- 3ds

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Account Email textField

The primary account holder's email address.

Account Work Phone textField

The primary account holder's work telephone number. This field is not an entity.

Date of Birth textField

The primary account holder's date of birth, formatted as YYYYMMDD.

Gender textField

The primary account holder's gender.

National ID Number textField

The primary account holder's national ID number. Used for identity verification.

National ID Type dropDown

The primary account holder's national ID type. Used for identity verification.

- US SSN
- US SSN HASH
- US SSN4
- US SSN FIRST5
- BR CPF
- MX CURP
- CO CEDULA

Driver License Number textField

The primary account holder's driver license number.

Driver License Issuer textField

Primary account driver license issuer

Routing Address textField

The primary account holder's routing address.

Routing Standard textField

The primary account holder's routing standard.

Account Number textField

The primary account holder's account number.

Passport Number textField

The primary account holder's passport number.

Passport machine Readable Line 1 textField

The primary account holder's passport information in machine-readable format, line 1.

Passport machine Readable Line 2 textField

The primary account holder's passport information in machine-readable format, line 2.

Passport Expiration Date textField

The primary account holder's passport expiration date, formatted as YYYY-MM-DD.

Passport Country textField

The primary account holder's passport country, in ISO 3166-1 alpha-2 format, such as "US".

Transaction ID textField

The identifier used by the merchant to identify the transaction, such as a purchase order number.

Credit Card Number textField

The credit card number used in the transaction.

Online TLD textField

The description of the online TLD handle source. Used to prevent collisions between different online TLD handles. For help determining the correct online TLD for the ID you wish to send with your query, speak to a LexisNexis representative. This field is required if the Online TLD Handle field is populated.

Online TLD Handle textField

A unique third-party identifier, such as a LexID or a DUNS Number. Used for rule creation and investigation. This field is required if the Online TLD field is populated.

Line of Business textField

The line of business specified by the customer.

Application Name textField

The name of the application sending the event.

Shipping Account Holder's Street Address 1 textField

The shipping account holder's street address, line 1.

Shipping Account Holder's Street Address 2 textField

The shipping account holder's street address, line 2.

Shipping Account Holder's City textField

The shipping account holder's city.

Shipping Account Holder's State textField

The shipping account holder's state.

Shipping Account Holder's ZIP or Postal Code textField

The shipping account holder's ZIP or postal code.

Shipping Account Holder's Country textField

The shipping account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

Routing Number textField

The routing number for the account. When using this attribute in a Condition/Expression Condition rule or Expression variable, the value will be treated as a string if quotes are used to enclose it and as a number if no quotes are used.

Transaction Amount textField

The numeric currency amount. If a decimal is used, exactly two digits must follow it.

Transaction Currency textField

The currency used for the transaction, formatted in ISO 4217 currency code, such as "USD". This field is required when Transaction Amount is populated.

Account Login textField

A unique identifier for the customer, such as a username or account ID. Used to check whether the customer is on a watch list.

Password textField

The password associated with the Account Login. This is hashed and sent to LexisNexis. Used to check whether the customer is on a watch list.

Social Security Number textField

The customer's social security number.

Account Number (Hash) textField

The customer's account number. This is hashed and sent to LexisNexis.

Driver License Number (Hash) textField

The customer's driver license number. This is hashed and sent to LexisNexis.

IP Address textField

The customer's IP address as detected by a web server. This must be a valid external address.

Page FingerPrint textField

The page fingerprint. This is hashed and sent to LexisNexis.

Device ID textField

The ExactID persistent global identifier, which relies on a variety of persistent markers (browser cookies, Adobe Flash cookies, HTML 5 local storage) to allow ThreatMetrix to 100% accurately identify a device.

Fuzzy Device ID textField

The SmartID device identifier, which is cookieless, and is based exclusively on device attributes to improve detection of returning visitors, especially those trying to elude identification, and reduces false positives.

HTTP Referer Domain textField

For TD Cloud, the domain of the HTTP referrer detected during profiling. For TD Mobile, this field can be optionally populated by the 'Custom URL' option in the TrustDefender Mobile Library. This relates to the Profiled Domain property below but only includes the domain portion of the passed URL as opposed to the whole URL which is present in the Profiled Domain property. This is passed to the library by the customer's native application. Described in more detail in the TMX Knowledgebase, Article ID 378.

Profiled Domain textField

For TD Cloud, the URL (i.e. domain + path + querystring) of the referring page. For TD Mobile, the same as the HTTP Referer Domain property.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - apiKey string required
 - orgId string required
 - service_type string required
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_email string
 - account_telephone string required
 - account_work_phone string
 - account_date_of_birth string
 - account_gender string
 - account_national_id_number string
 - account_national_id_type string
 - account_drivers_license_number string
 - account_drivers_license_issuer string
 - account_routing_address string
 - account_routing_standard string
 - account_number string
 - account_passport_number string
 - account_passport_machine_readable_line1 string

- account_passport_machine_readable_line2 string
- account_passport_expiration_date string
- account_passport_country string
- transaction_id string
- cc_number_hash string
- online_tld string
- online_tld_handle string
- line_of_business string
- application_name string
- shipping_account_address_street1 string
- shipping_account_address_street2 string
- shipping_account_address_city string
- shipping_account_address_state string
- shipping_account_address_zip string
- shipping_account_address_country string
- ach_routing_number string
- transaction_amount number
- transaction_currency string
- account_login string
- password_hash string
- ssn_hash string
- ach_account_hash string
- drivers_licence_number_hash string
- input_ip_address string
- page_fingerprint string
- device_id string
- fuzzy_device_id string
- http_referer_domain string
- profiled_domain string

Output Schema

- output object
 - rawResponse object
 - account_address_city string
 - account_address_state string
 - account_address_street1 string
 - account_address_zip string
 - account_date_of_birth string
 - account_first_name string
 - account_last_name string
 - account_lex_id string
 - account_lex_id_region string
 - account_telephone string
 - account_telephone_is_possible string
 - account_telephone_is_valid string
 - account_telephone_type string
 - api_call_datetime string
 - api_type string
 - api_version string
 - champion_request_duration string
 - event_datetime string
 - event_type string
 - integration_hub_results object
 - 3c8qvza7:Phone Finder object
 - Execute Phone Finder object
 - rule_id string
 - tps_datetime string
 - tps_duration string
 - tps_result string
 - tps_type string

- tps_vendor string
- tps_vendor_raw_response object
 - Status object
 - ConversationId string
 - RequestId string
 - TransactionStatus string
 - Products array
- tps_was_timeout string
- national_id_number string
- national_id_type string
- org_id string
- policy string
- policy_details_api object
 - policy_detail_api array
- policy_engine_version string
- policy_score string
- reason_code array
- request_id string
- request_result string
- review_status string
- risk_rating string
- service_type string
- tps_was_timeout string

Output Example


```

{ "rawResponse" :
{ "account_address_city" : "Los Angeles",
  "account_address_state" : "ca",
  "account_address_street1" : "1234 example ave",
  "account_address_zip" : "91243",
  "account_date_of_birth" : "19830421",
  "account_first_name" : "John",
  "account_last_name" : "Doe",
  "account_lex_id" : "US|1319573870",
  "account_lex_id_region" : "US",
  "account_telephone" : "+134586439734",
  "account_telephone_is_possible" : "yes",
  "account_telephone_is_valid" : "yes",
  "account_telephone_type" : "FIXED_LINE_OR_MOBILE",
  "api_call_datetime" : "2021-08-19 05:46:35.088",
  "api_type" : "session-query",
  "api_version" : "12.3.2",
  "champion_request_duration" : "2465",
  "event_datetime" : "2021-08-19 05:46:35.088",
  "event_type" : "payment",
  "integration_hub_results" :
{ "3c8qvza7:Phone Finder" :
{ "Execute Phone Finder" :
{ "rule_id" : "198139573",
  "tps_datetime" : "2021-08-19 05:46:35.098",
  "tps_duration" : "2457",
  "tps_result" : "ok",
  "tps_type" : "LexisNexisPhoneFinderProduction_v3_FirstClass",
  "tps_vendor" : "LexisNexis - Connectors",
  "tps_vendor_raw_response" :
{ "Status" :
{ "ConversationId" : "31000689434669",
  "RequestId" : "1117166609",
  "TransactionStatus" : "passed" },
  "Products" :
[
{ "ProductType" : "PhoneFinder",
  "ExecutedStepName" : "Phone Finder",
  "ProductConfigurationName" : "GSA_GIVE_PF",
  "ProductStatus" : "pass",
  "Items" :
[
{ "ItemName" : "PrepaidPhoneNumber",
  "ItemStatus" : "pass" },

{ "ItemName" : "LastChangeDateIMEI",
  "ItemStatus" : "pass" },

{ "ItemName" : "NoContractCarrier",
  "ItemStatus" : "pass" },

{ "ItemName" : "VOIPPhone",
  "ItemStatus" : "pass" },

{ "ItemName" : "LastChangeDateIMSI",
  "ItemStatus" : "pass" },

{ "ItemName" : "SurnameMismatch",
  "ItemStatus" : "pass" },

```

```

{ "ItemName" : "LostStolen",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneReturnedOften",
  "ItemStatus" : "pass" },

{ "ItemName" : "WirelessServiceType",
  "ItemStatus" : "fail",
  "ItemReason" :
  { "Code" : "WirelessServiceType.LOW",
    "Description" : "Phone Service Type is Wireless" } },

{ "ItemName" : "SourceSelfReported",
  "ItemStatus" : "fail",
  "ItemReason" :
  { "Code" : "SourceSelfReported.MEDIUM",
    "Description" : "Phone linked to identity by self-reported sources only" } },

{ "ItemName" : "LandlineServiceType",
  "ItemStatus" : "pass" },

{ "ItemName" : "CableServiceType",
  "ItemStatus" : "pass" },

{ "ItemName" : "UnknownServiceType",
  "ItemStatus" : "pass" },

{ "ItemName" : "1stFirstSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "2ndFirstSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhonePorted2ndRange",
  "ItemStatus" : "pass" },

{ "ItemName" : "3rdFirstSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhonePorted3rdRange",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhonePorted",
  "ItemStatus" : "pass" },

{ "ItemName" : "FrequentlyPhonePorted",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneSpoofedNumOfDays",
  "ItemStatus" : "pass" },

{ "ItemName" : "SpoofingPhoneNumber",
  "ItemStatus" : "pass" },

{ "ItemName" : "SpoofingDestination",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneAssociatedWithMoreThanXIdentities",
  "ItemStatus" : "pass" },

{ "ItemName" : "EmailCount(Month)",
  "ItemStatus" : "pass" },

```

```

{ "ItemName" : "DeviceCount(Month)",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneHighCountryCount",
  "ItemStatus" : "pass" },

{ "ItemName" : "RecentPhoneFirstSeen",
  "ItemStatus" : "fail",
  "ItemReason" :
  { "Code" : "RecentPhoneFirstSeen.LOW",
    "Description" : "Phone Number First Seen Recently in Digital Identity Network" } },

{ "ItemName" : "DigitalIDBadReputation",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneNumberAssociatedWithFraud",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneInRejectedTransaction",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneSearch",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneOnGlobalBlacklist",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneOTPRequest",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneNotActive",
  "ItemStatus" : "pass" },

{ "ItemName" : "SpoofedPhoneNumber",
  "ItemStatus" : "pass" },

{ "ItemName" : "SubjectIsBusiness",
  "ItemStatus" : "pass" },

{ "ItemName" : "PhoneForwarding",
  "ItemStatus" : "pass" },

{ "ItemName" : "SubjectDeceased",
  "ItemStatus" : "pass" },

{ "ItemName" : "NoFirstSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "CommercialAddress",
  "ItemStatus" : "pass" },

{ "ItemName" : "NoLastSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "MismatchAreaCodeAndAddressArea",
  "ItemStatus" : "pass" },

{ "ItemName" : "NoFirstAndLastSeenDate",
  "ItemStatus" : "pass" },

{ "ItemName" : "NotCurrentAddress",

```

```

    "ItemStatus" : "pass" },

    { "ItemName" : "LastSeenDateAge",
      "ItemStatus" : "fail",
      "ItemReason" :
        { "Code" : "LastSeenDateAge.MEDIUM",
          "Description" : "Last Seen Date is older than \"365\" days" } } ],
  "ParameterDetails" :
  [
    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_LexIDs",
      "Values" :
        [
          { "Value" : "1319573870" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Deceased_Indicators",
      "Values" :
        [
          { "Value" : "N" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Full_Names",
      "Values" :
        [
          { "Value" : "John Doe" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Street_1s",
      "Values" :
        [
          { "Value" : "54345 san mario ave" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Street_2s",
      "Values" :
        [
          { "Value" : "" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_StateCityZIPs",
      "Values" :
        [
          { "Value" : "CUPERTINO, CA 95014" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Time_With_Phones",
      "Values" :
        [
          { "Value" : "0" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Time_Last_Seen_With_Phones",
      "Values" :
        [
          { "Value" : "302" } ] },

    { "Group" : "IDENTITY_RECORDS",
      "Name" : "Consumer_Address_Types",
      "Values" :
        [
          { "Value" : "Residential" } ] },
  ]

```

```

{ "Group" : "IDENTITY_RECORDS",
  "Name" : "Consumer_Address_Statuses",
  "Values" :
  [
    { "Value" : "C" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Number",
  "Values" :
  [
    { "Value" : "4085555568" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Type",
  "Values" :
  [
    { "Value" : "POSSIBLE WIRELESS" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Carrier",
  "Values" :
  [
    { "Value" : "NEW CINGULAR WIRELESS PCS, LLC" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Listing_Name",
  "Values" :
  [
    { "Value" : "Doe John" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Status",
  "Values" :
  [
    { "Value" : "ACTIVE" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Listing_Type",
  "Values" :
  [
    { "Value" : "RESIDENTIAL" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Address_Type",
  "Values" :
  [
    { "Value" : "" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Port_Code",
  "Values" :
  [
    { "Value" : "Ported" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Caller_ID",
  "Values" :
  [
    { "Value" : "Doe John" } ] },

{ "Group" : "PRIMARY_PHONE",

```

```

      "Name" : "Primary_Phone_Port_Count",
      "Values" :
      [
        { "Value" : "1" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Phone_Verification_Indicator",
      "Values" :
      [
        { "Value" : "1" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Primary_Phone_No_Contract_Carrier",
      "Values" :
      [
        { "Value" : "0" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Phone_Verification_Msg",
      "Values" :
      [
        { "Value" : "Input phone number matches name" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Origination_Spoof_Count",
      "Values" :
      [
        { "Value" : "0" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Spoofed_Count",
      "Values" :
      [
        { "Value" : "0" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Destination_Spoof_Count",
      "Values" :
      [
        { "Value" : "0" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Primary_Phone_Risk_Indicator_Status",
      "Values" :
      [
        { "Value" : "WARN" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Primary_Phone_Risk_Indicator_Messages",
      "Values" :
      [
        { "Value" : "Phone Number First Seen Recently in Digital Identity Network" },

        { "Value" : "Last Seen Date is older than \"365\" days" },

        { "Value" : "Phone linked to identity by self-reported sources only" },

        { "Value" : "Phone Service Type is Wireless" } ] },

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Primary_Phone_Prepaid",
      "Values" :

```

```

[
  { "Value" : "0" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "OTP_Count",
  "Values" :
  [
    { "Value" : "1" } ] },

{ "Group" : "IDENTITY_RECORDS",
  "Name" : "Consumer_Ownership_at_Carrier_Indicators",
  "Values" :
  [
    { "Value" : "0" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "OTP_Last_Year",
  "Values" :
  [
    { "Value" : "2019" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "OTP_Last_Month",
  "Values" :
  [
    { "Value" : "07" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "OTP_Last_Day",
  "Values" :
  [
    { "Value" : "11" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "OTP_Last_Status",
  "Values" :
  [
    { "Value" : "1" } ] },

{ "Group" : "IDENTITY_RECORDS",
  "Name" : "Consumer_Source_Counts",
  "Values" :
  [
    { "Value" : "1" } ] },

{ "Group" : "IDENTITY_RECORDS",
  "Name" : "Consumer_Self_Reported_Only",
  "Values" :
  [
    { "Value" : "1" } ] },

{ "Group" : "IDENTITY_RECORDS",
  "Name" : "Consumer_to_Phone_Sources",
  "Values" :
  [
    { "Value" : "CreditInquiry" } ] },

{ "Group" : "PRIMARY_PHONE",
  "Name" : "Primary_Phone_Source_Count",
  "Values" :
  [
    { "Value" : "0" } ] },

```

```

    { "Group" : "PRIMARY_PHONE",
      "Name" : "Primary_Phone_Self_Reported_Only",
      "Values" :
        [
          { "Value" : "0" } ] } ] } ],
    "tps_was_timeout" : "no" } } },
    "national_id_number" : "1234",
    "national_id_type" : "us_ssn4",
    "org_id" : "3c8qvza7",
    "policy" : "phone finder",
    "policy_details_api" :
    { "policy_detail_api" :
      [
        { "type" : "champion",
          "id" : "0",
          "customer" :
            { "score" : "0",
              "pvid" : "1493204",
              "review_status" : "pass",
              "risk_rating" : "neutral",
              "rules" :
                [
                  { "rid" : "198139573",
                    "reason_code" : "Execute Phone Finder",
                    "score" : "0" } ] } } ] },
        "policy_engine_version" : "12.3.1",
        "policy_score" : "0",
        "reason_code" :
        [ "Execute Phone Finder" ],
        "request_id" : "5c4910b9-7018-4200-8b3b-11de65ff91aa",
        "request_result" : "success",
        "review_status" : "pass",
        "risk_rating" : "neutral",
        "service_type" : "basic",
        "tps_was_timeout" : "no" } }

```

Emailage

Evaluate email address metadata points such as domain details, email details, risk indicators, and other PII.

Properties

Email textField

Email of the user

IP Address textField

IP Address of the user

First Name textField

The customer's first name.

Last Name textField

The customer's last name.

Phone textField

The customer's phone number, including area code and local exchange. This is used to verify that the customer's phone number is in the same billing location as the cardholder. Most formats are accepted, but ISO E.164 format is highly recommended.

Secondary Email textField

If an additional email is available for the transaction, it is sent under this input field. Example: For money transfers, this is the recipient's email. NOTE: We do not provide a score for this email. It is mainly used as supporting data for risk assessment, similar to phone, address, name, etc.

Is Existing Customer? toggleSwitch

Indicates if the customer is a repeat customer.

Customer ID textField

This parameter can be used as an unique identifier for the customer.

Tracking ID textField

The trackingId associated with the original scoring request. This parameter can be used when you want to add an internal system identifier for a query. This identifier will be returned with the results.

Partner ID textField

ID used to identify an Emailage Partner.

Customer Identifier textField

ID used to identify an Emailage Partner's customer.

Billing Address textField

The billing address for the customer.

Billing City textField

The billing city for the customer.

Billing State or Region textField

The billing state or region for the customer.

Billing Postal Code textField

The billing postal (ZIP) code for the customer.

Billing Country textField

The billing country for the customer. This can be passed as the full country name or as an ISO 3166-1 alpha-2

Shipping Address textField

The shipping address for the customer.

Shipping City textField

The shipping city for the customer.

Shipping State or Region textField

The shipping state or region for the customer.

Shipping Postal Code textField

The shipping postal (ZIP) code for the customer.

Shipping Country textField

The shipping country for the customer. This can be passed as the full country name or as an ISO 3166-1 alpha-2

Card First 6 textField

The first six digits of a bank card number or payment card number and it is part of ISO/IEC 7812. Used to identify a card brand, issuing institution or bank, country of issuance, card type, and category of cards.

Transaction Amount textField

The customer's transaction amount.

Transaction Currency textField

The currency used for the customer's transaction as an ISO 4217 code.

Transaction Origin textField

Indicates who initiated the transaction. Inbound is where the customer initiates the transaction, and outbound is where the company initiated the transaction.

User Record ID textField

This is a user defined Record ID. This parameter can be used when you want to add an identifier for a query. This identifier will be returned with the results.

Transaction Type ID dropDown

The Transaction Type ID of the event being scored. Can be used instead of the transactionTypeDescription. Do not enter both the transactionTypeid and the transactionTypeDescription.

- Account creation (Default)
- Account login (Default)
- Email change (Default)
- Password reset (Default)
- Purchase (Default)
- Recurring purchase (Default)
- Referral (Default)
- Survey (Default)
- Job posting (Default)
- Job application (Default)
- Promotions (Default)
- Payment (Default)
- Banking (Default)
- Digital (Default)
- Comment (Default)
- Insurance (Default)
- Transaction Other (Default)

Transaction Type Description dropDown

The Transaction Type Description of event being scored. Can be used instead of the transactionTypeid. Do not enter both the transactionTypeid and the transactionTypeDescription.

- Account creation
- Account login
- Email change
- Password reset
- Purchase

- Recurring purchase
- Referral
- Survey
- Job posting
- Job application
- Promotions
- Payment
- Banking
- Digital
- Comment
- Insurance
- Transaction Other

Time of Service textField

Number of days until service.

Service Date textField

The date and time of the service. Examples: Traveling - Date of flight, Hospitality - Date of stay, Ticketing - Date of event, Technology/Finance/eCommerce - Date of the service. Date/time parameter must be specified in UTC (Zulu) and be formatted in the ISO8601 style as below: yyyy-mm-ddThh:mm:ssZ (e.g: 2008-09-15T15:53:00Z)

Service Location textField

The location of the final service/transaction.

Service Details textField

Further detail of the service or transaction.

Service Category textField

The general category of the service

Delivery Type textField

The type of delivery of the goods or service.

Useragent textField

The User-Agent HTTP header.

Device ID textField

Vendor code representing the device ID manufacturer used to determine the device ID. NOTE: Send only the 3 digit code. The vendor codes are as follows: 100 - Emailage 110 - 41st Parameter 120 - ThreatMetrix 130 - Iovation 140 - RiskFort 150 - DigitalResolve 160 - RSA 170 - Symantec (Verisign) 180 - Nudata 190 - Kount 200 - InAuth 990 - Other

Device Source textField

Vendor code representing the device ID manufacturer used to determine the device ID. NOTE: Send only the 3 digit code. The vendor codes are as follows: 100 - Emailage 110 - 41st Parameter 120 - ThreatMetrix 130 - Iovation 140 - RiskFort 150 - DigitalResolve 160 - RSA 170 - Symantec (Verisign) 180 - Nudata 190 - Kount 200 - InAuth 990 - Other

User Email textField

The Emailage username used to make the query. By default, if user_email is not specified, we use the account's default user and the associated department. If this value is applied, we use the specified user and department. NOTE: This is NOT the email address being queried. If this field is populated with an email other than one authorized to run queries, 3001 errors will be generated

accept-language HTTP header textField

The accept-language HTTP header (Language Culture Name).

Response Language textField

The language returned in the API response.

Input Schema

- default object
 - properties object
 - apiUrl3 string required
 - clientId string required
 - clientSecret string required
 - email string required
 - ip string
 - firstname string
 - lastname string
 - phone string
 - secondary_email string
 - existingcustomer boolean
 - customerid string
 - trackingId string
 - partnerid string
 - customeridentifier string
 - billaddress string
 - billcity string
 - billregion string
 - billpostal string
 - billcountry string
 - shipaddress string
 - shipcity string
 - shipregion string
 - shippostal string
 - shipcountry string
 - cardFirstSix string
 - transamount string
 - transcurrency string

- transorigin string
- urid string
- transactionTypeID string/number
- transactionTypeDescription string
- time_to_service string
- service_date string
- service_location string
- service_detail string
- service_category string
- delivery_type string
- useragent string
- deviceid string
- devicesource string
- user_email string
- acceptlang string
- response_language string

Output Schema

- output object
 - rawResponse object
 - query object
 - email string
 - queryType string
 - count integer
 - created string
 - lang string
 - responseCount integer
 - firstname string
 - lastname string
 - phone string
 - billaddress string
 - billcity string
 - billregion string
 - billpostal string
 - billcountry string
 - results array
 - responseStatus object
 - status string
 - errorCode string
 - description string

Output Example

```

{ "rawResponse" :
  { "query" :
    { "email" : "johndoe@example.com",
      "queryType" : "EmailAgeVerification",
      "count" : 1,
      "created" : "2021-10-01T10:44:54Z",
      "lang" : "en-US",
      "responseCount" : 1,
      "firstname" : "John",
      "lastname" : "Doe",
      "phone" : "+14055555968",
      "billaddress" : "1234 asdf asdf",
      "billcity" : "Los Angeles",
      "billregion" : "CA",
      "billpostal" : "23464",
      "billcountry" : "US",
      "results" :
        [
          { "userdefinedrecordid" : "",
            "email" : "johndoe@example.com",
            "eName" : "",
            "emailAge" : "",
            "email_creation_days" : "",
            "domainAge" : "1995-08-13T00:00:00Z",
            "domain_creation_days" : "9546",
            "firstVerificationDate" : "2010-07-19T00:00:00Z",
            "first_seen_days" : "4092",
            "lastVerificationDate" : "2021-10-01T10:43:02Z",
            "status" : "Verified",
            "country" : "",
            "fraudRisk" : "065 Very Low",
            "EAScore" : "65",
            "EAReason" : "Email Created at least 11.2 Years Ago",
            "EAStatusID" : "2",
            "EAReasonID" : "14",
            "EAAdviceID" : "3",
            "EAAdvice" : "Lower Fraud Risk",
            "EARiskBandID" : "1",
            "EARiskBand" : "Fraud Score 1 to 100",
            "source_industry" : "",
            "fraud_type" : "",
            "lastflaggedon" : "",
            "location" : "",
            "smfriends" : "",
            "totalhits" : "4",
            "uniquehits" : "1",
            "imageurl" : "",
            "emailExists" : "Yes",
            "domainExists" : "Yes",
            "company" : "",
            "title" : "",
            "domainname" : "example.com",
            "domaincompany" : "Google",
            "domaincountryname" : "",
            "domaincategory" : "Webmail",
            "domainincorporate" : "No",
            "domainrisklevel" : "Moderate",
            "domainrelevantinfo" : "Valid Domain",
            "domainrisklevelID" : "3",
            "domainrelevantinfoID" : "509",

```

```
"domaincountrymatch" : "No",
"domainriskcountry" : "No",
"smlinks" :
[ ],
"phone_status" : "Valid",
"shipforward" : "",
"billriskcountry" : "No",
"namematch" : "U",
"phoneowner" : "",
"phoneownertype" : "",
"phonecarriertype" : "",
"phonecarriernetworkcode" : "",
"phonecarriername" : "",
"phoneownermatch" : "",
"correlationId" : "1ef2273f-bc5b-4949-bcd5-efc681ed1623",
"transAmount" : "",
"transCurrency" : "" } ] },
"responseStatus" :
{ "status" : "success",
  "errorCode" : "0",
  "description" : "" } }
```

Knowledge-Based Authentication

Challenge users with knowledge-based questions.

Properties

Mode dropDown

Mode in which the transaction should run

- live
- testing (Default)
- simulated

Locale dropDown

Language in which the customer wants to receive the response

- US English
- Formal Spanish
- Haitian Creole (only for authentication)

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

Account Email textField

The primary account holder's email address.

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

SSN textField

Social Security Number

SSN Type dropDown

Type of SSN provided

- ssn4
- ssn9
- ssn-first5
- noSSN
- other

Day of Birth textField

Day (DD) Possible values are 1 – 31 .

Month of Birth textField

Month (MM) Possible values are numbers 1 – 12 .

Year of Birth textField

Year of Birth (YYYY) e.g. 1985, 1958, 2001

Lex ID textField

Unique identifier that is assigned to a subject by LexisNexis®. A LexID® number does not include any SPII (sensitive personally identifiable information). Either the LexID number or the indicated name elements are required.

Simulation Mode dropDown

An element that governs the response given by RDP This element is required only when Mode is set to simulated .

- Random
- Error Simulation Values
- Communications Error

- Internal Application_Error
- Invalid Information
- Invalid Login
- Invalid Mode

Reference textField

Internal tracking number that your organization can assign to a transaction.

GLBA textField

Integer value based on the GLBA (Gramm-Leach-Bliley Act) that indicates the reason for the request

DPPA textField

Integer value pursuant to the DPPA (Driver's Privacy Protection Act) of 1994 that indicates the reason for the request

Venue dropDown

Type of environment where the transaction takes place

- online
- callcenter
- batch
- point-of-sale
- customer-service
- ivr

Use Custom Screens toggleSwitch

HTML Template textArea

CSS codeEditor

Script codeEditor

Input Schema

- default object
 - properties object
 - apiUrl2 string required
 - username string required
 - password string required
 - accountId string required
 - settingsMode string required
 - SimulationType string
 - Reference string
 - GLBA string
 - DPPA string
 - Locale string required
 - Venue string
 - LexID string
 - day string
 - month string
 - year string
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_email string
 - account_telephone string
 - ssnNumber string

■ ssnType string

Output Schema

- output object
 - rawResponse object
 - Status object
 - ConversationId string
 - RequestId string
 - TransactionStatus string
 - TransactionReasonCode object
 - Code string
 - LexID string
 - Products array

Output Example

```
{ "rawResponse" :
  { "Status" :
    { "ConversationId" : "31000761962129",
      "RequestId" : "1205338429",
      "TransactionStatus" : "failed",
      "TransactionReasonCode" :
        { "Code" : "failed_iauth_questions" },
      "LexID" : "1319573870" },
    "Products" :
      [
        { "ProductType" : "Velocity",
          "ExecutedStepName" : "pre_id_velocity",
          "ProductConfigurationName" : "GSA_PreID",
          "ProductStatus" : "pass",
          "Items" :
            [
              { "ItemName" : "FUTILITY",
                "ItemStatus" : "pass" } ] },
        { "ProductType" : "Discovery",
          "ExecutedStepName" : "discovery",
          "ProductConfigurationName" : "GIVE_Discovery",
          "ProductStatus" : "pass" },
        { "ProductType" : "Velocity",
          "ExecutedStepName" : "post_id_velocity",
          "ProductConfigurationName" : "GIVE_PostID",
          "ProductStatus" : "pass",
          "Items" :
            [
              { "ItemName" : "FREQUENCY",
                "ItemStatus" : "pass" },
              { "ItemName" : "QUIZ",
                "ItemStatus" : "pass" } ] },
        { "ProductType" : "IdentityEvent",
          "ExecutedStepName" : "identity_events",
          "ProductConfigurationName" : "GIVE_IE",
          "ProductStatus" : "pass" },
        { "ProductType" : "IIDQA",
          "ExecutedStepName" : "authentication",
          "ProductConfigurationName" : "GIVE_KBA",
          "ProductStatus" : "fail",
          "ProductReason" :
            { "Code" : "failed_iauth_questions" } } ] } }
```

One Time Password

Send a one-time password.

Properties

Delivery method for the OTP dropDown

Delivery method for the OTP

- Text
- Email

SMS Body textField

Defines the custom SMS text body.

Default:

```
Your One Time Password is ${OTP}.${LineBreak}We will never call you for this code.${LineBreak}Your  
passcode will expire in ${ExpirePeriod} minutes
```

Email Title textField

Defines the custom OTP Email Header.

Default:

```
Please, check out this email! It's your one time passcode!
```

Email Title textField

Defines the custom OTP Email Body.

Default:

```
Your One Time Passcode is ${OTP}.${LineBreak}We will never call you for this code.${LineBreak}Your  
passcode will expire in ${ExpirePeriod} minutes
```

Delivery language for the OTP message dropDown

Delivery language for the OTP message

- English
- French
- Spanish

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

Account Email textField

The primary account holder's email address.

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Date of Birth textField

The primary account holder's date of birth, formatted as YYYYMMDD.

Gender textField

The primary account holder's gender.

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

National ID Number textField

The primary account holder's national ID number. Used for identity verification.

National ID Type dropDown

The primary account holder's national ID type. Used for identity verification.

- US SSN
- US SSN HASH
- US SSN4
- US SSN FIRST5
- BR CPF
- MX CURP
- CO CEDULA

Telephone Context textField

The context of the telephone, for e.g.: Mobile

Telephone GEO textField

Telephone geolocation, for e.g.: US

Event Type dropDown

NOTE: If event_type is passed to attribute query, it WILL increment velocity counters etc just like a session query. if there is no event_type on attribute query, it will run but not increment velocity etc counters.

- Login
- Payment
- Account Creation (Default)
- Transfer
- Transaction Other
- Auction Bid
- Details Change
- Add Listing
- Account Balance
- Transaction History
- Digital Download
- Digital Stream

Use Custom Screens toggleSwitch

HTML Template textArea

CSS codeEditor

Script codeEditor

Input Schema

- default object
 - properties object
 - apiUrl4 string required
 - orgId2 string required
 - apiKey2 string required
 - event_type string
 - Method string required
 - SmsBody string
 - EmailTitle string
 - EmailBody string
 - Language string required
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_date_of_birth string
 - account_gender string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_national_id_number string
 - account_national_id_type string
 - account_email string
 - account_telephone string
 - account_telephone_context string
 - account_telephone_geo string

- complete object
 - properties object
 - apiUrl4 string required
 - orgId2 string required
 - apiKey2 string required
 - Method string required
 - Language string required
 - parameters object
 - otp string required

Output Schema

- output object
 - rawResponse object
 - account_address_country string
 - account_email string
 - account_email_activities array
 - account_email_attributes array
 - account_email_first_seen string
 - account_email_last_event string
 - account_email_last_update string
 - account_email_result string
 - account_email_score string
 - account_email_worst_score string
 - account_first_name string
 - account_last_name string
 - account_middle_name string
 - account_name_activities array
 - account_name_attributes array
 - account_name_first_seen string
 - account_name_last_event string
 - account_name_last_update string
 - account_name_result string
 - account_name_score string
 - account_name_worst_score string
 - action string
 - action_template string
 - api_call_datetime string
 - api_caller_ip string
 - api_type string
 - auth_method string

- auth_status string
- champion_request_duration string
- enabled_services array
- event_date string
- event_datetime string
- event_last_update string
- event_type string
- input_request_id string
- integration_hub_results object
 - 11jr7q70:Authentication object
 - Authentication object
 - rule_id string
 - tps_datetime string
 - tps_duration string
 - tps_error string
 - tps_result string
 - tps_type string
 - tps_vendor string
 - tps_vendor_raw_response object
 - Status object
 - ConversationId string
 - RequestId string
 - TransactionStatus string
 - Reference string
 - InputEcho array
 - Products array
 - tps_was_timeout string
- national_id_type null
- org_id string
- original_event_created string

- original_event_updated string
- policy string
- policy_details_api object
 - policy_detail_api array
- policy_engine_version string
- policy_score string
- primary_industry string
- reason_code array
- request_duration string
- request_id string
- request_id_activities array
- request_result string
- review_status string
- risk_rating string
- secondary_industry string
- service_type string
- summary_risk_score string
- tmx_reason_code array
- tmx_risk_rating string
- tps_datetime string
- tps_duration string
- tps_error string
- tps_result string
- tps_type string
- tps_vendor string
- tps_vendor_raw_response string
- tps_was_timeout string

Output Example

```

{ "rawResponse" :
{ "account_address_country" : "us",
  "account_email" : "john@doe.com",
  "account_email_activities" :
  [ "_CHALLENGED" ],
  "account_email_attributes" :
  [ "_CHALLENGED" ],
  "account_email_first_seen" : "2021-10-12",
  "account_email_last_event" : "2021-10-18",
  "account_email_last_update" : "2021-10-18",
  "account_email_result" : "success",
  "account_email_score" : "0",
  "account_email_worst_score" : "0",
  "account_first_name" : "John",
  "account_last_name" : "Doe",
  "account_middle_name" : "",
  "account_name_activities" :
  [ "_CHALLENGED" ],
  "account_name_attributes" :
  [ "_CHALLENGED" ],
  "account_name_first_seen" : "2020-07-30",
  "account_name_last_event" : "2021-10-18",
  "account_name_last_update" : "2021-10-18",
  "account_name_result" : "success",
  "account_name_score" : "0",
  "account_name_worst_score" : "0",
  "action" : "response",
  "action_template" : "default_accept",
  "api_call_datetime" : "2021-10-18 10:43:50.321",
  "api_caller_ip" : "44.240.16.43",
  "api_type" : "authentication",
  "auth_method" : "otp",
  "auth_status" : "authentication_success",
  "champion_request_duration" : "631",
  "enabled_services" :
  [ "TMX100" ],
  "event_date" : "2021-10-18 10:00:00",
  "event_datetime" : "2021-10-18 10:43:50.321",
  "event_last_update" : "2021-10-18 10:00:00",
  "event_type" : "init_auth",
  "input_request_id" : "5120df86-801e-450f-b854-abbc85225590",
  "integration_hub_results" :
  { "11jr7q70:Authentication" :
  { "Authentication" :
  { "rule_id" : "206676243",
    "tps_datetime" : "2021-10-18 10:43:50.326",
    "tps_duration" : "629",
    "tps_error" : "passed",
    "tps_result" : "ok",
    "tps_type" : "LN_RDP_Auth_Hub_Continue",
    "tps_vendor" : "LexisNexis - Connectors",
    "tps_vendor_raw_response" :
    { "Status" :
    { "ConversationId" : "31000768645499",
      "RequestId" : "1217029359",
      "TransactionStatus" : "passed",
      "Reference" : "Reference1" },
      "InputEcho" :
      [
      { "Type" : "Initiate",

```

```

    "Persons" :
    [
      { "Addresses" :
        [
          { "Context" : "primary",
            "Country" : "us" } ],
        "Context" : "primary",
        "Emails" :
        [ "john@doe.com" ],
        "Name" :
        { "FirstName" : "John",
          "LastName" : "Doe",
          "MiddleName" : "" } } ] },
    "Products" :
    [
      { "ProductType" : "OTP",
        "ExecutedStepName" : "auth_select",
        "ProductConfigurationName" : "TMX_Test_OTP",
        "ProductStatus" : "pass" } ] },
    "tps_was_timeout" : "no" } } },
    "national_id_type" : null,
    "org_id" : "2234ds24f",
    "original_event_created" : "2021-10-18 10:00:00",
    "original_event_updated" : "2021-10-18 10:00:00",
    "policy" : "authentication",
    "policy_details_api" :
    { "policy_detail_api" :
      [
        { "type" : "champion",
          "id" : "0",
          "customer" :
          { "score" : "0",
            "pvid" : "1512519",
            "review_status" : "pass",
            "risk_rating" : "neutral",
            "rules" :
            [
              { "rid" : "206676243",
                "reason_code" : "Authentication",
                "score" : "0" } ] } } ] },
        "policy_engine_version" : "12.5",
        "policy_score" : "0",
        "primary_industry" : "fintech",
        "reason_code" :
        [ "Authentication" ],
        "request_duration" : "636",
        "request_id" : "ef94941c-8c6a-4295-aa37-18a840dff665",
        "request_id_activities" :
        [ "_CHALLENGED" ],
        "request_result" : "success",
        "review_status" : "pass",
        "risk_rating" : "neutral",
        "secondary_industry" : "platform",
        "service_type" : "all",
        "summary_risk_score" : "0",
        "tmx_reason_code" :
        [ "_ACC_EMAIL_GBL_VEL_6_7_8_8",
          "_ACC_EMAIL_GBL_AGE_GT_DY",
          "_ACC_NAME_GBL_VEL_6_7_8_8",
          "_ACC_NAME_GBL_AGE_GT_3MTHS",
          "_ACC_EMAIL_LCL_VEL_6_7_8_8",
          "_ACC_EMAIL_LCL_AGE_GT_DY",

```

```

    "_ACC_NAME_LCL_VEL_6_7_8_8",
    "_ACC_NAME_LCL_AGE_GT_DY",
    "_EXPRESSION_ERROR" ],
    "tmx_risk_rating" : "neutral",
    "tps_datetime" : "2021-10-18 10:43:50.326",
    "tps_duration" : "629",
    "tps_error" : "passed",
    "tps_result" : "ok",
    "tps_type" : "LN_RDP_Auth_Hub_Continue",
    "tps_vendor" : "LexisNexis - Connectors",
    "tps_vendor_raw_response" : "{ \"Status\": { \"ConversationId\": \"31000768645499\", \"RequestId\": \"1217029359\", \"TransactionStatus\": \"passed\", \"Reference\": \"Reference1\", \"InputEcho\": [ { \"Type\": \"Initiate\", \"Persons\": [ { \"Addresses\": [ { \"Context\": \"primary\", \"Country\": \"us\" } ], \"Context\": \"primary\", \"Emails\": [ \"johndoe@example.com\" ], \"Name\": { \"FirstName\": \"John\", \"LastName\": \"Doe\", \"MiddleName\": \"Joe\" } } ] }, { \"Products\": [ { \"ProductType\": \"OTP\", \"ExecutedStepName\": \"auth_select\", \"ProductConfigurationName\": \"TMX_Test_OTP\", \"ProductStatus\": \"pass\" } ] }, \"tps_was_timeout\" : \"no\" } }

```

Knowledge-Based Authentication (Authentication Project)

Challenge users with knowledge-based questions.

Properties

First Name textField

The primary account holder's first name.

Middle Name textField

The primary account holder's middle name

Last Name textField

The primary account holder's last name

Telephone Number textField

The primary account holder's telephone number. Can contain the following characters: 0-9 , . ; { } (and). All braces must be in pairs. White space is removed automatically.

Account Email textField

The primary account holder's email address.

Date of Birth textField

The primary account holder's date of birth, formatted as YYYYMMDD.

Gender textField

The primary account holder's gender.

Street Address 1 textField

The primary account holder's street address 1

Street Address 2 textField

The primary account holder's street address 2

City textField

The primary account holder's city

State textField

The primary account holder's State

ZIP textField

The primary account holder's ZIP

Country textField

The primary account holder's country, in ISO 3166-1 alpha-2 format, such as "US".

National ID Number textField

The primary account holder's national ID number. Used for identity verification.

National ID Type dropDown

The primary account holder's national ID type. Used for identity verification.

- US SSN
- US SSN HASH
- US SSN4
- US SSN FIRST5
- BR CPF
- MX CURP
- CO CEDULA

Telephone Context textField

The context of the telephone, for e.g.: Mobile

Telephone GEO textField

Telephone geolocation, for e.g.: US

Event Type dropDown

NOTE: If event_type is passed to attribute query, it WILL increment velocity counters etc just like a session query. if there is no event_type on attribute query, it will run but not increment velocity etc counters.

- Login
- Payment
- Account Creation (Default)
- Transfer
- Transaction Other
- Auction Bid
- Details Change
- Add Listing
- Account Balance
- Transaction History
- Digital Download
- Digital Stream

Use Custom Screens toggleSwitch

HTML Template textArea

CSS codeEditor

Script codeEditor

Input Schema

- default object
 - properties object
 - apiUrl4 string required
 - orgId2 string required
 - apiKey2 string required
 - event_type string
 - account_first_name string
 - account_middle_name string
 - account_last_name string
 - account_date_of_birth string
 - account_gender string
 - account_address_street1 string
 - account_address_street2 string
 - account_address_city string
 - account_address_state string
 - account_address_zip string
 - account_address_country string
 - account_national_id_number string
 - account_national_id_type string
 - account_email string
 - account_telephone string
 - account_telephone_context string
 - account_telephone_geo string

Output Schema

- output object
 - rawResponse object
 - account_address_city string
 - account_address_country string
 - account_address_state string
 - account_address_street1 string
 - account_email string
 - account_first_name string
 - account_last_name string
 - auth_method string
 - auth_status string
 - event_datetime string
 - event_type string
 - answers object
 - QuestionSetId string
 - Questions array
 - input_request_id string
 - original_event_created string
 - original_event_updated string
 - policy string
 - policy_engine_version string
 - policy_site_id string
 - request_duration string
 - request_id string
 - request_result string
 - review_status string

Output Example

```
{ "rawResponse" :
  { "account_address_city" : "Los Angeles",
    "account_address_country" : "us",
    "account_address_state" : "ca",
    "account_address_street1" : "12434 S0mething ave",
    "account_email" : "jon@doe.com",
    "account_first_name" : "jon",
    "account_last_name" : "doe",
    "auth_method" : "kba",
    "auth_status" : "authentication_success",
    "event_datetime" : "2021-10-22 06:41:27.055",
    "event_type" : "init_auth",
    "answers" :
    { "QuestionSetId" : "2331385118",
      "Questions" :
      [
        { "QuestionId" : "3054678218",
          "Choices" :
          [
            { "Choice" : "6178344158" } ] } ] },
      "input_request_id" : "257f5956-68c2-4f2e-b932-391f6aeb2b8",
      "original_event_created" : "2021-10-22 06:00:00",
      "original_event_updated" : "2021-10-22 06:00:00",
      "policy" : "authentication",
      "policy_engine_version" : "12.5",
      "policy_site_id" : "P2/otin102.prod.sac",
      "request_duration" : "427",
      "request_id" : "471df61e-b1ac-4fb0-b5d5-5cfc24ffeb91",
      "request_result" : "success",
      "review_status" : "pass" } }
```

TrueID: Verify Document

Verify user identities with government ID validation and selfie liveness checks.

Properties

Mode dropDown

Mode in which the transaction should run

- live
- testing (Default)
- simulated

Locale dropDown

Language in which the customer wants to receive the response

- US English
- Formal Spanish
- Haitian Creole (only for authentication)

Simulation Mode dropDown

An element that governs the response given by RDP This element is required only when Mode is set to simulated .

- Random
- Error Simulation Values
- Communications Error
- Internal Application_Error
- Invalid Information
- Invalid Login
- Invalid Mode

Venue dropDown

Type of environment where the transaction takes place

- online
- callcenter
- batch
- point-of-sale
- customer-service
- ivr

Workflow dropDown

Type of workflow

- ID (Default)
- ID + Selfie

Use Custom Screens toggleSwitch

HTML Template textArea

CSS codeEditor

Script codeEditor

HTML Template textArea

CSS codeEditor

Script codeEditor

Input Schema

- default object
 - properties object
 - trueIdUsername string
 - trueIdPassword string
 - acasEndpoint string
 - acuantJavascriptWebSdkScriptSource string
 - acuantConfigurationScript string
 - acuantJavascriptWebSdkScript string
 - acuantCameraScript string
 - acuantPassiveLivenessScript string
 - openCvScript string
 - apiUrl2 string
 - username string
 - password string
 - accountId string
 - settingsMode string
 - SimulationType string
 - Reference string
 - Locale string
 - Venue string
 - workflowType string

Output Schema

- output object
 - rawResponse object
 - Status object
 - ConversationId string
 - RequestId string
 - TransactionStatus string
 - Products array
 - frontImageFileName string
 - backImageFileName string
 - selfImageFileName string

Output Example

```

{ "rawResponse" :
{ "Status" :
{ "ConversationId" : "31000804638459",
  "RequestId" : "1275210509",
  "TransactionStatus" : "passed" },
"Products" :
[
{ "ProductType" : "TrueID",
  "ExecutedStepName" : "True_ID_Step",
  "ProductConfigurationName" : "GIVE_TrueID",
  "ProductStatus" : "pass",
  "ParameterDetails" :
[
{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocumentName",
  "Values" :
[
{ "Value" : "US Passport" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocAuthResult",
  "Values" :
[
{ "Value" : "Passed" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIssuerCode",
  "Values" :
[
{ "Value" : "USA" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIssuerName",
  "Values" :
[
{ "Value" : "USA" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIssuerType",
  "Values" :
[
{ "Value" : "Country" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocClassCode",
  "Values" :
[
{ "Value" : "Passport" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocClass",
  "Values" :
[
{ "Value" : "Passport" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocClassName",
  "Values" :
[
{ "Value" : "Passport" } ] },

```

```

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIsGeneric",
  "Values" :
  [
    { "Value" : "false" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIssue",
  "Values" :
  [
    { "Value" : "2014" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocIssueType",
  "Values" :
  [
    { "Value" : "Passport" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "DocSize",
  "Values" :
  [
    { "Value" : "ID3" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "ClassificationMode",
  "Values" :
  [
    { "Value" : "Automatic" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "OrientationChanged",
  "Values" :
  [
    { "Value" : "false" } ] },

{ "Group" : "AUTHENTICATION_RESULT",
  "Name" : "PresentationChanged",
  "Values" :
  [
    { "Value" : "false" } ] },

{ "Group" : "IMAGE_METRICS_RESULT",
  "Name" : "Side",
  "Values" :
  [
    { "Value" : "Front" } ] },

{ "Group" : "IMAGE_METRICS_RESULT",
  "Name" : "GlareMetric",
  "Values" :
  [
    { "Value" : "99" } ] },

{ "Group" : "IMAGE_METRICS_RESULT",
  "Name" : "SharpnessMetric",
  "Values" :
  [
    { "Value" : "78" } ] },

{ "Group" : "IMAGE_METRICS_RESULT",

```

```

    "Name" : "IsTampered",
    "Values" :
    [
      { "Value" : "0" } ] },

  { "Group" : "IMAGE_METRICS_RESULT",
    "Name" : "IsCropped",
    "Values" :
    [
      { "Value" : "0" } ] },

  { "Group" : "IMAGE_METRICS_RESULT",
    "Name" : "HorizontalResolution",
    "Values" :
    [
      { "Value" : "454" } ] },

  { "Group" : "IMAGE_METRICS_RESULT",
    "Name" : "VerticalResolution",
    "Values" :
    [
      { "Value" : "454" } ] },

  { "Group" : "IMAGE_METRICS_RESULT",
    "Name" : "Light",
    "Values" :
    [
      { "Value" : "White" } ] },

  { "Group" : "IMAGE_METRICS_RESULT",
    "Name" : "MimeType",
    "Values" :
    [
      { "Value" : "image/jpeg" } ] },

  { "Group" : "IDAUTH_FIELD_DATA",
    "Name" : "Fields_DOB_Month",
    "Values" :
    [
      { "Value" : "8" } ] },

  { "Group" : "IDAUTH_FIELD_DATA",
    "Name" : "Fields_DOB_Day",
    "Values" :
    [
      { "Value" : "16" } ] },

  { "Group" : "IDAUTH_FIELD_DATA",
    "Name" : "Fields_BirthPlace",
    "Values" :
    [
      { "Value" : "Los Angeles" } ] },

  { "Group" : "IDAUTH_FIELD_DATA",
    "Name" : "Fields_DocumentClassCode",
    "Values" :
    [
      { "Value" : "P" } ] },

  { "Group" : "IDAUTH_FIELD_DATA",
    "Name" : "Fields_DocumentClassName",
    "Values" :

```

```

    [
      { "Value" : "Passport" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_DocumentNumber",
      "Values" :
      [
        { "Value" : "234345354" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_ExpirationDate_Year",
      "Values" :
      [
        { "Value" : "2023" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_ExpirationDate_Month",
      "Values" :
      [
        { "Value" : "2" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_expirationDate_Day",
      "Values" :
      [
        { "Value" : "21" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_IssuingAuthority",
      "Values" :
      [
        { "Value" : "DEPARTMENT OF PASSPORT" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_IssuingStateCode",
      "Values" :
      [
        { "Value" : "USA" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_IssuingStateName",
      "Values" :
      [
        { "Value" : "USA" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_CountryCode",
      "Values" :
      [
        { "Value" : "USA" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_Sex",
      "Values" :
      [
        { "Value" : "M" } ] },

    { "Group" : "IDAUTH_FIELD_DATA",
      "Name" : "Fields_IssueDate_Year",
      "Values" :
      [
        { "Value" : "2018" } ] },

```

[illegible]

TrueID: Delete Document

Delete government documents from LexisNexis.

Properties

Delete Front Image dropDown

- Yes (Default)
- No

Delete Back Image dropDown

- Yes (Default)
- No

Delete Selfie Image dropDown

- Yes (Default)
- No

Input Schema

- default object
 - properties object
 - deleteFrontImage string
 - deleteBackImage string
 - deleteSelfieImage string

Output Schema

- output object
 - rawResponse object
 - frontImageDeleted boolean
 - backImageDeleted boolean
 - selfieImageDeleted boolean

Output Example

```
{ "rawResponse" :  
  { "frontImageDeleted" : true,  
    "backImageDeleted" : true,  
    "selfieImageDeleted" : true } }
```

LexisNexis Connector Release Notes

New features and improvements in the LexisNexis connector.

April 2025

The LexisNexis Connector now respects localized error messages

Fixed

Error handling for the LexisNexis connector has been corrected and now respects localized error messages. As a result, select error outcomes might produce different message text.

March 2024

The LexisNexis connector is now available

New

You can use the LexisNexis connector to:

- Get risk assessments from ThreatMetrix with the LexisNexis Dynamic Decision Platform
- Use the LexisNexis Dynamic Decision Platform to access Emailage, Phone Find, and Other services defined by your LexisNexis Policy
- Authenticate users with OTPs
- Authenticate users with security questions

This new connector replaces the previous LexisNexis connector to take advantage of the latest LexisNexis APIs and provide a simplified configuration and modern end-user experiences. For the LexisNexis Legacy connector documentation, refer to [LexisNexis Legacy Connector](#).

Location Policy Connector

The Location Policy connector lets you check a user's IP and geographic location in your PingOne DaVinci flow.

You can use the Location Policy connector to:

- Implement risk intelligence by creating a location policy.
- Allow or deny requests from specified locales

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Location Policy connector

In DaVinci, add a Location Policy connector. For help, see [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Allow requests from specified locales

The connector has several capabilities that allow you to allow requests from specified locales:

- Allow by CIDR Block or IP Range
- Allow by Location Name

No special configuration is needed. Add the capability and populate its properties according to the help text.

Deny requests from specified locales

The connector has several capabilities that allow you to deny requests from specified locales:

- Deny by CIDR Block or IP Range
- Deny by Location Name

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Allow by CIDR Block or IP Range

Allow transactions based on CIDR blocks or IP ranges.

Properties

IP Addresses `textArea`

The list of CIDR blocks or IP addresses to allow, such as “131.10.55.1/24”. Separate multiple IP addresses with commas.

Input Schema

default `object`

ipAddressList `string`

Output Schema

output `object`

ipAddressList `array`

Deny by CIDR Block or IP Range

Deny transactions based on CIDR blocks or IP ranges.

Properties

IP Addresses `textArea`

The list of CIDR blocks or IP addresses to allow, such as “131.10.55.1/24”. Separate multiple IP addresses with commas.

Input Schema

default `object`

ipAddressList `string`

Output Schema

output `object`

ipAddressList `array`

Allow by Location Name

Allow transactions that originate from named locations.

Properties

Locations `textArea`

The list of geographies, regions, countries, or cities to allow. Separate multiple regions with a comma.

Input Schema**default** object**regions** string**Output Schema****output** object**regions** array**Deny by Location Name**

Deny transactions that originate from named locations.

Properties**Locations** textArea

The list of geographies, regions, countries, or cities to allow. Separate multiple regions with a comma.

Input Schema**default** object**regions** string**Output Schema****output** object**regions** array**Location Policy Connector Release Notes**

New features and improvements in the Location Policy connector. Updated April 9, 2025.

April 2025

Updated

The Location Policy connector now outputs country result

The **Allow by Location Name** and **Deny by Location Name** capabilities now provide the location information associated with the user's IP address. This makes it easy to branch the flow more specifically after an allow or deny result by evaluating the user's exact country.

M-O



Marketo Connector

The Marketo connector lets you add, search, and update leads into Marketo in your PingOne DaVinci flow.



Microsoft Edge Connector

The Microsoft Edge for Business connector lets you use Microsoft Edge for Business to improve authentication security in your PingOne DaVinci flow.



Microsoft Teams

Microsoft Teams Connector

The Microsoft Teams connector lets you manage user memberships and send messages in Microsoft Teams from your PingOne DaVinci flow.



OIDC and OAuth IdP Connector

The OIDC and OAuth IdP connector lets you authenticate users with an IdP that supports OpenID Connect 1.0 or OAuth 2.0 in your PingOne DaVinci flow.

OneTrust

PRIVACY, SECURITY & GOVERNANCE

OneTrust Connector

The OneTrust connector lets you use OneTrust to manage receipts for user consent in your PingOne DaVinci flow.

Marketo Connector

The Marketo connector lets you add, search, and update leads into Marketo in your PingOne DaVinci flow.

You can use the Marketo connector to:

- Manage leads in Marketo
- Manage lists in Marketo

Setup

Resources

For information and setup help, see the following:

- Marketo documentation:
 - [Marketo Setup Steps](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A Marketo license

- Your Marketo credentials

Setting up Marketo

Follow the instructions in [Marketo Setup Checklist](#).

Configuring the Marketo connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

API URL

The API endpoint for your Adobe Marketo instance, for example, `abc123.mktorest.com/rest`

Client ID

Your Adobe Marketo client ID

Client Secret

Your Adobe Marketo client secret

Using the connector in a flow

Lead management

The connector has several capabilities that allow you to manage users:

- Create Lead
- Read Lead
- Update Lead
- Search Lead

No special configuration is needed. Add the capability and populate its properties according to the help text.

List Management

The connector has several capabilities that allow you to manage lists:

- **Create Static List**
- **Get List Information**
- **Read Static List Leads**
- **Add Leads to List**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Create Lead

Create a new lead.

Properties

First Name textField

The user's first name.

Middle Name textField

The user's middle name.

Last Name textField

The user's last name.

Email textField required

The user's email address.

Phone Number textField

The user's phone number.

Custom Attributes keyValueList

Additional attributes.

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result object
 - id string
 - status string
 - success string
 - statusCode number
 - headers object

Create Static List

Create a new static list.

Properties

List Name textField required

Enter a name for the new list.

Output Schema

- output object
 - rawResponse object
 - result object
 - id number
 - name string
 - createdAt date
 - updatedAt date
 - folder object
 - id number
 - type string
 - name string
 - computedUrl string
 - statusCode number
 - headers object

Get List Information

Get information about one or more lists using the list ID, name, or folder.

Properties

Search Type dropDown required

Select "Use List ID" or "Use List Name" to get information about a single list, or select a folder to get information about all lists within it.

- Use Folder Name (Default)
- Use List ID
- Use List Name

Folder dropDown required

Select the folder that contains the lists you want information about.

List Name textField

The name of the list to get information about, such as "Founders".

List Type dropDown

Select the type of list you are reading. Smart lists support additional accuracy and functionality.

- Static List (Default)
- Smart List (Default)

List ID textField required

The unique ID for the list, such as "56789".

Output Schema

- output object
 - rawResponse object
 - result array
 - statusCode number
 - headers object

Read Lead

Read a lead using the lead ID.

Properties

Lead ID textField required

The unique identifier for the lead, such as "318581".

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result object
 - id string
 - email string
 - firstName string
 - lastName string
 - updatedAt string
 - createdAt string
 - success string
 - statusCode number
 - headers object

Update Lead

Update an existing lead using the lead ID.

Properties

Lead ID textField required

The unique identifier for the lead, such as "318581".

First Name textField

The user's first name.

Middle Name textField

The user's middle name.

Last Name textField

The user's last name.

Email textField required

The user's email address.

Phone Number textField

The user's phone number.

Custom Attributes keyValueList

Additional attributes.

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result array
 - success string
 - statusCode number
 - headers object

Search Leads

Search for one or more leads.

Properties

Search Attribute dropDown required

Select the Marketo lead attribute that you want to search.

- Cookies
- Department
- Email
- Email Suspended Cause
- External Company ID
- External Sales Person ID
- ID
- Lead Partition ID
- Marketo Name

Search Values textField required

Enter the values to look for in the search attribute. Separate multiple values with a comma, such as "138273,[jsmith@example.com](#)".

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result array
 - success string
 - statusCode number
 - headers object

Read Static List Leads

Read leads in a static list using the list ID.

Properties

List ID textField required

The unique ID for the list, such as "56789".

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result array
 - success string
 - statusCode number
 - headers object

Add Leads to List

Add leads to a list using lead IDs.

Properties

List ID textField required

The unique ID for the list, such as "56789".

Lead IDs textField required

Enter the unique ID of the leads to add to the list. Separate multiple values with a comma, such as "456123,987654".

Output Schema

- output object
 - rawResponse object
 - result object
 - requestId string
 - result array
 - success string
 - statusCode number
 - headers object

Make Custom API Call

Define and use your own call to Adobe Marketo.

Properties

Custom Endpoint textField required

This endpoint is added to the base API URL selected in the connector configuration. Remember to remove "rest/" from the endpoint

HTTP Method dropdown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE
- PATCH

Query Parameters keyValuePairList

Query parameters for the request.

Additional Headers keyValuePairList

Define additional headers to send to Adobe Marketo. For help, see the API documentation.

Body codeEditor

The body of the API call.

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

Microsoft Edge for Business Connector

The Microsoft Edge for Business connector lets you use Microsoft Edge for Business to improve authentication security in your PingOne DaVinci flow.

Microsoft Edge for Business is a secure, high-performance browser built for enterprise needs, offering enhanced productivity, AI-powered features, and native integration with Microsoft 365—designed to protect corporate data while supporting modern workplace demands.

You can use the Microsoft Edge for Business connector to include operating system device signals collected by Microsoft Edge for Business in a PingOne DaVinci flow.

Setup

Resources

You can find information and setup help in the following:

- Microsoft Edge for Business documentation
 - <https://www.microsoft.com/en-us/edge/business/?form=MA13Fj>
 - [Register an application in Microsoft Entra ID](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- Administrator access to Microsoft Azure
- An Azure App Registration for the Microsoft Edge for Business Device Trust integration.
- Administrator access to Microsoft 365 admin center for Microsoft Edge for Business policy configuration.

Setting up Microsoft Edge for Business

To use the connector, you'll need:

- Administrator access to Microsoft Azure
- An Azure App Registration for the Microsoft Edge for Business Device Trust integration.
- Administrator access to Microsoft 365 admin center for Microsoft Edge for Business policy configuration.

To set up Azure App Registration:

1. Sign on to the [Azure portal](#).
2. Create the application:
 1. Search for and select **Azure Active Directory**.
 2. Under **Manage**, select **App registrations** > **New registration**.

3. Register a new **Application**.
 4. Select the application you registered in the previous step.
 5. On the **App Registration** page for the new application, configure the permissions required to allow the application to access the Device Trust API.
 6. On the **APIs my organization uses** tab, search for the **Microsoft Edge management service**.
 7. Select **Application permissions** and add the **DeviceTrust.Read.All** permission.
 8. Click the **Grant admin consent confirmation**.
 9. Click **Register**.
3. On your app's **Overview** page, note the **Application (client) ID** and **Directory (tenant) ID**. You'll use these in the connector configuration.

The screenshot shows the Microsoft Azure portal interface for the 'PingOne DaVinci' application. The breadcrumb navigation indicates the path: Home > Ping Identity | App registrations > PingOne DaVinci. Below the application name, there are links for 'Delete', 'Endpoints', and 'Preview features'. A feedback banner is present. The 'Essentials' section lists the following details:

- Display name: [PingOne DaVinci](#)
- Application (client) ID: **5db65414-a030-4082-852c-213aef4329f2**
- Object ID: **e4ba22d4-7815-4239-9d12-93ec4efdf943**
- Directory (tenant) ID: **07ec9af2-7ce5-4ab7-8638-115736bbf990**
- Supported account types: [All Microsoft account users](#)

4. Create a client secret:
1. Under **Manage**, click **Certificates & secrets**.
 2. On the **Client secrets** tab, click **New client secret**.
 3. Enter a name and select an expiry time. Click **Add**.
 4. Note the **Value** of the secret. You'll use this in the connector configuration.

Certificates (0) <u>Client secrets (1)</u> Federated credentials (0)			
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.			
+ New client secret			
Description	Expires	Value ⓘ	Secret ID
DaVinci	8/10/2024	jMD8Q~GwvnrWLnj~p30nc0N ...	5c0e4e15-a241-4e12-860c-cb ...

To configure Edge for Business for PingOne DaVinci:

1. Sign on to **Microsoft 365 admin center**.
2. Go to the Microsoft Edge configuration.
3. On the **Connectors** tab, click **Set up** under the Ping Identity Device Trust feature.
4. In the right panel, enter the following PingOne DaVinci domains:
 - auth.pingone.com
 - auth.pingone.ca
 - auth.pingone.eu
 - auth.pingone.asia
 - auth.pingone.au
5. Click **Save Configuration**

The Microsoft Edge for Business Device Trust is now configured.

Configuring the Microsoft Edge for Business connector

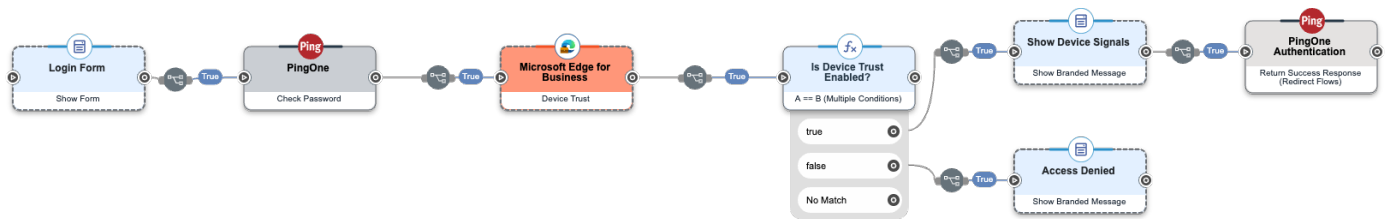
1. [Add the connector in DaVinci](#).
2. Configure it as follows:
 - **Azure Tenant ID:** The tenant ID of your Microsoft Azure Tenant.
 - **Client ID:** The client ID you created in Setting up Microsoft Edge for Business.
 - **Client Secret:** The client secret you created in Setting up Microsoft Edge for Business.

Using the connector in a flow

Device Trust

The **Device Trust** capability allows PingOne DaVinci to receive the Microsoft Edge for Business Device Signals, which include device attributes such as Serial Number, MAC Addresses, and Hostname. If the CrowdStrike agent is installed, the CrowdStrike agent ID is also included.

The following is an example of a PingOne DaVinci flow that blocks access to users who are not using the expected Microsoft Edge for Business enrolled browser:



Capabilities

Device Trust

Authenticate against Microsoft Edge for Business Device Trust API

Input Schema

- default object
 - properties object

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object
 - deviceTrustEnabled boolean
 - deviceId string
 - tenantId string
 - profileKeyTrustLevel string
 - keyTrustLevel string
 - deviceSignals object
 - browserVersion string
 - builtInDnsClientEnabled boolean
 - crowdStrikeAgent object
 - agentId string
 - customerId string
 - deviceManufacturer string
 - deviceModel string
 - diskEncrypted string
 - displayName string
 - hostname string
 - imei array
 - meid array
 - macAddresses array
 - operatingSystem string
 - osFirewall string
 - osVersion string
 - passwordPotentionWarningTrigger string
 - realtimeUrlCheckMode string
 - screenLockSecured string

- secureBootEnabled string
- serialNumber string
- sitelsolationEnabled boolean
- systemDnsServers array
- trigger string
- windowsUserDomain string

Microsoft Teams Connector

The Microsoft Teams connector lets you manage user memberships and send messages in Microsoft Teams from your PingOne DaVinci flow.

You can use the Microsoft Teams connector to:

- Add, remove, and list members of a team
- Add, remove, and list members of a channel
- Send messages in channels and chats
- Define custom API calls to Microsoft Azure

Setup

Resources

For information and setup help, see the following:

- Microsoft documentation:
 - [Register an application with the Microsoft identity platform](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

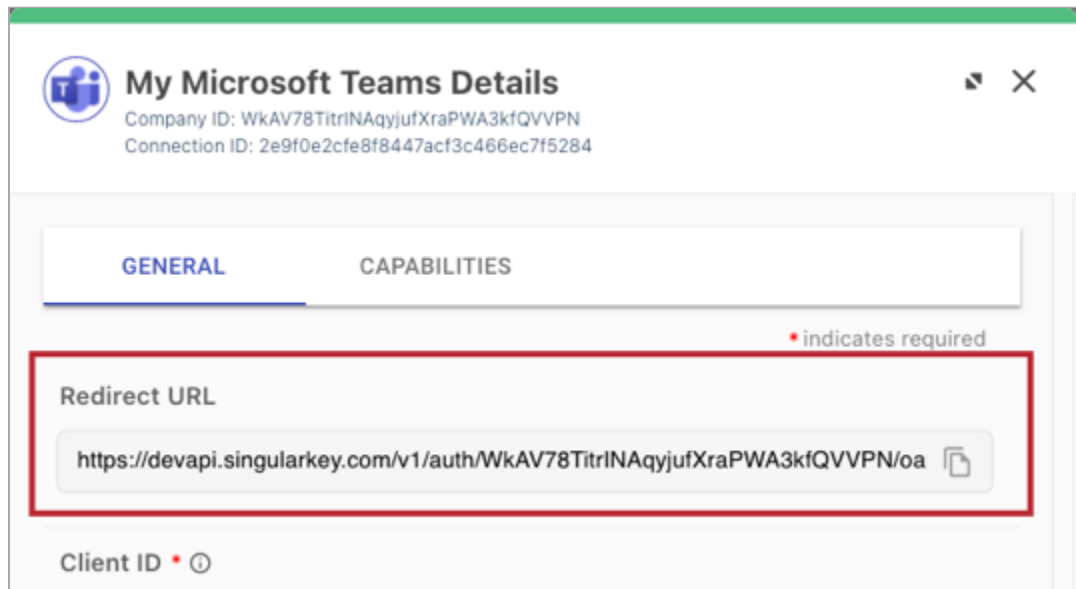
- A Microsoft Teams account
- Administrator access to Microsoft Azure

Setting up Microsoft Teams

1. Sign on to the [Azure portal](#).
2. Create the application:
 1. Search for and select **Azure Active Directory**.
 2. Under **Manage**, select **App registrations** → **New registration**.
 3. On the **Register an Application** page, for **Supported account types**, select **Accounts in any organizational directory and personal Microsoft accounts**.
 4. In the **Redirect URI** section, select **Web** and add the redirect URL for your DaVinci environment, such as:

```
https://auth.pingone.com/79d0edb0-4421-1bcb-acb5-222e3132eb5b/davinci/oauth2/callback
```

To get your redirect URL, add a **Microsoft Teams** connection in DaVinci, open the connection settings, and copy the **Redirect URL**. For help adding the connection, see [Adding a connector](#).



5. Click **Register**.
3. On your app's **Overview** page, note the **Application (client) ID** and **Directory (tenant) ID**. You'll use these in the connector configuration.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header with the Microsoft Azure logo and a search bar. Below the header, the breadcrumb navigation shows 'Home > Ping Identity | App registrations >'. The main heading is 'PingOne DaVinci'. Below this, there are three tabs: 'Delete', 'Endpoints', and 'Preview features'. A notification banner asks for feedback on the Microsoft identity platform. Under the 'Essentials' section, the following details are listed:

- Display name: [PingOne DaVinci](#)
- Application (client) ID: **5db65414-a030-4082-852c-213aef4329f2**
- Object ID: **e4ba22d4-7815-4239-9d12-93ec4efd943**
- Directory (tenant) ID: **07ec9af2-7ce5-4ab7-8638-115736bbf990**
- Supported account types: [All Microsoft account users](#)

4. Create a client secret:

1. Under **Manage**, click **Certificates & secrets**. On the **Client secrets** tab, click **New client secret**.
2. Enter a name and select an expiry time. Click **Add**.
3. Note the **Value** of the secret. You'll use this in the connector configuration.

The screenshot shows the 'Client secrets' tab in the Azure portal. It displays a table with columns: Description, Expires, Value, and Secret ID. A new client secret has been created with the description 'DaVinci', an expiry date of '8/10/2024', and a value that is partially visible and truncated. The Secret ID is '5c0e4e15-a241-4e12-860c-cb ...'. There are icons for copying and deleting the secret.

Description	Expires	Value	Secret ID
DaVinci	8/10/2024	jMD8Q~GwvnrWLnj~p30nc0N ...	5c0e4e15-a241-4e12-860c-cb ...

5. Give the connector permission to manage users and send messages:

1. Under **Manage**, click **API permissions**.
2. Click **Add a permission** and add the following Microsoft Graph API permissions:

Type	Permission
Delegated	User.Read

Type	Permission
Delegated	ChannelMessage.Send
Delegated	Chat.ReadWrite
Delegated	ChatMessage.Send
Delegated	offline_access
Application	ChannelMember.ReadWrite.All
Application	ChannelSettings.ReadWrite.All
Application	Chat.ReadWrite.All
Application	Group.Read.All
Application	TeamMember.ReadWrite.All
Application	User.ReadWrite.All

Configuring the Microsoft Teams connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

DaVinci Redirect URL

Your DaVinci redirect URL. This allows Microsoft to redirect the browser back to DaVinci, after the user authenticates with the **Sign on with Microsoft** capability. Use this in [Setting up Microsoft Teams](#).

Application Redirect URL

Your application's redirect URL, such as <https://app.yourorganization.com>. Enter this URL if you embed the DaVinci widget in your application. This allows DaVinci to redirect the browser back to your application.

Client ID

The **Application (client) ID** that you noted in [Setting up Microsoft Teams](#).

Client Secret

The client secret **Value** that you noted in [Setting up Microsoft Teams](#).

Tenant ID

The **Directory (tenant) ID** that you noted in [Setting up Microsoft Teams](#).

Using the connector in a flow

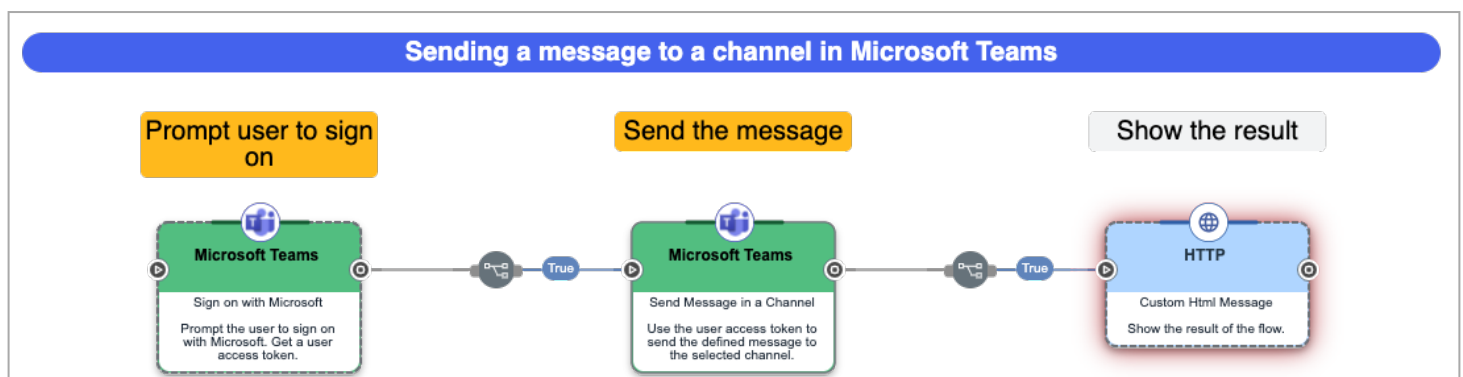
Managing team and channel memberships

The connector has several capabilities that allow you to manage the users that belong to each team or channel in Microsoft Teams:

- Teams:
 - Add a Member to a Team
 - Remove a Member from a Team
 - List Team Members
- Channels:
 - Add a Member to a Channel
 - Remove a Member from a Channel
 - List Channel Members

No special configuration is needed. Add the capability and populate its properties according to the help text.

Sending a message to a channel

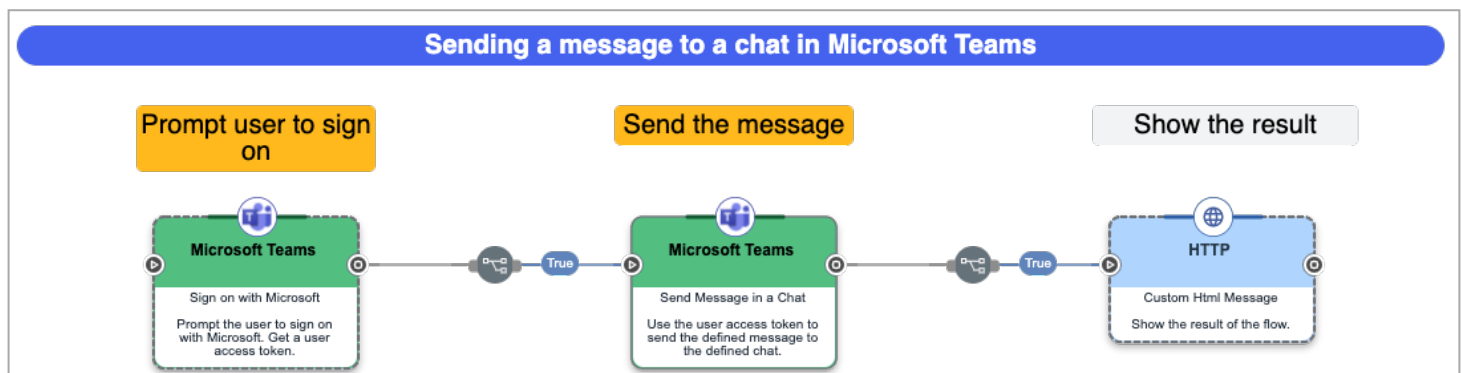


You can use the connector to send a message to a channel.

This flow requires the user to sign on with Microsoft and agree to let the connector send messages on their behalf. The **Sign on with Microsoft** node directs the browser to Microsoft. After the user signs on, Microsoft redirects the browser back to DaVinci to continue the flow.

1. Download the [Microsoft Teams Channel Message](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Select the **Send Message in Channel** node.
3. In the **Team** list, select the team associated with the channel or select **Use Team ID** and enter an ID in the **Team ID** field, such as `98c28bef-98f1-a658-435b-71eee19c8f5e`.
4. In the **Channel** list, select the channel or select **Use Channel ID** and enter an ID in the **Channel ID** field, such as `98c28bef-a658-435b-98f1-71eee19c8f5e`.
5. Click **Apply**.
6. Test the flow:
 1. Click **Save**, **Deploy**, and **Try Flow**.
 2. In Microsoft Teams, check the channel to see the message.

Sending a message to a chat



You can use the connector to send a message to a chat.

This flow requires the user to sign on with Microsoft and agree to let the connector send messages on their behalf. The **Sign on with Microsoft** node directs the browser to Microsoft. After the user signs on, Microsoft redirects the browser back to DaVinci to continue the flow.

The flow also requires a chat ID. For help getting a chat ID, see [Listing a User's Chats](#).

1. Download the [Microsoft Teams - Chat message](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Select the **Send a Message in a Chat** node.
3. In the **Chat ID** field, enter the unique ID of one of the user's chats, such as `19:ce95abaa0e9f4d22a0e0faa6aad76c56@thread.v2`. For help getting a chat ID, see [Listing a User's Chats](#).
4. In the **Message Object** field, create a JSON object with the message details. This allows you to use all features supported by the Microsoft Graph API, such as HTML formatting, user @mentions, and file attachments.

For example:

```
{
  "body": {
    "contentType": "html",
    "content": "Welcome, <at id=\"0\">Jane Smith</at>"
  },
  "mentions": [
    {
      "id": 0,
      "mentionText": "Jane Smith",
      "mentioned": {
        "user": {
          "displayName": "Jane Smith",
          "id": "19:ce95abaa0e9f4d22a0e0faa6aad76c56@thread.v2",
          "userIdentityType": "aadUser"
        }
      }
    }
  ]
}
```

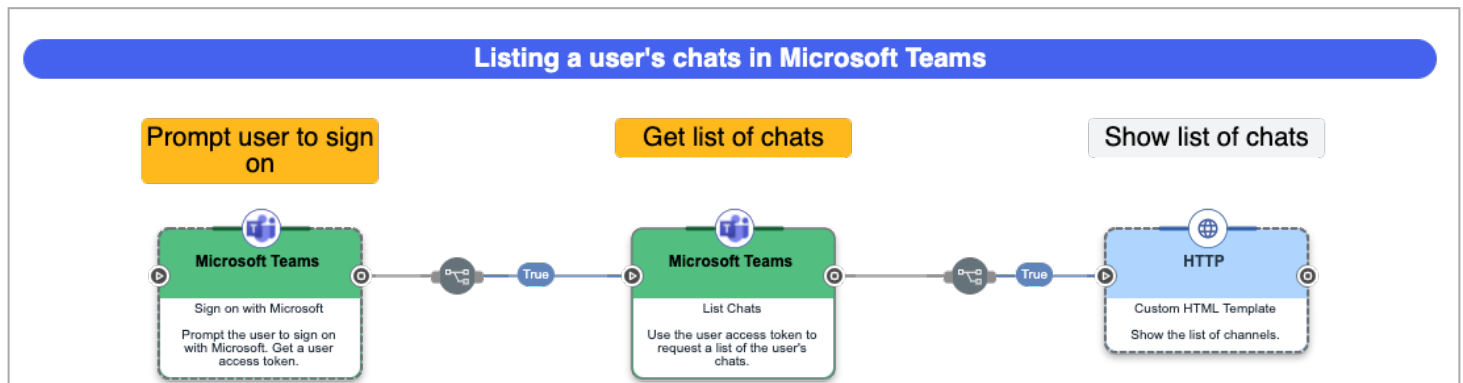
For help creating the JSON object, see [Chat message](#) in the Microsoft Graph API documentation.

5. Click **Apply**.

6. Test the flow:

1. Click **Save, Deploy, and Try Flow**.
2. In Microsoft Teams, check the chat to see the message.

Listing a user's chats



You can use the connector to get a list of chats that the user belongs to. You can use the chat IDs from this flow to send messages to specific chats.

Download the [Microsoft Teams - Chat list](#) flow template. For help, see [Using DaVinci flow templates](#).

This flow requires the user to sign on with Microsoft and agree to let the connector send messages on their behalf. The **Sign on with Microsoft** node directs the browser to Microsoft. After the user signs on, Microsoft redirects the browser back to DaVinci to continue the flow.

The **Custom HTML Message** node shows a list of chats. You can copy a chat ID to send messages to that chat on behalf of the user.

List of chats

To use the **Send a Message in a Chat** capability:

1. Copy the id value of the chat that you want to target.
2. In the **Microsoft Teams - Send a Message in a Chat** flow template, paste the chat ID in the **Chat ID** field of the **Send a Message in a Chat** node.

```
{
  "rawResponse": {
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#chats",
    "@odata.count": 3,
    "value": [
      {
        "id": "19:ce95abaa0e9f4d22a0e0fea6aad76c56@thread.v2",
        "topic": "testGroupChat2",
        "createdDateTime": "2022-07-27T18:26:35.108Z",
        "lastUpdatedDateTime": "2022-07-27T18:26:35.108Z",
        "chatType": "group",
        "webUrl": "https://teams.microsoft.com/l/chat/19%3Ace95abaa0e9f4d22a0e0",
        "tenantId": "07ec9af2-7ce5-4ab7-8638-115736bbf990",
        "onlineMeetingInfo": null
      },
      {
        "id": "19:c0333d23441046c6a8eba678c970f06d@thread.v2",
        "topic": null,
        "createdDateTime": "2022-07-07T17:38:58.375Z",
        "lastUpdatedDateTime": "2022-08-22T16:15:06.425Z",
        "chatType": "group",
        "webUrl": "https://teams.microsoft.com/l/chat/19%3Ac0333d23441046c6a8eb",
        "tenantId": "07ec9af2-7ce5-4ab7-8638-115736bbf990",
        "onlineMeetingInfo": null
      }
    ]
  }
}
```

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connection to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Add a Member to a Team

Add a member to a team and assign a display name.

Properties

Member dropDown required

The member to target. For a dynamic value, select Use Member ID and enter a value in the Member ID field.

- Use Member/Membership ID

Member ID textField

The ID of the member, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Roles textFieldArrayView

The roles to assign to the member, such as "owner" or "guest". Basic members should not have any assigned roles. Type a role name and press Enter to add it.

Display Name textField

The display name to assign to the member.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - members string required
 - memberId string
 - teams string required
 - teamId string
 - roles array
 - displayName string

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - @odata.type string
 - id string
 - roles array
 - displayName string
 - visibleHistoryStartDateTime string
 - userId string
 - email string
 - tenantId string
 - statusCode integer
 - headers object
 - transfer-encoding string
 - content-type string
 - location string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Remove a Member from a Team

Remove a member from team.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Member dropDown required

The member to target. For a dynamic value, select Use Member ID and enter a value in the Member ID field.

- Use Member/Membership ID

Membership ID textField

The ID of the membership, such as

"MCMjMSMjMDdlYzlhZjltN2NINS00YWl3LTg2MzgtMTE1NzM2YmJmOTkwlyM5OGMyOGJlZi05OGYxLTQzNWItYTl1OC03MWVIZT

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - members string required
 - membershipId string
 - teams string required
 - teamId string

Output Schema

- output object
 - rawResponse string
 - statusCode integer
 - headers object
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - date string
 - connection string

List Team Members

Get a list of members of a team.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - teams string required
 - teamId string

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - @odata.count integer
 - value array
 - Array Item Schema object
 - @odata.type string
 - id string
 - roles array
 - displayName string
 - visibleHistoryStartDateTime string
 - userId string
 - email null/string
 - tenantId string
 - statusCode integer
 - headers object
 - transfer-encoding string
 - content-type string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Add a Member to a Channel

Add a member to a channel and assign a display name.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Channel dropDown required

The channel to target. For a dynamic value, select Use Channel ID and enter a value in the Channel ID field.

- Use channel ID

Channel ID textField required

The ID of the channel to target, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Member dropDown required

The member to target. For a dynamic value, select Use Member ID and enter a value in the Member ID field.

- Use Member/Membership ID

Member ID textField

The ID of the member, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Roles textFieldArrayView

The roles to assign to the member, such as "owner" or "guest". Basic members should not have any assigned roles. Type a role name and press Enter to add it.

Display Name textField

The display name to assign to the member.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - teams string required
 - teamId string
 - channels string required
 - channelId string
 - members string required
 - memberId string
 - roles array
 - displayName string

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - @odata.type string
 - id string
 - roles array
 - displayName string
 - visibleHistoryStartDateTime string
 - userId string
 - email string
 - tenantId string
 - statusCode integer
 - headers object
 - transfer-encoding string
 - content-type string
 - location string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Remove a Member from a Channel

Remove a member from a channel.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Channel dropDown required

The channel to target. For a dynamic value, select Use Channel ID and enter a value in the Channel ID field.

- Use channel ID

Channel ID textField required

The ID of the channel to target, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Member dropDown required

The member to target. For a dynamic value, select Use Member ID and enter a value in the Member ID field.

- Use Member/Membership ID

Membership ID textField

The ID of the membership, such as

"MCMjMSMjMDdlYzlhZjltN2NINS00YWI3LTg2MzgtMTE1NzM2YmJmOTkwlyM5OGMyOGJlZi05OGYxLTQzNWItYTY1OC03MWWIZT

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - teams string required
 - teamId string
 - channels string required
 - channelId string
 - members string required
 - membershipId string

Output Schema

- output object
 - rawResponse string
 - statusCode integer
 - headers object
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - date string
 - connection string

List Channel Members

Get a list of members in a channel.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Channel dropDown required

The channel to target. For a dynamic value, select Use Channel ID and enter a value in the Channel ID field.

- Use channel ID

Channel ID textField required

The ID of the channel to target, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - teams string required
 - teamId string
 - channels string required
 - channelId string

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - @odata.count integer
 - value array
 - Array Item Schema object
 - @odata.type string
 - id string
 - roles array
 - Array Item Schema string
 - displayName string
 - visibleHistoryStartDateTime string
 - userId string
 - email string
 - tenantId string
 - statusCode integer
 - headers object
 - transfer-encoding string
 - content-type string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Send Message in a Channel

Send a message in a channel on behalf of a user.

Properties

Team dropDown required

The team to target. For a dynamic value, select Use Team ID and enter a value in the Team ID field.

- Use team ID

Team ID textField

The ID of the team, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

Channel dropDown required

The channel to target. For a dynamic value, select Use Channel ID and enter a value in the Channel ID field.

- Use channel ID

Channel ID textField required

The ID of the channel to target, such as "0b2b7c5b-4eb2-5c7b-a94b-bea34ac31c30".

User Access Token textField

The user's access token. This token is provided by the Sign on with Microsoft capability.

Message Object textArea

The JSON object that contains the message body. For help, see "Chat message" in the Microsoft Graph REST API documentation.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - teams string required
 - teamId string
 - channels string required
 - channelId string
 - userAccessToken string required
 - messageBodyData string required

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - id string
 - replyTold string
 - etag string
 - messageType string
 - createdDateTime string
 - lastModifiedDateTime string
 - lastEditedDateTime string
 - deletedDateTime string
 - subject string
 - summary string
 - chatId string
 - importance string
 - locale string
 - webUrl string
 - policyViolation string
 - eventDetail string
 - from object
 - application string
 - device string
 - user object
 - id string
 - displayName string
 - userIdentityType string
 - body object
 - contentType string
 - content string

- channelId object
 - teamId string
 - channelId string
- attachments array
- mentions array
- reactions array
- statusCode integer
- headers object
 - transfer-encoding string
 - content-type string
 - location string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Send Message in a Chat

Send a message in a chat on behalf of a user.

Properties

User Access Token textField

The user's access token. This token is provided by the Sign on with Microsoft capability.

Chat ID textField

The ID of the chat, such as "19:ce95abaa0e9f4d22a0e0faa6aad76c56@thread.v2".

Message Object textArea

The JSON object that contains the message body. For help, see "Chat message" in the Microsoft Graph REST API documentation.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - chatId string required
 - userAccessToken string required
 - messageBodyData string required

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - id string
 - replyTold string
 - etag string
 - messageType string
 - createdDateTime string
 - lastModifiedDateTime string
 - lastEditedDateTime string
 - deletedDateTime string
 - subject string
 - summary string
 - chatId string
 - importance string
 - locale string
 - webUrl string
 - channelId string
 - policyViolation string
 - eventDetail string
 - from object
 - application string
 - device string
 - user object
 - id string
 - displayName string
 - userIdentityType string
 - body object
 - contentType string

- content string
- attachments array
- mentions array
- reactions array
- statusCode integer
- headers object
 - transfer-encoding string
 - content-type string
 - location string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

List Chats

Get a list of chats for a user.

Properties

User Access Token textField

The user's access token. This token is provided by the Sign on with Microsoft capability.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - userAccessToken string required

Output Schema

- output object
 - rawResponse object
 - @odata.context string
 - @odata.count integer
 - value array
 - Array Item Schema object
 - id string
 - topic string
 - createdDateTime string
 - lastUpdatedDateTime string
 - chatType string
 - webUrl string
 - tenantId string
 - onlineMeetingInfo string
 - statusCode integer
 - headers object
 - transfer-encoding string
 - content-type string
 - strict-transport-security string
 - request-id string
 - client-request-id string
 - x-ms-ags-diagnostic string
 - odata-version string
 - date string
 - connection string

Sign on with Microsoft

Redirect the browser and prompt the user to authenticate with Microsoft. This creates a token needed to list the user's chats or send messages as the user.

Properties

Display Name button
showPoweredBy toggleSwitch
skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required

Output Schema

- output object
 - rawResponse object
 - token_type string
 - scope string
 - expires_in integer
 - ext_expires_in integer
 - access_token string
 - refresh_token string
 - statusCode integer
 - headers object
 - cache-control string
 - pragma string
 - content-type string
 - expires string
 - strict-transport-security string
 - x-content-type-options string
 - p3p string
 - x-ms-request-id string
 - x-ms-ests-server string
 - x-xss-protection string
 - set-cookie array
 - Array Item Schema string
 - Array Item Schema string
 - Array Item Schema string
 - date string
 - connection string
 - content-length string
 - tokens string
 - connectionId string

◦ connectorId string

Make a Custom API Call

Define and use your own call to the Microsoft Team REST API

Properties

Endpoint textField required

The API endpoint, such as "https://admin.googleapis.com/admin/directory/v1/users/user@example.com".

HTTP Method dropDown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE

Query Parameters keyValuePairList

Query parameters for the request.

Additional Headers keyValuePairList

Define additional headers to send to Microsoft Teams. For help, see the API documentation.

Body codeEditor

The body of the API call.

Input Schema

- default object
 - properties object
 - clientId string required
 - clientSecret string required
 - tenantId string required
 - endpoint string required
 - method string required

Output Schema

- output object
 - rawResponse object
 - statusCode integer
 - headers object

OIDC and OAuth IdP Connector

The OIDC and OAuth IdP connector lets you authenticate users with an identity provider (IdP) that supports OpenID Connect (OIDC) or OAuth 2.0 in your PingOne DaVinci flow.

You can use the OIDC and OAuth IdP connector to authenticate users with an IdP.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#) 
 - [Using connectors securely](#) 
 - [Using DaVinci flow templates](#) 

Configuring the OIDC and OAuth IdP connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Provider Name

The name of the IdP.

Auth Type

The authorization or authentication type, such as **OAuth2** or **OpenId**.

Redirect URL

Include this URL in your IdP configuration to allow it to redirect the browser back to DaVinci. If you use a custom PingOne domain, modify the URL accordingly.

Issuer URL

If **OpenId** is selected as the **Auth Type**, include this URL, which contains information about the IdP that can be validated.

Authorization Endpoint

The IdP endpoint, such as `/rest/api/3``. This endpoint is added to the base API URL selected in the connector endpoint configuration.

Token Endpoint

The IdP token endpoint, which is used to request or refresh tokens.

Token Attachment

If a token is attached, prepend its name with either `bearer` or `token` , as appropriate.

UserInfo Endpoint

The IdP endpoint, which returns information about an authenticated user.

App ID

The unique identifier for an IdP tenant.

Client Secret

The IdP secret, which the application must have to obtain a token.

Scope

The OIDC scope used during authentication to authorize access to user information. Separate scopes with a space. For example, enter `openid email profile` .

User Info Post Process

The code that contains information about an authenticated user using HTTP POST.

Application Return to URL

The URL that returns user to the application after an embedded flowplayer video has played or social login authentication is complete.

Using the connector in a flow

OIDC or OAuth authentication

You can use the **Sign On** capability to authenticate a user with OIDC or OAuth2.

User information collection

You can use the **Get User Details** capability to validate an ID token.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Access token management

The connector has several capabilities to manage access tokens:

- **Get Access Token (Client Credentials Grant)**
- **Get Access Token (Password Credentials Grant)**

Capabilities

Sign On

Properties

Sign On button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Output Schema

oauth2 object

accessToken string

expiresIn string

Get User Details

Properties

Sign On button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Get Access Token (Client Credentials Grant)

Input Schema

default object

type object

additionalProperties additionalProperties: true

Get Access Token (Password Credentials Grant)

Properties

Username textField required

Password textField required

Input Schema

default object

username string required

password string required

OneTrust Connector

The OneTrust connector lets you use OneTrust to manage receipts for user consent in your PingOne DaVinci flow.

Using OneTrust as part of your user privacy and data governance solution, this connector lets you track whether a user has consented to a specific document, such as your terms and conditions. Specifically, the connector can create a consent receipt or get an existing consent receipt.

Setup

Resources

For information and setup help, see the following:

- OneTrust documentation (sign on required)
 - [Consent Management](#)
 - [Managing OAuth 2.0 Client Credentials](#)
 - [Managing OAuth 2.0 API Keys](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a OneTrust license.

Setting up OneTrust consent management

1. Set up consent management in OneTrust as shown in [Consent Management](#).

For your Collection Point, use the following settings:

- Choose the **Custom API** type.
- On the **Collection Points** → *<your collection point>* → **Settings** tab, turn on **Enable Consent Withheld Transactions on this Collection Point**.

2. Create client credentials as shown in [Managing OAuth 2.0 Client Credentials](#), with the following settings:

- **Access Token Lifetime: 1 hour**
- **Restrict IP Addresses: Off**
- **Scopes:**
 - **CONSENT**
 - **CONSENT_READ**

Note your client ID and secret. You'll use them to set up the connector configuration.

Configuring the OneTrust connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Client ID

The client ID you created in [Setting up OneTrust consent management](#).

Client Secret

The client secret you created in [Setting up OneTrust consent management](#).

Setting up PingOne

The example flows below use the PingOne user directory to store consent receipts. To use the provided flow templates:

- 1. If you don't have an existing PingOne connection in DaVinci, set up the [PingOne connector](#), including the required PingOne setup.
- 2. In PingOne, add a user attribute to hold a list of the user's consent receipts. For help, see [Adding user attributes](#). Use the following details:
 - **Attribute Type:** JSON
 - **Name:** consentReceipts
 - Select **Allow multiple values**

Setting up OneTrust URL variables in DaVinci

The flow templates provided below use variables to populate your organization's OneTrust URLs.

To use the flow templates, set the following variables in DaVinci.



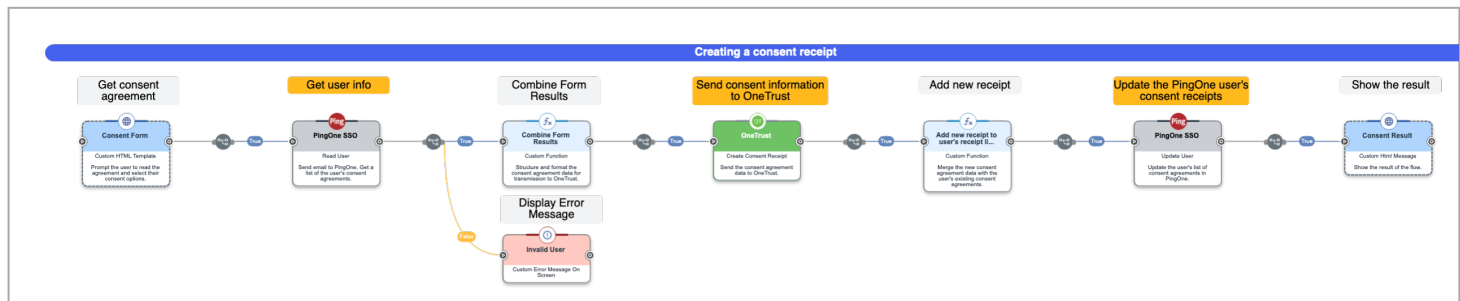
Note

For help, see [Adding a variable](#) in the DaVinci documentation.

Name	Variable Context	Data Type	Example Value
oneTrustPrivacyPortalDomain	string	company	https://yourorganization-privacy.my.onetrust.com
oneTrustApplicationDomain	string	company	https://yourorganization.my.onetrust.com
oneTrustDataSubjectPortal	string	company	https://yourorganization-privacy.my.onetrust.com

Using the connector in a flow

Creating a consent receipt



This flow collects the user's consent and user ID, checks that the user account exists, and sends the consent and user information to OneTrust. After OneTrust generates a consent receipt, the flow adds the new receipt to the user's list of existing receipts and updates the user account in `include::partial$common_product_keydefs.adoc[tags=pingone]`.

Note

This flow uses `include::partial$common_product_keydefs.adoc[tags=pingone]` as an example user directory. You can modify the flow to use a different directory.

1. Download the [OneTrust - New consent receipt](#) flow template. For help, see [Using DaVinci flow templates](#).

2. Customize the consent form:

1. Select the **Consent Form** node.
2. In the **HTML Template** field, modify the HTML to include the text of the terms and conditions (or other document) that you want consent for, and modify the example form controls to show the relevant "purposes", "options", and "custom preferences" in your OneTrust consent management scheme.

Tip

- Click **Switch View** to see the HTML formatted with syntax highlighting.
- Click the **Maximize** (⌵) icon to give yourself more room to work.
- To access a variety of useful tools, right-click the field when you're in syntax highlighting mode (dark background).

3. In the **Output Fields List** section, edit the **Property Name** of the purposes, options, and custom preferences to match the element IDs of the purposes and options you included in the HTML form. Remove any unwanted properties by clicking **Edit** at the end of the list.

4. Click **Apply**.

3. Add the IDs for your OneTrust purposes, options, and custom preferences.

Note

The flow uses a custom function to match the consent form inputs with the IDs of your OneTrust consent management elements. The function then builds a **purposes** object that is ready to send to OneTrust.

1. In OneTrust, get the **id** value for each purpose, option, and custom preference you want to use:

1. Go to the OneTrust **Universal Consent & Preference Management** portal. For example, <https://company.my.onetrust.com/consent>.
2. For purposes, see **Purposes** → *<your purpose>* → **Details** → **Purpose ID**.
3. For custom preferences, see **Purposes** → *<your purpose>* → **Custom Preferences** → **ID**. Also, go to **Options** and note the options listed.
4. For options, see **Collection Points** → *<your collection point>* → **Integrations** → **Example Payload**. Match the IDs under **Options** with the options that you noted in the **Custom Preferences** view.

The screenshot shows the 'Custom Preference Details' page in OneTrust. On the left, a JSON payload is displayed:

```

CustomPreferences: [
  {
    "Id": "00e581b4-2a2a-4fa6-b521-4ffd834aa822",
    "Options": [
      "55af8ed4-c546-4d1b-93ac-6bc929aa1fda",
      "efebdac6-4252-41ab-95c1-0dbf76b8a55d",
      "254482e1-fff9-469e-98bc-21f2d3dba973"
    ]
  }
]

```

On the right, the 'Custom Preference Details' table is shown with the 'Options' tab selected. The table lists three options:

Name
Option C
Option D
Option E

Arrows indicate the mapping from the IDs in the JSON payload to the options in the table: the first ID maps to Option C, the second ID maps to Option D, and the third ID maps to Option E.

2. Select the **Combine Form Results** node.

3. In the **Variable Input List** section, edit the **Variable Name** of the purposes, options, and custom preferences to match the **Property Name** in your **Consent Form** node. In the **Value** field, click **{}** and select the matching variable from your **Consent Form** node. Remove any unwanted properties by clicking **Edit** at the end of the list.

4. In the **Code** field, modify the code to use the name and ID of your own purposes, options, and custom preferences and remove unused elements.

5. Click **Apply**.

4. Configure the **OneTrust** node:

1. Select the **OneTrust** node.

2. In the **API Token** field, enter the API token from **Collection Points** → **Integrations** → **Your API Token** in OneTrust.

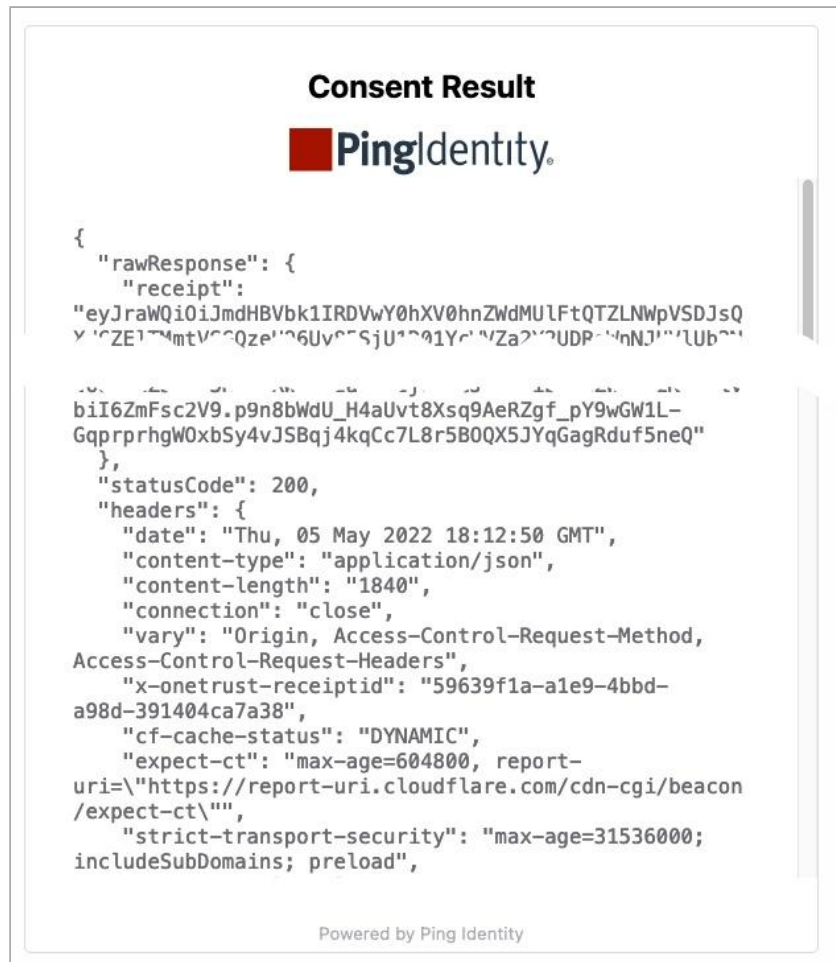
3. Modify the **Additional Data Elements** list to reflect the data elements you included when configuring your collection point in OneTrust. To see the data elements, go to **Collection Points** → **Details** → **Configuration** → **Data Elements**.

4. Click **Apply**.

5. Test the flow:

1. Click **Save**, **Deploy**, then **Run**.

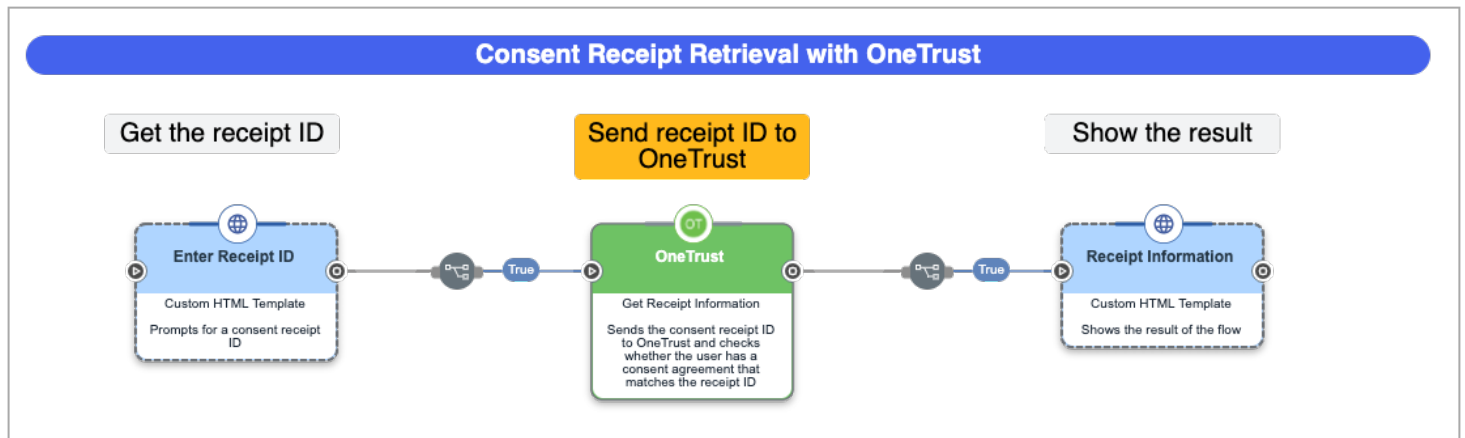
2. On the consent form, enter the email address for one of the identities in your include::partial\$common_product_keydefs.adoc[tags=pingone] directory, select the purposes, options, and custom preferences, then click **I Agree**.
3. See the resulting consent receipt, including the receipt ID.



Tip

Note the value of `x-onetrust-receiptid`. You'll use this to test the "Get information about an existing consent receipt" use case below.

Getting information about an existing consent receipt



You can use a receipt ID to check for an existing consent receipt in OneTrust. This allows you to check whether a user has consented to your terms before using your service, for example.

1. Download the [OneTrust - Consent receipt retrieval](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Test the flow:
 1. Click **Save, Deploy**, then **Run**.
 2. In the **Enter Receipt ID** form, enter the receipt ID that you copied from your test run of the **Creating a consent receipt** flow. Click **Next**.

Enter Receipt ID

RECEIPT ID

56653446-c199-4334-bad3-0ba221d80de1

Next

Powered by Ping Identity

3. See the receipt information.

Receipt Information



```
{
  "rawResponse": {
    "id": "56653446-c199-4334-bad3-0ba221d80de1",
    "otJwtVersion": 1,
    "dataSubjectIdentifierHash":
"a637db09375e04918753afb79c3d4bbdabe2add07fe41dbf8e245
aa50942e8515e8d450ee2ee960076410157a6c6053840a5e92817d
5b4f3a213aeef1dfbe5d6",
    "dataSubjectIdentifier": "johndoe@example.com",
    "collectionPointUUID": "f065f317-dac1-4c75-
a5fe-6e9b575dc241",
    "collectionPointVersion": 4,
    "collectionPointName": "DaVinci",
    "consentCreationDate":
"2022-05-05T21:41:07.462291",
    "receiptJwt":
"eyJraWQiOiJmdHBVbk1IRDVwY0hXV0hnZWdMUlFtQTZLNWpVSDJsQ
XdCZElTMmtVSGQzeU96Uy85SjU1R01YcWVZa2Y2UDRqWnNJUVlUb2N
06Vqp0VLNrwQLLce8H-iLHKjp5JyknDSb/_Wjxc3p14w",
    "customPayload": null,
    "purposes": [
      {
        "id": "8cbb78dc-9283-4a48-9a23-8fe2eb17b30d",
```

Powered by Ping Identity

Capabilities

Create Consent Receipt

Create Receipt from a Collection Point

Properties

Privacy Portal Domain textField required

The URL of your OneTrust Privacy Portal, such as "https://company-privacy.my.onetrust.com".

API Token textField required

Your OneTrust API token.

User Identifier textField required

The unique identifier for the user, such as a username or user ID.

Additional Data Elements keyValueList

Additional information collected about the user.

Purposes textField required

The flow variable that contains the “purposes” to associate with the consent.

Input Schema

- default object
 - properties object
 - privacyPortalDomain string required
Data Subject Portal Domain
 - apiToken string required
API Token
 - userIdentifier string required
User identifier
 - dataElements array required
Data Elements
 - purposes string required

Output Schema

- output object
 - rawResponse object
 - access_token string
 - refresh_token string
 - id_token string
 - token_type string
 - expires_at number
 - statusCode number
 - headers object
 - claims object
 - moc string
 - sub string
 - attachments
 - notes
 - syncGroup
 - iss
 - language
 - processVersion number
 - enableParentPrimaryIdentifiers boolean
 - authenticationRequired boolean
 - dynamicCollectionPoint boolean
 - processId string
 - dsDataElements array
 - doubleOptIn boolean
 - consentType string
 - additionalIdentifiers object
 - iat string
 - customPayload
 - jti string

- policy_uri
- identifier string
- parentPrimaryIdentifiersType
- gacString
- tcStringV2
- reconfirmActivePurpose boolean
- allowNotGivenConsents boolean
- notices array
- isAnonymous boolean
- multipleIdentifierTypes boolean
- purposes array
- tenantId string
- overrideActivePurpose boolean
- parentPrimaryIdentifiers array
- otJwtVersion number
- enableGeolocation boolean

Get Receipt Information

Get Receipt Information

Properties

Application Domain textField required

The URL of your OneTrust domain, such as "https://company.my.onetrust.com".

Receipt ID textField required

The flow variable that contains the unique identifier for the consent receipt.

Include "Consent Not Given" Transactions toggleSwitch

When enabled, OneTrust returns results for transactions where the user did not provide consent.

Input Schema

- default object
 - properties object
 - applicationDomain string required
Application Domain
 - clientId string required
Client ID
 - clientSecret string required
Client Secret
 - receiptId string required
Receipt ID
 - includeNotGiven boolean required
Include Not Given Transactions

Output Schema

- output object
 - collectionPointName string
 - attributes object
 - collectionPointType string
 - collectionPointUUID string
 - collectionPointVersion number
 - consentCreationDate string
 - customPayload string
 - dataSubjectIdentifier string
 - dataSubjectIdentifierHash string
 - doubleOptIn boolean
 - unsubscribeAll boolean
 - id string
 - interactionDate string
 - isAnonymous boolean
 - language string
 - origin string
 - otJwtVersion number
 - purposes array
 - receiptJwt string
 - test boolean

P-R

PingFederate

PingFederate Connector

Tap into the power of your existing PingFederate authentication policies by including them in your PingOne DaVinci flows.

PingID

PingID connector

You can use the PingID connector to add MFA (multi-factor authentication) to flows, including passwordless login flows.

PingOne

PingOne Connector

Use the PingOne DaVinci connector to add PingOne functionality for your DaVinci flow.

PingOne

Advanced Identity Cloud

PingOne Advanced Identity Cloud Access Request Connector

The PingOne Advanced Identity Cloud Access Request connector lets you manage users and create access requests in PingOne Advanced Identity Cloud in your PingOne DaVinci flow.

PingOne

Advanced Identity Cloud

PingOne Advanced Identity Cloud Login Connector

The PingOne Advanced Identity Cloud Login connector lets you authenticate users using the default journey in PingOne Advanced Identity Cloud in your PingOne DaVinci flow.

PingOne

PingOne Authentication Connector

The PingOne Authentication connector lets you authenticate users and manage PingOne user authentication sessions in your PingOne DaVinci flow.

PingOne Authorize

PingOne Authorize Connector

This connector lets you use PingOne Authorize for policy-based authorization decisions in your PingOne DaVinci flow.

PingOne

PingOne Credentials Connector

Use the PingOne Credentials connector to issue, verify, and manage digital verifiable credentials with PingOne Credentials.

PingOne

PingOne Forms Connector

The PingOne Forms connector lets you include branded forms and messages in your PingOne DaVinci flow.

PingOne MFA

PingOne MFA Connector

PingOne MFA is a cloud-based MFA service that protects an organization's network, applications, and data resources while providing secure and seamless experiences for your customers and users.



PingOne Notifications Connector

The PingOne Notifications connector enables you to send custom voice, SMS, and email notifications to cover a wide range of use cases for your customers.

PingOne Protect

PingOne Protect Connector

You can use the PingOne Protect connector as part of a PingOne DaVinci flow to improve user experience, reduce MFA fatigue, and lower the probability of unintentional push approvals, while still issuing challenges or even denying access altogether in high-risk situations.



PingOne RADIUS Gateway connector

The PingOne RADIUS Gateway connector enables you to integrate PingOne DaVinci flows with a PingOne RADIUS Gateway.



PingOne Scope Consent Connector

The PingOne Scope Consent connector lets you view consent records on an application or user basis, revoke or update user consent records, or prompt users to provide or decline consent to sign-on policies and record these decisions.

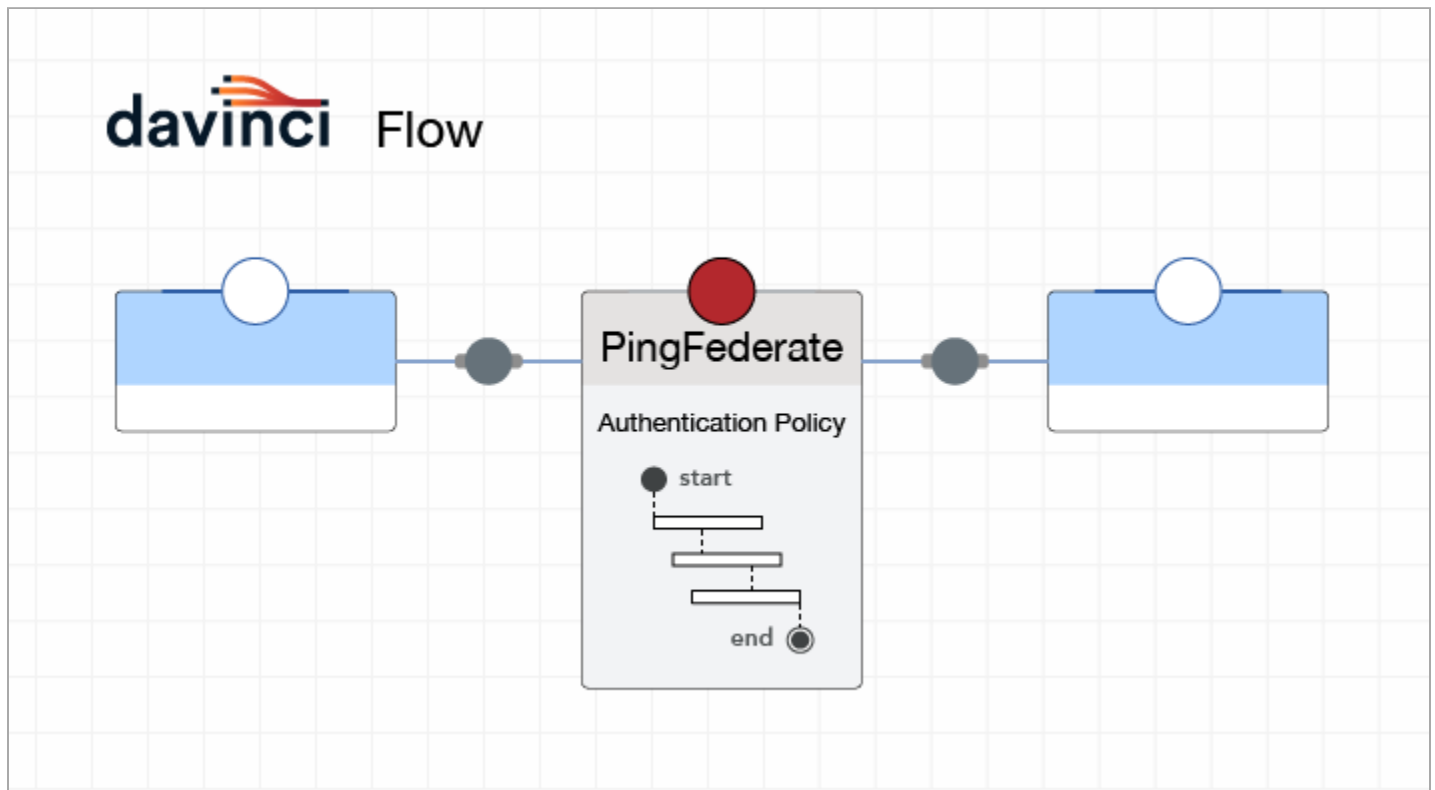
PingOne Verify

PingOne Verify Connector

Use the PingOne Verify DaVinci connector to securely verify a user's identity based on a government-issued document and other user-submitted data, such as a live face capture (selfie).

PingFederate Connector

Tap into the power of your existing PingFederate authentication policies by including them in your PingOne DaVinci flows.



The connector provides two ways to use PingFederate in your flow:

Redirectless method

The connector embeds the [JavaScript Widget for the PingFederate Authentication API](#) in your DaVinci flow. This lets you create a user experience that starts and stays in DaVinci without redirecting the browser.

- The JavaScript Widget provides the user interface and communicates with the PingFederate authentication API.
- Your PingFederate authentication policy can include any of the integrations on the [widget compatibility list](#).
- To tailor the user experience to match your DaVinci flow or company branding, you can customize the JavaScript Widget's HTML, CSS, and JavaScript.

Redirect method

This method redirects the browser to PingFederate to complete an authentication policy. When the policy completes, PingFederate redirects the browser back to DaVinci.

- The user interface is provided by an authentication application or adapter Velocity HTML templates, as configured in your PingFederate authentication policy.
- Your authentication policy can include any component you want. You aren't restricted to JavaScript Widget-compatible integrations.
- You can customize these templates in PingFederate. For help, see [Customizable user-facing pages](#) and the integration-specific documentation.

With both methods, the PingFederate connector makes the following available in your DaVinci flow:

- The access token
- The refresh token
- The ID token (decoded and encoded)
- The complete (raw) response

Setup

Resources

For information and setup help, see the following:

- PingFederate documentation
 - [JavaScript Widget for the PingFederate Authentication API](#) 
 - [Authentication applications and the authentication API](#) 
 - [Compatibility list for the PingFederate Authentication API and JavaScript Widget](#) 
 - [Authentication policies](#) 
 - [Customizable user-facing pages](#) 
- DaVinci documentation:
 - [Adding a connector](#) 
 - [Using connectors securely](#) 
 - [Using DaVinci flow templates](#) 

Requirements

To use the connector, you'll need:

- A configured PingFederate environment
- A configured PingFederate authentication policy



Note

If you want to use the redirectless approach, make sure your policy only includes adapters that are compatible with the [PingFederate JavaScript Widget](#) .

Setting up PingFederate

Enabling the authentication application programming interface (API)

Enable the authentication API if:

- You want to use the connector with the redirectless (JavaScript Widget) method.
- You want to use the connector with the redirect method and you want to use an [authentication application](#) in your PingFederate authentication policy.
 1. In PingFederate, go to **Authentication → Integration → Authentication API Applications**.
 2. Click **Enable Authentication API**.
 3. (Optional) If you're using the redirect method and want to use an authentication application in your authentication policy, add an authentication application. For help, see [Configuring authentication applications](#) in the PingFederate documentation.
 4. Click **Save**.
 5. If you added an authentication application, select it in your authentication policy:
 1. Go to **Authentication → Policies → Your policy**.
 2. In the **Authentication Application** list, select your authentication application.
 3. Click **Done**.

Adding DaVinci as an OAuth client in PingFederate

1. In PingFederate, go to **Applications → OAuth Clients → Clients**. Click **Add Client**.
2. In the **Client ID** field, enter a unique ID, such as `davinci-client`. Note the ID. You'll enter it in the connector settings.
3. In the **Client Name** field, enter a name, such as `DaVinci Client`.
4. For **Client Authentication**, select **Client Secret**.
5. For **Client Secret** field, click **Change Secret**, then click **Generate Secret**. Note the secret. You'll enter it in the connector settings.
6. If you want to use the connector with the redirectless method, select **Allow Authentication API OAuth Initiation**.
7. For **Allowed Grant Types**, select **Authorization Code**.
8. (Optional) If you want to use refresh tokens, for **Allowed Grant Types**, select **Refresh Token**.
9. For the **OpenID Connect ID Token Signing Algorithm**, select **RSA using SHA-256**.
10. Click **Save**.

Configuring the PingFederate connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Redirect URL

This connector's redirect URL. If you use the connector with the redirect method, add this URL as a **Redirect URI** in your PingFederate OAuth Client configuration. This lets PingFederate redirect the browser back to this connector to continue the DaVinci flow. You don't need this with the redirectless method.

Client ID

The client ID that you noted in **Adding DaVinci as an OAuth Client in PingFederate**.

Client Secret

The client secret that you noted in **Adding DaVinci as an OAuth Client in PingFederate**.

Scope

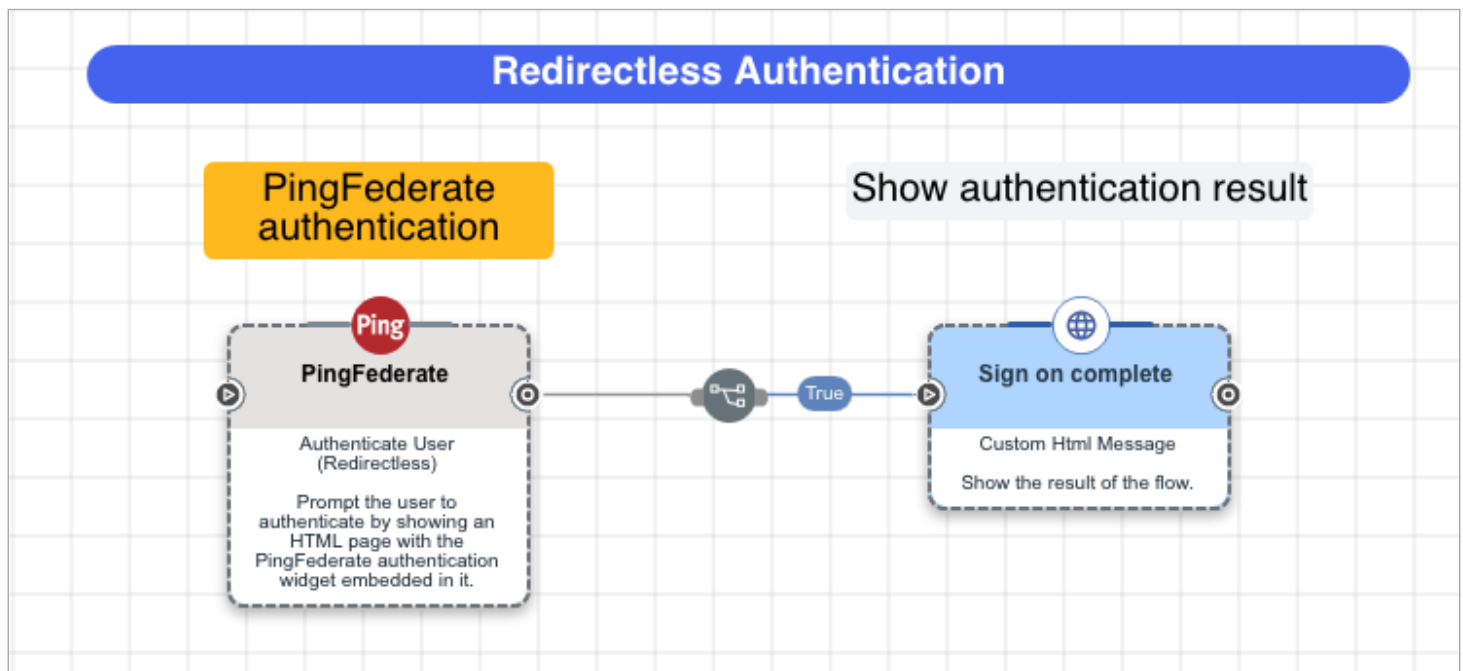
The scope requested from PingFederate, including **openid**. If you configured other scopes in your PingFederate. OAuth Client, add them here. Separate multiple scopes with a space.

Base URL

Enter your PingFederate base URL. For example, <https://pf.example.com:9031> .

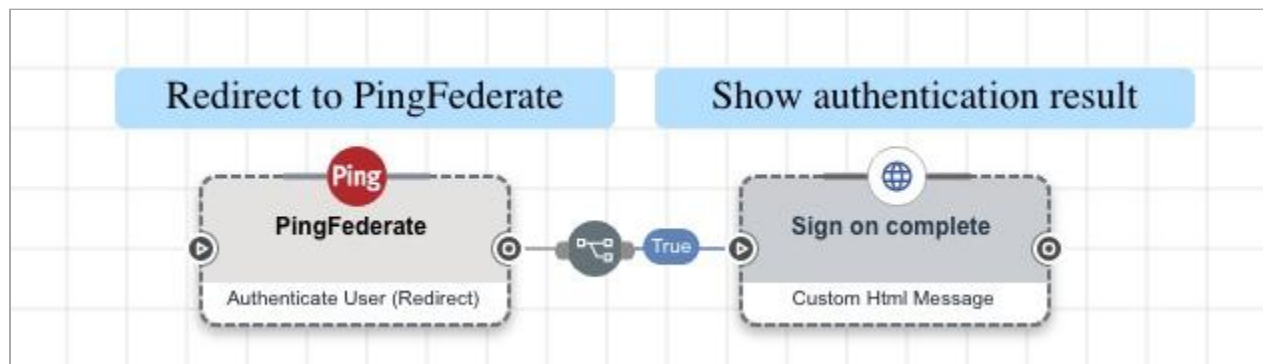
Using the connector in a flow

Using the connector with the redirectless method



1. Download the [PingFederate - Authentication \(Redirectless\)](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Select the **Authenticate User (Redirectless)** node.
 1. (Optional) If you have your own custom version of the PingFederate JavaScript Widget, enter the URL in the **PingFederate JavaScript Widget URL** field.
 2. (Optional) If you want to show your own logo on the PingFederate JavaScript Widget, enter the image URL in the **PingFederate JavaScript Widget Logo URL** field.
 3. (Optional) If you want to customize the page that will contain the PingFederate JavaScript Widget, edit the **HTML Template**, **CSS**, and **Script** fields. For information and tips, see **Building a custom page** in the [HTTP](#) connector documentation.
 4. Click **Apply**.
3. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.
4. Continue building your flow by replacing the **Custom HTML Message** node with a path to the resource that the user initially requested.

Using the connector with the redirect method



The **Authenticate User (Redirect)** capability allows you to redirect the browser to PingFederate to allow the user to authenticate.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Authenticate User (Redirectless)

Embed a PingFederate authentication policy in the DaVinci flow. The authentication policy can include components that work with the PingFederate JavaScript Widget.

Properties

PingFederate JavaScript Widget URL textField required

Default: https://s3.amazonaws.com/pingone/public_downloads/pingfederate/widget/latest/pf.authn-widget.js 

PingFederate JavaScript Widget Logo URL textField HTML Template textArea

Default:

```
<div class="content" style="padding: 30px">
  <div class="heading">Authentication Application</div>
  <form id="skForm">
    <input id="skinput-response" type="hidden" name="response" value="" />
    <button data-skform="skForm" data-skbuttontype="form-submit" data-skbuttonvalue="submit" data-skvalue="submit" id="skbutton" data-skcomponent="skbutton" type="button" style="display:none" />
  </div>
</button>
</form>
<div id="authnwidget">
</div>
```

CSS codeEditor

Default:

```
@import "https://assets.pingone.com/ux/end-user/0.36.1/end-user.css";
@import "https://s3.amazonaws.com/pingone/public_downloads/pingfederate/widget/latest/main-styles.css";
```

Script codeEditor

Write custom JavaScript. Caution: Custom code is for advanced users only. Before using custom code, review the security risks in the DaVinci documentation by searching for "Using custom code safely".

Default:

```
var script = document.createElement('script');
script.src = '{{widgetUrl}}';
script.onload = function () {
    load();
};
document.head.appendChild(script);

function load() {
    var authnWidget = new PfAuthnWidget("{{issuerUrl}}", {
        divId: 'authnwidget',
        logo: '{{widgetLogoUrl}}',
    });

    var config = {
        client_id: '{{clientId}}',
        scope: ['{{scope}}'],
        state: '{{state}}',
        response_type: 'code',
        onAuthorizationSuccess: function (response) {
            document.getElementById('skinput-response').value = JSON.stringify(response);
            document.getElementById('skbutton').click();
        },
        onAuthorizationFailed: function (response) {
            document.getElementById('skinput-response').value = JSON.stringify(response);
            document.getElementById('skbutton').click();
        },
    };
    authnWidget.initRedirectless(config);
}
```


Input Schema

- default object
 - properties object
 - widgetUrl string required
PingFederate JavaScript Widget URL
 - widgetLogoUrl string
PingFederate JavaScript Widget Logo URL
 - customHTML string required
HTML Template
 - customCSS string required
CSS
 - customScript string required
Script

Output Schema

- output object
 - rawResponse object
 - access_token string
 - refresh_token string
 - id_token string
 - token_type string
 - expires_at number
 - statusCode number
 - headers object
 - sub string
 - aud string
 - jti string
 - iss string
 - iat number
 - exp number
 - auth_time string
 - tokens object
 - access_token string
 - refresh_token string
 - id_token string
 - token_type string
 - expires_at number
 - connectionId string
 - connectorId string

Authenticate User (Redirect)

Redirect to a PingFederate authentication policy, then return to the DaVinci flow. The authentication policy can include any components you want.

Properties

Display Name button
Show "Powered by" Message toggleSwitch
Skip Button Press toggleSwitch

Output Schema

- output object
 - sub string
 - aud string
 - jti string
 - iss string
 - iat number
 - exp number
 - auth_time string
 - tokens object
 - access_token string
 - refresh_token string
 - id_token string
 - token_type string
 - expires_at number
 - connectionId string
 - connectorId string

PingID Connector

PingID is a cloud-based multi-factor authentication (MFA) service that protects an organization's network, applications, and data resources while providing secure and seamless experiences for your customers and users.

The PingID connector supports the use of:

- Customer-friendly authentication flows to increase security without adding unnecessary friction to the end user experience.
- User enrollment flows:
 - Automatically: Allow customers to automatically enroll an authentication method for users during the authentication process.
 - One-time device authentication: Include device details within an authentication request. Enables a user to authenticate for one session only, without pairing the device.

Setup

Resources

- PingOne documentation:
 - [Getting started with PingOne](#)
 - [Adding an application](#)
- [PingID documentation](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne license ([Try PingOne for free](#))
- A PingID license.
- A PingOne environment with a [configured Worker app](#).
- A PingID tenant linked to the PingOne environment.

Setting up PingID

For instructions on how to set up PingID, see the [PingID documentation](#).

Setting up the connector

In DaVinci, add a **PingID** connector. For help, see [Adding a connector](#).

Connector settings

Environment ID

Your PingOne Environment ID. In PingOne, go to **Settings → Environment Properties**.

Client ID

The Client ID for your PingOne Worker application. In PingOne, go to your application **Applications → Applications → Configuration**.

Client Secret

The Client Secret for your PingOne Worker application. In PingOne, go to your application **Applications → Applications → Configuration**.

Region

Your PingOne environment region. In PingOne, go to **Settings → Environment Properties**.

Using the connector in a flow

Enrolling a device

To seamlessly add MFA for your users and increase MFA adoption, use the PingID connector. You can include device enrollment as part of user registration, or as a just-in-time (JIT) registration within an authentication flow.

The user can select an authentication method for MFA from a list of methods defined by the PingID configuration. This list can include traditional methods, such as email and SMS, and more secure and frictionless methods, such as FIDO2 biometrics and PingID mobile app. For help, see the [Creating an authentication flow](#) guide.

Authenticating users

Use the PingID connector to increase security by adding an authentication factor that requires the user to prove their identity using a trusted device.

For help, see the [Creating an authentication flow](#) guide.

PingID flow templates

Ping Identity provides out-of-the-box DaVinci subflows that you can add to a main flow to register authentication devices and to use those devices to authenticate with PingID.

The following PingID flows are available:

- **PingID registration sub-flow** [🔗](#)

Use this subflow to register a new authentication method for use with PingID.



Note

The variable `pingIdUserId` represents the ID attribute from PingOne and must be provided when triggering the flow.

- **PingID authentication sub-flow** [🔗](#)

Use this subflow to add PingID as a secondary authentication factor to a main flow, as part of an authentication process.

- Customize PingID authentication sub-flow variables.

Click the **Variables** node to customize any of the following options:

- **AdminMessage** : The administrative message you want to display during authentication.
- **SMSBackup** : Use the user's mobile number as a backup authentication method, so they can receive a one-time passcode by SMS, if the user forgets their registered authentication device.
- **phoneBackup** : Use the user's mobile number as a backup authentication method, to receive a one-time passcode by voice message, if the user forgets their registered authentication device.
- **emailBackup** : Use the user's email address as a backup authentication method, to receive a one-time passcode by email, if the user forgets their registered authentication device.
- **useCode** : When set to `true`, the user can click a **Use Code** button to enter an OTP, rather than waiting for a push notification to arrive.
- **OTP Fallback** : When set to `true`, user's can authenticate with a one-time passcode in the event that the PingID server cannot reach their device, or the push response cannot be completed.

- **Define a list of mandatory authentication devices**

You can define a list of mandatory authentication methods. If defined, users are forced to register all of the required authentication methods in order to access their resources.

1. In the relevant PingID authentication subflow, click the **Flow Settings** node.
2. In the **Variable Name** field, select **mandatoryAuthenticationMethods**, and then enter the authentication methods that the user must register with their account. Valid authentication methods include:

- `PINGID_DESKTOP`

- `PINGID_MOBILE`

- SMS
- VOICE
- EMAIL
- TOTP
- SECURITY_KEY
- PLATFORM
- YUBIKEY
- OATH_TOKEN

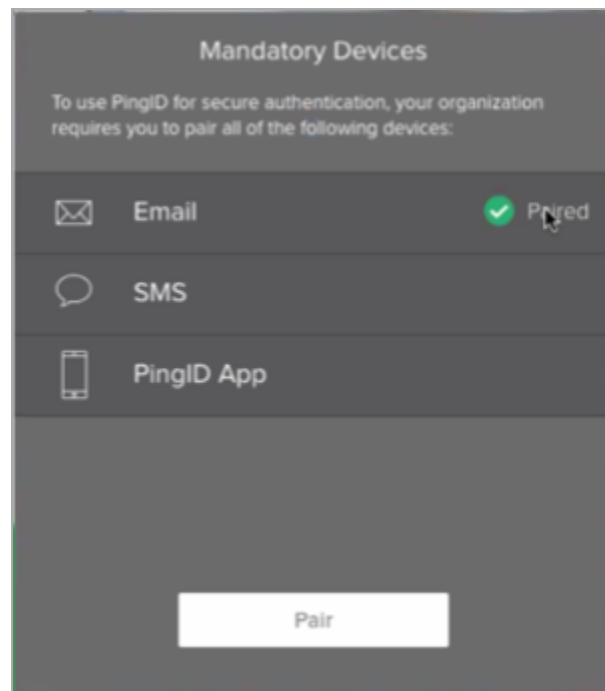
Note

This field is empty by default. Authentication methods must be entered in upper case, with a space between each entry. If no authentication method is defined, the user is not required to pair a specific device.

Example:

SMS VOICE EMAIL

The next time the user attempts to authenticate, even if they have one of the mandatory methods paired with their account, they are forced to register all of the authentication methods specified in the **mandatoryAuthenticationMethods** list, before they can access their resources.



 Note

- This flow requires the PingID - registration welcome page flow. The variable `pingIDUserId` must be provided when triggering the flow.
- The following PingID Connector variables override the equivalent values in the PingID admin console **Configuration** tab:

PingID PingIDconnector variable	PingID PingIDadmin console location
SMSBackup , phoneBackup , emailBackup	Alternate Authentication Methods, Backup Authentication (SMS , Voice , or Email checkbox).
OTP Fallback	Mobile App Authentication, One-time Passcode Fallback
useCode	Mobile App Authentication, Direct Passcode Usage

 Note

It is recommended that you review the [PingID connector limitations](#) section.

Search for the relevant flow in the [DaVinci flow library](#).

PingID connector limitations

This section describes the known limitations relating to the PingID Connector, and evaluation of PingID policy.

PingID Connector limitations

- The PingID Devices page is not available when using the PingID Authentication sub-flow. The **Settings** button is therefore not displayed on the **Authentication** screen.
- The PingID connector only support the English language. Localization is not currently supported.

PingID policy-related limitations

- Backup authentication: If a backup authentication configuration is defined in the PingID authentication sub-flow, it overrides any backup configuration defined in a PingID policy.
- Authentication success message: When authenticating successfully, the Authentication Successful screen appears by default, even if the **Show Approved Authentication** check box is not selected in PingID policy. This behavior can only be modified by editing the flow.
- PingID policy rule evaluation: The Evaluate Policy capability does not enforce the following policy rules:
 - Limit push notifications rule
 - Mobile OS version rule

- Recent authentication from office rule
 - Authentication from company network rule: authenticating device in company offices section
 - Recent authentication from company network rule: authenticating device in company offices section
- IPv6 address support: If you only have an IPv6 address configured on your local machine, PingID policy is not evaluated.
 - PingID policy log entries: Log entries do not support multiple users authenticating from the same browser. Log entries for transaction details such as IP address, transaction time, and geolocation are overwritten by the last user that authenticates.
 - If you want to disable the OTP fallback or Direct passcode Usage (**Use Code** button) features, you must disable the relevant feature in the flow settings node in DaVinci, and the Admin portal.

PingID Legacy Connector

You can use the PingID connector to add MFA (multi-factor authentication) to flows, including passwordless login flows.

PingID is a cloud-based authentication service that allows your users to carry out MFA (multi-factor authentication) using a variety of methods, including the PingID mobile app, security keys, and biometrics.

Setup

Resources

- PingID documentation:
 - [Overview of PingID authentication types](#)
 - [PingID Integrations](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Setting up the connector

In DaVinci, add a **PingID** connection. For help, see [Adding a connector](#).

After creating the connector, configure it by going to its **General** tab and pasting in the content of the PingID properties file that you downloaded.


PingID Details
Company ID: 0422xH9L3ED7RE7yPTgEtTK8GiZUYXv7
Connection ID: 7cfb64c2d10f3d4ebe0515639d9c8e6f

GENERAL
CAPABILITIES
IN FLOWS

* indicates required

PingID properties file * ⓘ

```
#Auto-Generated from PingOne, downloaded by id=[SSO] email=[JaneTan@PingIdentity.com]
#Thu Jan 13 06:44:38 MST 2022
use_base64_key=S64hIYuEJm0nOoFp9AkIMzAIVxI/P4OIoFa0/ASpbsg=
use_signature=true
token=e0e3514ca867461ab46316fb599b8e22
idp_url=https://idpxnyl3m.pingidentity.eu/pingid
org_alias=a2527b32-42e4-4856-9f79-eabaf29b8999
admin_url=https://idpxnyl3m.pingidentity.eu/pingid
authenticator_url=https://authenticator.pingone.eu/pingid/ppm
```

Close
Apply

Using the connector in a flow

MFA flows

For examples of using the PingID connector in basic MFA flows, see the following templates in the [Flow Library](#):

- PingID - Basic MFA flow (username/password + MFA)
- PingID - MFA flow + Risk (username/password + risk evaluation, MFA according to risk score generated for user)

In flows of this type, a connector using the Initialize MFA capability should be placed in the flow at the point where you want an MFA challenge to be issued, for example, after the user has entered their password.

MFA in passwordless flows

For examples of using the PingID connector to combine MFA with passwordless login, see the following templates in the [Flow Library](#):

- PingID - FIDO2 Passwordless (FIDO2 username, no password required)
- PingID - FIDO2 Passwordless + Risk (FIDO2 username, no password + risk evaluation, action based on risk score generated for user)

In passwordless login flows, two PingID connectors should be added to the flow:

- A connector using the Initialize Passwordless Authentication capability
- Later in the flow, a second connector using the Finalize Passwordless Authentication capability and using as input the *passwordlessContext* that was returned by the initialize step. The username must also be provided as input.

Capabilities

Initialize MFA

Multi-Factor Authentication and on-the-fly registration.

Properties

Username textField required

The username for the user in PingOne.

First Name textField required

User's first name.

Last Name textField required

User's last name.

User Groups textField required

The groups to which the user belongs. Used for applying PingID policies that have been defined.

Mobile Number textField required

User's mobile phone number.

Landline Number textField required

User's landline number.

Application Name textField required

The name of the application the user is trying to access.

Application ID textField required

The ID of the application the user is trying to access. Used for applying PingID policies that have been defined.

Application Icon (URL) textField required

The URL of the icon that is used for the application the user is trying to access.

IP of accessing device textField required

The IP of the device trying to access the application. Used for applying PingID policies that have been defined.

Attributes selectNameValueListColumn

Use this section to add attribute to the request

Input Schema

- default object

- properties object

- customAuth object required

- Custom Auth Properties

- pingIdProperties string minLength: 0 maxLength: 1000

- PingID properties file

- skRedirectUri string minLength: 0 maxLength: 100 pattern: [-a-zA-Z0-9@:%_+~#={1,256}.[a-zA-Z0-9()]{1,6} ([-a-zA-Z0-9()@:%_+~#?&//=]*)]

- Return URL

- sub string required minLength: 0 maxLength: 100

- Subject

- fname string minLength: 0 maxLength: 100

- First Name

- lname string minLength: 0 maxLength: 100

- Last Name

- group string minLength: 0

- User Groups

- phone string minLength: 0 maxLength: 100

- Mobile Number

- voiceNumber string minLength: 0 maxLength: 100

- Phone Number

- appName string minLength: 0 maxLength: 100

- Application Name

- saasid string minLength: 0 maxLength: 100

- Application ID

- appIconUrl string minLength: 0 maxLength: 1000

- Application Icon (URL)

- pingIdIp string minLength: 0 maxLength: 100

- Policy Evaluation IP

Input Example

```
{ "properties" :  
  { "customAuth" :  
    { "pingIdProperties" : "PingID props file" },  
    "sub" : "User" } }
```

Output Schema

- output object
 - ppmResponse string
 - status string
 - sub string
 - accessingDevice object
 - ip string
 - authenticationDevice object
 - id string
 - authenticationType string

Initialize Passwordless Authentication

Passwordless authentication using FIDO2 supported devices.

Properties

Attributes selectNameValueListColumn

Use this section to add attribute to the request

Input Schema

- default object

- properties object

- customAuth object required

- Custom Auth Properties

- pingIdProperties string minLength: 0 maxLength: 1000

PingID properties file

- skRedirectUri string minLength: 0 maxLength: 100 pattern: [-a-zA-Z0-9@:%_\+\~#={1,256}\.[a-zA-Z0-9()]{1,6}\([-a-zA-Z0-9()@:%_\+\~#?&//=]*)]

Return URL

Input Example

```
{ "properties" :
  { "customAuth" :
    { "pingIdProperties" : "PingID props file" } } }
```

Output Schema

- output object

- ppmResponse string

- status string

- sub string

- passwordlessContext string

Finalize Passwordless Authentication

Policy evaluation to complete the Passwordless Authentication.

Properties

Username textField required

The username for the user in PingOne.

Passwordless Context textField required

Information returned by the initializePasswordlessAuthentication capability of the connector. Required to continue the passwordless session.

First Name textField required

User's first name.

Last Name textField required

User's last name.

User Groups textField required

The groups to which the user belongs. Used for applying PingID policies that have been defined.

Mobile Number textField required

User's mobile phone number.

Landline Number textField required

User's landline number.

Application Name textField required

The name of the application the user is trying to access.

Application ID textField required

The ID of the application the user is trying to access. Used for applying PingID policies that have been defined.

Application Icon (URL) textField required

The URL of the icon that is used for the application the user is trying to access.

IP of accessing device textField required

The IP of the device trying to access the application. Used for applying PingID policies that have been defined.

Attributes selectNameValueListColumn

Use this section to add attribute to the request

Input Schema

- default object

- properties object

- customAuth object required

- Custom Auth Properties

- pingIdProperties string minLength: 0 maxLength: 1000

- PingID properties file

- skRedirectUri string minLength: 0 maxLength: 100 pattern: [-a-zA-Z0-9@:%_\+\~#={1,256}\.[a-zA-Z0-9()]{1,6}\([-a-zA-Z0-9()@:%_\+\~#?&/=]*)]

- Return URL

- sub string required minLength: 0 maxLength: 100

- Subject

- passwordlessContext string required

- Passwordless Context

- fname string minLength: 0 maxLength: 100

- First Name

- lname string minLength: 0 maxLength: 100

- Last Name

- group string minLength: 0

- User Groups

- phone string minLength: 0 maxLength: 100

- Mobile Number

- voiceNumber string minLength: 0 maxLength: 100

- Phone Number

- appName string minLength: 0 maxLength: 100

- Application Name

- saasid string minLength: 0 maxLength: 100

- Application ID

- applconUrl string minLength: 0 maxLength: 1000

- Application Icon (URL)

■ pingIdIp string minLength: 0 maxLength: 100

Policy Evaluation IP

Input Example

```
{ "properties" :  
  { "customAuth" :  
    { "pingIdProperties" : "PingID props file" },  
    "sub" : "User",  
    "passwordlessContext" : "context" } }
```

Output Schema

- output object
 - ppmResponse string
 - status string
 - sub string
 - accessingDevice object
 - ip string
 - authenticationType string

Troubleshooting

If you are having trouble with the PingID connector, you can try the following:

- Verify that when you created and configured the connector on the Connections page, you pasted correctly the contents of your PingID properties file.
- For each connector in the flow, make sure that all the mandatory inputs have been provided.
- Use the Analytics feature to see where the flow stopped.
- Select the Options icon, and turn on **Show Node ID**. This will make it easier to identify the source of inputs and outputs.

PingID Connector Release Notes

New features and improvements in the PingID Connector.

February 2025

New Read Device Authentication Policy capability

New

The **Read Device Authentication Policy** capability allows you to read device authentication policies in your PingOne DaVinci flow.

November 2023

PingID authentication subflow enhancements

Improved

The PingID authentication subflow now includes the following features:

- We've added the ability to evaluate and apply PingID policy to the PingID sub-flows To support this enhancement, we've added the Policy Evaluation capability to the PingID connector.
- Administrators can now define a list of mandatory authentication methods. If defined, users are forced to register all the required authentication methods to access their resources.
- If a user does not have a registered device during an authentication flow, after they successfully register a new device they are also required to authenticate with the new device.

August 2023

Character limit for User Groups field

Fixed

When using the legacy PingID connector in a DaVinci flow, there was a problem if the **User Groups** field contained more than 100 characters. This 100-character limit has been removed.

April 2023

PingID Connector

Improved

We've enhanced the PingID Connector to enable the user to enter their One-time Passcode (OTP) when triggering Multi-factor Authentication (MFA). It's now possible for the user to enter a TOTP/HOTP-generated OTP when starting authentication using the Create Device Authentication endpoint.

January 2023

New PingID Connector flows

New

Following the release of the new PingID DaVinci connector, we've added the following out-of-the-box flows:

- [PingID registration subflow](#)

- [PingID authentication subflow](#)

PingID devices page availability

Issue

The PingID Devices page is not available when using the PingID Authentication sub-flow. The 'Settings' button is therefore not displayed on the Authentication screen.

Localization support

Issue

The PingID Connector only supports English language.

December 2022

PingID Connector now available

New

The new PingID connector is now available.

Use this connector to register and authenticate your users with PingID when the PingID tenant is connected to a PingOne environment.

The PingID connector is based on the PingOne API and includes an increased set of capabilities. It replaces the previous PingID connector (now called PingID Legacy Connector).

PingID policy support

Issue

PingID policy is not currently supported.

PingOne Connector

Use the PingOne DaVinci connector to add PingOne functionality for your DaVinci flow.

The PingOne connector has capabilities that you can tie together to achieve your desired outcome. The connector acts like a worker application with each capability calling one or more endpoints in PingOne using your application for authentication.

You can use the PingOne connector to:

- Create a sign-on flow for authentication
- Reset a user's password
- Register new users in the PingOne user store
- Unlock a locked user account
- Create, edit, and delete users in the PingOne user store

- Verify a user's email address
- View a user's population
- Manage a user's group memberships
- Manage user groups
- View agreements and consents for a user
- Migrate users from an LDAP datastore to PingOne
- Authenticate users through Kerberos

Setup

Resources

You can find information in, the following sections of the PingOne documentation:

- PingOne:
 - [Introduction to PingOne](#)
 - [Getting started with PingOne](#)
 - [Adding an application](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne license ([Try PingOne for free](#))
- A PingOne environment with a configured Worker app

Setting up PingOne

Setting up your PingOne environment

Learn more in [Getting started with PingOne](#).

Adding a Worker application

Add a Worker application in the PingOne admin console before setting up the PingOne connector in DaVinci.

1. In the PingOne admin console, add a Worker app. Learn more in [Adding an application](#).

**Note**

Attribute mappings are not required.

2. Ensure that you set the authentication method as **Client secret basic**.

The PingOne connector receives a token using your application's credentials.

3. Enable the application. Learn more in [Adding an application](#).

The capabilities in the PingOne connector call endpoints in PingOne with a token received using the application's credentials. To enable all capabilities, your application needs the required role assignments for the associated capability. If the application doesn't have the required role assignment, you'll see error messages stating that the required authorization isn't configured.

Assigning Roles to the application

To use the appropriate capabilities, the Worker app used by the connector needs the **Environment Admin** and **Identity Data Admin** roles.

**Note**

The user that creates the Worker app must have the **Environment Admin** and **Identity Data Admin** roles to assign the roles to a Worker app.

1. In the PingOne admin console, go to **Applications > Applications**.

Learn more about [Adding an application](#) in the PingOne documentation.

2. Locate the appropriate application and click it to open the details panel.
3. Click the **Roles** tab and then click the **Pencil** icon to edit the roles.
4. Review the assigned roles to ensure that they include **Environment Admin** and **Identity Data Admin** roles. If not, click **+ Add role** to assign them.

Getting your application credentials

Get the **Client ID** and **Client secret** from the PingOne admin console before setting up the PingOne connector in DaVinci.

1. In your PingOne environment, go to **Applications > Applications**.

Learn more about [Adding an application](#) in the PingOne documentation.

2. Locate the appropriate application and click it to open the details panel.
3. On the **Configuration** tab, expand **General** and locate the **Client ID** and **Client secret**. Copy these values to a secure location.

Getting your environment details

Get your **Environment ID** and **Region** before setting up the PingOne connector in DaVinci.

1. In your PingOne environment, go to **Settings > Environment Properties**.

2. Locate the **Environment ID** and **Region**. Copy these values to a secure location.

Setting up the PingOne connector configuration

In DaVinci, add a PingOne connection. Learn more in [Adding a connector](#) in the DaVinci documentation.

Connector configuration

Environment ID

The unique identifier for the appropriate PingOne environment. Learn more about finding the environment ID in [Environment properties](#) in the PingOne documentation.

Client ID

The unique public identifier for the PingOne application. Learn more about finding the client ID in [Viewing application details](#) in the PingOne documentation.

Client secret

The cryptographic secret that is known only to the application and the authorization server. Learn more about finding the client secret in [Viewing a client secret](#) in the PingOne documentation.

Region

The geographic region that hosts your PingOne tenant. Learn more about finding the region in [Environment properties](#) in the PingOne documentation.

Using the connector in a flow

You can use sample flows as a starting point or create your own flows to satisfy your requirements. The following section shows some popular sample flows. Open the [Flow Library](#) to see them all.

Authenticating users and resetting passwords

Use this flow to create authentication flows that include the ability for users to reset or recover their passwords.

Search for **PingOne - Sign On and Password Reset** in the [Flow Library](#)

Learn more in [Creating an authentication flow](#) in the DaVinci documentation.

Registering users and setting up MFA

Use this flow to create registration flows with optional user enrollment to MFA.

Search for **PingOne - Register with verify email and MFA enrollment** in the [Flow Library](#)

Learn more in [Creating an authentication flow](#) in the DaVinci documentation.

Authenticating users with Risk and MFA

Use this flow to create sign-on flows that include a password check and a conditional step-up to second-factor authentication using [PingOne Risk](#)

Search for **PingOne - Sign On and Adaptive MFA** in the [Flow Library](#)

Learn more in [Creating an authentication flow](#) in the DaVinci documentation.

Registering users with agreements and verifying email

Use this flow to create registration flows that include email address verification and agreement consent.

Search for **PingOne - Register with Agreements and Verify Email** in the [Flow Library](#)

Learn more in [Creating an authentication flow](#) in the DaVinci documentation.

Registering users and verifying email

Use this flow to create registration flows that include email address verification.

Search for **PingOne - Register with Verify Email** in the [Flow Library](#)

Learn more in [Creating an authentication flow](#) in the DaVinci documentation.

Managing group memberships

The connector has several capabilities that allow you to manage the groups that a user belongs to in PingOne:

- **Read User Group Membership**
- **Create User Group Membership**
- **Delete User Group Membership**

No special flow configuration is needed. Add the capability that you want and populate its properties according to the help text.

Managing user groups

The connector has several capabilities that allow you to manage groups.

- **Create Group**
 - Create a new user group in PingOne and optionally set the metadata on the group. Only the **Group Name** is required.



Important

Updating a group's metadata using the **Update Group** capability on a DaVinci flow overwrites any existing metadata on PingOne Groups.

- **Read Group**

- Read a user group. Only the **Group ID** is required.

- **Update Group**

- Update an existing user group with the supplied information and optionally update a group's metadata. The **Group ID** is required to verify the group exists and the **Group Name** is required only when updating a group.

- **Delete Group**

- Delete a specified group. Only the **Group ID** is required.

- **Read Group Members**

- Read up to 100 users within a group. The list is filterable by match attributes and an identifier. Only the **Group ID** is required.

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Migrating users from an external directory to PingOne

The connector allows you to use your existing authentication flow to migrate users to the PingOne user store from an external directory.



Tip

Learn more about setting up a directory as a gateway in PingOne in [Gateways](#) in the PingOne documentation.

In your authentication flow, add the PingOne connector with the **Migrate User Through Gateway** capability. This capability validates the user's credentials against the directory for authentication, then migrates the user account to PingOne.

The **Gateway User Type List** property allows you to filter by specific gateways and user types.

Unlike the **Authenticate users via Kerberos** capability, the **Migrate User Through Gateway** capability supports only user types with user migration, with the **Enable migration of new users upon first authentication** option enabled.



Note

If you're building a flow to support LDAP authentication for users provisioned from Microsoft Active Directory into PingOne through an [LDAP gateway provisioning connection](#) and an [inbound rule](#), use the **Check Password** capability.

Authenticate users via Kerberos

Use this capability to use Kerberos to seamlessly authenticate users who have user records in an on-premises Microsoft Active Directory.

This capability requires an LDAP gateway and a user type. If the selected user type is not configured to migrate users upon their first authentication, the **Create PingOne User** toggle is not applicable and not shown.

The [example flow](#) uses the **PingOne** node to authenticate the user via Kerberos and evaluates as follows.

- **Successful**: The **PingOne Authentication** node returns a success response.
- **Failure**: The **Username/Password Form** node asks for the user's username and password and the flow continues to the **Button Pressed** node. The user has the options to press:
 - **Submit**: The user submits login and the flow continues to the **Sign In** node, the **User Lookup** node, and **PingOne node** in which a user migrates through a gateway and lastly continues on to the **Check Password** node.

Note

If you are building a flow to support Kerberos authentication for users provisioned from Microsoft Active Directory into PingOne through an [LDAP gateway provisioning connection](#) and an [inbound rule](#), remove the **PingOne** node that migrates users and link the **False** branch of the **User Lookup** node to the **Invalid Username/Password** node.

The **User Lookup** node should always return **True** unless provisioning fails to create the user record in PingOne, in which case you should review the provisioning audit events in **Event types > Provisioning** in the PingOne admin console.

- **Forgot Password**: Flow continues to **Forgot Password** node.
- **No match**: Flow continues to the **An Unexpected Error** node which displays a custom error message.

Tip

Learn more about setting up Active Directory as a gateway in PingOne in the following:

- [LDAP Gateways](#)
- [Creating SPNs](#)
- [Configuring end user browsers](#)
- [Adding a Gateway](#)

Learn more about using the connector in a flow in [Creating an authentication flow](#) in the DaVinci documentation.

Alternative Identifier

An alternative identifier is a domain, ID, or custom value used to identify a population.

The following example shows a population with a domain alternative identifier used with the **Read Population** capability.

```
{
  "id": "42fc7d8f-db37-4a42-8eb8-6664e7f62f79",
  "environment": {
    "id": "<env_id>"
  },
  "name": "Sample Population with an Alternative Identifier",
  "userCount": 256,
  "createdAt": "2024-10-17T19:16:09.272Z",
  "updatedAt": "2024-11-17T15:23:33.272Z",
  "alternativeIdentifiers": [
    "pingidentity.com",
    "another_alt_identifier"
  ],
  "default": false
}
```

The following images show setting the alternative identifier value directly in the field and having the value pulled from a prior node's form value.

The image displays two screenshots of the PingOne user management interface, specifically the 'Population' section. Both screenshots show a dropdown menu labeled 'Use Alternative ID' and a text input field for the 'Alternative Identifier'.

In the top screenshot, the 'Alternative Identifier' field contains the text 'pingidentity.com'. To the right of the input field is a circular icon containing a curly brace '{'.

In the bottom screenshot, the 'Alternative Identifier' field contains a value pulled from a prior node, indicated by a blue border and a globe icon. The text 'altId' is visible next to the globe icon. To the right of the input field is a circular icon containing a curly brace '{'.

Update User through Gateway

Use this capability to retrieve a user's attributes through a PingOne gateway and update the PingOne user profile with them.

In the **PingOne Attribute** list, select the attribute that you want to match against the provided identifier to find a user. The default is **User ID**.

In the **Identifier** field, enter the user ID, username, or email address of the user that you want to find.

 **ACTION:**

Update User through Gateway

GENERAL

SETTINGS

SCHEMA

MAPPING: >

* indicates required

PingOne Attribute ⓘ

User ID ▼

Identifier ⓘ


The variable you enter in **Identifier** points to an outcome attribute from an earlier node, where the user is successfully authenticated, and the user and user identifier are known.

You can also use the **Authenticate User via Kerberos** capability, followed by the **Update User through Gateway** capability to have PingOne authenticate users using the Kerberos protocol and then update PingOne user attributes with attribute values from the on-premises Microsoft Active Directory (AD).

Note

The **Update User through Gateway** capability configuration doesn't include which LDAP Gateway and user type to select to find a user, as the PingOne user's record contains the LDAP Gateway and user type.

Capabilities

Find User

Find a user by identifier.

Properties

Custom SCIM Filter toggleSwitch

SCIM Filter textField

PingOne Attributes textFieldArrayView

Enter the PingOne attributes you want to use to find a user, such as username, userID, or email.

Identifier textField

Enter the identifier, which was captured earlier in the flow, that you want to use to find a user. For example, if the attributes specified are email and username, and the identifier is username, the system will search for users whose email or username match the value captured under username.

Return User Password Status toggleSwitch

The output will include a property named 'passwordStatus' which correlates to the user's password state status in PingOne.

Input Schema

- default object
 - properties object
 - matchAttributes array uniqueItems: true
 - userIdentifierForFindUser string
User attribute to match attributes.
 - returnUserPasswordStatus boolean
 - scimFilter string
SCIM filter to match users.

Output Schema

- output object
 - matchedUser object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- passwordStatus string
- userFilter string
- userCount integer
- rawResponse object
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "matchedUsers" :
    { "_embedded" :
      { "users" :
        [
          { "environment" :
            { "id" : "5007e871-f0e7-4fc9-9ab9-b23b3ae76069" },
            "id" : "f442f27a-6d9c-4280-891f-bed26a9bd9ce",
            "username" : "johndoe" } ] } },
      "passwordState" :
        { "status" : "OK" } },
      "responseStatus" : 200,
      "headers" :
        { "XPing" : "X-Ping" },
      "passwordStatus" : "OK|PASSWORD_EXPIRED|MUST_CHANGE_PASSWORD|NO_PASSWORD|PASSWORD_LOCKED_OUT|UNKNOWN",
      "matchedUser" :
        { "environment" :
          { "id" : "5007e871-f0e7-4fc9-9ab9-b23b3ae76069" },
          "id" : "f442f27a-6d9c-4280-891f-bed26a9bd9ce",
          "username" : "johndoe" } } }
```

Find Multiple Users

Find a set of users by an identifier.

Properties

Custom SCIM Filter toggleSwitch

SCIM Filter textField

PingOne Attributes textFieldArrayView

Enter the PingOne attributes you want to use to find a user, such as username, userID, or email.

Identifier textField

Enter the identifier, which was captured earlier in the flow, that you want to use to find a user. For example, if the attributes specified are email and username, and the identifier is username, the system will search for users whose email or username match the value captured under username.

Input Schema

- default object
 - properties object
 - matchAttributes array uniqueItems: true
 - userIdentifierForFindUser string
User attribute to match attributes.
 - scimFilter string
SCIM filter to match users.

Output Schema

- output object
 - matchedUsers array
 - count integer
 - userFilter string
 - rawResponse object
 - _embedded object
 - matchedUsers array
 - count integer
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "_embedded" :
    { "matchedUsers" :
      [
        { "_embedded" :
          { "user" :
            { "preferredLanguage" : "EN",
              "timezone" : "EST",
              "lastSignOn" :
                { "at" : "00:00:00:0000",
                  "remoteIp" : "127.0.0.1" },
              "title" : "test",
              "type" : "Admin",
              "locale" : "EN",
              "enabled" : true,
              "createdAt" : "00:00:00:0000",
              "verifyStatus" : "NOT_VERIFIED",
              "nickname" : "test",
              "mfaEnabled" : false,
              "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
              "email" : "ping@pingidentity.com",
              "username" : "test" } } } ] } },
      "matchedUsers" :
      [
        { "_embedded" :
          { "user" :
            { "preferredLanguage" : "EN",
              "timezone" : "EST",
              "lastSignOn" :
                { "at" : "00:00:00:0000",
                  "remoteIp" : "127.0.0.1" },
              "title" : "test",
              "type" : "Admin",
              "locale" : "EN",
              "enabled" : true,
              "createdAt" : "00:00:00:0000",
              "verifyStatus" : "NOT_VERIFIED",
              "nickname" : "test",
              "mfaEnabled" : false,
              "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
              "email" : "ping@pingidentity.com",
              "username" : "test" } } } ] } }
```

Check Password

Validate a user's password.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Password textField

The user's password to validate.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - password string required minLength: 1
Password

Output Schema

- output object
 - passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - rawResponse object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "passwordState" :  
    { "environment" :  
      { "id" : "5007e871-f0e7-4fc9-9ab9-b23b3ae76069" },  
      "user" :  
        { "id" : "f442f27a-6d9c-4280-891f-bed26a9bd9ce" },  
        "passwordPolicy" :  
          { "id" : "b91ef66e-2b21-449a-a158-afc2d870ab92" },  
          "status" : "OK",  
          "lastChangedAt" : "2021-03-15T08:50:24.426Z" } } } }
```

Create User

Create a user with the attribute values provided.

Properties

Username textField required

The unique identifier for the user.

Population dropDown

The name of the population.

- Use Population ID (Default)
- Use Alternative ID

Population ID textField

The unique identifier for the population.

Password textField

Given Name textField

Family Name textField

Email textField

Primary Phone textField

Mobile Phone textField

Preferred Language textField

Locale textField

Other Attributes variableInputList

Add other attributes and their values.

Lifecycle Status dropDown

Indicate whether new users must initially verify their identities through email. If they do, they will receive an email containing a verification code when their accounts are created.

- ACCOUNT_OK (Default)
- VERIFICATION_REQUIRED

Input Schema

- default object
 - properties object
 - population string required minLength: 0 maxLength: 100
Population
 - alternativeIdentifier string minLength: 0 maxLength: 255
Alternative Identifier
 - populationId string minLength: 0 maxLength: 100
Population ID
 - given string
 - family string
 - email string
 - primaryPhone string
 - mobilePhone string
 - username string required
 - preferredLanguage string
 - locale string
 - passwordForCreateUser string
 - lifecycleStatus string required

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Read User

Find user information.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Update User

Update user attributes.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Username textField required

The unique identifier for the user.

Given Name textField

Family Name textField

Email textField

Primary Phone textField

Mobile Phone textField

Preferred Language textField

Locale textField

Other Attributes variableInputList

Add other attributes and their values.

User Attributes to Clear textFieldArrayView

Type the PingOne user attributes you want to clear for a user, such as name or primaryPhone, and hit enter after each one.

PingOne User Attributes link

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - given string
 - family string
 - email string
 - primaryPhone string
 - mobilePhone string
 - username string
 - preferredLanguage string
 - locale string

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Delete User

Delete users.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Update User Status

Enable or disable user accounts.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Enable User toggleSwitch

Enable or disable the user's account.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - enabled boolean required
Enable Status Of User

Output Schema

- output object
 - user object
 - enabled boolean
 - rawResponse object
 - enabled boolean
 - headers object
 - statusCode integer

Send Email Verification Code

Send a verification code to the user that can be used to verify their email.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Validate Verification Code

Verifies the provided code that was sent to a user's email during account creation.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Verification Code textField

The code emailed to the user to verify their email address.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - verificationCode string required minLength: 0 maxLength: 100
Code to verify a user's account

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
- headers object
- statusCode integer

Send Password Recovery Code

Send recovery codes to users' email addresses to recover forgotten passwords.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - rawResponse object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { } }
```

Validate Password Recovery Code

Validate recovery codes and allow users to reset their passwords.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Recovery Code textField

The code to validate.

New Password textField

The user's new password.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - recoveryCode string required
 - newPassword string required minLength: 1

Output Schema

- output object
 - passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - rawResponse object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { } }
```

Change Password

Change a user's password to a new password using their current password for validation.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Current Password textField

The user's current password.

New Password textField

The user's new password.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - newPassword string minLength: 1
 - currentPassword string minLength: 1

Output Schema

- output object
 - passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - rawResponse object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "passwordState" :  
    { "environment" :  
      { "id" : "5da98f13-ad62-4234-ba04-2b6e2e85c8ca" },  
      "user" :  
        { "id" : "c3042000-188f-4bc7-a269-dee1602cf7af" },  
        "passwordPolicy" :  
          { "id" : "5da98f13-ad62-4234-86d3-01018f6ef0ad" },  
          "status" : "OK",  
          "lastChangedAt" : "2019-01-08T20:18:31.264Z" } } }  
  }
```

Set Password

Set a user's password, optionally forcing the user to change password at next login.

Properties

PingOne Attribute dropdown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Password Value textField

The user's new password, which can be in a cleartext or pre-encoded format.

Force Change Password toggleSwitch

Indicate whether the user must change their password the next time they sign on.

Bypass PingOne Password Policy toggleSwitch

Indicate whether the password policy used to authenticate the user's population should be ignored.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - passwordValue string required minLength: 1
 - forceChange boolean
 - bypassPolicy boolean

Output Schema

- output object
 - passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - rawResponse object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string
 - warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
 - status string
 - lastChangedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "passwordState" :  
    { "environment" :  
      { "id" : "5da98f13-ad62-4234-ba04-2b6e2e85c8ca" },  
      "user" :  
        { "id" : "c3042000-188f-4bc7-a269-dee1602cf7af" },  
        "passwordPolicy" :  
          { "id" : "5da98f13-ad62-4234-86d3-01018f6ef0ad" },  
          "status" : "OK",  
          "lastChangedAt" : "2019-01-08T20:18:31.264Z" } } }  
  }
```

Create Account Link

Create an account link for a user.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

External ID textField

ID of a user at an identity provider.

Identity Provider dropDown

The name of the PingOne Identity Provider.

- Use Identity Provider ID (Default)

Identity Provider ID textField

ID of the PingOne Identity Provider.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - identityProvider string required minLength: 0 maxLength: 100
The id of the identity provider the account link is for
 - identityProviderId string minLength: 0 maxLength: 100
The id of the identity provider the account link is for
 - externalId string required minLength: 0 maxLength: 3000
The id of the account at the identity provider

Output Schema

- output object
- properties object
 - id string
 - environment object
 - id string
 - identityProvider object
 - id string
 - user object
 - id string
 - externalId string
- rawResponse object
 - id string
 - environment object
 - id string
 - identityProvider object
 - id string
 - user object
 - id string
 - externalId string
- headers object
- statusCode integer

Read Account Links

Reads account links for a user

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - linkedAccounts array
 - rawResponse object
 - `_embedded` object
 - linkedAccounts array
 - count number
 - size number
 - headers object
 - statusCode integer

Delete Account Link

Delete a users account link

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Account link ID textField

ID of the account link.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - accountLinkId string required minLength: 0 maxLength: 100
Account link ID

Output Schema

- output object
 - headers object
 - statusCode integer

Check User Agreement

Indicate whether users need to accept or sign agreements before proceeding.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Agreement dropDown

The name of the agreement.

- Use Agreement ID (Default)

Agreement ID textField

A unique identifier for the agreement the user has accepted or signed.

Accept Language textField

The language in which the agreement is written and indicated by an IETF BCP 47 language tag, such as "en-US" or "az-Arab".

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - agreementId string minLength: 0 maxLength: 100
Agreement ID
 - acceptLanguage string minLength: 0 maxLength: 100
BCP 47 Language tag used as Accept-Language header

Output Schema

- output object
 - agreementPresentation object
 - agreementPresentationId string
 - agreementText string
 - agreementTitle string
 - agreementAcceptCheckboxText string
 - agreementContinueButtonText string
 - agreementDeclineButtonText string
 - userAgreement object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean

- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string
 - locale string
 - enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- rawResponse object
 - _embedded object
 - agreement object
 - id string
 - name string

- environment object
 - id string
- reconsentPeriodDays number
- totalConsents number
- totalExpiredConsents number
- consentsAggregatedAt string
- enabled boolean
- revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean
- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string
 - locale string
 - enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string

- language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "_embedded" :
    { "agreement" :
      { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
        "environment" :
          { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
        "name" : "Agreement_1_UPDATED_1601679632",
        "reconsentPeriodDays" : 360,
        "totalConsents" : 0,
        "totalExpiredConsents" : 0,
        "consentsAggregatedAt" : "2021-01-15T20:45:17.463Z",
        "enabled" : false },
      "revision" :
      { "id" : "aab73db4-9432-4149-9d24-daa8e6e1289b",
        "environment" :
          { "id" : "af2e0f45-d9cb-4aa1-a8e8-432e040ddc30" },
        "agreement" :
          { "id" : "d462d436-cf80-421c-8c05-881e9958c4b4" },
        "language" :
          { "id" : "7e156496-4e67-4adc-a139-ebbbe2c1aea" },
        "effectiveAt" : "2098-08-01T22:45:44.497Z",
        "contentType" : "text/plain",
        "requireReconsent" : false },
        "language" :
      { "id" : "a00abf13-22fc-4d66-a89e-7f6abb1d323f",
        "environment" :
          { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
        "displayName" : "Language_1601679509",
        "agreement" :
          { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
        "enabled" : true,
        "locale" : "en-US" } },
      "lastConsent" :
      { "language" :
        { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
        "revision" :
          { "id" : "90eb5621-eae8-4fa1-aafb-2a884d6848cb" },
        "at" : "2021-08-01T22:45:44.497Z",
        "expiresAt" : "2098-08-01T22:45:44.497Z" },
        "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
        "environment" :
          { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
        "user" :
          { "id" : "f880dacd-19d1-4d4e-9f2e-9d175bd03e1b" },
        "agreement" :
          { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
        "status" : "ACCEPTED" } } }
```

Read User Agreements

Find information about agreements users have accepted or signed.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Accept Language textField

The language in which the agreement is written and indicated by an IETF BCP 47 language tag, such as "en-US" or "az-Arab".

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - acceptLanguage string minLength: 0 maxLength: 100
BCP 47 Language tag used as Accept-Language header

Output Schema

- output object
 - userAgreements array
 - rawResponse object
 - _embedded object
 - userAgreements array
 - count number
 - size number
 - headers object
 - statusCode integer

Output Example

```

{ "rawResponse" :
{ "_embedded" :
{ "userAgreements" :
[
{ "_embedded" :
{ "agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"name" : "Agreement_1_UPDATED_1601679632",
"reconsentPeriodDays" : 360,
"totalConsents" : 0,
"totalExpiredConsents" : 0,
"consentsAggregatedAt" : "2021-01-15T20:45:17.463Z",
"enabled" : false },
"revision" :
{ "id" : "aab73db4-9432-4149-9d24-daa8e6e1289b",
"environment" :
{ "id" : "af2e0f45-d9cb-4aa1-a8e8-432e040ddc30" },
"agreement" :
{ "id" : "d462d436-cf80-421c-8c05-881e9958c4b4" },
"language" :
{ "id" : "7e156496-4e67-4adc-a139-ebbbbe2c1aea" },
"effectiveAt" : "2098-08-01T22:45:44.497Z",
"contentType" : "text/plain",
"requireReconsent" : false },
"language" :
{ "id" : "a00abf13-22fc-4d66-a89e-7f6abb1d323f",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"display_name" : "Language_1601679509",
"agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"enabled" : true,
"locale" : "en-US" } },
"lastConsent" :
{ "language" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"revision" :
{ "id" : "90eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"at" : "2021-08-01T22:45:44.497Z",
"expiresAt" : "2098-08-01T22:45:44.497Z" },
"id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"user" :
{ "id" : "f880dacd-19d1-4d4e-9f2e-9d175bd03e1b" },
"agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"status" : "ACCEPTED" } ] },
"count" : 1,
"size" : 1 },
"userAgreements" :
[
{ "_embedded" :
{ "agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"name" : "Agreement_1_UPDATED_1601679632",

```

```

    "reconsentPeriodDays" : 360,
    "totalConsents" : 0,
    "totalExpiredConsents" : 0,
    "consentsAggregatedAt" : "2021-01-15T20:45:17.463Z",
    "enabled" : false },
  "revision" :
  { "id" : "aab73db4-9432-4149-9d24-daa8e6e1289b",
    "environment" :
    { "id" : "af2e0f45-d9cb-4aa1-a8e8-432e040ddc30" },
    "agreement" :
    { "id" : "d462d436-cf80-421c-8c05-881e9958c4b4" },
    "language" :
    { "id" : "7e156496-4e67-4adc-a139-ebbbbe2c1aea" },
    "effectiveAt" : "2098-08-01T22:45:44.497Z",
    "contentType" : "text/plain",
    "requireReconsent" : false },
  "language" :
  { "id" : "a00abf13-22fc-4d66-a89e-7f6abb1d323f",
    "environment" :
    { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
    "displayName" : "Language_1601679509",
    "agreement" :
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
    "enabled" : true,
    "locale" : "en-US" } },
  "lastConsent" :
  { "language" :
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
    "revision" :
    { "id" : "90eb5621-eae8-4fa1-aafb-2a884d6848cb" },
    "at" : "2021-08-01T22:45:44.497Z",
    "expiresAt" : "2098-08-01T22:45:44.497Z" },
  "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
  "environment" :
  { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
  "user" :
  { "id" : "f880dacd-19d1-4d4e-9f2e-9d175bd03e1b" },
  "agreement" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
  "status" : "ACCEPTED" } ] }

```

Revoke User Agreement

Revoke agreements users have accepted or signed.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Agreement dropDown

The name of the agreement.

- Use Agreement ID (Default)

Agreement ID textField

A unique identifier for the agreement the user has accepted or signed.

Accept Language textField

The language in which the agreement is written and indicated by an IETF BCP 47 language tag, such as "en-US" or "az-Arab".

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - agreementId string minLength: 0 maxLength: 100
Agreement ID
 - acceptLanguage string minLength: 0 maxLength: 100
BCP 47 Language tag used as Accept-Language header

Output Schema

- output object
 - userAgreement object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean
 - language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string

- locale string
- enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- rawResponse object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string

- environment object
 - id string
- effectiveAt string
- contentType string
- requireReconsent boolean
- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
- environment object
 - id string
- displayName string
- locale string
- enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- headers object

- statusCode integer

Output Example

```
{ "rawResponse" :
  { "_embedded" :
    { "agreement" :
      { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
        "environment" :
          { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
          "name" : "Agreement_1_UPDATED_1601679632",
          "reconsentPeriodDays" : 360,
          "totalConsents" : 0,
          "totalExpiredConsents" : 0,
          "consentsAggregatedAt" : "2021-01-15T20:45:17.463Z",
          "enabled" : false },
        "revision" :
          { "id" : "aab73db4-9432-4149-9d24-daa8e6e1289b",
            "environment" :
              { "id" : "af2e0f45-d9cb-4aa1-a8e8-432e040ddc30" },
              "agreement" :
                { "id" : "d462d436-cf80-421c-8c05-881e9958c4b4" },
              "language" :
                { "id" : "7e156496-4e67-4adc-a139-ebbbbe2c1aea" },
              "effectiveAt" : "2098-08-01T22:45:44.497Z",
              "contentType" : "text/plain",
              "requireReconsent" : false },
            "language" :
              { "id" : "a00abf13-22fc-4d66-a89e-7f6abb1d323f",
                "environment" :
                  { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
                  "displayName" : "Language_1601679509",
                  "agreement" :
                    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
                    "enabled" : true,
                    "locale" : "en-US" } },
                "lastConsent" :
                  { "language" :
                      { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
                      "revision" :
                        { "id" : "90eb5621-eae8-4fa1-aafb-2a884d6848cb" },
                        "at" : "2021-08-01T22:45:44.497Z",
                        "expiresAt" : "2098-08-01T22:45:44.497Z" },
                        "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
                        "environment" :
                          { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
                          "user" :
                            { "id" : "f880dacd-19d1-4d4e-9f2e-9d175bd03e1b" },
                            "agreement" :
                              { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
                              "status" : "ACCEPTED" } } }
```

Accept User Agreement

Accept user agreements.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Agreement Presentation ID textField

The unique identifier for the agreement information to ensure the correct agreement revision and language is being accepted.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - agreementPresentationId string required
Read User Agreement and Read Agreement capabilities generate this id in their agreement presentation output.

Output Schema

- output object
 - userAgreement object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean
 - language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string

- locale string
- enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- rawResponse object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string

- environment object
 - id string
- effectiveAt string
- contentType string
- requireReconsent boolean
- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
- environment object
 - id string
- displayName string
- locale string
- enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- headers object

- statusCode integer

Read Agreement Content

Find information about the agreement content.

Properties

Agreement dropDown

The name of the agreement.

- Use Agreement ID (Default)

Agreement ID textField

A unique identifier for the agreement the user has accepted or signed.

Accept Language textField

The language in which the agreement is written and indicated by an IETF BCP 47 language tag, such as "en-US" or "az-Arab".

User Locale textField

The user's location, which determines the language in which the agreement is written and indicated by an IETF BCP 47 language tag, such as "en-US" or "az-Arab".

Input Schema

- default object
 - properties object
 - agreementId string minLength: 0 maxLength: 100
Agreement ID
 - acceptLanguage string minLength: 0 maxLength: 100
BCP 47 Language tag used as Accept-Language header
 - userLocale string minLength: 0 maxLength: 100
User Locale

Output Schema

- output object
 - agreementPresentation object
 - agreementPresentationId string
 - agreementText string
 - agreementTitle string
 - agreementAcceptCheckboxText string
 - agreementContinueButtonText string
 - agreementDeclineButtonText string
 - userAgreement object
 - _embedded object
 - agreement object
 - id string
 - name string
 - environment object
 - id string
 - reconsentPeriodDays number
 - totalConsents number
 - totalExpiredConsents number
 - consentsAggregatedAt string
 - enabled boolean
 - revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean

- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string
 - locale string
 - enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string
 - language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- rawResponse object
 - _embedded object
 - agreement object
 - id string
 - name string

- environment object
 - id string
- reconsentPeriodDays number
- totalConsents number
- totalExpiredConsents number
- consentsAggregatedAt string
- enabled boolean
- revision object
 - id string
 - environment object
 - id string
 - effectiveAt string
 - contentType string
 - requireReconsent boolean
- language object
 - userExperience object
 - acceptCheckboxText string
 - continueButtonText string
 - declineButtonText string
 - id string
 - environment object
 - id string
 - displayName string
 - locale string
 - enabled boolean
- lastConsent object
 - id string
 - expiresAt string
 - revision object
 - id string

- language object
 - id string
- id string
- environment object
 - id string
- user object
 - id string
- status string
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
{ "_embedded" :
{ "agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"name" : "Agreement_1_UPDATED_1601679632",
"reconsentPeriodDays" : 360,
"totalConsents" : 0,
"totalExpiredConsents" : 0,
"consentsAggregatedAt" : "2021-01-15T20:45:17.463Z",
"enabled" : false },
"revision" :
{ "id" : "aab73db4-9432-4149-9d24-daa8e6e1289b",
"environment" :
{ "id" : "af2e0f45-d9cb-4aa1-a8e8-432e040ddc30" },
"agreement" :
{ "id" : "d462d436-cf80-421c-8c05-881e9958c4b4" },
"language" :
{ "id" : "7e156496-4e67-4adc-a139-ebbbe2c1aea" },
"effectiveAt" : "2098-08-01T22:45:44.497Z",
"contentType" : "text/plain",
"requireReconsent" : false },
"language" :
{ "id" : "a00abf13-22fc-4d66-a89e-7f6abb1d323f",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"displayName" : "Language_1601679509",
"agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"enabled" : true,
"locale" : "en-US" } },
"lastConsent" :
{ "language" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"revision" :
{ "id" : "90eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"at" : "2021-08-01T22:45:44.497Z",
"expiresAt" : "2098-08-01T22:45:44.497Z" },
"id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
"environment" :
{ "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
"user" :
{ "id" : "f880dacd-19d1-4d4e-9f2e-9d175bd03e1b" },
"agreement" :
{ "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },
"status" : "ACCEPTED" } }
```

Read Population

Find population information.

Properties

Population dropDown

The name of the population.

- Use Population ID (Default)
- Use Alternative ID

Alternative Identifier textField

Enter an Alternative Identifier to look for populations.

Population ID textField

The unique identifier for the population.

Input Schema

- default object
 - properties object
 - population string required minLength: 0 maxLength: 100
Population
 - alternativeIdentifier string minLength: 0 maxLength: 255
Alternative Identifier
 - populationId string minLength: 0 maxLength: 100
Population ID

Output Schema

- output object
 - population object
 - id string
 - name string
 - description string
 - userCount number
 - createdAt string
 - updatedAt string
 - passwordPolicy object
 - id string
 - preferredLanguage string
 - defaultIdentityProvider object
 - id string
 - type string
 - alternativeIdentifiers array
 - theme object
 - id string
 - populations array
 - rawResponse object
 - id string
 - name string
 - description string
 - userCount number
 - createdAt string
 - updatedAt string
 - passwordPolicy object
 - id string
 - preferredLanguage string

- defaultIdentityProvider object
 - id string
 - type string
- alternativeIdentifiers array
- theme object
 - id string
- headers object
- statusCode integer

Read Population Internal

Find population internal.

Properties

Population dropDown

The name of the population.

- Use Population ID (Default)
- Use Alternative ID

Alternative Identifier textField

Enter an Alternative Identifier to look for populations.

Population ID textField

The unique identifier for the population.

Input Schema

- default object
 - properties object
 - population string required minLength: 0 maxLength: 100
Population
 - alternativeIdentifier string minLength: 0 maxLength: 255
Alternative Identifier

Output Schema

- output object
 - population object
 - id string
 - name string
 - description string
 - userCount number
 - createdAt string
 - updatedAt string
 - passwordPolicy object
 - id string
 - preferredLanguage string
 - defaultIdentityProvider object
 - id string
 - type string
 - alternativeIdentifiers array
 - theme object
 - id string
 - populations array
 - rawResponse object
 - id string
 - name string
 - description string
 - userCount number
 - createdAt string
 - updatedAt string
 - passwordPolicy object
 - id string
 - preferredLanguage string

- defaultIdentityProvider object
 - id string
 - type string
- alternativeIdentifiers array
- theme object
 - id string
- headers object
- statusCode integer

Read User Group Memberships

Find information about the groups to which users belong.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.

Output Schema

- output object
 - groupMemberships array
 - rawResponse object
 - _embedded object
 - groupMemberships array
 - count number
 - size number
 - headers object
 - statusCode integer

Create User Group Membership

Add a user to a group.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Group dropDown

The name of the group.

- Use Group ID (Default)

Group ID textField

The unique identifier for the group.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - groupId string minLength: 0 maxLength: 100
Group ID
 - groupName string
 - description string
 - externalId string
 - userFilter string
SCIM filter for users
 - memberGroupRelationship boolean
 - customData object

Output Schema

- output object
 - groupMembership object
 - id string
 - name string
 - population object
 - id string
 - type string
 - rawResponse object
 - groupMembership object
 - id string
 - name string
 - population object
 - id string
 - type string
 - headers object
 - statusCode integer

Delete User Group Membership

Remove a user from a group.

Properties

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Group dropDown

The name of the group.

- Use Group ID (Default)

Group ID textField

The unique identifier for the group.

Input Schema

- default object
 - properties object
 - matchAttribute string required
PingOne user attribute to identify a user with.
 - identifier string required
User attribute to match attributes.
 - groupId string minLength: 0 maxLength: 100
Group ID
 - groupName string
 - description string
 - externalId string
 - userFilter string
SCIM filter for users
 - memberGroupRelationship boolean
 - customData object

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Migrate User through Gateway

Validate a user's credentials and, if valid, migrate the user from a PingOne gateway to PingOne.

Properties

Username textField required

The user's unique identifier in the PingOne gateway.

Password textField required

The user's password in the PingOne gateway.

Gateway User Type List variableInputList required

The gateway and user type to target when validating the user's credentials. These values are based on the gateways configured in your PingOne environment.

Input Schema

- default object
 - properties object
 - usernameGateway string required

The user's unique identifier in the PingOne gateway.
 - passwordGateway string required minLength: 4 maxLength: 100

The user's password in the PingOne gateway.
 - gatewayUserTypeList array required

The gateway and user type to target when validating the user's credentials. These values are based on the gateways configured in your PingOne environment.

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Create Group

Create a user group.

Properties

Group Name textField required

The name of the group.

Group Description textArea required

The description of the group.

Dynamic User Filter textField required

A filter to automatically assign users to the group.

Population dropDown

The name of the population.

- Use Population ID (Default)
- Use Alternative ID

Population ID textField

The unique identifier for the population.

Edit Metadata Properties JSON toggleSwitch

Metadata Properties keyValueList

This input will overwrite the current metadata for the group.

Metadata Properties textArea

This input will overwrite the current metadata for the group.

Input Schema

- default object
 - properties object
 - groupId string
 - groupName string required
 - description string
 - externalId string
 - userFilter string
 - SCIM filter for users
 - memberGroupRelationship boolean
 - customData object

Output Schema

- output object
 - group object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string
 - rawResponse object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string

- headers object
- statusCode integer

Read Group

Read a user group.

Properties

Group ID textField

The unique identifier for the group.

Input Schema

- default object
 - properties object
 - groupId string required minLength: 0 maxLength: 100
Group ID

Output Schema

- output object
 - group object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string
 - rawResponse object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string

- headers object
- statusCode integer

Update Group

Update a user group.

Properties

Group ID textField

The unique identifier for the group.

Group Name textField required

The name of the group.

Group Description textArea required

The description of the group.

Dynamic User Filter textField required

A filter to automatically assign users to the group.

Edit Metadata Properties JSON toggleSwitch

Metadata Properties keyValuePairList

This input will overwrite the current metadata for the group.

Metadata Properties textArea

This input will overwrite the current metadata for the group.

Input Schema

- default object
 - properties object
 - groupId string required
 - groupName string
 - description string
 - externalId string
 - userFilter string
 - SCIM filter for users
 - memberGroupRelationship boolean
 - customData object

Output Schema

- output object
 - group object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string
 - rawResponse object
 - id string
 - environment object
 - id string
 - customData object
 - population object
 - id string
 - name string
 - description string
 - isExternal string
 - externalId string
 - userFilter string
 - createdAt string
 - updatedAt string

- headers object
- statusCode integer

Delete Group

Delete a user group.

Properties

Group ID textField

The unique identifier for the group.

Input Schema

- default object
 - properties object
 - groupId string required minLength: 0 maxLength: 100
Group ID

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Read Group Members

Read up to 100 members of a group.

Properties

Group ID textField

The unique identifier for the group.

PingOne Attributes textFieldArrayView

Enter the PingOne attributes you want to use to find a user, such as username, userID, or email.

Identifier textField

Enter the identifier, which was captured earlier in the flow, that you want to use to find a user. For example, if the attributes specified are email and username, and the identifier is username, the system will search for users whose email or username match the value captured under username.

Direct Member Relationship toggleSwitch

The output will only include members that are directly assigned to the group, instead of including any members assigned by a filter.

Input Schema

- default object
 - properties object
 - groupId string required minLength: 0 maxLength: 100
 - Group ID

Output Schema

- output object
 - matchedUsers array
 - count integer
 - rawResponse object
 - _embedded object
 - matchedUsers array
 - count integer
 - headers object
 - statusCode integer

Output Example

```

{ "rawResponse" :
  { "_embedded" :
    { "matchedUsers" :
      [
        { "_embedded" :
          { "user" :
            { "preferredLanguage" : "EN",
              "timezone" : "EST",
              "lastSignOn" :
                { "at" : "00:00:00:0000",
                  "remoteIp" : "127.0.0.1" },
              "title" : "test",
              "type" : "Admin",
              "locale" : "EN",
              "enabled" : true,
              "createdAt" : "00:00:00:0000",
              "verifyStatus" : "NOT_VERIFIED",
              "nickname" : "test",
              "mfaEnabled" : false,
              "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
              "email" : "ping@pingidentity.com",
              "username" : "test" } } } ] } },
      "matchedUsers" :
      [
        { "_embedded" :
          { "user" :
            { "preferredLanguage" : "EN",
              "timezone" : "EST",
              "lastSignOn" :
                { "at" : "00:00:00:0000",
                  "remoteIp" : "127.0.0.1" },
              "title" : "test",
              "type" : "Admin",
              "locale" : "EN",
              "enabled" : true,
              "createdAt" : "00:00:00:0000",
              "verifyStatus" : "NOT_VERIFIED",
              "nickname" : "test",
              "mfaEnabled" : false,
              "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
              "email" : "ping@pingidentity.com",
              "username" : "test" } } } ] } }

```

Authenticate User via Kerberos

Authenticate Active Directory users seamlessly via the Kerberos protocol.

Properties

Gateway dropDown required

Select the gateway that connects to the Active Directory servers where the users are located.

User Type dropDown required

Select the user type through which the users can be found.

Default: `useUserId`

Create PingOne User toggleSwitch

When enabled, DaVinci creates a PingOne user account using attributes from Active Directory. Disable this to support a legacy integration where DaVinci is configured as an External IdP in PingOne.

Input Schema

- default object
 - properties object
 - gatewayId string required
Gateway Id
 - userId string required
User Type ID
 - createUserIfNotFound boolean

Output Schema

- output object
 - user object
 - id string
 - username string
 - environment object
 - id string
 - population object
 - id string
 - rawResponse object
 - statusCode number
 - headers object

Unlock User

Unlock a user by their user ID.

Properties

User ID textField

ID of the User.

Input Schema

- default object
 - properties object
 - userId string required

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Single-Factor Sign On

Sign on with username and password

Properties

Sign On Form dropDown required

Select the sign on form for single-factor authentication.

Form Theme dropDown required

Choose a form theme from the themes configured in PingOne environment or use a Theme ID. If no theme is selected, the default active theme will be displayed

- PingOne Active Theme (Default)
- Use Theme ID

Theme ID textField

The ID of the PingOne theme to use when rendering the form, such as “aa4b3e81-cf7e-8685-4b7b-7ec89cfcf7c8”.

Input Schema

- default object
 - properties object
 - singleFactorSignInFormId string required
Single-Factor Sign On Form ID

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- passwordState object
 - environment object
 - id string
 - user object
 - id string
 - passwordPolicy object
 - id string

- warnings object
 - expires string
 - noChangeUntil string
 - failuresRemaining number
- status string
- lastChangedAt string
- buttonValue string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignIn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string

- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Update User through Gateway

Retrieve a user's attributes through a PingOne gateway and update the PingOne user profile with them.

Properties

Override User toggleSwitch

User ID is mapped automatically unless you override them here.

PingOne Attribute dropDown

Select the attribute that you want to match against the provided identifier to find a user.

- User ID (Default)
- Username
- Email

Identifier textField

Enter the User ID, Username, or Email address of the user that you want to find.

Input Schema

- default object
 - properties object
 - overrideUser boolean
Override User
 - matchAttribute string
PingOne user attribute to identify a user with.
 - identifier string
User attribute to match attributes.
 - authentication object
 - userId string
 - methods array

Output Schema

- output object
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - emailVerified boolean
 - updatedAt string
 - address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string

- countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawResponse object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string

- type string
- locale string
- enabled boolean
- identityProvider object
 - id string
 - type string
- lifecycle object
 - status string
- createdAt string
- verifyStatus string
- nickname string
- mfaEnabled boolean
- id string
- email string
- emailVerified boolean
- updatedAt string
- address object
 - streetAddress string
 - locality string
 - region string
 - postalCode string
 - countryCode string
- externalId string
- photo object
 - href string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string

- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- headers object
- statusCode integer

Read Theme

Read a theme.

Properties

Theme ID textField

The ID of the PingOne theme to use when rendering the form, such as "aa4b3e81-cf7e-8685-4b7b-7ec89cfc7c8".

Input Schema

- default object
 - properties object
 - themeld string required minLength: 0 maxLength: 100
- Theme ID

Output Schema

- output object
 - theme object
 - id string
 - environment object
 - id string
 - template string
 - default boolean
 - configuration object
 - logoType string
 - logo object
 - href string
 - id string
 - backgroundColor string
 - backgroundType string
 - backgroundImage object
 - href string
 - id string
 - bodyTextColor string
 - cardColor string
 - headingTextColor string
 - linkTextColor string
 - buttonTextColor string
 - buttonColor string
 - name string
 - footer string
 - rawResponse object
 - id string
 - environment object
 - id string

- template string
- default boolean
- configuration object
 - logoType string
 - logo object
 - href string
 - id string
 - backgroundColor string
 - backgroundType string
 - backgroundImage object
 - href string
 - id string
 - bodyTextColor string
 - cardColor string
 - headingTextColor string
 - linkTextColor string
 - buttonTextColor string
 - buttonColor string
 - name string
 - footer string
- headers object
- statusCode integer

Limitations

The following are known issues or limitations with the PingOne connector:

LiveSync operations

The PingOne connector does not support LiveSync operations.

If you attempt to implement LiveSync, you receive the following error:

Operation `org.identityconnectors.framework.api.operations.SyncApiOp` is not supported by the Connector.

For data synchronization, implement scheduled reconciliation which is supported.

PingOne Connector Release Notes

New features and improvements in the PingOne connector. Updated June 4, 2025.

June 2025

Read Theme

New

You can now use the **Read Theme** capability to get theme details with the theme ID. This helps when designing PingOne DaVinci multi-brand experiences.

Update User through Gateway

New

You can now use the **Update User through Gateway** capability to retrieve a user's attributes through a PingOne gateway and update the PingOne user profile with them.

April 2025

Authenticate User via Kerberos

Improved

The **Authenticate User via Kerberos** capability now supports the selection of a user type, regardless of whether user migration is enabled or not.

The ability to select a user type without user migration allows you to create DaVinci flows to offer seamless SSO authentication experience to users provisioned from Microsoft Active Directory into PingOne through an [LDAP gateway provisioning connection](#) and an [inbound rule](#).

Note

The selected LDAP gateway must be configured with at least one user type.

March 2025

Read Population

Improved

You can now use the **Read Population** capability to include the default preferred language to support building an authentication experience.

Update User

Improved

You can now use the **Update User** capability to clear user attributes from a user profile.

December 2024*Read Population***Improved**

You can now use the **Read Population** capability to determine a user's population based on an alternative identifier value and can also specify a theme to support multi-brand authentication experiences.

October 2024*Managing group metadata***Improved**

The following capabilities allow you to manage group metadata.

- Read Group
- Create Group
- Update Group

April 2024*PingOne user lookup capabilities now update the global variable for user ID***Improved**

The following capabilities now update the `p1userid` global variable in DaVinci with the user ID when the user is successfully found:

- Find User
- Check Password
- Create User
- Read User

This update allows you to use the `p1userid` global variable in the flow to ensure the user ID will be populated at the right times.

February 2024*Authenticate user through Kerberos***New**

You can use the new **Authenticate User Via Kerberos** capability to authenticate Active Directory users seamlessly through the Kerberos protocol.

August 2023

Search for users with a custom SCIM filter

New

Previously, when searching for users with **Find User** and **Find Multiple Users**, the capability builds a SCIM filter based on a list of attributes and a search term.

You can now provide your own filter by toggling on the new **Custom SCIM Filter** field, allowing you to pick the operators used for filtering and allow different values to be searched for each attribute.

Create and update user mappings updated to resolve error from PingOne

Improved

The **Create User** and **Update User** capabilities mappings no longer pass empty values to PingOne. Previously, PingOne sent an error to DaVinci due to empty values.

If a field is included with no value, the connector would normally pass it to PingOne as an empty string. If no field or value is included, the connector would normally pass it as a null value. Now, these values are omitted and not passed as empty values.

June 2023

Unlock user account

New

The new **Unlock User** capability allows you to unlock a locked PingOne user account:

New group CRUD capabilities

New

To support group manipulation during flows in DaVinci, we have added the following capabilities:

- **Create Group**
- **Read Group**
- **Update Group**
- **Delete Group**
- **Read Group Members**

These allow you to create, manage, and read groups in a PingOne environment.

April 2023

Find multiple users

New

You can now use the **Find Multiple Users** capability to search and return up to 100 users.

October 2022

Manage group memberships for PingOne users

New

The following new capabilities allow you to manage which groups a user belongs to:

- **Create User Group Membership**
- **Delete User Group Membership**

Combined with the existing **Read User Group Memberships** capability, this provides you with a more complete membership management experience.

Migrate users from an LDAP datastore to PingOne

New

The new **Migrate User through Gateway** capability allows you to authenticate a user against an LDAP gateway set up in PingOne, then automatically migrate the account to the main PingOne user store.

By integrating this into your existing authentication flow, you can migrate users gradually as they sign on.

The **Gateway User Type List** property allows you to filter by specific gateways and user types.

Force a user to set a new password next time they sign on

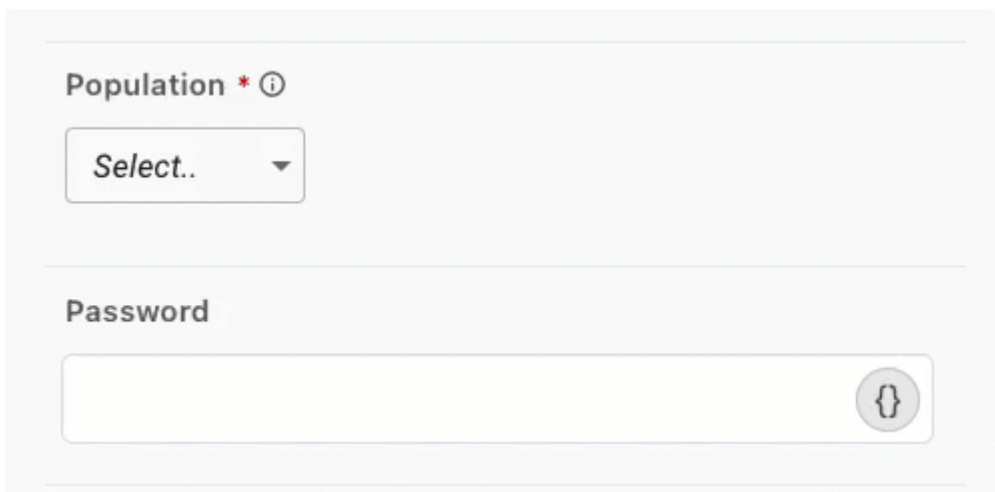
New

This change allows you to set a flag that forces a user to set a new password next time they sign on.

Previously, the new password had to be set by the administrator when flagging the account.

Dynamically populated capability fields

Improved



The screenshot shows a user management interface with two main sections. The top section is titled 'Population' with a red asterisk and an information icon. Below the title is a dropdown menu with the text 'Select..' and a downward arrow. The bottom section is titled 'Password' and contains a text input field. To the right of the input field is a circular icon containing a curly brace '{'.

When configuring a connector capability, DaVinci now populates properties, such as **Population** and **Agreement**, with information from PingOne.

Your existing configuration still works, and you can always select **Use Population ID** (or the equivalent) to show a manual entry field. This lets you manually enter a value or use a dynamic value from your flow.

Simpler attributes list for creating and updating users

Improved

Previously, the **Create User** and **Update User** capabilities allowed you to define additional user attribute mappings by manually typing attributes and values in the **Other Attributes** section.

To make the configuration more convenient, the attribute names and data types are now populated automatically from your PingOne environment.

Default error messages for capabilities

Improved

All connector capabilities now use the default error messages from the PingOne API. This makes it easier to set up a flow with meaningful error messages.

You can override these messages on the **Mappings (Error Messages)** tab of the capability configuration.

Use your default PingOne population

Improved

When configuring capabilities that need a population, you can now select **Use Default Population** instead of selecting a specific population.

When you set a default population in PingOne, all capabilities with this setting will automatically use that population.

February 2022

The PingOne connector is now available

New

You can use the PingOne connector to:

- Create a sign-on flow for authentication
- Reset a user's password
- Register new users in the PingOne user store
- Create, edit, and delete users in the PingOne user store
- Verify a user's email address
- View a user's population
- View a user's group membership

- View agreements and consents for a user

PingOne Advanced Identity Cloud Access Request Connector

The PingOne Advanced Identity Cloud Access Request connector lets you manage users and create access requests in PingOne Advanced Identity Cloud in your PingOne DaVinci flow.

You can use the PingOne Advanced Identity Cloud Access Request connector to:

- Manage users
- Create access requests
- Make custom API calls

Setup

Resources

For information and setup help, see the following:

- Identity Cloud documentation:
 - [About Identity Governance](#)
 - [Identity Governance REST API](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne Advanced Identity Cloud environment
- An Access Request license for Identity Governance

Setting up PingOne Advanced Identity Cloud

Setting up a service account

The service account acts like an administrator account and is required for all user CRUD capabilities as well as for System Requests using the **Make a Custom API Call** capability.

To set up a service account:

1. Sign on to the Advanced Identity Cloud admin portal.

2. Select **Account**, then **Tenant Settings**.
3. Under **Service Accounts**, select **New Service Account**.
4. Give the new service account a name and select `fr:idm:* All Identity Management APIs`.
5. Click **Save**.
6. Note the **ID**. You will use it for the **Service Account ID** in the connector configuration.
7. Click **Download Key** to save the key as a `.jwk` file. You will use it for the **Service Account Key** in the connector configuration.

Setting up an end user account

The end user account acts on behalf of any single user and is required for user-centric capabilities, such as **Get Request**, **Get Requestable Items**, and **Create Request**, as well as for the End User Requests using the **Make a Custom API Call**. This setup is not required for using the connector's user CRUD capabilities or making a custom API call.

The Frodo command-line interface (CLI) is a Ping Identity-developed utility that allows for advanced management of Advanced Identity Cloud. The following steps create credentials that are unique to your DaVinci environment and you can only have one set of credentials for Advanced Identity Cloud for a given DaVinci environment. If you have multiple environments, such as for staging and production, repeat these steps so each DaVinci environment has its own end user credentials in your Advanced Identity Cloud tenant.

To set up an end user account:

1. Install Frodo CLI 2.0.0-36 or later.

1. In your CLI, enter the following command:

```
% brew tap rockcarver/frodo-cli
```

2. Install the latest pre-release by entering the following command:

```
% brew install frodo-cli-next
```

2. Link the Frodo CLI to your Identity Cloud environment. In your CLI, enter the following command, adding your Advanced Identity Cloud **email** and **password** credentials:

```
% frodo conn save https://openam-frodo-dev.forgeblocks.com/am <email> '<password>'
```

3. Use the Frodo CLI to create a client ID for the end user and the OIDC issuer.

1. For regular environments, enter the following command, adding your **client ID**, **domain**, **DaVinci environment ID**, and **Identity Cloud tenant ID** parameters:

```
% frodo admin generate-rfc7523-authz-grant-artefacts --client-id <client ID> --scope "openid fr:am:* fr:idm:* fr:iga:*" --iss https://<domain>/<DaVinci environment ID>/davinci <Identity Cloud tenant ID>
```


 Note

See the following example of the command with the appropriate parameters:

+

```
% frodo admin generate-rfc7523-authz-grant-artefacts --client-id myclientid --scope "openid fr:am:* fr:idm:* fr:iga:*" --iss https://auth.pingone.eu/b5063c3e-d9c8-42c6-99bf-9e19a96a617b/davinci open-am-mycompany
```

2. For a custom domain environment, enter the following command, adding your **client ID**, **domain**, and **Identity Cloud tenant ID** parameters:

```
% frodo admin generate-rfc7523-authz-grant-artefacts --client-id <client ID> --scope "openid fr:am:* fr:idm:* fr:iga:*" --iss https://<domain>/davinci <Identity Cloud tenant ID>
```

 Note

See the following example of the command with the appropriate parameters:

+

```
% frodo admin generate-rfc7523-authz-grant-artefacts --client-id myclientid --scope "openid fr:am:* fr:idm:* fr:iga:*" --iss https://mydomain.com/davinci open-am-mydomain
```

4. Copy the **End User Client ID** and **End User Client Private Key** from that end user account to your PingOne Advanced Identity Cloud Access Request connector configuration.

Configuring the PingOne Advanced Identity Cloud Access Request connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Identity Cloud Base URL

The API URL to target.

Realm

The PingOne Advanced Identity Cloud realm.

Service Account ID

The account ID from your PingOne Advanced Identity Cloud service account. Paste the ID that you noted when you set up the service account.

Service Account Private Key

The private key from your PingOne Advanced Identity Cloud service account. Paste the complete contents of the `.jwk` file that you downloaded when you set up the service account.

End User Client ID

The client ID from the end user account.

End User Client Private Key

The client private key from the end user account.

Using the connector in a flow

Manage users in Identity Cloud

The connector has several capabilities that allow you to manage users:

- Find Users
- Get User Information
- Create User
- Update User
- Delete User

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating access requests

You can use the PingOne Advanced Identity Cloud Access Request connector to allow a user to create an access request. If you know the information about the access request you want to create, such as the IDs for the user and entitlements, you can use the **Create Request** capability directly. If you need to get that information at runtime, you can use the **Get User Information** or **Get List of Requestable Items** capabilities first and use the results in the **Create Request** capability.

To create an access request:

1. Add a node in the flow with the capability to capture a user identifier, such as email or username.
2. Add the PingOne Advanced Identity Cloud Access Request connector with **Get Request** in a subsequent node in the flow. Configure with the **Identity Management Attribute** and specific **Identifier** captured earlier in the field.
3. Add another node with the **Get Requestable Items** capability and configure with the **Identity Management Attribute** and specific **Identifier** captured earlier in the field.
4. Add another node with the **Create Request** capability and configure based on the help text.

Note

You can get **User IDs**, **Application IDs**, **Entitlement IDs** and **Role IDs** using the **Get Requestable Items** capability and include them as variables in the **Create Request** capability configuration fields. The following screenshot shows the valid JSON structure for all of the ID fields as well as the format for a variable:

The screenshot displays two examples of input fields for 'User IDs'. Both fields are labeled 'User IDs * ⓘ' and have a JSON schema icon on the right. The top field contains the static JSON array `[\"f787e983-a6ee-4418-9874-a36dae8bae82\"]`. The bottom field contains a dynamic variable `[\"{{ping_id}}\"]`, where the variable `{{ping_id}}` is highlighted with a red circle and a 'Ping' icon.

The above examples show a single ID. Separate multiple IDs with a comma, for example: `[\"1234\", \"2345\", \"3456\"]`.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify. You can use the **Request Type** list to change between **System Requests** and **End User Requests**.

 Note

System Requests are used for general administration of Advanced Identity Cloud, such as user management.
End User Requests are used for user-centric tasks with Identity Governance, such as managing access requests and access reviews.

Capabilities

Find Users

Search for users based on identifier or filter.

Properties

Custom Filter toggleSwitch

When enabled, you can search for users based on a custom filter instead of an identifier.

Filter textField

The Common REST filter query to use, such as "givenName eq 'John' and sn eq 'Doe'

". For help, see the IDM documentation > REST API Reference > Common REST > Query."

Identity Management Attributes textFieldArrayView

Select the attribute(s) that contains the user identifier provided in the identifier field. Used to identify the user.

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountprivateKey string
 - useCustomFilter boolean required
 - customFilter string
 - matchAttributes array
 - userIdentifier string

Output Schema

- output object
 - rawResponse object
 - result array
 - resultCount integer
 - pagedResultsCookie string
 - totalPagedResultsPolicy string
 - totalPagedResults integer
 - remainingPagedResults integer
 - statusCode number
 - headers object
 - userIds array

Get User Information

Get information about a user.

Properties

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - matchAttribute string required
 - userIdentifier string required

Output Schema

- output object
 - rawResponse object
 - _id string
 - _rev string
 - country string
 - frUnindexedString1 string
 - mail string
 - memberOfOrgIDs array
 - frIndexedDate5 string
 - frUnindexedString2 string
 - frIndexedDat4 string
 - frUnindexedString3 string
 - frIndexedDate3 string
 - frUnindexedString4 string
 - postalCode string
 - frUnindexedString5 string
 - profileImage string
 - frIndexedString5 string
 - frIndexedString4 string
 - frIndexedString3 string
 - frIndexedString2 string
 - frIndexedString1 string
 - frIndexedMultivalued3 array
 - frUnindexedInteger5 number
 - consentedMappings array
 - frIndexedMultivalued4 array
 - frUnindexedInteger4 number
 - frIndexedMultivalued5 array
 - frUnindexedInteger3 number

- frUnindexedInteger2 number
- effectiveGroups array
- frIndexedMultivalued1 array
- frIndexedMultivalued2 array
- frUnindexedInteger1 number
- givenName string
- stateProvince string
- postalAddress string
- telephoneNumber string
- city string
- displayName string
- effectiveAssignments array
- description string
- effectiveApplications array
- accountStatus string
- frUnindexedDate3 string
- frUnindexedMultivalued1 array
- frUnindexedDate2 string
- frUnindexedDate5 string
- frUnindexedMultivalued3 array
- frUnindexedDate4 string
- frUnindexedMultivalued2 array
- aliasList array
- frUnindexedMultivalued5 array
- frUnindexedMultivalued4 array
- kbaInfo array
- frIndexedInteger4 number
- frIndexedInteger3 number
- frIndexedInteger2 number
- frIndexedInteger1 number

- sn string
- frUnindexedDate1 string
- frIndexedInteger5 number
- preferences object
- userName string
- frIndexedDate2 string
- frIndexedDate1 string
- effectiveRoles array
- statusCode number
- headers object

Create User

Create a new user account.

Properties

Username textField required

The username assigned to the new user.

First Name textField required

The first name of the new user.

Last Name textField required

The last name of the new user.

Email Address textField required

The email address of the new user.

Password textField required

The password for the new user.

User Attributes variableInputList

Add user attributes and their values.

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - userName string required
 - givenName string required
 - sn string required
 - mail string required
 - password string
 - userAttributes array

Output Schema

- output object
 - rawResponse object
 - _id string
 - _rev string
 - country string
 - frUnindexedString1 string
 - mail string
 - memberOfOrgIDs array
 - frIndexedDate5 string
 - frUnindexedString2 string
 - frIndexedDat4 string
 - frUnindexedString3 string
 - frIndexedDate3 string
 - frUnindexedString4 string
 - postalCode string
 - frUnindexedString5 string
 - profileImage string
 - frIndexedString5 string
 - frIndexedString4 string
 - frIndexedString3 string
 - frIndexedString2 string
 - frIndexedString1 string
 - frIndexedMultivalued3 array
 - frUnindexedInteger5 number
 - consentedMappings array
 - frIndexedMultivalued4 array
 - frUnindexedInteger4 number
 - frIndexedMultivalued5 array
 - frUnindexedInteger3 number

- frUnindexedInteger2 number
- effectiveGroups array
- frIndexedMultivalued1 array
- frIndexedMultivalued2 array
- frUnindexedInteger1 number
- givenName string
- stateProvince string
- postalAddress string
- telephoneNumber string
- city string
- displayName string
- effectiveAssignments array
- description string
- effectiveApplications array
- accountStatus string
- frUnindexedDate3 string
- frUnindexedMultivalued1 array
- frUnindexedDate2 string
- frUnindexedDate5 string
- frUnindexedMultivalued3 array
- frUnindexedDate4 string
- frUnindexedMultivalued2 array
- aliasList array
- frUnindexedMultivalued5 array
- frUnindexedMultivalued4 array
- kbaInfo array
- frIndexedInteger4 number
- frIndexedInteger3 number
- frIndexedInteger2 number
- frIndexedInteger1 number

- sn string
- frUnindexedDate1 string
- frIndexedInteger5 number
- preferences object
- userName string
- frIndexedDate2 string
- frIndexedDate1 string
- effectiveRoles array
- statusCode number
- headers object

Update User

Update information about a user.

Properties

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

User Attributes variableInputList

Add user attributes and their values.

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - userAttributes array

Output Schema

- output object
 - rawResponse object
 - _id string
 - _rev string
 - country string
 - frUnindexedString1 string
 - mail string
 - memberOfOrgIDs array
 - frIndexedDate5 string
 - frUnindexedString2 string
 - frIndexedDat4 string
 - frUnindexedString3 string
 - frIndexedDate3 string
 - frUnindexedString4 string
 - postalCode string
 - frUnindexedString5 string
 - profileImage string
 - frIndexedString5 string
 - frIndexedString4 string
 - frIndexedString3 string
 - frIndexedString2 string
 - frIndexedString1 string
 - frIndexedMultivalued3 array
 - frUnindexedInteger5 number
 - consentedMappings array
 - frIndexedMultivalued4 array
 - frUnindexedInteger4 number
 - frIndexedMultivalued5 array
 - frUnindexedInteger3 number

- frUnindexedInteger2 number
- effectiveGroups array
- frIndexedMultivalued1 array
- frIndexedMultivalued2 array
- frUnindexedInteger1 number
- givenName string
- stateProvince string
- postalAddress string
- telephoneNumber string
- city string
- displayName string
- effectiveAssignments array
- description string
- effectiveApplications array
- accountStatus string
- frUnindexedDate3 string
- frUnindexedMultivalued1 array
- frUnindexedDate2 string
- frUnindexedDate5 string
- frUnindexedMultivalued3 array
- frUnindexedDate4 string
- frUnindexedMultivalued2 array
- aliasList array
- frUnindexedMultivalued5 array
- frUnindexedMultivalued4 array
- kbaInfo array
- frIndexedInteger4 number
- frIndexedInteger3 number
- frIndexedInteger2 number
- frIndexedInteger1 number

- sn string
- frUnindexedDate1 string
- frIndexedInteger5 number
- preferences object
- userName string
- frIndexedDate2 string
- frIndexedDate1 string
- effectiveRoles array
- statusCode number
- headers object

Delete user

Delete a user account.

Properties

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - matchAttribute array required
 - userIdentifier string required

Output Schema

- output object
 - rawResponse object
 - _id string
 - _rev string
 - country string
 - frUnindexedString1 string
 - mail string
 - memberOfOrgIDs array
 - frIndexedDate5 string
 - frUnindexedString2 string
 - frIndexedDat4 string
 - frUnindexedString3 string
 - frIndexedDate3 string
 - frUnindexedString4 string
 - postalCode string
 - frUnindexedString5 string
 - profileImage string
 - frIndexedString5 string
 - frIndexedString4 string
 - frIndexedString3 string
 - frIndexedString2 string
 - frIndexedString1 string
 - frIndexedMultivalued3 array
 - frUnindexedInteger5 number
 - consentedMappings array
 - frIndexedMultivalued4 array
 - frUnindexedInteger4 number
 - frIndexedMultivalued5 array
 - frUnindexedInteger3 number

- frUnindexedInteger2 number
- effectiveGroups array
- frIndexedMultivalued1 array
- frIndexedMultivalued2 array
- frUnindexedInteger1 number
- givenName string
- stateProvince string
- postalAddress string
- telephoneNumber string
- city string
- displayName string
- effectiveAssignments array
- description string
- effectiveApplications array
- accountStatus string
- frUnindexedDate3 string
- frUnindexedMultivalued1 array
- frUnindexedDate2 string
- frUnindexedDate5 string
- frUnindexedMultivalued3 array
- frUnindexedDate4 string
- frUnindexedMultivalued2 array
- aliasList array
- frUnindexedMultivalued5 array
- frUnindexedMultivalued4 array
- kbaInfo array
- frIndexedInteger4 number
- frIndexedInteger3 number
- frIndexedInteger2 number
- frIndexedInteger1 number

- sn string
- frUnindexedDate1 string
- frIndexedInteger5 number
- preferences object
- userName string
- frIndexedDate2 string
- frIndexedDate1 string
- effectiveRoles array
- statusCode number
- headers object

Get Requestable Items

Get a list of requestable items.

Properties

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - endUserClientPrivateKey string required
 - endUserClientId string required
 - matchAttribute string required
 - userIdentifier string required

Output Schema

- output object
 - rawResponse object
 - result array
 - searchAfterKey array
 - totalCount integer
 - resultCount integer
 - statusCode number
 - headers object
 - applicationIds array
 - entitlementIds array
 - roleIds array

Create Request

Start an access request by providing a list of requested items.

Properties

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "jsmith@example.com". This is checked against the selected Identity Management Attribute(s).

User IDs textField

Array of user IDs in JSON array format, such as ["1d0e...ca94b","debd...2bcf","11e4...cd95"].

Application IDs textField

Array of application IDs in JSON array format, such as ["1d0e...ca94b","debd...2bcf","11e4...cd95"].

Entitlement IDs textField

Array of entitlement IDs in JSON array format, such as ["1d0e...ca94b","debd...2bcf","11e4...cd95"].

Role IDs textField

Array of role IDs in JSON array format, such as ["1d0e...ca94b","debd...2bcf","11e4...cd95"].

Priority dropDown required

Select a priority level for the request. Your organization can consider the priority level when reviewing the request.

- Low (Default)
- Medium
- High

Request Action dropDown required

Select an action for the request.

- Add (Default)
- Remove

Expiry Date dateTimePicker required

The date that the request should expire. Use this when the resource is required before a certain date and the request won't be relevant after that date.

Justification textField required

Comment on the reason for requesting access to the selected resources.

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - endUserId string required
 - endUserClientPrivateKey string required
 - matchAttribute string required
 - userIdentifier string required
 - userIds string required
 - applicationIds string
 - entitlementIds string
 - roleIds array
 - priority string required
 - requestType string required
 - expiryDate string
 - justification string

Output Schema

- output object
 - rawResponse object
 - result array
 - statusCode number
 - headers object

Get Request

Get information about an existing request.

Properties

Identity Management Attribute dropdown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Request ID textField required

The unique ID of the request, such as "bcac0387-e5ea-4c22-981c-df0ea340f1ee".

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - endUserClientPrivateKey string required
 - endUserClientId string required
 - matchAttribute string required
 - userIdentifier string required
 - requestId string required

Output Schema

- output object
 - rawResponse object
 - id string
 - requester object
 - mail string
 - givenName string
 - id string
 - sn string
 - userName string
 - isAdmin boolean
 - requestType string
 - request object
 - common object
 - priority string
 - expiryDate string
 - justification string
 - entitlementId string
 - applicationId string
 - userId string
 - isDraft boolean
 - user object
 - _rev string
 - accountStatus string
 - aliasList array
 - assignedDashboard array
 - city string
 - cn string
 - consentedMappings array
 - country string

- description string
- displayName string
- effectiveApplications array
- effectiveAssignments array
- effectiveGroups array
- effectiveRoles array
- fr object
 - realm string
- frIndexedDate1 string
- frIndexedDate2 string
- frIndexedDate3 string
- frIndexedDate4 string
- frIndexedDate5 string
- frIndexedInteger1 number
- frIndexedInteger2 number
- frIndexedInteger3 number
- frIndexedInteger4 number
- frIndexedInteger5 number
- frIndexedMultivalued1 array
- frIndexedMultivalued2 array
- frIndexedMultivalued3 array
- frIndexedMultivalued4 array
- frIndexedMultivalued5 array
- frIndexedString1 string
- frIndexedString2 string
- frIndexedString3 string
- frIndexedString4 string
- frIndexedString5 string
- frUnindexedDate1 string
- frUnindexedDate2 string

- frUnindexedDate3 string
- frUnindexedDate4 string
- frUnindexedDate5 string
- frUnindexedInteger1 string
- frUnindexedInteger2 string
- frUnindexedInteger3 string
- frUnindexedInteger4 string
- frUnindexedInteger5 string
- frUnindexedMultivalued1 array
- frUnindexedMultivalued2 array
- frUnindexedMultivalued3 array
- frUnindexedMultivalued4 array
- frUnindexedMultivalued5 array
- frUnindexedString1 string
- frUnindexedString2 string
- frUnindexedString3 string
- frUnindexedString4 string
- frUnindexedString5 string
- givenName string
- id string
- kbaInfo array
- lastSync string
- mail string
- memberOfOrgIDs array
- postalAddress string
- postalCode string
- preferences object
 - marketing boolean
 - updates boolean
- profileImage string

- sn string
- stateProvince string
- telephoneNumber string
- userName string
- glossary object
 - idx object
 - /entitlement object
 - entitlementOwner string
 - requestable boolean
 - /application object
 - requestable boolean
 - types array
- entitlement object
 - Label string
 - Name string
 - _id string
- assignment object
 - _rev string
 - attributes array
 - description string
 - fr object
 - realm string
 - id string
 - mapping string
 - metadata object
 - entityType string
 - created string
 - name string
 - type string

- application object
 - _rev string
 - fr object
 - realm string
 - id string
 - metadata object
 - entityType string
 - created string
 - name string
 - templateName string
 - templateVersion string
 - url string
- applicationOwner array
- decision object
 - status string
 - decision string
 - outcome string
 - startDate string
 - completionDate string
 - deadline string
 - comments array
 - actors object
 - active array
 - inactive array
 - actorTags array
- events object
 - expiration object
 - date string
- phases array

- workflow object
 - instanceId string
 - id string
- statusCode number
- headers object

Make Custom API Call

Define and use your own API call to Identity Cloud.

Properties

Request Type dropDown required

The type of request.

- System Request (Default)
- End User Request

Identity Management Attribute dropDown

Select the attribute that contains the user identifier provided in the identifier field. Used to identify the user.

- User ID (Default)
- Username
- Email

Identifier textField

The unique identifier, such as "[jsmith@example.com](#)". This is checked against the selected Identity Management Attribute(s).

Endpoint textField required

The Identity Cloud API endpoint.

HTTP Method dropDown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE
- PATCH

Query Parameters keyValuePairList

Define additional query parameters for the request.

Additional Headers keyValuePairList

Additional headers for the request.

Body codeEditor

The body of the API call.

Input Schema

- default object
 - properties object
 - baseUrl string required
 - realm string required
 - serviceAccountId string required
 - serviceAccountPrivateKey string required
 - apiRequestType string required
 - endpoint string required
 - method string required
 - queryParameters array
 - headers array
 - bodyData object

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

PingOne Advanced Identity Cloud Access Request Connector Release Notes

New features and improvements in the PingOne Advanced Identity Cloud Access Request connector.

April 2024

The PingOne Advanced Identity Cloud Access connector is now available

New

You can use the PingOne Advanced Identity Cloud Access connector to:

- Manage users

- Create access requests
- Make custom API calls

PingOne Advanced Identity Cloud Login Connector

The PingOne Advanced Identity Cloud Login connector lets you authenticate users using the default journey in PingOne Advanced Identity Cloud in your PingOne DaVinci flow.

Setup

Resources

For information and setup help, see the following:

- Advanced Identity Cloud documentation:
 - [About Identity Governance](#)
 - [Identity Governance REST API](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- An Advanced Identity Cloud license
- A license for Identity Governance

Setting up PingOne Advanced Identity Cloud

To allow DaVinci to access PingOne Advanced Identity Cloud environment, create an application:

1. In PingOne Advanced Identity Cloud, go to **Applications**.
2. Click **+ Custom Application**.
3. Select **OIDC - OpenId Connect**, then click **Next**.
4. Select **Web**, then click **Next**.
5. Enter the application name and description, and select an owner. Click **Next**.
6. Define a client ID and secret.

**Note**

The **Client ID** and **Client Secret** are needed for the connector configuration.

7. Click **Create Application**.
8. On the application details view, go to the **Sign On** tab.
9. In the PingOne Advanced Identity Cloud Login connector configuration, copy the **DaVinci Redirect URL** value from the connector settings and paste it into the **Sign-in URLs** field.
10. For **Grant Types**, use the defaults (`Authorization Code` , `Client Credentials` , and `Refresh Token`).
11. For **Scopes**, use `openid` at minimum. You can define additional OIDC scopes, such as `profile` , `email` , `address` , and `phone` .
12. Click **Save**.

Configuring the PingOne Advanced Identity Cloud Login connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Client ID

The client ID you defined when configuring your application in PingOne Advanced Identity Cloud.

Client Secret

The client secret you defined when configuring your application in PingOne Advanced Identity Cloud.

Issuer URL

The URL containing information about the identity provider (IdP) that can be validated.

Scope

The OpenID Connect (OIDC) scopes used to request certain information about the user. Separate scopes with a space, such as `openid email profile` .

Application Redirect URL

Your application's redirect URL, such as "https://app.yourorganization.com/". Enter this URL if you embed the DaVinci widget in your application. This allows DaVinci to redirect the browser back to your application.

DaVinci Redirect URL

Enter this URL in your Advanced Identity Cloud console under the **Application** tab.

Using the connector in a flow

Authenticating users

You can use the **PingOne Advanced Identity Cloud Login** capability to authenticate users, with Advanced Identity Cloud acting as a social identity provider.

The connector redirects the browser to Advanced Identity Cloud, initiates the default journey to allow the user to authenticate, then returns to DaVinci with the authentication result.

Capabilities

PingOne Advanced Identity Cloud Login

Authenticate the user using the default journey in PingOne Advanced Identity Cloud.

Output Schema

- output object
 - iss string
 - sub string
 - aud string
 - exp number
 - iat number
 - auth_time number
 - name string
 - family_name string
 - given_name string
 - zoneinfo string
 - locale string
 - email string
 - address string
 - phone_number string
 - tokens object
 - access_token string
 - refresh_token string
 - id_token string

PingOne Advanced Identity Cloud Login Connector Release Notes

New features and improvements in the PingOne Advanced Identity Cloud Login connector.

April 2024

The PingOne Advanced Identity Cloud Login connector is now available

New

You can use the PingOne Advanced Identity Cloud Login connector to authenticate users using the default journey.

PingOne Authentication Connector

The PingOne Authentication connector lets you authenticate users and manage PingOne user authentication sessions in your PingOne DaVinci flow.

You can use the PingOne Authentication connector to:

- Authenticate users by integrating DaVinci flows into your application using a browser redirect or the DaVinci widget
- Authenticate users with external identity provider (IdP)s configured in PingOne
- Create, update, or delete PingOne authentication sessions
- Check whether a user has an active session
- Verify a user's code for device authorization flows
- Authorize or decline device access to a user's account

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a PingOne license.

Configuring the PingOne Authentication connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

The PingOne Authentication connector automatically communicates with the PingOne environment associated with your DaVinci environment.

Using the connector in a flow

Authenticating users by redirecting the browser to your DaVinci flow

This is the recommended method for integrating a DaVinci flow into your application. It allows you to authenticate users by redirecting the browser from your application, through PingOne, to your DaVinci flow. This method supports either OpenID Connect (OIDC), Security Assertion Markup Language (SAML), or Microsoft 365 applications.

 Note

The ability to use a flow to orchestrate authentication for Microsoft 365 applications is currently in limited release. To request access to these parameters, open a support case.

For detailed setup instructions, see [Launching a PingOne flow with a redirect](#).

To use this method, end your flow with the following two capabilities:

- Success path: **Return a Success Response (Redirect Flows)**

 Note

You can optionally configure **ID Token Custom Claims** to add additional attributes to the OIDC ID Token, SAML assertion, or WS-Federation security token for Microsoft 365.

For SAML assertions, the default attribute format is `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`.

For WS-Federation security tokens, the default attribute format is `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`.

To override the default attribute format, append the pipe character followed by the desired format to the attribute name. For example:

- If you enter `attr1` as the **Claim Name** value, the resulting attribute format is just the default value.
- If you enter `attr1|http://schemas.microsoft.com/ws/2008/06/identity/claims/5678` as the **Claim Name** value, the resulting attribute format is `http://schemas.microsoft.com/ws/2008/06/identity/claims/5678`.

 Note

In addition to fulfilling an OIDC, SAML, or Microsoft 365 authentication request, this capability creates a PingOne user authentication session. If you don't need session management capabilities, you can ignore the session that is created.

- Error path: **Return an Error Response (Redirect Flows)**

Authenticating users by embedding the DaVinci widget in your web application

This is an alternate method for integrating a DaVinci flow into your application when a redirect is not possible. It allows you to authenticate users with your DaVinci flow by embedding a widget within your application. The browser stays on your organization's domain throughout the transaction. This method only supports OIDC.

For detailed setup instructions, see [Launching a flow with the widget](#).

To use this method, end your flow with the following two capabilities:

- Success path: **Return a Success Response (Widget Flows)**

 Note

In addition to fulfilling an OIDC authentication request, this capability creates a PingOne user authentication session. If you don't need session management capabilities, you can ignore the session that is created.

- Error path: **Send Error JSON Response**

**Note**

This capability is in the [HTTP connector](#).

Authenticating users with an external identity provider

The connector allows you use an external identity provider that you have configured in PingOne to authenticate users in your flow.

You can use the **Link with PingOne User** setting to link the resulting user information to PingOne accounts to enable self-service features and centralize user management within your organization.

Attributes from the external provider are also made available in your flow as part of the output schema for the capability.

**Note**

For more information about external identity providers in PingOne, see [Identity Providers](#) and [Adding an external identity provider sign-on step](#).

There are two ways to do this:

Include the skIdP component in a Custom HTML Template

This approach allows you to build a custom HTML page with sign on buttons that are powered by DaVinci authentication connectors and identity providers configured in PingOne.

1. In a flow, add the HTTP connector with the **Custom HTML Template** capability.
2. In the **HTML Template** field, click `{}`, select **SK-Components**, and add the **skIdP** component.
3. In the **HTML Template** field, click the **skIdP** component to open the configuration.
4. From the **Identity Provider Connector** list, select your PingOne Authentication connector.
5. From the **PingOne External Identity Provider** list, select an identity provider.

**Tip**

To manage the identity providers on this list, go to `*include::partial$davinci_rc_p1_menu_cascades.adoc[tags=p1.menucascade.integrations.externalidps]*` in your PingOne environment.

6. Complete the rest of the skIdP configuration according to the help text. Click **Apply**.

Use the Sign On with External Identity Provider capability in a flow

1. In a flow, add the PingOne Authentication connector with the **Sign On with External Identity Provider** capability.
2. In the capability configuration, from the **Identity Provider** list, select an identity provider.
3. Complete the rest of the capability configuration according to the help text.

 Note

In the **Authentication Context Reference** field, select whether to pass the requested authentication context via the `AuthnContextClassRef` or `AuthnContextDeclRef` element based on your agreement with the SAML IdP.

4. Click **Apply**.

Checking whether a user has an active session

The **Check a User's Session Status** capability lets you check whether a user has an active authentication session that matches the authentication method and time period you define.

This lets you create detailed sign on policies. For example, you could skip reauthentication when a user has already signed on with MFA in the past 8 hours.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating or updating a session

The **Create or Update a Session** capability lets you capture information in your flow and use it to create a PingOne user authentication session.

When creating the session, you can include the authentication method or methods that the user used to sign on. This information is associated with the session, and it allows you to create detailed sign on policies that branch based on the authentication method. For details, see **Checking whether a user has an active session**.

No special configuration is needed. Add the capability and populate its properties according to the help text.

 Note

You don't need to add this capability in flows that end with the **Return a Success Response (Redirect Flows)** or **Return a Success Response (Widget Flows)** capability. Those capabilities already create sessions.

Deleting a session

The **Delete a Session** capability allows you to sign a user out and optionally delete their PingOne user authentication session.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Managing device authorization with a user code

The **Verify User Code (Device Auth Flows)** capability allows you to grant device access to a user's PingOne account.

Once the user code is verified in the flow, you can use the following capabilities to authorize or decline device access:

- **Authorize User Code (Device Auth Flows)**
- **Decline User Code (Device Auth Flows)**

Capabilities

Return Success Response (Redirect Flows)

Create a PingOne session and redirect back to the source of the authentication request. Use this to complete flows that are initiated by a redirect to PingOne.

Properties

User ID textField required

The user's PingOne user ID.

Authentication Methods dropdownWithCreate required

The authentication method that the user signed on with. For a dynamic value, select Use Custom Authentication Method and enter a value in the Custom Authentication Method field.

- Password-based authentication (pwd) (Default)
- Multiple-factor authentication (mfa)
- Use Custom Authentication Methods
- One-time password (otp)
- Risk-based authentication (rba)
- Confirmation using SMS (sms)

Custom Authentication Methods textField

The authentication method that the user signed on with, such as "pwd". Use the abbreviations from the Authentication Methods list or enter a custom value. Separate multiple values with a space, such as "pwd geo fpt".

Reduced Scopes textField

The scopes to request for the user, such as "openid email". This field allows you to request a limited subset of the original scopes. You cannot add any scopes that are not part of the original request. Separate multiple scopes with a space. Leave this blank to pass along all of the scopes from the original request.

idTokenClaims selectNameValueListColumn

accessTokenClaims selectNameValueListColumn

Idle Timeout timeInterval

The amount of time that the session will remain valid after the user becomes inactive.

Default: 43200

Input Schema

- default object
 - authentication object
 - userId string
 - methods array
 - ip string
 - policyId string
 - sessionToken string
 - parameters object
 - properties object
 - userId string
 - identifiedDeviceId string
 - authenticationMethods string
 - customAuthenticationMethods string
 - scopes string
 - idTokenClaims array
 - accessTokenClaims array
 - idleTimeout number

Return Success Response (Widget Flows)

Create a PingOne session and return the OIDC tokens to the originating web application. Use this to complete flows that are initiated within a widget in a web application.

Properties

PingOne Application dropdown

The PingOne OIDC application to use to create the session in PingOne. For a dynamic value, select Use Application ID and enter a value in the Application ID field.

- Use Application ID (Default)

Application ID textField required

The unique identifier for the application.

User ID textField required

The user's PingOne user ID.

Authentication Methods dropdownWithCreate required

The authentication method that the user signed on with. For a dynamic value, select Use Custom Authentication Method and enter a value in the Custom Authentication Method field.

- Password-based authentication (pwd) (Default)
- Multiple-factor authentication (mfa)
- Use Custom Authentication Methods
- One-time password (otp)
- Risk-based authentication (rba)
- Confirmation using SMS (sms)

Custom Authentication Methods textField

The authentication method that the user signed on with, such as "pwd". Use the abbreviations from the Authentication Methods list or enter a custom value. Separate multiple values with a space, such as "pwd geo fpt".

Reduced Scopes textField

The scopes to request for the user, such as "openid email". Leave this blank to request all scopes configured in the PingOne application, or enter a subset of the application scopes. Separate multiple scopes with a space.

idTokenClaims selectNameValueListColumn

accessTokenClaims selectNameValueListColumn

Idle Timeout timeInterval

The amount of time that the session will remain valid after the user becomes inactive.

Default: 43200

Additional Properties selectNameValueListColumn

Define any additional information to include in the response.

Additional Properties Name textField

The name of the property that contains the information defined in Additional Properties, such as "additionalProperties".

Default: `additionalProperties`

Input Schema

- default object
 - authentication object
 - `userId` string
 - `methods` array
 - `ip` string
 - `policyId` string
 - `sessionToken` string
 - `properties` object
 - `application` string required
 - `applicationId` string
 - `userId` string
 - `identifiedDeviceId` string
 - `authenticationMethods` string
 - `customAuthenticationMethods` string
 - `widgetScopes` string
 - `idTokenClaims` array
 - `accessTokenClaims` array
 - `idleTimeout` number

Output Schema

- success boolean
- access_token string
- token_type string
- expires_in number
- scope string
- id_token string
- sessionToken string
- sessionTokenMaxAge number
- identifiedDeviceId string
- additionalProperties object::

Return Error Response (Redirect Flows)

Return error information to the source of the authentication request. Use this to complete flows that are initiated by a redirect to PingOne.

Properties

Custom Error Message toggleSwitch

When enabled, you can provide detailed error information in the fields below.

Error Message dropdownWithCreate

Returned in error field in query parameter

- invalid_request
- invalid_client
- invalid_grant
- unauthorized_client
- unsupported_grant_type
- invalid_scope

errorCode textField

errorDescription textField

errorReason textField

Input Schema

- default object
 - parameters object

Check Session

Check whether the user has an active session in PingOne.

Properties

Valid Authentication Method dropdown*WithCreate required*

The check only passes if the user signed on with the selected authentication method. For a custom value, enter your authentication method reference value in the field, such as "kba" or "mca". This field does not support multiple values.

- Password-based authentication (pwd) (Default)
- Multiple-factor authentication (mfa)
- Any authentication method
- One-time password (otp)
- Risk-based authentication (rba)
- Confirmation using SMS (sms)

Last Sign On Was Within... *timeInterval*

The check only passes if the user signed on within this period of time.

Default: 480

Input Schema

- default object
 - sessionToken string
 - parameters object
 - properties object
 - checkSessionAuthenticator string required
 - authenticationMethodLastUsedIn number

Output Schema

- output object
 - session object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - createdAt string
 - activeAt string
 - idleTimeoutInMinutes number
 - lastSignIn object
 - remoteIp string
 - authenticators array
 - expiresAt string

Create or Update Session

Create or update an authentication session.

Properties

User ID textField required

The user's PingOne user ID.

Authentication Methods dropdownWithCreate required

The authentication method that the user signed on with. For a dynamic value, select Use Custom Authentication Method and enter a value in the Custom Authentication Method field.

- Password-based authentication (pwd) (Default)
- Multiple-factor authentication (mfa)
- Use Custom Authentication Methods
- One-time password (otp)
- Risk-based authentication (rba)
- Confirmation using SMS (sms)

Custom Authentication Methods textField

The authentication method that the user signed on with, such as "pwd". Use the abbreviations from the Authentication Methods list or enter a custom value. Separate multiple values with a space, such as "pwd geo fpt".

Idle Timeout timeInterval

The amount of time that the session will remain valid after the user becomes inactive.

Default: 43200

Input Schema

- default object
 - authentication object
 - userId string
 - methods array
 - ip string
 - policyId string
 - sessionToken string
 - properties object
 - userId string
 - identifiedDeviceId string
 - authenticationMethods string
 - customAuthenticationMethods string
 - idleTimeout number

Output Schema

- output object
 - session object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - createdAt string
 - activeAt string
 - idleTimeoutInMinutes number
 - lastSignOn object
 - remotelp string
 - authenticators array
 - expiresAt string

Delete Session

Delete an authentication session.

Properties

Soft Delete toggleSwitch

When enabled, PingOne signs the user out but does not delete the session.

Input Schema

- default object
 - sessionToken string
 - properties object
 - softDelete boolean

Output Schema

- output object

Sign On with External Identity Provider

Authenticate the user using an external identity provider configured in PingOne.

Properties

PingOne External Identity Provider dropDown

Select an external identity provider from your PingOne environment.

- Use Identity Provider ID (Default)

PingOne External Identity Provider ID textField

The ID of an external identity provider from your PingOne environment, such as "df417355-adc4-2846-41f1-6f4b0b9bd12c".

Policy Purpose radioSelect required

Specify whether this policy is intended for users to authenticate at Microsoft via the OpenID Connect protocol or to fulfill the multi-factor authentication requirement as defined in Entra ID external authentication method.

- OIDC Authentication (Default)
- Entra ID External Authentication Method

ID Token Hint textField

ID token hint provided by Entra ID for step up authentication.

Link with PingOne User toggleSwitch

When enabled, DaVinci creates or updates a linked PingOne user account using attributes from the external IdP.

PingOne Population dropDown

The PingOne population to use when authenticating the user.

- Use Population ID (Default)

Population ID textField

The ID of the PingOne population to use when authenticating the user, such as "aa4b3e81-cf7e-8685-4b7b-7ec89cfcf7c8".

ACR Values textField required

Enter the space-separated list of values to pass context to the IdP via OIDC.

Login Hint textField required

Username to prepopulate at the external IdP.

Application Return to Url textField required

When using the embedded flow player widget and an IdP/Social Login connector, provide a callback URL to return back to the application.

Requested Authentication Context textField

Enter the space-separated list of values to pass context to the IdP via SAML 2.0.

Authentication Context Reference radioSelect

Select the reference element to pass the context based on your agreement with the SAML IdP. The Requested Authentication Context field must be populated beforehand.

- AuthnContextClassRef
- AuthnContextDeclRef

Input Schema

- default object
 - properties object
 - identityProvider string required minLength: 0 maxLength: 100
Identity Provider
 - identityProviderId string minLength: 0 maxLength: 100
Identity Provider ID
 - population string minLength: 0 maxLength: 100
Population
 - populationId string minLength: 0 maxLength: 100
Population ID
 - linkWithP1User boolean
Link with PingOne User
 - acrValues string minLength: 0 maxLength: 300
ACR Values
 - loginHint string minLength: 0 maxLength: 100
Login Hint
 - policyPurpose string
Describes whether this flow will be used for Microsoft OIDC or for EAM
 - idTokenHint string minLength: 0 maxLength: 10000
ID Token Hint provided by Entra ID
 - returnUrl string minLength: 0 maxLength: 300
Return URL
 - requestedAuthenticationContext string minLength: 0
Requested Authentication Context
 - authenticationContextReference
Authentication Context Reference

Output Schema

- output object
 - isLinkedUser boolean
 - user object
 - preferredLanguage string
 - timezone string
 - lastSignOn object
 - at string
 - remotelp string
 - title string
 - type string
 - locale string
 - enabled boolean
 - identityProvider object
 - id string
 - type string
 - lifecycle object
 - status string
 - createdAt string
 - verifyStatus string
 - nickname string
 - mfaEnabled boolean
 - id string
 - email string
 - updatedAt string
 - memberOfGroupIDs string
 - address object
 - streetAddress string
 - locality string
 - region string

- postalCode string
- countryCode string
- externalId string
- photo object
 - href string
- memberOfGroupNames string
- population object
 - id string
- primaryPhone string
- accountId string
- mobilePhone string
- name object
 - formatted string
 - given string
 - middle string
 - family string
 - honorificPrefix string
 - honorificSuffix string
- account object
 - canAuthenticate boolean
 - status string
 - lockedAt string
 - secondsUntilUnlock string
 - unlockAt string
- username string
- rawIdpAttributes object
- statusCode integer

Verify User Code (Device Auth Flows)

Verify that a given user code exists.

Properties

User ID textField required

The user's PingOne user ID.

User Code textField required

The user code provided by the end user

Input Schema

- default object
 - properties object
 - userId string required
 - userCode string required

Output Schema

- output object
 - scope string
 - appld string
 - remotelp string

Authorize User Code (Device Auth Flows)

Grant a device access to a user's account. Should be done only after the user code has been verified and the scopes have been accepted by the user.

Properties

User Code textField required

The user code provided by the end user

User ID textField required

The user's PingOne user ID.

Authentication Methods dropdownWithCreate required

The authentication method that the user signed on with. For a dynamic value, select Use Custom Authentication Method and enter a value in the Custom Authentication Method field.

- Password-based authentication (pwd) (Default)
- Multiple-factor authentication (mfa)
- Use Custom Authentication Methods
- One-time password (otp)
- Risk-based authentication (rba)
- Confirmation using SMS (sms)

Custom Authentication Methods textField

The authentication method that the user signed on with, such as "pwd". Use the abbreviations from the Authentication Methods list or enter a custom value. Separate multiple values with a space, such as "pwd geo fpt".

Reduced Scopes textField

The scopes to request for the user, such as "openid email". This field allows you to request a limited subset of the original scopes. You cannot add any scopes that are not part of the original request. Separate multiple scopes with a space. Leave this blank to pass along all of the scopes from the original request.

idTokenClaims selectNameValueListColumn

accessTokenClaims selectNameValueListColumn

Idle Timeout timeInterval

The amount of time that the session will remain valid after the user becomes inactive.

Default: 43200

Input Schema

- default object
 - authentication object
 - userId string
 - methods array
 - ip string
 - policyId string
 - sessionToken string
 - properties object
 - userCode string required
 - userId string
 - identifiedDeviceId string
 - authenticationMethods string
 - customAuthenticationMethods string
 - scopes string
 - idTokenClaims array
 - accessTokenClaims array
 - idleTimeout number

Decline User Code (Device Auth Flows)

Deny a device access to a user's account. This should be done after the user code has been verified if the user does not consent to the requested scopes.

Properties

User Code textField required

The user code provided by the end user

Input Schema

- default object
 - properties object
 - userCode string required

PingOne Authentication Connector Release Notes

New features and improvements in the PingOne Authentication connector.

February 2025

Improved flexibility with SAML and WS-Federation attributes sent to PingOne

New

When authenticating users by redirecting the browser to your DaVinci flow, the DaVinci flow policy returns additional attributes to PingOne. You can now override the default format of those attributes.

Note

The ability to use a flow to orchestrate authentication for Microsoft 365 applications is currently in limited release. To request access to these parameters, open a support case.

February 2024

Added capabilities for device authorization

New

The following capabilities have been added to the connector to allow for device authorization:

- Verify User Code (Device Auth Flows)
- Authorize User Code (Device Auth Flows)
- Decline User Code (Device Auth Flows)

Added RequestedAuthnContext for SAML external IdPs

New

The **Sign On with External Identity Provider** capability now includes the following fields:

- Requested Authentication Context
- Authentication Context Reference

You can now select whether to pass the requested authentication context using the `AuthnContextClassRef` or the `AuthnContextDeclRef` based on your agreement with the SAML IdP.

June 2023

Added Variable option for last sign on

New

The **Check Session** capability now includes a `Variable` option for the **Last Sign On** field, which enables variable and parameter use.

May 2023

Authenticate with PingOne external identity providers

New

The **Sign On with External Identity Provider** capability lets you use [PingOne external identity providers](#) to authenticate users in your DaVinci flows. You can optionally link the resulting user information to PingOne accounts to enable self-service features and centralize user management within your organization.

Learn more in [PingOne Authentication connector](#).

March 2023

The PingOne Authentication Connector is now available

New

You can use the PingOne Authentication connector to:

- Authenticate users by integrating DaVinci flows into your application using a browser redirect or the DaVinci widget
- Create, update, or delete PingOne authentication sessions
- Check whether a user has an active session

PingOne Authorize Connector

This connector lets you use PingOne Authorize for policy-based authorization decisions in your PingOne DaVinci flow.

PingOne Authorize controls what users can see and do inside of applications and APIs. It allows organizations to centrally configure authorization requirements, ranging from simple rules to real-time, fine-grained policies.

PingOne Authorize can integrate with other PingOne services, such as PingOne Protect, and exploit information in a PingOne user profile to augment authorization events in real-time.

Use the PingOne Authorize connector to:

- Externalize authorization from your DaVinci flows, allowing separation of duties between the team controlling the user experience and the team controlling what users are authorized to see and do.

- Leverage real-time data in fine-grained policies that go beyond identity and roles.
- Make adaptive, context-aware authorization decisions that result in permit, deny, or challenge outcomes.
- Assemble and provide DaVinci with authorized information used in flows, for example, retrieving the list of accounts that a user is authorized to access.

Setup

Resources

For information and setup help, learn more in the following documentation:

- PingOne Authorize documentation:
 - [Introduction to Authorization](#)
 - [Getting started with PingOne Authorize](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne Authorize license
- A PingOne environment with a configured worker application

Setting up PingOne Authorize

1. Follow the instructions in [Getting started with PingOne Authorize](#).
2. In the [Trust Framework](#), define the resources needed to build policies.
3. [Write policies](#) for authorization decisions that you want to include in your flow. Include advice in your policies for statements you want to return to your flows.
4. [Publish](#) the policies to a [Decision Endpoint](#).

Setting up the PingOne Authorize connector configuration

In DaVinci, add a **PingOne Authorize** connection. Learn more in [Adding a connector](#).

Connector configuration

Client ID

The **Client ID** of the worker application that you created in PingOne.

Client Secret

The **Client Secret** from the **Configuration** tab of your PingOne worker application.

Endpoint

The decision endpoint to which the connector submits decision requests. On the [Decision Endpoints](#) page in PingOne Authorize, expand the appropriate endpoint to get the **URL** or the **Endpoint ID**.

Using the connector in a flow

The PingOne Authorize connector provides these capabilities:

Make Decision Request

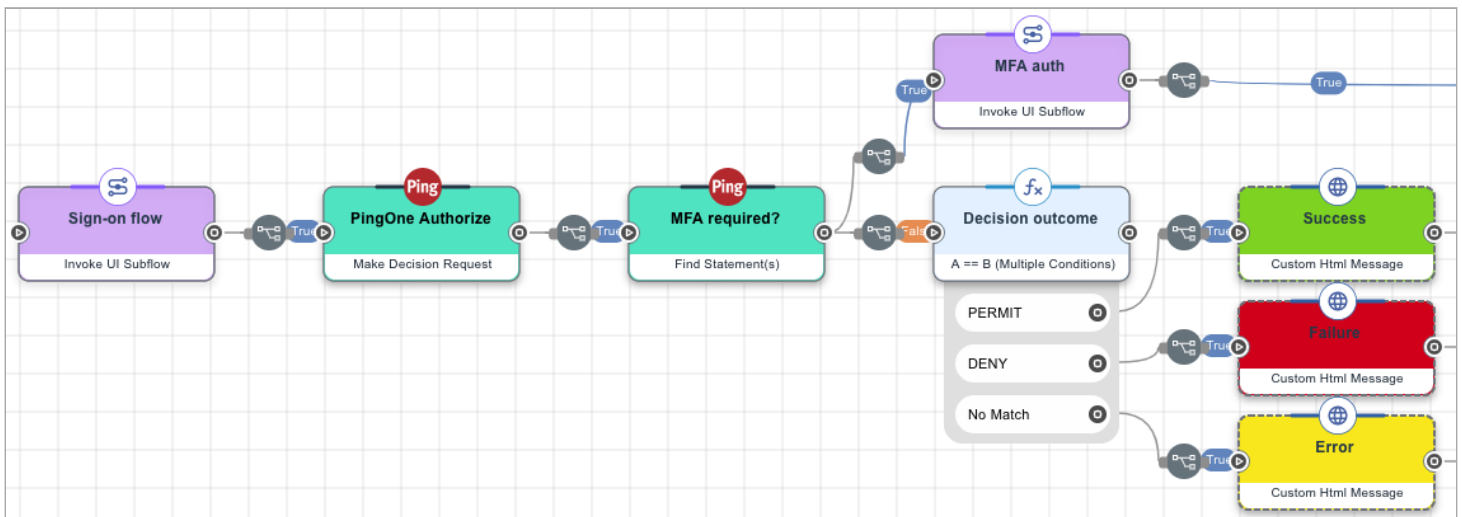
Add authorization decision requests to your flows. Decision requests return permit, deny, indeterminate, or not applicable decisions that you can act on in your flows.

Find Statements

Find statements returned in decision responses and use them as inputs in subsequent nodes. Add multiple PingOne Authorize connector nodes at different points in your flow to use the authorized information returned in statements.

When a statement code is found, you can act on it in your flow. For example, you can use it to determine if multi-factor authentication (MFA) is required or a risk update is needed. You can also extract authorized information from the statement payload, for use in scenarios such as reporting fraud case information or providing a list of authorized IDs or accounts in your flow.

In the following example, the first PingOne Authorize connector uses information about an authenticated user to make an authorization decision. The second PingOne Authorize connector finds a statement code in the decision response to determine if MFA is required.



Make a decision request

Collect user information with an HTML form, then use the first PingOne Authorize connector to send the information to PingOne Authorize, and use the decision response in your flow.

1. In your flow, build a sign-on flow that populates a **User ID** field in an **HTTP** connector with the **HTML Form** capability.
2. Send user information to PingOne Authorize:
 1. After your sign-on flow, add the **PingOne Authorize** connector and select the node in your flow.
 2. Select the **Make Decision Request** capability.
 3. In the **User ID** field, click **{}** and select the **User ID** variable from your **HTML Form** node.
3. Populate attribute information in the decision request:
 1. In the **Fields** section, click **+** to add one or more key-value pairs. These pairs map to attributes in PingOne Authorize.
 2. In the **Key** field, enter the full name of the attribute that you want to map to the decision request.
 3. In the **Value** field, click **{}** and select a variable from a node. Alternatively, you can enter a hard-coded value.

Tip

To edit key-value pairs, click the **Pencil** icon. In edit mode, the icon turns into an **X** icon. Click the **X** icon to leave edit mode. To delete a Key-Value pair in edit mode, click the **-** icon under **Key**.

Key	Value
 Groups.Name	 groupname 

4. Click **Apply**.

4. Add a node to capture the decision response from PingOne Authorize:

1. After the **PingOne Authorize** node, add a **Function** connector and select the node in your flow.
2. Select the **A == B (Multiple Conditions)** trigger.
3. In the **Value A** field, click **{}** and select the **decision** variable from your **PingOne Authorize** node.
4. Click **Add** and enter **PERMIT** in the **Value 1** field.
5. Click **Add** and enter **DENY** in the **Value 2** field.



Note

In this example flow, Not Applicable and Indeterminate decisions fall under **No Match** and connect to an **Error** node.

6. Click **Apply**.

5. Add nodes to your flow that act on the **Permit**, **Deny**, and **No Match** decision responses.

6. Test your flow:

1. Click **Save**, **Deploy**, then **Run**.
2. Review status messages.

Find statements

Use the second PingOne Authorize connector to find a statement code that matches advice in a policy, then use the code in your flow to determine if MFA is required. If the code is found in decision response statements, then the outcome of the node is true.

1. Find a statement code in the decision response from the first **PingOne Authorize** node:

1. After the first **PingOne Authorize** node in your flow, add another **PingOne Authorize** connector and select the node in your flow.
2. Select the **Find Statement(s)** capability.
3. In the **Statement Code** field, enter the statement **Code** from **Advice and Obligations** in your policy rule. For example, the following image shows the **MFA_REQ** advice code in a PingOne Authorize rule.

The screenshot shows a configuration interface for a rule named "MFA required when user is not in their registered country". The rule is active, indicated by a green checkmark. Below the rule name is a "+ Add Rule" button. Under the heading "Advice and Obligations (1 total)", there is a detailed configuration for the "MFA Required" obligation. This configuration includes a "Description" field, a "Code" field set to "MFA_REQ", an "Applies To" field set to "Permit", a "Payload" field, and an "Attributes" field. There are also icons for "Obligatory" and a menu icon.

4. In the **Statements** field, click **{}** and select the **statements (array)** output variable from the first **PingOne Authorize** node in your flow.

The screenshot shows the "Find Statement(s)" configuration window. It has a "GENERAL" tab and a "SETTINGS" tab. A note indicates that an asterisk (*) indicates required fields. The "Statement Code" field is set to "MFA_REQ". The "Statements" field shows a search for "statements" from the "PingOne Authorize" node. Below this, a list of output variables is displayed: "success (boolean)", "output (object)", "rawResponse (object)", "statusCode (number)", "statements (array)", and "decision (string)". The "statements (array)" variable is highlighted.

5. Click **Apply**.
2. After the second **PingOne Authorize** node in your flow, add nodes for an MFA flow.
3. Test your flow:
 1. Click **Save**, **Deploy**, then **Run**.
 2. Review status messages.

Capabilities

Make Decision Request

Submit a decision request to a PingOne Authorize endpoint

Properties

Parameters keyValuePairList

Input parameters for the decision request

User ID textField

The ID of the PingOne user on whose behalf the connector is making a decision request

Input Schema

- default object
 - properties object
 - parameters array
 - userId string
 - clientId string
 - clientSecret string
 - endpointUrl string

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - statements array
 - decision string
 - headers object

Find Statement(s)

Filter decision response statements by code

Properties

Statement Code textField

The advice code from a PingOne Authorize policy rule to search for in an array of statements from a decision response

Statements textField

The array of statements to search through in a decision response

Input Schema

- default object
 - properties object
 - statements string
 - code string

Output Schema

- output object
 - statements array

PingOne Credentials Connector

Use the PingOne Credentials connector to issue, verify, and manage digital verifiable credentials with PingOne Credentials.

The connector sets up flows that help users issue credentials based on credentials templates and issuance rules that are configured and tied to the PingOne Digital Wallet Application.

This connector also helps set up flows that the credential verification service receives and responds to using the Decentralized Identity Foundation's [JWT VC Presentation Profile](#). Capabilities use the PingOne native protocols, which only work with apps that use the PingOne Neo Native SDKs.

Setup

Resources

For information and setup help, see the following sections of the PingOne Credentials and DaVinci documentation:

- PingOne Credentials:
 - [Introduction to PingOne Credentials](#)
 - [Getting started with PingOne Credentials](#)
- DaVinci:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the PingOne Credentials connector, you'll need:

- A PingOne license with PingOne credentials ([Try PingOne for free](#))
- A PingOne environment with a configured application
- A PingOne application associated with a digital wallet and a Digital Wallet URL used to send notifications to the user related to the credentials

Depending on flow use case and the capabilities you use, you might also need:

- A PingOne Digital Wallet Application ID, the Identifier (UUID) associated with the credential digital wallet app. For more information on developing and registering the wallet app that runs the PingOne Neo SDK, see [Getting started with PingOne Credentials](#).
- A Credential Type ID, the Identifier (UUID) associated with the credential type, used by compatible wallet apps. You can learn more about creating and updating a credential type in the [PingOne admin console](#), or [PingOne Credential Types API endpoint](#).
- A Issuance Rule ID, the Identifier (UUID) of the credential issuance rules operations to create, read, and update rules for issuing, updating, and revoking credentials by credential type. Credential issuance rules can be set through the [PingOne admin console](#), or [Credential Issuance Rules API endpoint](#).

Setting up PingOne

Setting up your PingOne environment

Sign up for PingOne and configure an environment with PingOne Credentials. Make sure to also add the PingOne DaVinci service to your environment. Follow the instructions in [Getting started with PingOne](#) and [Creating an environment](#).

Getting your environment details

Get your **Environment ID** and **Region** before setting up the PingOne Credentials connector in DaVinci:

1. In your PingOne environment, go to **Settings → Environment Properties**.
2. Locate the **Environment ID** and **Region**.
3. Copy these values to a secure location.

Getting your application credentials

Get the **Client ID** and **Client secret** from the PingOne console before setting up the PingOne Credentials connector in DaVinci:

1. In your PingOne environment, go to **Applications → Applications**. If you haven't added the application yet, see [Adding an application](#).
2. Locate the appropriate application and then click its entry to open the details panel.
3. On the **Profile** tab, locate the **Client ID** and **Client secret**.
4. Copy these values to a secure location.

Setting up the connector

In DaVinci, go to **Connections** and add a **PingOne Credentials** connection. For help, see [Adding a connector](#).

Connector settings

Environment ID

The unique identifier for the appropriate PingOne environment. To find the environment ID, see [Environment properties](#).

Client ID

The unique public identifier for the PingOne application. To find the client ID, see [Viewing application details](#).

Client secret

The cryptographic secret that is known only to the application and the authorization server. To find the client secret, see [Viewing a client secret](#).

Region

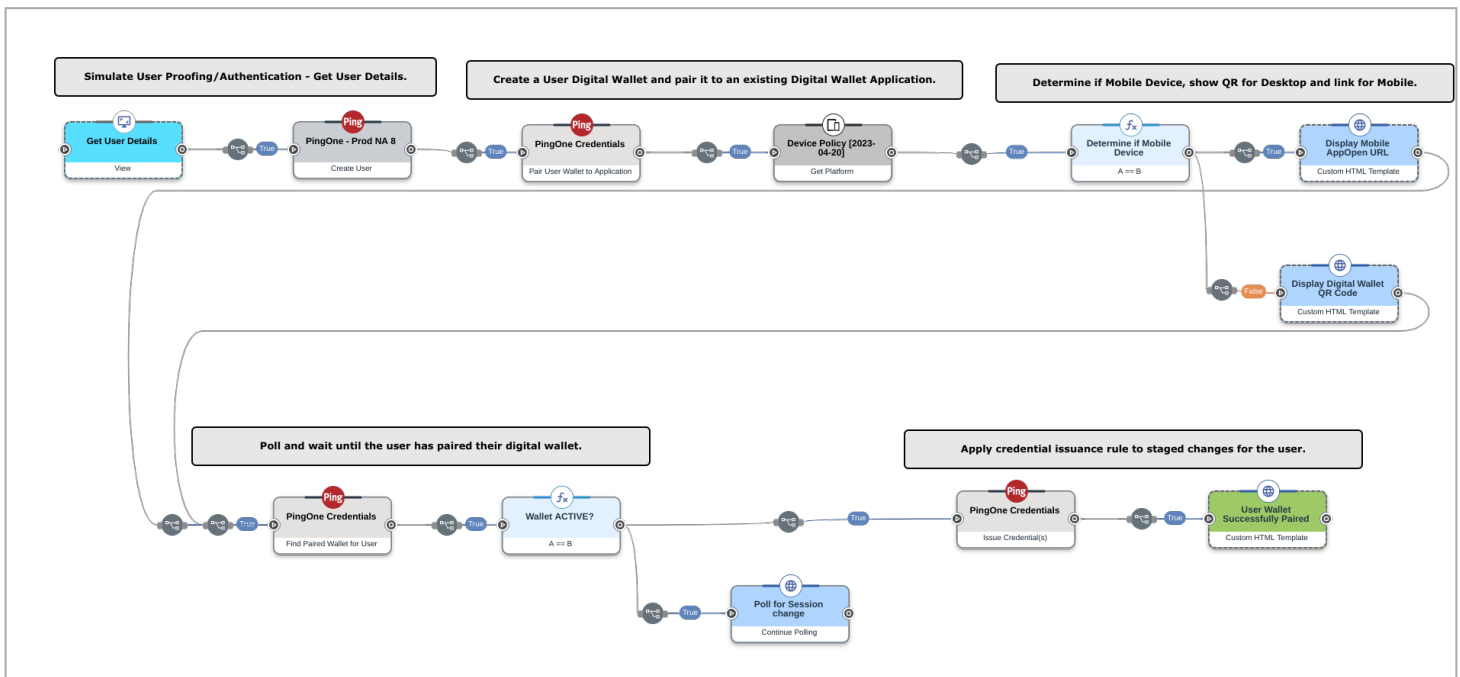
The geographic region that hosts your PingOne tenant. To find the region, see [Environment properties](#).

Using the connector in a flow

You can use the PingOne Credentials connector to issue, verify, and manage digital verifiable credentials.

The following example flows show issuance and verification demonstrations.

The example issuance flow contains the following nodes.



1. Simulate user proofing/authentication:

1. The **Get user details** node lets the user input their information into PingOne.
2. The **Create user** node creates the user in PingOne.

2. Create user digital wallet and pair it to the existing digital wallet application:

1. The **Pair user wallet to application** node creates a digital wallet for the user. The digital wallet application must already be configured in PingOne.

3. Determine if mobile device, then show QR code for desktop and link for mobile:

1. The **Determine if Mobile Device** node determines if the user has a mobile device or not. If the user has a mobile device, then the digital wallet app URL opens. If the user is on a desktop, a QR code for the digital wallet app displays.

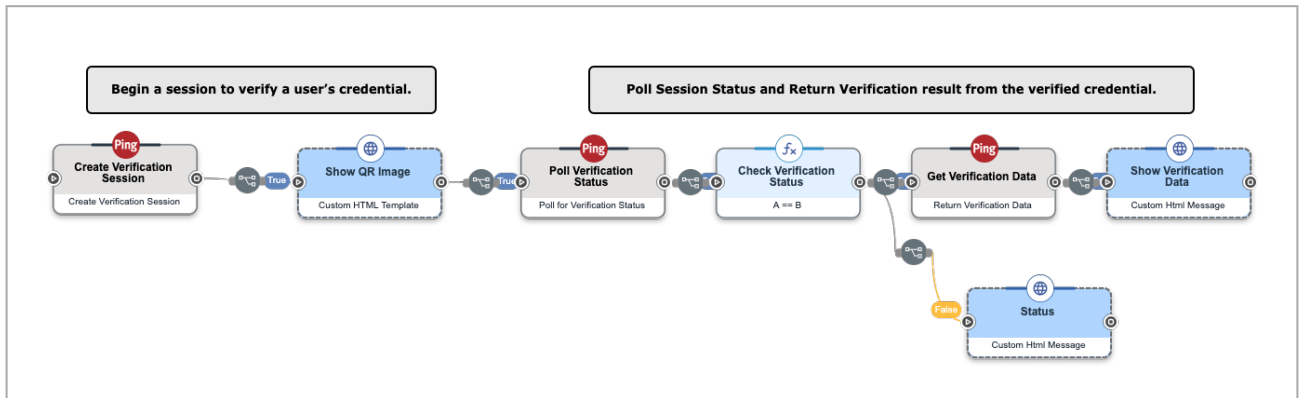
4. Poll and wait until the user has paired their digital wallet:

1. The **Find paired wallet for user** node filters all user wallets to find if a paired wallet exists for the configured PingOne application.
2. The **Wallet ACTIVE? A==B** node determines whether a digital wallet for the user has been paired or not.
3. The **Continue polling** node continues to check for the digital wallet application status. When the status changes to paired, then the flow continues.

5. Apply credential issuance rule to staged changes for the user:

1. The **Issue credentials** node is used to apply the changes staged by the credential issuance rule for the credential type in an environment.
2. **User wallet successfully paired** node displays a success message to the user when the digital wallet is successfully paired.

The example verification flow contains the following nodes.



6. Begin a session to verify a user's credential:

1. The **Create verification session** node lets an issuer begin a verification session to verify a user's credential.
2. The **Show QR Image** node displays a QR code for the user to verify their credential.

7. Poll session status and return verification result from the verified credential:

1. The **Poll for verification status** node checks and returns the status of the verification session.
2. The **Check verification status** node checks for the verification status to be "verified".
3. The **Return verification data** node returns data from the verified credential.
4. The **Show verification data** node displays the verified credential data.

Capabilities

Find Paired Wallet for User

Check to see if a user has a paired wallet

Properties

User ID textField

PingOne user ID

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
- User Id

Output Schema

- output object
 - digitalWallets object
 - size number
 - pairedWallets array
 - rawResponse object
 - size number
 - pairedWallets array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "pairedDigitalWallets" :
    { "size" : 2,
      "digitalWallets" :
        [
          { "id" : "11dd742c-9f9b-4bde-b8f7-1ce6c8f56c3d",
            "createdAt" : "2023-04-14T16:04:51.449Z",
            "updatedAt" : "2023-04-14T16:04:51.449Z",
            "environment" :
              { "id" : "73056e49-0ebc-4a58-a126-dc9e1efb4ffe" },
            "user" :
              { "id" : "5a942438-cca2-4edd-ac53-c1384c6e0329" },
            "digitalWalletApplication" :
              { "id" : "1ab1e656-e7fa-46b9-a5ce-3eb7444e4eb8" },
            "status" : "ACTIVE",
            "pairingSession" :
              { "id" : "54bfc17-4981-4764-a243-a2449e0f06e8",
                "createdAt" : "2023-04-14T16:04:51.449Z",
                "updatedAt" : "2023-04-14T16:04:51.449Z",
                "environment" :
                  { "id" : "73056e49-0ebc-4a58-a126-dc9e1efb4ffe" },
                "user" :
                  { "id" : "5a942438-cca2-4edd-ac53-c1384c6e0329" },
                "digitalWallet" :
                  { "id" : "11dd742c-9f9b-4bde-b8f7-1ce6c8f56c3d" },
                "challenge" : "qid86j8gjbfb3oj3",
                "qrUrl" : "https://api-test.pingone.com/v1/distributedid/requests/057d510a-860f-493f-b969-9206920cb416" },
            "notification" :
              { "methods" :
                  [ "EMAIL",
                    "SMS" ],
                "results" :
                  [
                    { "method" : "EMAIL",
                      "sent" : true,
                      "notification" :
                        { "id" : "00be2a92-3df7-4817-aa21-f835f91f3da9" } },
                    { "method" : "SMS",
                      "sent" : true,
                      "notification" :
                        { "id" : "0064c622-d8b2-4141-bc3f-b017f677a08a" } } ] } } ] } } }
```

Read User Wallet

Return a specified digital wallet for a user

Properties

Digital Wallet ID textField

Identifier (UUID) of the digital wallet associated with the provisioned credential.

User ID textField

PingOne user ID

Input Schema

- default object
 - properties object
 - digitalWalletId string required minLength: 0 maxLength: 100
Digital Wallet Id
 - userId string required minLength: 0 maxLength: 100
User Id

Output Schema

- output object
 - userDigitalWallet object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - digitalWalletApplication object
 - id string
 - status string
 - createdAt string
 - updatedAt string
 - pairingSession
 - id string
 - createdAt string
 - updatedAt string
 - environment object
 - id string
 - user object
 - id string
 - digitalWallet object
 - id string
 - challenge string
 - qrUrl string
 - status string
 - notification object
 - methods array
 - results array

- rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - digitalWalletApplication object
 - id string
 - status string
 - createdAt string
 - updatedAt string
 - pairingSession
 - id string
 - createdAt string
 - updatedAt string
 - environment object
 - id string
 - user object
 - id string
 - digitalWallet object
 - id string
 - challenge string
 - qrUrl string
 - status string
 - notification object
 - methods array
 - results array
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "userDigitalWallet" :
    { "id" : "43148164-4a97-4c57-9db6-918a73f6f6ac",
      "createdAt" : "2023-03-02T18:22:38.366Z",
      "updatedAt" : "2023-03-02T18:22:38.366Z",
      "environment" :
        { "id" : "6a2b43f8-457f-45ab-bcdd-2e001f095e46" },
      "user" :
        { "id" : "3d930cdf-9dd2-42b7-b9be-99540ea3469f" },
      "digitalWalletApplication" :
        { "id" : "f7ae218d-83de-41f8-8ae5-f2ce78a84623" },
      "status" : "PAIRING_REQUIRED",
      "pairingSession" :
        { "id" : "7829a13d-45b7-4416-804b-6d552e2cb3bd",
          "createdAt" : "2023-03-02T18:22:38.366Z",
          "updatedAt" : "2023-03-02T18:22:38.366Z",
          "environment" :
            { "id" : "6a2b43f8-457f-45ab-bcdd-2e001f095e46" },
          "user" :
            { "id" : "3d930cdf-9dd2-42b7-b9be-99540ea3469f" },
          "digitalWallet" :
            { "id" : "43148164-4a97-4c57-9db6-918a73f6f6ac" },
          "challenge" : "p829otr1e433tep2",
          "qrUrl" : "https://api-test.pingone.com/v1/distributedid/requests/fcbd2ad7-887b-41d5-9fdc-970273b5ec78",
          "status" : "INITIAL" },
      "notification" :
        { "methods" :
          [ "EMAIL",
            "SMS" ],
          "results" :
            [
              { "method" : "EMAIL",
                "sent" : false,
                "error" :
                  { "id" : "c4211b03-2734-4d9a-8a80-3934d2ec1796",
                    "code" : "NOT_FOUND",
                    "message" : "The request could not be completed. The requested resource was not found." } },
              { "method" : "SMS",
                "sent" : false,
                "error" :
                  { "id" : "c4211b03-2734-4d9a-8a80-3934d2ec1796",
                    "code" : "NOT_FOUND",
                    "message" : "The request could not be completed. The requested resource was not found." } } ] } } } }
```

Pair User Wallet to Application

Create a digital wallet and pair it to an application for a user

Properties

Notification Methods dropDownMultiSelect

- Email
- SMS

User ID textField

PingOne user ID

Input Schema

- default object
 - properties object
 - notificationMethods array uniqueItems: true
 - userId string required minLength: 0 maxLength: 100
- User Id

Output Schema

- output object
 - userDigitalWallet object
 - _links object
 - environment object
 - href string
 - digitalWalletApplications object
 - href string
 - qrUrl object
 - href string
 - appOpen object
 - href string
 - id string
 - environment object
 - id string
 - user object
 - id string
 - digitalWalletApplication object
 - id string
 - status string
 - createdAt string
 - updatedAt string
 - pairingSession object
 - id string
 - createdAt string
 - updatedAt string
 - environment object
 - id string
 - user object
 - id string

- digitalWallet object
 - id string
- challenge string
- qrUrl string
- status string
- notification object
 - methods array
- results array
- rawResponse object
 - _links object
 - environment object
 - href string
 - digitalWalletApplications object
 - href string
 - qrUrl object
 - href string
 - appOpen object
 - href string
 - id string
 - environment object
 - id string
 - user object
 - id string
 - digitalWalletApplication object
 - id string
 - status string
 - createdAt string
 - updatedAt string
 - pairingSession object
 - id string

- createdAt string
- updatedAt string
- environment object
 - id string
- user object
 - id string
- digitalWallet object
 - id string
- challenge string
- qrUrl string
- status string
- notification object
 - methods array
- results array
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "userDigitalWallet" :
    { "_links" :
      { "environment" :
        { "href" : "https://api.test-one-pingone.com/v1/environments/18889d16-ea1b-4350-b4a7-be55faea0ebb" },
        "digitalWalletApplications" :
        { "href" : "https://api.test-one-pingone.com/v1/environments/18889d16-ea1b-4350-b4a7-be55faea0ebb/digitalWalletApplications/985fd4b0-6802-402d-917a-5420b4ca5eff" },
        "appOpen" :
        { "href" : "https://neowallet.ping-eng.com/appopen/?u=https%3A%2F%2Fapi.test-one-pingone.com%2Fv1%2Fdistributedid%2Frequests%2F8f4281ad-cc4d-43b0-bfc2-3059da8a4c0a" },
        "qrUrl" :
        { "href" : "https://api.test-one-pingone.com/v1/distributedid/requests/8f4281ad-cc4d-43b0-bfc2-3059da8a4c0a" } },
      "environment" :
      { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },
      "user" :
      { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },
      "digitalWalletApplication" :
      { "id" : "985fd4b0-6802-402d-917a-5420b4ca5eff" },
      "status" : "PAIRING_REQUIRED",
      "pairingSession" :
      { "id" : "6e244046-1f91-4fc2-86c7-b8365a3b6284",
        "createdAt" : "2025-01-28T00:30:54.729645592Z",
        "updatedAt" : "2025-01-28T00:30:54.729645842Z",
        "environment" :
        { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },
        "user" :
        { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },
        "digitalWallet" :
        { "id" : "f121ef78-4ebe-42b0-82e4-32232c77d7da" },
        "challenge" : "3caois8okj6m436o",
        "qrUrl" : "https://api.test-one-pingone.com/v1/distributedid/requests/8f4281ad-cc4d-43b0-bfc2-3059da8a4c0a" },
        "notification" :
        { "methods" :
          [ "EMAIL",
            "SMS" ],
          "results" :
          [
            { "method" : "EMAIL",
              "sent" : true,
              "notification" :
              { "id" : "00cbf8d0-d2d5-4266-9214-99ee270b5448" } },
            { "method" : "SMS",
              "sent" : true,
              "notification" :
              { "id" : "00c0312f-c031-48d5-b60e-5424a4ee25cb" } } ] },
          "id" : "f121ef78-4ebe-42b0-82e4-32232c77d7da" } } }
```

Update User Wallet

Update the status of a digital wallet for a user

Properties

User ID textField

PingOne user ID

Digital Wallet ID textField

Identifier (UUID) of the digital wallet associated with the provisioned credential.

Status dropDown

Status of the wallet

- ACTIVE (Default)
- DISABLED

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User Id
 - `digitalWalletId` string required minLength: 0 maxLength: 100
Digital Wallet Id
 - `digitalWalletStatus` string required minLength: 0 maxLength: 100
Digital Wallet Status

Output Schema

- output object
 - userDigitalWallet object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - digitalWalletApplication object
 - id string
 - status string
 - applicationInstance object
 - id string
 - deviceData object
 - appPackage string
 - sdkVersion string
 - osType string
 - osVersion string
 - manufacturer string
 - model string
 - pushSandbox boolean
 - pushToken string
 - createdAt string
 - updatedAt string
 - notification object
 - methods array
 - results array
 - rawResponse object
 - id string

- environment object
 - id string
- user object
 - id string
- digitalWalletApplication object
 - id string
- status string
- applicationInstance object
 - id string
- deviceData object
 - appPackage string
 - sdkVersion string
 - osType string
 - osVersion string
 - manufacturer string
 - model string
 - pushSandbox boolean
 - pushToken string
- createdAt string
- updatedAt string
- notification object
 - methods array
- results array
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "userDigitalWallet" :
    { "environment" :
      { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },
      "user" :
      { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },
      "digitalWalletApplication" :
      { "id" : "985fd4b0-6802-402d-917a-5420b4ca5eff" },
      "status" : "DISABLED",
      "applicationInstance" :
      { "id" : "a5683da7-b7c6-4189-9c54-999ad5aa896b" },
      "deviceData" :
      { "appPackage" : "com.pingidentity.pingonewallet.sample",
        "sdkVersion" : "1.1.0",
        "osType" : "IOS",
        "osVersion" : "18.1.1",
        "manufacturer" : "Apple",
        "model" : "iPhone15,2",
        "pushSandbox" : false,
        "pushToken" : "1077a9061162cdd15ddd682f7420479dafb66efe6c65eaced8f8c0f01746ab2e" },
      "notification" :
      { "methods" :
        [ "EMAIL",
          "SMS" ],
        "results" :
        [
          { "method" : "EMAIL",
            "sent" : true,
            "notification" :
            { "id" : "0069d1d2-d91e-405d-992d-c6eb40a44f82" } },
          { "method" : "SMS",
            "sent" : true,
            "notification" :
            { "id" : "009d97e7-876e-4652-b74e-96511f491e73" } } ] },
        "pairingAttempts" :
        [
          { "success" : true,
            "attemptedAt" : "2025-01-26T23:22:48.330480980Z" } ],
        "id" : "7a70cefe-d375-40ff-a1ce-510491b91ca9",
        "createdAt" : "2025-01-26T23:22:30.325Z",
        "updatedAt" : "2025-01-29T19:19:19.207542024Z" } } }
```

Delete User Digital Wallet

Remove a digital wallet and all associated credentials for a user

Properties

User ID textField

PingOne user ID

Digital Wallet ID textField

Identifier (UUID) of the digital wallet associated with the provisioned credential.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User Id
 - `digitalWalletId` string required minLength: 0 maxLength: 100
Digital Wallet Id

Output Schema

- output object
 - `rawResponse` object
 - `headers` object
 - `statusCode` integer

Read Credential

Read a credential

Properties

Credential ID textField

Identifier (UUID) of the provisioned user credential

User ID textField

PingOne user ID

Input Schema

- default object
 - properties object
 - credentialId string required minLength: 0 maxLength: 100
Credential ID
 - userId string required minLength: 0 maxLength: 100
User Id

Output Schema

- output object
 - userCredential object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - credentialType object
 - id string
 - version object
 - number number
 - uri string
 - title string
 - status string
 - createdAt string
 - updatedAt string
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - credentialType object
 - id string
 - version object
 - number number
 - uri string
 - title string
 - status string

- createdAt string
- updatedAt string
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :  
  { "userCredential" :  
    { "id" : "31175df4-207d-411e-a6d3-95090bc1b000",  
      "createdAt" : "2025-01-26T20:50:09.116Z",  
      "updatedAt" : "2025-01-26T22:03:07.640Z",  
      "environment" :  
        { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },  
      "user" :  
        { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },  
      "credentialType" :  
        { "id" : "20d91c39-a84f-410c-b07e-6594a2c862a0",  
          "version" :  
            { "number" : 1,  
              "uri" : "https://api.test-one-pingone.com/v1/distributedid/credentialTypes/20d91c39-a84f-410c-b07e-6594a2c862a0/v1" } },  
          "title" : "verifiedEmployee",  
          "status" : "ISSUED" } } } }
```

Read All Credentials

Return all credentials for a user

Properties

User ID textField

PingOne user ID

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
- User Id

Output Schema

- output object
 - userCredentials object
 - _embedded object
 - items array
 - size number
 - rawResponse object
 - _embedded object
 - items array
 - size number
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "userCredentials" :
    { "_embedded" :
      { "items" :
        [
          { "id" : "31175df4-207d-411e-a6d3-95090bc1b000",
            "createdAt" : "2025-01-26T20:50:09.116Z",
            "updatedAt" : "2025-01-26T22:03:07.640Z",
            "environment" :
              { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },
            "user" :
              { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },
            "credentialType" :
              { "id" : "20d91c39-a84f-410c-b07e-6594a2c862a0",
                "version" :
                  { "number" : 1,
                    "uri" : "https://api.test-one-pingone.com/v1/distributedid/credentialTypes/20d91c39-a84f-410c-b07e-6594a2c862a0/v1" } },
            "title" : "verifiedEmployee",
            "status" : "ISSUED" } ] },
          { "size" : 1 } } } }
```

Revoke Credential

Revoke a user's credential

Properties

User ID textField

PingOne user ID

Credential ID textField

Identifier (UUID) of the provisioned user credential

Notification Methods dropDownMultiSelect

- Email
- SMS

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User Id
 - `credentialId` string required minLength: 0 maxLength: 100
Credential ID
 - `notificationMethods` array uniqueItems: true

Output Schema

- output object
 - userCredential object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - credentialType object
 - id string
 - version object
 - number integer
 - uri string
 - title string
 - status string
 - createdAt string
 - updatedAt string
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - credentialType object
 - id string
 - version object
 - number integer
 - uri string
 - title string
 - status string

- createdAt string
- updatedAt string
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :  
  { "userCredential" :  
    { "id" : "31175df4-207d-411e-a6d3-95090bc1b000",  
      "createdAt" : "2025-01-26T20:50:09.116Z",  
      "updatedAt" : "2025-01-29T15:55:34.604072679Z",  
      "environment" :  
        { "id" : "18889d16-ea1b-4350-b4a7-be55faea0ebb" },  
      "user" :  
        { "id" : "0b229251-0fba-472d-adf9-450dea1e237d" },  
      "credentialType" :  
        { "id" : "20d91c39-a84f-410c-b07e-6594a2c862a0",  
          "version" :  
            { "number" : 1,  
              "uri" : "https://api.test-one-pingone.com/v1/distributedid/credentialTypes/20d91c39-a84f-410c-b07e-6594a2c862a0/v1" } },  
          "title" : "verifiedEmployee",  
          "status" : "REVOKED",  
          "expiresAt" : "2025-01-29T15:55:33.325Z" } } }  
    }
```

Issue/Update/Revoke Credential(s)

Apply credential issuance rule to staged changes

Properties

Apply Issue for User ID(s) textFieldArrayView

Array of one or more user IDs for which credentials should be issued

Apply Update for User ID(s) textFieldArrayView

Array of one or more identifiers (UUIDs) of users whose credentials are in an update action state and should be updated

Apply Revoke for User ID(s) textFieldArrayView

Array of one or more identifiers (UUIDs) of users whose credentials are in a revoke action state and should be revoked

Issuance Rule ID textField

Identifier (UUID) of the credential issuance rule.

Credential Type ID textField

Identifier (UUID) associated with the credential type.

Input Schema

- default object
 - properties object
 - applyIssue array uniqueItems: true
Issue
 - applyUpdate array uniqueItems: true
Update
 - applyRevoke array uniqueItems: true
Revoke
 - issuanceRuleId string required minLength: 0 maxLength: 100
Issuance Rule Id
 - credentialTypeId string required minLength: 0 maxLength: 100
Credential Type ID

Output Schema

- output object
 - stagedChanges object
 - _embedded object
 - stagedChanges array
 - size number
 - rawResponse object
 - _embedded object
 - stagedChanges array
 - size number
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "stagedChanges" :
    { "_embedded" :
      { "stagedChanges" :
        [
          { "environment" :
              { "id" : "e43b0fcb-f382-439f-a812-5fe72ee03c70" },
              "credentialType" :
              { "id" : "bdb8e84c-b26c-4f5f-a0dd-bc263b548efe" },
              "issuanceRule" :
              { "id" : "3320b796-d12d-48f8-a49a-2a48a29e9f50" },
              "user" :
              { "id" : "4bed75bf-54a2-421f-a42c-597c39b261f7" },
              "action" : "ISSUE",
              "scheduled" : false,
              "id" : "78cdc229-858f-4ae7-80b6-73349b2cfea7",
              "createdAt" : "2023-04-04T21:46:03.249Z" } ] },
          "size" : 1 } } }
```

Create Verification Session

Begin a session to verify a user's credential

Properties

Message textField

A message shown to the user by the compatible wallet app to alert the user

Protocol dropdown

Protocol to use for verification; can be OPENID4VP or NATIVE. Defaults to NATIVE.

- NATIVE (Default)
- OPENID4VP

Application Instance textField

Application Instance Id.

didMethod dropdown

DID Method

- WEB (Default)
- JWK
- ION

Filter by DIDs textFieldArrayView

Array of unique decentralized identifiers (DIDs) to be searched for the Issuer of the presented credential (OPENID4VP only).

Filter by PingOne Environment ID textFieldArrayView

Array of PingOne environment IDs to be searched for the Issuer of the presented credential.

Requested Credentials variableInputList

Requested Credentials. Variable Name ⇒credential type, value⇒(comma separated keys)

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Variables variableInputList

If Custom variables are defined in the notification body, map them here.

Input Schema

- default object
 - properties object
 - message string minLength: 0 maxLength: 100
Message
 - protocol string required minLength: 0 maxLength: 100
didMethod
 - applicationInstance string minLength: 0 maxLength: 100
Application Instance Id
 - issuerFilterDids array uniqueItems: true
Issue Filter Dids
 - issuerFilterEnvIds array uniqueItems: true
Issue Filter Environment Ids
 - requestedCredentials array
Requested Credentials
 - templateLocale null/string
 - templateVariant null/string
 - templateVariables array

Output Schema

- output object
 - credVerPresentationSession object
 - _links object
 - qr object
 - href string
 - appOpenUrl object
 - href string
 - id string
 - qrCodeImage string
 - osType string
 - status string
 - createdAt string
 - expiresAt string
 - applicationInstance object
 - id string
 - notification object
 - template object
 - locale string
 - variant string
 - variables object string
 - rawResponse object
 - _links object
 - qr object
 - href string
 - appOpenUrl object
 - href string
 - id string
 - qrCodeImage string
 - osType string

- status string
- createdAt string
- expiresAt string
- applicationInstance object
 - id string
- notification object
 - template object
 - locale string
 - variant string
 - variables object string
- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :
  { "credVerPresentationSession" :
    { "_links" :
      { "qr" :
        { "href" : " data:image/png;base64,iVBORw0KGgoAAAANSUhEU...." },
        "appOpenUrl" :
        { "href" : "openid-vc://?request_uri=https://api-test.pingone.com/v1/distributedid/verifications/
presentationSessions/8460cee9-74ae-4bb8-a8de-38830dbf19c2/requestSD" } } },
      "id" : "8460cee9-74ae-4bb8-a8de-38830dbf19c2",
      "status" : "INITIAL",
      "applicationInstance" :
      { "id" : "b378c504-3b26-4be1-a9a0-85b5ba12b142" },
      "createdAt" : "2025-01-13T14:00:21.181885042Z",
      "expiresAt" : "2025-01-13T14:05:21.181883482Z",
      "notification" :
      { "template" :
        { "locale" : "en",
          "variant" : "variant_B",
          "variables" :
          { "name" : "foo",
            "family" : "foo1" } } } } } }
```

Poll for Verification Status

Return the status of a verification session

Properties

Credential Verification ID textField

Identifier (UUID) of the verification credential data

Input Schema

- default object
 - properties object
 - credentialsVerificationId string required minLength: 0 maxLength: 100
Credentials Verification ID

Output Schema

- output object
 - credVerificationStatus object
 - id string
 - qrCodeImage string
 - osType string
 - status string
 - rawResponse object
 - id string
 - qrCodeImage string
 - osType string
 - status string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "credVerificationStatus" :  
    { "id" : "a5efb6a1-c8bf-4fc7-b550-78d5707e0761",  
      "status" : "INITIAL" } } }
```

Return Verification Data

Return data from verified credential

Properties

Credential Verification ID textField

Identifier (UUID) of the verification credential data

Input Schema

- default object
 - properties object
 - credentialsVerificationId string required minLength: 0 maxLength: 100
Credentials Verification ID

Output Schema

- output object
 - credVerificationData object
 - id string
 - status string
 - sessionData object
 - id string
 - credentialsDataList array
 - rawResponse object
 - id string
 - status string
 - sessionData object
 - id string
 - credentialsDataList array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "credVerificationData" :
    { "id" : "10d5bab3-70e0-4e05-871e-04ef9c4b297b",
      "status" : "VERIFICATION_SUCCESSFUL",
      "sessionData" :
        { "id" : "10d5bab3-70e0-4e05-871e-04ef9c4b297b",
          "credentialsDataList" :
            [
              { "issuerId" : "e43b0fcb-f382-439f-a812-5fe72ee03c70",
                "issuerName" : "Issuer name",
                "type" : "VerifiedEmployee",
                "data" :
                  [
                    { "key" : "CardImage",
                      "value" : "<svg xmlns='http://www.w3.org/2000/svg' viewBox='0 0 740 480'><rect fill='none' width='736' height='476' stroke='#CACHED3' stroke-width='3' rx='10' ry='10' x='2' y='2'></rect><rect fill='#FFFFFF' height='476' rx='10' ry='10' width='736' x='2' y='2' opacity='50'></rect><image href='\"' opacity='50' height='476' rx='10' ry='10' width='736' x='2' y='2'></image><line y2='160' x2='695' y1='160' x1='42.5' stroke='#000000'></line><text fill='#000000' font-weight='450' font-size='30' x='45' y='90'>VerifiedEmployee</text><text fill='#000000' font-size='25' font-weight='300' x='45' y='130'>Target</text><text fill='#000000' font-weight='500' font-size='20' x='50' y='228'>First Name: M</text><text fill='#000000' font-weight='500' font-size='20' x='50' y='278'>Last Name: </text></svg>" },
                    { "key" : "First Name",
                      "value" : "M" } ],
                  "verificationStatus" : "VALID" } ] } } } }
```

PingOne Forms Connector

The PingOne Forms connector lets you include branded forms and messages in your PingOne DaVinci flow.

You can use the PingOne Forms connector to:

- Build flows that include user experiences that you create on the **Experiences → Forms** tab in PingOne.
- Show messages using the branding that you define on the **Experiences → Branding & Themes** tab in PingOne.



Important

Forms are only supported in flows that integrate with your application using the [Redirect method](#).

Setup

Resources

For information and setup help, see the following documentation:

- [PingOne Forms](#)

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a PingOne license.

Setting up PingOne Forms

Creating a form

If you want to include a form in your flow, create it in PingOne. For help, see [Creating a form](#).

Configuring branding for a custom message

If you want to include a branded message in your flow, configure your branding in PingOne. For help, refer to [Branding and themes](#).

Setting up the PingOne Forms connector configuration

In DaVinci, add a PingOne Forms connector. For help, refer to [Adding a connector](#).

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Including a form in a flow

The **Show Form** capability lets you present any form that you create with the drag-and-drop form builder. You can optionally prepopulate form fields with variables from your flow.

For more information on creating forms, refer to [Forms](#).

To add a form to a DaVinci flow:

1. In your DaVinci flow, add the PingOne Forms connector.
2. Select the **Show Form** capability.
3. Select the node that appears in your flow.
4. In the **Form** list, select a form that you created in your PingOne environment.
5. In the **Form Theme** list, select a theme for the form. You can select **Use Theme ID** to enter the **Theme ID** associated with a theme configured in **User Experience > Branding and Themes** in the PingOne admin console.

Note

This list is populated with themes configured in PingOne under **User Experience → Branding & Themes**. Each theme also has a unique Theme ID that can be copied and pasted into the connector after selecting **Use Theme ID**.

If no theme is selected, the default PingOne Active Theme will be displayed.

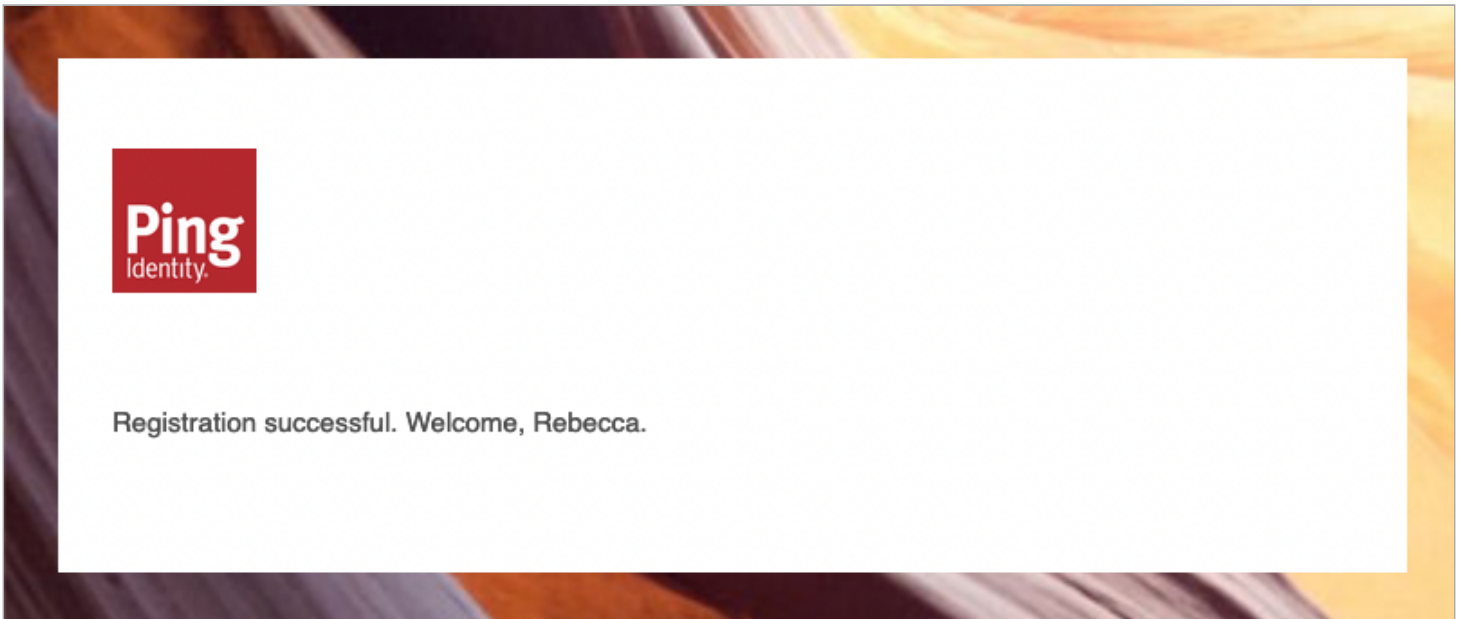
6. Configure the fields displayed.

Note

The fields will vary depending on the kind of form you are configuring. Learn more in [Creating a form](#).

Showing a message with your branding

The **Show Branded Message** capability lets you show the user a message within a frame that is branded according to the settings on the **Experiences > Branding & Themes** tab in PingOne.



1. In your flow, add the PingOne Forms connector and select the **Show Branded Message** capability. Select the node that appears in your flow.
2. In the **Message** field, enter static text or click **{}** to include variables from your flow.
3. In the **Form Theme** list, select a theme for the branded message.

Note

This list is populated with themes configured in PingOne under **User Experience > Branding & Themes**. Each theme also has a unique Theme ID that can be copied and pasted into the connector after selecting **Use Theme ID**.

If no theme is selected, the default PingOne Active Theme will be displayed.

4. Click **Apply**.

Capabilities

Show Form

Show a form from the drag-and-drop form builder.

Properties

Form dropDown required

The form to show. You can add forms in your PingOne environment. For a dynamic value or to use a form that isn't listed, select "Use Form ID".

Forms link

Link with PingOne User toggleSwitch

When enabled, DaVinci creates or updates a linked PingOne user account using attributes from the external IdP.

PingOne Population dropDown

The PingOne population to use when authenticating the user.

- Use Population ID (Default)

Population ID textField

The ID of the PingOne population to use when authenticating the user, such as "aa4b3e81-cf7e-8685-4b7b-7ec89cfcf7c8".

Initial Field Values keyValuePairList

Optionally provide a value to pre-populate the fields in your form. Users can keep the pre-populated value or change it before submitting the form.

Dynamic Text keyValuePairList

Provide a string to populate the dynamic text in your form. Dynamic text is defined in Translatable Rich Text and Label fields by wrapping a key in curly braces, such as {{userFirstName}}.

Device Profiling sectionLabel

Enable Device Profiling toggleSwitch

Enable PingOne Protect SDK to collect device information.

Include Behavioral Data toggleSwitch

When enabled, collects behavioral data to identify non-human activity. Enable Device Profiling must be enabled beforehand.

Enable Universal Device Identification toggleSwitch

Identify the device via a unique device ID combined with a digital signature that ensures information collected about the device has not been tampered with.

Enable PingID Agent toggleSwitch

When enabled, the Signals SDK collects attributes from the PingID Device Trust Agent.

PingID Agent Timeout (ms) textField

The time, in milliseconds, for establishing a connection with the PingID Device Trust Agent. If left blank, the default value is set by the Signals SDK. If specified, the value must be between 200 and 10,000 milliseconds.

PingID Agent Port textField

The port number to use when connecting to the PingID Device Trust Agent. If left blank, the default port 9400 will be used.

Social Login sectionLabel***Application Return URL textField***

When using the embedded flow player widget and an IdP/Social Login connector, provide a callback URL to return back to the application.

Authentication Method Source dropDown required

Determines where to get the list of authentication methods to present to the user. Select an MFA policy, specify a policy ID, or specify the exact authentication method list.

- Use current default MFA policy (Default)
- Use MFA Policy ID
- Use Custom Authentication Method List

MFA Policies link***MFA Policy ID textField required***

The ID of the MFA Policy to use during flow execution, such as "aa4b3e81-cf7e-8685-4b7b-7ec89cfc7c8".

Custom Authentication Method List textField required

The list of MFA authentication methods that you want to make available to the user, such as "EMAIL,TOTP". To allow all devices, enter "EMAIL, MOBILE, SMS, VOICE, TOTP, FIDO2, MAGIC_LINK". Separate multiple values with a comma.

Enable Magic Link Authentication toggleSwitch

When enabled, the Magic Link option is available in the authentication method list.

User ID textField required

The ID of the user to authenticate, such as "488e2f16-b765-4620-833d-f673669fecf6".

Enable Polling toggleSwitch

Use polling to loop this part of the flow, or a challenge to pause the flow on this node, while waiting for another part of the flow to complete.

pollInterval textField

The amount of time in milliseconds to wait between each polling status check.

Default: 2000

pollRetries textField

The maximum number of times to check the polling status before failing, such as 60.

Default: 60

pollChallengeStatus toggleSwitch

When enabled, the form remains on the screen while DaVinci polls a challenge variable in another branch of the flow. When disabled, the flow continues past the form and loops at the next Continue Polling node.

challenge textField

Select a challenge variable from your flow, such as from a Challenge or Flow Conductor node. When this challenge is completed in another branch of the flow, the main flow continues past the form.

Input Schema

- default object
 - language string
 - properties object
 - form string required
 - theme string required
 - themeld string
 - linkWithP1User boolean
 - population string
 - populationId string
 - formData array
 - enableRisk boolean
 - collectBehavioralData boolean
 - universalDeviceIdentification boolean
 - pingidAgent boolean
 - pingidAgentTimeout string
 - pingidAgentPort string
 - authenticationMethodSource string
 - mfaPolicyId string
 - authenticationMethodList string
 - userId string
 - linkFormsUrl string
 - linkBrandingThemesUrl string
 - linkMFAPolicies string
 - challenge string
 - enablePolling boolean
 - pollInterval string
 - pollRetries string
 - pollChallengeStatus boolean
 - enableMagicLinkAuthentication boolean

- publicKeyCredentialCreationOptions string
- publicKeyCredentialRequestOptions string

Output Schema

- output object
 - formData object
 - themeld string
 - event object
 - type string
 - buttonValue string

Show Branded Message

Show a message with your PingOne branding theme.

Properties

Message textArea

The message to show to the user.

Button Text textField

The text to show on the continue button, such as "Submit" or "Continue".

Default: `Submit`

showContinueButton toggleSwitch

When enabled, the user interface includes a button that allows the user to continue the flow.

Input Schema

- default object
 - properties object
 - theme string required
 - themeld string
 - message string
 - buttonText string
 - showContinueButton boolean

Output Schema

- output object
 - themeld string

PingOne Forms Connector Release Notes

New features and improvements in the PingOne Forms connector. Updated May 22, 2024.

May 2024

The Show Form capability now includes social login

Improved

Social login simplifies a user's sign-on process by allowing them to sign on using their existing social accounts. If you select a **Form** configured in PingOne, you will see the additional **Link with PingOne User** and **PingOne Population** fields to configure the social login button.

This feature is in limited release. Contact Ping support to request access to this feature.

April 2024

Specify branding and theme for forms within the PingOne Forms Connector

New

The **Show Form** and **Show Branded Message** capabilities now include the ability to specify a theme with the new **Form Theme** field, which displays the themes configured in your PingOne environment under **Branding & Themes**.

Additionally, you can also select **Use Theme ID** and paste the unique Theme ID. Learn more in [Selecting a theme](#).

September 2023

The Forms connector now supports risk profiling

New

The **Show Form** capability now has two new fields:

- You can turn on **Enable Device Profiling** to connect with the PingOne Protect SDK. When enabled, device information is collected for risk profiling.
- After you turn on **Enable Device Profiling**, you can then turn on **Include Behavioral Data** to identify non-human activity as an additional safeguard.

April 2023

The Forms connector is now available

New

You can use the Forms connector to:

- Build flows around user experiences that you create on the **Experiences > Forms** tab in PingOne.
- Show messages using the branding that you define on the **Experiences > Branding & Themes** tab in PingOne.

PingOne MFA Connector

PingOne MFA is a cloud-based multi-factor authentication (MFA) service that protects an organization's network, applications, and data resources while providing secure and seamless experiences for your customers and users.

The PingOne MFA connector supports the use of:

- Customer-friendly authentication flows to increase security without adding unnecessary friction to the end user experience
- User enrollment flows:
 - Automatically: Allow customers to automatically enroll an authentication method for users during different operations, such as registering the user email or phone number as part of a user provisioning
 - Manually: Allow users to manage their devices and add authentication methods during enrollment
 - One-time device authentication: Include device details within an authentication request. Enables a user to authenticate for one session only, without pairing the device.
- Usernameless and passwordless sign-on and authentication flows using appropriate, secure authentication methods, such as FIDO biometrics

Setup

Resources

- PingOne documentation:
 - [Introduction to PingOne MFA](#)
 - [Getting started with PingOne MFA](#)
 - [Adding an application](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne MFA license ([Try PingOne for free](#))
- A PingOne MFA environment with a configured Worker app
- A multi-factor authentication (MFA) policy. See [MFA policies](#).

Setting up PingOne MFA

Setting up your PingOne MFA environment

Follow the instructions in [Getting started with PingOne MFA](#).

Setting up the connector

In DaVinci, add a **PingOne MFA** connection. For help, see [Adding a connector](#).

Connector settings

Environment ID

Your PingOne Environment ID. In PingOne, go to **Settings → Environment Properties**.

Policy ID

The unique identifier for the device authentication policy. You can define MFA policies and reference them as part of the connector setup. See [MFA policies](#).

Client ID

The Client ID for your PingOne Worker application. In PingOne, go to **Applications → Applications → Configuration**.

Client Secret

The Client Secret for your PingOne Worker application. In PingOne, go to **Applications → Applications → Configuration**.

Region

Your PingOne environment region. In PingOne, go to **Settings → Environment Properties**.

Using the connector in a flow

Enrolling a device

To enable users and increase MFA adoption, use the PingOne MFA connector to include a device enrollment as part of user registration or as a just-in-time (JIT) registration within an authentication flow.

The user can select an authentication method for MFA from a list of methods defined by your organization's policy. This list can include traditional methods, such as email and SMS, and more secure and frictionless methods, such as FIDO2 biometrics and a native mobile SDK.

You can define device enrollment as either mandatory or optional.

You can choose to enable MFA automatically when device enrollment completes so that the next time the user authenticates, the device is available for them to use to authenticate.

Search the [Flow Library](#) for the following out-of-the-box PingOne MFA device enrollment templates:

- PingOne — Registration and MFA Enrollment

 Note

This flow must include the **PingOne - Device Registration sub-flow** to provide on-the-fly device enrollment for users during registration.

- PingOne — Registration and MFA Auto-Enrollment

In this flow, the Admin selects which devices to enroll for the user.

For help, see the [Creating an authentication flow](#) guide.

Authenticating users

Use the PingOne MFA connector to increase security by adding an authentication factor that requires the user to prove their identity using a trusted device.

Search the [Flow Library](#) for the following out-of-the-box PingOne MFA authentication templates:

- PingOne — Sign on and MFA

 Note

This flow must include the **PingOne - Device Registration sub-flow** to provide on-the-fly device enrollment for users during registration.

- PingOne - Sign on and Adaptive MFA

 Note

This flow must include the following sub-flows:

- PingOne - Device Registration sub-flow to provide on-the-fly enrollment for users that have not yet registered a device
- PingOne - MFA Authentication sub-flow

- PingOne - One-time use device authentication

Indicate whether a paired device is used, or specify a device explicitly for one-time authentication.

For help, see the [Creating an authentication flow](#) guide.

Configuring passwordless authentication

Use the PingOne MFA connector to enhance your end user's login experience and increase security by adding passwordless authentication using standard methods such as SMS, OTP, biometric authentication, and QR code scanning. The end user must enable biometric authentication on their machine and enroll it for use with PingOne MFA to benefit from frictionless biometric login, removing the need to enter a password each time they sign on.

You can use the PingOne MFA connector to design the following types of passwordless authentication flows:

- PingOne Usernameless sign-on with biometrics

User authenticates by scanning their compatible FIDO authenticator, without requiring a username or password.

- PingOne - Passwordless authentication

User enters a username and uses any compatible device to authenticate. If the user device is not yet registered, they must verify the device using a one-time passcode (OTP) sent to the email or mobile number (using one-time use device authentication). After successfully verifying the device they can register it for passwordless authentication.

- PingOne - Passwordless sign-on with biometrics

User enters their username and either provides their existing password, or uses their device biometrics to authenticate.

- PingOne - QR code passwordless sign-on

User signs on by scanning a QR code using a mobile application, with no need to input any other information.

**Note**

This flow requires a custom mobile app that uses the PingOne MFA mobile SDK.

**Note**

In order to get the benefits of frictionless biometric login instead of having to enter their user credentials each time they sign on, end users must enable biometric authentication on their device and enroll it for use with PingOne MFA.

You can find sample passwordless authentication flows in the [Flow Library](#). For help, refer to the [Creating an authentication flow](#) guide.

Capabilities

Read Device

Read information for a device associated with a user.

Properties

User ID textField

The unique identifier for the user.

Device ID textField

The unique identifier for the MFA device.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - deviceId string required minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - headers object
 - statusCode integer
 - device object
 - id string
 - type string

- status string
- nickname string
- phone string
- extension string
- email string
- secret string
- keyUri string
- oathToken string
- serialNumber string
- rp object
 - id string
 - name string
- platform string
- publicKeyCredentialCreationOptions string
- attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
- displayName string
- createdAt string
- updatedAt string

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```


Read All Devices

Read information for all user devices

Properties

User ID textField

The unique identifier for the user.

Filters toggleSwitch

Filter devices by activation status and device type.

Status dropDown

non-active devices are not usable during an authentication.

- ALL (Default)
- ACTIVE
- ACTIVATION REQUIRED

Device Types dropDownMultiSelect

- Email
- SMS
- Voice
- Authenticator App
- Mobile Applications
- Fido2 Biometrics
- Security Key
- Oath token

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - setFilterFlag boolean
 - statusFilter string
 - deviceTypes array uniqueItems: true

Output Schema

- output object
 - rawResponse object
 - _embedded object
 - devices array
 - applications array
 - allowedtypes array
 - order array
 - id string
 - mfaSettings object
 - environment object
 - id string
 - pairing object
 - maxAllowedDevices integer
 - mfaPolicy object
 - authentication object
 - deviceSelection string
 - size number
 - headers object
 - statusCode integer
 - devices array
 - allowedtypes array
 - applications array
 - mfaSettings object
 - environment object
 - id string
 - pairing object
 - maxAllowedDevices integer

- mfaPolicy object
 - authentication object
 - deviceSelection string
- order array
 - id string

Output Example

```

{ "rawResponse" :
  { "_embedded" :
    { "devices" :
      [
        { "device" :
          { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
            "type" : "SMS",
            "status" : "ACTIVE",
            "nickname" : "Work Device",
            "phone" : "+972528888888",
            "extension" : "###1",
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],
        "applications" :
          [
            { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
              "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
              "name" : "IOS nativeApp",
              "enabled" : true,
              "mobile" :
                { "bundleId" : "com.pingIdentity.p14c.sample",
                  "integrityDetection" :
                    { "mode" : "DISABLED" } } } ],
            "allowedtypes" :
              [ "SMS",
                "VOICE",
                "MOBILE",
                "TOTP",
                "OATH_TOKEN",
                "YUBIKEY",
                "PINGID_DESKTOP",
                "PLATFORM",
                "SECURITY_KEY" ],
            "order" :
              [
                { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

                { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
            "mfaSettings" :
              { "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
                "pairing" :
                  { "maxAllowedDevices" : 5 } },
            "mfaPolicy" :
              { "authentication" :
                { "deviceSelection" : "DEFAULT_TO_FIRST" } } },
            "count" : 1,
            "size" : 1 },
        "devices" :
          [
            { "device" :
              { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
                "type" : "SMS",
                "status" : "ACTIVE",
                "nickname" : "Work Device",
                "phone" : "+972528888888",
                "extension" : "###1",
                "createdAt" : "2021-01-15T20:45:17.463Z",
                "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],

```

```

"applications" :
[
  { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
    "name" : "iOS nativeApp",
    "enabled" : true,
    "mobile" :
      { "bundleId" : "com.pingIdentity.p14c.sample",
        "integrityDetection" :
          { "mode" : "DISABLED" } } } ],
"allowedtypes" :
[ "SMS",
  "VOICE",
  "MOBILE",
  "TOTP",
  "OATH_TOKEN",
  "YUBIKEY",
  "PINGID_DESKTOP",
  "PLATFORM",
  "SECURITY_KEY" ],
"order" :
[
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

  { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
"mfaSettings" :
{ "environment" :
  { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
  "pairing" :
    { "maxAllowedDevices" : 5 } },
"mfaPolicy" :
{ "authentication" :
  { "deviceSelection" : "DEFAULT_TO_FIRST" } } }

```

Create Device

Create devices to use during authentication.

Properties

User ID textField

The unique identifier for the user.

Device Type dropDown

The type of device used during authentication.

- Email
- SMS
- Voice
- Authenticator App
- Mobile Applications
- Fido2 Biometrics
- Security Key
- Oath token
- Enter Device Type

Enter Device Type textField

Activation Status dropDown

The current status of the device. If a device has an ACTIVATION_REQUIRED status, activate it before you add it as a trusted device.

- ACTIVE
- ACTIVATION REQUIRED

Phone Number textField

The phone number to associate with the device. Applies only to devices that use SMS and Voice SMS messages during authentication.

Extension textField

The phone extension for this device. It can include digits, comma, # and *. If there is more than one extension then a comma should separate the extension and the nested extension.

Email textField

The email address to associate with the device. Applies only to devices that use email during authentication.

Device Nickname textField

A nickname that identifies this device. The device nickname is limited to 100 characters.

Relying Party ID textField

If you define a Relying Party ID (RPID) here, it overrides the RPID defined in the FIDO policy in the PingOne admin console.

Relying Party Name textField

A string that specifies the relying party's human-readable display name.

Serial Number textField

The unique identifier for the OAuth token.

Notification Policy dropDown

A unique identifier for the policy.

- Enter Notification Policy ID

Notification Policy ID textField***Notification Name dropDown***

The name of a custom notification defined in PingOne. If the form you want is not listed, select Enter Custom Value.

- Enter Custom Value

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Notification Variables variableInputList

If Custom variables are defined in the notification body, map them here.

User Agent textField

Browser user agent

Custom FIDO2 Challenge textField

Applicable for FIDO2 pairing requests. Specify a custom challenge that will replace the automatically generated challenge sent with the pairing request. Must be a valid Base64URL string that decodes to at least 32 bytes of data array.

Test Mode textField

Create device for test purposes only

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `deviceType` string required
 - `customDeviceType` null/string/object
 - `status` string required
 - `nickname` string
 - `phone` string
 - `extension` string
 - `email` string
 - `rpId` string
Relying Party ID
 - `rpName` string
Relying Party Name
 - `serialNumber` string
Serial Number
 - `notificationPolicyId` string minLength: 0 maxLength: 100
 - `customNotificationPolicyId` null/string/object
 - `templateVariant` null/string
 - `customTemplateVariant` null/string/object
 - `templateLocale` null/string
 - `templateVariables` array
 - `userAgent` string
User Agent
 - `challenge` string
Custom FIDO2 Challenge
 - `createDeviceTestMode` string
Create Test Device
 - `oneTimeDeviceTestMode` string

Create Test Device

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - test object
 - otp string
 - headers object
 - statusCode integer

- device object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```

Activate Device

Activate devices for the first time.

Properties

User ID textField

The unique identifier for the user.

Device ID textField

The unique identifier for the MFA device.

One-time Passcode textField

The one-time passcode (OTP) sent to the user.

Attestation textField

A read-only string that specifies the public key and signed challenge used to complete registration and device activation. The attestation is generated by the browser as a response to a specific user action, such as a fingerprint scan or tap on a security key.

Origin textField

The address of the server sending the initial registration challenge to the device.

OATH Token Resync toggleSwitch

Indicates if OATH token resync is permitted during registration

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `deviceId` string required minLength: 0 maxLength: 100
 - `otp` string
 - Passcode
 - `attestation` string
 - WebAuthn assertion
 - `origin` string
 - Origin
 - `oathResync` boolean
 - Allow OATH token resync

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - headers object
 - statusCode integer
 - device object
 - id string
 - type string

- status string
- nickname string
- phone string
- extension string
- email string
- secret string
- keyUri string
- oathToken string
- serialNumber string
- rp object
 - id string
 - name string
- platform string
- publicKeyCredentialCreationOptions string
- attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
- displayName string
- createdAt string
- updatedAt string

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```

Delete Device

Delete devices.

Properties

User ID textField

The unique identifier for the user.

Device ID textField

The unique identifier for the MFA device.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - deviceId string required minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Resend OTP for Pairing

If user did not receive the one-time passcode (OTP) that was sent for pairing a device, you can resend the OTP.

Properties

User ID textField

The unique identifier for the user.

Device ID textField

The unique identifier for the MFA device.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - deviceId string required minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```

Update Device Nickname

Update device nicknames.

Properties

User ID textField

The unique identifier for the user.

Device ID textField

The unique identifier for the MFA device.

Device Nickname textField

A nickname that identifies this device. The device nickname is limited to 100 characters.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - deviceId string required minLength: 0 maxLength: 100
 - nickname string required
 - Device nickname

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer
 - nickname string

Output Example

```
{ "rawResponse" :  
  { "nickname" : true } }
```

Read MFA Status

Indicates whether MFA is enabled for the user.

Properties

User ID textField

The unique identifier for the user.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer
 - mfaEnabled boolean

Output Example

```
{ "rawResponse" :  
  { "mfaEnabled" : true } }
```

Update MFA Status

Enables or disables MFA for the user.

Properties

User ID textField

The unique identifier for the user.

Enable User MFA toggleSwitch

Enable or disable user MFA.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - mfaEnabled boolean required
 - MFA Enable Status Of User

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer
 - mfaEnabled boolean

Output Example

```
{ "rawResponse" :  
  { "mfaEnabled" : true } }
```

Read Device Authentication Policy

Read MFA device authentication policies.

Properties

Device Authentication Policy dropDown

A unique identifier for the policy.

- Enter Device Authentication Policy ID

Device Authentication Policy ID textField required

Input Schema

- default object
 - properties object
 - deviceAuthenticationPolicyId string required minLength: 0 maxLength: 100
 - customDeviceAuthenticationPolicyId null/string/object

Output Schema

- output object
 - rawResponse object
 - id string
 - name string
 - forSignOnPolicy boolean
 - default boolean
 - sms object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer
 - timeUnit string
 - email object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer
 - timeUnit string

- voice object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer
 - timeUnit string
- mobile object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - window object
 - stepSize object
 - duration integer
 - timeUnit string
- totp object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer

- timeUnit string
- platform object
 - enabled boolean
- securityKey object
 - enabled boolean
- rememberMe object
 - web object
 - enabled boolean
 - lifeTime object
 - duration integer
 - timeUnit string
- createdAt string
- updatedAt string
- headers object
- statusCode integer
- deviceAuthenticationPolicy object
 - id string
 - name string
 - forSignInPolicy boolean
 - default boolean
 - sms object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer

- timeUnit string
- email object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer
 - timeUnit string
- voice object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
 - lifeTime object
 - duration integer
 - timeUnit string
- mobile object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer

- timeUnit string
- window object
 - stepSize object
 - duration integer
 - timeUnit string
- totp object
 - enabled boolean
 - otp object
 - failure object
 - count integer
 - coolDown object
 - duration integer
 - timeUnit string
- platform object
 - enabled boolean
- securityKey object
 - enabled boolean
- rememberMe object
 - web object
 - enabled boolean
 - lifeTime object
 - duration integer
 - timeUnit string
- createdAt string
- updatedAt string

Output Example

```

{ "rawResponse" :
{ "deviceAuthenticationPolicy" :
{ "id" : "58bet177-1871-420b-b1b5-4dcad2d07958",
  "environment" :
  { "id" : "14b3c9b9-107b-48ae-8c0a-e65f94054ebb" },
  "name" : "Default For Sign On Policy",
  "sms" :
  { "enabled" : true,
    "otp" :
    { "failure" :
      { "count" : 3,
        "coolDown" :
        { "duration" : 0,
          "timeUnit" : "MINUTES" } },
      "lifeTime" :
      { "duration" : 30,
        "timeUnit" : "MINUTES" } } },
    "email" :
    { "enabled" : true,
      "otp" :
      { "failure" :
        { "count" : 3,
          "coolDown" :
          { "duration" : 0,
            "timeUnit" : "MINUTES" } },
        "lifeTime" :
        { "duration" : 30,
          "timeUnit" : "MINUTES" } } },
      "voice" :
      { "enabled" : true,
        "otp" :
        { "failure" :
          { "count" : 3,
            "coolDown" :
            { "duration" : 0,
              "timeUnit" : "MINUTES" } },
          "lifeTime" :
          { "duration" : 30,
            "timeUnit" : "MINUTES" } } },
        "mobile" :
        { "enabled" : true,
          "otp" :
          { "failure" :
            { "count" : 3,
              "coolDown" :
              { "duration" : 0,
                "timeUnit" : "MINUTES" } },
            "window" :
            { "stepSize" :
              { "duration" : 30,
                "timeUnit" : "MINUTES" } } } },
          "totp" :
          { "enabled" : true,
            "otp" :
            { "failure" :
              { "count" : 3,
                "coolDown" :
                { "duration" : 0,
                  "timeUnit" : "MINUTES" } } } },
            "platform" :

```

```
{ "enabled" : true },
"securityKey" :
{ "enabled" : true },
"rememberMe" :
{ "web" :
{ "enabled" : false,
"lifeTime" :
{ "duration" : 30,
"timeUnit" : "DAYS" } } },
"createdAt" : "2021-07-19T18:24:58.779Z",
"updatedAt" : "2021-07-19T18:24:58.795Z" } } }
```

Create Device Authentication

Create authentication experiences with virtual or physical devices.

Properties

User ID Not Required toggleSwitch

Indicates whether the user id is required or obtained from the authentication method used.

User ID textField

The unique identifier for the user.

MFA Policy ID textField

The ID of your PingOne MFA device authentication policy.

User Agent textField

Browser user agent

Device Details dropDown

Indicates whether to use the user's default authentication method or to provide a specific authentication method.

- ID
- One-Time Device

Device ID textField

The selected device id

Device Type textField

The one-time device type

SMS Phone Number textField

The phone number to associate with the one-time SMS device.

Voice Phone Number textField

The phone number to associate with the one-time Voice device.

Email textField

The email address to associate with the one-time device.

Test Mode textField

Create device for test purposes only

Notification Type dropDown

Indicates whether the notification is intended for a user authentication flow or a device authorization flow.

- Strong Authentication

- Transaction

Notification Policy dropDown

A unique identifier for the policy.

- Enter Notification Policy ID

Notification Policy ID textField

Notification Name dropDown

The name of a custom notification defined in PingOne. If the form you want is not listed, select Enter Custom Value.

- Enter Custom Value

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Notification Variables variableInputList

If Custom variables are defined in the notification body, map them here.

Mobile Payload textField

A signed challenge generated by PingOne MFA mobile SDK.

Application dropDown

The unique identifier of the native application which initiated the authentication flow.

- Enter Application ID

Application ID textField

Mobile Client Context variableInputList

Additional attributes that can be passed to the mobile application during the authentication.

Relying Party ID textField

If you define a Relying Party ID (RPID) here, it overrides the RPID defined in the FIDO policy in the PingOne admin console.

Custom FIDO2 Challenge textField

Applicable for FIDO2 authentication requests. Specify a custom challenge that will replace the automatically generated challenge sent with the authentication request. Must be a valid Base64URL string that decodes to at least 32 bytes of data array.

One-time Passcode textField

The one-time passcode (OTP) of the device used to authenticate. If the Device ID is not provided, the OTP is validated against all the applicable devices.

Input Schema

- default object
 - properties object
 - `userId` string minLength: 0 maxLength: 100
 - `mfaPolicyId` string minLength: 0 maxLength: 100
 - `authTemplateName` null/string
 - string
 - STRONG_AUTHENTICATION
 - TRANSACTION
 - null
 - `notificationPolicyId` string minLength: 0 maxLength: 100
 - `customNotificationPolicyId` null/string/object
 - `templateVariant` null/string
 - `customTemplateVariant` null/string/object
 - `templateLocale` null/string
 - `templateVariables` array
 - `mobilePayload` null/string
 - Mobile Payload
 - `applicationId` string minLength: 0 maxLength: 100
 - Application ID
 - `customApplicationId` null/string/object
 - `clientContext` array
 - Mobile Client Context
 - `userAgent` string
 - User Agent
 - `rpId` string
 - Relying Party ID
 - `deviceAuthenRpId` string
 - Relying Party ID
 - `challenge` string

Custom FIDO2 Challenge

- createDeviceTestMode string

Create Test Device

- oneTimeDeviceTestMode string

Create Test Device

- usernameLess boolean

User ID Not Required

- selectedDevice null/string

- string

- id

- oneTime

- null

- selectedDeviceId null/string

- oneTimeDeviceType null/string

- string

- SMS

- VOICE

- EMAIL

- null

- oneTimeSmsDevice null/string

- oneTimeVoiceDevice null/string

- oneTimeEmailDevice null/string

- otp string

Passcode

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - test object
 - otp string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                  [
                    { "type" : "EMAIL",
                      "email" : "o*****@pingidentity.com" } ] } } } }
```

Read Device Authentication

Read device authentication information.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

Input Schema

- default object
 - properties object
 - deviceAuthenticationId string required minLength: 0 maxLength: 100
- Device Authentication ID

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-ee8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                  [
                    { "type" : "EMAIL",
                      "email" : "o*****@pingidentity.com" } ] } } } }
```

Device Selection

Enables users to choose the way they authenticate if more than one option is available.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

Device ID textField

The unique identifier for the MFA device.

WebAuthn Browser Compatibility textField

Input Schema

- default object
 - properties object
 - deviceId string required minLength: 0 maxLength: 100
 - deviceAuthenticationId string required minLength: 0 maxLength: 100
Device Authentication ID
 - compatibility null/string
WebAuthn Compatibility

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                  [
                    { "type" : "EMAIL",
                      "email" : "o*****@pingidentity.com" } ] } } } }
```

Device Passcode

Ensures that device one-time passcodes (OTPs) are valid.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

One-time Passcode textField

The one-time passcode (OTP) sent to the user.

Input Schema

- default object
 - properties object
 - otp string required
Passcode
 - deviceAuthenticationId string required minLength: 0 maxLength: 100
Device Authentication ID

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-ee8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                [
                  { "type" : "EMAIL",
                    "email" : "o*****@pingidentity.com" } ] } } } }
```

FIDO Assertion

Ensures that assertions provided to authenticate devices are valid.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

Assertion textField

A string that specifies the authenticator assertion response. The string contains the signed challenge needed to complete the MFA authentication.

Origin textField

The address of the server sending the initial registration challenge to the device.

WebAuthn Browser Compatibility textField

Input Schema

- default object

- properties object

- assertion string required

- WebAuthn assertion

- origin string required

- Origin

- deviceAuthenticationId string required minLength: 0 maxLength: 100

- Device Authentication ID

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
    "user" :
      { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
    "status" : "ASSERTION_REQUIRED",
    "selectedDevice" :
      { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
    "policy" :
      { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
    "publicKeyCredentialRequestOptions" : "{ \"challenge\":
      [-85,59,-40,126,-17,11,-105,-114,-112,98,26,-11,65,108,101,35,106,81,-40,49,81,-68,5,48,-6,43,-107,-2,-115,68
      ,15,81],\"timeout\":120000,\"rpId\":\"pingone.com\", \"allowCredentials\": [{ \"type\":\"public-key\", \"id\":
      [1,62,-107,73,-122,23,-91,-57,-123,-52,121,-112,-115,30,112,13,-76,119,55,-87,-80,94,-71,-85,111,-102,-83,115
      ,
      75,-106,-44,63,-71,-14,-93,9,-19,-63,-117,4,-98,-63,80,93,-19,-118,124,87,-63,21,-5,-86,79,-99,-114,-26,-1,-9
      2,-110,67,127,39,38,-18,71]},{ \"type\":\"public-key\", \"id\":
      [41,-87,-83,-39,39,126,-86,-71,-93,25,-10,-79,19,58,116,62,-52,14,127,-91,35,-117,1,117,9,124,10,-23,48,-119,
      16,89]}], \"userVerification\":\"preferred\"}",
    "createdAt" : "2021-01-15T20:45:17.463Z",
    "updatedAt" : "2021-01-15T20:45:17.463Z",
    "_embedded" :
      { "devices" :
          [
            { "type" : "SECURITY_KEY",
              "rp" :
                { "id" : "pingone.com",
                  "name" : "PingOne MFA" } } ] } } }
```

Cancel Push Notification

Cancels the push notification sent to user's device if it hasn't been acted on.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

Input Schema

- default object
 - properties object
 - deviceAuthenticationId string required minLength: 0 maxLength: 100
Device Authentication ID

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - selectedDevice object
 - id string
 - status string
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```

{ "rawResponse" :
  { "_embedded" :
    { "devices" :
      [
        { "id" : "e1ad986f-1497-46a7-ad2c-631b4f8311dd",
          "type" : "MOBILE",
          "status" : "ACTIVE",
          "usableStatus" :
            { "status" : "ENABLED" },
          "deviceIntegrityState" :
            { "compromised" : "UNKNOWN",
              "reason" : "PLAY_ERROR",
              "timestamp" : 1.714468544848E12 },
          "os" :
            { "version" : "8",
              "type" : "iOS" },
          "apiVersion" : "2.0",
          "model" :
            { "name" : "Iphone 12",
              "marketingName" : "Iphone 12" },
          "application" :
            { "id" : "f0d76ca7-0b65-4e44-b272-794a91d87294",
              "nativeName" : "PingOneInternal",
              "version" : "1.11.0",
              "name" : "NativeAppForInternalApp",
              "pushSandbox" : false,
              "passcodeRefreshDuration" :
                { "duration" : 30,
                  "timeUnit" : "SECONDS" } },
          "pushEnabled" : true,
          "manufacturer" : "apple",
          "sdkVersion" : "1.11.0(9230)",
          "rooted" : false,
          "lockEnabled" : true,
          "locale" : "en-GB",
          "notificationProvider" : "APNS",
          "notification" : "enabled",
          "background" : "unknown",
          "allowPushNotification" : true,
          "pushStatus" :
            { "status" : "ENABLED" },
          "otpEnabled" : true,
          "otpStatus" :
            { "status" : "ENABLED" },
          "pushFails" :
            [ 1.714629982277E12 ] } ] },
        { "id" : "001c2d36-fa6a-402a-9842-96b30bc7af95",
          "environment" :
            { "id" : "9ffc5b7c-4c7e-4fcc-8834-964ab0b0f914" },
          "status" : "DEVICE_SELECTION_REQUIRED",
          "selectedDevice" :
            { "id" : "e1ad986f-1497-46a7-ad2c-631b4f8311dd" },
          "user" :
            { "id" : "d2f8be92-4dd6-4b65-891e-f1d20cec00a8" },
          "createdAt" : "2024-05-02T06:05:48.362Z",
          "updatedAt" : "2024-05-02T06:06:22.290Z",
          "aggregateFido2Devices" : false } }

```

Read Pairing Key

Read pairing key information associated with users.

Properties

User ID textField

The unique identifier for the user.

Pairing Key ID textField

The unique identifier for the pairing key.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `pairingKeyId` string required minLength: 0 maxLength: 100
 - Pairing Key ID

Output Schema

- output object
 - rawResponse object
 - id string
 - code string
 - status string
 - error object
 - code string
 - message string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "b47a7af3-598c-4bc9-9ad7-43e6bf5d8cca",
    "environment" :
      { "id" : "9f1b3773-aae5-4903-b3a2-837c5b6f6467" },
    "code" : "01552143316127",
    "status" : "UNCLAIMED",
    "applications" :
      [
        { "id" : "2a0d74e5-d856-44f5-ae21-7c3ec8d9ce37" } ],
    "user" :
      { "id" : "8dd4ed0f-391c-40d6-a1c9-ef0f6e3e8b40" },
    "createdAt" : "2021-12-21T09:37:00.816Z",
    "updatedAt" : "2021-12-21T09:37:00.816Z",
    "expiresAt" : "2021-12-23T09:37:00.816Z" } }
```

Create Pairing Key

Create pairing keys that can be used by native mobile applications to create trust with PingOne MFA.

Properties

User ID textField

The unique identifier for the user.

Applications dropdownMultiSelect required

Select the application(s) that can be used with this pairing key. Leave this list empty to allow all available native applications in the environment to be used.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - applicationIds null/array
 - array
 - null

Output Schema

- output object
 - rawResponse object
 - id string
 - code string
 - status string
 - error object
 - code string
 - message string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "id" : "b47a7af3-598c-4bc9-9ad7-43e6bf5d8cca",  
    "environment" :  
      { "id" : "9f1b3773-aae5-4903-b3a2-837c5b6f6467" },  
      "code" : "01552143316127",  
      "status" : "UNCLAIMED",  
      "applications" :  
        [  
          { "id" : "2a0d74e5-d856-44f5-ae21-7c3ec8d9ce37" } ],  
        "user" :  
          { "id" : "8dd4ed0f-391c-40d6-a1c9-ef0f6e3e8b40" },  
        "createdAt" : "2021-12-21T09:37:00.816Z",  
        "updatedAt" : "2021-12-21T09:37:00.816Z",  
        "expiresAt" : "2021-12-23T09:37:00.816Z" } }  
}
```

Delete Pairing Key

Delete unclaimed pairing keys.

Properties

User ID textField

The unique identifier for the user.

Pairing Key ID textField

The unique identifier for the pairing key.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - pairingKeyId string required minLength: 0 maxLength: 100
 - Pairing Key ID

Output Schema

- output object
 - rawResponse object
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { } }
```

Create Authentication Code

Create a single-use code to authenticate a user during sign-on using a mobile application. You can embed this code in a scannable QR code, or require that the user manually enter it to sign on.

Properties

Application dropDown

The unique identifier for the mobile application used to authenticate a user.

- Enter Application ID

Application ID textField required

Duration textField

The period of time that the authentication code is valid, which can be anywhere from 10 seconds to 30 minutes.

Time Unit dropDown required

The units of time used to indicate the authentication code duration.

- SECONDS (Default)
- MINUTES

User Approval dropDown

Specify whether the user will need to approve the authentication after they scan the authentication code using a mobile application.

- REQUIRED (Default)
- NOT_REQUIRED

Mobile Client Context variableInputList

Additional attributes that can be passed to the mobile application during the authentication.

Input Schema

- default object
 - properties object
 - authenticatingApplicationId string required minLength: 0 maxLength: 100
Application ID
 - customAuthenticatingApplicationId null/string/object
 - duration string required
Duration in seconds
 - timeUnit string
 - userApproval string required
 - clientContext array
Mobile Client Context

Output Schema

- output object
 - rawResponse object
 - id string
 - code string
 - uri string
 - status string
 - userApproval string
 - user object
 - id string
 - lifeTime object
 - duration integer
 - timeUnit string
 - clientContext object
 - _embedded object
 - device object
 - id string
 - os object
 - version string
 - type string
 - model object
 - name string
 - marketingName string
 - application object
 - nativeName string
 - version string
 - error object
 - code string
 - message string
 - createdAt string

- updatedAt string
- expiresAt string
- headers object
- statusCode integer
- authenticationCode object
 - id string
 - code string
 - uri string
 - status string
 - userApproval string
 - user object
 - id string
 - lifeTime object
 - duration integer
 - timeUnit string
 - clientContext object
 - _embedded object
 - device object
 - id string
 - os object
 - version string
 - type string
 - model object
 - name string
 - marketingName string
 - application object
 - nativeName string
 - version string
- error object
 - code string

- message string
- createdAt string
- updatedAt string
- expiresAt string

Output Example

```
{ "rawResponse" :
  { "id" : "b47a7af3-598c-4bc9-9ad7-43e6bf5d8cca",
    "environment" :
      { "id" : "9f1b3773-aae5-4903-b3a2-837c5b6f6467" },
    "code" : "HP2EG680",
    "uri" : "pingonesdk?authentication_code=HP2EG680",
    "applications" :
      [
        { "id" : "2a0d74e5-d856-44f5-ae21-7c3ec8d9ce37" } ],
    "lifeTime" :
      { "duration" : 10,
        "timeUnit" : "SECONDS" },
    "userApproval" : "NOT_REQUIRED",
    "status" : "UNCLAIMED",
    "clientContext" :
      { "var1" : "hello world",
        "var2" : 3 },
    "_embedded" :
      { "device" :
          { "id" : "dec6f008-b40e-45fd-a7ef-f255f77c5990",
            "os" :
              { "version" : "12",
                "type" : "ANDROID" },
            "model" :
              { "name" : "SM-G991B",
                "marketingName" : "SM-G991B" },
            "application" :
              { "nativeName" : "PingOneInternal",
                "version" : "1.7.0" } } },
          "user" :
            { "id" : "bec1b927-d1fb-494f-9bb5-bbe4f625f7bb" },
            "createdAt" : "2021-12-21T09:37:00.816Z",
            "updatedAt" : "2021-12-21T09:37:00.816Z",
            "expiresAt" : "2021-12-23T09:37:00.816Z" } }
```

Read Authentication Code

Read the authentication code.

Properties

Authentication Code ID textField

The unique identifier for the authentication code.

Input Schema

- default object
 - properties object
 - authenticationCodeId string required minLength: 0 maxLength: 100
- Authentication Code ID

Output Schema

- output object
 - rawResponse object
 - id string
 - code string
 - uri string
 - status string
 - userApproval string
 - user object
 - id string
 - lifeTime object
 - duration integer
 - timeUnit string
 - clientContext object
 - _embedded object
 - device object
 - id string
 - os object
 - version string
 - type string
 - model object
 - name string
 - marketingName string
 - application object
 - nativeName string
 - version string
 - error object
 - code string
 - message string
 - createdAt string

- updatedAt string
- expiresAt string
- headers object
- statusCode integer
- authenticationCode object
 - id string
 - code string
 - uri string
 - status string
 - userApproval string
 - user object
 - id string
 - lifeTime object
 - duration integer
 - timeUnit string
 - clientContext object
 - _embedded object
 - device object
 - id string
 - os object
 - version string
 - type string
 - model object
 - name string
 - marketingName string
 - application object
 - nativeName string
 - version string
- error object
 - code string

- message string
- createdAt string
- updatedAt string
- expiresAt string

Output Example

```
{ "rawResponse" :
  { "id" : "b47a7af3-598c-4bc9-9ad7-43e6bf5d8cca",
    "environment" :
      { "id" : "9f1b3773-aae5-4903-b3a2-837c5b6f6467" },
    "code" : "HP2EG680",
    "uri" : "pingonesdk?authentication_code=HP2EG680",
    "applications" :
      [
        { "id" : "2a0d74e5-d856-44f5-ae21-7c3ec8d9ce37" } ],
    "lifeTime" :
      { "duration" : 10,
        "timeUnit" : "SECONDS" },
    "userApproval" : "NOT_REQUIRED",
    "status" : "UNCLAIMED",
    "clientContext" :
      { "var1" : "hello world",
        "var2" : 3 },
    "_embedded" :
      { "device" :
          { "id" : "dec6f008-b40e-45fd-a7ef-f255f77c5990",
            "os" :
              { "version" : "12",
                "type" : "ANDROID" },
            "model" :
              { "name" : "SM-G991B",
                "marketingName" : "SM-G991B" },
            "application" :
              { "nativeName" : "PingOneInternal",
                "version" : "1.7.0" } } },
          "user" :
            { "id" : "bec1b927-d1fb-494f-9bb5-bbe4f625f7bb" },
            "createdAt" : "2021-12-21T09:37:00.816Z",
            "updatedAt" : "2021-12-21T09:37:00.816Z",
            "expiresAt" : "2021-12-23T09:37:00.816Z" } }
```

Set Device Order

Setting the device order explicitly orders a user's existing active devices

Properties

User ID textField

The unique identifier for the user.

Set Device Order dropDown

Select how to set the device order

- Set default device
- Set device order

Device ID textField

Enter the device ID of the device which should be set as the default device.

Input attributes as JSON? toggleSwitch

Set Device Order multipleTextFields

Enter the device IDs in the order that the devices should be listed for the user.

Attributes codeEditor

An array of objects that determines the explicit order of a user's devices. The first device listed becomes the default device. This property is used as a body parameter to set the order of existing devices.

Default:

```
{
  "order": [
    {
      "id": "{{deviceID}}"
    },
    {
      "id": "{{deviceID2}}"
    }
  ]
}
```

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `setDeviceOrder` string
 - `defaultDeviceId` string minLength: 0 maxLength: 100
 - `useDeviceOrderJsonAttributes` boolean
 - `deviceOrderList` array
 - `jsonAttributes` null/string/object

Output Schema

- output object
 - rawResponse object
 - _embedded object
 - devices array
 - applications array
 - allowedtypes array
 - order array
 - id string
 - mfaSettings object
 - environment object
 - id string
 - pairing object
 - maxAllowedDevices integer
 - mfaPolicy object
 - authentication object
 - deviceSelection string
 - size number
 - headers object
 - statusCode integer
 - devices array
 - order array
 - id string

Output Example

```

{ "rawResponse" :
  { "_embedded" :
    { "devices" :
      [
        { "device" :
          { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
            "type" : "SMS",
            "status" : "ACTIVE",
            "nickname" : "Work Device",
            "phone" : "+972528888888",
            "extension" : "###1",
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],
        "applications" :
          [
            { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
              "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
              "name" : "IOS nativeApp",
              "enabled" : true,
              "mobile" :
                { "bundleId" : "com.pingIdentity.p14c.sample",
                  "integrityDetection" :
                    { "mode" : "DISABLED" } } } ],
            "allowedtypes" :
              [ "SMS",
                "VOICE",
                "MOBILE",
                "TOTP",
                "OATH_TOKEN",
                "YUBIKEY",
                "PINGID_DESKTOP",
                "PLATFORM",
                "SECURITY_KEY" ],
            "order" :
              [
                { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

                { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
            "mfaSettings" :
              { "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
                "pairing" :
                  { "maxAllowedDevices" : 5 } },
            "mfaPolicy" :
              { "authentication" :
                { "deviceSelection" : "DEFAULT_TO_FIRST" } } },
            "count" : 1,
            "size" : 1 },
        "devices" :
          [
            { "device" :
              { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
                "type" : "SMS",
                "status" : "ACTIVE",
                "nickname" : "Work Device",
                "phone" : "+972528888888",
                "extension" : "###1",
                "createdAt" : "2021-01-15T20:45:17.463Z",
                "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],

```



```

"applications" :
[
  { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
    { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
    "name" : "IOS nativeApp",
    "enabled" : true,
    "mobile" :
    { "bundleId" : "com.pingIdentity.p14c.sample",
      "integrityDetection" :
      { "mode" : "DISABLED" } } } ],
"allowedtypes" :
[ "SMS",
  "VOICE",
  "MOBILE",
  "TOTP",
  "OATH_TOKEN",
  "YUBIKEY",
  "PINGID_DESKTOP",
  "PLATFORM",
  "SECURITY_KEY" ],
"order" :
[
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

  { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
"mfaSettings" :
{ "environment" :
  { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
  "pairing" :
  { "maxAllowedDevices" : 5 } },
"mfaPolicy" :
{ "authentication" :
  { "deviceSelection" : "DEFAULT_TO_FIRST" } } }

```

Cancel Device Authentication

Cancel the authentication process for a specific device.

Properties

Device Authentication ID textField

The unique identifier for the MFA Device Authentication.

Reason For Cancellation\n textField

The reason that the authentication was canceled.

Possible values are SIGNOUT, CHANGE_DEVICE, ADD_DEVICE. Any other reason will get the value - DEFAULT.

Input Schema

- default object
 - properties object
 - reason string
Reason
 - deviceAuthenticationId string required minLength: 0 maxLength: 100
Device Authentication ID

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                [
                  { "type" : "EMAIL",
                    "email" : "o*****@pingidentity.com" } ] } } } }
```

Create Device

Create devices to use during authentication.

Properties

User ID textField

The unique identifier for the user.

Device Type textField

The type of device used during authentication. Supported values are: SMS, EMAIL, VOICE, TOTP, YUBIKEY, OATH_TOKEN, PLATFORM, SECURITY_KEY, FIDO2.

Activation Status dropDown

The current status of the device. If a device has an ACTIVATION_REQUIRED status, activate it before you add it as a trusted device.

- ACTIVE
- ACTIVATION REQUIRED

Phone Number textField

The phone number to associate with the device. Applies only to devices that use SMS and Voice SMS messages during authentication.

Email textField

The email address to associate with the device. Applies only to devices that use email during authentication.

Device Nickname textField

A nickname that identifies this device. The device nickname is limited to 100 characters.

Relying Party ID textField

If you define a Relying Party ID (RPID) here, it overrides the RPID defined in the FIDO policy in the PingOne admin console.

Relying Party Name textField

A string that specifies the relying party's human-readable display name.

YubiKey textField

The one-time passcode used to authenticate the YubiKey.

Serial Number textField

The unique identifier for the OAuth token.

User Agent textField

Browser user agent

Custom FIDO2 Challenge textField

Applicable for FIDO2 pairing requests. Specify a custom challenge that will replace the automatically generated challenge sent with the pairing request. Must be a valid Base64URL string that decodes to at least 32 bytes of data array.

MFA Policy ID textField

The ID of the PingID policy evaluation.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `workforceDeviceType` string required
 - `status` string required
 - `nickname` string
 - `phone` string
 - `email` string
 - `rpId` string
Relying Party ID
 - `rpName` string
Relying Party Name
 - `userAgent` string
User Agent
 - `challenge` string
Custom FIDO2 Challenge
 - `workforcePolicyMfaPolicyId` string minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - test object
 - otp string
 - headers object
 - statusCode integer

- device object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```

Create Device Authentication

Create authentication experiences with virtual or physical devices.

Properties

User ID Not Required toggleSwitch

Indicates whether the user id is required or obtained from the authentication method used.

User ID textField

The unique identifier for the user.

MFA Policy ID textField

The ID of the PingID policy evaluation.

User Agent textField

Browser user agent

Device Details dropDown

Indicates whether to use the user's default authentication method or to provide a specific authentication method.

- ID
- One-Time Device

Device ID textField

The selected device id

Device Type textField

The one-time device type

SMS Phone Number textField

The phone number to associate with the one-time SMS device.

Voice Phone Number textField

The phone number to associate with the one-time Voice device.

Email textField

The email address to associate with the one-time device.

Relying Party ID textField

If you define a Relying Party ID (RPID) here, it overrides the RPID defined in the FIDO policy in the PingOne admin console.

WebAuthn Browser Compatibility textField***Custom FIDO2 Challenge textField***

Applicable for FIDO2 authentication requests. Specify a custom challenge that will replace the automatically generated challenge sent with the authentication request. Must be a valid Base64URL string that decodes to at least 32 bytes of data array.

FIDO Compatibility textField

A string that specifies the FIDO Authenticators that are allowed to be used. Options are FULL (compatible with FIDO2, platform biometrics, and security key) and NONE (not compatible with FIDO).

One-time Passcode textField

The one-time passcode (OTP) of the device used to authenticate. If the Device ID is not provided, the OTP is validated against all the applicable devices.

IP textField

The IP address of the user who initiated the flow.

Application Name textField

The name of the application being authenticated.

Input Schema

- default object
 - properties object
 - `userId` string minLength: 0 maxLength: 100
 - `workforcePolicyMfaPolicyId` string minLength: 0 maxLength: 100
 - `userAgent` string
 - User Agent
 - `rpId` string
 - Relying Party ID
 - `deviceAuthenRpId` string
 - Relying Party ID
 - `createDeviceTestMode` string
 - Create Test Device
 - `oneTimeDeviceTestMode` string
 - Create Test Device
 - `usernameLess` boolean
 - User ID Not Required
 - `selectedDevice` null/string
 - string
 - `id`
 - `oneTime`
 - null
 - `selectedDeviceId` null/string
 - `oneTimeDeviceType` null/string
 - string
 - SMS
 - VOICE
 - EMAIL
 - null
 - `oneTimeSmsDevice` null/string

- oneTimeVoiceDevice null/string
- oneTimeEmailDevice null/string
- challenge string
 - Custom FIDO2 Challenge
- fidoCompatibility null/string
 - WebAuthn Compatibility
- compatibility null/string
 - WebAuthn Compatibility
- otp string
 - Passcode
- ip string
 - IP
- applicationName string minLength: 0 maxLength: 100
 - The name of the application being authenticated

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - test object
 - otp string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                [
                  { "type" : "EMAIL",
                    "email" : "o*****@pingidentity.com" } ] } } } }
```

Create Pairing Key

Create pairing keys that can be used by the PingID mobile app to create trust with PingID.

Properties

User ID textField

The unique identifier for the user.

Applications dropdownMultiSelect required

Select the application(s) that can be used with this pairing key. Leave this list empty to allow all available native applications in the environment to be used.

MFA Policy ID textField

The ID of the PingID policy evaluation.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `applicationIds` null/array
 - array
 - null
 - `workforcePolicyMfaPolicyId` string minLength: 0 maxLength: 100

Output Schema

- output object
 - rawResponse object
 - id string
 - code string
 - status string
 - error object
 - code string
 - message string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "b47a7af3-598c-4bc9-9ad7-43e6bf5d8cca",
    "environment" :
      { "id" : "9f1b3773-aae5-4903-b3a2-837c5b6f6467" },
    "code" : "01552143316127",
    "status" : "UNCLAIMED",
    "applications" :
      [
        { "id" : "2a0d74e5-d856-44f5-ae21-7c3ec8d9ce37" } ],
    "user" :
      { "id" : "8dd4ed0f-391c-40d6-a1c9-ef0f6e3e8b40" },
    "createdAt" : "2021-12-21T09:37:00.816Z",
    "updatedAt" : "2021-12-21T09:37:00.816Z",
    "expiresAt" : "2021-12-23T09:37:00.816Z" } }
```

Read All Devices

Read information for all user devices

Properties

User ID textField

The unique identifier for the user.

Filters toggleSwitch

Filter devices by activation status and device type.

Status dropDown

non-active devices are not usable during an authentication.

- ALL (Default)
- ACTIVE
- ACTIVATION REQUIRED

Device Types dropDownMultiSelect

- Email
- SMS
- Voice
- Authenticator App
- Fido2 Biometrics
- Security Key
- Oath token
- YubiKey
- Desktop app
- PingID Mobile app

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `setFilterFlag` boolean
 - `statusFilter` string
 - `workforceDeviceTypes` array uniqueItems: true

Output Schema

- output object
 - rawResponse object
 - _embedded object
 - devices array
 - applications array
 - allowedtypes array
 - order array
 - id string
 - mfaSettings object
 - environment object
 - id string
 - pairing object
 - maxAllowedDevices integer
 - mfaPolicy object
 - authentication object
 - deviceSelection string
 - size number
 - headers object
 - statusCode integer
 - devices array
 - allowedtypes array
 - applications array
 - mfaSettings object
 - environment object
 - id string
 - pairing object
 - maxAllowedDevices integer

- mfaPolicy object
 - authentication object
 - deviceSelection string
- order array
 - id string

Output Example

```

{ "rawResponse" :
  { "_embedded" :
    { "devices" :
      [
        { "device" :
          { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
            "type" : "SMS",
            "status" : "ACTIVE",
            "nickname" : "Work Device",
            "phone" : "+972528888888",
            "extension" : "###1",
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],
        "applications" :
          [
            { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
              "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
              "name" : "IOS nativeApp",
              "enabled" : true,
              "mobile" :
                { "bundleId" : "com.pingIdentity.p14c.sample",
                  "integrityDetection" :
                    { "mode" : "DISABLED" } } } ],
            "allowedtypes" :
              [ "SMS",
                "VOICE",
                "MOBILE",
                "TOTP",
                "OATH_TOKEN",
                "YUBIKEY",
                "PINGID_DESKTOP",
                "PLATFORM",
                "SECURITY_KEY" ],
            "order" :
              [
                { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

                { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
            "mfaSettings" :
              { "environment" :
                { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
                "pairing" :
                  { "maxAllowedDevices" : 5 } },
            "mfaPolicy" :
              { "authentication" :
                { "deviceSelection" : "DEFAULT_TO_FIRST" } } },
            "count" : 1,
            "size" : 1 },
        "devices" :
          [
            { "device" :
              { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
                "type" : "SMS",
                "status" : "ACTIVE",
                "nickname" : "Work Device",
                "phone" : "+972528888888",
                "extension" : "###1",
                "createdAt" : "2021-01-15T20:45:17.463Z",
                "updatedAt" : "2021-01-15T20:45:17.463Z" } } ],

```

```

"applications" :
[
  { "id" : "43eb4421-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
    "name" : "iOS nativeApp",
    "enabled" : true,
    "mobile" :
      { "bundleId" : "com.pingIdentity.p14c.sample",
        "integrityDetection" :
          { "mode" : "DISABLED" } } } ],
"allowedtypes" :
[ "SMS",
  "VOICE",
  "MOBILE",
  "TOTP",
  "OATH_TOKEN",
  "YUBIKEY",
  "PINGID_DESKTOP",
  "PLATFORM",
  "SECURITY_KEY" ],
"order" :
[
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb" },

  { "id" : "01f3db05-93b6-4c45-a93e-f9ac84d076c6" } ],
"mfaSettings" :
{ "environment" :
  { "id" : "143459b9-107b-48ae-8c0a-e65f94054ebb" },
  "pairing" :
    { "maxAllowedDevices" : 5 } },
"mfaPolicy" :
{ "authentication" :
  { "deviceSelection" : "DEFAULT_TO_FIRST" } } }

```

Evaluate Policy

Evaluate PingID policy

Properties

User ID textField

The unique identifier for the user.

IP textField

The IP of the requesting device.

User Agent textField

The requesting device's user agent.

Application Id textField

The ID of the application being authenticated.

Application Name textField

The name of the application being authenticated.

Risk Level textField

The Risk Level score that is received from the Risk management service.

User Groups textField

The groups that the user is part of.

Last MFA transaction dropDown

Details of the last Multi-factor authentication (MFA) transaction.

- PingOne Cookie
- Custom

Last sign-on details textField

Enter the last sign-on section from the PingOne Cookie.

Last transaction IP textField

The IP address of the most recent transaction.

Last transaction authentication method textField

The authentication method used for the most recent transaction.

Last transaction time textField

The time at which the most recent transaction occurred.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - ip string
 - riskLevel string
 - applicationName string
 - applicationId string
 - userAgent string
 - groups array
 - lastMFATransaction null/string
 - string
 - pingoneCookieLastTransaction
 - customLastTransaction
 - null
 - policyRecentPingOneCookie string
 - policyRecentAuthMethod string
 - policyRecentIp string
 - policyRecentAuthTimestamp string

Output Schema

- output object
 - rawResponse object
 - action string
 - id string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "action" : "AUTHENTICATE",  
    "id" : "1a14fe10-56c9-449e-9609-bfe1d6984ffd" } } }
```

Create Remembered Device

Create a known accessing device

Properties

User ID textField

The unique identifier for the user.

MFA Policy ID textField

The ID of your PingOne MFA device authentication policy.

Session ID textField

The active PingOne session for the user.

Device Type dropDown

- Browser

Payload textField

Identify the device via a unique device ID combined with a digital signature that ensures information collected about the device has not been tampered with.

Check Last Authentication Method textField

Check if the last authentication method used to remember the accessing device matches an allowed authentication method in the current MFA policy being used.

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
 - mfaPolicyId string required minLength: 0 maxLength: 100
 - rememberMeDeviceType string required
 - rememberMePayload string required
 - rememberMeCookie string

Output Schema

- output object
 - rawResponse object
 - id string
 - type string
 - status string
 - nickname string
 - phone string
 - extension string
 - email string
 - secret string
 - keyUri string
 - oathToken string
 - serialNumber string
 - rp object
 - id string
 - name string
 - platform string
 - publicKeyCredentialCreationOptions string
 - attributes object
 - previousDeviceType string
 - isCrossPlatform boolean
 - displayName string
 - createdAt string
 - updatedAt string
 - headers object
 - set-cookie string
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "device" :  
    { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",  
      "type" : "SMS",  
      "status" : "ACTIVE",  
      "nickname" : "Work Device",  
      "phone" : "+972528888888",  
      "extension" : "###1",  
      "createdAt" : "2021-01-15T20:45:17.463Z",  
      "updatedAt" : "2021-01-15T20:45:17.463Z" } } }
```

Check Remember Me State

Check if the accessing device is known

Properties

User ID textField

The unique identifier for the user.

MFA Policy ID textField

The ID of your PingOne MFA device authentication policy.

Session ID textField

The active PingOne session for the user.

Device Type dropDown

- Browser

Payload textField

Identify the device via a unique device ID combined with a digital signature that ensures information collected about the device has not been tampered with.

Cookie textField

The cookie that was generated when the remembered device was created.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
 - `mfaPolicyId` string required minLength: 0 maxLength: 100
 - `rememberMeDeviceType` string required
 - `rememberMePayload` string required
 - `rememberMeCookie` string required

Output Schema

- output object
 - rawResponse object
 - id string
 - user object
 - id string
 - environment object
 - id string
 - policy object
 - id string
 - selectedDevice object
 - id string
 - application object
 - id string
 - status string
 - authenticators array
 - publicKeyCredentialRequestOptions string
 - _links object
 - _embedded object
 - devices array
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "43eb5621-eae8-4fa1-aafb-2a884d6848cb",
    "environment" :
      { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
      "user" :
        { "id" : "c362abbc-eeeb-4ea5-b9c1-097a376b0086" },
        "status" : "OTP_REQUIRED",
        "selectedDevice" :
          { "id" : "9362abac-eeeb-6ea5-b9cc-097a375b0043" },
          "policy" :
            { "id" : "6122abac-eeeb-6ea5-b9cc-097a375b0043" },
            "createdAt" : "2021-01-15T20:45:17.463Z",
            "updatedAt" : "2021-01-15T20:45:17.463Z",
            "_embedded" :
              { "devices" :
                  [
                    { "type" : "EMAIL",
                      "email" : "o*****@pingidentity.com" } ] } } } }
```

PingOne MFA Connector Release Notes

New features and improvements in the PingOne MFA Connector.

May 2025

Remembered devices

Improved

The connector now supports the "remember me" functionality that was added to MFA in [February 2025](#).

July 2023

Ability to override MFA policy

Improved

We've enhanced the Policy ID field to the Create Device Authentication Capability that enables you to override the MFA policy that is configured in the MFA connector settings.

April 2023

PingOne MFA Connector

Improved

We've enhanced the PingOne MFA Connector to enable the user to enter their One-time Passcode (OTP) when triggering Multi-factor Authentication (MFA). It's now possible for the user to enter a TOTP/HOTP-generated OTP when starting authentication using the Create Device Authentication endpoint.

PingOne Notifications Connector

The PingOne Notifications connector enables you to send custom voice, SMS, and email notifications to cover a wide range of use cases for your customers.

You can create a custom **General** notifications template in PingOne and reference it in the Notifications connector. For help, see [Notification templates](#).

Note

To add notifications for multi-factor authentication (MFA) use cases, such as push notifications for pairing and authentication within an MFA flow, use the [PingOne MFA connector](#).

Setup

Resources

For information and setup help, see the following:

- PingOne documentation:
 - [Introduction to PingOne](#)
 - [Getting started with PingOne](#)
 - [Notification templates](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the PingOne Notifications connector, you must configure a PingOne environment and create the relevant users.

Setting up the connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Environment ID

Your PingOne Environment ID. In PingOne, go to **Settings → Environment Properties**.

Notification Policy ID

(Optional) The unique identifier of the PingOne notification policy. You can define a notification policy and reference it as part of the connector setup. For more information, see [Notification policies](#).

If a Notification Policy ID is not specified, the default policy is used. In PingOne, go to **User Experience → Notification Policies** and in the **Notification Policies** list, select the **Policy ID** for the policy you want to use.

Client ID

The Client ID of your PingOne Worker application. In PingOne, go to **Applications → Applications → (Your Application) → Configuration**. Expand the **General** section.

Client Secret

The Client Secret of your PingOne Worker application. In PingOne, go to **Applications → Applications → (Your Application) → Configuration**. Expand the **General** section and then click the button to reveal the client secret.

Region

Your PingOne environment region. In PingOne, see **Settings → Environment Properties**.

Using the connector in a flow

You can use the PingOne Notifications connector to add custom voice, SMS, or email notifications in a flow. The PingOne Notifications connector uses the configurations defined in PingOne, including any customer sender configurations, if defined. You can also specify a PingOne notification policy to apply to the connector.

The PingOne Notifications connector is usually added to an existing flow at the point that you want a notification to be sent.

Capabilities

Send Email

Send users customized email messages.

Properties

User ID textField required

The unique identifier for the user.

Email textField required

The email address to which notifications are sent.

Notification Name dropDown

The name of a custom notification defined in PingOne. If the form you want is not listed, select Enter Custom Value.

- Enter Custom Value

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Notification Variables variableInputList

If custom variables are defined in the notification body, map them here.

Wait For Vendor Response toggleSwitch

Indicates whether the connector should wait for the notification vendor to respond to the message request.

Input Schema

- default object
 - properties object
 - `userId` string minLength: 0 maxLength: 100
 - `templateVariant` null/string
 - `customTemplateVariant` null/string/object
 - `templateLocale` null/string
 - `templateVariables` array
 - `email` string
 - `sendSync` boolean
 - Send synchronize notification

Output Schema

- output object
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - policy object
 - id string
 - deliveryMethod string
 - from string
 - subject string
 - body string
 - address string
 - updatedAt string
 - createdAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :
  { "id" : "00584480-5795-448f-8ade-fcc792c7dbbe",
    "environment" :
      { "id" : "602cc283-b258-444e-acd0-5553330a206c" },
    "user" :
      { "id" : "1528312c-ccff-48ff-be64-3c56d0110aba" },
    "policy" :
      { "id" : "6f5377b1-df6f-4999-9a24-70a7cb534e8e" },
    "deliveryMethod" : "Email",
    "from" : "\"PingOne\" <noreply@pingidentity.com>",
    "subject" : "Custom email notification",
    "body" : "Hi John, Enter your custom message here",
    "address" : "galdalal@pingidentity.com",
    "updatedAt" : "2022-08-01T14:21:50.010Z",
    "createdAt" : "2022-08-01T14:21:49.560Z" } }
```

Send SMS

Send users customized SMS messages.

Properties

User ID textField required

The unique identifier for the user.

Phone Number textField required

The phone number to which notifications are sent.

Notification Name dropDown

The name of a custom notification defined in PingOne. If the form you want is not listed, select Enter Custom Value.

- Enter Custom Value

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Notification Variables variableInputList

If custom variables are defined in the notification body, map them here.

Wait For Vendor Response toggleSwitch

Indicates whether the connector should wait for the notification vendor to respond to the message request.

Input Schema

- default object
 - properties object
 - `userId` string minLength: 0 maxLength: 100
 - `templateVariant` null/string
 - `customTemplateVariant` null/string/object
 - `templateLocale` null/string
 - `templateVariables` array
 - `phone` string
 - `sendSync` boolean
 - Send synchronize notification

Output Schema

- output object
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - policy object
 - id string
 - deliveryMethod string
 - content string
 - phone string
 - sender string
 - updatedAt string
 - createdAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "id" : "001b1fc7-a41f-4018-a70e-1c3f7b97a970",  
    "environment" :  
      { "id" : "602cc283-b258-444e-acd0-5553330a206c" },  
    "user" :  
      { "id" : "1528312c-ccff-48ff-be64-3c56d0110aba" },  
    "policy" :  
      { "id" : "6f5377b1-df6f-4999-9a24-70a7cb534e8e" },  
    "deliveryMethod" : "SMS",  
    "content" : "Enter your custom message here",  
    "phone" : "+972547639689",  
    "sender" : "+19895464225",  
    "updatedAt" : "2022-08-01T14:21:50.010Z",  
    "createdAt" : "2022-08-01T14:21:49.560Z" } }
```

Send Voice Message

Send users customized voice messages..

Properties

User ID textField required

The unique identifier for the user.

Phone Number textField required

The phone number to which notifications are sent.

Notification Name dropDown

The name of a custom notification defined in PingOne. If the form you want is not listed, select Enter Custom Value.

- Enter Custom Value

Custom Value textField

You can enter a custom template name, or leave blank to use the default template. You can also enter a parameter from a previous connector, or any text.

Notification Locale textField

Add a locale to allow localized notifications for end-users. ISO Language Codes are supported.

Notification Variables variableInputList

If custom variables are defined in the notification body, map them here.

Wait For Vendor Response toggleSwitch

Indicates whether the connector should wait for the notification vendor to respond to the message request.

Input Schema

- default object
 - properties object
 - `userId` string minLength: 0 maxLength: 100
 - `templateVariant` null/string
 - `customTemplateVariant` null/string/object
 - `templateLocale` null/string
 - `templateVariables` array
 - `phone` string
 - `sendSync` boolean
 - Send synchronize notification

Output Schema

- output object
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - policy object
 - id string
 - deliveryMethod string
 - content string
 - phone string
 - sender string
 - updatedAt string
 - createdAt string
 - headers object
 - statusCode integer

Output Example

```
{ "rawResponse" :  
  { "id" : "002855e3-f505-4142-91b4-bcc252c5efcb",  
    "environment" :  
      { "id" : "602cc283-b258-444e-acd0-5553330a206c" },  
    "user" :  
      { "id" : "1528312c-ccff-48ff-be64-3c56d0110aba" },  
    "policy" :  
      { "id" : "6f5377b1-df6f-4999-9a24-70a7cb534e8e" },  
    "deliveryMethod" : "Voice",  
    "content" : "Enter your custom message here",  
    "phone" : "+972547639689",  
    "sender" : "+12106102319",  
    "updatedAt" : "2022-08-01T14:21:50.010Z",  
    "createdAt" : "2022-08-01T14:21:49.560Z" } }
```

PingOne Protect Connector

This connector lets you use PingOne Protect in a PingOne DaVinci flow to improve the user experience, reduce multi-factor authentication (MFA) fatigue, lower the probability of unintentional push approvals, and issue challenges or deny access in high-risk situations.

PingOne Protect is a cloud-based service that applies machine learning and configurable, intelligent security policies to analyze user identity and detect potential threats. PingOne Protect combines multiple risk factors to calculate an overall risk score.

When you add a PingOne Protect connector in a flow, you can define different paths based on the recommended action (when available), the risk level, or the risk score calculated by PingOne Protect in a risk evaluation. For example:

- Skip the MFA challenge for low risk.
- Use a specific authentication method if user behavior data suggests medium or high risk.
- Block access completely for high risk, such as when the recommended action is bot mitigation or if impossible user travel is detected.

Learn more in the [PingOne Protect documentation](#).

Setup

Resources

Learn more in the following documentation:

- PingOne Protect documentation:
 - [Introduction to PingOne Protect](#)
 - [Getting started with PingOne Protect](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne Protect license
- A PingOne environment with PingOne Protect added. Learn more in [Adding an environment](#).
- A worker application configured in your PingOne environment. Learn more in [Adding an application](#).
- A PingOne Protect risk policy. You can use the default risk policy or create a custom risk policy. Learn more in [Risk policies](#).

Setting up the connector

1. Follow the instructions in [Getting started with PingOne Protect](#).
2. In DaVinci, add a [PingOne Protect connector](#).

Connector configuration

Environment ID

The **Environment ID** from the **Environment Properties** page of the relevant environment in PingOne.

Client ID

The **Client ID** of the worker application you created in PingOne.

Client Secret

The **Client Secret** from the **Configuration** tab of your PingOne worker application.

Using the connector in a flow

Use the PingOne Protect connector to add risk evaluations to different types of flows, such as sign-on with MFA or passwordless sign-on. You can use the PingOne Protect connector in template flows available in the [Integration Directory](#), such as:

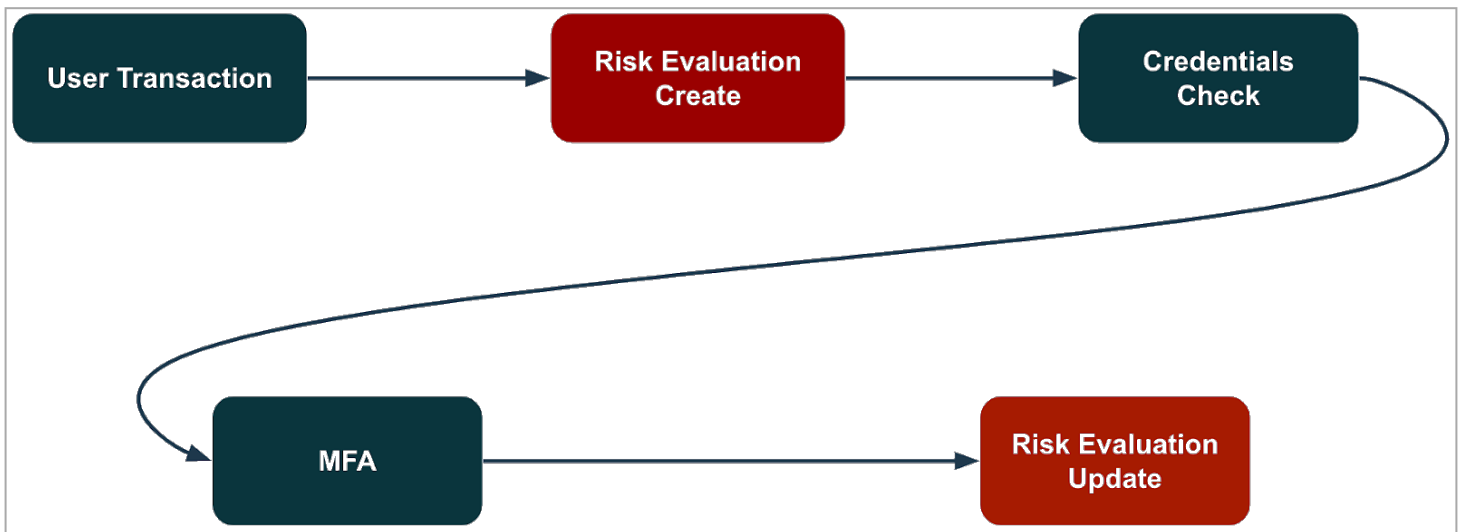
- [PingOne Adaptive Authentication with MFA via OTP or FIDO](#)
- [PingOne for Customers Passwordless](#)
- [Authentication Journey with Threat Detection](#)

Learn more about risk evaluations and how the response result affects the user flow in [Reviewing risk evaluations](#).

The PingOne Protect connector provides these capabilities:

- **Create Risk Evaluation:** Add in the flow where you want to base the next action on the risk score or level calculated. For example, show an MFA prompt for medium or high risk but automatically grant access for low risk.
- **Update Risk Evaluation:** Add in the flow after authentication has been completed. This capability represents the system's ability to learn over time to improve results and is essential for risk evaluation precision.

The following diagram shows an example user transaction flow with the two different PingOne Protect connector capabilities:



Create Risk Evaluation

Evaluate risk for a specific transaction based on predictors, such as user location anomaly, IP reputation, and bot detection. Learn more in [Predictors](#).

Steps

1. In your flow, add a **PingOne Protect connector** and select the **Create Risk Evaluation** capability.
2. On the **General** tab, enter the following information:
 - **User Name**
 - **User ID**
 - **IP**
 - **Risk Policy ID** (optional): If you've created custom risk policies beyond the default risk policy, you can enter the ID of the risk policy you want to use in the flow.

You can find the ID for a risk policy on the **Risk Policies** page in your environment in PingOne. If you don't provide a risk policy ID, the connector uses the default risk policy.

- **Custom Attributes** (optional): If you're using a policy that includes one or more custom predictors that require external data, use the **Custom Attributes** field to enter the names of the custom attributes and their values.

For example:

```
{"managedDevice" : isManaged, "transactionValue" : transactionValueVar}
```

The attribute names must match the attribute names you used in the custom predictors that you created and included in the risk policy. Learn more in [Adding custom predictors](#) and [Using third-party risk scores with PingOne Protect](#).

Custom Attributes ⓘ

```
{ "managedDevice": isManaged ,  
  "transactionValue": transactionValueVar }
```

3. Click **Apply**.
4. To improve risk analysis, include the data for additional risk-related variables provided by the Signals (Protect) SDK.

Note

Risk evaluation can be performed without the Signals (Protect) SDK payload if there's no way to provide the payload. However, some predictors require the SDK payload and won't return a risk level if the payload is missing. Learn more in [Predictors](#).

Manual deployment

You can manually deploy the Signals (Protect) SDK when integrating using the DaVinci APIs. For mobile applications or integrating your webpage with DaVinci using APIs instead of redirecting, you'll:

- Deploy the Signals (Protect) SDK.
- Send the SDK payload and the rest of the required data, such as username, user ID, IP address, and any custom attributes to DaVinci using the API.
- Include a variable in your flow that represents the data obtained.

To manually deploy the SDK:

1. Follow the [PingOne Protect Native SDKs](#) documentation to implement the SDK in your mobile app or webpage.
2. Set global variables using the SDK to pass risk-related information from the SDK and map the information into the risk evaluation in DaVinci.
3. In DaVinci, click the applicable PingOne Protect connector with the **Create Risk Evaluation** capability in your flow to open its settings.

1. On the **Device Configurations** tab, for **Risk input from device**, enter the name of the variable that represents the data obtained from the SDK in your manual implementation.
2. In the **User Agent** field, enter the user agent string for the browser, if available.



Note

User Agent is included in the SDK payload by default.

3. To improve risk analysis, use the **Cookie** field to provide the value of a persistent cookie, if available.
4. If you want to maintain your own device IDs, you can assign external device IDs that are not managed by the SDK, such as device serial number or mobile application installation ID. External IDs can be sent to DaVinci using the API.

For example, in a workforce user flow, you can use the [Google Chrome Device Trust connector](#) to map the user device serial number when using the Chrome browser.

5. To pass the risk information from the SDK to DaVinci, map the global variables that you set with the SDK into DaVinci:

1. On the **Log Fields Mapping** tab, click **+ Field**.
2. Select and enter the global variables you set with the SDK.

skrisk component

You can include the **skrisk** component in your flow to collect device and user behavioral data from user interactions with custom HTML templates in [HTTP connectors](#), such as an HTTP sign-on or password reset flow. Learn more about **skrisk** in [SK-Components](#).

With this approach, the information from the Signals Web SDK is obtained automatically. However, for the Signals Mobile SDK, you must implement the steps in the [SDK documentation](#) manually.

The **skrisk** component must be added to the following:

- The first HTTP connector with a **Custom HTML Template** in your flow that requires user interaction.
- Any subsequent HTTP connectors with a **Custom HTML Template** in the flow, including subflows called by a parent flow.

For example, you can create a subflow that performs the risk evaluation within a parent flow. In this case, add the **skrisk** component to relevant HTTP connectors in the parent flow that call this subflow.

You can find subflow templates in the [Integration Directory](#), such as [Login with Self-Service Journey](#), [PingOne Sign On and Password Reset](#), and [User Registration Journey](#). Learn more in [Using DaVinci flow templates](#).

Adding the **skrisk** component to multiple connectors in a flow allows the SDK to collect additional data throughout the flow and improves bot detection.

1. Add an **HTTP connector** with the **Custom HTML Template** capability to your flow.
2. On the **General** tab, in the **HTML Template** field, click **{}**, click **SK-Component**, and then select **skrisk** in the list.



Important

The **skrisk** component should always be at the beginning of the HTML template. Make sure that all HTML tags you add appear below the **skrisk** component in the **HTML Template** field.

3. Double-click the **skrisk** component that you added to open its properties.
4. Enter the **Environment ID** for your PingOne environment.
5. The **Collect behavior data** setting collects device and user behavioral data. By default, **Collect behavioral data** is set to **True**.
Set **Collect behavior data** to **False** if this connector doesn't require interaction from the user.
6. (Optional) Change the default **Risk Property Name** as needed.
7. If you want the device data in the SDK payload to be provided as a signed JSON Web Token (JWT), set **Enable Universal Device Identification** to **True**.
8. Click **Save**.

9. On the **General** tab of the HTTP connector, scroll down to the **Output Fields List** and add a field to represent the output provided by the `skrisk` component.

1. For **Property Name**, enter the same name that you used for **Risk Property Name**. In the PingOne Protect connector, you'll select this property name as one of the inputs.

2. Add a **Display Name**.

3. Click **Apply**.

10. Click the **PingOne Protect** connector with the **Create Risk Evaluation** capability in your flow.

11. On the **Device Configurations** tab, configure **Risk input from device** as follows:

1. Click `{}`.

2. Click to enable the **Show all nodes** toggle.

3. Select the **HTTP connector** in the list.

4. Under **output**, select the name that you provided previously for the output of the `skrisk` component.

In the following image, `<output>` represents the output from step 9.

PingOne Protect

id:
connectionId:

< ACTION:

Create Risk Evaluation

GENERAL **DEVICE CONFIGURATIONS** **>**

*** indicates required**

Risk input from device

Http

success (boolean)

output (object)

PingOne Forms connector

You can enable device profiling to collect device information and user data from user interactions with [PingOne Forms connectors](#) in your flow. Learn more in [Forms](#).

Enable device profiling in any user-facing forms as follows:

- The first PingOne Forms connector in your flow
- Any subsequent PingOne Forms connectors in the flow, including any in a subflow or parent flow

To enable device profiling in a PingOne Forms connector:

1. Add a PingOne Forms connector to your flow.
2. On the **General** tab, click the **Enable Device Profiling** toggle to enable the SDK to collect device information from user interactions with the form.
3. (Optional) Click the **Include Behavioral Data** toggle to identify non-human activity through behavioral data collection.

Note

To enable **Include Behavioral Data**, you must first turn on **Enable Device Profiling**.

4. If you want the device data in the SDK payload to be provided as a signed JWT, set **Enable Universal Device Identification** to **True**.
5. Click **Apply**.

Update Risk Evaluation

Update an existing risk evaluation to include the flow completion status for the risk evaluation. Updating the completion status allows PingOne Protect to refine and improve the accuracy of future risk evaluations. Always include a PingOne Protect connector with the Update Risk Evaluation capability in your flows to allow PingOne Protect to learn over time. The Update Risk Evaluation event includes one of the following flow completion statuses for the risk evaluation:

- **SUCCESS** when the user was granted access or passed the MFA challenge

Only events with `completionStatus=SUCCESS` allow the predictors to learn.

- **FAILED** when the user was denied access or failed the MFA challenge

If a user is unable to successfully complete an event, such as if their authentication failed, the risk evaluation for the event is updated as `completionStatus=FAILED`.

Note

If `completionStatus` isn't updated, the status remains `completionStatus=IN_PROGRESS`, and the predictor can't learn from the event and stays in training mode.

Steps

1. Add a **PingOne Protect connector** with the **Update Risk Evaluation** capability in your flow at the end of each possible path.
2. Update the risk evaluation completion status for **SUCCESS** and **FAILED** events.

Learn more in [Updating completion status for risk evaluations](#).

Capabilities

Create Risk Evaluation

Evaluate risk for a specific transaction. Risk results are based on predictors like user behavior anomalies, IP reputation analysis, Geo velocity and other risk models.

Properties

User ID textField required

The ID of the user whose risk is being evaluated.

User Name textField

The username of the user whose risk is being evaluated.

User Type dropDown

Indicates whether the user exists in the PingOne directory or in an external directory.

- EXTERNAL (Default)
- PING_ONE

User Groups textField

User groups names.

Password textField

The password entered by the user.

Password Hash Algorithm dropDown

Password hashing method.

- SHA_256 (Default)
- SHA_384

IP textField

The IP address of the user who initiated the flow.

Application ID textField

The ID for the application or resource the user wants to access.

Application Name textField

The name of the application or resource the user wants to access.

Flow Type textField

The type of flow in which risk is evaluated.

Default: AUTHENTICATION

Flow Subtype textField

The subtype of the flow.

Session ID textField

The unique session ID associated with the event.

Risk input from device textField***User Agent textField***

The user agent of the browser/device that triggered the flow.

Cookie textField

The cookie of the browser/device that triggered the flow.

External ID textField

A unique device identifier generated and managed independently of the Signals SDK (SKrisk).

Risk Policy ID textField

The risk policy set used during risk evaluation.

Custom Attributes textField

Your Custom Attributes defined at Ping.

Input Schema

- default object
 - properties object
 - clientId string required minLength: 0 maxLength: 100
Client ID
 - clientSecret string required minLength: 0 maxLength: 100
Client Secret
 - envId string required
 - userId string minLength: 0 maxLength: 100
User ID
 - userName string minLength: 0 maxLength: 100
User Name
 - userType string minLength: 0 maxLength: 100
User Type
 - userGroups string minLength: 0 maxLength: 100
User Groups
 - password string
Password
 - passwordAlgorithm string
Password Hash Algorithm
 - ipAddress string minLength: 0 maxLength: 100
IP Address
 - completionStatus string minLength: 0 maxLength: 50
Completion Status
 - targetResourceId string minLength: 0 maxLength: 100
Target Resource ID
 - targetResourceName string minLength: 0 maxLength: 100
Target Resource Name
 - flowType string minLength: 0 maxLength: 50
Flow Type

- subtype string minLength: 0 maxLength: 50

Flow Subtype

- sessionId string

- sharingType string minLength: 0 maxLength: 100

Sharing Type

- userAgent string minLength: 0 maxLength: 8190

User Agent

- targetedPolicy boolean

Targeted Policies Evaluation

- riskPolicySetId string

- customAttributes string

- skRiskFP string

- cookie string

- externalId string

Output Schema

- output object
 - rawResponse object
 - id string
 - environment object
 - id string
 - createdAt string
 - updatedAt string
 - event object
 - completionStatus string
 - targetResource object
 - id string
 - name string
 - ip string
 - flow object
 - type string
 - subtype string
 - session object
 - id string
 - user object
 - id string
 - name string
 - type string
 - groups array
 - sharingType string
 - browser object
 - userAgent string
 - cookie string
 - origin string

- device object
 - externalId string
- riskPolicySet object
 - id string
 - name string
- result object
 - level string
 - type string
 - score number
 - source string
 - recommendedAction string
- details object
 - anonymousNetworkDetected boolean
 - country string
 - impossibleTravel boolean
 - ipAddressReputation object
 - level string
 - score integer
 - type string
 - domain object
 - asn integer
 - sld string
 - tld string
 - organization string
 - isp string
 - ipRisk object
 - level string
 - reason string
 - type string

- ipVelocityByUser object
 - level string
 - reason string
 - type string
 - threshold object
 - high integer
 - medium integer
 - source string
 - calculatedAt string
 - expiresAt string
 - velocity object
 - distinctCount integer
 - during integer
- userVelocityByIp object
 - level string
 - reason string
 - type string
 - threshold object
 - high integer
 - medium integer
 - source string
 - calculatedAt string
 - expiresAt string
 - velocity object
 - distinctCount integer
 - during integer
- estimatedSpeed number
- estimatedDistance number
- state string
- city string

- longitude number
- latitude number
- device object
 - browser object
 - name string
 - os object
 - name string
 - id string
 - externalId string
 - estimatedDistance number
 - lastSeen string
 - externalLastSeen string
 - agent object
 - name string
 - locale string
 - version string
 - macAddress array
 - loggedInUser object
 - domainName string
 - objectSid string
 - name string
 - customScript object
 - exitCode integer
 - output string
 - os object
 - name string
 - version string
- previousSuccessfulTransaction object
 - anonymousNetworkDetected boolean
 - country string

- state string
- city string
- ip string
- timestamp string
- userBasedRiskBehavior object
 - level string
 - reason string
 - type string
- userRiskBehavior object
 - level string
 - reason string
 - type string
- geoVelocity object
 - level string
 - reason string
 - type string
- anonymousNetwork object
 - level string
 - reason string
 - type string
- userLocationAnomaly object
 - level string
 - reason string
 - type string
 - status string
- botDetection object
 - level string
 - reason string
 - type string

- detected object
 - rule object
 - id integer
- suspiciousDevice object
 - level string
 - reason string
 - type string
 - detected object
 - rule object
 - id integer
- newDevice object
 - level string
 - reason string
 - status string
 - type string
- trustedDevice object
 - level string
 - reason string
 - type string
 - status string
- trafficAnomaly object
 - reason string
 - level string
 - type string
 - detected object
 - rule object
 - id integer
 - threshold object
 - high integer
 - medium integer

- velocity object
 - distinctCount integer
 - during integer

Output Example

```

{ "rawResponse" :
{ "id" : "57f879e5-752e-47f2-a230-0afb07ad95ef",
  "environment" :
  { "id" : "9ad15e9e-3ac6-43f7-a053-d46b87d6c4a7" },
  "createdAt" : "2020-10-21T17:48:35.474Z",
  "updatedAt" : "2020-10-21T17:48:35.474Z",
  "event" :
  { "completionStatus" : "SUCCESS",
    "targetResource" :
    { "id" : "969e4a59-5cf9-44c3-a1ba-9f392bf7f622",
      "name" : "Jira" },
    "ip" : "47.153.27.192",
    "flow" :
    { "type" : "AUTHENTICATION",
      "subtype" : null },
    "session" :
    { "id" : "31618b01-08cd-4bee-b0d3-90b895671bb4" },
    "user" :
    { "id" : "john",
      "name" : "John DeMock",
      "type" : "EXTERNAL",
      "groups" :
      [
        { "name" : "dev" },
        { "name" : "sre" } ] },
    "sharingType" : "SHARED",
    "browser" :
    { "userAgent" : "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36",
      "cookie" : "f5c107c5-7c42-4937-807d-589b6a77a630" },
      "device" :
      { "externalId" : "Id-5dfb66d3-f6cb-4156-b330-bdebe1337h9d" },
      "origin" : "P1_ORCHESTRATION" },
    "riskPolicySet" :
    { "id" : "9d369d4a-f1d5-0f31-12ac-62d9e01ac852",
      "name" : "Default Risk Policy Set" },
    "result" :
    { "level" : "LOW",
      "type" : "VALUE",
      "score" : 50,
      "source" : "OVERRIDE",
      "recommendedAction" : "BOT_MITIGATION" },
    "details" :
    { "ipAddressReputation" :
      { "score" : 0,
        "domain" :
        { "asn" : 5650,
          "sld" : "",
          "tld" : "",
          "organization" : "frontier communications",
          "isp" : "frontier communications of america inc." },
        "level" : "LOW" },
        "estimatedSpeed" : 0,
        "anonymousNetworkDetected" : false,
        "country" : "united states",
        "previousSuccessfulTransaction" :
        { "ip" : "47.153.27.192",
          "timestamp" : "2023-02-26T15:42:16.711Z",
          "anonymousNetworkDetected" : false,

```

```

"country" : "united states",
"state" : "california",
"city" : "torrance" },
"device" :
{ "id" : "Id-5dfb66d3-f6cb-4156-b330-bdebe1448f8c",
  "externalId" : "Id-5dfb66d3-f6cb-4156-b330-bdebe1337h9d",
  "estimatedDistance" : 0,
  "os" :
  { "name" : "Windows" },
  "browser" :
  { "name" : "Chrome" },
  "lastSeen" : "2024-01-30T-13:58:24.650Z",
  "externalLastSeen" : "2024-01-30T-13:58:24.650Z",
  "agent" :
  { "customScript" :
    { "exitCode" : 5,
      "output" : "this is the output of the script" },
    "loggedInUser" :
    { "name" : "username",
      "objectSid" : "objectSid",
      "domainName" : "domainName" },
    "macAddress" :
    [ "0a-23-3b-fa-34-bb",
      "3d-21-fb-12-8b-h5",
      "ak-le-12-07-88-25" ],
    "os" :
    { "name" : "macOS",
      "version" : "14.6.1" },
      "name" : "mac-ABCD",
      "id" : "94970C21-D879-6ACD-E208-99C6ECF9D7EA",
      "locale" : "en_US",
      "version" : "1.0.0" } },
  "state" : "california",
  "city" : "torrance",
  "estimatedDistance" : 0,
  "impossibleTravel" : false,
  "ipVelocityByUser" :
  { "level" : "LOW",
    "threshold" :
    { "source" : "MIN_NOT_REACHED" },
    "velocity" :
    { "distinctCount" : 1,
      "during" : 3600 },
    "type" : "VELOCITY" },
  "userLocationAnomaly" :
  { "level" : "LOW",
    "status" : "KNOWN_LOCATION",
    "type" : "USER_LOCATION_ANOMALY" },
  "userVelocityByIp" :
  { "level" : "LOW",
    "threshold" :
    { "source" : "MIN_NOT_REACHED" },
    "velocity" :
    { "distinctCount" : 1,
      "during" : 3600 },
    "type" : "VELOCITY" },
  "geoVelocity" :
  { "level" : "LOW",
    "type" : "GEO_VELOCITY" },
  "newDevice" :
  { "level" : "LOW",
    "reason" : "This device has been used recently",

```

```

"status" : "KNOWN_DEVICE",
"type" : "DEVICE" },
"trustedDevice" :
{ "reason" : "PingID Device trust verified successfully",
  "level" : "LOW",
  "type" : "DEVICE",
  "status" : "TRUST_VERIFIED" },
"botDetection" :
{ "level" : "MEDIUM",
  "type" : "BOT",
  "reason" : "Automation framework detected",
  "detected" :
  { "rule" :
    { "id" : 620 } } },
"suspiciousDevice" :
{ "level" : "MEDIUM",
  "type" : "DEVICE",
  "reason" : "Timezone offset mismatch",
  "detected" :
  { "rule" :
    { "id" : 557 } } },
"ipRisk" :
{ "level" : "LOW",
  "type" : "IP_REPUTATION" },
"userBasedRiskBehavior" :
{ "level" : "LOW",
  "reason" : "NA",
  "type" : "USER_RISK_BEHAVIOR" },
"anonymousNetwork" :
{ "level" : "LOW",
  "type" : "ANONYMOUS_NETWORK" },
"trafficAnomaly" :
{ "reason" : "Number of unique users per device is above High threshold",
  "level" : "HIGH",
  "type" : "TRAFFIC_ANOMALY",
  "detected" :
  { "rule" :
    { "id" : 803 },
    "threshold" :
    { "high" : 4,
      "medium" : 3 },
    "velocity" :
    { "distinctCount" : 5,
      "during" : 3600 } } } } }

```

Update Risk Evaluation

Update an existing risk evaluation to refine future results.

Properties

Risk Evaluation ID textField

ID of the Risk Evaluation

Risk Evaluation status textField

status of the Risk Evaluation

Input Schema

- default object
 - properties object
 - clientId string required minLength: 0 maxLength: 100
Client ID
 - clientSecret string required minLength: 0 maxLength: 100
Client Secret
 - envId string required
 - completionStatus string minLength: 0 maxLength: 50
Completion Status
 - riskId string required minLength: 0 maxLength: 100
Risk Evaluation ID

Output Schema

- output object
 - rawResponse object
 - completionStatus string
 - ip string
 - flow object
 - type string
 - subtype string
 - session object
 - id string
 - user object
 - id string
 - name string
 - type string
 - groups array
 - sharingType string
 - origin string

Output Example

```
{ "rawResponse" :
  { "completionStatus" : "SUCCESS",
    "targetResource" :
      { "id" : "969e4a59-5cf9-44c3-a1ba-9f392bf7f622",
        "name" : "Jira" },
    "ip" : "47.153.27.192",
    "flow" :
      { "type" : "AUTHENTICATION",
        "subtype" : null },
    "session" :
      { "id" : "31618b01-08cd-4bee-b0d3-90b895671bb4" },
    "user" :
      { "id" : "john",
        "name" : "John DeMock",
        "type" : "EXTERNAL",
        "groups" :
          [
            { "name" : "dev" },
            { "name" : "sre" } ] },
    "sharingType" : "SHARED",
    "origin" : "P1_ORCHESTRATION" } }
```

Send Risk Evaluation Feedback

Submit feedback to help refine risk classification or clear a user's risk status.

Properties

Risk Evaluation ID textField required

The ID of the risk evaluation you are providing feedback on.

Feedback Category dropDown required

The type of feedback to submit for the risk evaluation.

- FALSE_HIGH_RISK
- FRIENDLY_BOT
- NEW_ACCOUNT_FRAUD
- COMPROMISED_ACCOUNT
- AUTOMATED_ATTACK

Reason dropDown

Reason for FALSE_HIGH_RISK

- OFFICE_NETWORK
- COMPANY_VPN
- WRONG_LOCATION
- ORG_NETWORK
- SUCCESSFUL_MFA
- OTHER

Reason dropDown

Reason for FRIENDLY_BOT

- KNOWN_CRAWLER
- KNOWN_AGGREGATOR
- INTERNAL_AUTOMATION
- OTHER

Reason dropDown

Reason for NEW_ACCOUNT_FRAUD

- SUSPICIOUS_EMAIL_ADDRESS
- USERNAME_GUESSING
- OTHER

Reason dropDown

Reason for COMPROMISED_ACCOUNT

- USER_CLAIMS_IT_IS_NOT_THEM
- UNSUCCESSFUL_MFA
- OTHER

Reason dropDown

Reason for AUTOMATED_ATTACK

- CREDENTIAL_STUFFING
- PASSWORD_SPRAY
- OTHER

Input Schema

- default object
 - properties object
 - clientId string required minLength: 0 maxLength: 100
Client ID
 - riskEvaluationId string required
Risk Evaluation ID
 - feedbackCategory string required minLength: 0 maxLength: 100
Feedback Category
 - reason string minLength: 0 maxLength: 100
Reason for Feedback (optional)

Output Schema

- output object
 - rawResponse object
 - status string
 - message string

Output Example

```
{ "rawResponse" :  
  { "status" : "SUCCESS",  
    "message" : "Feedback submitted successfully" } }
```

Troubleshooting

To start troubleshooting issues with the PingOne Protect connector, try the following:

- Test your implementation. Learn more in the [PingOne Protect Integration Testing knowledgebase article](#).
- For each connector in the flow, make sure you provided all required inputs.
- For mobile applications, if you're using the **skrisk** component to include the data provided by the Signals (Protect) SDK, make sure that you followed the steps in the [PingOne Protect Native SDKs documentation](#).
- To use the DaVinci Analytics feature to see where the flow stopped, open your flow and click **Analytics** in the lower-left corner of the flow editor. Learn more in [Debugging and analytics](#).
- Open your flow, click the **More Options** (:) icon, and click the **Show Node ID** toggle. This makes it easier to identify the source of inputs and outputs.

PingOne RADIUS Gateway Connector

The PingOne RADIUS Gateway connector enables you to integrate PingOne DaVinci flows with a PingOne RADIUS Gateway.

Setup

Resources

For information and setup help, see the following:

- PingOne documentation:
 - [Getting started with PingOne](#)
 - [PingOne Gateways documentation](#)

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne license.
- A PingOne environment.
- A RADIUS gateway. To create and configure a RADIUS gateway see [RADIUS Gateways](#).

Setting up the connector

In DaVinci, go to **Connections** and add a PingOne RADIUS gateway connector. For help, see [Adding a connector](#).

Using the connector in a flow

Use the RADIUS Gateway connector to instruct DaVinci to respond to a RADIUS Gateway authentication session request. The connector can send one of the following responses:

- **Accept:** Indicates that a user has completed all the required authentication steps. The RADIUS gateway sends an `ACCESS_ACCEPT` response to the RADIUS client, and grants the user access.

Note

You can send user RADIUS attributes back to the RADIUS client, and the connector also provides the option to define vendor-specific attributes.

- **Reject:** Indicates that a user failed a required authentication step. The RADIUS gateway sends an `ACCESS_REJECT` response to the RADIUS client, and rejects the user's authentication request.
- **Challenge:** Instructs the gateway to send a challenge to the authenticating user by sending an `'ACCESS_CHALLENGE'` response to the RADIUS client.

Note

This response type is only supported when using a RADIUS client that supports `ACCESS_CHALLENGE` requests.

- **Poll:** Indicates that the user is authenticating with the PingID mobile app, and the DaVinci flow is waiting for a push response.

RADIUS gateway flow templates

PingOne provides out-of-the-box DaVinci flows that you can integrate into your RADIUS gateway.

 Note

To use a RADIUS gateway flow template, you first need to add the PingID connector and the PingOne RADIUS Gateway connector.

The following RADIUS gateway flows are available:

- **RADIUS Gateway - authentication**  flow: This flow can be used to authenticate users when accessing RADIUS clients that support the RADIUS PAP protocol. You can customize the following options:
 - OTP Fallback: If the PingID server can't reach the device or the push response can't be completed, allow users to authenticate with a one-time passcode instead.
 - Newline Character: Select a line separation character to use for RADIUS server challenge messages.
 - RADIUS response attribute.

To download this flow, search for **RADIUS gateway - authentication**  flow in the DaVinci flow library.

- **RADIUS Gateway - registration and authentication flow** : This flow can be used to register and authenticate users when accessing RADIUS clients that support Challenge mode. Customization options are the same as those in the RADIUS Gateway - authentication flow.
- **RADIUS Gateway - no challenge authentication flow** : This flow can be used when accessing RADIUS clients that support the RADIUS PAP protocol to authenticate users with VPN clients that do not support Challenge mode. You can customize the Custom Separator to enable users to enter the OTP with their password. If you define a specific custom separator:
 - When a user wants to authenticate using PingID mobile app they only need to add the custom separator after their password and then the word push.
 - When using other OTP-based authentication methods (such as PingID Desktop app or a YubiKey), the user should add a custom separator after their password and then the OTP. For example `password,123456`.
 - If the user is registered with multiple devices supported by this mode, an OTP generated by any one of those devices will authenticate the user.
 - This flow does not support on-the-fly registration.

 Note

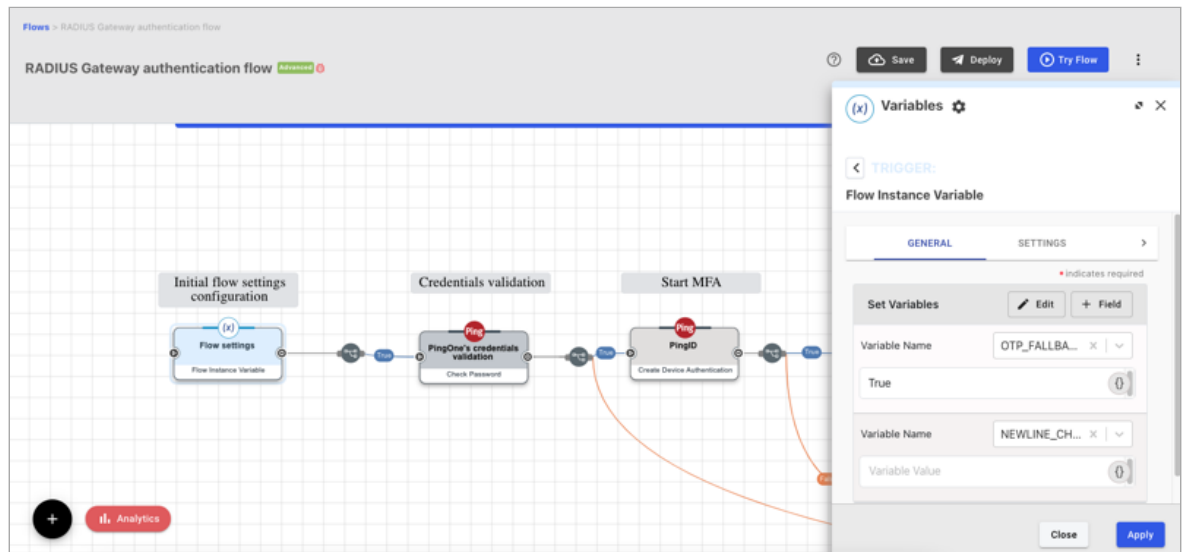
If a custom separator is not defined the user can enter their password followed by the OTP, without a separator. For example `<password>OTP`.

- **RADIUS Gateway - advanced protocols authentication flow** : This flow can be used when accessing RADIUS clients that support advanced protocols (such as MS-CHAPv2) to authenticate users. A comma is defined as the Custom Separator by default to enable users to enter the OTP with their username. The custom separator must be the same as that defined in your NPS, and you can customize it in the **Flow settings** node, if required. The custom separator enables the following user experience:
 - When a user wants to authenticate using PingID mobile app they only need to add the custom separator after their username and then the word push.
 - When using other OTP-based authentication methods (such as PingID Desktop app or a YubiKey), the user should add a custom separator after their username and then the OTP. For example `John,123456`.

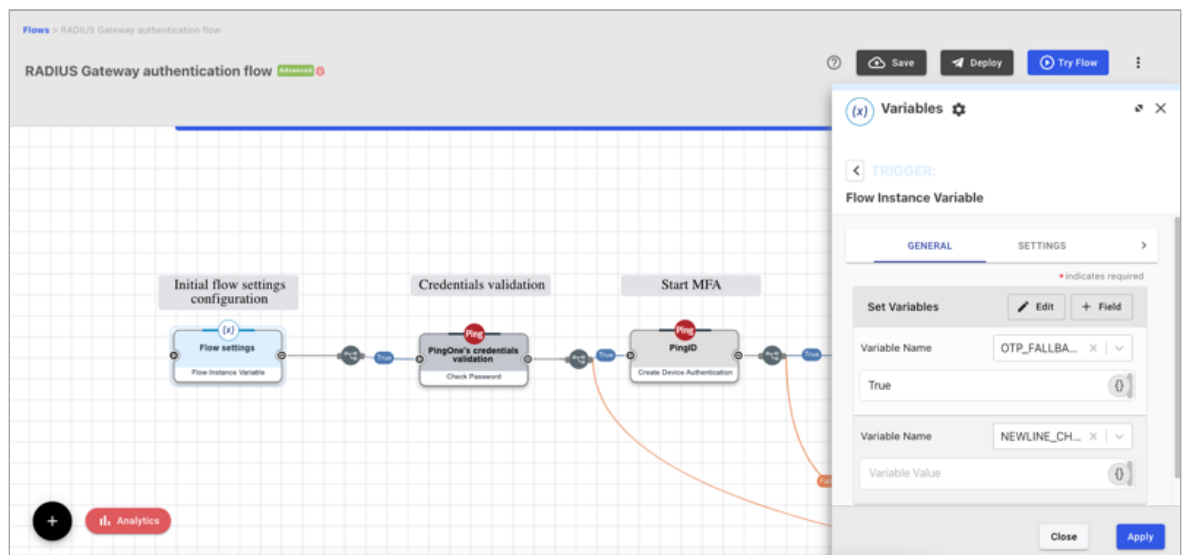
- If the user is registered with multiple devices supported by this mode, an OTP generated by any one of those devices will authenticate the user.
- This flow does not support on-the-fly registration.

To customize the RADIUS Gateway authentication flow template:

1. In the DaVinci Flow library search for RADIUS gateway authentication flow and import the flow. For help, see [Using DaVinci flow templates](#).



2. To configure an OTP Fallback, select the **Flow settings** node and modify the `OTP_FALLBACK` variable. Possible values: `True` or `False`.
3. To define a Newline Character, select the **Flow settings** node and modify the `NEWLINE_CHARACTER` variable. Choose from:
 - None: (leave the field empty if you do not want to define a newline character).
 - `\n`: Unix style.
 - `\r\n`: Windows style.
 - `<br>`: HTML
4. To add a RADIUS response attribute : Select the **Authentication Approved** node, click **Add**, and define the attribute properties.



Capabilities

Radius Response

The returned message sent to the RADIUS client.

Properties

Response Type dropDown

The type of returned message sent to the RADIUS client. Valid response types are CHALLENGE, POLL, ACCEPT, or REJECT.

- CHALLENGE
- POLL
- ACCEPT
- REJECT

Response Value textField

The text that displays in the Reply-Message, which is sent to the RADIUS client and visible to the user, limited to 253 characters.

Use the following fields to map values from your flow to RADIUS attributes. label
Attribute Mapping attributesRulesList

Input Schema

- default object
 - properties object
 - responseType string required
 - responseValue string
 - description string
 - attributeMapping array

Output Schema

- output object
 - text string

PingOne RADIUS Gateway Connector Release Notes

New features and improvements in the PingOne RADIUS Gateway connector.

November 2023

PingOne RADIUS Gateway flow enhancement

Improved

We've added the ability to evaluate PingID authentication policies to all RADIUS Gateway flows. To support this enhancement, we've also added the Policy Evaluation capability to the PingID connector.

April 2023

New flows for the PingOne RADIUS Gateway connector

Improved

We have added the following flow templates to support authentication for MS-CHAP v2 protocol, authentication in no-challenge mode, and on-the-fly registration:

- [RADIUS Gateway - registration and authentication flow](#)
- [RADIUS Gateway - no challenge authentication flow](#)
- [RADIUS Gateway - advanced protocols authentication flow](#)

December 2022

PingOne RADIUS Gateway connector now available

New

The new PingOne RADIUS Gateway connector is now available.

Use this connector to orchestrate user authentication flows that are initiated by authentication requests using the RADIUS protocol.

PingOne Scope Consent Connector

The PingOne Scope Consent connector lets you view consent records on an application or user basis, revoke or update user consent records, or prompt users to provide or decline consent to sign-on policies and record these decisions.

You can use the PingOne Scope Consent connector to:

- View a list of application consent records a user has granted, declined, or revoked
- Determine whether a user has granted consent for an application
- Accept or decline consent for an application on behalf of a user
- Update the application consent record as revoked

- Check, prompt for, and record user decisions regarding consent for an application

Setup

Resources

For information and setup help, see the following sections of the PingOne documentation:

- PingOne:
 - [Introduction to PingOne](#)
 - [Getting started with PingOne](#)
 - [Adding an application](#)
 - [Agreements](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A PingOne license ([Try PingOne for free](#))
- A PingOne environment with a configured Worker app

Setting up PingOne

Setting up your PingOne environment

See [Getting started with PingOne](#).

Adding a Worker application

Add a Worker application in the PingOne console before setting up the PingOne connector in DaVinci:

1. In the PingOne console, add a Worker app. See [Adding an application](#).



Note

Attribute mappings are not required.

2. Ensure that you set the authentication method as `Client secret basic`.

The PingOne connector receives a token using your application's credentials.

3. Enable the application. See [Enabling or disabling an application](#).

The capabilities in the PingOne connector call endpoints in PingOne with a token received using the application's credentials. To enable all capabilities, your application needs the required role assignments for the associated capability. If the application doesn't have the required role assignment, you'll see error messages stating that the required authorization isn't configured.

Assigning Roles to the application

To use the appropriate capabilities, the Worker app used by the connector needs the **Environment Admin** and **Identity Data Admin** roles.

Note

The user that creates the Worker app must have the **Environment Admin** and **Identity Data Admin** roles to assign the roles to a Worker app.

1. In your PingOne environment, go to **Applications → Applications**.
If you haven't added the application yet, see [Adding an application](#).
2. Locate the appropriate application and click it to open the details panel.
3. Click the **Roles** tab and then click the **Pencil** icon to edit the roles.
4. Review the assigned roles to ensure that they include **Environment Admin** and **Identity Data Admin** roles. If not, click **+** **Add role** to assign them.

Getting your application credentials

Get the **Client ID** and **Client secret** from the PingOne console before setting up the PingOne connector in DaVinci:

1. In your PingOne environment, go to **Applications → Applications**.
If you haven't added the application yet, see [Adding an application](#).
2. Locate the appropriate application and click it to open the details panel.
3. On the **Configuration** tab, expand **General** and locate the **Client ID** and **Client secret**. Copy these values to a secure location.

Getting your environment details

Get your **Environment ID** and **Region** before setting up the PingOne connector in DaVinci:

1. In your PingOne environment, go to **Settings → Environment Properties**.
2. Locate the **Environment ID** and **Region**. Copy these values to a secure location.

Setting up the PingOne connector configuration

In DaVinci, add a PingOne connection. For help, see [Adding an application](#).

Connector configuration

Environment ID

The unique identifier for the appropriate PingOne environment. To find the environment ID, see [Environment properties](#).

Client ID

The unique public identifier for the PingOne application. To find the client ID, see [Viewing application details](#).

Client secret

The cryptographic secret that is known only to the application and the authorization server. To find the client secret, see [Viewing a client secret](#).

Region

The geographic region that hosts your PingOne tenant. To find the region, see [Environment properties](#).

Using the connector in a flow

Manage user consent

You can use the PingOne Scope Consent connector to view and manage user consent to an application as part of a DaVinci flow policy.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Use one of the following capabilities to view information about consent records:

- **Read User Consent:** Use to view a list of all application consent records a specific user has granted, declined, or revoked.
- **Check User Consent:** Use to determine whether a user has granted consent for a specific application.

Use one of the following capabilities to manage and update user consent records:

- **Save User Consent:** Use to accept or decline consent for an application on behalf of a user.
- **Revoke User Consent:** Use to update the application consent record for a user as revoked.

Use **Get User Consent** to check, prompt for, and record user decisions regarding consent to application as part of a DaVinci flow policy. Use this capability in a flow at the point where you want to prompt the user for their consent. Use the **Custom Screens** tab to edit the HTML and CSS to customize the appearance and text of the prompt that is displayed to the user. For example, change **Do you approve the request?** to **Do you accept this request?** or change the buttons from **Approve** and **Decline** to **Yes** and **No**.

Capabilities

Read User Consent

Find information about consent users have granted for all applications.

Properties

User Attribute dropdown required

Select the attribute you want to use to locate a user.

- User ID
- Username
- Email

User Identifier textField required

Enter the user ID, username, or email address of the user you want to locate.

Input Schema

- default object
 - properties object
 - matchUserAttribute string required
PingOne user attribute to identify a user with.
 - userIdentifier string required
User attribute to match user.

Output Schema

- output object
 - consents array
 - properties object
 - application object
 - properties object
 - id string
 - name string
 - type string
 - consentId string
 - consentStatus string
 - consentScopes array
 - rawResponse object
 - _embedded object
 - consents array
 - count number
 - size number
 - statusCode number
 - headers object

Check User Consent

Indicate whether users have granted consent for an application.

Properties

User Attribute dropDown required

Select the attribute you want to use to locate a user.

- User ID
- Username
- Email

User Identifier textField required

Enter the user ID, username, or email address of the user you want to locate.

Application Attribute dropDown required

Select the application attribute that you want to use to locate an application.

- Application ID
- Application Name

Application Identifier textField required

Enter the application ID or name of the application you want to locate.

Input Schema

- default object
 - properties object
 - matchUserAttribute string required
PingOne user attribute to identify a user with.
 - userIdentifier string required
User attribute to match user.
 - matchApplicationAttribute string required
PingOne application attribute to identify an application with.
 - applicationIdentifier string required
Application attribute to match application.

Output Schema

- output object
 - application object
 - id string
 - name string
 - type string
 - consentId string
 - consentStatus string
 - consentScopes array
 - rawResponse object
 - _embedded object
 - consents array
 - count number
 - size number
 - statusCode number
 - headers object

Save User Consent

Accept or decline user consent for an application. It replaces the existing consent for the application if there is one.

Properties

User Attribute dropDown required

Select the attribute you want to use to locate a user.

- User ID
- Username
- Email

User Identifier textField required

Enter the user ID, username, or email address of the user you want to locate.

Application Attribute dropDown required

Select the application attribute that you want to use to locate an application.

- Application ID
- Application Name

Application Identifier textField required

Enter the application ID or name of the application you want to locate.

Scopes textField required

Enter the space-separated list of scopes that have been requested. These scopes are validated against the allowed scopes assigned to the PingOne application.

Consent Result textField required

The accept or decline consent result from the user and indicated by "true", "false", "yes", "no", "accepted", or "declined".

Input Schema

- default object
 - userAgent string
User Agent
 - ip string
Client IP Address
 - properties object
 - matchUserAttribute string required
PingOne user attribute to identify a user with.
 - userIdentifier string required
User attribute to match user.
 - matchApplicationAttribute string required
PingOne application attribute to identify an application with.
 - applicationIdentifier string required
Application attribute to match application.
 - scopesUnconditionalRequired string required
Scopes.
 - consentResult string required
Consent Result.

Output Schema

- output object
 - application object
 - id string
 - name string
 - type string
 - consentId string
 - consentStatus string
 - consentScopes array
 - rawResponse object
 - statusCode number
 - headers object

Revoke User Consent

Revoke and remove user consent for an application.

Properties

User Attribute dropDown required

Select the attribute you want to use to locate a user.

- User ID
- Username
- Email

User Identifier textField required

Enter the user ID, username, or email address of the user you want to locate.

Consent Attribute dropDown required

Enter the consent ID, application ID, or application name of the consent record you want to locate.

- Consent ID
- Application ID
- Application Name

Consent Identifier textField required

A unique identifier for the consent record.

Input Schema

- default object
 - properties object
 - matchUserAttribute string required
PingOne user attribute to identify a user with.
 - userIdentifier string required
User attribute to match user.
 - matchConsentAttribute string required
PingOne consent attribute to identify an consent with.
 - consentIdentifier string required
Consent attribute to match consent.

Output Schema

- output object
 - application object
 - id string
 - name string
 - type string
 - consentId string
 - consentStatus string
 - consentScopes array
 - rawResponse object
 - statusCode number
 - headers object

Get User Consent

This capability facilitates application consent by checking, prompting, and recording user decisions regarding consent. This action includes the HTML template and other resources like CSS. You can customize them under the Custom Screens tab.

Properties

Always Prompt for Consent toggleSwitch required

Indicates whether the user will always be prompted to consent to the application's request. If disabled, users will only be prompted to consent to these requests if they have not already done so.

User Attribute dropdown required

Select the attribute you want to use to locate a user.

- User ID
- Username
- Email

User Identifier textField required

Enter the user ID, username, or email address of the user you want to locate.

Application Attribute dropdown required

Select the application or specify an application identifier that will be used to check, prompt and store consent for the user.

- Application ID
- Application Name

Application Identifier textField required

Enter the unique identifier of the application that will be used to check, prompt and store consent for the user.

Application Name textField required

Enter the name of the application that will be used to check, prompt and store consent for the user.

Scopes textField required

Scopes define the user information that the application wants to access and the user will need to consent to allowing, such as the user's name, email address, and phone number. You must provide at least one scope. You may provide multiple scopes, each separated by a space.

Scopes textField required

Enter the space-separated list of scopes that have been requested. These scopes are validated against the allowed scopes assigned to the PingOne application.

Scopes textField required

Enter the space-separated list of scopes that have been requested. These scopes are validated against the allowed scopes assigned to the PingOne application.

appConsentHtmlConfig

Output Schema

- output object
 - matchedUser object
 - application object
 - id string
 - name string
 - type string
 - consentId string
 - consentStatus string
 - consentScopes array
 - rawResponse object
 - statusCode number
 - headers object

PingOne Scope Consent Connector Release Notes

New features and improvements in the PingOne Scope Consent connector.

January 2025

Simplified Get User Consent capability

Improved

Previously, to select how the capability identifies the application from the **Application Attribute** field, you had to select either **Application ID** or **Application Name** and enter a value into the corresponding field.

Now, you can always enter the applicable scope into the **Scopes** field regardless of the **Application Attribute** field value.

January 2024

PingOne Scope Consent connector now available

New

The new PingOne Scope Consent connector is now available.

Use this connector to view consent records on an application or user basis, revoke or update user consent records, or prompt users to provide or decline consent to sign-on policies and record these decisions.

PingOne Verify Connector

Use the PingOne Verify DaVinci connector to securely verify a user's identity based on a government-issued document and other user-submitted data, such as a live face capture (selfie).

The user ID information is captured using a unique QR code and sent to the PingOne ID Verification service. The PingOne ID Verification service interacts with service providers that verify the submitted user ID information. When a user's ID information is successfully verified, the PingOne ID Verification service approves the user authentication and sends the ID verification status to the browser or to the next connector in the flow.

Setup

Resources

Learn more about setup help in the following sections of PingOne Verify and DaVinci:

- PingOne Verify documentation
 - [Introduction to PingOne Verify](#)
 - [Getting started with PingOne Verify](#)
- DaVinci documentation
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the PingOne Verify connector, you'll need:

- A PingOne license with PingOne Verify ([Try PingOne for free](#))
- A PingOne environment with a configured application

Setting up PingOne

Setting up your PingOne environment

Sign up for PingOne and configure an environment with PingOne Verify. Learn more in [Getting started with PingOne](#).

Getting your environment details

Get your **Environment ID** and **Region** before setting up the PingOne Verify connector in DaVinci:

1. In the PingOne admin console, go to **Settings > Environment Properties**.
2. Locate the **Environment ID** and **Region**.
3. Copy these values to a secure location.

Getting your application credentials

Get the **Client ID** and **Client secret** from your PingOne admin console before setting up the PingOne Verify connector in DaVinci:

1. In the PingOne admin console, go to **Applications > Applications**. If you haven't added the application yet, you can find instructions in [Adding an application](#) in the PingOne documentation.
2. Locate the appropriate application and then click its entry to open the details panel.
3. On the **Profile** tab, locate the **Client ID** and **Client secret**.
4. Copy these values to a secure location.

Setting up the connector

In DaVinci, go to **Connections** and add a **PingOne Verify** connection. Learn more in [Adding a connector](#).

Connector settings

Environment ID

The unique identifier for the appropriate PingOne environment. You can learn how to find the environment ID in [Environment properties](#) in the PingOne documentation.

Client ID

The unique public identifier for the PingOne application. Learn how to find the client ID in [Viewing application details](#) in the PingOne documentation.

Client secret

The cryptographic secret that is known only to the application and the authorization server. Learn how to find the client secret in [Viewing a client secret](#) in the PingOne documentation.

Region

The geographic region that hosts your PingOne tenant. Learn how to find the region in [Environment properties](#) in the PingOne documentation.

Using the PingOne Verify connector in a flow

You can use the PingOne Verify connector to add user verification based on a government-issued document and live face capture (selfie) and the other [PingOne Verify types of verification](#) configurable with a [PingOne Verify policy](#).

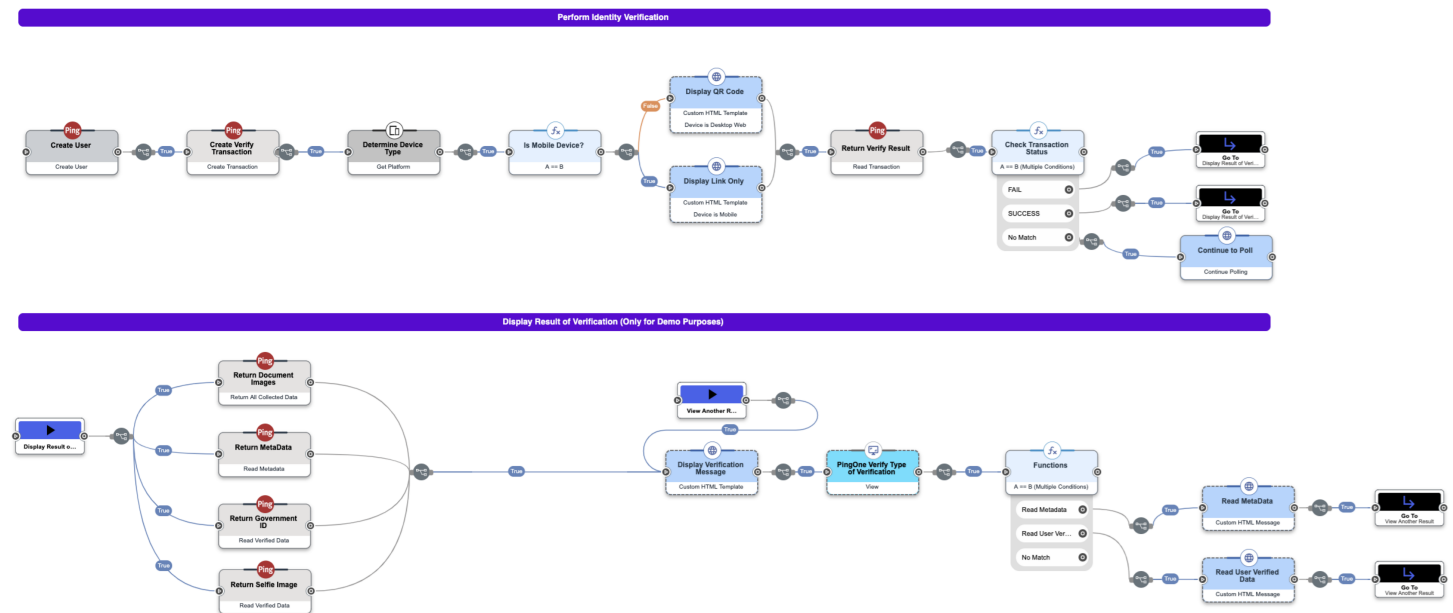
The PingOne Verify connector is typically added to an existing flow, such as a registration flow or sign-on flow.

Note

When **Debug Mode** is selected in the flow settings, logs can include sensitive data. Learn more in [Debugging and Analytics](#).

In the flow example below, when a user's ID information is successfully verified, the PingOne ID Verification service approves the user authentication and sends the ID verification status to the browser or to the next connector in the flow.

The example flow contains the following nodes:



The **Get User Details** node lets the user input their information into PingOne using the **Create User** node. This information is also used for biographic matching requirements needed in a PingOne Verify transaction.

The **Create Verify Transaction** node enables the user verification status and creates the PingOne Verify transaction. You can use this node to add biographic fields, such as a user's first name, last name, and birth date, which are used for biographic matching. If the transaction succeeds, the user sees a unique QR code in the browser.

The **Return Verify Result** and **Check Transaction Status** nodes read the results of the verification transaction, and then check the status of the transaction. The status is evaluated as follows:

- **Fail** : The flow continues to **Read government ID** node, **Return all collected** node, and **Read metadata** node.
- **Success** : The flow continues to **Read government ID** node, **Return all collected** node, and **Read metadata** node.
- **No match** : The flow shows the QR code again, and the user can try again.

The `Return Document Images`, `Read Metadata`, `Return Government ID`, and `Return Selfie Image` nodes read the verified data from the government ID, user-submitted data, and metadata related to the verification. The output can be selectively used in the `Display User Data` node.

`Read Metadata` results include biographic matching that was required in the `Create Verify Transaction` node. The biographic matching results show the comparison between what the end user inputs as their data against the verified data extracted from their government ID, returning a confidence level of high, medium, or low.

Capabilities

Create Transaction

Create verify transaction

Properties

User ID textField

ID of the user

Device OS Type dropDown

The OS type of the device to receive SMS messages during verification.

- Mobile Web (Default)

Verify Policy dropDown

Name of the verify policy.

- Use Verify Policy ID

Verify Policy ID textField

ID of the verify policy.

Notification Phone Number textField

The phone number to receive SMS notifications during verification.

Notification Email Address textField

The email address to receive email notifications during verification.

Verification Phone Number multipleTextFields

The phone number(s) to be verified for phone-verification-required policy.

Verification Email Address multipleTextFields

The email address(es) to be verified for email-verification-required policy.

Reference Image textField

Base64 encoded reference image for facial-comparison-only verify policy.

Biographic Fields selectNameValueListColumn

Use this section to add biographic fields

- Given Name
- Family Name
- Name
- Address
- Birthdate

Challenge textField

Optional challenge. If not provided, a random challenge will be generated.

Redirect URL textField

The Redirect URL where the user is returned to after document collection. Only secure (https://) URLs are allowed.

Redirect Message textField

Displayed after document collection and before redirecting to the specified URL. Requires a configured Redirect URL. Limited to 256 characters.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `deviceOsType` string required
device OS type
 - `verifyPolicy` string minLength: 0 maxLength: 100
verify policy
 - `verifyPolicyId` string minLength: 0 maxLength: 100
verify policy ID
 - `notifyPhone` string
phone number for notification
 - `notifyEmail` string
email address for notification
 - `verifyPhone` array uniqueItems: true
phone number(s) for verification
 - `verifyEmail` array uniqueItems: true
email address(es) for verification
 - `referenceImage` string
base64 encoded reference image for facial-comparison-only verify policy
 - `biographic` array
biographic info
 - `challenge` string minLength: 1 maxLength: 100
challenge Id
 - `redirectUri` string
Redirect URL
 - `redirectMessage` string
Redirect message

Output Schema

- output object
 - transaction object
 - id string
 - verifyPolicy object
 - id string
 - transactionStatus object
 - status string
 - qrUrl string
 - webVerificationUrl string
 - webVerificationCode string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - rawResponse object
 - id string
 - verifyPolicy object
 - id string
 - transactionStatus object
 - status string
 - qrUrl string
 - webVerificationUrl string
 - webVerificationCode string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - headers object
 - statusCode integer
 - challenge string

Output Example

```
{ "rawResponse" :  
  { "transaction" :  
    { "id" : "c8d41d45-7f0b-42b6-88ee-fba3f6e883bf",  
      "verifyPolicy" :  
        { "id" : "a661f3bf-0e7b-45aa-a9db-6fc926ccacd3" },  
      "transactionStatus" :  
        { "status" : "REQUESTED" },  
      "qrUrl" : "https://api.pingone.com/v1/idValidations/webVerifications/c8d41d45-7f0b-42b6-88ee-fba3f6e883bf/qr",  
      "webVerificationUrl" : "https://verifycredential.pingone.com/verify-webapp/index.html?txnid=c8d41d45-7f0b-42b6-88ee-fba3f6e883bf&url=https%3A%2F%2Fapi.pingone.com%2Fv1%2FidValidations%2FwebVerifications&code=082754",  
      "webVerificationCode" : "082754",  
      "createdAt" : "2021-11-04T17:32:17.195Z",  
      "updatedAt" : "2021-11-04T17:32:17.195Z",  
      "expiresAt" : "2021-11-04T18:02:17.195Z" } } }
```

Read Transaction

Read verify transaction

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - transaction object
 - id string
 - verifyPolicy object
 - id string
 - transactionStatus object
 - status string
 - providerMessagesList array
 - qrUrl string
 - webVerificationUrl string
 - webVerificationCode string
 - verifiedDocuments string
 - createdAt string
 - updatedAt string
 - expiresAt string
 - rawResponse object
 - id string
 - verifyPolicy object
 - id string
 - transactionStatus object
 - status string
 - providerMessagesList array
 - qrUrl string
 - webVerificationUrl string
 - webVerificationCode string
 - verifiedDocuments string
 - createdAt string
 - updatedAt string
 - expiresAt string

- headers object
- statusCode integer

Output Example

```
{ "rawResponse" :  
  { "transaction" :  
    { "id" : "c8d41d45-7f0b-42b6-88ee-fba3f6e883bf",  
      "verifyPolicy" :  
        { "id" : "a661f3bf-0e7b-45aa-a9db-6fc926ccacd3" },  
        "transactionStatus" :  
          { "status" : "REQUESTED" },  
        "qrUrl" : "https://api.pingone.com/v1/idValidations/webVerifications/c8d41d45-7f0b-42b6-88ee-fba3f6e883bf/qr",  
        "webVerificationUrl" : "https://verifycredential.pingone.com/verify-webapp/index.html?txnid=c8d41d45-7f0b-42b6-88ee-fba3f6e883bf&url=https%3A%2F%2Fapi.pingone.com%2Fv1%2FidValidations%2FwebVerifications&code=082754",  
        "webVerificationCode" : "082754",  
        "createdAt" : "2021-11-04T17:32:17.195Z",  
        "updatedAt" : "2021-11-04T17:32:17.195Z",  
        "expiresAt" : "2021-11-04T18:02:17.195Z" } } } }
```

Read Transactions

Read Verify transactions

Properties

User ID textField

ID of the user

limit textField

Number of transactions to return

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `limit` integer
Specifies the maximum number of latest records to return

Output Schema

- output object
 - transactions object
 - `_embedded` object
 - `verifyTransactions` array
 - `size` number
 - `rawResponse` object
 - `_embedded` object
 - `verifyTransactions` array
 - `size` number
 - `headers` object
 - `statusCode` integer

Read User Data

Read verified user data

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
User ID
 - transactionId string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - userData object
 - id string
 - transactionStatus object
 - status string
 - verifiedUserData object
 - firstName string
 - lastName string
 - middleName string
 - gender string
 - expirationDate string
 - idNumber string
 - addressStreet string
 - addressCity string
 - addressState string
 - addressZip string
 - country string
 - issueDate string
 - weight string
 - height string
 - hairColor string
 - eyeColor string
 - nationality string
 - issuingCountry string
 - personalNumber string
 - birthDate string
 - idType string
 - rawResponse object
 - id string

- transactionStatus object
 - status string
- verifiedUserData object
 - firstName string
 - lastName string
 - middleName string
 - gender string
 - expirationDate string
 - idNumber string
 - addressStreet string
 - addressCity string
 - addressState string
 - addressZip string
 - country string
 - issueDate string
 - weight string
 - height string
 - hairColor string
 - eyeColor string
 - nationality string
 - issuingCountry string
 - personalNumber string
 - birthDate string
 - idType string
- headers object
- statusCode integer

Read Government ID

Read verified data parsed off the government ID images

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - `governmentID` object
 - `_embedded` object
 - `verifiedData` array
 - `size` number
 - `rawResponse` object
 - `_embedded` object
 - `verifiedData` array
 - `size` number
 - `headers` object
 - `statusCode` integer

Read Verified Data

Read Verified Data

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

attempt textField

Limit the number verified attempts. Valid values (ALL, LATEST, 1, 2, 3, 4)

Verified Type(s) dropDownMultiSelect

Selected Verified data type(s)

- Selfie
- Government ID
- Front Image
- Back Image
- Barcode
- Cropped Portrait
- Cropped Document
- Cropped Signature
- Voice Sample
- Voice Input
- End User Client

Input Schema

- default object
 - properties object
 - userId string required
Verified Type
 - transactionId string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - verifiedData object
 - _embedded object
 - verifiedData array
 - size number
 - rawResponse object
 - _embedded object
 - verifiedData array
 - size number
 - headers object
 - statusCode integer

Read Selfie

Read selfie provided by the user

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - selfie object
 - `_embedded` object
 - `verifiedData` array
 - `size` number
 - `rawResponse` object
 - `_embedded` object
 - `verifiedData` array
 - `size` number
 - `headers` object
 - `statusCode` integer

Read Metadata

Read metadata related to verification

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Metadata Type dropDown

Type of the metadata. Select ALL to get all metadata.

- LIVENESS
- FACIAL_COMPARISON
- BIOGRAPHIC_MATCH
- DOCUMENT_AUTHENTICATION
- DOCUMENT_MANUAL_AUTHENTICATION
- VOICE_ENROLLMENT
- VOICE_VERIFICATION

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
User ID
 - transactionId string required minLength: 0 maxLength: 100
Transaction ID
 - metadataType string
metadata type

Output Schema

- output object
 - metaData object
 - _embedded object
 - metaData array
 - size number
 - rawResponse object
 - _embedded object
 - metaData array
 - size number
 - headers object
 - statusCode integer

Read Verify Policy

Read verify policy for verification

Properties

Verify Policy dropDown

Name of the verify policy.

- Use Verify Policy ID (Default)

Verify Policy ID textField

ID of the verify policy.

Input Schema

- default object
 - properties object
 - verifyPolicySelect string required minLength: 0 maxLength: 100
verify policy
 - verifyPolicyIdSelect string minLength: 0 maxLength: 100
verify policy ID

Output Schema

- output object
 - verifyPolicy object
 - id string
 - environment object
 - id string
 - name string
 - description string
 - default boolean
 - governmentId object
 - verify string
 - facialComparison object
 - verify string
 - threshold string
 - liveness object
 - verify string
 - threshold string
 - email object
 - verify string
 - createMfaDevice boolean
 - otp object
 - attempts object
 - count number
 - lifeTime object
 - duration number
 - timeUnit object
 - deliveries object
 - count number
 - cooldown object
 - duration number

- timeUnit string
- notification object
 - templateName string
 - variantName string
- phone object
 - verify string
 - createMfaDevice boolean
 - otp object
 - attempts object
 - count number
 - lifeTime object
 - duration number
 - timeUnit object
 - deliveries object
 - count number
 - cooldown object
 - duration number
 - timeUnit string
 - notification object
 - templateName string
 - variantName string
 - createdAt string
 - updatedAt boolean
 - rawResponse object
 - id string
 - environment object
 - id string
 - name string
 - description string
 - default boolean

- governmentId object
 - verify string
- facialComparison object
 - verify string
 - threshold string
- liveness object
 - verify string
 - threshold string
- email object
 - verify string
 - createMfaDevice boolean
 - otp object
 - attempts object
 - count number
 - lifeTime object
 - duration number
 - timeUnit object
 - deliveries object
 - count number
 - cooldown object
 - duration number
 - timeUnit string
 - notification object
 - templateName string
 - variantName string
- phone object
 - verify string
 - createMfaDevice boolean

- otp object
 - attempts object
 - count number
 - lifeTime object
 - duration number
 - timeUnit object
 - deliveries object
 - count number
 - cooldown object
 - duration number
 - timeUnit string
 - notification object
 - templateName string
 - variantName string
- createdAt string
- updatedAt boolean
- headers object
- statusCode integer

Set Verify Status

Set verify status for user

Properties

User ID textField

ID of the user

Verify Status dropDown

Verify status of the user to be set.

- ENABLED (Default)
- DISABLED
- NOT_INITIATED

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
User ID
 - verifyStatus string required
verify status

Output Schema

- output object
 - verifyStatus object
 - verifyStatus string
 - rawResponse object
 - verifyStatus string
 - headers object
 - statusCode integer

Return All Collected Data

Return all data collected from the user.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Document Types dropDownMultiSelect

Types of the data collected. The document types accepted are determined by the transaction's policy requirements.

- Driver License Front
- Driver License Back
- Driver License Code
- Passport Front
- Passport Card Front
- Passport Card Back
- Selfie
- Phone
- Email
- Voice Sample
- Voice Input

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `documentTypes` array uniqueItems: true
document types

Output Schema

- output object
 - documents object
 - `_embedded` object
 - documents array
 - size number
 - rawResponse object
 - `_embedded` object
 - documents array
 - size number
 - headers object
 - statusCode integer

Read Collected Data

Return a piece of data collected from the user.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Document ID textField

ID of the data collected from user.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `documentId` string required minLength: 0 maxLength: 100
document ID

Output Schema

- output object
 - document object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - headers object
 - statusCode integer

Submit Collected Data

Submit a piece of data collected from the user during verification.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Document Type dropDown

Type of the data collected. The document types accepted are determined by the transaction's policy requirements.

- Driver License Front (Default)
- Driver License Back
- Driver License Code
- Passport Front
- Passport Card Front
- Passport Card Back
- Selfie
- Phone
- Email
- Voice Sample
- Voice Input

Voice Sample Index textField

voice sample index starting from 1.

Document Value textField

Base64 encoded jpeg or textual data collected from user.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `documentTypeName` string required minLength: 0 maxLength: 255
document type
 - `voiceSampleIndex` integer
voice sample index starting from 1
 - `documentValue` string required
base64 encoded jpeg or textual document depending on document type

Output Schema

- output object
 - document object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - headers object
 - statusCode integer

Update Collected Data

Update a piece of data collected from the user.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Document ID textField

ID of the data collected from user.

Document Type dropDown

Type of the data collected. The document types accepted are determined by the transaction's policy requirements.

- Driver License Front (Default)
- Driver License Back
- Driver License Code
- Passport Front
- Passport Card Front
- Passport Card Back
- Selfie
- Phone
- Email
- Voice Sample
- Voice Input

Document Value textField

Base64 encoded jpeg or textual data collected from user.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `documentId` string required minLength: 0 maxLength: 100
document ID
 - `documentTypeName` string required minLength: 0 maxLength: 255
document type
 - `documentValue` string required
base64 encoded jpeg or textual document depending on document type

Output Schema

- output object
 - document object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - rawResponse object
 - id string
 - environment object
 - id string
 - user object
 - id string
 - verifyTransaction object
 - id string
 - type string
 - value string
 - status string
 - source object
 - provider string
 - headers object
 - statusCode integer

Delete Collected Data

Delete a piece of data collected from the user.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Document ID textField

ID of the data collected from user.

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `documentId` string required minLength: 0 maxLength: 100
document ID

Output Schema

- output object
 - `rawResponse` object
 - `headers` object
 - `statusCode` integer

Process All Data Collected

Process all data collected from the user during verification.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID

Output Schema

- output object
 - documents object
 - _embedded object
 - documents array
 - size number
 - rawResponse object
 - _embedded object
 - documents array
 - size number
 - headers object
 - statusCode integer

Create Response for External Client

Create JSON response for an integration with a mobile application.

Properties

Web Verification URL textField

web verification url

Challenge textField

Required challenge. To be added to the output for polling in subsequent step.

Is Last Client Step toggleSwitch

If isLastClientStep is false, the continueLink will be generated and added to the output, otherwise the link will not be added.

Input Schema

- default object
 - properties object
 - webVerificationUrl string required
web verification url
 - challengeId string required minLength: 1 maxLength: 100
challenge Id
 - isLastClientStep boolean
If isLastClientStep is false, the continueLink will be generated and added to the output, otherwise the link will not be added.

Output Schema

- output object
 - clientState string
 - webVerificationUrl string
 - continueLink string
 - challenge string

Replace Background

Reshape the background of a selfie image.

Properties

User ID textField

ID of the user

Transaction ID textField

ID of the transaction

Selfie ID textField

ID of the selfie

colorPicker colorPicker

Select color.

Aspect Width textField

Width of the aspect ratio

Aspect Height textField

Height of the aspect ratio

Input Schema

- default object
 - properties object
 - `userId` string required minLength: 0 maxLength: 100
User ID
 - `transactionId` string required minLength: 0 maxLength: 100
Transaction ID
 - `selfId` string minLength: 0 maxLength: 100
Selfie ID
 - `colorPicker` string
Color Picker
 - `aspectHeight` integer minimum: 1 maximum: 1000
Aspect ratio height
 - `aspectWidth` integer minimum: 1 maximum: 1000
Aspect ratio width

Output Schema

- output object
 - backgroundReplace object
 - id string
 - type string
 - data object
 - IMAGE string
 - FORMAT string
 - createdAt string
 - rawResponse object
 - id string
 - type string
 - data object
 - IMAGE string
 - FORMAT string
 - createdAt string
 - headers object
 - statusCode integer

Identity Record Matching

Identity Record Matching.

Properties

User ID textField

ID of the user

Biographic Fields selectNameValueListColumn

Use this section to add biographic fields

- Given Name
- Family Name
- Name
- Address
- Birthdate

Probe Biographic Fields selectNameValueListColumn

Use this section to add probe biographic fields

- Given Name
- Family Name
- Name
- Address
- Birthdate

Input Schema

- default object
 - properties object
 - userId string required minLength: 0 maxLength: 100
User ID
 - biographic array required
Probe Biographic Info

Output Schema

- output object
 - matchingResults object
 - detailedResults object
 - address object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - birth_date object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - given_name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - family_name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - overallWeightedScore number

- overallConfidenceScore string
- rawResponse object
 - detailedResults object
 - address object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - birth_date object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - given_name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - family_name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - name object
 - probeValue string
 - galleryValue string
 - rawScore number
 - confidence string
 - overallWeightedScore number
 - overallConfidenceScore string

- headers object
- statusCode integer

Troubleshooting

The following resources can help you solve issues with the connector.

Solutions

The flow fails with no error message

Ensure that the application is enabled in PingOne. Learn more in [Enabling or disabling an application](#).

The flow fails when reading or updating a user

Ensure that you are using the PingOne `user ID` attribute, not the `username` attribute.

Resources

Audit

You can use the audit log to identify potential issues. Learn more in [Audit](#).

Testing capabilities

Testing your flows frequently is the key to making them work correctly. Learn more in [Getting Started with DaVinci](#).

S-U



Salesforce Connector

The Salesforce connector lets you manage users and records in Salesforce from your PingOne DaVinci flows.



SAML IdP Connector

The SAML IdP connector lets you authenticate users with a SAML IdP-based identity provider in your PingOne DaVinci flow.



Screen Connector

The Screen connector lets you display forms and customized UI to retrieve information from a user or show flow progress in your PingOne DaVinci flow.



SecurID Connector

The SecurID connector lets you use RSA SecurID for multi-factor authentication (MFA) in your PingOne DaVinci flow.



SEON Connector

The SEON connector lets you uncover fraud patterns through SEON's device fingerprinting and intelligent insights in your PingOne DaVinci flow.



ServiceNow Connector

The ServiceNow connector lets you manage users, group memberships, and incidents in ServiceNow from your PingOne DaVinci flow.



Socure Connector

The Socure connector lets you verify identity documents and get fraud scores in your PingOne DaVinci flows.



Splunk Connector

The Splunk connector lets you gain real-time operational intelligence through Splunk in your PingOne DaVinci flow.



String Connector

The String connector lets you transform the text value of a variable in your PingOne DaVinci flow.



Teleport Connector

The Teleport connector lets you visually organize and subdivide a flow within your PingOne DaVinci flow canvas.



Token Management Connector

The Token Management connector lets you create and read JWT tokens and manage OpenID Connect 1.0 redirects in your PingOne DaVinci flow.



TransUnion TLOxp Connector

The TransUnion TLOxp connector lets you verify a user's identity information in your PingOne DaVinci flow by checking TransUnion's trusted data sources.

Salesforce Connector

The Salesforce connector lets you manage users and records in Salesforce from your PingOne DaVinci flows.

You can use the Salesforce connector to:

- Read, create, and update users.
- Read, update, and search records.
- Upload documents.
- Set up a custom API call to Salesforce.

Setup

Resources

For information and setup help, see the following:

- Salesforce:
 - [Quick Start](#)
 - [OAuth 2.0 JWT Bearer Flow for Server-to-Server Integration](#)
 - [User fields](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A Salesforce administrator account
- Your Salesforce access and connected app information:
 - Username
 - Salesforce domain name

Setting up Salesforce

To configure the Salesforce environment to use the Salesforce connector in DaVinci:

1. Sign on to a Salesforce production, developer, or sandbox account.
2. Create a new application to tie to the Salesforce connector:
 1. In the **Platform Tools** section, click **App Manager**.
 2. Click **New Connected App**.
 3. Complete the required fields for app name, API name, and contact email.

Note

You must enter a valid email. This is required for multi-factor authentication (MFA) when performing sensitive operations like looking at the **Client ID** and **Secret**.

4. For **Call back URL**, enter `https://oauth.pingone.com/ocs/ppm/rest/v1/oauth/oastempcredresponse/` to approve the application to the administrative user later.

 Note

This URL is required for the Salesforce administrator to approve the application later.

3. Create a certificate that will act as a digital signature for the Salesforce connector:

1. Follow the steps to create a certificate in the [Salesforce DX Developer Guide](#) or use your own if you already have one.
2. Select the **Use digital signature** check box and then select your **Public Key** from the previous step.
3. For **Selected OAuth Scopes**, select **Manage user data via APIs (api)**.

 Note

Ensure that the **Require Secret for Web Server Flow** and **Require Secret for Refresh Token Flow** boxes are selected.

4. Save the application.

5. Approve the application:

 Note

The Salesforce connector requires a Salesforce administrator account. The specified administrator must approve the application.

1. Select **App Manager** and find the application that you created.
2. In the drop-down list, select **View**.
3. To get the **Consumer Key** and **Secret**, click **Manage Consumer Details**, then **Open**.
4. Enter the one-time passcode (OTP) value from your email in the **Verification Code** field, then click **Verify**.
5. Open an incognito or private browser session and go to the PingOne OAuth configuration service.
6. In the drop-down list, select **Salesforce Production Connector** or **Salesforce Sandbox Connector**.

 Note

If you are using a Salesforce developer account, select the **Salesforce Production Connector** option.

7. Copy the **Consumer Key** and **Secret** from the Salesforce application details window in the **Client ID** and **Client Secret** fields in the PingOne OAuth configuration service, then click **Connect**.
8. Sign on and approve the application.

 Note

Be sure to sign on with the administrator account that will use the Salesforce connector.

6. In DaVinci, add a Salesforce connector to your flow.

7. Click **Configure** and complete the following fields:

Username

The administrator email used to approve the OAuth application.

Consumer Key

The consumer key that you created for your connected app in Salesforce. This can be found under **Manage Consumer Details** in your Salesforce environment.

Private Key

The consumer key that you created to set up JSON Web Token (JWT) Bearer authentication in Salesforce.

Domain Name

Your Salesforce domain name, such as `mycompany-dev-ed`. Leave off the `.my.salesforce.com` or `.lightning.force.com`. If your Salesforce account does not have a domain name, you must set one up. For more information, see [Custom Domains](#) in the Salesforce documentation.

Using the connector in a flow

User management

The connector has several capabilities that allow you to manage users:

- Read User
- Create User
- Update User

No special configuration is needed. Add the capability and populate its properties according to the help text.

Record management

The connector has several capabilities that allow you to manage records:

- Read Record
- Search Record
- Update Record

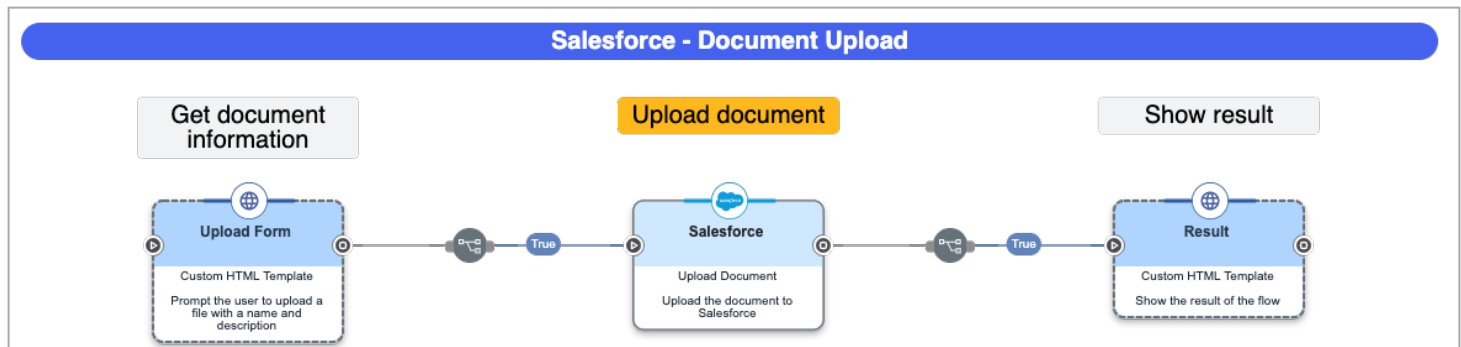
No special configuration is needed. Add the capability and populate its properties according to the help text.



Tip

For help building a query for the **Search Record** capability, see [Salesforce Object Query Language](#) in the Salesforce documentation.

Document upload



This flow allows the user to upload a document, such as an image or PDF, to Salesforce.

1. Download the [Salesforce - Document upload](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the file upload form.

The screenshot shows a web form titled "Upload a document" with the Ping Identity logo at the top. Below the title is the instruction "Select a file to upload to Salesforce.".

The form contains the following elements:

- A text input field labeled "Document Name".
- A text input field labeled "Description".
- A "Browse..." button next to a text field that says "No file selected."
- A large blue "Upload" button at the bottom.

1. Select the **Upload Form** node.
2. In the **HTML Template** field, customize the page that users see when signing on.

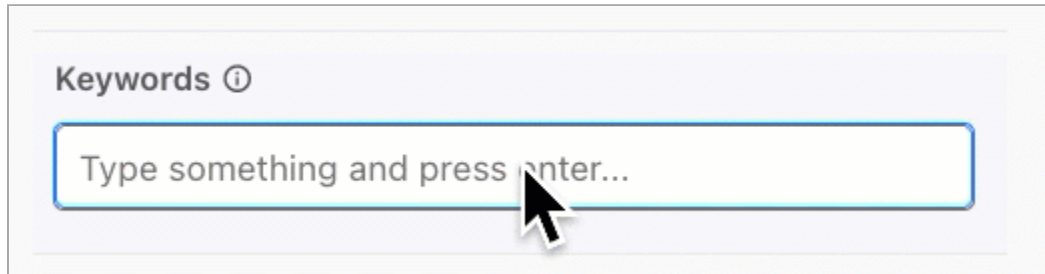
Tip

- Click **Switch View** to see the HTML formatted with syntax highlighting.
- Click the **Maximize** (☐) icon to give yourself more room to work.
- To access a variety of useful tools, right-click the field when you're in syntax highlighting mode (dark background).

3. Click **Apply**.

3. Customize the file upload destination and keywords:

1. Select the **Upload Document** node.
2. (Optional) In the **Name** and **Description** fields, customize the values.
3. In the **Folder** list, select the destination Salesforce folder. If the folder you want isn't listed, select **Use Custom Folder ID** and enter the ID, such as `0018a000002XKVQAA4`, in the **Custom Folder ID** field.
4. (Optional) In the **Keywords** field, enter the searchable tags to associate with the documents in Salesforce. Enter a keyword and press Enter to add it.



5. (Optional) Add additional field information in the **Document Fields** section by adding Salesforce fields and assigning values.

6. Click **Apply**.

4. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Create User

Create a new user.

Properties

Username textField required

The user's sign-on username, such as "[jsmith@example.com](#)". Must be in the form of an email address, using all lowercase characters. It must also be unique across all organizations.

First Name textField

The user's first name.

Last Name textField required

The user's last name.

Email textField required

The user's email address.

Alias textField required

The user's alias.

Email Encoding dropDown required

The email encoding for the user, such as ISO-8859-1 or UTF-8.

- Unicode (UTF-8) (Default)
- General US & Western Europe (ISO-8859-1, ISO-LATIN-1)
- Japanese (Shift-JIS)
- Japanese (JIS)
- Japanese (EUC)
- Korean (ks_c_5601-1987)
- Traditional Chinese (Big5)
- Simplified Chinese (GB2312)
- Traditional Chinese Hong Kong (Big5-HKSCS)
- Japanese (Shift-JIS_2004)

Profile dropDown required

Profiles contain settings and permissions, which control what users can do. Displays up to 100 results. If the profile you want is not listed, select Use Profile ID.

- Use Profile ID (Default)

Profile ID textField required

The ID of the user's profile, such as "00e8a0000024zkIAAA".

Timezone dropDown required

The user's timezone.

- (GMT+14:00) Line Islands Time (Pacific/Kiritimati)
- (GMT+13:00) Apia Standard Time (Pacific/Apia)
- (GMT+14:00) Apia Daylight Time (Pacific/Apia)
- (GMT+13:00) Phoenix Islands Time (Pacific/Enderbury)
- (GMT+13:00) Tokelau Time (Pacific/Fakaofu)
- (GMT+13:00) Tonga Standard Time (Pacific/Tongatapu)
- (GMT+12:45) Chatham Standard Time (Pacific/Chatham)
- (GMT+13:45) Chatham Daylight Time (Pacific/Chatham)
- (GMT+12:00) New Zealand Standard Time (Antarctica/McMurdo)
- (GMT+13:00) New Zealand Daylight Time (Antarctica/McMurdo)
- (GMT+12:00) Anadyr Standard Time (Asia/Anadyr)
- (GMT+12:00) Petropavlovsk-Kamchatski Standard Time (Asia/Kamchatka)
- (GMT+12:00) New Zealand Standard Time (Pacific/Auckland)
- (GMT+13:00) New Zealand Daylight Time (Pacific/Auckland)
- (GMT+12:00) Fiji Standard Time (Pacific/Fiji)
- (GMT+13:00) Fiji Summer Time (Pacific/Fiji)
- (GMT+12:00) Tuvalu Time (Pacific/Funafuti)
- (GMT+12:00) Marshall Islands Time (Pacific/Kwajalein)
- (GMT+12:00) Marshall Islands Time (Pacific/Majuro)
- (GMT+12:00) Nauru Time (Pacific/Nauru)
- (GMT+12:00) Gilbert Islands Time (Pacific/Tarawa)
- (GMT+12:00) Wake Island Time (Pacific/Wake)
- (GMT+12:00) Wallis & Futuna Time (Pacific/Wallis)
- (GMT+11:00) Casey Time (Antarctica/Casey)
- (GMT+11:00) Magadan Standard Time (Asia/Magadan)
- (GMT+11:00) Sakhalin Standard Time (Asia/Sakhalin)
- (GMT+11:00) Magadan Standard Time (Asia/Srednekolymsk)
- (GMT+11:00) Bougainville Standard Time (Pacific/Bougainville)

- (GMT+11:00) Vanuatu Standard Time (Pacific/Efate)
- (GMT+11:00) Solomon Islands Time (Pacific/Guadalcanal)
- (GMT+11:00) Kosrae Time (Pacific/Kosrae)
- (GMT+11:00) Norfolk Island Standard Time (Pacific/Norfolk)
- (GMT+12:00) Norfolk Island Daylight Time (Pacific/Norfolk)
- (GMT+11:00) New Caledonia Standard Time (Pacific/Noumea)
- (GMT+11:00) Ponape Time (Pacific/Ponape)
- (GMT+10:30) Lord Howe Standard Time (Australia/Lord_Howe)
- (GMT+11:00) Lord Howe Daylight Time (Australia/Lord_Howe)
- (GMT+10:00) Dumont-d'Urville Time (Antarctica/DumontDUrville)
- (GMT+10:00) Australian Eastern Standard Time (Antarctica/Macquarie)
- (GMT+11:00) Australian Eastern Daylight Time (Antarctica/Macquarie)
- (GMT+10:00) Vladivostok Standard Time (Asia/Ust-Nera)
- (GMT+10:00) Vladivostok Standard Time (Asia/Vladivostok)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Brisbane)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Currie)
- (GMT+11:00) Australian Eastern Daylight Time (Australia/Currie)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Hobart)
- (GMT+11:00) Australian Eastern Daylight Time (Australia/Hobart)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Lindeman)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Melbourne)
- (GMT+11:00) Australian Eastern Daylight Time (Australia/Melbourne)
- (GMT+10:00) Australian Eastern Standard Time (Australia/Sydney)
- (GMT+11:00) Australian Eastern Daylight Time (Australia/Sydney)
- (GMT+10:00) Chamorro Standard Time (Pacific/Guam)
- (GMT+10:00) Papua New Guinea Time (Pacific/Port_Moresby)
- (GMT+10:00) Chamorro Standard Time (Pacific/Saipan)
- (GMT+10:00) Chuuk Time (Pacific/Truk)
- (GMT+09:30) Australian Central Standard Time (Australia/Adelaide)
- (GMT+10:30) Australian Central Daylight Time (Australia/Adelaide)

- (GMT+09:30) Australian Central Standard Time (Australia/Broken_Hill)
- (GMT+10:30) Australian Central Daylight Time (Australia/Broken_Hill)
- (GMT+09:30) Australian Central Standard Time (Australia/Darwin)
- (GMT+09:00) Yakutsk Standard Time (Asia/Chita)
- (GMT+09:00) East Timor Time (Asia/Dili)
- (GMT+09:00) Eastern Indonesia Time (Asia/Jayapura)
- (GMT+09:00) Yakutsk Standard Time (Asia/Khandyga)
- (GMT+09:00) Korean Standard Time (Asia/Pyongyang)
- (GMT+09:00) Korean Standard Time (Asia/Seoul)
- (GMT+09:00) Japan Standard Time (Asia/Tokyo)
- (GMT+09:00) Yakutsk Standard Time (Asia/Yakutsk)
- (GMT+09:00) Palau Time (Pacific/Palau)
- (GMT+08:45) Australian Central Western Standard Time (Australia/Eucla)
- (GMT+08:00) Brunei Darussalam Time (Asia/Brunei)
- (GMT+08:00) Ulaanbaatar Standard Time (Asia/Choibalsan)
- (GMT+08:00) Hong Kong Standard Time (Asia/Hong_Kong)
- (GMT+08:00) Irkutsk Standard Time (Asia/Irkutsk)
- (GMT+08:00) Malaysia Time (Asia/Kuala_Lumpur)
- (GMT+08:00) Malaysia Time (Asia/Kuching)
- (GMT+08:00) China Standard Time (Asia/Macau)
- (GMT+08:00) Central Indonesia Time (Asia/Makassar)
- (GMT+08:00) Philippine Standard Time (Asia/Manila)
- (GMT+08:00) China Standard Time (Asia/Shanghai)
- (GMT+08:00) Singapore Standard Time (Asia/Singapore)
- (GMT+08:00) Taipei Standard Time (Asia/Taipei)
- (GMT+08:00) Ulaanbaatar Standard Time (Asia/Ulaanbaatar)
- (GMT+08:00) Australian Western Standard Time (Australia/Perth)
- (GMT+07:00) Davis Time (Antarctica/Davis)
- (GMT+07:00) Indochina Time (Asia/Bangkok)
- (GMT+07:00) Moscow Standard Time + 4 (Asia/Barnaul)

- (GMT+07:00) Indochina Time (Asia/Ho_Chi_Minh)
- (GMT+07:00) Hovd Standard Time (Asia/Hovd)
- (GMT+07:00) Western Indonesia Time (Asia/Jakarta)
- (GMT+07:00) Krasnoyarsk Standard Time (Asia/Krasnoyarsk)
- (GMT+07:00) Krasnoyarsk Standard Time (Asia/Novokuznetsk)
- (GMT+07:00) Novosibirsk Standard Time (Asia/Novosibirsk)
- (GMT+07:00) Indochina Time (Asia/Phnom_Penh)
- (GMT+07:00) Western Indonesia Time (Asia/Pontianak)
- (GMT+07:00) Moscow Standard Time + 4 (Asia/Tomsk)
- (GMT+07:00) Indochina Time (Asia/Vientiane)
- (GMT+07:00) Christmas Island Time (Indian/Christmas)
- (GMT+06:30) Myanmar Time (Asia/Rangoon)
- (GMT+06:30) Cocos Islands Time (Indian/Cocos)
- (GMT+06:00) Vostok Time (Antarctica/Vostok)
- (GMT+06:00) East Kazakhstan Time (Asia/Almaty)
- (GMT+06:00) Kyrgyzstan Time (Asia/Bishkek)
- (GMT+06:00) Bangladesh Standard Time (Asia/Dhaka)
- (GMT+06:00) Omsk Standard Time (Asia/Omsk)
- (GMT+06:00) East Kazakhstan Time (Asia/Qostanay)
- (GMT+06:00) Bhutan Time (Asia/Thimphu)
- (GMT+06:00) China Standard Time (Asia/Urumqi)
- (GMT+06:00) Indian Ocean Time (Indian/Chagos)
- (GMT+05:45) Nepal Time (Asia/Kathmandu)
- (GMT+05:30) India Standard Time (Asia/Colombo)
- (GMT+05:30) India Standard Time (Asia/Kolkata)
- (GMT+05:00) Mawson Time (Antarctica/Mawson)
- (GMT+05:00) West Kazakhstan Time (Asia/Aqtau)
- (GMT+05:00) West Kazakhstan Time (Asia/Aqtobe)
- (GMT+05:00) Turkmenistan Standard Time (Asia/Ashgabat)
- (GMT+05:00) West Kazakhstan Time (Asia/Atyrau)

- (GMT+05:00) Tajikistan Time (Asia/Dushanbe)
- (GMT+05:00) Pakistan Standard Time (Asia/Karachi)
- (GMT+05:00) West Kazakhstan Time (Asia/Oral)
- (GMT+05:00) West Kazakhstan Time (Asia/Qyzylorda)
- (GMT+05:00) Uzbekistan Standard Time (Asia/Samarkand)
- (GMT+05:00) Uzbekistan Standard Time (Asia/Tashkent)
- (GMT+05:00) Yekaterinburg Standard Time (Asia/Yekaterinburg)
- (GMT+05:00) French Southern & Antarctic Time (Indian/Kerguelen)
- (GMT+05:00) Maldives Time (Indian/Maldives)
- (GMT+04:30) Afghanistan Time (Asia/Kabul)
- (GMT+04:00) Azerbaijan Standard Time (Asia/Baku)
- (GMT+04:00) Gulf Standard Time (Asia/Dubai)
- (GMT+04:00) Gulf Standard Time (Asia/Muscat)
- (GMT+04:00) Georgia Standard Time (Asia/Tbilisi)
- (GMT+04:00) Armenia Standard Time (Asia/Yerevan)
- (GMT+04:00) Samara Standard Time (Europe/Astrakhan)
- (GMT+04:00) Samara Standard Time (Europe/Samara)
- (GMT+04:00) Moscow Standard Time + 1 (Europe/Saratov)
- (GMT+04:00) Moscow Standard Time + 1 (Europe/Ulyanovsk)
- (GMT+04:00) Seychelles Time (Indian/Mahe)
- (GMT+04:00) Mauritius Standard Time (Indian/Mauritius)
- (GMT+04:00) Réunion Time (Indian/Reunion)
- (GMT+03:30) Iran Standard Time (Asia/Tehran)
- (GMT+04:30) Iran Daylight Time (Asia/Tehran)
- (GMT+03:00) East Africa Time (Africa/Addis_Ababa)
- (GMT+03:00) East Africa Time (Africa/Asmera)
- (GMT+03:00) East Africa Time (Africa/Dar_es_Salaam)
- (GMT+03:00) East Africa Time (Africa/Djibouti)
- (GMT+03:00) East Africa Time (Africa/Kampala)
- (GMT+03:00) East Africa Time (Africa/Mogadishu)

- (GMT+03:00) East Africa Time (Africa/Nairobi)
- (GMT+03:00) Syowa Time (Antarctica/Syowa)
- (GMT+03:00) Arabian Standard Time (Asia/Aden)
- (GMT+03:00) Arabian Standard Time (Asia/Baghdad)
- (GMT+03:00) Arabian Standard Time (Asia/Bahrain)
- (GMT+03:00) Arabian Standard Time (Asia/Kuwait)
- (GMT+03:00) Arabian Standard Time (Asia/Qatar)
- (GMT+03:00) Arabian Standard Time (Asia/Riyadh)
- (GMT+03:00) Eastern European Standard Time (Europe/Istanbul)
- (GMT+03:00) Moscow Standard Time (Europe/Kirov)
- (GMT+03:00) Moscow Standard Time (Europe/Minsk)
- (GMT+03:00) Moscow Standard Time (Europe/Moscow)
- (GMT+03:00) Moscow Standard Time (Europe/Simferopol)
- (GMT+03:00) Volgograd Standard Time (Europe/Volgograd)
- (GMT+03:00) East Africa Time (Indian/Antananarivo)
- (GMT+03:00) East Africa Time (Indian/Comoro)
- (GMT+03:00) East Africa Time (Indian/Mayotte)
- (GMT+02:00) Central Africa Time (Africa/Blantyre)
- (GMT+02:00) Central Africa Time (Africa/Bujumbura)
- (GMT+02:00) Eastern European Standard Time (Africa/Cairo)
- (GMT+02:00) Central Africa Time (Africa/Gaborone)
- (GMT+02:00) Central Africa Time (Africa/Harare)
- (GMT+02:00) South Africa Standard Time (Africa/Johannesburg)
- (GMT+02:00) Central Africa Time (Africa/Juba)
- (GMT+02:00) Central Africa Time (Africa/Khartoum)
- (GMT+02:00) Central Africa Time (Africa/Kigali)
- (GMT+02:00) Central Africa Time (Africa/Lubumbashi)
- (GMT+02:00) Central Africa Time (Africa/Lusaka)
- (GMT+02:00) Central Africa Time (Africa/Maputo)
- (GMT+02:00) South Africa Standard Time (Africa/Maseru)

- (GMT+02:00) South Africa Standard Time (Africa/Mbabane)
- (GMT+02:00) Eastern European Standard Time (Africa/Tripoli)
- (GMT+02:00) Central Africa Time (Africa/Windhoek)
- (GMT+02:00) Eastern European Standard Time (Asia/Amman)
- (GMT+03:00) Eastern European Summer Time (Asia/Amman)
- (GMT+02:00) Eastern European Standard Time (Asia/Beirut)
- (GMT+03:00) Eastern European Summer Time (Asia/Beirut)
- (GMT+02:00) Eastern European Standard Time (Asia/Damascus)
- (GMT+03:00) Eastern European Summer Time (Asia/Damascus)
- (GMT+02:00) Eastern European Standard Time (Asia/Famagusta)
- (GMT+03:00) Eastern European Summer Time (Asia/Famagusta)
- (GMT+02:00) Eastern European Standard Time (Asia/Gaza)
- (GMT+03:00) Eastern European Summer Time (Asia/Gaza)
- (GMT+02:00) Eastern European Standard Time (Asia/Hebron)
- (GMT+03:00) Eastern European Summer Time (Asia/Hebron)
- (GMT+02:00) Israel Standard Time (Asia/Jerusalem)
- (GMT+03:00) Israel Daylight Time (Asia/Jerusalem)
- (GMT+02:00) Eastern European Standard Time (Asia/Nicosia)
- (GMT+03:00) Eastern European Summer Time (Asia/Nicosia)
- (GMT+02:00) Eastern European Standard Time (Europe/Athens)
- (GMT+03:00) Eastern European Summer Time (Europe/Athens)
- (GMT+02:00) Eastern European Standard Time (Europe/Bucharest)
- (GMT+03:00) Eastern European Summer Time (Europe/Bucharest)
- (GMT+02:00) Eastern European Standard Time (Europe/Chisinau)
- (GMT+03:00) Eastern European Summer Time (Europe/Chisinau)
- (GMT+02:00) Eastern European Standard Time (Europe/Helsinki)
- (GMT+03:00) Eastern European Summer Time (Europe/Helsinki)
- (GMT+02:00) Eastern European Standard Time (Europe/Kaliningrad)
- (GMT+02:00) Eastern European Standard Time (Europe/Kiev)
- (GMT+03:00) Eastern European Summer Time (Europe/Kiev)

- (GMT+02:00) Eastern European Standard Time (Europe/Mariehamn)
- (GMT+03:00) Eastern European Summer Time (Europe/Mariehamn)
- (GMT+02:00) Eastern European Standard Time (Europe/Riga)
- (GMT+03:00) Eastern European Summer Time (Europe/Riga)
- (GMT+02:00) Eastern European Standard Time (Europe/Sofia)
- (GMT+03:00) Eastern European Summer Time (Europe/Sofia)
- (GMT+02:00) Eastern European Standard Time (Europe/Tallinn)
- (GMT+03:00) Eastern European Summer Time (Europe/Tallinn)
- (GMT+02:00) Eastern European Standard Time (Europe/Uzhgorod)
- (GMT+03:00) Eastern European Summer Time (Europe/Uzhgorod)
- (GMT+02:00) Eastern European Standard Time (Europe/Vilnius)
- (GMT+03:00) Eastern European Summer Time (Europe/Vilnius)
- (GMT+02:00) Eastern European Standard Time (Europe/Zaporozhye)
- (GMT+03:00) Eastern European Summer Time (Europe/Zaporozhye)
- (GMT+01:00) Central European Standard Time (Africa/Algiers)
- (GMT+01:00) West Africa Standard Time (Africa/Bangui)
- (GMT+01:00) West Africa Standard Time (Africa/Brazzaville)
- (GMT+01:00) Central European Standard Time (Africa/Ceuta)
- (GMT+02:00) Central European Summer Time (Africa/Ceuta)
- (GMT+01:00) West Africa Standard Time (Africa/Douala)
- (GMT+01:00) West Africa Standard Time (Africa/Kinshasa)
- (GMT+01:00) West Africa Standard Time (Africa/Lagos)
- (GMT+01:00) West Africa Standard Time (Africa/Libreville)
- (GMT+01:00) West Africa Standard Time (Africa/Luanda)
- (GMT+01:00) West Africa Standard Time (Africa/Malabo)
- (GMT+01:00) West Africa Standard Time (Africa/Ndjamena)
- (GMT+01:00) West Africa Standard Time (Africa/Niamey)
- (GMT+01:00) West Africa Standard Time (Africa/Porto-Novo)
- (GMT+01:00) Central European Standard Time (Africa/Tunis)
- (GMT+01:00) Central European Standard Time (Arctic/Longyearbyen)

- (GMT+02:00) Central European Summer Time (Arctic/Longyearbyen)
- (GMT+01:00) Central European Standard Time (Europe/Amsterdam)
- (GMT+02:00) Central European Summer Time (Europe/Amsterdam)
- (GMT+01:00) Central European Standard Time (Europe/Andorra)
- (GMT+02:00) Central European Summer Time (Europe/Andorra)
- (GMT+01:00) Central European Standard Time (Europe/Belgrade)
- (GMT+02:00) Central European Summer Time (Europe/Belgrade)
- (GMT+01:00) Central European Standard Time (Europe/Berlin)
- (GMT+02:00) Central European Summer Time (Europe/Berlin)
- (GMT+01:00) Central European Standard Time (Europe/Bratislava)
- (GMT+02:00) Central European Summer Time (Europe/Bratislava)
- (GMT+01:00) Central European Standard Time (Europe/Brussels)
- (GMT+02:00) Central European Summer Time (Europe/Brussels)
- (GMT+01:00) Central European Standard Time (Europe/Budapest)
- (GMT+02:00) Central European Summer Time (Europe/Budapest)
- (GMT+01:00) Central European Standard Time (Europe/Busingen)
- (GMT+02:00) Central European Summer Time (Europe/Busingen)
- (GMT+01:00) Central European Standard Time (Europe/Copenhagen)
- (GMT+02:00) Central European Summer Time (Europe/Copenhagen)
- (GMT+01:00) Central European Standard Time (Europe/Gibraltar)
- (GMT+02:00) Central European Summer Time (Europe/Gibraltar)
- (GMT+01:00) Central European Standard Time (Europe/Ljubljana)
- (GMT+02:00) Central European Summer Time (Europe/Ljubljana)
- (GMT+01:00) Central European Standard Time (Europe/Luxembourg)
- (GMT+02:00) Central European Summer Time (Europe/Luxembourg)
- (GMT+01:00) Central European Standard Time (Europe/Madrid)
- (GMT+02:00) Central European Summer Time (Europe/Madrid)
- (GMT+01:00) Central European Standard Time (Europe/Malta)
- (GMT+02:00) Central European Summer Time (Europe/Malta)
- (GMT+01:00) Central European Standard Time (Europe/Monaco)

- (GMT+02:00) Central European Summer Time (Europe/Monaco)
- (GMT+01:00) Central European Standard Time (Europe/Oslo)
- (GMT+02:00) Central European Summer Time (Europe/Oslo)
- (GMT+01:00) Central European Standard Time (Europe/Paris)
- (GMT+02:00) Central European Summer Time (Europe/Paris)
- (GMT+01:00) Central European Standard Time (Europe/Podgorica)
- (GMT+02:00) Central European Summer Time (Europe/Podgorica)
- (GMT+01:00) Central European Standard Time (Europe/Prague)
- (GMT+02:00) Central European Summer Time (Europe/Prague)
- (GMT+01:00) Central European Standard Time (Europe/Rome)
- (GMT+02:00) Central European Summer Time (Europe/Rome)
- (GMT+01:00) Central European Standard Time (Europe/San_Marino)
- (GMT+02:00) Central European Summer Time (Europe/San_Marino)
- (GMT+01:00) Central European Standard Time (Europe/Sarajevo)
- (GMT+02:00) Central European Summer Time (Europe/Sarajevo)
- (GMT+01:00) Central European Standard Time (Europe/Skopje)
- (GMT+02:00) Central European Summer Time (Europe/Skopje)
- (GMT+01:00) Central European Standard Time (Europe/Stockholm)
- (GMT+02:00) Central European Summer Time (Europe/Stockholm)
- (GMT+01:00) Central European Standard Time (Europe/Tirane)
- (GMT+02:00) Central European Summer Time (Europe/Tirane)
- (GMT+01:00) Central European Standard Time (Europe/Vaduz)
- (GMT+02:00) Central European Summer Time (Europe/Vaduz)
- (GMT+01:00) Central European Standard Time (Europe/Vatican)
- (GMT+02:00) Central European Summer Time (Europe/Vatican)
- (GMT+01:00) Central European Standard Time (Europe/Vienna)
- (GMT+02:00) Central European Summer Time (Europe/Vienna)
- (GMT+01:00) Central European Standard Time (Europe/Warsaw)
- (GMT+02:00) Central European Summer Time (Europe/Warsaw)
- (GMT+01:00) Central European Standard Time (Europe/Zagreb)

- (GMT+02:00) Central European Summer Time (Europe/Zagreb)
- (GMT+01:00) Central European Standard Time (Europe/Zurich)
- (GMT+02:00) Central European Summer Time (Europe/Zurich)
- (GMT+00:00) Greenwich Mean Time (Africa/Abidjan)
- (GMT+00:00) Greenwich Mean Time (Africa/Accra)
- (GMT+00:00) Greenwich Mean Time (Africa/Bamako)
- (GMT+00:00) Greenwich Mean Time (Africa/Banjul)
- (GMT+00:00) Greenwich Mean Time (Africa/Bissau)
- (GMT+00:00) Western European Standard Time (Africa/Casablanca)
- (GMT+01:00) Western European Summer Time (Africa/Casablanca)
- (GMT+00:00) Greenwich Mean Time (Africa/Conakry)
- (GMT+00:00) Greenwich Mean Time (Africa/Dakar)
- (GMT+00:00) Western European Standard Time (Africa/El_Aaiun)
- (GMT+01:00) Western European Summer Time (Africa/El_Aaiun)
- (GMT+00:00) Greenwich Mean Time (Africa/Freetown)
- (GMT+00:00) Greenwich Mean Time (Africa/Lome)
- (GMT+00:00) Greenwich Mean Time (Africa/Monrovia)
- (GMT+00:00) Greenwich Mean Time (Africa/Nouakchott)
- (GMT+00:00) Greenwich Mean Time (Africa/Ouagadougou)
- (GMT+00:00) Greenwich Mean Time (Africa/Sao_Tome)
- (GMT+00:00) Greenwich Mean Time (America/Danmarkshavn)
- (GMT+00:00) Greenwich Mean Time (Antarctica/Troll)
- (GMT+02:00) Central European Summer Time (Antarctica/Troll)
- (GMT+00:00) Western European Standard Time (Atlantic/Canary)
- (GMT+01:00) Western European Summer Time (Atlantic/Canary)
- (GMT+00:00) Western European Standard Time (Atlantic/Faeroe)
- (GMT+01:00) Western European Summer Time (Atlantic/Faeroe)
- (GMT+00:00) Western European Standard Time (Atlantic/Madeira)
- (GMT+01:00) Western European Summer Time (Atlantic/Madeira)
- (GMT+00:00) Greenwich Mean Time (Atlantic/Reykjavik)

- (GMT+00:00) Greenwich Mean Time (Atlantic/St_Helena)
- (GMT+00:00) Greenwich Mean Time (Europe/Dublin)
- (GMT+01:00) Irish Standard Time (Europe/Dublin)
- (GMT+00:00) Greenwich Mean Time (Europe/Guernsey)
- (GMT+01:00) British Summer Time (Europe/Guernsey)
- (GMT+00:00) Greenwich Mean Time (Europe/Isle_of_Man)
- (GMT+01:00) British Summer Time (Europe/Isle_of_Man)
- (GMT+00:00) Greenwich Mean Time (Europe/Jersey)
- (GMT+01:00) British Summer Time (Europe/Jersey)
- (GMT+00:00) Western European Standard Time (Europe/Lisbon)
- (GMT+01:00) Western European Summer Time (Europe/Lisbon)
- (GMT+00:00) Greenwich Mean Time (Europe/London)
- (GMT+01:00) British Summer Time (Europe/London)
- (GMT+00:00) Greenwich Mean Time GMT)
- (GMT-01:00) East Greenland Standard Time (America/Scoresbysund)
- (GMT+00:00) East Greenland Summer Time (America/Scoresbysund)
- (GMT-01:00) Azores Standard Time (Atlantic/Azores)
- (GMT+00:00) Azores Summer Time (Atlantic/Azores)
- (GMT-01:00) Cape Verde Standard Time (Atlantic/Cape_Verde)
- (GMT-02:00) Fernando de Noronha Standard Time (America/Noronha)
- (GMT-02:00) South Georgia Time (Atlantic/South_Georgia)
- (GMT-03:00) Brasilia Standard Time (America/Araguaina)
- (GMT-03:00) Argentina Standard Time (America/Argentina/Buenos_Aires)
- (GMT-03:00) Argentina Standard Time (America/Argentina/La_Rioja)
- (GMT-03:00) Argentina Standard Time (America/Argentina/Rio_Gallegos)
- (GMT-03:00) Argentina Standard Time (America/Argentina/Salta)
- (GMT-03:00) Argentina Standard Time (America/Argentina/San_Juan)
- (GMT-03:00) Argentina Standard Time (America/Argentina/San_Luis)
- (GMT-03:00) Argentina Standard Time (America/Argentina/Tucuman)
- (GMT-03:00) Argentina Standard Time (America/Argentina/Ushuaia)

- (GMT-03:00) Brasilia Standard Time (America/Bahia)
- (GMT-03:00) Brasilia Standard Time (America/Belem)
- (GMT-03:00) Argentina Standard Time (America/Catamarca)
- (GMT-03:00) French Guiana Time (America/Cayenne)
- (GMT-03:00) Argentina Standard Time (America/Cordoba)
- (GMT-03:00) Brasilia Standard Time (America/Fortaleza)
- (GMT-03:00) West Greenland Standard Time (America/Godthab)
- (GMT-02:00) West Greenland Summer Time (America/Godthab)
- (GMT-03:00) Argentina Standard Time (America/Jujuy)
- (GMT-03:00) Brasilia Standard Time (America/Maceio)
- (GMT-03:00) Argentina Standard Time (America/Mendoza)
- (GMT-03:00) St. Pierre & Miquelon Standard Time (America/Miquelon)
- (GMT-02:00) St. Pierre & Miquelon Daylight Time (America/Miquelon)
- (GMT-03:00) Uruguay Standard Time (America/Montevideo)
- (GMT-03:00) Suriname Time (America/Paramaribo)
- (GMT-03:00) Chile Standard Time (America/Punta_Arenas)
- (GMT-03:00) Brasilia Standard Time (America/Recife)
- (GMT-03:00) Brasilia Standard Time (America/Santarem)
- (GMT-03:00) Brasilia Standard Time (America/Sao_Paulo)
- (GMT-03:00) Chile Standard Time (Antarctica/Palmer)
- (GMT-03:00) Rothera Time (Antarctica/Rothera)
- (GMT-03:00) Falkland Islands Standard Time (Atlantic/Stanley)
- (GMT-03:30) Newfoundland Standard Time (America/St_Johns)
- (GMT-02:30) Newfoundland Daylight Time (America/St_Johns)
- (GMT-04:00) Atlantic Standard Time (America/Anguilla)
- (GMT-04:00) Atlantic Standard Time (America/Antigua)
- (GMT-04:00) Atlantic Standard Time (America/Aruba)
- (GMT-04:00) Paraguay Standard Time (America/Asuncion)
- (GMT-03:00) Paraguay Summer Time (America/Asuncion)
- (GMT-04:00) Atlantic Standard Time (America/Barbados)

- (GMT-04:00) Atlantic Standard Time (America/Blanc-Sablon)
- (GMT-04:00) Amazon Standard Time (America/Boa_Vista)
- (GMT-04:00) Amazon Standard Time (America/Campo_Grande)
- (GMT-04:00) Venezuela Time (America/Caracas)
- (GMT-04:00) Amazon Standard Time (America/Cuiaba)
- (GMT-04:00) Atlantic Standard Time (America/Curacao)
- (GMT-04:00) Atlantic Standard Time (America/Dominica)
- (GMT-04:00) Atlantic Standard Time (America/Glace_Bay)
- (GMT-03:00) Atlantic Daylight Time (America/Glace_Bay)
- (GMT-04:00) Atlantic Standard Time (America/Goose_Bay)
- (GMT-03:00) Atlantic Daylight Time (America/Goose_Bay)
- (GMT-04:00) Atlantic Standard Time (America/Grenada)
- (GMT-04:00) Atlantic Standard Time (America/Guadeloupe)
- (GMT-04:00) Guyana Time (America/Guyana)
- (GMT-04:00) Atlantic Standard Time (America/Halifax)
- (GMT-03:00) Atlantic Daylight Time (America/Halifax)
- (GMT-04:00) Atlantic Standard Time (America/Kralendijk)
- (GMT-04:00) Bolivia Time (America/La_Paz)
- (GMT-04:00) Atlantic Standard Time (America/Lower_Princes)
- (GMT-04:00) Amazon Standard Time (America/Manaus)
- (GMT-04:00) Atlantic Standard Time (America/Marigot)
- (GMT-04:00) Atlantic Standard Time (America/Martinique)
- (GMT-04:00) Atlantic Standard Time (America/Moncton)
- (GMT-03:00) Atlantic Daylight Time (America/Moncton)
- (GMT-04:00) Atlantic Standard Time (America/Montserrat)
- (GMT-04:00) Atlantic Standard Time (America/Port_of_Spain)
- (GMT-04:00) Amazon Standard Time (America/Porto_Velho)
- (GMT-04:00) Atlantic Standard Time (America/Puerto_Rico)
- (GMT-04:00) Chile Standard Time (America/Santiago)
- (GMT-03:00) Chile Summer Time (America/Santiago)

- (GMT-04:00) Atlantic Standard Time (America/Santo_Domingo)
- (GMT-04:00) Atlantic Standard Time (America/St_Barthelemy)
- (GMT-04:00) Atlantic Standard Time (America/St_Kitts)
- (GMT-04:00) Atlantic Standard Time (America/St_Lucia)
- (GMT-04:00) Atlantic Standard Time (America/St_Thomas)
- (GMT-04:00) Atlantic Standard Time (America/St_Vincent)
- (GMT-04:00) Atlantic Standard Time (America/Thule)
- (GMT-03:00) Atlantic Daylight Time (America/Thule)
- (GMT-04:00) Atlantic Standard Time (America/Tortola)
- (GMT-04:00) Atlantic Standard Time (Atlantic/Bermuda)
- (GMT-03:00) Atlantic Daylight Time (Atlantic/Bermuda)
- (GMT-05:00) Colombia Standard Time (America/Bogota)
- (GMT-05:00) Eastern Standard Time (America/Cancun)
- (GMT-05:00) Eastern Standard Time (America/Cayman)
- (GMT-05:00) Eastern Standard Time (America/Coral_Harbour)
- (GMT-05:00) Eastern Standard Time (America/Detroit)
- (GMT-04:00) Eastern Daylight Time (America/Detroit)
- (GMT-05:00) Acre Standard Time (America/Eirunepe)
- (GMT-05:00) Eastern Standard Time (America/Grand_Turk)
- (GMT-04:00) Eastern Daylight Time (America/Grand_Turk)
- (GMT-05:00) Ecuador Time (America/Guayaquil)
- (GMT-05:00) Cuba Standard Time (America/Havana)
- (GMT-04:00) Cuba Daylight Time (America/Havana)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Indianapolis)
- (GMT-04:00) Eastern Daylight Time (America/Indiana/Indianapolis)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Marengo)
- (GMT-04:00) Eastern Daylight Time (America/Indiana/Marengo)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Petersburg)
- (GMT-04:00) Eastern Daylight Time (America/Indiana/Petersburg)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Vevay)

- (GMT-04:00) Eastern Daylight Time (America/Indiana/Vevay)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Vincennes)
- (GMT-04:00) Eastern Daylight Time (America/Indiana/Vincennes)
- (GMT-05:00) Eastern Standard Time (America/Indiana/Winamac)
- (GMT-04:00) Eastern Daylight Time (America/Indiana/Winamac)
- (GMT-05:00) Eastern Standard Time (America/Iqaluit)
- (GMT-04:00) Eastern Daylight Time (America/Iqaluit)
- (GMT-05:00) Eastern Standard Time (America/Jamaica)
- (GMT-05:00) Eastern Standard Time (America/Kentucky/Monticello)
- (GMT-04:00) Eastern Daylight Time (America/Kentucky/Monticello)
- (GMT-05:00) Peru Standard Time (America/Lima)
- (GMT-05:00) Eastern Standard Time (America/Louisville)
- (GMT-04:00) Eastern Daylight Time (America/Louisville)
- (GMT-05:00) Eastern Standard Time (America/Montreal)
- (GMT-04:00) Eastern Daylight Time (America/Montreal)
- (GMT-05:00) Eastern Standard Time (America/Nassau)
- (GMT-04:00) Eastern Daylight Time (America/Nassau)
- (GMT-05:00) Eastern Standard Time (America/New_York) (Default)
- (GMT-04:00) Eastern Daylight Time (America/New_York) (Default)
- (GMT-05:00) Eastern Standard Time (America/Nipigon)
- (GMT-04:00) Eastern Daylight Time (America/Nipigon)
- (GMT-05:00) Eastern Standard Time (America/Panama)
- (GMT-05:00) Eastern Standard Time (America/Pangnirtung)
- (GMT-04:00) Eastern Daylight Time (America/Pangnirtung)
- (GMT-05:00) Eastern Standard Time (America/Port-au-Prince)
- (GMT-04:00) Eastern Daylight Time (America/Port-au-Prince)
- (GMT-05:00) Acre Standard Time (America/Rio_Branco)
- (GMT-05:00) Eastern Standard Time (America/Thunder_Bay)
- (GMT-04:00) Eastern Daylight Time (America/Thunder_Bay)
- (GMT-05:00) Eastern Standard Time (America/Toronto)

- (GMT-04:00) Eastern Daylight Time (America/Toronto)
- (GMT-06:00) Central Standard Time (America/Bahia_Banderas)
- (GMT-05:00) Central Daylight Time (America/Bahia_Banderas)
- (GMT-06:00) Central Standard Time (America/Belize)
- (GMT-06:00) Central Standard Time (America/Chicago)
- (GMT-05:00) Central Daylight Time (America/Chicago)
- (GMT-06:00) Central Standard Time (America/Costa_Rica)
- (GMT-06:00) Central Standard Time (America/El_Salvador)
- (GMT-06:00) Central Standard Time (America/Guatemala)
- (GMT-06:00) Central Standard Time (America/Indiana/Knox)
- (GMT-05:00) Central Daylight Time (America/Indiana/Knox)
- (GMT-06:00) Central Standard Time (America/Indiana/Tell_City)
- (GMT-05:00) Central Daylight Time (America/Indiana/Tell_City)
- (GMT-06:00) Central Standard Time (America/Managua)
- (GMT-06:00) Central Standard Time (America/Matamoros)
- (GMT-05:00) Central Daylight Time (America/Matamoros)
- (GMT-06:00) Central Standard Time (America/Menominee)
- (GMT-05:00) Central Daylight Time (America/Menominee)
- (GMT-06:00) Central Standard Time (America/Merida)
- (GMT-05:00) Central Daylight Time (America/Merida)
- (GMT-06:00) Central Standard Time (America/Mexico_City)
- (GMT-05:00) Central Daylight Time (America/Mexico_City)
- (GMT-06:00) Central Standard Time (America/Monterrey)
- (GMT-05:00) Central Daylight Time (America/Monterrey)
- (GMT-06:00) Central Standard Time (America/North_Dakota/Beulah)
- (GMT-05:00) Central Daylight Time (America/North_Dakota/Beulah)
- (GMT-06:00) Central Standard Time (America/North_Dakota/Center)
- (GMT-05:00) Central Daylight Time (America/North_Dakota/Center)
- (GMT-06:00) Central Standard Time (America/North_Dakota/New_Salem)
- (GMT-05:00) Central Daylight Time (America/North_Dakota/New_Salem)

- (GMT-06:00) Central Standard Time (America/Rainy_River)
- (GMT-05:00) Central Daylight Time (America/Rainy_River)
- (GMT-06:00) Central Standard Time (America/Rankin_Inlet)
- (GMT-05:00) Central Daylight Time (America/Rankin_Inlet)
- (GMT-06:00) Central Standard Time (America/Regina)
- (GMT-06:00) Central Standard Time (America/Resolute)
- (GMT-05:00) Central Daylight Time (America/Resolute)
- (GMT-06:00) Central Standard Time (America/Swift_Current)
- (GMT-06:00) Central Standard Time (America/Tegucigalpa)
- (GMT-06:00) Central Standard Time (America/Winnipeg)
- (GMT-05:00) Central Daylight Time (America/Winnipeg)
- (GMT-06:00) Easter Island Standard Time (Pacific/Easter)
- (GMT-05:00) Easter Island Summer Time (Pacific/Easter)
- (GMT-06:00) Galapagos Time (Pacific/Galapagos)
- (GMT-07:00) Mountain Standard Time (America/Boise)
- (GMT-06:00) Mountain Daylight Time (America/Boise)
- (GMT-07:00) Mountain Standard Time (America/Cambridge_Bay)
- (GMT-06:00) Mountain Daylight Time (America/Cambridge_Bay)
- (GMT-07:00) Mexican Pacific Standard Time (America/Chihuahua)
- (GMT-06:00) Mexican Pacific Daylight Time (America/Chihuahua)
- (GMT-07:00) Mountain Standard Time (America/Creston)
- (GMT-07:00) Mountain Standard Time (America/Dawson)
- (GMT-07:00) Mountain Standard Time (America/Dawson_Creek)
- (GMT-07:00) Mountain Standard Time (America/Denver)
- (GMT-06:00) Mountain Daylight Time (America/Denver)
- (GMT-07:00) Mountain Standard Time (America/Edmonton)
- (GMT-06:00) Mountain Daylight Time (America/Edmonton)
- (GMT-07:00) Mountain Standard Time (America/Fort_Nelson)
- (GMT-07:00) Mexican Pacific Standard Time (America/Hermosillo)
- (GMT-07:00) Mountain Standard Time (America/Inuvik)

- (GMT-06:00) Mountain Daylight Time (America/Inuvik)
- (GMT-07:00) Mexican Pacific Standard Time (America/Mazatlan)
- (GMT-06:00) Mexican Pacific Daylight Time (America/Mazatlan)
- (GMT-07:00) Mountain Standard Time (America/Ojinaga)
- (GMT-06:00) Mountain Daylight Time (America/Ojinaga)
- (GMT-07:00) Mountain Standard Time (America/Phoenix)
- (GMT-07:00) Mountain Standard Time (America/Whitehorse)
- (GMT-07:00) Mountain Standard Time (America/Yellowknife)
- (GMT-06:00) Mountain Daylight Time (America/Yellowknife)
- (GMT-08:00) Pacific Standard Time (America/Los_Angeles)
- (GMT-07:00) Pacific Daylight Time (America/Los_Angeles)
- (GMT-08:00) Northwest Mexico Standard Time (America/Santa_Isabel)
- (GMT-07:00) Northwest Mexico Daylight Time (America/Santa_Isabel)
- (GMT-08:00) Pacific Standard Time (America/Tijuana)
- (GMT-07:00) Pacific Daylight Time (America/Tijuana)
- (GMT-08:00) Pacific Standard Time (America/Vancouver)
- (GMT-07:00) Pacific Daylight Time (America/Vancouver)
- (GMT-08:00) Pitcairn Time (Pacific/Pitcairn)
- (GMT-09:00) Alaska Standard Time (America/Anchorage)
- (GMT-08:00) Alaska Daylight Time (America/Anchorage)
- (GMT-09:00) Alaska Standard Time (America/Juneau)
- (GMT-08:00) Alaska Daylight Time (America/Juneau)
- (GMT-09:00) Alaska Standard Time (America/Metlakatla)
- (GMT-08:00) Alaska Daylight Time (America/Metlakatla)
- (GMT-09:00) Alaska Standard Time (America/Nome)
- (GMT-08:00) Alaska Daylight Time (America/Nome)
- (GMT-09:00) Alaska Standard Time (America/Sitka)
- (GMT-08:00) Alaska Daylight Time (America/Sitka)
- (GMT-09:00) Alaska Standard Time (America/Yakutat)
- (GMT-08:00) Alaska Daylight Time (America/Yakutat)

- (GMT-09:00) Gambier Time (Pacific/Gambier)
- (GMT-09:30) Marquesas Time (Pacific/Marquesas)
- (GMT-10:00) Hawaii-Aleutian Standard Time (America/Adak)
- (GMT-09:00) Hawaii-Aleutian Daylight Time (America/Adak)
- (GMT-10:00) Hawaii-Aleutian Standard Time (Pacific/Honolulu)
- (GMT-10:00) Hawaii-Aleutian Standard Time (Pacific/Johnston)
- (GMT-10:00) Cook Islands Standard Time (Pacific/Rarotonga)
- (GMT-10:00) Tahiti Time (Pacific/Tahiti)
- (GMT-11:00) Samoa Standard Time (Pacific/Midway)
- (GMT-11:00) Niue Time (Pacific/Niue)
- (GMT-11:00) Samoa Standard Time (Pacific/Pago_Pago)

Locale dropDown required

The user's locale.

- Afrikaans (South Africa)
- Amharic (Ethiopia)
- Arabic (United Arab Emirates)
- Arabic (Bahrain)
- Arabic (Algeria)
- Arabic (Egypt)
- Arabic (Iraq)
- Arabic (Jordan)
- Arabic (Kuwait)
- Arabic (Lebanon)
- Arabic (Libya)
- Arabic (Morocco)
- Arabic (Oman)
- Arabic (Qatar)
- Arabic (Saudi Arabia)
- Arabic (Sudan)
- Arabic (Syria)

- Arabic (Tunisia)
- Arabic (Yemen)
- Azerbaijani (Azerbaijan)
- Belarusian (Belarus)
- Bulgarian (Bulgaria)
- Bangla (Bangladesh)
- Bangla (India)
- Bosnian (Bosnia & Herzegovina)
- Catalan (Spain)
- Catalan (Spain,Euro)
- Czech (Czechia)
- Welsh (United Kingdom)
- Danish (Denmark)
- German (Austria)
- German (Austria,Euro)
- German (Belgium)
- German (Switzerland)
- German (Germany)
- German (Germany,Euro)
- German (Luxembourg)
- German (Luxembourg,Euro)
- Dzongkha (Bhutan)
- Greek (Cyprus)
- Greek (Greece)
- English (United Arab Emirates)
- English (Antigua & Barbuda)
- English (Australia)
- English (Barbados)
- English (Belgium)
- English (Bermuda)

- English (Bahamas)
- English (Botswana)
- English (Belize)
- English (Canada)
- English (Cameroon)
- English (Cyprus)
- English (Germany)
- English (Eritrea)
- English (Fiji)
- English (Falkland Islands)
- English (United Kingdom)
- English (Ghana)
- English (Gibraltar)
- English (Gambia)
- English (Guyana)
- English (Hong Kong SAR China)
- English (Indonesia)
- English (Ireland)
- English (Ireland,Euro)
- English (Israel)
- English (India)
- English (Jamaica)
- English (Kenya)
- English (Cayman Islands)
- English (Liberia)
- English (Madagascar)
- English (Malta)
- English (Mauritius)
- English (Malawi)
- English (Malaysia)

- English (Namibia)
- English (Nigeria)
- English (Netherlands)
- English (New Zealand)
- English (Papua New Guinea)
- English (Philippines)
- English (Pakistan)
- English (Rwanda)
- English (Solomon Islands)
- English (Seychelles)
- English (Singapore)
- English (St. Helena)
- English (Sierra Leone)
- English (Sint Maarten)
- English (Eswatini)
- English (Tonga)
- English (Trinidad & Tobago)
- English (Tanzania)
- English (Uganda)
- English (United States) (Default)
- English (Vanuatu)
- English (Samoa)
- English (South Africa)
- Spanish (Argentina)
- Spanish (Bolivia)
- Spanish (Chile)
- Spanish (Colombia)
- Spanish (Costa Rica)
- Spanish (Cuba)
- Spanish (Dominican Republic)

- Spanish (Ecuador)
- Spanish (Spain)
- Spanish (Spain,Euro)
- Spanish (Guatemala)
- Spanish (Honduras)
- Spanish (Mexico)
- Spanish (Nicaragua)
- Spanish (Panama)
- Spanish (Peru)
- Spanish (Puerto Rico)
- Spanish (Paraguay)
- Spanish (El Salvador)
- Spanish (United States)
- Spanish (Uruguay)
- Spanish (Venezuela)
- Estonian (Estonia)
- Basque (Spain)
- Persian (Iran)
- Finnish (Finland)
- Finnish (Finland,Euro)
- French (Belgium)
- French (Canada)
- French (Switzerland)
- French (France)
- French (France,Euro)
- French (Guinea)
- French (Haiti)
- French (Comoros)
- French (Luxembourg)
- French (Morocco)

- French (Monaco)
- French (Mauritania)
- French (Wallis & Futuna)
- Irish (Ireland)
- Gujarati (India)
- Hawaiian (United States)
- Hindi (India)
- Hmong (United States)
- Croatian (Croatia)
- Haitian Creole (Haiti)
- Haitian Creole (United States)
- Hungarian (Hungary)
- Armenian (Armenia)
- Indonesian (Indonesia)
- Icelandic (Iceland)
- Italian (Switzerland)
- Italian (Italy)
- Hebrew (Israel)
- Japanese (Japan)
- Yiddish (United States)
- Georgian (Georgia)
- Kazakh (Kazakhstan)
- Kalaallisut (Greenland)
- Khmer (Cambodia)
- Kannada (India)
- Korean (North Korea)
- Korean (South Korea)
- Kyrgyz (Kyrgyzstan)
- Luxembourgish (Luxembourg)
- Lao (Laos)

- Lithuanian (Lithuania)
- Luba-Katanga (Congo - Kinshasa)
- Latvian (Latvia)
- Te reo (New Zealand)
- Macedonian (North Macedonia)
- Malayalam (India)
- Marathi (India)
- Malay (Brunei)
- Malay (Malaysia)
- Maltese (Malta)
- Burmese (Myanmar (Burma))
- Nepali (Nepal)
- Dutch (Aruba)
- Dutch (Belgium)
- Dutch (Netherlands)
- Dutch (Suriname)
- Norwegian (Norway)
- Punjabi (India)
- Polish (Poland)
- Pashto (Afghanistan)
- Portuguese (Angola)
- Portuguese (Brazil)
- Portuguese (Cape Verde)
- Portuguese (Mozambique)
- Portuguese (Portugal)
- Portuguese (São Tomé & Príncipe)
- Romansh (Switzerland)
- Rundi (Burundi)
- Romanian (Moldova)
- Romanian (Romania)

- Russian (Armenia)
- Russian (Belarus)
- Russian (Kyrgyzstan)
- Russian (Kazakhstan)
- Russian (Lithuania)
- Russian (Moldova)
- Russian (Poland)
- Russian (Russia)
- Russian (Ukraine)
- Serbian (Latin) (Bosnia and Herzegovina)
- Serbian (Latin) (Serbia)
- Montenegrin (Montenegro)
- Montenegrin (Montenegro, USD)
- Slovak (Slovakia)
- Slovenian (Slovenia)
- Samoan (United States)
- Samoan (Samoa)
- Somali (Djibouti)
- Somali (Somalia)
- Albanian (Albania)
- Serbian (Cyrillic) (Bosnia and Herzegovina)
- Serbian (Cyrillic) (Serbia)
- Serbian (Serbia)
- Swedish (Sweden)
- Swahili (Kenya)
- Tamil (India)
- Tamil (Sri Lanka)
- Telugu (India)
- Tajik (Tajikistan)
- Thai (Thailand)

- Tigrinya (Ethiopia)
- Tagalog (Philippines)
- Turkish (Turkey)
- Ukrainian (Ukraine)
- Urdu (Pakistan)
- Uzbek (LATN,UZ)
- Vietnamese (Vietnam)
- Xhosa (South Africa)
- Yoruba (Benin)
- Chinese (China)
-
-
- Chinese (Hong Kong SAR China)
- ()
- Chinese (Macao SAR China)
- Chinese (Malaysia)
- Chinese (Singapore)
- Chinese (Taiwan)
- ()
- Zulu (South Africa)

Language dropDown required

The user’s language, such as French or Chinese (Traditional).

- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- Dutch
- English (Default)
- Finnish
- French
- German

- Italian
- Japanese
- Korean
- Norwegian
- Portuguese (Brazil)
- Russian
- Spanish
- Spanish (Mexico)
- Swedish
- Thai

User Fields variableInputList

Add user fields and their values.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - username string required
Username
 - firstName string
First Name
 - lastName string required
Last Name
 - email string required
Email
 - alias string required
Alias
 - emailEncodingKey string required
Email Encoding
 - profile string required
Profile
 - profileId string
Profile ID
 - timeZoneSidKey string required
Timezone
 - localeSidKey string required

Locale

- languageLocaleKey string required

Language

- userFieldsCreate array

User Fields

Output Schema

- output object
 - rawResponse object
 - id string
 - success boolean
 - errors array
 - statusCode number
 - headers object
 - id string

Read User

Get information about a user.

Properties

User ID textField required

The unique ID of the user, such as "0058a00000LYDB8AAP".

Fields textFieldArrayView

Specifies which field values to get for the user. Leave this blank to get all fields.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - userId string required
User ID
 - userFieldsRead array
Fields

Output Schema

- output object
 - rawResponse object
 - attributes object
 - type string
 - url string
 - Id string
 - Username string
 - LastName string
 - FirstName string
 - Name string
 - CompanyName string
 - Division string
 - Department string
 - Title string
 - Street string
 - City string
 - State string
 - PostalCode string
 - Country string
 - Latitude number
 - Longitude number
 - GeocodeAccuracy string
 - Address object
 - city string
 - country string
 - geocodeAccuracy string
 - latitude number
 - longitude number
 - postalCode string

- state string
- street string
- Email string
- EmailPreferencesAutoBcc boolean
- EmailPreferencesAutoBccStayInTouch boolean
- EmailPreferencesStayInTouchReminder boolean
- SenderEmail string
- SenderName string
- Signature string
- StayInTouchSubject string
- StayInTouchSignature string
- StayInTouchNote string
- Phone string
- Fax string
- MobilePhone string
- Alias string
- CommunityNickname string
- BadgeText string
- IsActive boolean
- TimeZoneSidKey string
- UserRoleId string
- LocaleSidKey string
- ReceivesInfoEmails boolean
- ReceivesAdminInfoEmails boolean
- EmailEncodingKey string
- ProfileId string
- UserType string
- LanguageLocaleKey string
- EmployeeNumber string
- DelegatedApproverId string

- ManagerId string
- LastLoginDate string
- LastPasswordChangeDate string
- CreatedDate string
- CreatedById string
- LastModifiedDate string
- LastModifiedById string
- SystemModstamp string
- NumberOfFailedLogins integer
- OfflineTrialExpirationDate string
- OfflinePdaTrialExpirationDate string
- UserPermissionsMarketingUser boolean
- UserPermissionsOfflineUser boolean
- UserPermissionsCallCenterAutoLogin boolean
- UserPermissionsSFContentUser boolean
- UserPermissionsKnowledgeUser boolean
- UserPermissionsInteractionUser boolean
- UserPermissionsSupportUser boolean
- UserPermissionsJigsawProspectingUser boolean
- UserPermissionsSiteforceContributorUser boolean
- UserPermissionsSiteforcePublisherUser boolean
- UserPermissionsWorkDotComUserFeature boolean
- ForecastEnabled boolean
- UserPreferencesActivityRemindersPopup boolean
- UserPreferencesEventRemindersCheckboxDefault boolean
- UserPreferencesTaskRemindersCheckboxDefault boolean
- UserPreferencesReminderSoundOff boolean
- UserPreferencesDisableAllFeedsEmail boolean
- UserPreferencesDisableFollowersEmail boolean
- UserPreferencesDisableProfilePostEmail boolean

- UserPreferencesDisableChangeCommentEmail boolean
- UserPreferencesDisableLaterCommentEmail boolean
- UserPreferencesDisProfPostCommentEmail boolean
- UserPreferencesContentNoEmail boolean
- UserPreferencesContentEmailAsAndWhen boolean
- UserPreferencesApexPagesDeveloperMode boolean
- UserPreferencesReceiveNoNotificationsAsApprover boolean
- UserPreferencesReceiveNotificationsAsDelegatedApprover boolean
- UserPreferencesHideCSNGetChatterMobileTask boolean
- UserPreferencesDisableMentionsPostEmail boolean
- UserPreferencesDisMentionsCommentEmail boolean
- UserPreferencesHideCSNDesktopTask boolean
- UserPreferencesHideChatterOnboardingSplash boolean
- UserPreferencesHideSecondChatterOnboardingSplash boolean
- UserPreferencesDisCommentAfterLikeEmail boolean
- UserPreferencesDisableLikeEmail boolean
- UserPreferencesSortFeedByComment boolean
- UserPreferencesDisableMessageEmail boolean
- UserPreferencesHideLegacyRetirementModal boolean
- UserPreferencesJigsawListUser boolean
- UserPreferencesDisableBookmarkEmail boolean
- UserPreferencesDisableSharePostEmail boolean
- UserPreferencesEnableAutoSubForFeeds boolean
- UserPreferencesDisableFileShareNotificationsForApi boolean
- UserPreferencesShowTitleToExternalUsers boolean
- UserPreferencesShowManagerToExternalUsers boolean
- UserPreferencesShowEmailToExternalUsers boolean
- UserPreferencesShowWorkPhoneToExternalUsers boolean
- UserPreferencesShowMobilePhoneToExternalUsers boolean
- UserPreferencesShowFaxToExternalUsers boolean

- UserPreferencesShowStreetAddressToExternalUsers boolean
- UserPreferencesShowCityToExternalUsers boolean
- UserPreferencesShowStateToExternalUsers boolean
- UserPreferencesShowPostalCodeToExternalUsers boolean
- UserPreferencesShowCountryToExternalUsers boolean
- UserPreferencesShowProfilePicToGuestUsers boolean
- UserPreferencesShowTitleToGuestUsers boolean
- UserPreferencesShowCityToGuestUsers boolean
- UserPreferencesShowStateToGuestUsers boolean
- UserPreferencesShowPostalCodeToGuestUsers boolean
- UserPreferencesShowCountryToGuestUsers boolean
- UserPreferencesShowForecastingChangeSignals boolean
- UserPreferencesHideS1BrowserUI boolean
- UserPreferencesDisableEndorsementEmail boolean
- UserPreferencesPathAssistantCollapsed boolean
- UserPreferencesCacheDiagnostics boolean
- UserPreferencesShowEmailToGuestUsers boolean
- UserPreferencesShowManagerToGuestUsers boolean
- UserPreferencesShowWorkPhoneToGuestUsers boolean
- UserPreferencesShowMobilePhoneToGuestUsers boolean
- UserPreferencesShowFaxToGuestUsers boolean
- UserPreferencesShowStreetAddressToGuestUsers boolean
- UserPreferencesLightningExperiencePreferred boolean
- UserPreferencesPreviewLightning boolean
- UserPreferencesHideEndUserOnboardingAssistantModal boolean
- UserPreferencesHideLightningMigrationModal boolean
- UserPreferencesHideSfxWelcomeMat boolean
- UserPreferencesHideBiggerPhotoCallout boolean
- UserPreferencesGlobalNavBarWTShown boolean
- UserPreferencesGlobalNavGridMenuWTShown boolean

- UserPreferencesCreateLEXAppsWTShown boolean
- UserPreferencesFavoritesWTShown boolean
- UserPreferencesRecordHomeSectionCollapseWTShown boolean
- UserPreferencesRecordHomeReservedWTShown boolean
- UserPreferencesFavoritesShowTopFavorites boolean
- UserPreferencesExcludeMailAppAttachments boolean
- UserPreferencesSuppressTaskSFXReminders boolean
- UserPreferencesSuppressEventSFXReminders boolean
- UserPreferencesPreviewCustomTheme boolean
- UserPreferencesHasCelebrationBadge boolean
- UserPreferencesUserDebugModePref boolean
- UserPreferencesSRHOverrideActivities boolean
- UserPreferencesNewLightningReportRunPageEnabled boolean
- UserPreferencesReverseOpenActivitiesView boolean
- UserPreferencesShowTerritoryTimeZoneShifts boolean
- UserPreferencesHasSentWarningEmail boolean
- UserPreferencesNativeEmailClient boolean
- ContactId string
- AccountId string
- CallCenterId string
- Extension string
- FederationIdentifier string
- AboutMe string
- FullPhotoUrl string
- SmallPhotoUrl string
- IsExtIndicatorVisible boolean
- OutOfOfficeMessage string
- MediumPhotoUrl string
- DigestFrequency string
- DefaultGroupNotificationFrequency string

- JigsawImportLimitOverride integer
- LastViewedDate string
- LastReferencedDate string
- BannerPhotoUrl string
- SmallBannerPhotoUrl string
- MediumBannerPhotoUrl string
- IsProfilePhotoActive boolean
- IndividualId string
- statusCode number
- headers object

Update User

Update information for a user.

Properties

User ID textField required

The unique ID of the user, such as "0058a00000LYDB8AAP".

User Fields variableInputList

Add the user fields that you want to update and provide their values.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - userId string required
User ID
 - userFieldsUpdate array required
User Fields

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

Read Record

Get information about a record.

Properties

Object Type textField required

The type of standard or custom object, such as "User", "Lead", or "Document".

Record ID textField required

The unique ID of the record, such as "0058a00000LYDB8AAP".

Fields textFieldArrayView

Specifies which field values to get for the record. Leave this blank to get all fields.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - objectType string required
Object Type
 - recordId string required
Record ID
 - recordFieldsRead array
Fields

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

Update Record

Update information in a record.

Properties

Object Type textField required

The type of standard or custom object, such as "User", "Lead", or "Document".

Record ID textField required

The unique ID of the record, such as "0058a00000LYDB8AAP".

Record Fields variableInputList

Add the record fields that you want to update and provide their values.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - objectType string required
Object Type
 - recordId string required
Record ID
 - recordFieldsUpdate array required
Object Fields

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

Search Record

Query records using SOQL.

Properties

SOQL Query textArea

Enter a query using Salesforce Object Query Language, such as "SELECT FirstName from User WHERE Id = '0058a00000Ky3eP'".

Next Records URL textField

If you expect more than 2000 results, connect multiple Search Record nodes in series. In each node, populate the Next Records URL field with the Next Records URL variable from the previous node.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - query string
Query
 - nextRecordsUrl string
Next Records URL

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object
 - nextRecordsUrl string

Upload Document

Upload a new document.

Properties

Name textField required

The name of the document.

File textField required

Base64-encoded file data.

Folder dropDown required

The folder that contains the document. Displays up to 100 results. If the folder you want is not listed, select Use Folder ID.

- Use Folder ID (Default)

Folder ID textField required

The ID of the folder that contains the document, such as "0018a000002XKVQAA4".

Description textField

A text description of the document.

Keywords textFieldArrayView

Searchable keywords to associate with the document. Type a keyword and press Enter to add it.

Document Fields variableInputList

Add document fields and their values.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - documentName string required
Document Name
 - file string required
File
 - documentFolder string required
Document Folder
 - documentFolderId string
Document Folder ID
 - documentDescription string
Document Description
 - documentKeywords array
Document Keywords
 - documentFields array
Document Fields

Output Schema

- output object
 - rawResponse object
 - id string
 - success boolean
 - errors array
 - statusCode number
 - headers object
 - id string

Make Custom API Call

Define a custom API call to Salesforce.

Properties

Endpoint textField required

The Salesforce API endpoint, such as `/services/data/v54.0/subjects/User`.

Method dropDown required

The HTTP Method.

- GET
- POST
- PUT
- DELETE
- PATCH

Query Parameters keyValuePairList

Add query parameters and provide their values.

Headers keyValuePairList

Add HTTP headers and provide their values.

Body codeEditor

The raw JSON body, such as `{ "Username": "jsmith@example.com", "ProfileId": "00e8a0000024zkjAAA" }`.

Input Schema

- default object
 - properties object
 - adminUsername string required
Username
 - consumerKey string required
Consumer Key
 - privateKey string required
Private Key
 - domainName string required
Domain Name
 - endpoint string required
Endpoint
 - method string required
Method
 - queryParameters array
Query Parameters
 - headers array
Headers
 - body object
Body

Output Schema

- output object
 - rawResponse object
 - statusCode number
 - headers object

SAML IdP Connector

The Security Assertion Markup Language (SAML) IdP connector lets you authenticate users with a SAML IdP-based identity provider in your PingOne DaVinci flow.

SAML 2.0 is a well-supported standard for authentication and authorization. You can use this connector to show a customizable sign-on button that allows your users to authenticate with your organization's SAML IdP identity provider.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need administrator access to your identity provider's SAML IdP configuration.

Configuring the SAML IdP connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration



Note

Consult your identity provider's documentation for help finding and configuring your SAML IdP settings.

DaVinci SAML SP Metadata URL

Your DaVinci SAML IdP SP Metadata URL. This allows an identity provider to redirect the browser back to DaVinci. Enter this URL in your provider's SAML IdP configuration.

Identity Provider SAML Metadata

This field accepts the SAML IdP metadata provided by your identity provider. This information should be available in your identity provider's SAML IdP configuration.

 Note

The connector does not support the following in the **Identity Provider SAML Metadata** field:

- The `md:` prefix, which is associated with the SAML Metadata specification
- The `ds:` prefix, which is associated with the XML Digital Signature specification
- The `xmlns` attribute in the `EntityDescriptor`, which is associated with XML Namespace.

Application Redirect URL

Your application's redirect URL, such as <https://app.yourorganization.com/>. Enter this URL if you [embed the DaVinci widget in your application](#). This allows DaVinci to redirect the browser back to your application.

Using the connector in a flow

Authenticating users

The **Sign On with SAML Identity Provider** capability lets you show a customizable sign-on button in your flow. When a user clicks this button, the connector sends a SAML authentication request to your configured SAML provider.

You can configure standard SAML parameters, such as `relayState` and `notBeforeSkew`. For help with these, consult your preferred SAML documentation.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Sign On with SAML Identity Provider

Authenticate the user with an identity provider that supports SAML.

Properties

Display Name button

signRequest toggleSwitch

When enabled, DaVinci signs the SAML request using the X.509 certificate. The certificate is provided to the identity provider through the DaVinci SAML SP Metadata URL, which is available in the connector settings.

nameIdFormat dropDown

Select the name format used by the identity provider.

Force Authentication toggleSwitch

When enabled, the user must re-authenticate even if they have an existing session. Enable this for high-value and high-risk transactions.

Authentication Context Class Reference textArea

The Context Class Reference to use for the transaction, such as "{ \"comparison\": \"exact\", \"class_refs\": [\"urn:oasis:names:tc:SAML:2.0:ac:classes:Password\"] }\". This allows you to define the type of authentication required for the transaction.

requireSessionIndex toggleSwitch

When enabled, a unique session identifier is carried through the authentication process and allows DaVinci to identify the user's session. Enable this for improved security.

Allow Unencrypted Assertions toggleSwitch

When enabled, DaVinci accepts SAML assertions from the identity provider that are not encrypted. Only enable this for low-risk transactions in an environment where encryption is not possible.

RelayState Parameter textField

Optional information to include when sending the SAML request to the identity provider, formatted as a URL. This information is included in the response from the identity provider.

Audience Parameter textField

The audience value to provide in the SAML request, such as "https://sp.example.com". This value must match one of the audiences listed in the SAML assertion. When this field is blank, the connector uses the DaVinci entity ID.

NotBeforeSkew Parameter textField

The allowable difference in time between when a SAML assertion becomes valid and the current time, in seconds. Use this to accommodate for differences in clock time between systems.

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Output Schema

- output object
 - rawResponse object
 - response_header object
 - version string
 - destination string
 - in_response_to string
 - id string
 - type string
 - user object
 - name_id string
 - session_index string
 - given_name string
 - surname string
 - email string
 - name string
 - attributes object
 - tenantid string
 - objectidentifier string
 - displayname string
 - identityprovider string
 - authnmethodsreferences array
 - givenname string
 - surname string
 - emailaddress string
 - name string

Output Example

```
{ "rawResponse" :
  { "response_header" :
    { "version" : "2.0",
      "destination" : "https://devapi.singularkey.com/auth/i7Ln1NrP7eFpLTNxw7fMTHb/saml2/assert",
      "in_response_to" : "_fa95d1e27c6adf712baaf3d875eb4b21b4cb28940c",
      "id" : "_d7d681de-d33f-4e01-9bdf-49ec28eaa63b" },
      "type" : "authn_response",
      "user" :
        { "name_id" : "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com",
          "session_index" : "_d093086e-36bc-4dfd-b9eb-23d97032b800",
          "given_name" : "joe@singularkey.com",
          "surname" : "Smith",
          "email" : "joe@singularkey.com",
          "name" : "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com",
          "attributes" :
            { "tenantid" : "06d45dd3-d5ac-498c-bf2c-78b17e619b3e",
              "objectidentifier" : "e48b41d4-7f30-4bec-a071-19ce0528adaf",
              "displayname" : "joe@singularkey.com Smith",
              "identityprovider" : "live.com",
              "authnmethodsreferences" :
                [ "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
                  "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/unspecified" ],
              "givenname" : "joe@singularkey.com",
              "surname" : "Smith",
              "emailaddress" : "joe@singularkey.com",
              "name" :
                "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com" } } } }
```

Sign On with SAML Identity Provider (Dynamic)

Authenticate the user with an identity provider that supports SAML. Use a different connector based on a variable from the flow.

Properties

Display Name button

ID of SAML IdP Connection textField

The ID of another DaVinci SAML connector instance, such as "f33f64e40bcf79c2ce86ad0dcc563457". Populate this with a variable to dynamically change which SAML connector is used based on the context of the flow.

signRequest toggleSwitch

When enabled, DaVinci signs the SAML request using the X.509 certificate. The certificate is provided to the identity provider through the DaVinci SAML SP Metadata URL, which is available in the connector settings.

RelayState Parameter textField

Optional information to include when sending the SAML request to the identity provider, formatted as a URL. This information is included in the response from the identity provider.

nameIdFormat dropDown

Select the name format used by the identity provider.

Force Authentication toggleSwitch

When enabled, the user must re-authenticate even if they have an existing session. Enable this for high-value and high-risk transactions.

Authentication Context Class Reference textArea

The Context Class Reference to use for the transaction, such as "{ \"comparison\": \"exact\", \"class_refs\": [\"urn:oasis:names:tc:SAML:2.0:ac:classes:Password\"] }\". This allows you to define the type of authentication required for the transaction.

requireSessionIndex toggleSwitch

When enabled, a unique session identifier is carried through the authentication process and allows DaVinci to identify the user's session. Enable this for improved security.

Allow Unencrypted Assertions toggleSwitch

When enabled, DaVinci accepts SAML assertions from the identity provider that are not encrypted. Only enable this for low-risk transactions in an environment where encryption is not possible.

Audience Parameter textField

The audience value to provide in the SAML request, such as "https://sp.example.com". This value must match one of the audiences listed in the SAML assertion. When this field is blank, the connector uses the DaVinci entity ID.

NotBeforeSkew Parameter textField

The allowable difference in time between when a SAML assertion becomes valid and the current time, in seconds. Use this to accommodate for differences in clock time between systems.

showPoweredBy toggleSwitch
skipButtonPress toggleSwitch

Output Schema

- output object
 - rawResponse object
 - response_header object
 - version string
 - destination string
 - in_response_to string
 - id string
 - type string
 - user object
 - name_id string
 - session_index string
 - given_name string
 - surname string
 - email string
 - name string
 - attributes object
 - tenantid string
 - objectidentifier string
 - displayname string
 - identityprovider string
 - authnmethodsreferences array
 - givenname string
 - surname string
 - emailaddress string
 - name string

Output Example

```
{ "rawResponse" :
  { "response_header" :
    { "version" : "2.0",
      "destination" : "https://devapi.singularkey.com/auth/i7Ln1NrP7eFpLTNxw7fMTHb/saml2/assert",
      "in_response_to" : "_fa95d1e27c6adf712baaf3d875eb4b21b4cb28940c",
      "id" : "_d7d681de-d33f-4e01-9bdf-49ec28eaa63b" },
      "type" : "authn_response",
      "user" :
        { "name_id" : "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com",
          "session_index" : "_d093086e-36bc-4dfd-b9eb-23d97032b800",
          "given_name" : "joe@singularkey.com",
          "surname" : "Smith",
          "email" : "joe@singularkey.com",
          "name" : "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com",
          "attributes" :
            { "tenantid" : "06d45dd3-d5ac-498c-bf2c-78b17e619b3e",
              "objectidentifier" : "e48b41d4-7f30-4bec-a071-19ce0528adaf",
              "displayname" : "joe@singularkey.com Smith",
              "identityprovider" : "live.com",
              "authnmethodsreferences" :
                [ "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
                  "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/unspecified" ],
              "givenname" : "joe@singularkey.com",
              "surname" : "Smith",
              "emailaddress" : "joe@singularkey.com",
              "name" :
                "joe_singularkey.com#EXT#_joesingularkey.onmicrosYPBIZ#EXT#@singularkeyb2c.onmicrosoft.com" } } } }
```

Screen Connector

The Screen connector lets you display forms and customized UI to retrieve information from a user or show flow progress in your PingOne DaVinci flow.

You can use the Screen connector to:

- Display a form for collecting user information.
- Present custom UI elements and views in one or more nodes of a flow.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)

- [Using connectors securely](#)
- [Using DaVinci flow templates](#)

Configuring the Screen connector

In DaVinci, add a Screen connector. For more information, see [Adding a connector](#).

Note

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Present a custom view

You can use the **View** capability to create a unique ID for a user. No special flow configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

View

Present a custom view

Properties

screen0Config

Input Schema

- default object
 - parameters object

Output Schema

- output object
 - screenComponentList object

Client side polling with Message

Properties

screen0Config

SecurID Connector

The SecurID connector lets you use RSA SecurID for multi-factor authentication (MFA) in your PingOne DaVinci flow.

Setup

Resources

For information and setup help, see the following:

- SecurID documentation
 - [Manage the SecurID Authentication API Keys](#)
 - [Identity Sources for the Cloud Authentication Service](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need an RSA SecurID Cloud Authentication license

Configuring the SecurID connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

SecurID Authentication API REST URL

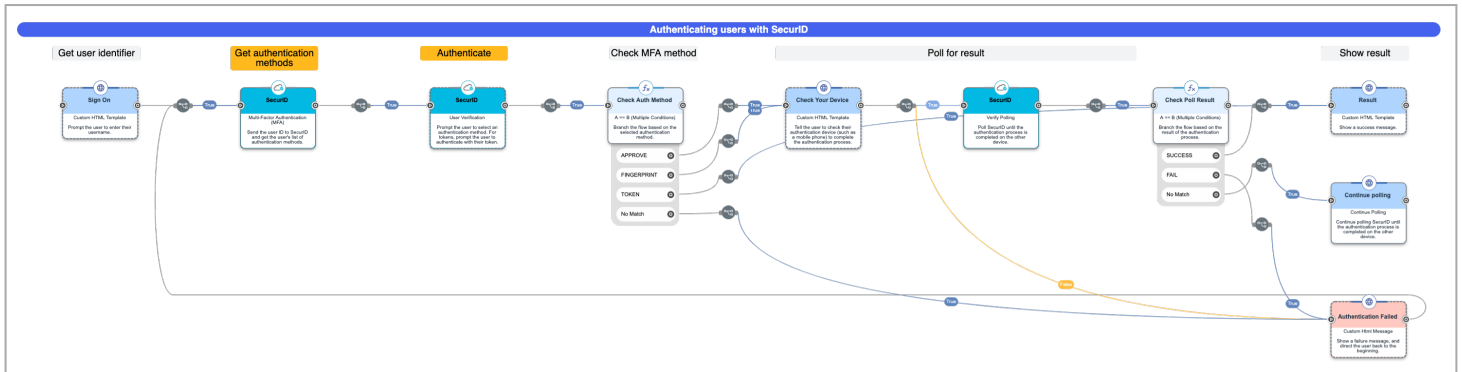
Your authentication API URL, such as <https://company.auth.securid.com>. For help getting your URL, see [Copy the SecurID Authentication API REST URL](#).

Client Key

Your SecurID authentication client key, such as `vowc450ahs6nry66vok0pvaizwnfr43ewsqcm7tz`. To get a client key, see [Add a SecurID Authentication API Key](#).

Using the connector in a flow

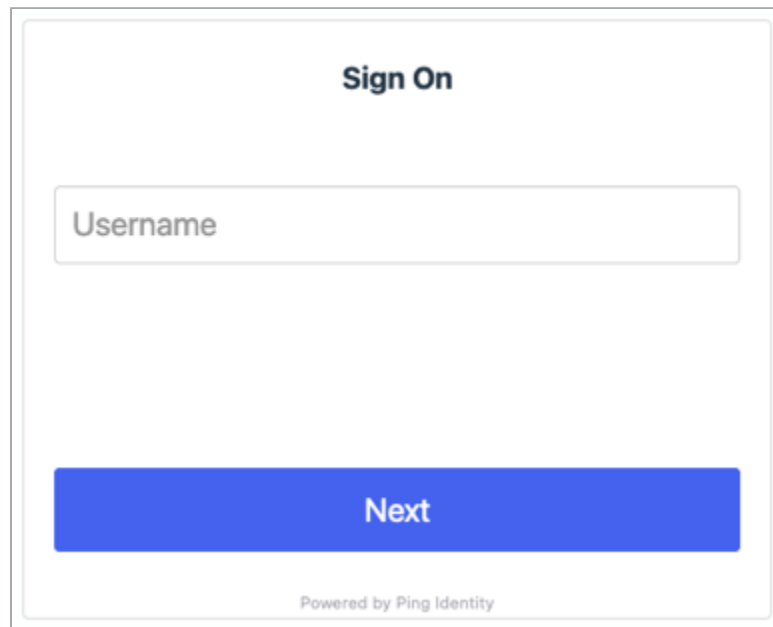
Authenticating users



This flow allows a user to authenticate with SecurID. It asks the user to enter their user ID in an HTML form, prompts them to select and complete a SecurID authentication method, then shows the results on an HTML page.

Because some authentication methods are completed on the user's mobile device, the flow includes a loop that polls SecurID until the authentication challenge is complete.

1. Download the [SecurID - MFA](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the sign on form.

A sign-on form template with a white background and a thin grey border. At the top center is the text "Sign On" in bold. Below it is a large, rounded rectangular input field with the placeholder text "Username". At the bottom center is a solid blue button with the text "Next" in white. At the very bottom center, in small grey text, is "Powered by Ping Identity".

1. On the flow canvas, select the **Sign On** node.
2. In the **Fields List**, customize the **Display Name** to help your users enter their identifier correctly, depending on whether your organization uses a name, ID, or email address.

Tip

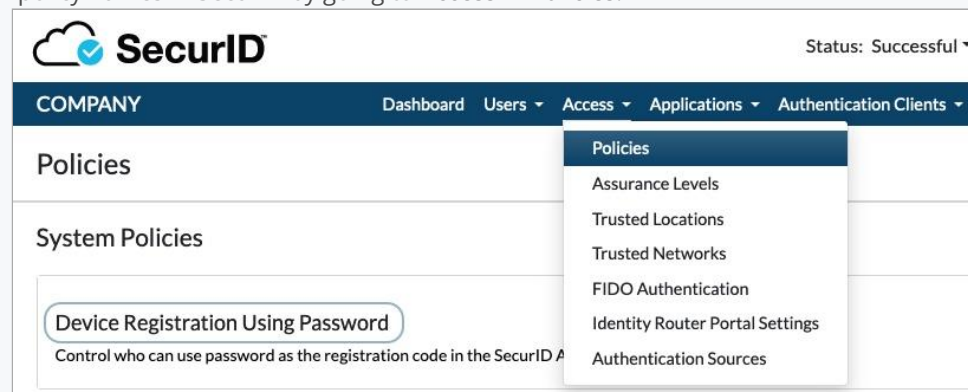
The ID entered must match a user in one of the identity sources you have configured in SecurID. For more information, see [Identity Sources for the Cloud Authentication Service](#).

3. (Optional) Customize the assurance policy:

1. On the flow canvas, select the **Multi-Factor Authentication (SecurID)** node.
2. In the **Assurance Policy Name** field, enter the policy you want to use, such as `All Users Low Assurance Level`.

Tip

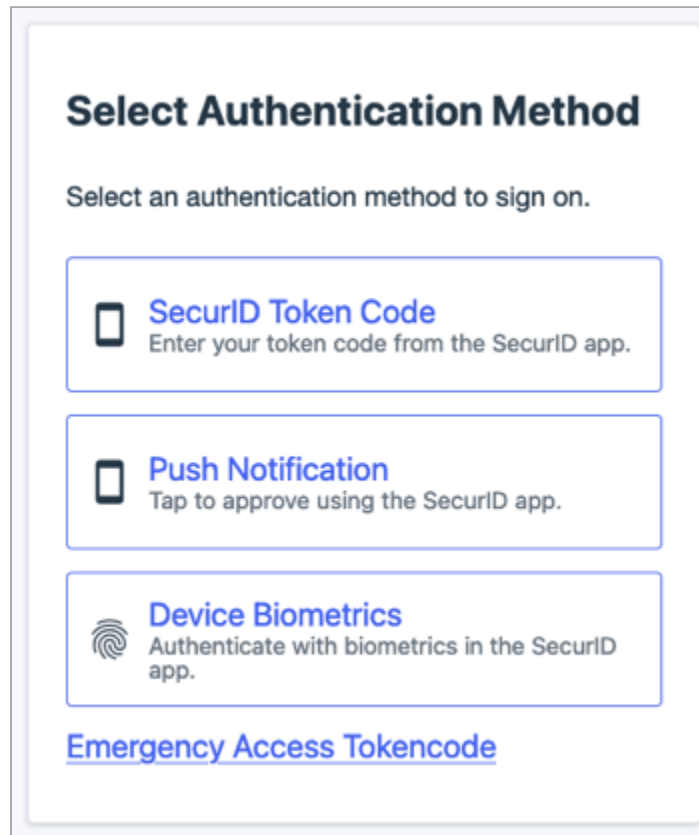
See your policy names in SecurID by going to **Access → Policies**.



Note

You can set this value dynamically by clicking `{}` and selecting a variable from another node in your flow.

4. (Optional) Customize the default **Select Authentication Method** interface.

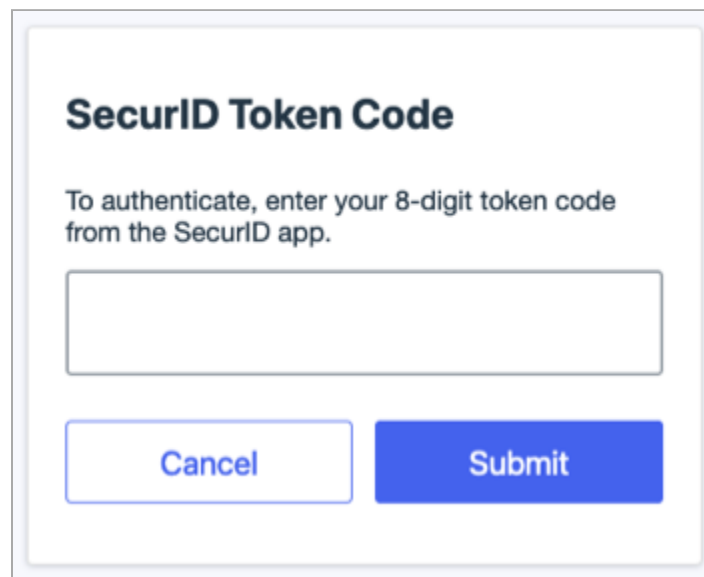


1. On the flow canvas, select the **User Verification (SecurID)** node.
2. On the **Select Authentication** tab, modify the **HTML Template**, **CSS**, and **Script** fields.

Tip

- Click **Switch View** to see the HTML formatted with syntax highlighting.
- Click the **Maximize** (⌕) icon to give yourself more room to work.
- To access a variety of useful tools, right-click the field when you're in syntax highlighting mode (dark background).

5. (Optional) Customize the default **SecurID Token Code** interface on the **SecurID Token Code** tab.

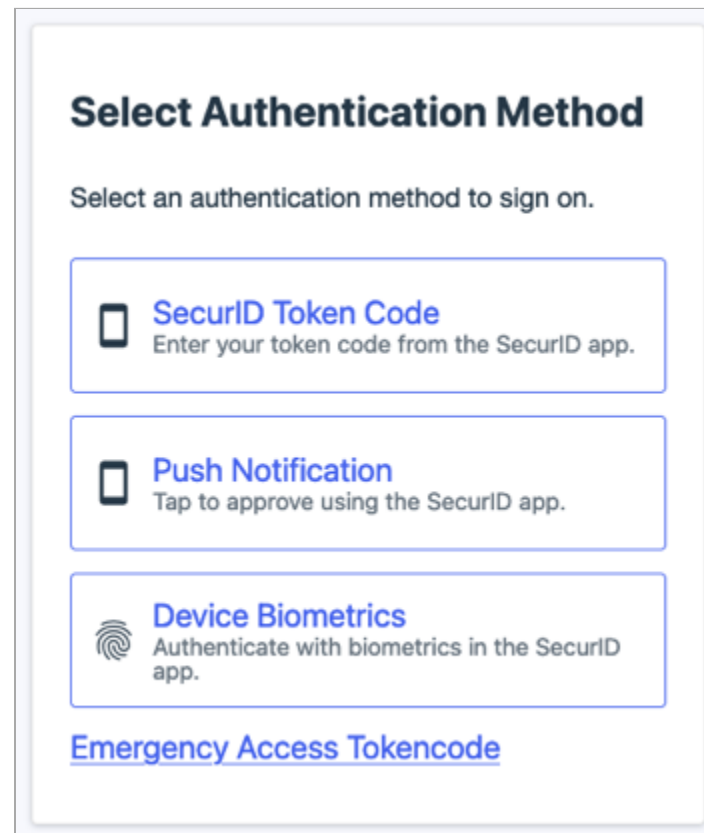


SecurID Token Code

To authenticate, enter your 8-digit token code from the SecurID app.

[Cancel](#) [Submit](#)

6. (Optional) Customize the default **Emergency Access Token Code** interface on the **Emergency Access Token Code** tab.



Select Authentication Method

Select an authentication method to sign on.

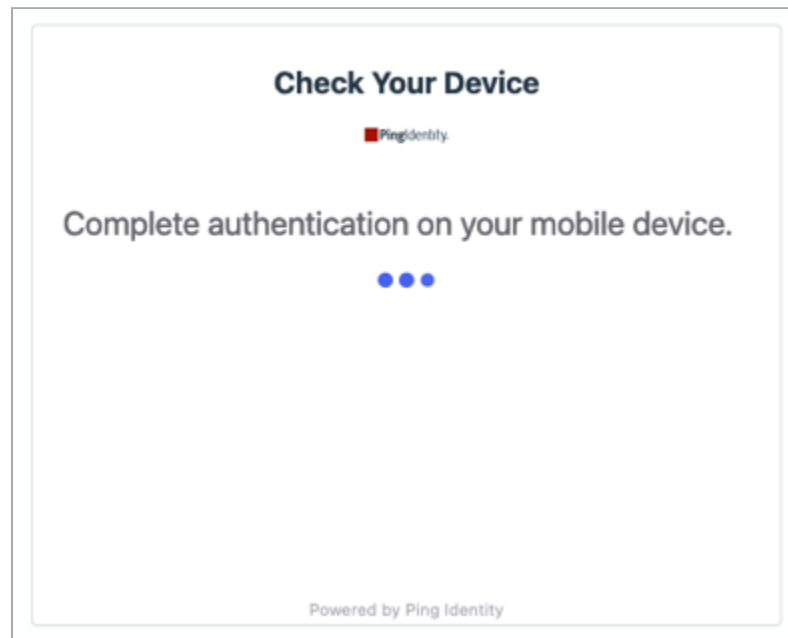
 **SecurID Token Code**
Enter your token code from the SecurID app.

 **Push Notification**
Tap to approve using the SecurID app.

 **Device Biometrics**
Authenticate with biometrics in the SecurID app.

[Emergency Access Tokencode](#)

7. (Optional) Customize the default **Check Your Device** interface.



1. On the flow canvas, select the **Check Your Device** node.
2. Modify the **Message Title**, **Message**, and other fields.
8. Test the flow by clicking **Save**, **Deploy**, and **Try Flow**.

Capabilities

Multi-Factor Authentication (MFA)

Get the user's authentication methods and start the authentication process.

Properties

User Identifier textField

The unique identifier for the user, such as an email, account name, user ID.

Assurance Policy Name textField

The name of your SecurID policy, such as "All Users Low Assurance Level".

Keep Record toggleSwitch

When enabled, SecurID keeps a record of each completed transaction.

Authentication Attempt Timeout textField

A number in seconds representing how long the server will keep the authentication attempt ID available after each call. During this time is is possible to make other calls using the "authnAttemptId". The server may reject initialization requests if the value provided is beyond the allowable maximum. Defaults to a server-defined session lifetime. Optional.

Input Schema

- default object
 - properties object
 - subjectName string required
 - assurancePolicyId string required
 - apiUrl string required
 - clientKey string required

Output Schema

- output object
 - headers object
 - vary string
 - cache-control string
 - content-type string
 - strict-transport-security string
 - date string
 - keep-alive string
 - expires string
 - x-xss-protection string
 - pragma string
 - transfer-encoding string
 - x-content-type-options string
 - connection string
 - x-frame-options string
 - status integer
 - data object
 - context object
 - authnAttemptId string
 - messageId string
 - inResponseTo string
 - credentialValidationResults array
 - Array Item Schema object
 - methodId string
 - methodResponseCode string
 - methodReasonCode string
 - authnAttributes array
 - attemptResponseCode string
 - attemptReasonCode string

- challengeMethods object
 - challenges array
 - Array Item Schema object
 - methodSetId string
 - requiredMethods array
 - Array Item Schema object
 - methodId string
 - displayName string
 - priority integer
 - versions array
 - Array Item Schema object
 - versionId string
 - methodAttributes array
 - Array Item Schema object
 - name string
 - value string
 - dataType string
 - valueRequired boolean
 - referenceId null
 - prompt object
 - promptResourceId string
 - defaultText string
 - formatRegex null
 - defaultValue null
 - valueBeingDefined boolean
 - sensitive boolean
 - minLength null
 - maxLength null
 - promptArgs array

User Verification

Prompt the user to select a method and complete the authentication process.

Properties

Input Schema

- default object
 - properties object
 - apiUrl string required
 - clientKey string required

Output Schema

- output object
 - challenge string
 - headers object
 - vary string
 - cache-control string
 - content-type string
 - strict-transport-security string
 - date string
 - keep-alive string
 - expires string
 - x-xss-protection string
 - pragma string
 - transfer-encoding string
 - x-content-type-options string
 - connection string
 - x-frame-options string
 - status integer
 - data object
 - context object
 - authnAttemptId string
 - messageId string
 - inResponseTo string
 - credentialValidationResults array
 - Array Item Schema object
 - methodId string
 - methodResponseCode string
 - methodReasonCode string
 - authnAttributes array
 - attemptResponseCode string

- attemptReasonCode string
- challengeMethods object
 - challenges array
 - Array Item Schema object
 - methodSetId string
 - requiredMethods array
 - Array Item Schema object
 - methodId string
 - displayName string
 - priority integer
 - versions array
 - Array Item Schema object
 - versionId string
 - methodAttributes array
 - Array Item Schema object
 - name string
 - value string
 - dataType string
 - valueRequired boolean
 - referenceId null
 - prompt object
 - promptResourceId string
 - defaultText string
 - formatRegex null
 - defaultValue null
 - valueBeingDefined boolean
 - sensitive boolean
 - minLength null
 - maxLength null
 - promptArgs array

Verify Polling

Use this to poll from securid

Input Schema

- default object
 - properties object
 - apiUri string required
 - clientKey string required

Output Schema

- output object
 - result string

SEON Connector

The SEON connector lets you uncover fraud patterns through SEON's device fingerprinting and intelligent insights in your PingOne DaVinci flow.

You can use the SEON connector to:

- Request a fraud score from SEON.
- Send feedback to SEON.

Setup

Resources

For information and setup help, see the following:

- SEON documentation:
 - [Quick Start](#)
 - [Developer Resources](#)

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A SEON license
- Your SEON credentials

Setting up SEON

Follow the instructions in [Quick Start](#).

Configuring the SEON connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

License Key

Your SEON license key. For help, see the [SEON REST API documentation](#).

API Base URL

The API URL to target.

Using the connector in a flow

Fraud score request

You can use the **Request Fraud Score** capability to get the fraud score for submitted data.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Feedback

You can use the **Send Feedback** capability to send feedback to SEON to improve their fraud identification.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Request Fraud Score

Get the fraud score for data submitted.

Properties

***Config Type* dropDown required**

The configuration type. Can be either Multiselect or JSON.

- Multiselect (Default)
- JSON

***Config* dropDownMultiSelect**

- Email
- Phone Number (19 Digits Limit)
- IP
- AML
- Device Fingerprinting

***Config Response Fields* dropDownMultiSelect**

- ID
- State
- Fraud Score
- IP Details
- Email Details
- Phone Details
- BIN Details
- Version
- Applied Rules
- Device Details

- Calculation Time
- SEON ID
- Rule Category Details
- Blackbox Score
- Geolocation Details

Config textArea

JSON config

User selectNameValueListColumn

- Email
- Phone Number (19 Digits Limit)
- Password Hash
- Email Address Domain
- User Full Name
- Username
- User First Name
- User Middle Name
- User Last Name
- User Place of Birth
- User Photo ID Number
- User ID
- User Created
- User Category
- User Account Status
- User Bank Account Number
- User Bank
- User Bank Account Balance
- User Verification Level
- User Date of Birth (YYYY-MM-DD)
- User Country
- User City

- User Region
- User Zip Code
- User Address Line 1
- User Address Line 2
- Action Type
- IP
- Affiliate ID
- Affiliate Name
- Session ID (64 Characters Limit)
- Session
- Device ID

Payment selectNameValueListColumn

- Receiver Full Name
- Receiver Bank Account Number
- Details URL
- Payment Method
- Payment Provider
- Card Full Name
- Card Bin (15 Characters Limit)
- Card Hash (500 Characters Limit)
- Card Expiration Date (YYYY-MM-DD)
- Card Last Four Digits
- AVS Result
- CVV Result
- Transaction Type
- Transaction Amount
- Transaction Currency (4 Characters Limit)
- Status of 3D Secure Results
- Payment ID

E-commerce selectNameValueListColumn

- Shipping Country
- Shipping City
- Shipping Region
- Shipping Zip Code
- Shipping Address
- Shipping Address Line 2
- Shipping Phone Number
- Shipping Full Name
- Shipping Method (50 Characters Limit)
- Gift
- Gift Message
- Merchant Category
- Merchant ID
- Merchant Created At
- Merchant Country
- Regulation
- Bonus Campaign ID
- Brand ID
- Order Memo
- Discount Code (50 Characters Limit)
- Items

Billing selectNameValueListColumn

- Billing Country
- Billing City
- Billing Region
- Billing Zip Code
- Billing Address Line
- Billing Address Line 2
- Billing Phone Number

Others selectNameValueListColumn

- Action Type
- Transaction ID (255 Characters Limit)
- SCA Method

Custom Fields keyValuePairList

You can use unlimited custom fields to inform our machine learning system and scoring engine. These can be string, boolean and numeric, for example is_intangible_item, is_pay_on_delivery, departure_airport, arrival_airport, days_to_board

Output Schema

output object

rawResponse object

properties object

success boolean

error object

data object

properties object

id string

state string

fraud_score number

bin_details object

properties object

card_bin string

bin_bank string

bin_card string

bin_type string

bin_level string

bin_country string

bin_country_code string

bin_website string

bin_phone string

bin_valid boolean

card_issuer string

version string

applied_rules array

items array

type object

properties

calculation_time number

seon_id number

ip_details object

properties object

success boolean

error object

data object

properties object

ip string

score number

country string

state_prov string

city string
timezone_offset string
isp_name string
latitude number
longitude number
type string
open_ports array
items array
 type integer
tor boolean
harmful boolean
vpn boolean
web_proxy boolean
public_proxy boolean
spam_number integer
spam_urls array
items array
 type string
applied_rules array
items array
 type object
 properties
history object
properties object
 hits integer
 customer_hits integer
 first_seen integer
 last_seen integer
flags array
items array
 type object
 properties
id string
 email_details object
 properties object
email string
score number
deliverable boolean
domain_details object
properties object
domain string

tld string
registered boolean
created string
updated string
expires string
registrar_name string
registered_to string
disposable boolean
free boolean
custom boolean
dmARC_enforced boolean
spf_strict boolean
valid_mx boolean
accept_all boolean
suspicious_tld boolean
website_exists boolean
account_details object
properties object
apple object
properties object
 registered boolean
ebay object
properties object
 registered boolean
facebook object
properties object
 registered boolean
 url string
 name string
 photo string
flickr object
properties object
 registered boolean
foursquare object
properties object
 registered boolean
github object
properties object
 registered boolean
google object
properties object

registered boolean
photo string
gravatar object
properties object
registered boolean
instagram object
properties object
registered boolean
lastfm object
properties object
registered boolean
linkedin object
properties object
registered boolean
url string
name string
company string
title string
location string
website string
twitter string
photo string
microsoft object
properties object
registered boolean
myspace object
properties object
registered boolean
pinterest object
properties object
registered boolean
skype object
properties object

registered boolean
country string
city string
gender string
name string
id string
handle string
bio string
age number
language string
state string
photo string
spotify object
properties object
 registered boolean
tumblr object
properties object
 registered boolean
twitter object
properties object
 registered boolean
vimeo object
properties object
 registered boolean
weibo object
properties object
 registered boolean
yahoo object
properties object
 registered boolean
breach_details object
properties object
haveibeenpwned_listed boolean
number_of_breaches integer
first_breach string
breaches array
items array
 type object
 properties
 phone_details object
 properties object

number number
valid boolean
type string
country string
carrier string
score number
account_details object
properties object
facebook object
properties object
 registered boolean
 photo string
 url string
 name string
google object
properties object
 registered boolean
 photo string
 url string
 name string
apple object
properties object
 registered boolean
twitter object
properties object
 registered boolean
 photo string
 url string
microsoft object
properties object
 registered boolean
yahoo object
properties object
 registered boolean
ebay object
properties object
 registered boolean
gravatar object
properties object

registered boolean
photo string
url string
name string
username string
instagram object
properties object
 registered boolean
spotify object
properties object
 registered boolean
tumblr object
properties object
 registered boolean
linkedin object
properties object
 registered boolean
 photo string
 url string
 location string
 name string
 company string
 title string
 website string
 twitter string
 connection_count number
weibo object
properties object
 registered boolean
github object
properties object
 registered boolean
vimeo object
properties object
 registered boolean
flickr object
properties object
 registered boolean
 photo string
 username string
foursquare object

properties* object**registered* boolean*****photo* string*****url* string*****name* string*****bio* string*****lastfm* object*****properties* object*****registered* boolean*****myspace* object*****properties* object*****registered* boolean*****pinterest* object*****properties* object*****registered* boolean*****skype* object*****properties* object*****registered* boolean*****photo* string*****location* string*****name* string*****country* string*****city* string*****gender* integer*****id* string*****handle* string*****bio* string*****age* integer*****language* string*****state* string*****discord* object*****properties* object*****registered* boolean*****ok* object*****properties* object*****registered* boolean*****city* string*****gender* integer*****age* integer*****date_joined* integer*****kakao* object**

properties object
 registered boolean

booking object

properties object
 registered boolean

airbnb object

properties object
 registered boolean
 image string
 url string
 location string
 name string
 about string
 first_name string
 created_at string
 reviewee_count string
 trips integer
 work string
 identity_verified string

amazon object

properties object
 registered boolean

qzone object

properties object
 registered boolean

adobe object

properties object
 registered boolean

mailru object

properties object
 registered boolean

wordpress object

properties object
 registered boolean

imgur object

properties object
 registered boolean

disneyplus object

properties object
 registered boolean

netflix object

properties object
 registered boolean

jdid object

properties object
 registered boolean

flipkart object

properties object
 registered boolean

bukalapak object

properties object
 registered boolean

archiveorg object

properties object
 registered boolean

lazada object

properties object
 registered boolean

zoho object

properties object
 registered boolean

samsung object

properties object
 registered boolean

evernote object

properties object
 registered boolean

envato object

properties object
 registered boolean

patreon object

properties object
 registered boolean

tokopedia object

properties object
 registered boolean

rambler object

properties object
 registered boolean

quora object

properties object
 registered boolean

atlassian object
properties object
 registered boolean
 aml_details object
 properties object
has_crimelist_match boolean
has_pep_match boolean
has_watchlist_match boolean
has_sanction_match boolean
result_payload object
properties object
searched_at string
sanctionlist_sources array
items array
 type object
 properties
crimelist_entries array
items array
 type object
 properties
watchlist_entries array
items array
 type object
 properties
sanctionlist_entries array
items array
 type object
 properties
pep_entries array
items array
 type object
 properties
 device_details object
 properties object
session_id string
type string
dns_ip string
dns_ip_country string
dns_ip_isp string
source string
device_hash string

device_name string
device_cellular_id string
android_id string
build_id string
build_device string
build_time integer
build_number string
build_manufacturer string
app_guid string
android_version string
last_boot_time integer
system_uptime integer
sensor_hash string
audio_volume_current integer
audio_mute_status boolean
battery_level integer
battery_charging boolean
battery_temperature integer
battery_voltage integer
battery_health string
has_proximity_sensor boolean
cpu_type string
cpu_count integer
cpu_speed integer
cpu_hash string
kernel_name string
kernel_version string
kernel_arch string
physical_memory integer
screen_brightness integer
screen_height integer
screen_width integer
screen_scale integer
total_storage integer
free_storage integer
network_config string
wifi_mac_address string
wifi_ssid string
carrier_name string
pasteboard_hash string
region_timezone string

region_language string
region_country string
carrier_country string
is_emulator boolean
is_rooted boolean
device_ip_address string
device_ip_country string
device_ip_isp string
 geolocation_details object
 properties object
user_billing_distance number
user_shipping_distance number
billing_shipping_distance number
ip_user_distance number
ip_billing_distance number
ip_shipping_distance number
 rule_category_details array
 items array
type object
properties
status string
headers object

Send Feedback

Send feedback to SEON to improve the fraud identification.

Properties

***Transactions* `keyValueList`**

The list of transactions you want to label with the label texts.

Output Schema

output object

rawResponse object

properties object

success boolean

error object

data object

status string

headers object

Make Custom API Call

Define a custom API call to SEON.

Properties

Endpoint textField required

The SEON API endpoint, such as "SeonRestService/fraud-api/v2.0". This endpoint is added to the base API URL selected in the connector configuration.

HTTP Method dropDown required

The HTTP method of the API call.

- GET (Default)
- POST
- PUT
- DELETE
- PATCH

Query Parameters keyValuePairList

Define additional query parameters to send to SEON. For help, see the SEON REST API documentation.

Additional Headers keyValuePairList

Define additional headers to send to SEON. For help, see the SEON REST API documentation.

Body textArea

The raw JSON body of the API call.

Output Schema

output object

rawResponse object

properties object

success boolean

error object

data object

status string

headers object

properties object

content-type string

content-length string

connection string

date string

x-amzn-requestid string

x-xss-protection string

access-control-allow-origin string

x-frame-options string

x-amzn-remapped-connection string

x-amz-apigw-id string

vary string

cache-control string

x-amzn-remapped-server string

expires string

x-content-type-options string

pragma string

x-amzn-remapped-date string

x-cache string

via string

x-amz-cf-pop string

x-amz-cf-id string

ServiceNow Connector

The ServiceNow connector lets you manage users, group memberships, and incidents in ServiceNow from your PingOne DaVinci flow.

You can use the ServiceNow connector to:

- Create, deactivate, modify, and search for users
- Add users to groups

- Read, create, and modify incidents

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a ServiceNow license.

Configuring the ServiceNow connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

API URL

The API URL to target, such as "mycompany.service-now.com". This domain is visible in the URL bar when you sign on to the ServiceNow administrator portal.

Admin Username

Your ServiceNow administrator username.

Admin Password

Your ServiceNow administrator password.

Using the connector in a flow

Searching for users

There are two ways to search for users with the ServiceNow connector:

- Search for a specific user by user ID using the **Search User** capability.
- Search for multiple users based on their attributes using the **Search** capability.

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing users

The connector has two capabilities that allow you to create, modify, activate, and deactivate users in ServiceNow:

- **Create User**
- **Modify User**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing group memberships

The **Add User to Group** connector allows you to manage the groups that a user belongs to in ServiceNow:

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Managing incidents

The connector has several capabilities that allow you to manage incidents in ServiceNow:

- **Read an incident**
- **Create an incident**
- **Modify an incident**

No special flow configuration is needed. Add the capability you want and populate its properties according to the help text.

Limitations

ServiceNow does not provide support for:

- Deleting users
- Removing users from groups
- Deleting incidents

Capabilities

Get User Information

Get information about a user.

Properties

User System ID textField required

The user's ServiceNow system ID, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Output Schema

- output object
 - rawResponse object
 - result object
 - calendar_integration string
 - country string
 - user_password string
 - last_login_time string
 - x_pd_integration_pagerduty_id string
 - hashed_user_id string
 - source string
 - sys_updated_on string
 - building string
 - web_service_access_only string
 - notification string
 - enable_multifactor_authn string
 - sys_updated_by string
 - sso_source string
 - sys_created_on string
 - sys_domain object
 - link string
 - value string
 - state string
 - vip string
 - sys_created_by string
 - zip string
 - home_phone string
 - time_format string
 - last_login string
 - default_perspective string

- active string
- sys_domain_path string
- cost_center string
- phone string
- name string
- employee_number string
- password_needs_reset string
- gender string
- city string
- failed_attempts string
- user_name string
- roles string
- title string
- sys_class_name string
- sys_id string
- internal_integration_user string
- ldap_server string
- mobile_phone string
- street string
- company string
- first_name string
- email string
- introduction string
- preferred_language string
- manager string
- locked_out string
- sys_mod_count string
- last_name string
- photo string
- avatar string

- middle_name string
- sys_tags string
- time_zone string
- schedule string
- date_format string
- location string
- statusCode number
- headers object

Search Users

Search for users based on an attribute filter.

Properties

Number of Results textField

The number of results to return from the search.

Email textField

The user's email address.

First Name textField

The user's first name.

Last Name textField

The user's last name.

Query Parameters keyValueList

Define additional query parameters to send to ServiceNow. For help, see the ServiceNow user table documentation.

Output Schema

- output object
 - rawResponse object
 - result array
 - statusCode number
 - headers object

Deactivate User

Deactivate a user by the ServiceNow ID.

Properties

User System ID textField required

The user's ServiceNow system ID, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Output Schema

- output object
 - statusCode number
 - headers object

Create User

Create a new user.

Properties

Username textField

The unique ID of the user.

First Name textField

The user's first name.

Middle Name textField

The user's middle name.

Last Name textField

The user's last name.

Phone textField

The user's phone number.

Email textField required

The user's email address.

Activate User toggleSwitch

When enabled, this sets the user account to active in ServiceNow.

Group dropDown

The relevant group.

City textField

The User's city

Employee Number textField

The User's employee number.

Custom Attributes keyValueList

Additional attributes for user creation or modification.

Output Schema

- output object
 - rawResponse object
 - result object
 - country string
 - user_password string
 - gender string
 - city string
 - sys_import_state_comment string
 - template_import_log string
 - sys_updated_on string
 - sys_class_name string
 - sys_target_sys_id object
 - link string
 - value string
 - notification string
 - sys_id string
 - sys_updated_by string
 - sys_created_on string
 - sys_import_set object
 - link string
 - value string
 - sys_transform_map object
 - link string
 - value string
 - first_name string
 - email string
 - preferred_language string
 - sys_created_by string
 - group string

- sys_import_row string
- home_phone string
- sys_row_error string
- sys_target_table string
- locked_out string
- sys_mod_count string
- active string
- last_name string
- import_set_run object
 - link string
 - value string
- middle_name string
- sys_tags string
- sys_import_state string
- phone string
- employee_number string
- mobile_number string
- username string
- group_record_id string
- group_sys_id string
- statusCode number
- headers object

Add User to Group

Add a user to a group.

Properties

User System ID textField required

The user's ServiceNow system ID, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Group dropDown

The relevant group.

Output Schema

- output object
 - statusCode number
 - headers object

Modify User

Modify a user.

Properties

User System ID textField required

The user's ServiceNow system ID, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Username textField

The unique ID of the user.

First Name textField

The user's first name.

Middle Name textField

The user's middle name.

Last Name textField

The user's last name.

Phone textField

The user's phone number.

Email textField

The user's email address.

Activate User toggleSwitch

When enabled, this sets the user account to active in ServiceNow.

Lock User Out toggleSwitch

When enabled, the user is locked out of ServiceNow.

Custom Attributes keyValueList

Additional attributes for user creation or modification.

Output Schema

- output object
 - rawResponse object
 - result object
 - calendar_integration string
 - country string
 - user_password string
 - last_login_time string
 - x_pd_integration_pagerduty_id string
 - hashed_user_id string
 - source string
 - sys_updated_on string
 - building string
 - web_service_access_only string
 - notification string
 - enable_multifactor_authn string
 - sys_updated_by string
 - sso_source string
 - sys_created_on string
 - sys_domain object
 - link string
 - value string
 - state string
 - vip string
 - sys_created_by string
 - zip string
 - home_phone string
 - time_format string
 - last_login string
 - default_perspective string

- active string
- sys_domain_path string
- cost_center string
- phone string
- name string
- employee_number string
- password_needs_reset string
- gender string
- city string
- failed_attempts string
- user_name string
- roles string
- title string
- sys_class_name string
- sys_id string
- internal_integration_user string
- ldap_server string
- mobile_phone string
- street string
- company string
- department string
- first_name string
- email string
- introduction string
- preferred_language string
- manager string
- locked_out string
- sys_mod_count string
- last_name string
- photo string

- avatar string
- middle_name string
- sys_tags string
- time_zone string
- schedule string
- date_format string
- location string
- statusCode number
- headers object

Create Incident

Create a new incident.

Properties

Caller ID textField

The ServiceNow system ID of the user with the issue, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Category dropDown

The incident category.

Subcategory dropDown

The incident subcategory.

Service dropDown

The service associated with the incident.

Configuration Item ID textField

The ServiceNow system ID of the related configuration item, such as "fd91bda9d10bdac51a8e4a18cc4bcbc8".

Short Description textArea

A brief description of the incident.

Description textArea

A complete description of the incident.

Channel dropDown

The channel (source) where the incident took place.

Status dropDown

The status of the incident.

Impact dropDown

The level of impact for the incident.

Urgency dropDown

The level of urgency for the incident.

Group dropDown

The relevant group.

Custom Attributes keyValueList

Additional attributes for user creation or modification.

Output Schema

- output object
 - rawResponse object
 - result object
 - x_pd_integration_conf_bridge string
 - parent string
 - made_sla string
 - caused_by string
 - watch_list string
 - upon_reject string
 - sys_updated_on string
 - child_incidents string
 - hold_reason string
 - origin_table string
 - task_effective_number string
 - approval_history string
 - number string
 - resolved_by string
 - sys_updated_by string
 - opened_by object
 - link string
 - value string
 - user_input string
 - sys_created_on string
 - sys_domain object
 - link string
 - value string
 - x_pd_integration_incident string
 - state string
 - route_reason string

- sys_created_by string
- knowledge string
- order string
- calendar_stc string
- closed_at string
- cmdb_ci string
- delivery_plan string
- contract string
- impact string
- active string
- work_notes_list string
- business_service object
 - link string
 - value string
- business_impact string
- priority string
- sys_domain_path string
- rfc string
- time_worked string
- expected_start string
- opened_at string
- business_duration string
- group_list string
- work_end string
- caller_id object
 - link string
 - value string
- reopened_time string
- resolved_at string
- approval_set string

- subcategory string
- work_notes string
- x_pd_integration_incident_id string
- universal_request string
- short_description string
- close_code string
- correlation_display string
- delivery_task string
- work_start string
- assignment_group object
 - link string
 - value string
- additional_assignee_list string
- business_stc string
- cause string
- description string
- origin_id string
- calendar_duration string
- close_notes string
- notify string
- service_offering string
- sys_class_name string
- closed_by string
- follow_up string
- parent_incident string
- sys_id string
- contact_type string
- reopened_by string
- incident_state string
- urgency string

- problem_id string
- company string
- reassignment_count string
- x_pd_integration_incident_key string
- activity_due string
- assigned_to string
- severity string
- comments string
- approval string
- sla_due string
- comments_and_work_notes string
- due_date string
- sys_mod_count string
- reopen_count string
- sys_tags string
- escalation string
- upon_approval string
- correlation_id string
- location string
- category string
- statusCode number
- headers object

Read Incident

Search for an incident by the incident number or by the ServiceNow ID.

Properties

Incident Search Attribute dropdown required

Determines whether to get incident information based on an incident number or by ServiceNow system ID.

- Use Incident ID (Default)
- Use Incident number

Incident Number textField required

The incident number, such as "INC0010077".

Incident ID textField required

The incident's ServiceNow system ID, such as "c4bcbc8bdac51a8e4afd91bda9d1018c".

Output Schema

- output object
 - rawResponse object
 - result object
 - x_pd_integration_conf_bridge string
 - parent string
 - made_sla string
 - caused_by string
 - watch_list string
 - upon_reject string
 - sys_updated_on string
 - child_incidents string
 - hold_reason string
 - origin_table string
 - task_effective_number string
 - approval_history string
 - number string
 - resolved_by string
 - sys_updated_by string
 - opened_by object
 - link string
 - value string
 - user_input string
 - sys_created_on string
 - sys_domain object
 - link string
 - value string
 - x_pd_integration_incident string
 - state string
 - route_reason string

- sys_created_by string
- knowledge string
- order string
- calendar_stc string
- closed_at string
- cmdb_ci string
- delivery_plan string
- contract string
- impact string
- active string
- work_notes_list string
- business_service object
 - link string
 - value string
- business_impact string
- priority string
- sys_domain_path string
- rfc string
- time_worked string
- expected_start string
- opened_at string
- business_duration string
- group_list string
- work_end string
- caller_id object
 - link string
 - value string
- reopened_time string
- resolved_at string
- approval_set string

- subcategory string
- work_notes string
- x_pd_integration_incident_id string
- universal_request string
- short_description string
- close_code string
- correlation_display string
- delivery_task string
- work_start string
- assignment_group object
 - link string
 - value string
- additional_assignee_list string
- business_stc string
- cause string
- description string
- origin_id string
- calendar_duration string
- close_notes string
- notify string
- service_offering string
- sys_class_name string
- closed_by string
- follow_up string
- parent_incident string
- sys_id string
- contact_type string
- reopened_by string
- incident_state string
- urgency string

- problem_id string
- company string
- reassignment_count string
- x_pd_integration_incident_key string
- activity_due string
- assigned_to string
- severity string
- comments string
- approval string
- sla_due string
- comments_and_work_notes string
- due_date string
- sys_mod_count string
- reopen_count string
- sys_tags string
- escalation string
- upon_approval string
- correlation_id string
- location string
- category string
- statusCode number
- headers object

Modify Incident

Modify an incident by its ServiceNow ID.

Properties

Incident ID textField required

The incident's ServiceNow system ID, such as "c4bcbc8bdac51a8e4afd91bda9d1018c".

Caller ID textField

The ServiceNow system ID of the user with the issue, such as "bdac51a8e4afd91bda9d1018cc4bcbc8".

Category dropDown

The incident category.

Subcategory dropDown

The incident subcategory.

Service dropDown

The service associated with the incident.

Configuration Item ID textField

The ServiceNow system ID of the related configuration item, such as "fd91bda9d10bdac51a8e4a18cc4bcbc8".

Short Description textArea

A brief description of the incident.

Description textArea

A complete description of the incident.

Channel dropDown

The channel (source) where the incident took place.

Status dropDown

The status of the incident.

Impact dropDown

The level of impact for the incident.

Urgency dropDown

The level of urgency for the incident.

Group dropDown

The relevant group.

Custom Attributes keyValuePairList

Additional attributes for user creation or modification.

Output Schema

- output object
 - rawResponse object
 - result object
 - x_pd_integration_conf_bridge string
 - parent string
 - made_sla string
 - caused_by string
 - watch_list string
 - upon_reject string
 - sys_updated_on string
 - child_incidents string
 - hold_reason string
 - origin_table string
 - task_effective_number string
 - approval_history string
 - number string
 - resolved_by string
 - sys_updated_by string
 - opened_by object
 - link string
 - value string
 - user_input string
 - sys_created_on string
 - sys_domain object
 - link string
 - value string
 - x_pd_integration_incident string
 - state string
 - route_reason string

- sys_created_by string
- knowledge string
- order string
- calendar_stc string
- closed_at string
- cmdb_ci string
- delivery_plan string
- contract string
- impact string
- active string
- work_notes_list string
- business_service object
 - link string
 - value string
- business_impact string
- priority string
- sys_domain_path string
- rfc string
- time_worked string
- expected_start string
- opened_at string
- business_duration string
- group_list string
- work_end string
- caller_id object
 - link string
 - value string
- reopened_time string
- resolved_at string
- approval_set string

- subcategory string
- work_notes string
- x_pd_integration_incident_id string
- universal_request string
- short_description string
- close_code string
- correlation_display string
- delivery_task string
- work_start string
- assignment_group object
 - link string
 - value string
- additional_assignee_list string
- business_stc string
- cause string
- description string
- origin_id string
- calendar_duration string
- close_notes string
- notify string
- service_offering string
- sys_class_name string
- closed_by string
- follow_up string
- parent_incident string
- sys_id string
- contact_type string
- reopened_by string
- incident_state string
- urgency string

- problem_id string
- company string
- reassignment_count string
- x_pd_integration_incident_key string
- activity_due string
- assigned_to string
- severity string
- comments string
- approval string
- sla_due string
- comments_and_work_notes string
- due_date string
- sys_mod_count string
- reopen_count string
- sys_tags string
- escalation string
- upon_approval string
- correlation_id string
- location string
- category string
- statusCode number
- headers object

Socure Connector

The Socure connector lets you verify identity documents and get fraud scores in your PingOne DaVinci flows.

The connector allows you to direct users to a unique verification URL where they submit their driver license or passport along with selfie photos. After Socure verifies the user's identity, it sends the results to DaVinci where you can branch your flow accordingly.

To make sure a camera is available to scan the documents and take photos, the user typically completes the verification process on a mobile device.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need a Socure license.

Configuring the Socure connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

ID+ Key

Your Socure ID+ key, such as "a1b234cd-75e1-9e01-f234-56abcdef6789".

Get this key from [Setting up Socure](#).

SDK Key

Your Socure SDK key, such as "d450e856-9e01-75e1-8cec-64efe8eef39b".

Get this key from [Setting up Socure](#).

API URL

The Socure API URL to target. Select the environment that you chose in [Getting your Socure ID+ and SDK keys](#).

Get this URL from [Setting up Socure](#).

Webhook URL

The DaVinci webhook URL for this instance of your connector.

Copy this URL. You'll use it in [Setting up Socure](#).

Setting up Socure

Allowing the DaVinci webhook URL in your Socure configuration

1. Sign on to the Socure administrator portal at <https://admin.socure.com>.
2. Go to **Developer** → **Webhook**. Click **New Webhook**.
3. In the **Subscription Type** list, select **Document Verification**.
4. In the **Subscription Channel Name** field, enter a name.
5. In the **Webhook URL** field, enter the webhook URL that you copied from your Socure connector configuration.
6. Leave the **Secret Key** field blank.
7. Leave the **Choose certificate** section blank.
8. Click **Test**. Check that the test was successful.

Allowing the DaVinci domain in your Socure configuration

Click **Create**.

See [IP address and domain reference](#) for a list of domains that DaVinci uses. Follow the steps below to add all the domains for your region:

1. Sign on to the Socure administrator portal at <https://admin.socure.com>.
2. Go to **Developers** → **IPs & Domains**.
3. Click **New Domain**.
4. In the **IP/DOMAINS** field, enter the domain. Click **Create**.
5. Repeat this process for each DaVinci domain in your region.

Getting your Socure ID+ and SDK keys



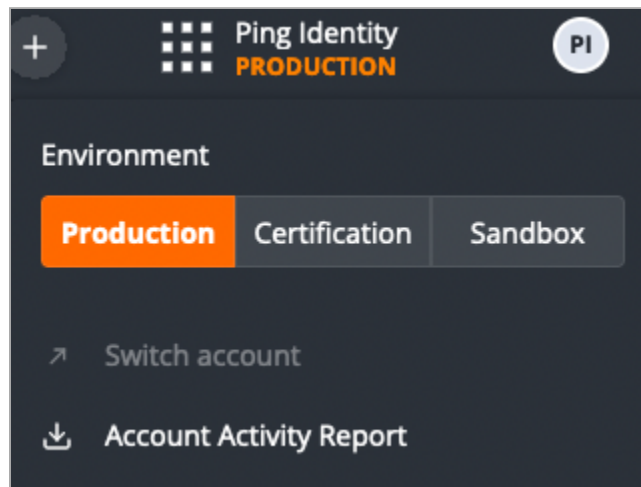
Important

Your **ID+ Key** and **SDK Key** are different for each environment.

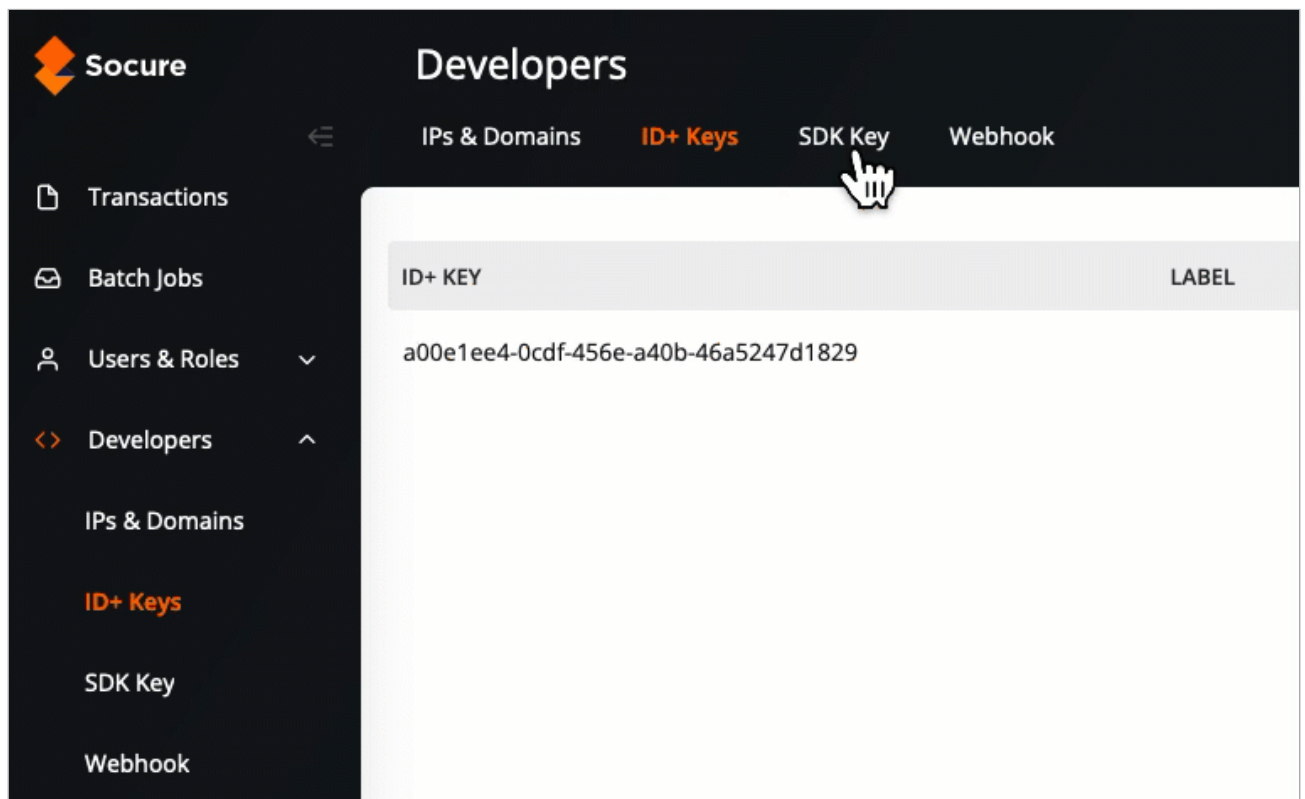
1. Sign on to the Socure administrator portal at <https://admin.socure.com>.

2. Select the environment you want to connect to:

1. Click your organization.
2. Click to select the **Production**, **Certification**, or **Sandbox** environment.

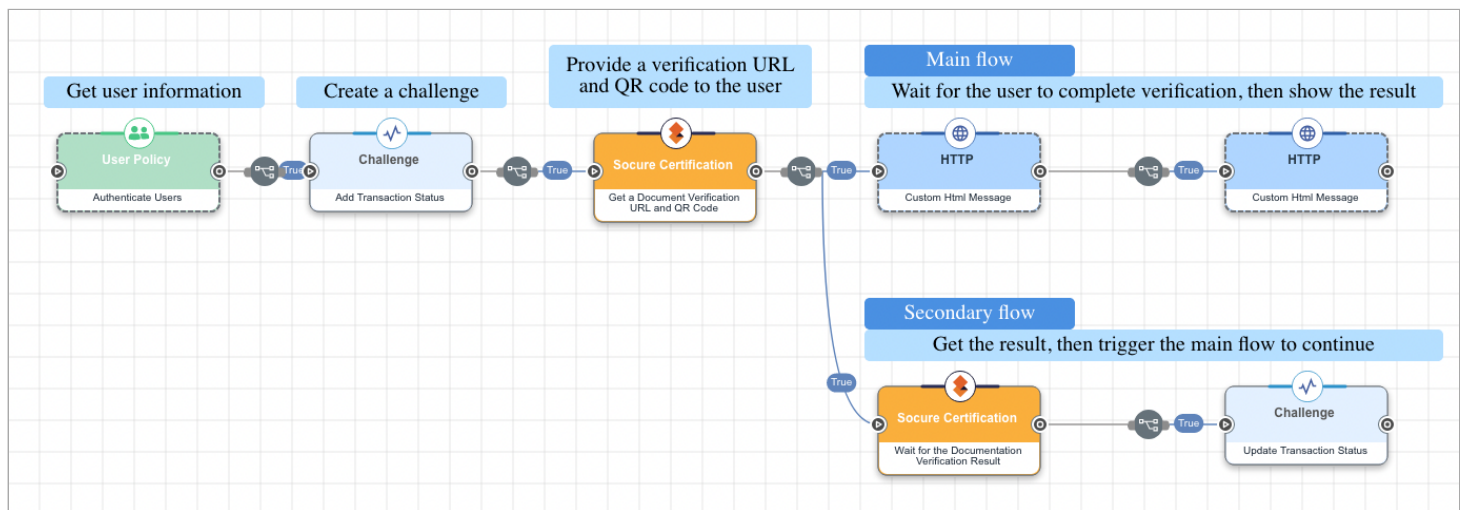


3. Go to **Developers** → **ID+ Keys** and **SDK Key** to get your ID+ and SDK keys.



Using the connector in a flow

Verify identity documents with a link or QR code



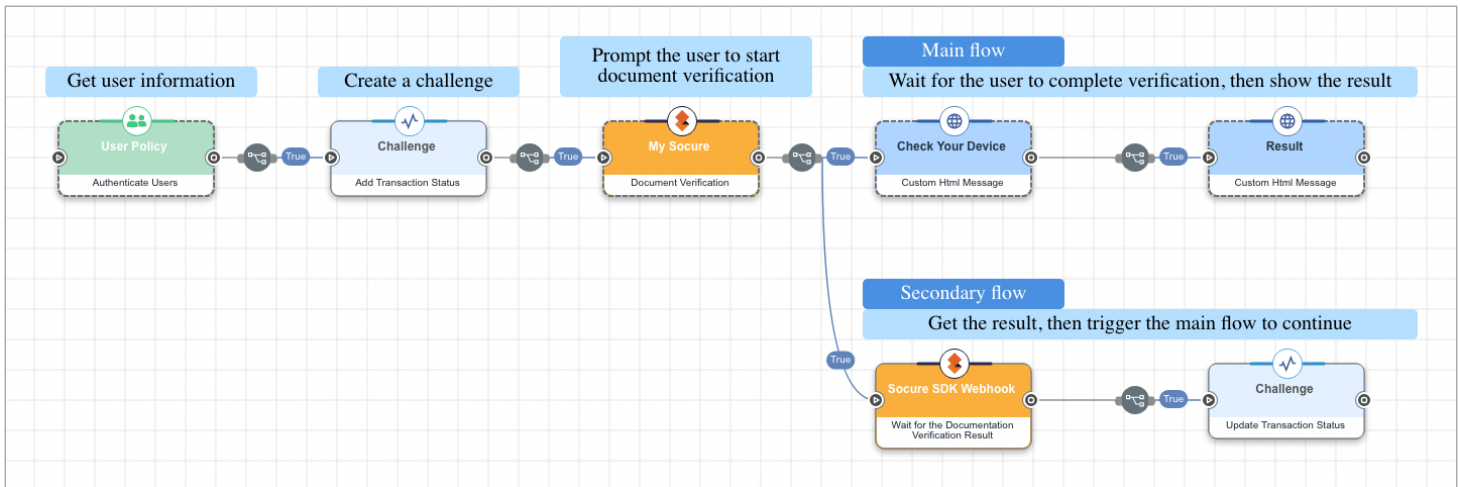
This flow uses Socure to get a unique verification URL and show it as a link and QR code in the user's web browser. When the user opens the link with their mobile device, they are guided through the process of submitting photos of their identification card (either a driver license or passport) and taking a selfie photo. After the documents and photos are accepted, the flow continues where it started in the web browser.

This flow creates a "challenge" to pause the main flow on the QR code while a secondary flow continues the verification process. When the verification process is complete, a [Challenge](#) connector resolves the challenge and triggers the main flow to continue. To learn more about this technique, see the [Challenge](#) connector.

1. Download the [Socure - Identity verification with link or QR code](#) flow template. For help, see [Using DaVinci flow templates](#).
2. On the flow canvas, select the **Get a Document Verification URL and QR Code** node.
3. (Optional) In the **Customer User ID** field, change the value to a test user ID that exists in your Socure records. In a real-world flow, click `{}` and populate this with a variable from earlier in your flow.
4. (Optional) Customize the document verification prompt:
 1. Select the **Verification Prompt** node.
 2. In the **Message Title** field, customize the title of the prompt.
 3. In the **Message** field, customize the user-facing text.
 4. Click **Apply**.
5. Test the flow:
 1. Click **Save**, **Deploy**, and **Try Flow**.
 2. With your mobile device, scan the QR code and open the link.
 3. Complete the document verification process on your mobile device.

4. See the result in your web browser on the original device.

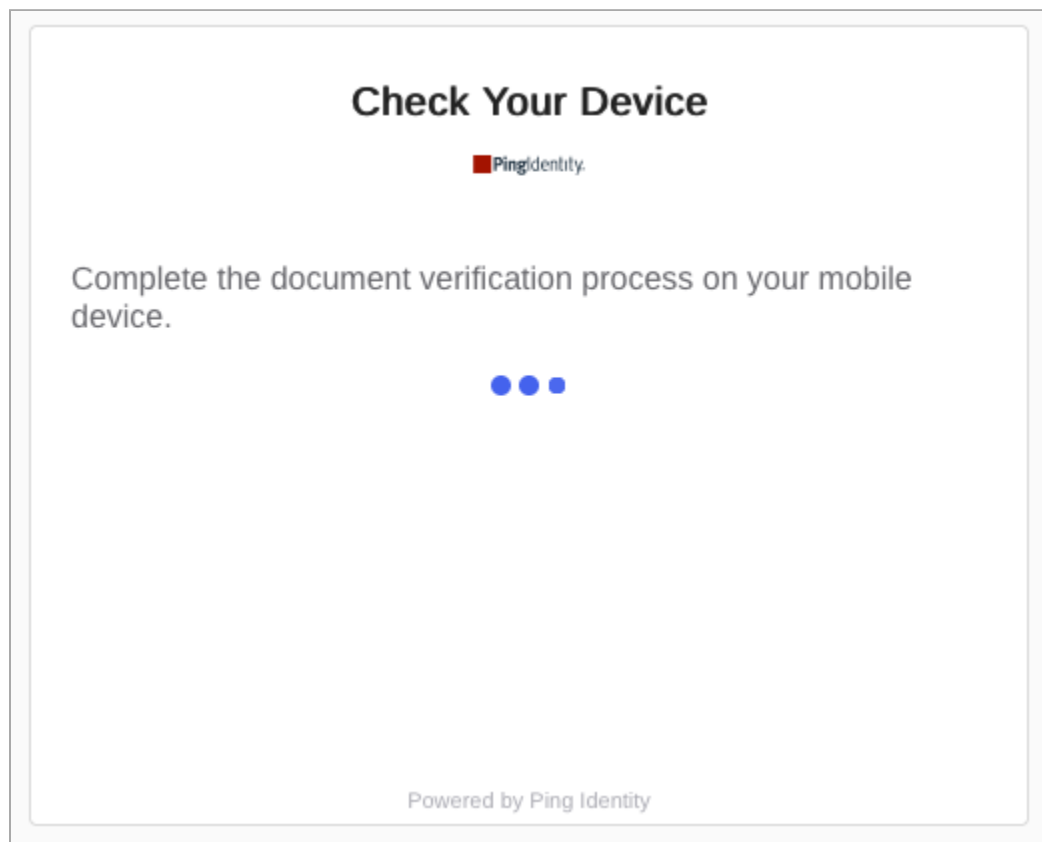
Verify identity documents with an SMS prompt



In this flow, Socure prompts the user to enter their phone number in their web browser. Socure sends an SMS message to the number, which guides the user through the process of submitting photos of their identification card (either a driver license or passport) and taking a selfie photo. After the documents and photos are accepted, the flow continues where it started in the web browser.

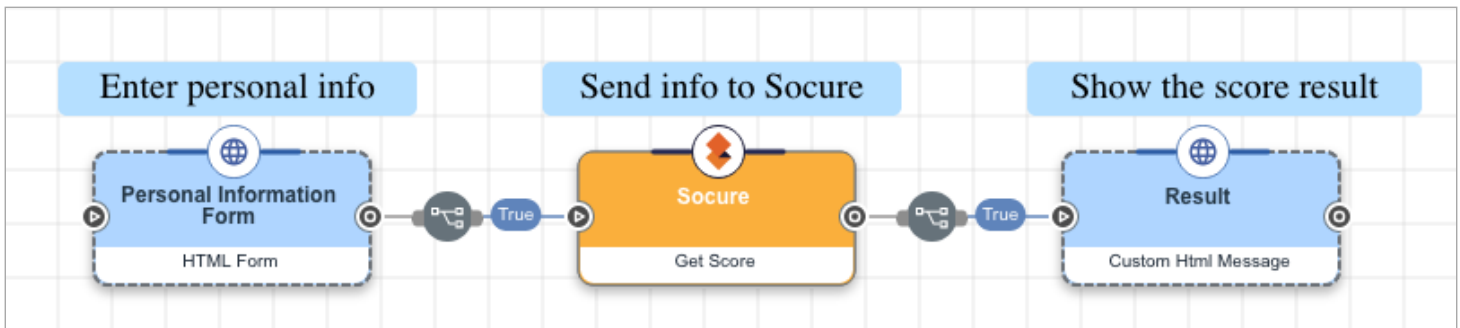
This flow creates a "challenge" to pause the main flow on the QR code while a secondary flow continues the verification process. When the verification process is complete, a [Challenge](#) connector resolves the challenge and triggers the main flow to continue. To learn more about this technique, see the [Challenge](#) connector.

1. Download the [Socure - Identity verification with SMS prompt](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the "Check Your Device" message:



1. Select the **Check Your Device** node.
 2. In the **Message Title** field, customize the title of the prompt.
 3. In the **Message** field, customize the user-facing text.
 4. Click **Apply**.
3. Test the flow:
1. Click **Save**, **Deploy**, and **Try Flow**.
 2. Register a new user or sign in with an existing user.
 3. Enter your mobile device SMS number.
 4. Complete the document verification process on your mobile device.
 5. See the result in your web browser on the original device.

Getting ID+ scores



You can use the connector to get a variety of risk scores, fraud scores, and other information based on information you provide about a person or device.

This flow sends information about a person to Socure then shows the resulting score. You can customize the information you send to and get from Socure.

1. Download the [Socure - ID+ score check](#) flow template. For help, see [Using DaVinci flow templates](#).
2. Select the Socure ID+ modules that you want to use:
 1. On the flow canvas, select the **Get an ID+ Score** node.
 2. In the **Modules** list, select one or more modules.

Note

Socure ID+ modules represent a variety of data sources that verify identities. For more information, see [ID+ Modules](#) in the Socure documentation.

When you use the **Get an ID+ Score** capability, you can select as many modules as you want, with the following limitations:

- Only select modules that you have a license to use in Socure.
- Only select one **Global Watchlist** module.
- If you select the **Decision** module, you have to select at least one other module. For more information, see [Decision](#) in the Socure documentation.
- The **Device Risk** capability requires a device session ID. To get a session ID, include the device profiling script in your web app. The script sends a device profile to Socure and provides a session ID that DaVinci uses to get the device risk score. For help, see [Sigma Device Client-Side Javascript](#) in the Socure documentation.

3. Populate the personal attributes by clicking and selecting variables from your flow.

Note

For demonstration purposes, the flow template includes an HTML form with pre-filled information. When you build your own flow, you can collect information about the person from a form, database, or another source in your flow.

4. Populate the **Document UUID** field with the unique ID for an identity document that the person submitted.
5. Click **Apply**.

6. Test the flow:

1. Click **Save**, **Deploy**, and **Try Flow**.
2. Submit the HTML form.

Capabilities

Verify a Document

Verify the authenticity of an identity document. This uses the Socure Predictive Document Verification Web SDK.

Properties

screen0Config ***title textField***

Default:

Socure Document Verification

bodyHeaderText textField

Default:

Receive you Document verification URL through SMS

Verification Level dropdown required

Set the verification process workflow for the transaction.

- Document upload only (Default)
- Document upload and document verification
- Document upload, document verification, and Phone RiskScore

Country textField

Two letter ISO Country

Input Schema

- registerInitiate object
 - properties object
 - sdkKey string required
 - parameters object
 - phoneNumber string required minLength: 6
- registerComplete object
 - parameters object
 - referenceId string
 - credId string

Wait for the Documentation Verification Result

Wait for Socure to send the result of a document verification check to the DaVinci webhook URL.

Output Schema

- output object
 - rawResponse object
 - id string
 - origId string
 - eventGroup string
 - reason string
 - environmentName string
 - event object
 - eventType string
 - data object
 - address string
 - dob string
 - documentNumber string
 - expirationDate string
 - firstName string
 - surName string
 - fullName string
 - parsedAddress object
 - referenceId string
 - customerUserId number
 - message string
 - uuid string

The value will be undefined for events other than DOCUMENTS_UPLOADED.
 - challenge string
 - credentialStatusObject object
 - detailStatus string
 - rawStatus object
 - challenge string
 - credId string

■ userId string

Output Example

```
{ "rawResponse" :
  { "id" : "efgh2345-6fg7-89h0-12ij-3k4567l890n",
    "origId" : "af096ad4-b9ba-4935-a148-61837aa535c4",
    "eventGroup" : "DocvNotification",
    "reason" : "DOCUMENTS_UPLOADED",
    "environmentName" : "production",
    "event" :
    { "eventType" : "DOCUMENTS_UPLOADED",
      "data" :
      { "address" : "965 Maxwell Street Petty, TX 75470",
        "dob" : "1979-05-07",
        "documentNumber" : "SOC86753099",
        "expirationDate" : "2022-10-13",
        "firstName" : "John",
        "surName" : "Smith",
        "fullName" : "John Smith",
        "parsedAddress" :
        { } },
        "referenceId" : "abcd1234-5ef6-78g9-01hi-2j3456k7890m",
        "customerUserId" : 121212,
        "message" : "Documents Upload Successful" } },
    "challenge" : "66680a42-2d4d-408f-aa64-f40c8dd752d0",
    "credentialStatusObject" :
    { "detailStatus" : "VERIFICATION_COMPLETED",
      "rawStatus" :
      { },
      "challenge" : "66680a42-2d4d-408f-aa64-f40c8dd752d0",
      "credId" : "6d9vb6l0p2e56jgfs7oke318akm556",
      "userId" : "1f9cd66c12e46eaf15c7e2e318a7c5d3" } }
```

Get an ID+ Score

Get a Socure ID+ score for a user based on the ID+ modules that you select. The result is a number between 0 and 1, with a higher value indicating higher probability of fraud.

Properties

modules dropDownMultiSelect

First Name textField

Sur Name textField

Email textField

Country textField

Physical Address textField

Physical Address 2 textField

City textField

State textField

Zip textField

Mobile Number textField

Geocodes (lat long) textField

National ID textField

Date of Birth textField

Company Name textField

Document UUID textField

Order Amount textField

Account Creation Date textField

Submission Date textField

Previous Order Count textField

Last Order Date textField

Order Channel textField

Customer User ID textField

The unique identifier for the user, such as "123".

Watchlist Filters textField

Recipient Country textField

Payment Type textField

Disbursement Type textField

Operation System textField

Device Type textField

Device Session ID textField

Device Interface textField

Input Schema

- login object
 - properties object
 - baseUrl string required
 - apiKey string required
 - modules array required
 - ip string
 - userAgent string

Output Schema

- output object
 - rawResponse object
 - referenceId string
 - nameAddressCorrelation object
 - reasonCodes array
 - score number
 - namePhoneCorrelation object
 - reasonCodes array
 - score number
 - fraud object
 - reasonCodes array
 - scores array
 - kyc object
 - reasonCodes array
 - cvi integer
 - correlationIndices object
 - nameAddressPhoneIndex integer
 - nameAddressSsnIndex integer
 - decision object
 - modelName string
 - modelVersion string
 - status string
 - fieldValidations object
 - firstName number
 - surName number
 - streetAddress number
 - city number
 - state number
 - zip number

- mobileNumber number
- dob number
- ssn number
- addressRisk object
 - reasonCodes array
 - score number
- emailRisk object
 - reasonCodes array
 - score number
- phoneRisk object
 - reasonCodes array
 - score number

Output Example

```

{ "rawResponse" :
  { "referenceId" : "123a456b-789c-1234-567c-9307e6e0a83f",
    "nameAddressCorrelation" :
    { "reasonCodes" :
      [ "I709",
        "I708",
        "I710" ],
      "score" : 0.9096 },
    "namePhoneCorrelation" :
    { "reasonCodes" :
      [ "I621",
        "I622",
        "I618" ],
      "score" : 0.9984 },
    "fraud" :
    { "reasonCodes" :
      [ "I610",
        "I626",
        "I705",
        "I609",
        "I553",
        "I611",
        "I614",
        "I127",
        "I630",
        "I708",
        "I618",
        "I555",
        "I707",
        "I602" ],
      "scores" :
      [
        { "name" : "sigma",
          "version" : "1.0",
          "score" : 0.167 } ] },
    "kyc" :
    { "reasonCodes" :
      [ "I919" ],
      "cvi" : 0,
      "correlationIndices" :
      { "nameAddressPhoneIndex" : 0,
        "nameAddressSsnIndex" : 0 },
      "decision" :
      { "modelName" : "SOCURE_FIX",
        "modelVersion" : "1.0",
        "status" : "REFER" },
      "fieldValidations" :
      { "firstName" : 0.99,
        "surName" : 0.99,
        "streetAddress" : 0.99,
        "city" : 0.99,
        "state" : 0.99,
        "zip" : 0.99,
        "mobileNumber" : 0.99,
        "dob" : 0.99,
        "ssn" : 0.99 } },
    "addressRisk" :
    { "reasonCodes" :
      [ "I610",
        "I705",

```

```
"I720",
"I708",
"I707" ],
"score" : 0.364 },
"emailRisk" :
{ "reasonCodes" :
[ "I520",
"I553",
"I555" ],
"score" : 0.133 },
"phoneRisk" :
{ "reasonCodes" :
[ "I610",
"I626",
"I609",
"I620",
"I611",
"I614",
"I630",
"I618",
"I602" ],
"score" : 0.122 } } }
```

Make Custom API Call

Define and invoke custom call to the Socure REST API.

Properties

Endpoint textField required

The Socure API endpoint, such as /api/3.0/EmailAuthScore.

HTTP Method dropDown required

The HTTP method of the API call.

- GET
- POST
- PUT
- DELETE

Query Parameters keyValueList

Define additional query parameters to send to Socure.

Additional Headers keyValueList

Additional headers for the request. Connector automatically adds 'Authorization' and 'Content-Type' headers.

Body codeEditor

The body of the API call.

Input Schema

- default object
 - properties object
 - apiKey string required
 - endpoint string required
 - method string required
 - queryParams array
 - headers array
 - bodyData object

Input Example

```
{ "properties" :  
  { "endpoint" : "/api/3.0/EmailAuthScore",  
    "method" : "POST",  
    "bodyData" :  
      { "modules" :  
        [ "addressrisk" ],  
        "firstName" : "John",  
        "surName" : "Smith",  
        "physicalAddress" : "123 Example Street",  
        "physicalAddress2" : "Apt. 5",  
        "city" : "New York",  
        "state" : "NY",  
        "zip" : "10001",  
        "country" : "us" } } } }
```

Output Schema

- output object
 - headers object
 - statusCode integer
 - rawResponse object

Get a Document Verification URL and QR Code

Get a unique document verification URL and QR code based on a user identifier.

Properties

Verification Level dropDown required

Set the verification process workflow for the transaction.

- Document upload only (Default)
- Document upload and document verification
- Document upload, document verification, and Phone RiskScore

Customer User ID textField

The unique identifier for the user, such as "123".

Phone Number textField

Used with Verification Level 3

Country textField

Two letter ISO Country

Input Schema

- documentVerificationUrl object::

Output Schema

- output object
 - qrcode string
 - url string

Splunk Connector

The Splunk connector lets you gain real-time operational intelligence through Splunk in your PingOne DaVinci flow.

Setup

Resources

You can find more information and setup help in:

- Splunk:
 - [Splunk Cloud Platform Documentation](#) 
- DaVinci documentation:
 - [Adding a connector](#) 
 - [Using connectors securely](#) 
 - [Using DaVinci flow templates](#) 

Requirements

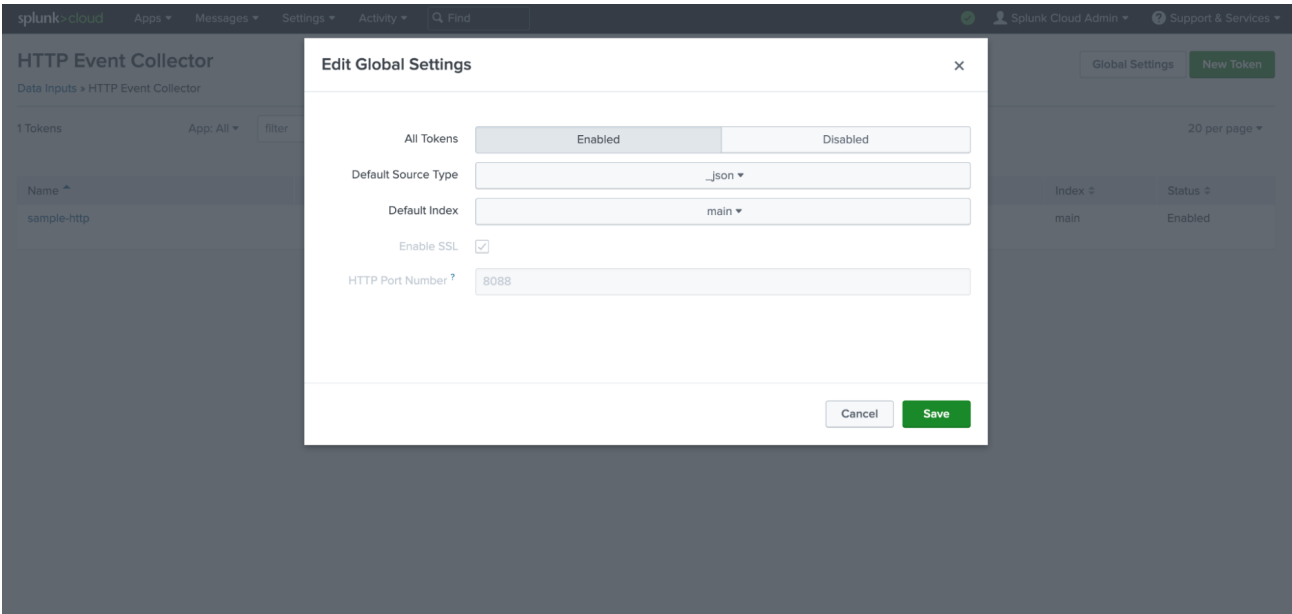
To use the connector, you'll need:

- A Splunk license
- Your Splunk credentials

Setting up Splunk

To set up Splunk, create an HTTP event collector token:

1. Click on **Settings > Data > Data Inputs**.
2. Click **HTTP Event Collector** or click **Actions > Add new button**.
3. Click **Global Settings** and use the following configuration:
 1. Enable the **All Tokens** field.
 2. Set the **Default Source Type** to **_json**.
 3. Set the **Default Index** to **Main**.

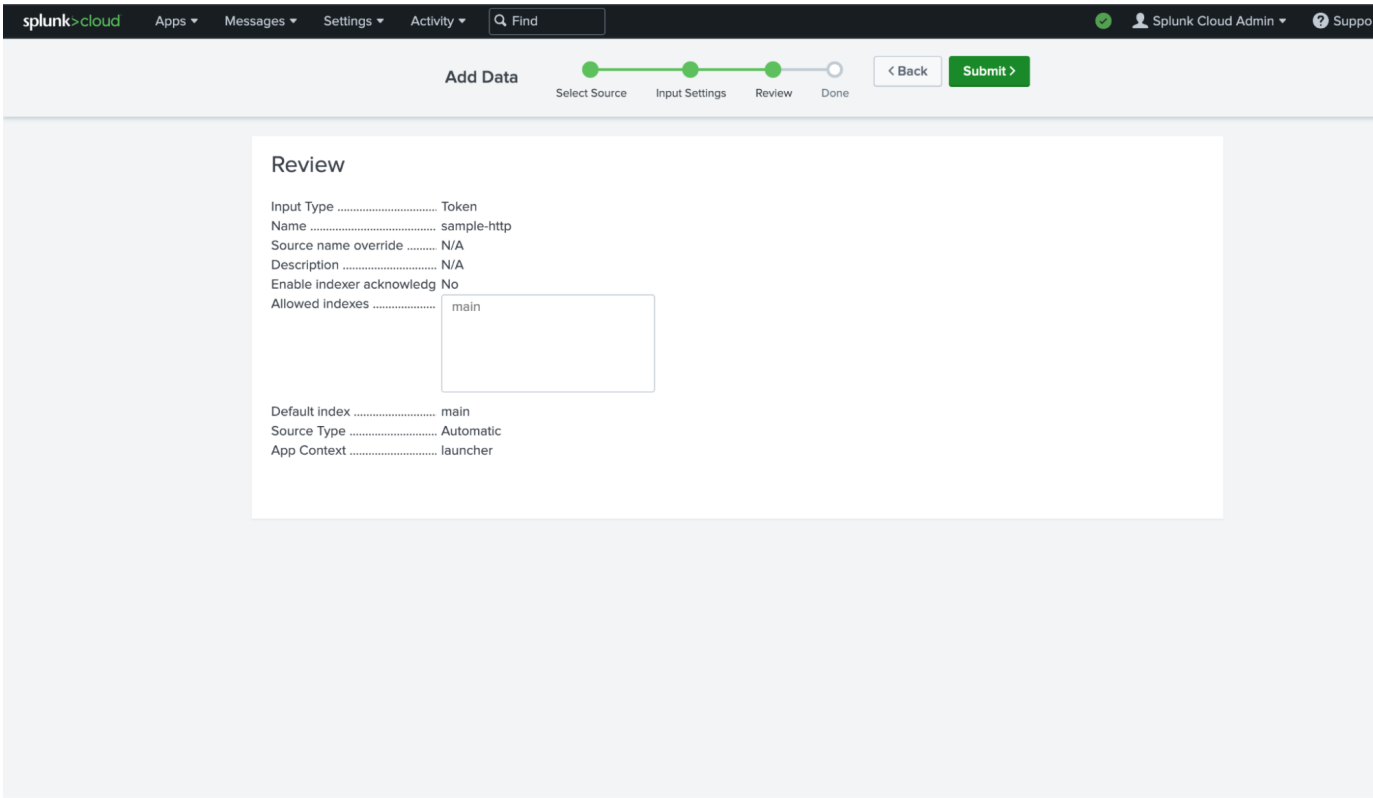


4. Click **Save**.

4. Provide the **Token Name**, then click **Next**.

5. Select **Source Type** as **Automatic** and **Selected Allowed Indexes**. Click **Review**.

6. Click **Submit**.



7. Copy the generated token.

Configuring the Splunk connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Base URL

The **Base URL** you received by email from setting up Splunk.

Port

Enter `8088`.

Token

Paste the **Token** created when setting up Splunk.

Using the connector in a flow

Post a Splunk event

You can use the **Post Splunk Event** capability to post a Splunk event:

1. Add the connector to the flow and configure the fields based on the configuration selected when creating a token.
2. Select the **Event (String)** or **Event (JSON)** to post.
3. Click **Apply**.

Capabilities

Post Splunk Event

Create a new Splunk event.

Properties

Time textField

The event time in the format {sec}.{ms}.

Host textField

The host value to assign to the event data.

Source textField

The source value to assign to the event data.

Source Type textField

The sourcetype value to assign to the event data.

Index textField

The name of the index by which the event data is to be indexed.

Event (String) textField

Event in raw text.

Event (JSON) codeEditor

Event in raw JSON.

Fields keyValueList required

Metadata in Key-Value format.

Input Schema

- default object
 - properties object
 - apiUrl string required
 - token string required
 - time string
 - host string required
 - source string required
 - sourcetype string required
 - index string required
 - event string

Output Schema

- output object
 - rawResponse object
 - code number
 - text string

Output Example

```
{ "rawResponse" :  
  { "code" : 0,  
    "text" : "Success" } }
```

Splunk Connector Release Notes

New features and improvements in the Splunk connector.

April 2025

The Splunk Connector now respects localized error messages

Fixed

Error handling for the Splunk connector has been corrected and now respects localized error messages. As a result, select error outcomes might produce different message text.

November 2024

The Splunk connector is now available

New

You can use the Splunk connector to gain real-time operational intelligence through Splunk in your PingOne DaVinci flow.

String Connector

The String connector lets you transform the text value of a variable in your PingOne DaVinci flow.

You can use the String connector to:

- Convert strings to lowercase, uppercase, or title case
- Convert any type of variable to a different data type
- Concatenate two or more strings
- Encode and decode a string
- Search and replace text in a string
- Generate a random string
- Remove white space from a string

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the String connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Using the connector in a flow

Changing the capitalization of a string

You can use the **Convert to Lowercase**, **Convert to Uppercase**, or **Convert to Title Case** capabilities to change a string's capitalization.

For example, if your **Input String** is `myVariableValue`, you'll get one of the following results depending on the capability you choose:

- `MYVARIABLEVALUE`
- `myvariablevalue`
- `Myvariablevalue`

Changing the case of a string can help you to standardize values before you compare them, such as when using the Function connector.

You can use the **Convert to Lowercase** capability with the **Concatenate** capability to generate usernames. For example, you can take the inputs `John` and `Smith` and convert them to lowercase before using the **Concatenate** capability to convert both variables to `johnsmith@example.com`.

To remove an unnecessary blank space at the beginning or end of your output string, enable **Remove White Space**.

Changing values to another data type

You can use the **Change Data Type** capability to change the data of any value to a **Boolean**, **Number**, or **String**. For example, if your **Input Value** is the string `true`, you can convert to the boolean `true`. Or take the number `3` and convert to the string `"3"`.

Changing the data type is useful for testing that the incoming data is in the correct format. For example, if you want to convert driver license numbers, such as `456123789`, from a string to number, the capability will return `True`. However, if the capability instead receives a passport ID, such as `P123456AA`, it will return `False` (error code `400`; invalid input).

No special configuration is needed. Add the capability and populate its properties according to the help text.

Concatenating two strings

The **Concatenate** capability lets you merge multiple strings.

The following example takes the input strings `john` and `smith` and converts them to `johnsmith@example.com`:

1. In the **Input Value** section, add `john` to the **Value 1** field or click `{}` and select a variable from your flow that contains the string that you want to concatenate.
2. In the **Value 2**, add `smith` or click `{}` and select a variable from your flow that contains the string that you want to concatenate.
3. Click **Add** to include an additional field to concatenate.

String

id: uov3npikay
connectionId: 843f85a3cd3c8ff97906d4502e238317

< TRIGGER:

Concatenate String

* indicates required

Input Value *

Value 1
john

Value 2
smith

Add Edit

Delimiter * ⓘ

Include Final Delimiter ⓘ

Close Apply

4. In the new **Value 3** field, add an email domain such as `@example.com`.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Decoding or encoding a string

The **Decode** and **Encode** capabilities let you decode and encode a string from one of several formats: **Base64**, **URL**, or **Base64 URL**.

For example, you can take the plain text input `johnsmith@example.com` and encode with Base64 to `am9obnNtaXRoQGV4YW1wbGUuY29t`.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Searching and replacing content

The **Find Substring** capability lets you find a substring and its index. The outputs will include a **found** variable which is a boolean returning true if the substring is found and an **index** variable which is the substring's position in the string.

For example, if you take the string `johnsmith@example.com` and search for the substring `exa`, you get the following output:

```
{
  "originalValue": "johnsmith@example.com"
  "match": ["exa"]
  "index": 10
  "found": true
}
```

The **Find and Replace** capability lets you search for text using literal matching or a regular expression. For example, you could replace every instance of `test` with `production`:

1. In the **Input String** field, click `{}` and select a variable from your flow that contains the string that you want to search for.
2. If your original variable value has blank space at the end that you don't want, enable **Trim White Space** to remove it.
3. In the **Input String** field, enter the text that you want to find in the string, such as `test`. Alternatively, you can enter a regular expression, such as `/te[xs]t/g`, which will match both `test` and `text` and the `/g` flag will apply the change to all matches in the input string.
4. If you entered a regular expression in the **Input String** field, enable **Search Using Regex**.

Note

Replace Mode is for simple matching. When **Search Using Regex** is enabled, the regex itself determines which matched text is replaced.

5. In the **New Value** field, enter the string that you want to replace the match with, such as `production`.

When **Search Using Regex?** is enabled, the **Search** field accepts regular expressions in the format `/<expression>/`.

Note

This uses the ECMA / JavaScript regex engine. Learn more in [Regular expressions - JavaScript](#) on the MDN site.

For example, you can mask part of a user's email address in the user interface by entering the following regular expression: `/(?<=. {2}).(?:[^\s]*?@)/g`.

 **String** 

id: g7w3hiyd10
connectionId: 843f85a3cd3c8ff97906d4502e238317

 **TRIGGER:**

Find and Replace

GENERALSETTINGS

S

Indicates required

Input Value * 

jsmith@example.com

Search * 

/(?<=.{2}).{?=[^@]*?@)/gm

New String Value * 

*

Search Using Regex? 

☒

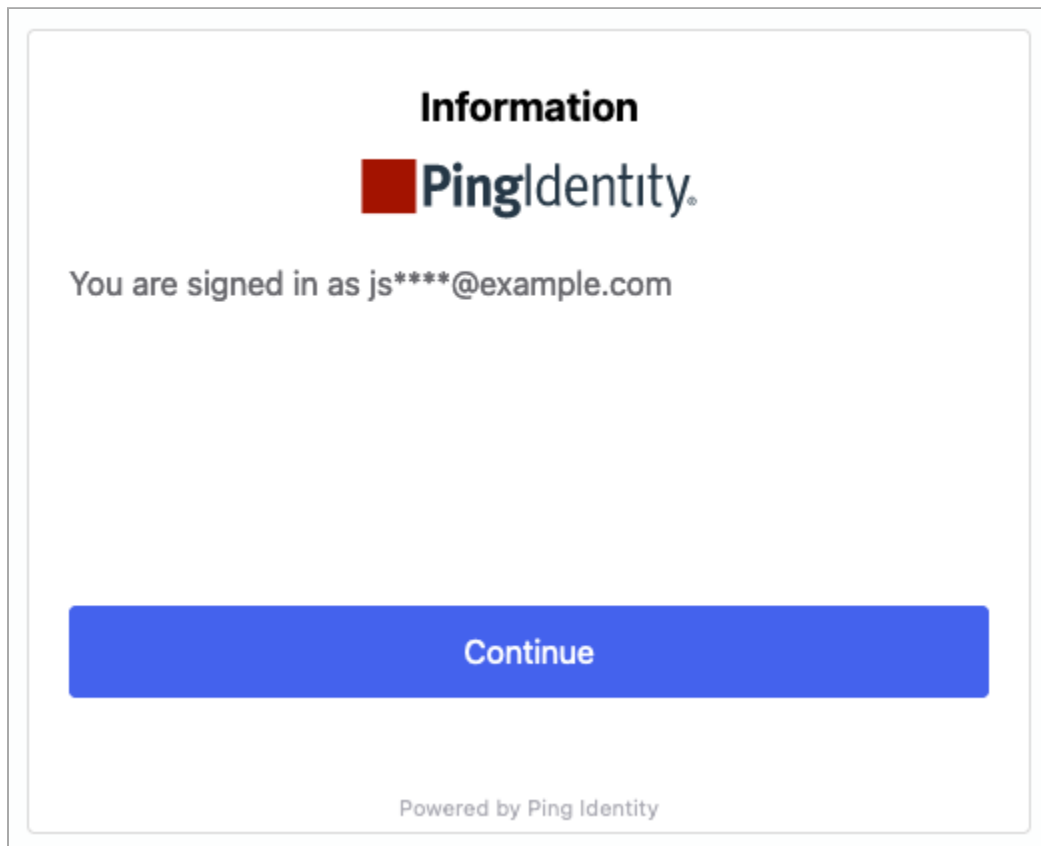
Trim White Space 

☐

Close

Apply

In this example, `jsmith@example.com` becomes `js**@example.com`:



Generating random strings

The **Generate String** capability lets you create pseudorandom numeric or alphanumeric strings of a certain length. You can use this to create temporary passwords or add unique suffixes to user identifiers.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Removing white space from string

The **Remove White Space** capability lets you remove leading or trailing white space from a variable.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Convert to Lowercase

Change a string value to lowercase and optionally remove white space, such as " MYVALUE" to "myvalue".

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - originalValue string/number required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "originalValue" : "Frank",  
  "newValue" : "frank" }
```

Convert to Uppercase

Change a string value to uppercase and optionally remove white space, such as " myvalue" to "MYVALUE".

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - originalValue string/number required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "originalValue" : "Frank",  
  "newValue" : "FRANK" }
```

Convert to Title Case

Change a string value to title case and optionally remove white space, such as " my value" to "My Value".

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - originalValue string/number required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "originalValue" : "my value",  
  "newValue" : "My Value" }
```

Change Data Type

Change the data type of any value to boolean, number, or string.

Properties

Input String textField

The value to process. Enter a string or select a string value from your flow.

Change to dropDown required

Select the data type to change the input value to.

- String (Default)
- Boolean
- Number

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - inputValue string/number required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "newValue" : "frank" }
```

Concatenate

Merge multiple strings together.

Properties

Input String multipleTextFields

The string to process. Enter a string or select a string value from your flow.

Delimiter textField

The optional string to include between each concatenated value, such as ", " or "-".

Include Final Delimiter toggleSwitch

When enabled, the delimiter is also included at the end of the concatenated string.

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - concatenateInput array required
 - concatenateDelimiter string
 - finalDelimiter boolean
 - shouldTrim boolean

Output Schema

- output object
 - originalValue string
 - newValue string

Decode String

Decode a string using one of several formats, such as Base64 or URL.

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

String Decode Method dropdown required

The decoding format applied to the input string.

- Base64 (Default)
- URL
- Base64 URL

Input Schema

- default object
 - properties object
 - originalValue string required
 - method string

Output Schema

- output object
 - originalValue string
 - newValue string

Encode String

Encode a string using one of several formats, such as Base64 or URL.

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

String Encode Method dropdown required

The encoding format applied to the input string.

- Base64 (Default)
- URL
- Base64 URL

Input Schema

- default object
 - properties object
 - originalValue string required
 - method string

Output Schema

- output object
 - originalValue string
 - newValue string

Find Substring

Find a substring and its index.

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Find Substring textField required

The substring to process. Enter a string or select a string value from your flow.

Input Schema

- default object
 - properties object
 - originalValue string required
 - finder string required

Output Schema

- output object
 - originalValue string
 - match string
 - index number
 - found boolean

Find and Replace

Replace part of a string using simple matching or Regex.

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Search textField

The text to search for in the original string value. For simple matching, enter literal text, such as "test". For more complex matching, enter a valid regular expression and enable Search Using Regex. For example, entering "te[xs]t/g" matches both "test" and "text".

New String Value textField

When a match is found, the text identified by the Search field is replaced with this string.

Search Using Regex? toggleSwitch

By default, the value in the Search field is used for simple matching. When enabled, the value in the Search field must be formatted as a regular expression such as "/<expression>/g"

Replace Mode dropDown

Determines whether the first match or all matches are replaced with the new value.

- All Matches
- First Match (Default)

Trim White Space toggleSwitch

When enabled, removes any white space at the beginning or end of the input string.

Input Schema

- default object
 - properties object
 - originalValue string/number required
 - oldToken string/number required
 - newToken string/number required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "newValue" : "frank" }
```

Generate String

Generate an alphabetic or alphanumeric string of a defined length.

Properties

String Length textField

Enter the number of characters you want in the string, such as "15".

Include Numbers toggleSwitch

By default, generated strings are a mix of uppercase and lowercase letters. When enabled, the string also includes numbers.

Input Schema

- default object
 - properties object
 - length number required
 - isAlphaNumeric boolean

Output Schema

- output object
 - generatedString string

Output Example

```
{ "generatedString" : "aivsdvjqwoit" }
```

Remove White Space

Remove leading or trailing white space.

Properties

Input Value textField

The string to process. Enter a string or select a string value from your flow.

Input Schema

- default object
 - properties object
 - originalValue string required

Output Schema

- output object
 - originalValue string
 - newValue string

Output Example

```
{ "newValue" : "my value" }
```

Teleport Connector

The Teleport connector lets you visually organize and subdivide a flow within your PingOne DaVinci flow canvas.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Teleport connector

In DaVinci, add a Teleport connector. For more information, see [Adding a connector](#).

Note

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Manage large flows

Use Teleport nodes to connect different sections of the flow. This makes the flow more readable by breaking it down into discrete sections. It also lets you reuse some sections of the flow rather than duplicating content.

Manage looping flows

When flows loop, the canvas can become cluttered. Avoid this by defining a start node at the point where the loop returns, then using the Teleport connector to go to that start node to execute the loop.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Define a Start Node

Define the node where the flow will start.

Properties

inputSchema codeEditor

Follow example for JSON schema.

Default:

```
{
  "type": "object",
  "properties": {
    "success": {
      "type": "boolean",
      "displayName": "success",
      "preferredControlType": "textField",
      "enableParameters": true,
      "propertyName": "success"
    }
  }
}
```

Input Schema

- default object

Go to Start Node

Go to a specific start node defined in the flow.

Properties

nodeInstanceId dropDown

Teleport to this node. Give your nodes a name in case you see duplicate names in the list

Input Schema

- default object

Return to Calling Node

Return to the node where the flow starts.

Properties

outputSchema codeEditor

Follow example for JSON schema.

Default:

```
{
  "type": "object",
  "properties": {
    "success": {
      "type": "boolean",
      "displayName": "success",
      "preferredControlType": "textField",
      "enableParameters": true,
      "propertyName": "success"
    }
  }
}
```

Input Schema

- default object

Token Management Connector

The Token Management connector lets you create and read JSON Web Token (JWT) tokens and manage OpenID Connect (OIDC) redirects in your PingOne DaVinci flow.

You can use the Token Management connector to:

- Create ID, access, or JWT tokens.
- Get details about tokens.
- Redirect user with error.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Token Management connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Note

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Token creation

The connector has several capabilities that allow you to create tokens:

- Create Tokens with OIDC Redirect
- Create Tokens with Custom Claims
- Create Tokens without OIDC Redirect

No special configuration is needed. Add the capability and populate its properties according to the help text.

Token details

The connector has several capabilities that allow you to get details about tokens:

- **Get Session Token Details**
- **Validate Token Details**

No special configuration is needed. Add the capability and populate its properties according to the help text.

Validating and parsing a JWT token

You can use the **Validate JWT Token** capability to parse and validate a JSON Web Token (JWT). The capability parses by getting the details, or claims, from the JWT token, such as the issuer, subject, or audience. Then, the capability validates by accepting the JWT token if it meets criteria, such as whether it has expired or if it has the correct issuer or audience.

If the validation rules are set and the JWT token passes, then the claims are parsed and output from the capability. If the validation rules are set and the JWT token fails, the flow continues down the False branch.

To validate a JWT token:

1. In your flow, add a **Token Management** connector with the **Validate JWT Token** capability.
2. In the **Token** field, enter the value or select the variable containing the JWT token to validate.
3. Select the **Public Key Type**. This field determines whether to provide a key directly from DaVinci, by pasting **Public Key PEM Contents**, or by pointing to a JWKS file by URL.
4. (Optional) Toggle the **Validate Expiration Time**. When enabled, the token must not be expired to be considered valid.
5. (Optional) Select which **Valid Algorithms** the token can be created from or select **Any**.
6. Enter any **Valid Issuers**, **Valid Subjects**, or **Valid Audiences** for the token to be considered valid. Click **Apply**.

OIDC redirect with error

You can use the **Redirect User with Error** capability to redirect users with error.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Capabilities

Create Tokens

ID/Access/Session JWT Tokens and OIDC Redirect

Properties

createSessionTokenFlag toggleSwitch

Input Schema

default object

userInfo object

skOpenId object

domainPublicHost string

Create Tokens with Custom Claims

ID/Access/Session JWT Tokens with Custom Claims and OIDC Redirect

Properties

claimsNameValuePairs selectNameValueListColumn

idTokenExpiry textField

claimsNameValuePairsAccessToken selectNameValueListColumn

accessTokenExpiry textField

createSessionTokenFlag toggleSwitch

claimsNameValuePairsSessionToken selectNameValueListColumn

sessionTokenExpiry textField

customScopesFlag toggleSwitch

customScopes textField

customScopesSeparateField toggleSwitch

customScopesSeparateFieldName textField

encryptionFlag toggleSwitch

encryptionKey codeEditor

encryptionAlg dropDown

encryptionContentAlg dropDown

shadowUserNotPresentFlag toggleSwitch

Input Schema

default object

userInfo object

skOpenId object

domainPublicHost string

Get Session Token Details

Session Token claims are extracted from the JWT token

Properties

sessionTokenName textField

Default:

sessionToken

sessionTokenLocation dropDown

sessionToken textField

resolveToUser toggleSwitch

Input Schema

default object

type object

Output Schema

output object

claims object

properties object

sub string

aud string

iss string

usage string

loa number

scope string

jti string

iat number

exp number

Get Token Details

Claims are extracted from any JWT token signed by DaVinci

Properties***genericToken*** textField***errorOnExpiry*** toggleSwitch**Input Schema*****default*** object***type*** object**Output Schema*****output*** object***claims*** object***properties*** object***sub*** string***aud*** string***iss*** string***usage*** string***loa*** number***scope*** string***jti*** string***iat*** number***exp*** number**Redirect User with Error**

Redirect user to RP with standard/customized error

Properties***customErrorFlag*** toggleSwitch***errorMessage*** textField***errorDescription*** textField***errorCode*** textField***errorReason*** textField**Input Schema*****default*** object***skOpenId*** object**Create Tokens**

Create Tokens (without any OIDC Redirect).

Properties

createIdTokenFlag toggleSwitch

claimsNameValuePairs selectNameValueListColumn

idTokenExpiry textField

createAccessTokenFlag toggleSwitch

claimsNameValuePairsAccessToken selectNameValueListColumn

accessTokenExpiry textField

createSessionTokenFlag toggleSwitch

claimsNameValuePairsSessionToken selectNameValueListColumn

sessionTokenExpiry textField

customScopesFlag toggleSwitch

customScopes textField

customScopesSeparateField toggleSwitch

customScopesSeparateFieldName textField

Input Schema

default object

userInfo object

skOpenId object

domainPublicHost string

Output Schema

output object

access_token string

id_token string

session_token string

Token Management Connector Release Notes

New features and improvements in the Token Management connector.

October 2024

Get Token Details is now Validate JWT Token

New

We have enhanced the **Get Token Details** capability to make it easier to work with JSON Web Tokens (JWT) in your flow. To reflect these new features, the capability is now named **Validate JWT Token**. The new capability is backward compatible with DaVinci tokens, but you can now decrypt any token created with PS*, RS*, ES*, or HS* algorithm by providing the associated public or secret key and, if applicable, the key ID.

You can now configure the capability to validate a variety of claims, including the algorithm, audience, issuers, or subjects. The **Error If Token Is Expired** field is now named **Validate Expiration Time**. When a token fails the validation rules, the flow continues down the False path. When the token passes, DaVinci provides the claims in the output schema and the flow continues down the True path.

TransUnion TLOxp Connector

The TransUnion TLOxp connector lets you verify a user's identity information in your PingOne DaVinci flow by checking TransUnion's trusted data sources.

After you have collected a user's personally identifying information, such as their name and date of birth, you can use the connector to:

- Match a user's personal information against TransUnion's records
 - TransUnion searches for a person that matches the provided information then provides a report token, an overall match score, and individual match scores for each attribute that was provided. You can adjust your search scope to return a single person, allow multiple results, or allow TransUnion to expand the search parameters if it doesn't find a result right away.
- Get additional information about a person
 - With the token provided from an information match report, you can search TransUnion for more information associated with the same person. Automatically collecting more information about a user can improve the user experience for your registration flows.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need TransUnion TLO API credentials. For help getting credentials, speak to a TransUnion representative.

Setting up TransUnion TLOxp

You must contact TransUnion support to get DaVinci and PingOne IP addresses added to the allow list for your TransUnion tenant.

For lists of IP addresses, see:

- [IP address and domain reference](#)
- [PingOne IP Addresses](#)

Configuration and TransUnion TLOxp connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

For help with these settings, speak to a TransUnion representative.

API URL

Your TransUnion TLO web service URL.

Username

Your TransUnion API user name.

Password

Your TransUnion API password.

DPPA Purpose Code

The Drivers' Privacy Protection Act (DPPA) code that determines the level of data access in the API.

GLB Purpose Code

The Gramm-Leach Bliley Act (GLBA) code that determines the level of data access in the API.



Important

The DPPA and GLBA codes are legal declarations required to safeguard the proper use of personal information. The codes you provide must correspond to allowable codes for your industry. To determine which codes are allowed for your industry, go to <https://tloxp.tlo.com/account.php?action=api> and sign on with your TLOxp API credentials. For help, speak to a TransUnion representative.

The example flows below use the following TransUnion TLOxp demo API settings:

- **API URL:** <https://demoapi.tlo.com/TLOWebService.asmx>
- **DPPA Purpose Code:** 1
- **GBL Purpose Code:** 1

Ask a TransUnion representative for a username and password to access the demo API.

Testing the connector

To test the connector, use the **Echo Test** capability and output the result in an HTML message.

1. In your flow, add the **TransUnion TLOxp** connector and select the **Echo Test** capability. Select the node that appears in your flow.
2. Following your **Echo Test** node, add an **HTTP** node and select the **Custom HTML Message** capability. Select the node that appears in your flow.
3. In the **Message** field, click **{}** and select the **rawResponse** object from your **Echo Test** node by clicking **(+)**.
4. Click **Apply**. Save, deploy, and run your flow.
5. If you receive an error, check the log for the **Echo Test** node. For help, see [Viewing flow analytics](#).

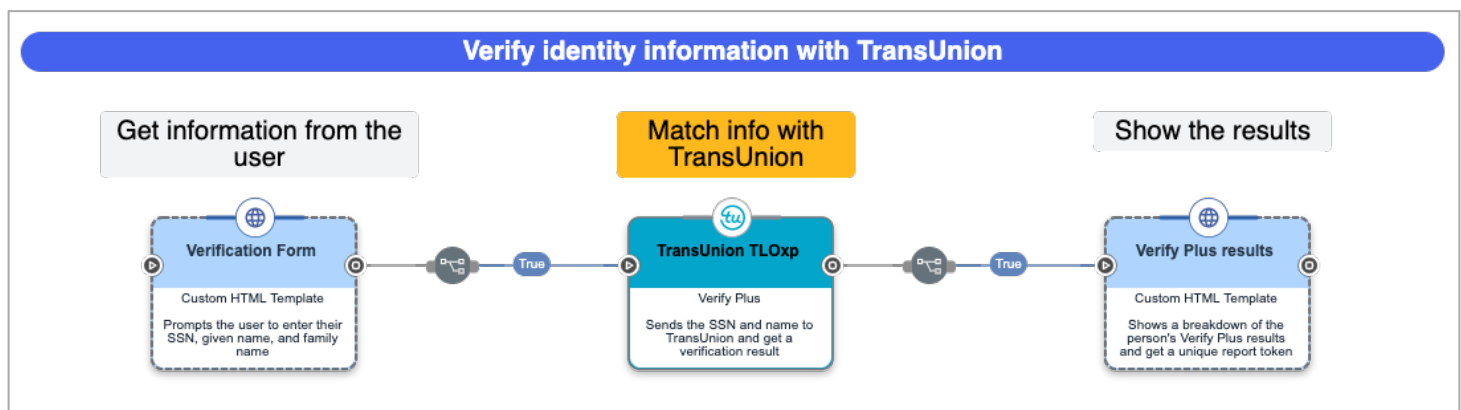
Using the connector in a flow

To see these use cases in a flow, search for **TransUnion TLOxp** in the [Flow Library](#).

Build these two use cases in the order presented to create a single flow.

If you want to follow them exactly as described, use the TransUnion demo API information mentioned in the **Connector configuration** section.

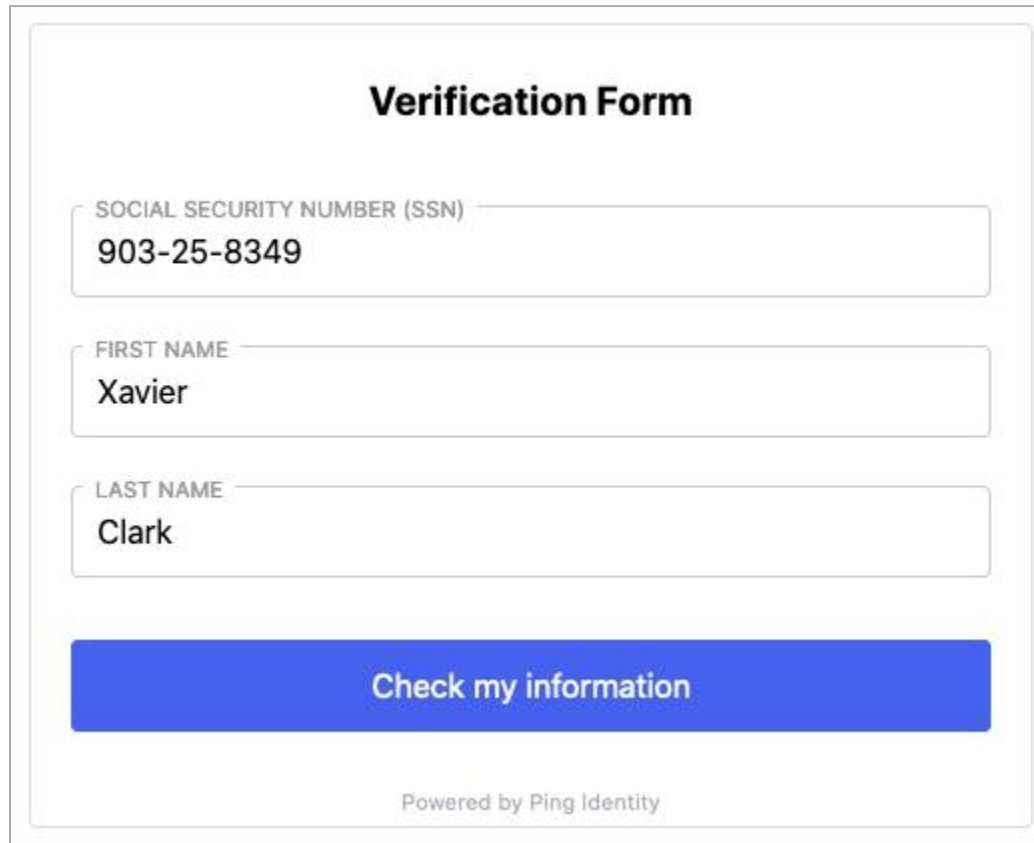
Looking up a person with TransUnion VerifyPlus



This flow collects user information with an HTML form, uses the connector to send it to TransUnion, then shows the results on an HTML page.

1. Download the [TransUnion TLOxp - VerifyPlus identity lookup](#) flow template. For help, see [Using DaVinci flow templates](#).

2. (Optional) Customize the verification form:



Verification Form

SOCIAL SECURITY NUMBER (SSN)

FIRST NAME

LAST NAME

Check my information

Powered by Ping Identity

1. Select the **Sign On Form** node.

2. In the **HTML Template** field, customize the page that users see when signing on. Click **Apply**.

3. (Optional) Customize how the connector sends user information to TransUnion:

1. Select the **Verify Plus** node.

2. (Optional) Turn on **Find Best Match** if you want TransUnion to apply additional checks and possibly additional searches in an attempt to match the results against the search criteria. For details, speak to a TransUnion representative.

3. (Optional) Turn off **Do Not Modify Search** if you want TransUnion to expand the search parameters in cases where no match was found.

4. Click **Apply**.

4. Test the flow:

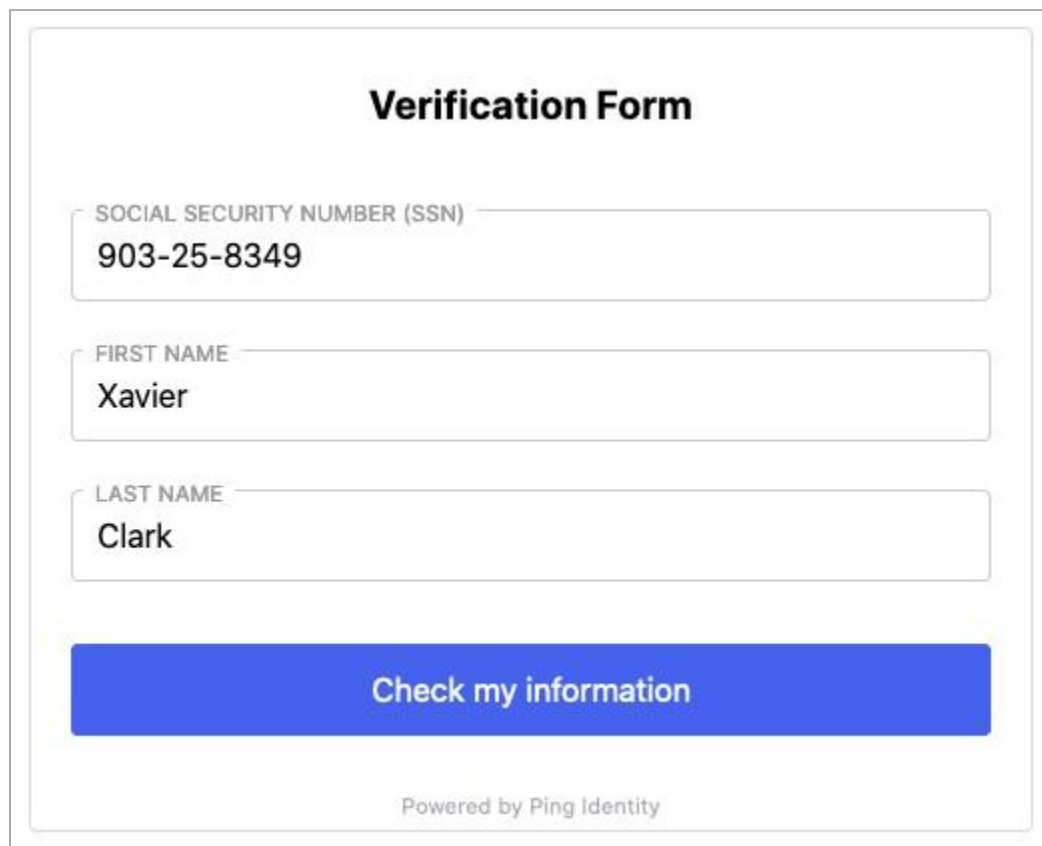
1. Click **Save**, **Deploy**, then **Run**.

2. Enter the following test information:

■ **Social Security Number (SSN):** 903-25-8349

■ **First Name:** Xavier

■ **Last Name:** Clark

A screenshot of a web-based verification form. The form is titled "Verification Form" in bold black text at the top center. Below the title are three input fields. The first field is labeled "SOCIAL SECURITY NUMBER (SSN)" and contains the text "903-25-8349". The second field is labeled "FIRST NAME" and contains the text "Xavier". The third field is labeled "LAST NAME" and contains the text "Clark". Below these fields is a large blue button with the text "Check my information" in white. At the bottom of the form, there is a small text label "Powered by Ping Identity".

Verification Form

SOCIAL SECURITY NUMBER (SSN)
903-25-8349

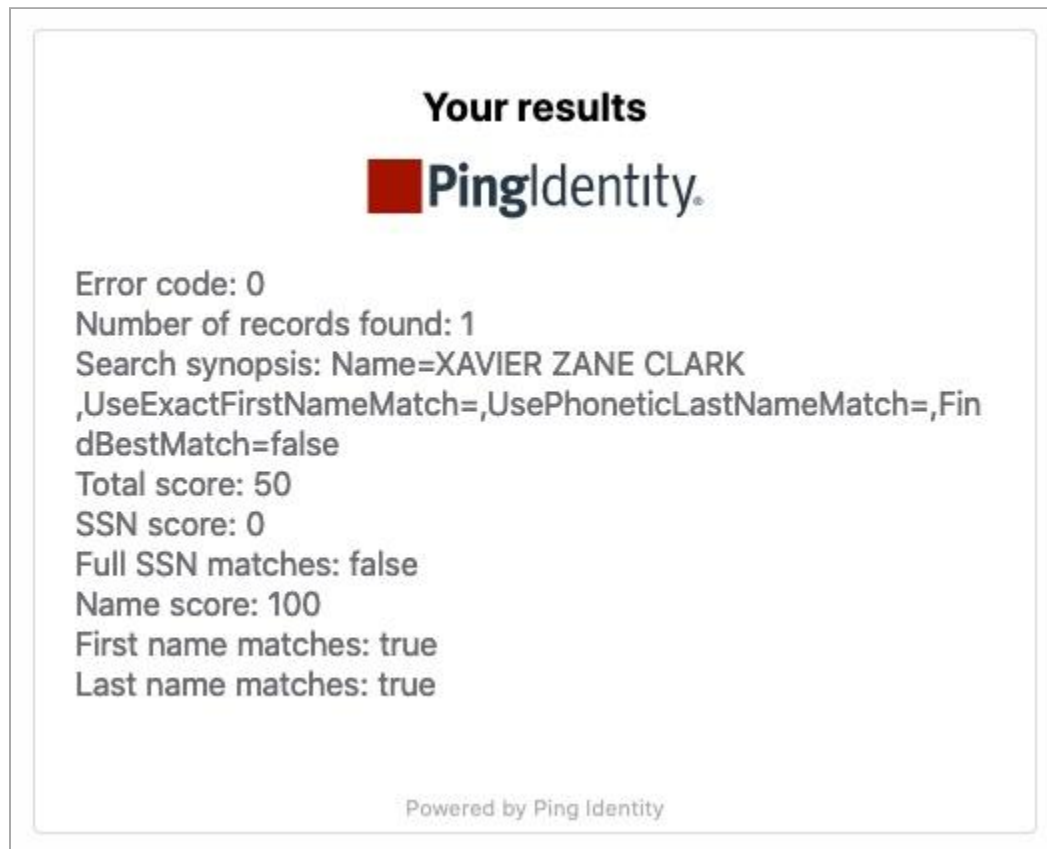
FIRST NAME
Xavier

LAST NAME
Clark

Check my information

Powered by Ping Identity

3. Click **Check my information**.
4. On the **Your results** page, we can see that TransUnion found one matching record with a total score of 50.



You can use the [Function](#) connector to check these variables to make branching decisions. For example:

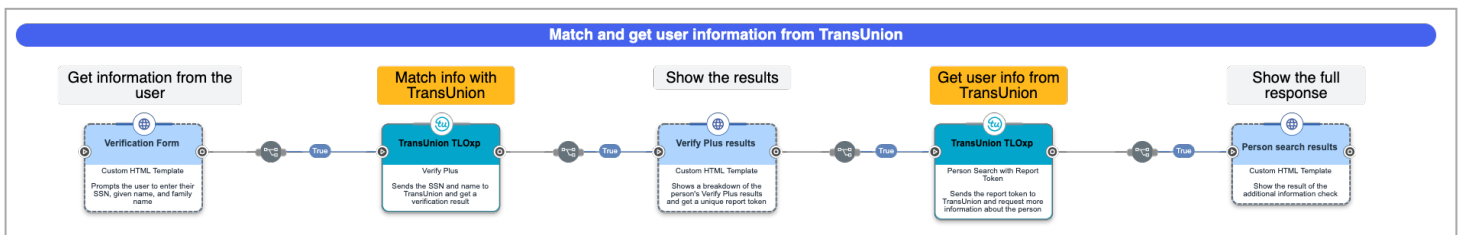
- When the `errorCode` attribute is anything other than `0`, bypass the verification process.
- When the `totalScore` attribute is below 50, show an error.



Tip

For a complete list of attributes you can work with in your flow, see the capability's output schema ([Verify Plus](#) → [Schema](#) → [Output Schema](#)).

Getting more information about a person



This flow takes the result of a VerifyPlus lookup and requests additional information about the person.

1. Download the [TransUnion TLOxp - Additional personal information](#) flow template. For help, see [Using DaVinci flow templates](#).
2. (Optional) Customize the verification form:

Verification Form

SOCIAL SECURITY NUMBER (SSN) 903-25-8349

FIRST NAME Xavier

LAST NAME Clark

Check my information

Powered by Ping Identity

1. Select the **Sign On Form** node.
2. In the **HTML Template** field, customize the page that users see when signing on. Click **Apply**.
3. (Optional) Customize how the connector sends user information to TransUnion:
 1. Select the **Verify Plus** node.
 2. (Optional) Turn on **Find Best Match** if you want TransUnion to apply additional checks and possibly additional searches in an attempt to match the results against the search criteria. For details, speak to a TransUnion representative.
 3. (Optional) Turn off **Do Not Modify Search** if you want TransUnion to expand the search parameters in cases where no match was found.
 4. Click **Apply**.
4. Test the flow:
 1. Click **Save, Deploy**, then **Run**.
 2. Complete the **Verification Form**:
 1. Enter the following test information:
 - **Social Security Number (SSN):** 903-25-8349
 - **First Name:** Xavier
 - **Last Name:** Clark

Verification Form

SOCIAL SECURITY NUMBER (SSN)

903-25-8349

FIRST NAME

Xavier

LAST NAME

Clark

Check my information

Powered by Ping Identity

2. Click **Check my information**.

3. On the **Your results** page, click **Get more information**.



- Review the information that TransUnion matched for Xavier Clark. It provides his various email addresses, names, phone numbers, and so on.

How you process this information will vary depending on your organization's needs. When you build your flow, follow your **Person Search with Report Token** node with a [Function](#) connector to branch your flow based on the results from TransUnion.

Capabilities

Echo Test

Test whether your credentials can reach the API

Properties

Echo Test Input textField

A test string for the TransUnion service to echo back.

Input Schema

- default object
 - properties object
 - echoTestInput string
- Test Input

Output Schema

- output object
 - rawResponse object
 - transactionId string
 - errorCode number
 - testOutput string
 - numberOfRecordsFound number
 - responseTime number

Output Example

```
{ "rawResponse" :  
  { "EchoTestResult" :  
    { "TransactionId" : "DEMO-TL01-1E91-737E-7540542",  
      "ResponseTime" : "0",  
      "ErrorCode" : 0,  
      "NumberOfRecordsFound" : 0,  
      "TestOutput" : "my test input" } },  
    "transactionId" : "DEMO-TL01-1E91-737E-7540542",  
    "errorCode" : 0,  
    "testOutput" : "my test input",  
    "numberOfRecordsFound" : 0,  
    "responseTime" : "0" }
```

Verify Plus

Verify your identity with TransUnion's Verify Plus endpoint.

Properties

Find Best Match toggleSwitch

Inform the Verify Plus service to return the best match for the search parameters.

Do Not Modify Search toggleSwitch

Inform the Verify Plus service to modify the search parameters if a good match is not found.

Social Security Number textField

The social security number of the identity you want to verify with Verify Plus.

First Name textField

The first name of the identity you want to verify with Verify Plus.

Middle Name textField

The middle name of the identity you want to verify with Verify Plus.

Last Name textField

The last name of the identity you want to verify with Verify Plus.

Address Line One textField

The Line One Address of the identity you want to verify with Verify Plus.

Address Line Two textField

The Line Two Address of the identity you want to verify with Verify Plus.

Address Line Three textField

The Line Three Address of the identity you want to verify with Verify Plus.

City textField

The resident city of the identity you want to verify with Verify Plus.

State textField

The resident state of the identity you want to verify with Verify Plus.

ZIP Code textField

The resident ZIP Code of the identity you want to verify with Verify Plus.

Country textField

The resident country of the identity you want to verify with Verify Plus.

Birth Day textField

The day portion of the birth date of the identity you want to verify with Verify Plus.

Birth Month textField

The month portion of the birth date of the identity you want to verify with Verify Plus.

Birth Year textField

The year portion of the birth date of the identity you want to verify with Verify Plus.

Input Schema

- default object
 - properties object
 - findBestMatch boolean
 - Find Best Match
 - doNotModifySearch boolean
 - Do Not Modify Search
 - ssn string
 - Social Security Number (SSN)
 - firstName string
 - First Name
 - middleName string
 - Middle Name
 - lastName string
 - Last Name
 - addressLineOne string
 - Address Line One
 - addressLineTwo string
 - Address Line Two
 - addressLineThree string
 - Address Line Three
 - city string
 - City
 - state string
 - State
 - zip string
 - ZIP Code
 - county string
 - County
 - dobDay string

Birth Day

■ dobMonth string

Birth Month

■ dobYear string

Birth Year

Output Schema

- output object
 - rawResponse object
 - transactionId string
 - errorCode number
 - numberOfRecordsFound number
 - responseTime number
 - searchSynopsis string
 - reportToken string
 - totalScore number
 - ssnScore number
 - fullSsnMatches boolean
 - nameScore number
 - firstNameMatches boolean
 - middleNameMatches boolean
 - lastNameMatches boolean
 - addressScore number
 - unitDesignationMatches boolean
 - streetAddressMatches boolean
 - cityStateZipMatches boolean
 - dobScore number
 - dobDayMatches boolean
 - dobMonthMatches boolean
 - dobYearMatches boolean

Output Example

```

{ "rawResponse" :
{ "PersonSearchResult" :
{ "TransactionId" : "DEMO-TL01-60BD-2899-5143141",
  "RequestId" : "",
  "ResponseTime" : "0",
  "ErrorCode" : 0,
  "NumberOfRecordsFound" : 1,
  "BillableRecordsFound" : "1",
  "ActualSearchInput" :
{ "Username" : "1DEMO.GSA",
  "HostIP" : "54.244.31.249",
  "RequestId" : "",
  "DPPAPurpose" : "1",
  "GLBPurpose" : "1",
  "ReportToken" : "838X-PW3C" },
  "NumberOfRecordsFoundWithModifiedSearch" : 0,
  "PersonSearchOutputRecords" :
{ "TLOPersonSearchOutputRecord" :
[
{ "ReportToken" : "838X-PW3C",
  "SSNRecords" :
{ "SSNRecord" :
[
{ "SSN" : "XXXXX6082",
  "SSNPlaceOfIssue" : "CALIFORNIA",
  "SSNIssueYears" : "1991",
  "SSNToken" : "ansLO+9hZuomWWSUVJdxQjA==",
  "SSNUnlockToken" : "2k1mbAxbtYi71gj0W0dAzc/s5g9MMrenOet0RrWUlkM=" },

{ "SSN" : "XXXXX9999",
  "SSNToken" : "aneu/Q0p/1oBF+QTqR4siLw==",
  "SSNUnlockToken" : "A0+LFYCLXQ/40fgYaePCYBqG7+0JWl0dL8MAQa8MqYc=" },

{ "SSN" : "XXXXX9999",
  "SSNToken" : "aBQeiGxrQf9QRPTNoV6RFMg==",
  "SSNUnlockToken" : "fDUi6y45LhcNn6NzEZLs6s+j4yQG57U6Q8U1Ck+AA4s=" },

{ "SSN" : "XXXXX6002",
  "SSNPlaceOfIssue" : "CALIFORNIA",
  "SSNIssueYears" : "1991",
  "SSNToken" : "av+hpuFXQ5egC6wrSmJQXug==",
  "SSNUnlockToken" : "BkN8kXf9MAscYQ1pi+u4fFJ9C9z1+5hNy0Foa0ekmPw=" },

{ "SSN" : "XXXXX9999",
  "SSNToken" : "ay+Rp9hLpA+/mNFHBVGEDcQ==",
  "SSNUnlockToken" : "W7GjS0fg3nwsUdSb0eGgmp6G739DAoZkf9Q/bALECMM=" } ] },
  "NumberOfAddresses" : "36",
  "EmailAddresses" : null,
  "NumberOfBankruptcies" : "0",
  "NumberOfBankruptcyRecords" : "0",
  "NumberOfLiens" : "32",
  "NumberOfJudgments" : "5",
  "MostRecentLienDate" :
{ "Day" : "03",
  "Month" : "06",
  "Year" : "2015" },
  "MostRecentJudgmentDate" :
{ "Day" : "05",
  "Month" : "08",
  "Year" : "2016" },

```

```

"Names" :
{ "BasicName" :
[
{ "FirstName" : "MARK",
  "MiddleName" : "ULYSSES",
  "LastName" : "MILLER",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "03",
    "Month" : "06",
    "Year" : "1998" },
  "DateLastSeen" :
  { "Day" : "03",
    "Month" : "09",
    "Year" : "2020" } },

{ "FirstName" : "MARK",
  "MiddleName" : "ULYSSES",
  "LastName" : "MILLER",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "01",
    "Month" : "02",
    "Year" : "2006" },
  "DateLastSeen" :
  { "Day" : "09",
    "Month" : "06",
    "Year" : "2019" } },

{ "FirstName" : "MARK",
  "MiddleName" : "",
  "LastName" : "SMITH",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "06",
    "Month" : "03",
    "Year" : "2008" },
  "DateLastSeen" :
  { "Day" : "06",
    "Month" : "03",
    "Year" : "2008" } } ] },
"IndividualsSharingSSN" :
{ "TLOIndividualSharingSSN" :
[
{ "Name" :
  { "FirstName" : "XAVIER",
    "MiddleName" : "",
    "LastName" : "WALKER",
    "NameSuffix" : "",
    "DateFirstSeen" :
    { "Day" : "01",
      "Month" : "05",
      "Year" : "2011" },
    "DateLastSeen" :
    { "Day" : "03",
      "Month" : "09",
      "Year" : "2020" } },
  "SSNRecord" :
  { "SSN" : "XXXXX6082",
    "SSNPlaceOfIssue" : "CALIFORNIA",
    "SSNIssueYears" : "1991",
    "SSNToken" : "ansLO+9hZuomWWSUVJdxQjA==" },

```

```

    "SSNUnlockToken" : "nWQwq+Em+2x8N0XY85xrgUMLcZNoIH9Mx1b3DNFJDww=" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "B/MPKi470wjhhoRyqjA10QAVChh0ypPxb/OXRjh6EU8=",
        "Day" : "XX",
        "Month" : "XX",
        "Year" : "1984" },
      "CurrentAge" : "36" },
    "ReportToken" : "JYWN-QR34" } ] },
  "DatesOfBirth" :
  { "BasicDateOfBirthRecord" :
    [
      { "DateOfBirth" :
        { "DOBUnlockToken" : "r3a1Me1Tj4q6N12oiJ0vC3nbIqGIojDs2KDCor0s7Ek=",
          "Day" : "XX",
          "Month" : "XX",
          "Year" : "1984" },
        "CurrentAge" : "36" },

      { "DateOfBirth" :
        { "DOBUnlockToken" : "Bvm7b0jsozo1x1i0KktpekkSx5NY8WMS6rNYzCuoy4=",
          "Day" : "XX",
          "Month" : "XX",
          "Year" : "1984" },
        "CurrentAge" : "36" },

      { "DateOfBirth" :
        { "DOBUnlockToken" : "/PGrSZr26S/cnDTF02hCqAT6k5ykrQ6epPYFRf0sqbY=",
          "Year" : "XXXX" },
        "CurrentAge" : "37" } ] },
  "Addresses" :
  { "BasicAddressRecord" :
    [
      { "ConfirmedAddress" : "",
        "PhoneCounts" : null,
        "DateFirstSeen" :
          { "Day" : "20",
            "Month" : "08",
            "Year" : "2020" },
        "DateLastSeen" :
          { "Day" : "17",
            "Month" : "11",
            "Year" : "2020" },
        "Address" :
          { "Line1" : "1464 S VALLEY LOOP STE 27",
            "City" : "CASTRO VALLEY",
            "State" : "CA",
            "Zip" : "94546",
            "County" : "ALAMEDA",
            "Zip4" : "5915",
            "BuildingName" : "THE USP STORE",
            "Description" : "",
            "SubdivisionName" : "" },
        "Phones" :
          { "BasicPhoneListing" :
            [
              { "ListingName" : "MILLER",
                "PhoneType" : "ActiveLandLine",
                "ListingType" : "Business",
                "Carrier" : "BANDWIDTH.COM CLEC LLC - CA",
                "CarrierType" : "LANDLINE",
                "City" : "HAYWARD",

```

```

    "State" : "CA",
    "County" : "ALAMEDA",
    "TimeZone" : "PT",
    "Score" : "100",
    "Scores" : "Score_1=100",
    "Phone" : "5105115379" },

    { "ListingName" : "THOMAS",
      "PhoneType" : "ActiveLandLine",
      "ListingType" : "Business",
      "Score" : "100",
      "Scores" : "Score_1=100",
      "Phone" : "8001043390" },

    { "ListingName" : "YOUNG, GEORGE FRANK",
      "PhoneType" : "ActiveLandLine",
      "ListingType" : "Business",
      "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
      "CarrierType" : "LANDLINE",
      "City" : "HAYWARD",
      "State" : "CA",
      "County" : "ALAMEDA",
      "TimeZone" : "PT",
      "Score" : "1",
      "Scores" : "Score_1=1",
      "Phone" : "5107055366" } ] } },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "09",
    "Year" : "2003" },
  "DateLastSeen" :
  { "Day" : "02",
    "Month" : "11",
    "Year" : "2020" },
  "Address" :
  { "Line1" : "17 S WASHINGTON SQUARE",
    "City" : "AMERICAN CANYON",
    "State" : "CA",
    "Zip" : "94503",
    "County" : "NAPA",
    "Zip4" : "1422",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "LA VIGNE" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "23",
    "Month" : "06",
    "Year" : "2014" },
  "DateLastSeen" :
  { "Day" : "23",
    "Month" : "06",
    "Year" : "2014" },
  "Address" :
  { "Line1" : "17 S WASHINGTON SQUARE RM 16",
    "City" : "AMERICAN CANYON",
    "State" : "CA",

```

```

    "Zip" : "94503",
    "County" : "NAPA",
    "Zip4" : "1422",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "05",
    "Month" : "10",
    "Year" : "2017" },
  "DateLastSeen" :
  { "Month" : "08",
    "Year" : "2020" },
  "Address" :
  { "Line1" : "3496 E ORANGE CROSSING",
    "City" : "HAYWARD",
    "State" : "CA",
    "Zip" : "94541",
    "County" : "ALAMEDA",
    "Zip4" : "3408",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "07",
    "Year" : "2010" },
  "DateLastSeen" :
  { "Day" : "03",
    "Month" : "06",
    "Year" : "2020" },
  "Address" :
  { "Line1" : "1110 S PINE PASS",
    "City" : "HERCULES",
    "State" : "CA",
    "Zip" : "94547",
    "County" : "CONTRA COSTA",
    "Zip4" : "2741",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" :
  { "BasicPhoneListing" :
    [
      { "ListingName" : "LOPEZ, HARRISON",
        "PhoneType" : "ActiveLandLine",
        "ListingType" : "Residential",
        "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
        "CarrierType" : "LANDLINE",
        "City" : "EL SOBRANTE-PINOLE",
        "State" : "CA",
        "County" : "CONTRA COSTA",
        "TimeZone" : "PT",
        "Score" : "100",
        "Scores" : "Score_1=100",

```

```

        "Phone" : "5101864432" } ] } },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "17",
    "Month" : "11",
    "Year" : "2008" },
  "DateLastSeen" :
  { "Day" : "22",
    "Month" : "05",
    "Year" : "2020" },
  "Address" :
  { "Line1" : "766 NE CHURCH STATION UNIT 26",
    "City" : "OAKLAND",
    "State" : "CA",
    "Zip" : "94602",
    "County" : "ALAMEDA",
    "Zip4" : "2648",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "30",
    "Month" : "06",
    "Year" : "2018" },
  "DateLastSeen" :
  { "Day" : "21",
    "Month" : "02",
    "Year" : "2020" },
  "Address" :
  { "Line1" : "327 E ORANGE STATION",
    "City" : "HAYWARD",
    "State" : "CA",
    "Zip" : "94541",
    "County" : "ALAMEDA",
    "Zip4" : "4388",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "16",
    "Month" : "10",
    "Year" : "2019" },
  "DateLastSeen" :
  { "Day" : "16",
    "Month" : "10",
    "Year" : "2019" },
  "Address" :
  { "Line1" : "2296 N ORANGE PIKE",
    "City" : "EMERYVILLE",
    "State" : "CA",
    "Zip" : "94608",
    "County" : "ALAMEDA",

```

```

"Zip4" : "1093",
"BuildingName" : "",
"Description" : "1 office, 331 apartments",
"SubdivisionName" : "",
"AddressMissingUnitDesignation" : "Yes" },
"Phones" :
{ "BasicPhoneListing" :
[
{ "ListingName" : "RODRIGUEZ, HARRISON XANDER",
"PhoneType" : "ActiveLandLine",
"ListingType" : "Business",
"Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
"CarrierType" : "LANDLINE",
"City" : "OAKLAND",
"State" : "CA",
"County" : "ALAMEDA",
"TimeZone" : "PT",
"Score" : "1",
"Scores" : "Score_1=1",
"Phone" : "5109018384" },

{ "ListingName" : "JONES, HARRISON GABRIEL",
"PhoneType" : "ActiveLandLine",
"ListingType" : "Business",
"Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
"CarrierType" : "LANDLINE",
"City" : "OAKLAND",
"State" : "CA",
"County" : "ALAMEDA",
"TimeZone" : "PT",
"Score" : "1",
"Scores" : "Score_1=1",
"Phone" : "5107761260" } ] } },

{ "ConfirmedAddress" : "",
"PhoneCounts" : null,
"DateFirstSeen" :
{ "Month" : "10",
"Year" : "2008" },
"DateLastSeen" :
{ "Month" : "08",
"Year" : "2010" },
"Address" :
{ "Line1" : "2296 N CENTRAL PIKE STE 45",
"City" : "EMERYVILLE",
"State" : "CA",
"Zip" : "94608",
"County" : "ALAMEDA",
"Zip4" : "1178",
"BuildingName" : "",
"Description" : "1 office, 331 apartments",
"SubdivisionName" : "" },
"Phones" : null },

{ "ConfirmedAddress" : "",
"PhoneCounts" : null,
"DateFirstSeen" :
{ "Day" : "16",
"Month" : "08",
"Year" : "2018" },
"DateLastSeen" :
{ "Day" : "16",

```



```

    "Month" : "08",
    "Year" : "2018" },
    "Address" :
    { "Line1" : "5557 SE WOODS LANE APT 23",
      "City" : "AMERICAN CANYON",
      "State" : "CA",
      "Zip" : "94503",
      "County" : "NAPA",
      "Zip4" : "1176",
      "BuildingName" : "",
      "Description" : "1 office, 216 apartments",
      "SubdivisionName" : "" },
    "Phones" :
    { "BasicPhoneListing" :
      [
        { "ListingName" : "JONES, QUENTIN KAMAL",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
          "CarrierType" : "LANDLINE",
          "City" : "VALLEJO",
          "State" : "CA",
          "County" : "SOLANO",
          "TimeZone" : "PT",
          "Score" : "1",
          "Scores" : "Score_1=1",
          "Phone" : "7077683498" },

        { "ListingName" : "THOMAS, MARK QUENTIN",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
          "CarrierType" : "LANDLINE",
          "City" : "VALLEJO",
          "State" : "CA",
          "County" : "SOLANO",
          "TimeZone" : "PT",
          "Score" : "100",
          "Scores" : "Score_1=100",
          "Phone" : "7077682348" },

        { "ListingName" : "SCOTT, ENZO",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
          "CarrierType" : "LANDLINE",
          "City" : "VALLEJO",
          "State" : "CA",
          "County" : "SOLANO",
          "TimeZone" : "PT",
          "Score" : "1",
          "Scores" : "Score_1=1",
          "Phone" : "7078535132" },

        { "ListingName" : "SCOTT, ENZO",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
          "CarrierType" : "LANDLINE",
          "City" : "VALLEJO",
          "State" : "CA",
          "County" : "SOLANO",

```

```

        "TimeZone" : "PT",
        "Score" : "1",
        "Scores" : "Score_1=1",
        "Phone" : "7078535323" } ] } },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "09",
    "Month" : "04",
    "Year" : "2018" },
  "DateLastSeen" :
  { "Day" : "09",
    "Month" : "04",
    "Year" : "2018" },
  "Address" :
  { "Line1" : "172 S OAK COURT",
    "City" : "HILTON",
    "State" : "NY",
    "Zip" : "14468",
    "County" : "MONROE",
    "Zip4" : "9173",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" :
  { "BasicPhoneListing" :
    [
      { "ListingName" : "JACKSON, YURI",
        "PhoneType" : "ActiveLandLine",
        "ListingType" : "Residential",
        "Carrier" : "OGDEN TELEPHONE COMPANY DBA FRONTIER OGDEN TELEPHONE COMPANY (FRONTIER)",
        "CarrierType" : "LANDLINE",
        "City" : "HILTON",
        "State" : "NY",
        "County" : "MONROE",
        "TimeZone" : "ET",
        "Score" : "86",
        "Scores" : "Score_1=86",
        "Phone" : "5855150834" } ] } },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "08",
    "Month" : "03",
    "Year" : "2018" },
  "DateLastSeen" :
  { "Day" : "08",
    "Month" : "03",
    "Year" : "2018" },
  "Address" :
  { "Line1" : "838 NW BEVERLY PASS",
    "City" : "PITTSBURG",
    "State" : "CA",
    "Zip" : "94565",
    "County" : "CONTRA COSTA",
    "Zip4" : "2499",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

```

```

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "25",
    "Month" : "07",
    "Year" : "2017" },
  "DateLastSeen" :
  { "Day" : "05",
    "Month" : "09",
    "Year" : "2017" },
  "Address" :
  { "Line1" : "176 S WASHINGTON SQUARE",
    "City" : "WESTLAKE VILLAGE",
    "State" : "CA",
    "Zip" : "91362",
    "County" : "VENTURA",
    "Zip4" : "5008",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "03",
    "Month" : "06",
    "Year" : "2017" },
  "DateLastSeen" :
  { "Day" : "03",
    "Month" : "06",
    "Year" : "2017" },
  "Address" :
  { "Line1" : "2239 N LAKE HARBOR",
    "City" : "LAWRENCEVILLE",
    "State" : "GA",
    "Zip" : "30044",
    "County" : "GWINNETT",
    "Zip4" : "6259",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "WEBB GIN FARMS" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "10",
    "Year" : "2011" },
  "DateLastSeen" :
  { "Day" : "02",
    "Month" : "06",
    "Year" : "2016" },
  "Address" :
  { "Line1" : "1284 S WASHINGTON PIKE",
    "City" : "EL SOBRANTE",
    "State" : "CA",
    "Zip" : "94803",
    "County" : "CONTRA COSTA",
    "Zip4" : "3638",
    "BuildingName" : "",

```

```

      "Description" : "",
      "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
        { "Day" : "07",
          "Month" : "10",
          "Year" : "2005" },
      "DateLastSeen" :
        { "Day" : "19",
          "Month" : "08",
          "Year" : "2015" },
      "Address" :
        { "Line1" : "8672 NW FIRST PASS",
          "City" : "OAKLAND",
          "State" : "CA",
          "Zip" : "94605",
          "County" : "ALAMEDA",
          "Zip4" : "4231",
          "BuildingName" : "",
          "Description" : "",
          "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
        { "Day" : "01",
          "Month" : "12",
          "Year" : "2003" },
      "DateLastSeen" :
        { "Day" : "07",
          "Month" : "01",
          "Year" : "2015" },
      "Address" :
        { "Line1" : "3946 E LAKE LANE RM 42",
          "City" : "EL SOBRANTE",
          "State" : "CA",
          "Zip" : "94803",
          "County" : "CONTRA COSTA",
          "Zip4" : "2764",
          "BuildingName" : "",
          "Description" : "1 office, 194 apartments",
          "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
        { "Month" : "06",
          "Year" : "2003" },
      "DateLastSeen" :
        { "Month" : "09",
          "Year" : "2005" },
      "Address" :
        { "Line1" : "3946 E VALLEY LANE APT 47",
          "City" : "EL SOBRANTE",
          "State" : "CA",
          "Zip" : "94803",
          "County" : "CONTRA COSTA",

```

```

    "Zip4" : "2783",
    "BuildingName" : "",
    "Description" : "1 office, 194 apartments",
    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "09",
    "Year" : "1999" },
  "DateLastSeen" :
  { "Day" : "01",
    "Month" : "03",
    "Year" : "2004" },
  "Address" :
  { "Line1" : "3946 E IVY LANE APT 15",
    "City" : "EL SOBRANTE",
    "State" : "CA",
    "Zip" : "94803",
    "County" : "CONTRA COSTA",
    "Zip4" : "2771",
    "BuildingName" : "",
    "Description" : "1 office, 194 apartments",
    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "13",
    "Month" : "10",
    "Year" : "1999" },
  "DateLastSeen" :
  { "Day" : "13",
    "Month" : "10",
    "Year" : "1999" },
  "Address" :
  { "Line1" : "3946 E MANOR LANE RM 10",
    "City" : "EL SOBRANTE",
    "State" : "CA",
    "Zip" : "94803",
    "County" : "CONTRA COSTA",
    "Zip4" : "7204",
    "BuildingName" : "",
    "Description" : "1 office, 194 apartments",
    "SubdivisionName" : "",
    "AddressMissingUnitDesignation" : "Yes" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "19",
    "Month" : "02",
    "Year" : "2014" },
  "DateLastSeen" :
  { "Day" : "19",
    "Month" : "02",
    "Year" : "2014" },
  "Address" :
  { "Line1" : "1491 S OAK AVENUE",

```

```

    "City" : "SAN FRANCISCO",
    "State" : "CA",
    "Zip" : "94102",
    "County" : "SAN FRANCISCO",
    "Zip4" : "5402",
    "BuildingName" : "FOX PLAZA",
    "Description" : "3 units, 446 apartments, 63 suites",
    "SubdivisionName" : "",
    "AddressMissingUnitDesignation" : "Yes" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "01",
    "Year" : "2011" },
  "DateLastSeen" :
  { "Day" : "03",
    "Month" : "01",
    "Year" : "2014" },
  "Address" :
  { "Line1" : "376 E WASHINGTON BOULEVARD",
    "City" : "OAKLAND",
    "State" : "CA",
    "Zip" : "94612",
    "County" : "ALAMEDA",
    "Zip4" : "3091",
    "BuildingName" : "",
    "Description" : "1 office, 243 apartments",
    "SubdivisionName" : "",
    "AddressMissingUnitDesignation" : "Yes" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "28",
    "Month" : "03",
    "Year" : "2009" },
  "DateLastSeen" :
  { "Day" : "05",
    "Month" : "08",
    "Year" : "2009" },
  "Address" :
  { "Line1" : "376 E ORANGE BOULEVARD STE 37",
    "City" : "OAKLAND",
    "State" : "CA",
    "Zip" : "94612",
    "County" : "ALAMEDA",
    "Zip4" : "3085",
    "BuildingName" : "",
    "Description" : "1 office, 243 apartments",
    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "04",
    "Year" : "2013" },
  "DateLastSeen" :
  { "Day" : "22",

```

```

      "Month" : "04",
      "Year" : "2013" },
    "Address" :
    { "Line1" : "2463 N CYPRESS BRIDGE",
      "City" : "SAN PABLO",
      "State" : "CA",
      "Zip" : "94806",
      "County" : "CONTRA COSTA",
      "Zip4" : "1528",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "27",
        "Month" : "11",
        "Year" : "2012" },
      "DateLastSeen" :
      { "Day" : "27",
        "Month" : "11",
        "Year" : "2012" },
      "Address" :
      { "Line1" : "2721 N QUEENS PIKE",
        "City" : "SAN FRANCISCO",
        "State" : "CA",
        "Zip" : "94122",
        "County" : "SAN FRANCISCO",
        "Zip4" : "3922",
        "BuildingName" : "",
        "Description" : "",
        "SubdivisionName" : "OUTSIDE LAND BL" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Month" : "07",
        "Year" : "2007" },
      "DateLastSeen" :
      { "Day" : "04",
        "Month" : "04",
        "Year" : "2011" },
      "Address" :
      { "Line1" : "1441 S QUEENS PIKE RM 34",
        "City" : "OAKLAND",
        "State" : "CA",
        "Zip" : "94612",
        "County" : "ALAMEDA",
        "Zip4" : "1290",
        "BuildingName" : "",
        "Description" : "2 units, 87 suites",
        "SubdivisionName" : "CASSERLY STREET" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "13",
        "Month" : "09",

```

```

    "Year" : "2010" },
    "DateLastSeen" :
    { "Day" : "13",
      "Month" : "09",
      "Year" : "2010" },
    "Address" :
    { "Line1" : "1110 S PINE PASS UNIT 22",
      "City" : "HERCULES",
      "State" : "CA",
      "Zip" : "94547",
      "County" : "CONTRA COSTA",
      "Zip4" : "",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "16",
      "Month" : "09",
      "Year" : "2008" },
    "DateLastSeen" :
    { "Day" : "16",
      "Month" : "09",
      "Year" : "2008" },
    "Address" :
    { "Line1" : "9784 S WASHINGTON PASS",
      "City" : "RICHMOND",
      "State" : "CA",
      "Zip" : "94804",
      "County" : "CONTRA COSTA",
      "Zip4" : "4347",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Month" : "12",
      "Year" : "2001" },
    "DateLastSeen" :
    { "Day" : "15",
      "Month" : "12",
      "Year" : "2007" },
    "Address" :
    { "Line1" : "951 S QUEENS COURT UNIT 26",
      "City" : "HERCULES",
      "State" : "CA",
      "Zip" : "94547",
      "County" : "CONTRA COSTA",
      "Zip4" : "2075",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,

```



```

    "DateFirstSeen" :
    { "Day" : "01",
      "Month" : "01",
      "Year" : "2004" },
    "DateLastSeen" :
    { "Month" : "06",
      "Year" : "2006" },
    "Address" :
    { "Line1" : "2358 N LAKE CROSSING",
      "City" : "SUISUN CITY",
      "State" : "CA",
      "Zip" : "94585",
      "County" : "SOLANO",
      "Zip4" : "6326",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "PETERSON RANCH" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "13",
      "Month" : "09",
      "Year" : "2005" },
    "DateLastSeen" :
    { "Day" : "13",
      "Month" : "09",
      "Year" : "2005" },
    "Address" :
    { "Line1" : "5710 SE ELM DRIVE",
      "City" : "OAKLAND",
      "State" : "CA",
      "Zip" : "94607",
      "County" : "ALAMEDA",
      "Zip4" : "3427",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "CENTRAL KEY ROUTE" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "11",
      "Month" : "12",
      "Year" : "1998" },
    "DateLastSeen" :
    { "Month" : "09",
      "Year" : "2005" },
    "Address" :
    { "Line1" : "321 E EIGHTH ESTATE RM 10",
      "City" : "VALLEJO",
      "State" : "CA",
      "Zip" : "94591",
      "County" : "SOLANO",
      "Zip4" : "8205",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

```

```

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "13",
    "Month" : "09",
    "Year" : "2004" },
  "DateLastSeen" :
  { "Day" : "13",
    "Month" : "09",
    "Year" : "2004" },
  "Address" :
  { "Line1" : "6318 SW BEVERLY COURT RM 10",
    "City" : "EL SOBRANTE",
    "State" : "CA",
    "Zip" : "94803",
    "County" : "CONTRA COSTA",
    "Zip4" : "7302",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "10",
    "Year" : "1998" },
  "DateLastSeen" :
  { "Month" : "06",
    "Year" : "2003" },
  "Address" :
  { "Line1" : "7731 NE PINE ROUTE",
    "City" : "OAKLAND",
    "State" : "CA",
    "Zip" : "94605",
    "County" : "ALAMEDA",
    "Zip4" : "3805",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "06",
    "Year" : "1998" },
  "DateLastSeen" :
  { "Month" : "12",
    "Year" : "1998" },
  "Address" :
  { "Line1" : "416 W ORANGE BOULEVARD",
    "City" : "PITTSBURG",
    "State" : "CA",
    "Zip" : "94565",
    "County" : "CONTRA COSTA",
    "Zip4" : "2077",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

```

```

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "21",
    "Month" : "11",
    "Year" : "1998" },
  "DateLastSeen" :
  { "Day" : "21",
    "Month" : "11",
    "Year" : "1998" },
  "Address" :
  { "Line1" : "651 SW PINE COURT UNIT 20",
    "City" : "OAKLAND",
    "State" : "CA",
    "Zip" : "94605",
    "County" : "ALAMEDA",
    "Zip4" : "5905",
    "BuildingName" : "",
    "Description" : "8 apartments",
    "SubdivisionName" : "" },
  "Phones" : null } ] },
"DriversLicenses" : null,
"ProfessionalLicenses" :
{ "TLOProfessionalLicense" :
  [
    { "ReportToken" : "838X-PW3C",
      "LicenseNumber" : "1432900",
      "LicenseType" : "REAL ESTATE BROKERS AND SALESPERSON",
      "LicenseState" : "CA",
      "LicenseStatus" : "EXPIRED",
      "IssueDate" :
      { "Day" : "25",
        "Month" : "05",
        "Year" : "2004" },
      "ExpirationDate" :
      { "Day" : "24",
        "Month" : "05",
        "Year" : "2008" },
      "JobFunctions" :
      { "string" :
        [ "REAL ESTATE BROKERS AND SALESPERSON" ] },
      "Name" :
      { "FirstName" : "MARK",
        "MiddleName" : "ULYSSES",
        "LastName" : "MILLER" },
      "Address" :
      { "Line1" : "2358 N LAKE CROSSING",
        "City" : "SUISUN CITY",
        "State" : "CA",
        "Zip" : "94585",
        "Zip4" : "6326" } } ] },
"OtherPhones" :
{ "BasicPhoneListing" :
  [
    { "ListingName" : "HILL, SIMON",
      "PhoneType" : "Mobile",
      "ListingType" : "Unknown",
      "Carrier" : "SPRINT SPECTRUM LP",
      "CarrierType" : "WIRELESS",
      "City" : "BEVERLY HILLS",
      "State" : "CA",
      "County" : "LOS ANGELES",

```

```

    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "05",
      "Month" : "02",
      "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "02",
      "Month" : "11",
      "Year" : "2020" },
    "Score" : "86",
    "Scores" : "Score_1=86",
    "Phone" : "3101481739" },

  { "ListingName" : "ROBINSON, SIMON",
    "PhoneType" : "Mobile",
    "ListingType" : "Unknown",
    "Carrier" : "SPRINT SPECTRUM LP",
    "CarrierType" : "WIRELESS",
    "City" : "OAKLAND",
    "State" : "CA",
    "County" : "ALAMEDA",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "18",
      "Month" : "12",
      "Year" : "2013" },
    "DateLastSeen" :
    { "Day" : "06",
      "Month" : "06",
      "Year" : "2020" },
    "Score" : "68",
    "Scores" : "Score_1=68",
    "Phone" : "5105581220" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
    "CarrierType" : "LANDLINE",
    "City" : "EL SOBRANTE-PINOLE",
    "State" : "CA",
    "County" : "CONTRA COSTA",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "31",
      "Month" : "07",
      "Year" : "2010" },
    "DateLastSeen" :
    { "Day" : "06",
      "Month" : "06",
      "Year" : "2020" },
    "Score" : "67",
    "Scores" : "Score_1=67",
    "Phone" : "5105396607" },

  { "ListingName" : "RODRIGUEZ, SIMON",
    "PhoneType" : "Mobile",
    "ListingType" : "Unknown",
    "Carrier" : "SPRINT SPECTRUM LP",
    "CarrierType" : "WIRELESS",
    "City" : "BEVERLY HILLS",
    "State" : "CA",

```

```

"County" : "LOS ANGELES",
"TimeZone" : "PT",
"DateFirstSeen" :
{ "Day" : "16",
  "Month" : "09",
  "Year" : "2009" },
"DateLastSeen" :
{ "Day" : "27",
  "Month" : "05",
  "Year" : "2020" },
"Score" : "67",
"Scores" : "Score_1=67",
"Phone" : "3101483617" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "FRONTIER CALIFORNIA INC",
  "CarrierType" : "LANDLINE",
  "City" : "LAKEWOOD",
  "State" : "CA",
  "County" : "LOS ANGELES",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "23",
    "Month" : "04",
    "Year" : "2009" },
  "DateLastSeen" :
  { "Day" : "01",
    "Month" : "09",
    "Year" : "2020" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "5625427730" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "METRO PCS INC (METROPCS)",
  "CarrierType" : "WIRELESS",
  "City" : "REDWOOD CITY",
  "State" : "CA",
  "County" : "SAN MATEO",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "29",
    "Month" : "07",
    "Year" : "2010" },
  "DateLastSeen" :
  { "Day" : "14",
    "Month" : "08",
    "Year" : "2020" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "6508938407" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "BANDWIDTH.COM CLEC LLC - CA",
  "CarrierType" : "LANDLINE",
  "City" : "OAKLAND",

```

```

"State" : "CA",
"County" : "ALAMEDA",
"TimeZone" : "PT",
"DateFirstSeen" :
{ "Day" : "08",
  "Month" : "09",
  "Year" : "2014" },
"DateLastSeen" :
{ "Day" : "08",
  "Month" : "09",
  "Year" : "2014" },
"Score" : "66",
"Scores" : "Score_1=66",
"Phone" : "5104689642" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "VoIP",
  "ListingType" : "Unknown",
  "Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
  "CarrierType" : "LANDLINE",
  "City" : "EL SOBRANTE-PINOLE",
  "State" : "CA",
  "County" : "CONTRA COSTA",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "31",
    "Month" : "07",
    "Year" : "2010" },
  "DateLastSeen" :
  { "Day" : "31",
    "Month" : "07",
    "Year" : "2010" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "5105396377" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "SPRINT SPECTRUM LP",
  "CarrierType" : "WIRELESS",
  "City" : "BEVERLY HILLS",
  "State" : "CA",
  "County" : "LOS ANGELES",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "29",
    "Month" : "07",
    "Year" : "2010" },
  "DateLastSeen" :
  { "Day" : "30",
    "Month" : "07",
    "Year" : "2010" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "3101481735" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
  "CarrierType" : "LANDLINE",

```

```

"City" : "VALLEJO",
"State" : "CA",
"County" : "SOLANO",
"TimeZone" : "PT",
"DateFirstSeen" :
{ "Month" : "06",
  "Year" : "2004" },
"DateLastSeen" :
{ "Day" : "24",
  "Month" : "07",
  "Year" : "2009" },
"Score" : "66",
"Scores" : "Score_1=66",
"Phone" : "7077616435" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
  "CarrierType" : "LANDLINE",
  "City" : "EL SOBRANTE-PINOLE",
  "State" : "CA",
  "County" : "CONTRA COSTA",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "01",
    "Month" : "09",
    "Year" : "2003" },
  "DateLastSeen" :
  { "Day" : "23",
    "Month" : "04",
    "Year" : "2009" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "5103463116" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "UNITED STATES CELLULAR - CA (U.S. CELLULAR)",
  "CarrierType" : "WIRELESS",
  "City" : "GARBERVILLE",
  "State" : "CA",
  "County" : "HUMBOLDT",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "20",
    "Month" : "10",
    "Year" : "2006" },
  "DateLastSeen" :
  { "Day" : "20",
    "Month" : "10",
    "Year" : "2006" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "7073463116" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
  "CarrierType" : "LANDLINE",

```

```

    "City" : "VALLEJO",
    "State" : "CA",
    "County" : "SOLANO",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "04",
      "Month" : "03",
      "Year" : "1999" },
    "DateLastSeen" :
    { "Day" : "23",
      "Month" : "05",
      "Year" : "2006" },
    "Score" : "66",
    "Scores" : "Score_1=66",
    "Phone" : "7076714803" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "GREENVILLE",
    "State" : "SC",
    "County" : "GREENVILLE",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "25",
      "Month" : "05",
      "Year" : "2020" },
    "DateLastSeen" :
    { "Day" : "25",
      "Month" : "05",
      "Year" : "2020" },
    "Score" : "38",
    "Scores" : "Score_1=38",
    "Phone" : "8644783437" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
    "CarrierType" : "LANDLINE",
    "City" : "PLEASANTON",
    "State" : "CA",
    "County" : "ALAMEDA",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "21",
      "Month" : "04",
      "Year" : "2020" },
    "DateLastSeen" :
    { "Day" : "21",
      "Month" : "04",
      "Year" : "2020" },
    "Score" : "38",
    "Scores" : "Score_1=38",
    "Phone" : "9258511739" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",

```



```

"Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
"CarrierType" : "LANDLINE",
"City" : "EL SOBRANTE-PINOLE",
"State" : "CA",
"County" : "CONTRA COSTA",
"TimeZone" : "PT",
"DateFirstSeen" :
{ "Day" : "22",
  "Month" : "08",
  "Year" : "2012" },
"DateLastSeen" :
{ "Day" : "22",
  "Month" : "08",
  "Year" : "2012" },
"Score" : "12",
"Scores" : "Score_1=12",
"Phone" : "5103844324" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "T-MOBILE USA INC",
  "CarrierType" : "WIRELESS",
  "City" : "OAKLAND",
  "State" : "CA",
  "County" : "ALAMEDA",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "27",
    "Month" : "08",
    "Year" : "2010" },
  "DateLastSeen" :
  { "Day" : "27",
    "Month" : "08",
    "Year" : "2010" },
  "Score" : "3",
  "Scores" : "Score_1=3",
  "Phone" : "5108395263" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "LandLine",
  "ListingType" : "Unknown",
  "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
  "CarrierType" : "LANDLINE",
  "City" : "FAIRFIELD-SUISUN",
  "State" : "CA",
  "County" : "SOLANO",
  "TimeZone" : "PT",
  "DateFirstSeen" :
  { "Day" : "18",
    "Month" : "11",
    "Year" : "2009" },
  "DateLastSeen" :
  { "Day" : "18",
    "Month" : "11",
    "Year" : "2009" },
  "Score" : "3",
  "Scores" : "Score_1=3",
  "Phone" : "7075572233" },

{ "ListingName" : "HILL, SIMON",
  "PhoneType" : "VoIP",

```

```

    "ListingType" : "Unknown",
    "Carrier" : "COMCAST PHONE OF CALIFORNIA LLC - CA",
    "CarrierType" : "LANDLINE",
    "City" : "OAKLAND",
    "State" : "CA",
    "County" : "ALAMEDA",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "10",
      "Month" : "08",
      "Year" : "2009" },
    "DateLastSeen" :
    { "Day" : "10",
      "Month" : "08",
      "Year" : "2009" },
    "Score" : "3",
    "Scores" : "Score_1=3",
    "Phone" : "5109647356" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
    "CarrierType" : "LANDLINE",
    "City" : "OAKLAND",
    "State" : "CA",
    "County" : "ALAMEDA",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "08",
      "Month" : "08",
      "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "08",
      "Month" : "08",
      "Year" : "2007" },
    "Score" : "3",
    "Scores" : "Score_1=3",
    "Phone" : "5106755256" },

  { "ListingName" : "HILL, SIMON",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "PACIFIC BELL TELEPHONE COMPANY (AT&T CALIFORNIA)",
    "CarrierType" : "LANDLINE",
    "City" : "VALLEJO",
    "State" : "CA",
    "County" : "SOLANO",
    "TimeZone" : "PT",
    "DateFirstSeen" :
    { "Day" : "14",
      "Month" : "07",
      "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "14",
      "Month" : "07",
      "Year" : "2007" },
    "Score" : "3",
    "Scores" : "Score_1=3",
    "Phone" : "7076711253" } ] },
  "Relatives" :
  { "TLOPersonSearchRelative" :

```

```
[
  { "Name" :
    { "FirstName" : "MARK",
      "MiddleName" : "U",
      "LastName" : "SMITH",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "1vob5rYq1mHLMZtDReNFtzTzKJwc010R6u0g0kEcEjc=",
        "Year" : "XXXX" },
      "CurrentAge" : "36" },
    "ReportToken" : "7KT7-141J",
    "CurrentAge" : "36",
    "DateOfBirth" :
    { "DOBUnlockToken" : "QjzeSpBkhbykHT4UxBPRKsnKWQA6W50kTfSAFb6QxFM=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "ZACHARY",
      "MiddleName" : "OMAR",
      "LastName" : "MILLER",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "Y+Me1tsZuy3+H+3jveUgwcwWaBpxeVSzY07ekm5mFw0=",
        "Year" : "XXXX" },
      "CurrentAge" : "33" },
    "ReportToken" : "CNKD-JQ4Y",
    "CurrentAge" : "33",
    "DateOfBirth" :
    { "DOBUnlockToken" : "d5UDBNu0jv/ghrZEU68FImCjvG4+PjatonLGCgppw5D4=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "XANDER",
      "MiddleName" : "ULYSSES",
      "LastName" : "MILLER",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "Mqfj7H/dC5Nbsyf+GaX3x3Qn51YwUJJIFRNtwSG/M6A=",
        "Year" : "XXXX" },
      "CurrentAge" : "58" },
    "ReportToken" : "QV97-3V32",
    "CurrentAge" : "58",
    "DateOfBirth" :
    { "DOBUnlockToken" : "cxPJq2wetXC0XSeg6n2zHCFSUczdBmissKnIFlsBGro=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "QUENTIN",
      "MiddleName" : "Q",
      "LastName" : "MILLER",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "TkPNMJunnwENuZ9FqYp5tpPCRRByfnLyd115qFdFIcM=",
        "Year" : "XXXX" },
      "CurrentAge" : "26" },
    "ReportToken" : "6TBB-W26D",
    "CurrentAge" : "26",
    "DateOfBirth" :
```

```

    { "DOBUnlockToken" : "DPF4DE2QtLMWRdnBfv5Xi7o0excfZLsvn0wg+gLkSx8=",
      "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "MARK",
        "MiddleName" : "ULYSSES",
        "LastName" : "MILLER",
        "NameSuffix" : "" },
      "DateOfBirthRecord" :
      { "DateOfBirth" :
        { "DOBUnlockToken" : "7AoUhZNUe6dkUdgwtvuq5aHS0SipIZ1I7vmbSCmD3cw=",
          "Year" : "XXXX" },
          "CurrentAge" : "36" },
        "ReportToken" : "HY24-7177",
        "CurrentAge" : "36",
        "DateOfBirth" :
        { "DOBUnlockToken" : "e1R7z4v1FWv5newiBVlBJ0The0aXN76qwbLqMij5c70=",
          "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "MARK",
        "MiddleName" : "",
        "LastName" : "MILLER",
        "NameSuffix" : "" },
      "DateOfBirthRecord" :
      { "DateOfBirth" :
        { "DOBUnlockToken" : "GdpbN6VurtSftjlEcOjva+7iVW9dXYcQ00AaRa+LAK0=",
          "Year" : "XXXX" },
          "CurrentAge" : "36" },
        "ReportToken" : "JYP6-7H9P",
        "CurrentAge" : "36",
        "DateOfBirth" :
        { "DOBUnlockToken" : "19a36iVFspinkFLPYjQEkgz6ILO+UNctB+nVQK9BQ9g=",
          "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "HARRISON",
        "MiddleName" : "ZACHARY",
        "LastName" : "MILLER",
        "NameSuffix" : "" },
      "DateOfBirthRecord" :
      { "DateOfBirth" :
        { "DOBUnlockToken" : "L2J3bmFgrwgyetQaI76JDB8VPAxR9LkK2nYBDWG0rwa=",
          "Year" : "XXXX" },
          "CurrentAge" : "56" },
        "DateOfDeath" :
        { "DateOfDeath" : null,
          "Name" :
            { "FirstName" : "HARRISON",
              "MiddleName" : "Z",
              "LastName" : "LEE HUMPHREY",
              "NameSuffix" : "",
              "ProfessionalSuffix" : "" },
            "SSNRecord" :
            { "SSN" : "XXXXX6264",
              "SSNPlaceOfIssue" : "MISSISSIPPI",
              "SSNIssueYears" : "1975",
              "SSNToken" : "azQQifq4R72aVs00R5sHC0Q==",
              "SSNUnlockToken" : "1wZ6vTtXY/A5VohwH4sx/2y2UFYqDyQWuYStWMaAZ4I=" },
            "DateOfBirthRecord" :
            { "DateOfBirth" :
              { "DOBUnlockToken" : "zGAnRTohn8AX/nWhlXaZbh8mrj8VqS8etmI8gU/dV+g=",

```

```

    "Day" : "XX",
    "Month" : "XX",
    "Year" : "1964" },
    "CurrentAge" : "56" },
    "Address" :
    { "Line1" : "238 N FIRST ROAD",
      "City" : "GREENVILLE",
      "State" : "MS",
      "Zip" : "38701",
      "County" : "WASHINGTON",
      "Zip4" : "7702" },
    "VerifyProof" : "",
    "Vendors" : "Atlas",
    "Relatives" : null,
    "ParentsFullName" : "",
    "Gender" : "",
    "DateOfMarriage" : null,
    "BirthOrder" : "",
    "BirthPlace" : "",
    "BirthPlaceCounty" : "",
    "DeathPlace" : "",
    "DeathPlaceCounty" : "",
    "CauseOfDeath" : "",
    "MilitaryService" : "",
    "Religion" : "",
    "Siblings" : "",
    "Sons" : "",
    "Daughters" : "",
    "NumberOfGrandChildren" : "",
    "NumberOfGreatGrandChildren" : "",
    "DateOfBirth" :
    { "DOBUnlockToken" : "9Mr56htfhJ+AV8JM0ElIXtaycIYZJvNZR7hSrDzruWA=",
      "Day" : "XX",
      "Month" : "XX",
      "Year" : "1964" } },
    "ReportToken" : "P8XT-LH4Y",
    "CurrentAge" : "56",
    "DateOfBirth" :
    { "DOBUnlockToken" : "L0Sz9k+H0g+0Vc/qNfVbmc0iKwMz+LLt8unJQDRs+Ls=",
      "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "HARRISON",
        "MiddleName" : "",
        "LastName" : "MILLER",
        "NameSuffix" : "" },
      "DateOfBirthRecord" :
      { "DateOfBirth" :
        { "DOBUnlockToken" : "OL0Jo18LyDQWRa9uh5b1bmU+azKenTWR2VT04nokx8U=",
          "Year" : "XXXX" },
          "CurrentAge" : "36" },
        "ReportToken" : "952R-PC3X",
        "CurrentAge" : "36",
        "DateOfBirth" :
        { "DOBUnlockToken" : "os0uyoiZEwNpq2lCufy1YhfVXtftBp0Z4lAdBKknobo=",
          "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "GABRIEL",
        "MiddleName" : "YURI",
        "LastName" : "MILLER",
        "NameSuffix" : "" },

```

```

    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "sqgpW7iSihVMp2uBDAq0IfqegvoFjuND5IvBpBj0Ar0=",
        "Year" : "XXXX" },
      "CurrentAge" : "37" },
    "ReportToken" : "63J7-553R",
    "CurrentAge" : "37",
    "DateOfBirth" :
    { "DOBUnlockToken" : "iv8nVVvKJzSzRujw43ub1vG3fVwg4WUE/FHeTCFB5B4=",
      "Year" : "XXXX" } },

    { "Name" :
      { "FirstName" : "DAVID",
        "MiddleName" : "OMAR",
        "LastName" : "MILLER",
        "NameSuffix" : "" },
      "DateOfBirthRecord" :
      { "DateOfBirth" :
        { "DOBUnlockToken" : "e4a8P0Gz/Pc0teZ8+gLQDcCI0ruzKWWntyZQ+Qzc5Zo=",
          "Year" : "XXXX" },
          "CurrentAge" : "57" },
        "ReportToken" : "CJTX-HY33",
        "CurrentAge" : "56",
        "DateOfBirth" :
        { "DOBUnlockToken" : "IYCZEhvHXpq3FqT7A6fvSspV0PFilpSgzC/Im5IVTB4=",
          "Year" : "XXXX" } } ] },
    "NumberOfUtilityRecordsAvailable" : "21",
    "Deceased" : "No" } ] } },
"transactionId" : "DEMO-TL01-60BD-2899-5143141",
"errorCode" : 0,
"numberOfRecordsFound" : 1,
"responseTime" : "0",
"deceased" : "No",
"names" :
[
  { "firstName" : "MARK",
    "middleName" : "ULYSSES",
    "lastName" : "MILLER" },

  { "firstName" : "MARK",
    "middleName" : "ULYSSES",
    "lastName" : "MILLER" },

  { "firstName" : "MARK",
    "middleName" : "",
    "lastName" : "SMITH" } ],
"emails" :
[ ],
"addressPhones" :
[ "5105115379",
  "8001043390",
  "5107055366",
  "5101864432",
  "5109018384",
  "5107761260",
  "7077683498",
  "7077682348",
  "7078535132",
  "7078535323",
  "5855150834" ],
"otherPhones" :
[ "3101481739",

```

```
"5105581220",  
"5105396607",  
"3101483617",  
"5625427730",  
"6508938407",  
"5104689642",  
"5105396377",  
"3101481735",  
"7077616435",  
"5103463116",  
"7073463116",  
"7076714803",  
"8644783437",  
"9258511739",  
"5103844324",  
"5108395263",  
"7075572233",  
"5109647356",  
"5106755256",  
"7076711253" ] }
```

Person Search with Report Token

Search for a person in TransUnion with a report token.

Properties

Report Token textField

The token returned from a Verify Plus response.

Input Schema

- default object
 - properties object
 - reportToken string required
 - Your report token to search with.

Output Schema

- output object
 - rawResponse object
 - transactionId string
 - errorCode number
 - numberOfRecordsFound number
 - responseTime number
 - deceased string
 - emails array
 - names array
 - addressPhones array
 - otherPhones array

Output Example

```

{ "rawResponse" :
{ "PersonSearchResult" :
{ "TransactionId" : "DEMO-TL01-6E1C-7399-9842857",
  "RequestId" : "",
  "ResponseTime" : "0",
  "ErrorCode" : 0,
  "NumberOfRecordsFound" : 1,
  "BillableRecordsFound" : "1",
  "ActualSearchInput" :
  { "Username" : "1DEMO.GSA",
    "HostIP" : "54.244.31.249",
    "RequestId" : "",
    "DPPAPurpose" : "1",
    "GLBPurpose" : "1",
    "ReportToken" : "F6NQ-274P" },
  "NumberOfRecordsFoundWithModifiedSearch" : 0,
  "PersonSearchOutputRecords" :
  { "TLOPersonSearchOutputRecord" :
    [
      { "ReportToken" : "F6NQ-274P",
        "SSNRecords" :
        { "SSNRecord" :
          [
            { "SSN" : "XXXXX8349",
              "SSNPlaceOfIssue" : "PUERTO RICO",
              "SSNIssueYears" : "1980",
              "SSNToken" : "aMHwHx5X8Z3REoKhF3VSXvw==",
              "SSNUnlockToken" : "GYXubHhAgWW7AgiUUFHj03AmGFVKsAmETTMdH/wX0k4=" } ] },
        "NumberOfAddresses" : "30",
        "EmailAddresses" :
        { "string" :
          [ "xavier.clark01@fantasyisland.com",
            "xavier.clark12@fantasyisland5.com",
            "xavier.clark23@fantasyisland2.com",
            "xavier.clark34@fantasyisland.com" ] },
        "NumberOfBankruptcies" : "1",
        "NumberOfBankruptcyRecords" : "1",
        "NumberOfLiens" : "0",
        "NumberOfJudgments" : "1",
        "MostRecentBankruptcyDate" :
        { "Day" : "12",
          "Month" : "02",
          "Year" : "2020" },
        "MostRecentBankruptcyRecordDate" :
        { "Day" : "12",
          "Month" : "02",
          "Year" : "2020" },
        "MostRecentJudgmentDate" :
        { "Day" : "05",
          "Month" : "05",
          "Year" : "2016" },
        "Names" :
        { "BasicName" :
          [
            { "FirstName" : "XAVIER",
              "MiddleName" : "ZANE",
              "LastName" : "CLARK",
              "NameSuffix" : "",
              "DateFirstSeen" :
              { "Day" : "01",

```

```

        "Month" : "03",
        "Year" : "1985" },
    "DateLastSeen" :
    { "Day" : "03",
      "Month" : "09",
      "Year" : "2020" } },

    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK PUIG",
      "NameSuffix" : "",
      "DateFirstSeen" :
      { "Day" : "01",
        "Month" : "04",
        "Year" : "1987" },
      "DateLastSeen" :
      { "Day" : "01",
        "Month" : "08",
        "Year" : "2020" } },

    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "RODRIGUEZ",
      "NameSuffix" : "",
      "DateFirstSeen" :
      { "Day" : "01",
        "Month" : "07",
        "Year" : "1999" },
      "DateLastSeen" :
      { "Day" : "02",
        "Month" : "11",
        "Year" : "2019" } },

    { "FirstName" : "CLARENCE",
      "MiddleName" : "XAVIER",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "DateFirstSeen" :
      { "Day" : "01",
        "Month" : "12",
        "Year" : "1991" },
      "DateLastSeen" :
      { "Day" : "12",
        "Month" : "11",
        "Year" : "2018" } },

    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "DateFirstSeen" :
      { "Day" : "20",
        "Month" : "10",
        "Year" : "1995" },
      "DateLastSeen" :
      { "Day" : "15",
        "Month" : "04",
        "Year" : "2018" } },

    { "FirstName" : "XAVIER",
      "MiddleName" : "Q",
      "LastName" : "CLARK",

```

```
"NameSuffix" : "",
"DateFirstSeen" :
{ "Day" : "20",
  "Month" : "10",
  "Year" : "1995" },
"DateLastSeen" :
{ "Day" : "15",
  "Month" : "04",
  "Year" : "2018" } },

{ "FirstName" : "Z",
  "MiddleName" : "ISAAC",
  "LastName" : "RODRIGUEZ CARLOS",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "12",
    "Month" : "04",
    "Year" : "2018" },
  "DateLastSeen" :
  { "Day" : "12",
    "Month" : "04",
    "Year" : "2018" } },

{ "FirstName" : "CLARENCE",
  "MiddleName" : "S",
  "LastName" : "CLARK",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "04",
    "Month" : "02",
    "Year" : "2012" },
  "DateLastSeen" :
  { "Day" : "08",
    "Month" : "05",
    "Year" : "2016" } },

{ "FirstName" : "XAVIER",
  "MiddleName" : "Z",
  "LastName" : "LOPEZ",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "01",
    "Month" : "08",
    "Year" : "2006" },
  "DateLastSeen" :
  { "Day" : "01",
    "Month" : "12",
    "Year" : "2014" } },

{ "FirstName" : "XAVIER",
  "MiddleName" : "Z",
  "LastName" : "SCOTT CASELLANOS",
  "NameSuffix" : "",
  "DateFirstSeen" :
  { "Day" : "08",
    "Month" : "08",
    "Year" : "2014" },
  "DateLastSeen" :
  { "Day" : "08",
    "Month" : "08",
    "Year" : "2014" } },
```

```

    { "FirstName" : "XAVIER",
      "MiddleName" : "Z",
      "LastName" : "LOPEZ",
      "NameSuffix" : "",
      "DateFirstSeen" :
      { "Day" : "20",
        "Month" : "10",
        "Year" : "1995" },
      "DateLastSeen" :
      { "Day" : "07",
        "Month" : "05",
        "Year" : "2011" } },

    { "FirstName" : "XAVIER",
      "MiddleName" : "Z",
      "LastName" : "PEREZ",
      "NameSuffix" : "",
      "DateFirstSeen" : null,
      "DateLastSeen" : null },

    { "FirstName" : "XAVIER",
      "MiddleName" : "S",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "DateFirstSeen" : null,
      "DateLastSeen" : null },

    { "FirstName" : "XAVIER",
      "MiddleName" : "H",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "DateFirstSeen" : null,
      "DateLastSeen" : null } ] },
  "DatesOfBirth" :
  { "BasicDateOfBirthRecord" :
    [
      { "DateOfBirth" :
        { "DOBUnlockToken" : "EN8K6axMDMJ0XrLQ8wHzaX6z/fSjCm1/C4RVKZtSJ0=",
          "Day" : "XX",
          "Month" : "XX",
          "Year" : "1966" },
        "CurrentAge" : "54" },

      { "DateOfBirth" :
        { "DOBUnlockToken" : "Ut5zC5M7mFA8Q0u6J8FqrvF1tdyNf01FgXtT81NXGAM=",
          "Month" : "XX",
          "Year" : "XXXX" },
        "CurrentAge" : "45" } ] },
  "Addresses" :
  { "BasicAddressRecord" :
    [
      { "ConfirmedAddress" : "",
        "PhoneCounts" : null,
        "DateFirstSeen" :
        { "Day" : "10",
          "Month" : "10",
          "Year" : "2018" },
        "DateLastSeen" :
        { "Day" : "17",
          "Month" : "11",
          "Year" : "2020" },
        "Address" :

```

```

    { "Line1" : "9508 S MANOR DRIVE STE 5",
      "City" : "DELRAY BEACH",
      "State" : "FL",
      "Zip" : "33484",
      "County" : "PALM BEACH",
      "Zip4" : "2586",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "ASPEN RIDGE" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "23",
      "Month" : "12",
      "Year" : "2015" },
    "DateLastSeen" :
    { "Month" : "11",
      "Year" : "2018" },
    "Address" :
    { "Line1" : "3323 E VALLEY PASS UNIT 44",
      "City" : "HIGHLAND BEACH",
      "State" : "FL",
      "Zip" : "33487",
      "County" : "PALM BEACH",
      "Zip4" : "1862",
      "BuildingName" : "",
      "Description" : "1 office, 36 apartments",
      "SubdivisionName" : "TOWNHOUSES HIGHLAND BEACH" },
    "Phones" :
    { "BasicPhoneListing" :
      [
        { "ListingName" : "LOPEZ, YUSIF GEORGE",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
          "CarrierType" : "LANDLINE",
          "City" : "DELRAY BEACH",
          "State" : "FL",
          "County" : "PALM BEACH",
          "TimeZone" : "ET",
          "Score" : "100",
          "Scores" : "Score_1=100",
          "Phone" : "5613919369" },

        { "ListingName" : "LOPEZ, YUSIF XAVIER",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
          "CarrierType" : "LANDLINE",
          "City" : "DELRAY BEACH",
          "State" : "FL",
          "County" : "PALM BEACH",
          "TimeZone" : "ET",
          "Score" : "1",
          "Scores" : "Score_1=1",
          "Phone" : "5613915366" } ] } },

    { "ConfirmedAddress" : "",

```

```

    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "19",
      "Month" : "06",
      "Year" : "2018" },
    "DateLastSeen" :
    { "Day" : "19",
      "Month" : "06",
      "Year" : "2018" },
    "Address" :
    { "Line1" : "3323 E EIGHTH PASS STE 1",
      "City" : "HIGHLAND BEACH",
      "State" : "FL",
      "Zip" : "33487",
      "County" : "PALM BEACH",
      "Zip4" : "1806",
      "BuildingName" : "",
      "Description" : "1 office, 36 apartments",
      "SubdivisionName" : "TOWNHOUSES HIGHLAND BEACH",
      "AddressMissingUnitDesignation" : "Yes" },
    "Phones" :
    { "BasicPhoneListing" :
      [
        { "ListingName" : "LOPEZ, YUSIF GEORGE",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
          "CarrierType" : "LANDLINE",
          "City" : "DELRAY BEACH",
          "State" : "FL",
          "County" : "PALM BEACH",
          "TimeZone" : "ET",
          "Score" : "100",
          "Scores" : "Score_1=100",
          "Phone" : "5613919369" },

        { "ListingName" : "LOPEZ, YUSIF XAVIER",
          "PhoneType" : "ActiveLandLine",
          "ListingType" : "Business",
          "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
          "CarrierType" : "LANDLINE",
          "City" : "DELRAY BEACH",
          "State" : "FL",
          "County" : "PALM BEACH",
          "TimeZone" : "ET",
          "Score" : "1",
          "Scores" : "Score_1=1",
          "Phone" : "5613915366" } ] } },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "01",
        "Month" : "09",
        "Year" : "2002" },
      "DateLastSeen" :
      { "Day" : "12",
        "Month" : "04",
        "Year" : "2018" },
      "Address" :

```

```

{ "Line1" : "3742 E EIGHTH GROVE RM 10",
  "City" : "HOMESTEAD",
  "State" : "FL",
  "Zip" : "33033",
  "County" : "MIAMI-DADE",
  "Zip4" : "7117",
  "BuildingName" : "",
  "Description" : "",
  "SubdivisionName" : "CORSIKA AT THE OASIS" },
"Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "08",
    "Year" : "2002" },
  "DateLastSeen" :
  { "Day" : "10",
    "Month" : "08",
    "Year" : "2017" },
  "Address" :
  { "Line1" : "3431 E EIGHTH DRIVE RM 50",
    "City" : "NORTH MIAMI",
    "State" : "FL",
    "Zip" : "33181",
    "County" : "MIAMI-DADE",
    "Zip4" : "2235",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "KEYSTONE ISLAND" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "01",
    "Month" : "08",
    "Year" : "2006" },
  "DateLastSeen" :
  { "Month" : "02",
    "Year" : "2012" },
  "Address" :
  { "Line1" : "7979 NE PINE SQUARE",
    "City" : "MIRAMAR",
    "State" : "FL",
    "Zip" : "33023",
    "County" : "BROWARD",
    "Zip4" : "2514",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "MIRAMAR" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "07",
    "Month" : "05",
    "Year" : "2011" },
  "DateLastSeen" :
  { "Day" : "07",
    "Month" : "05",

```



```

    "Year" : "2011" },
    "Address" :
    { "Line1" : "1454 S QUEENS GROVE RM 2",
      "City" : "POMPANO BEACH",
      "State" : "FL",
      "Zip" : "33064",
      "County" : "BROWARD",
      "Zip4" : "4600",
      "BuildingName" : "",
      "Description" : "1 office, 419 lots",
      "SubdivisionName" : "ACREAGE",
      "AddressMissingUnitDesignation" : "Yes" },
    "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "02",
        "Month" : "09",
        "Year" : "2010" },
      "DateLastSeen" :
      { "Day" : "02",
        "Month" : "09",
        "Year" : "2010" },
      "Address" :
      { "Line1" : "6690 SW IVY AVENUE RM 8",
        "City" : "ORLANDO",
        "State" : "FL",
        "Zip" : "32835",
        "County" : "ORANGE",
        "Zip4" : "2958",
        "BuildingName" : "",
        "Description" : "8 units",
        "SubdivisionName" : "SERENATA CONDO" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "05",
        "Month" : "02",
        "Year" : "2010" },
      "DateLastSeen" :
      { "Day" : "05",
        "Month" : "02",
        "Year" : "2010" },
      "Address" :
      { "Line1" : "PO BOX 172515",
        "City" : "MIAMI BEACH",
        "State" : "FL",
        "Zip" : "33141",
        "County" : "MIAMI-DADE",
        "Zip4" : "7848",
        "BuildingName" : "",
        "Description" : "",
        "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Day" : "01",

```

```

    "Month" : "06",
    "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "01",
      "Month" : "06",
      "Year" : "2007" },
    "Address" :
    { "Line1" : "295 N MAIN PATH APT 17",
      "City" : "TRUJILLO ALTO",
      "State" : "PR",
      "Zip" : "00976",
      "County" : "TRUJILLO ALTO",
      "Zip4" : "",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "01",
      "Month" : "06",
      "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "01",
      "Month" : "06",
      "Year" : "2007" },
    "Address" :
    { "Line1" : "1252 S WOODS PATH APT 3",
      "City" : "TRUJILLO ALTO",
      "State" : "PR",
      "Zip" : "00976",
      "County" : "TRUJILLO ALTO",
      "Zip4" : "",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "" },
    "Phones" : null },

  { "ConfirmedAddress" : "",
    "PhoneCounts" : null,
    "DateFirstSeen" :
    { "Day" : "31",
      "Month" : "07",
      "Year" : "1999" },
    "DateLastSeen" :
    { "Day" : "01",
      "Month" : "08",
      "Year" : "2006" },
    "Address" :
    { "Line1" : "1158 S PINE BOULEVARD",
      "City" : "WESTON",
      "State" : "FL",
      "Zip" : "33326",
      "County" : "BROWARD",
      "Zip4" : "3633",
      "BuildingName" : "",
      "Description" : "",
      "SubdivisionName" : "SECTOR EAST" },
    "Phones" : null },

```

```

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "18",
    "Month" : "10",
    "Year" : "2005" },
  "DateLastSeen" :
  { "Day" : "07",
    "Month" : "03",
    "Year" : "2006" },
  "Address" :
  { "Line1" : "8749 NW MADISON COURT RM 28",
    "City" : "SUNNY ISLES BEACH",
    "State" : "FL",
    "Zip" : "33160",
    "County" : "MIAMI-DADE",
    "Zip4" : "2722",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "TRUMP INTERNATIONAL SONESTA BE" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "11",
    "Month" : "09",
    "Year" : "2003" },
  "DateLastSeen" :
  { "Day" : "18",
    "Month" : "10",
    "Year" : "2005" },
  "Address" :
  { "Line1" : "8749 NW MADISON COURT RM 30",
    "City" : "SUNNY ISLES BEACH",
    "State" : "FL",
    "Zip" : "33160",
    "County" : "MIAMI-DADE",
    "Zip4" : "2722",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "TRUMP INTERNATIONAL SONESTA BE" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "09",
    "Year" : "2004" },
  "DateLastSeen" :
  { "Month" : "09",
    "Year" : "2004" },
  "Address" :
  { "Line1" : "8749 NW ORANGE COURT",
    "City" : "SUNNY ISLES BEACH",
    "State" : "FL",
    "Zip" : "33160",
    "County" : "MIAMI-DADE",
    "Zip4" : "2722",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "TRUMP INTERNATIONAL SONESTA BE" },

```

```

    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "06",
    "Month" : "10",
    "Year" : "1999" },
  "DateLastSeen" :
  { "Month" : "08",
    "Year" : "2004" },
  "Address" :
  { "Line1" : "430 W WASHINGTON ISLE UNIT 12",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "6123",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "24",
    "Month" : "01",
    "Year" : "2003" },
  "DateLastSeen" :
  { "Day" : "24",
    "Month" : "01",
    "Year" : "2003" },
  "Address" :
  { "Line1" : "1364 S PINE COURT UNIT 46",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "12",
    "Year" : "1997" },
  "DateLastSeen" :
  { "Day" : "24",
    "Month" : "01",
    "Year" : "2003" },
  "Address" :
  { "Line1" : "PO BOX 767636",
    "City" : "SAN JUAN",
    "State" : "PR",
    "Zip" : "00919",
    "County" : "SAN JUAN",
    "Zip4" : "1021",
    "BuildingName" : "",

```

```

      "Description" : "",
      "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Month" : "07",
        "Year" : "1999" },
      "DateLastSeen" :
      { "Day" : "23",
        "Month" : "01",
        "Year" : "2003" },
      "Address" :
      { "Line1" : "3565 E ORANGE COURT",
        "City" : "CORAL GABLES",
        "State" : "FL",
        "Zip" : "33134",
        "County" : "MIAMI-DADE",
        "Zip4" : "6308",
        "BuildingName" : "",
        "Description" : "",
        "SubdivisionName" : "CORAL GABLES COUNTRY CLUB PT" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Month" : "05",
        "Year" : "2002" },
      "DateLastSeen" :
      { "Month" : "06",
        "Year" : "2002" },
      "Address" :
      { "Line1" : "109 S CHURCH COURT RM 10",
        "City" : "TRUJILLO ALTO",
        "State" : "PR",
        "Zip" : "00976",
        "County" : "TRUJILLO ALTO",
        "Zip4" : "2307",
        "BuildingName" : "",
        "Description" : "",
        "SubdivisionName" : "" },
      "Phones" : null },

    { "ConfirmedAddress" : "",
      "PhoneCounts" : null,
      "DateFirstSeen" :
      { "Month" : "10",
        "Year" : "2000" },
      "DateLastSeen" :
      { "Month" : "10",
        "Year" : "2000" },
      "Address" :
      { "Line1" : "652 SW EIGHTH LANE",
        "City" : "TRUJILLO ALTO",
        "State" : "PR",
        "Zip" : "00976",
        "County" : "TRUJILLO ALTO",
        "Zip4" : "",
        "BuildingName" : "",
        "Description" : "" },

```

```

    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "12",
    "Year" : "1994" },
  "DateLastSeen" :
  { "Month" : "07",
    "Year" : "1998" },
  "Address" :
  { "Line1" : "633 SW EIGHTH LANE",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "6301",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Day" : "21",
    "Month" : "07",
    "Year" : "1997" },
  "DateLastSeen" :
  { "Day" : "21",
    "Month" : "07",
    "Year" : "1997" },
  "Address" :
  { "Line1" : "PO BOX 65625",
    "City" : "SAN JUAN",
    "State" : "PR",
    "Zip" : "00910",
    "County" : "SAN JUAN",
    "Zip4" : "1081",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "11",
    "Year" : "1988" },
  "DateLastSeen" :
  { "Month" : "06",
    "Year" : "1997" },
  "Address" :
  { "Line1" : "120 S CHURCH COURT RM 8",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "2419",
    "BuildingName" : "COND MONTEBELLO",
    "Description" : "" },

```

```

    "SubdivisionName" : "" },
    "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "10",
    "Year" : "1996" },
  "DateLastSeen" :
  { "Month" : "10",
    "Year" : "1996" },
  "Address" :
  { "Line1" : "514 SE CENTRAL LOOP",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "12",
    "Year" : "1995" },
  "DateLastSeen" :
  { "Month" : "12",
    "Year" : "1995" },
  "Address" :
  { "Line1" : "748 NE CYPRESS ROAD UNIT 48",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "07",
    "Year" : "1995" },
  "DateLastSeen" :
  { "Month" : "07",
    "Year" : "1995" },
  "Address" :
  { "Line1" : "593 SE CENTRAL ROAD STE 1",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

```

```

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "06",
    "Year" : "1994" },
  "DateLastSeen" :
  { "Month" : "06",
    "Year" : "1994" },
  "Address" :
  { "Line1" : "1447 ELM ROUTE",
    "City" : "TRUJILLO ALTO",
    "State" : "PR",
    "Zip" : "00976",
    "County" : "TRUJILLO ALTO",
    "Zip4" : "",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "12",
    "Year" : "1992" },
  "DateLastSeen" :
  { "Month" : "01",
    "Year" : "1994" },
  "Address" :
  { "Line1" : "472 W MAIN PATH APT 11",
    "City" : "SAN JUAN",
    "State" : "PR",
    "Zip" : "00927",
    "County" : "SAN JUAN",
    "Zip4" : "4855",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null },

{ "ConfirmedAddress" : "",
  "PhoneCounts" : null,
  "DateFirstSeen" :
  { "Month" : "12",
    "Year" : "1990" },
  "DateLastSeen" :
  { "Month" : "01",
    "Year" : "1992" },
  "Address" :
  { "Line1" : "421 W ORANGE COURT RM 44",
    "City" : "SAN JUAN",
    "State" : "PR",
    "Zip" : "00927",
    "County" : "SAN JUAN",
    "Zip4" : "4022",
    "BuildingName" : "",
    "Description" : "",
    "SubdivisionName" : "" },
  "Phones" : null } ] },
"DriversLicenses" :
{ "TL0DriversLicense" :

```



```
[
  { "DriversLicenseNumber" : "XXXXXXXXXXXX",
    "DriversLicenseNumberToken" : "b46yhov0jIimetkSIu5gxxF3hJlm00QM76YrY+rsJyTo=",
    "IssuingState" : "FL",
    "LicenseType" : "CLASS E",
    "MotorcycleCode" : "ALSO",
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUnlockToken" : "fLTqK2vRtfaK05ELyDEhwDEQCJgDU1X9astRdAobobw=",
        "Day" : "XX",
        "Month" : "XX",
        "Year" : "1966" },
      "CurrentAge" : "54",
      "AstrologicalSign" : "Libra" },
    "DateOfBirth" :
    { "DOBUnlockToken" : "zq9i60UQ8avQNrCpfYHS30UPNMx3Tg7ysHdGRWEBQm0=",
      "Day" : "XX",
      "Month" : "XX",
      "Year" : "1966" },
    "IssueDate" :
    { "Day" : "09",
      "Month" : "02",
      "Year" : "2010" },
    "OriginalIssueDate" :
    { "Day" : "09",
      "Month" : "07",
      "Year" : "1999" },
    "ExpirationDate" :
    { "Day" : "02",
      "Month" : "04",
      "Year" : "2018" },
    "SSNRecord" : null,
    "Gender" : "M",
    "Race" : "H",
    "CurrentAge" : "54",
    "Height" : "66",
    "OriginalHeight" : "506",
    "PrivacyFlag" : "T",
    "Name" :
    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "Title" : "",
      "ProfessionalSuffix" : "" },
    "Address" :
    { "Line1" : "3431 E EIGHTH DRIVE RM 50",
      "City" : "NORTH MIAMI",
      "State" : "FL",
      "Zip" : "33181",
      "County" : "MIAMI-DADE",
      "Zip4" : "2235" },
    "SourceRank" : "1",
    "Vendors" : "FD",
    "DriversLicenseUnlockToken" : "TuiTW5SjanXMsp2qntBj08p6G+Ew6Hm1lnFpaAK+eys=" },

  { "DriversLicenseNumber" : "XXXXXXXXXXXX",
    "DriversLicenseNumberToken" : "b46yhov0jIimetkSIu5gxxF3hJlm00QM76YrY+rsJyTo=",
    "IssuingState" : "FL",
    "LicenseType" : "CLASS E",
    "MotorcycleCode" : "ALSO",
    "OutOfStateLicenseNumber" : "XXXXXXX",
```

```

"OutOfStateLicenseNumberToken" : "b1a0mzyfLaIMMS3BTi/AWag==",
"OutOfStateIssuer" : "PR",
"DateOfBirthRecord" :
{ "DateOfBirth" :
{ "DOBUnlockToken" : "HYGV6bYHGDg380ZmcL1NFoz06jFBQr+mZQFunbIxijo=",
"Day" : "XX",
"Month" : "XX",
"Year" : "1966" },
"CurrentAge" : "54",
"AstrologicalSign" : "Libra" },
"DateOfBirth" :
{ "DOBUnlockToken" : "cGDtq3nB071rCXGqB49ERH4EIEMGX2cZinjIMuea2Lw=",
"Day" : "XX",
"Month" : "XX",
"Year" : "1966" },
"IssueDate" :
{ "Day" : "24",
"Month" : "01",
"Year" : "2006" },
"OriginalIssueDate" :
{ "Day" : "09",
"Month" : "07",
"Year" : "1999" },
"ExpirationDate" :
{ "Day" : "02",
"Month" : "04",
"Year" : "2010" },
"SSNRecord" : null,
"Gender" : "M",
"Race" : "H",
"CurrentAge" : "54",
"Height" : "66",
"OriginalHeight" : "506",
"PrivacyFlag" : "T",
"Name" :
{ "FirstName" : "XAVIER",
"MiddleName" : "Z",
"LastName" : "CLARK",
"NameSuffix" : "",
"Title" : "",
"ProfessionalSuffix" : "" },
"Address" :
{ "Line1" : "3431 E EIGHTH DRIVE RM 50",
"City" : "NORTH MIAMI",
"State" : "FL",
"Zip" : "33181",
"County" : "MIAMI-DADE",
"Zip4" : "2235" },
"SourceRank" : "1",
"Vendors" : "FD",
"DriversLicenseUnlockToken" : "+qxjmkleRYcjhILk+MPxLDuKhsQm20nyitG4Vsj+fms=",
"OutOfStateLicenseUnlockToken" : "noiEwp2QgVAgIjcm0060c4vFKMpz5JIsBeFYolrpSo4=" },

{ "DriversLicenseNumber" : "XXXXXXX",
"DriversLicenseNumberToken" : "b1a0mzyfLaIMMS3BTi/AWag==",
"IssuingState" : "PR",
"SSNRecord" :
{ "SSN" : "XXXXX8349",
"SSNPlaceOfIssue" : "PUERTO RICO",
"SSNIssueYears" : "1980",
"SSNToken" : "aMHwHx5X8Z3REoKhF3VSXvw==",
"SSNUnlockToken" : "4bzfd6kjrsgpx/CilBzAgWHwvSQJpDHUnoc0mmw+p3A=" },

```

```

    "Name" :
    { "FirstName" : "CLARENCE",
      "MiddleName" : "X",
      "LastName" : "CLARK",
      "NameSuffix" : "",
      "Title" : "",
      "ProfessionalSuffix" : "" },
    "Address" :
    { "Line1" : "633 SW WOODS DRIVE",
      "City" : "TRUJILLO ALTO",
      "State" : "PR",
      "Zip" : "00976" },
    "LicenseDateReported" :
    { "Day" : "24",
      "Month" : "02",
      "Year" : "1997" },
    "SourceRank" : "2",
    "Vendors" : "Buck",
    "DriversLicenseUnlockToken" : "6AjTaV79QKEV006iozctL19TWW9G3u0ZsD6zeEUIyXc=" } ] },
  "ProfessionalLicenses" :
  { "TLOProfessionalLicense" :
    [
      { "ReportToken" : "F6NQ-274P",
        "DateOfBirth" :
        { "DOBUUnlockToken" : "zafxTQiNyZ01AuBR0s1XSLI2AkaVCC0jPtF9VvYy2EM=",
          "Month" : "XX",
          "Year" : "XXXX" },
        "LicenseType" : "NONPILOT",
        "LicenseState" : "FL",
        "LicenseStatus" : "EXPIRED",
        "IssueDate" :
        { "Day" : "01",
          "Month" : "01",
          "Year" : "2020" },
        "ExpirationDate" :
        { "Day" : "01",
          "Month" : "07",
          "Year" : "2020" },
        "JobFunctions" :
        { "string" :
          [ "NONPILOT" ] },
        "Name" :
        { "FirstName" : "XAVIER",
          "MiddleName" : "ZANE",
          "LastName" : "CLARK" },
        "Address" :
        { "Line1" : "9508 S MANOR DRIVE STE 5",
          "City" : "DELRAY BEACH",
          "State" : "FL",
          "Zip" : "33484",
          "Zip4" : "2586" },
        "DateOfBirthRecord" :
        { "DateOfBirth" :
          { "DOBUUnlockToken" : "N8w4txnu1R+HEsEkTfsgduhvMNQdNDYDuUaWn340GfM=",
            "Month" : "XX",
            "Year" : "XXXX" },
          "CurrentAge" : "54" } },
      { "ReportToken" : "F6NQ-274P",
        "DateOfBirth" :
        { "DOBUUnlockToken" : "076nWpE1AHYExT2LLThXkPhp0rCHJLuMGKLBavJtKDA=",
          "Month" : "XX",

```

```

    "Year" : "XXXX" },
    "LicenseType" : "PILOT",
    "LicenseState" : "FL",
    "LicenseStatus" : "EXPIRED",
    "IssueDate" :
    { "Day" : "01",
      "Month" : "01",
      "Year" : "2020" },
    "ExpirationDate" :
    { "Day" : "01",
      "Month" : "07",
      "Year" : "2020" },
    "JobFunctions" :
    { "string" :
      [ "PILOT" ] },
    "Name" :
    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK" },
    "Address" :
    { "Line1" : "9508 S MANOR DRIVE STE 5",
      "City" : "DELRAY BEACH",
      "State" : "FL",
      "Zip" : "33484",
      "Zip4" : "2586" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "NIEnv8sP9Y8YoACM7e/V6VxYAAQZBuJjbsHVI7QZNMYS=",
        "Month" : "XX",
        "Year" : "XXXX" },
      "CurrentAge" : "54" } },

    { "ReportToken" : "F6NQ-274P",
      "LicenseNumber" : "A2168495",
      "LicenseType" : "PILOT SERVICE, AVIATION",
      "LicenseState" : "FL",
      "LicenseStatus" : "EXPIRED",
      "IssueDate" :
      { "Day" : "01",
        "Month" : "03",
        "Year" : "2019" },
      "ExpirationDate" :
      { "Day" : "01",
        "Month" : "09",
        "Year" : "2019" },
      "JobFunctions" :
      { "string" :
        [ "PILOT SERVICE, AVIATION" ] },
      "Name" :
      { "FirstName" : "XAVIER",
        "MiddleName" : "ZANE",
        "LastName" : "CLARK" },
      "Address" :
      { "Line1" : "9508 S MANOR DRIVE STE 5",
        "City" : "DELRAY BEACH",
        "State" : "FL",
        "Zip" : "33484",
        "Zip4" : "2586" } },

    { "ReportToken" : "F6NQ-274P",
      "LicenseNumber" : "A2168495",
      "LicenseType" : "PILOT",

```

```

    "LicenseState" : "FL",
    "LicenseStatus" : "EXPIRED",
    "IssueDate" :
    { "Day" : "01",
      "Month" : "03",
      "Year" : "2019" },
    "ExpirationDate" :
    { "Day" : "20",
      "Month" : "09",
      "Year" : "2019" },
    "JobFunctions" :
    { "string" :
      [ "PILOT" ] },
    "Name" :
    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK" },
    "Address" :
    { "Line1" : "9508 S MANOR DRIVE STE 5",
      "City" : "DELRAY BEACH",
      "State" : "FL",
      "Zip" : "33484",
      "Zip4" : "2586" } },

  { "ReportToken" : "F6NQ-274P",
    "LicenseNumber" : "A2168495",
    "LicenseType" : "PILOT",
    "LicenseState" : "FL",
    "LicenseStatus" : "EXPIRED",
    "IssueDate" :
    { "Day" : "20",
      "Month" : "06",
      "Year" : "2017" },
    "ExpirationDate" :
    { "Day" : "01",
      "Month" : "02",
      "Year" : "2019" },
    "JobFunctions" :
    { "string" :
      [ "PILOT" ] },
    "Name" :
    { "FirstName" : "XAVIER",
      "MiddleName" : "ZANE",
      "LastName" : "CLARK" },
    "Address" :
    { "Line1" : "3323 E VALLEY PASS UNIT 44",
      "City" : "HIGHLAND BEACH",
      "State" : "FL",
      "Zip" : "33487",
      "Zip4" : "1862" } },

  { "ReportToken" : "F6NQ-274P",
    "LicenseType" : "PILOT",
    "LicenseState" : "FL",
    "LicenseStatus" : "ACTIVE",
    "JobFunctions" :
    { "string" :
      [ "PILOT" ] },
    "Name" :
    { "FirstName" : "XAVIER",
      "LastName" : "CLARK" },
    "Address" :

```

```

{ "Line1" : "3431 E EIGHTH DRIVE RM 50",
  "City" : "NORTH MIAMI",
  "State" : "FL",
  "Zip" : "33181",
  "Zip4" : "2235" } },

{ "ReportToken" : "F6NQ-274P",
  "DateOfBirth" :
  { "DOBUUnlockToken" : "B0Ku39Ha64kyRUIhwnwwyDHyQgx5JjSLn9lBPXVEMsc=",
    "Month" : "XX",
    "Year" : "XXXX" },
  "LicenseType" : "PILOT",
  "LicenseState" : "FL",
  "LicenseStatus" : "ACTIVE",
  "JobFunctions" :
  { "string" :
    [ "PILOT" ] },
  "Name" :
  { "FirstName" : "XAVIER",
    "LastName" : "CLARK" },
  "Address" :
  { "Line1" : "3431 E EIGHTH DRIVE RM 50",
    "City" : "NORTH MIAMI",
    "State" : "FL",
    "Zip" : "33181",
    "Zip4" : "2235" },
  "DateOfBirthRecord" :
  { "DateOfBirth" :
    { "DOBUUnlockToken" : "FWANUEcKP/Owiu37Cqt+alw2Hwd3/pSs7LVV8VsfhrQ=",
      "Month" : "XX",
      "Year" : "XXXX" },
    "CurrentAge" : "54" } },

{ "ReportToken" : "F6NQ-274P",
  "LicenseType" : "PILOT",
  "AdditionalTypes" :
  { "string" :
    [ "AIRPLANE SINGLE ENGINE",
      "AIRPLANE MULTIENGINE" ] },
  "JobFunctions" :
  { "string" :
    [ "AIRLINE TRANSPORT PILOTS" ] },
  "Specialties" :
  { "string" :
    [ "AIRLINE TRANSPORT PILOT-AIRPLANE SINGLE ENGINE",
      "AIRLINE TRANSPORT PILOT-AIRPLANE MULTIENGINE" ] },
  "Name" :
  { "FirstName" : "XAVIER",
    "MiddleName" : "Z",
    "LastName" : "CLARK" },
  "Address" :
  { "Line1" : "3431 E EIGHTH DRIVE RM 50",
    "City" : "NORTH MIAMI",
    "State" : "FL",
    "Zip" : "33181",
    "Zip4" : "2235" } } ] },
"OtherPhones" :
{ "BasicPhoneListing" :
  [
    { "ListingName" : "RODRIGUEZ, IGOR",
      "PhoneType" : "Mobile",
      "ListingType" : "Unknown",

```

```
"Carrier" : "SPRINT SPECTRUM LP",
"CarrierType" : "WIRELESS",
"City" : "FORT LAUDERDALE",
"State" : "FL",
"County" : "BROWARD",
"TimeZone" : "ET",
"DateFirstSeen" :
{ "Day" : "13",
  "Month" : "04",
  "Year" : "2004" },
"DateLastSeen" :
{ "Day" : "02",
  "Month" : "11",
  "Year" : "2020" },
"Score" : "86",
"Scores" : "Score_1=86",
"Phone" : "9546829969" },

{ "ListingName" : "RODRIGUEZ, IGOR",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "SPRINT SPECTRUM LP",
  "CarrierType" : "WIRELESS",
  "City" : "FORT LAUDERDALE",
  "State" : "FL",
  "County" : "BROWARD",
  "TimeZone" : "ET",
  "DateFirstSeen" :
  { "Day" : "23",
    "Month" : "03",
    "Year" : "2004" },
  "DateLastSeen" :
  { "Day" : "09",
    "Month" : "02",
    "Year" : "2020" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "9546829970" },

{ "ListingName" : "RODRIGUEZ, IGOR",
  "PhoneType" : "Mobile",
  "ListingType" : "Unknown",
  "Carrier" : "SPRINT SPECTRUM LP",
  "CarrierType" : "WIRELESS",
  "City" : "NORTH DADE",
  "State" : "FL",
  "County" : "MIAMI-DADE",
  "TimeZone" : "ET",
  "DateFirstSeen" :
  { "Day" : "22",
    "Month" : "05",
    "Year" : "2007" },
  "DateLastSeen" :
  { "Day" : "15",
    "Month" : "05",
    "Year" : "2019" },
  "Score" : "66",
  "Scores" : "Score_1=66",
  "Phone" : "3058482659" },

{ "ListingName" : "RODRIGUEZ, ISAAC",
  "PhoneType" : "VoIP",
```

```

    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "MIAMI",
    "State" : "FL",
    "County" : "MIAMI-DADE",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "25",
      "Month" : "01",
      "Year" : "2003" },
    "DateLastSeen" :
    { "Day" : "12",
      "Month" : "11",
      "Year" : "2018" },
    "Score" : "66",
    "Scores" : "Score_1=66",
    "Phone" : "3051142469" },

  { "ListingName" : "RODRIGUEZ, IGOR",
    "PhoneType" : "Mobile",
    "ListingType" : "Unknown",
    "Carrier" : "SPRINT SPECTRUM LP",
    "CarrierType" : "WIRELESS",
    "City" : "FORT LAUDERDALE",
    "State" : "FL",
    "County" : "BROWARD",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "19",
      "Month" : "05",
      "Year" : "2017" },
    "DateLastSeen" :
    { "Day" : "19",
      "Month" : "05",
      "Year" : "2017" },
    "Score" : "66",
    "Scores" : "Score_1=66",
    "Phone" : "9546829965" },

  { "ListingName" : "RODRIGUEZ, IGOR",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "MIAMI",
    "State" : "FL",
    "County" : "MIAMI-DADE",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "02",
      "Month" : "04",
      "Year" : "2015" },
    "DateLastSeen" :
    { "Day" : "02",
      "Month" : "04",
      "Year" : "2015" },
    "Score" : "66",
    "Scores" : "Score_1=66",
    "Phone" : "3051132469" },

```



```

    { "ListingName" : "RODRIGUEZ, IGOR",
      "PhoneType" : "LandLine",
      "ListingType" : "Unknown",
      "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
      "CarrierType" : "LANDLINE",
      "City" : "FORT LAUDERDALE",
      "State" : "FL",
      "County" : "BROWARD",
      "TimeZone" : "ET",
      "DateFirstSeen" :
      { "Day" : "06",
        "Month" : "10",
        "Year" : "1999" },
      "DateLastSeen" :
      { "Day" : "31",
        "Month" : "01",
        "Year" : "2007" },
      "Score" : "66",
      "Scores" : "Score_1=66",
      "Phone" : "9543395243" },

    { "ListingName" : "RODRIGUEZ, IGOR",
      "PhoneType" : "Mobile",
      "ListingType" : "Unknown",
      "Carrier" : "USA MOBILITY WIRELESS INC",
      "CarrierType" : "PAGING",
      "City" : "MIAMI",
      "State" : "FL",
      "County" : "MIAMI-DADE",
      "TimeZone" : "ET",
      "DateFirstSeen" :
      { "Day" : "02",
        "Month" : "07",
        "Year" : "1999" },
      "DateLastSeen" :
      { "Day" : "02",
        "Month" : "07",
        "Year" : "1999" },
      "Score" : "66",
      "Scores" : "Score_1=66",
      "Phone" : "3057640409" },

    { "ListingName" : "RODRIGUEZ, IGOR",
      "PhoneType" : "Mobile",
      "ListingType" : "Unknown",
      "Carrier" : "ABC PAGING CITY BEEPERS INC",
      "CarrierType" : "PAGING",
      "City" : "MIAMI",
      "State" : "FL",
      "County" : "MIAMI-DADE",
      "TimeZone" : "ET",
      "Score" : "40",
      "Scores" : "Score_1=40",
      "Phone" : "3053395243" },

    { "ListingName" : "RODRIGUEZ, IGOR",
      "PhoneType" : "Mobile",
      "ListingType" : "Unknown",
      "Carrier" : "KENTUCKY RSA 3 CELLULAR GENERAL PARTNERSHIP (BLUEGRASS CELLULAR)",
      "CarrierType" : "WIRELESS",

```

```

    "City" : "BOWLING GREEN",
    "State" : "KY",
    "County" : "WARREN",
    "TimeZone" : "CT",
    "DateFirstSeen" :
    { "Day" : "16",
      "Month" : "08",
      "Year" : "2017" },
    "DateLastSeen" :
    { "Day" : "16",
      "Month" : "08",
      "Year" : "2017" },
    "Score" : "31",
    "Scores" : "Score_1=31",
    "Phone" : "2703246385" },

  { "ListingName" : "RODRIGUEZ, IGOR",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "FORT LAUDERDALE",
    "State" : "FL",
    "County" : "BROWARD",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "14",
      "Month" : "08",
      "Year" : "2013" },
    "DateLastSeen" :
    { "Day" : "14",
      "Month" : "08",
      "Year" : "2013" },
    "Score" : "17",
    "Scores" : "Score_1=17",
    "Phone" : "9544724320" },

  { "ListingName" : "RODRIGUEZ, IGOR",
    "PhoneType" : "LandLine",
    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "HOLLYWOOD",
    "State" : "FL",
    "County" : "BROWARD",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "05",
      "Month" : "01",
      "Year" : "2009" },
    "DateLastSeen" :
    { "Day" : "05",
      "Month" : "01",
      "Year" : "2009" },
    "Score" : "3",
    "Scores" : "Score_1=3",
    "Phone" : "9546125638" },

  { "ListingName" : "RODRIGUEZ, IGOR",
    "PhoneType" : "LandLine",

```

```

    "ListingType" : "Unknown",
    "Carrier" : "BELLSOUTH TELECOMMUNICATIONS INC DBA SOUTHERN BELL TELEPHONE & TELEGRAPH (AT&T
SOUTHEAST)",
    "CarrierType" : "LANDLINE",
    "City" : "MIAMI",
    "State" : "FL",
    "County" : "MIAMI-DADE",
    "TimeZone" : "ET",
    "DateFirstSeen" :
    { "Day" : "07",
      "Month" : "02",
      "Year" : "2007" },
    "DateLastSeen" :
    { "Day" : "07",
      "Month" : "02",
      "Year" : "2007" },
    "Score" : "3",
    "Scores" : "Score_1=3",
    "Phone" : "3051143469" } ] },
  "Relatives" :
  { "TLOPersonSearchRelative" :
    [
      { "Name" :
        { "FirstName" : "ETHAN",
          "MiddleName" : "",
          "LastName" : "RODRIGUEZ",
          "NameSuffix" : "" },
        "DateOfBirthRecord" :
        { "DateOfBirth" :
          { "DOBUUnlockToken" : "+vnNXmXgoiiBlk9HvNNtYvXhwy4ertscbjj+DkxMxC8=",
            "Year" : "XXXX" },
          "CurrentAge" : "78" },
        "ReportToken" : "DYCJ-D74P",
        "CurrentAge" : "78",
        "DateOfBirth" :
        { "DOBUUnlockToken" : "LoF4mUMmRqUKPvvImBFIbtRibinhXRT3Z/jNPR2CVUI=",
          "Year" : "XXXX" } },
      { "Name" :
        { "FirstName" : "XAVIER",
          "MiddleName" : "ZANE",
          "LastName" : "CLARK",
          "NameSuffix" : "" },
        "DateOfBirthRecord" :
        { "DateOfBirth" :
          { "DOBUUnlockToken" : "iwcPn/E2CrXGJ6sJYcXc0Ykmm2F4ZGM13+HunsgU+T4=",
            "Year" : "XXXX" },
          "CurrentAge" : "28" },
        "ReportToken" : "5TFX-2F39",
        "CurrentAge" : "28",
        "DateOfBirth" :
        { "DOBUUnlockToken" : "LnFM0Ue/w7E8p/nFYJiqMo9754SfZgRBF6Yo43f0/wY=",
          "Year" : "XXXX" } },
      { "Name" :
        { "FirstName" : "WINSTON",
          "MiddleName" : "XAVIER",
          "LastName" : "CLARK",
          "NameSuffix" : "" },
        "DateOfBirthRecord" :
        { "DateOfBirth" :
          { "DOBUUnlockToken" : "5eeJAv0hD/IeFNwy9Ue7mgd/sqUWMd6efbNzpih8Xwg=",

```

```

    "Year" : "XXXX" },
    "CurrentAge" : "26" },
    "ReportToken" : "84TW-NB6W",
    "CurrentAge" : "26",
    "DateOfBirth" :
    { "DOBUUnlockToken" : "53XSSw5i6BClk6UHUu0f0oefApn00H781ZbchjoBbFs=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "SIMON",
      "MiddleName" : "I",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "WCutfatkCCI1A6/xHbXIbGQFrDvKP+DmiH7Hwr1BYa0=",
        "Year" : "XXXX" },
        "CurrentAge" : "45" },
      "ReportToken" : "T5J3-PB3M",
      "CurrentAge" : "45",
      "DateOfBirth" :
      { "DOBUUnlockToken" : "cCN4k6dyASVtr0YWN9v/RfWIMRkq/sSQR8xRQeu7Uc=",
        "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "QUINCY",
      "MiddleName" : "Q",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "OtNDPknwDXb0KSzF5QTHR06ztXKyPHVfmtiRuT4m3As=",
        "Year" : "XXXX" },
        "CurrentAge" : "29" },
      "ReportToken" : "WTB8-PL42",
      "CurrentAge" : "29",
      "DateOfBirth" :
      { "DOBUUnlockToken" : "RkosW/x/4P3u/cz1c145FCxc0VjkGqM5uxKfyidr3U=",
        "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "QUINCY",
      "MiddleName" : "",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "KtDsKoG9Q6WHjk/nSAbX4AjpSLbtR+RmLFPXf1ZSU0U=",
        "Year" : "XXXX" },
        "CurrentAge" : "52" },
      "ReportToken" : "M8CP-L13Q",
      "CurrentAge" : "51",
      "DateOfBirth" :
      { "DOBUUnlockToken" : "Gde5V2NI+b4rT9lrb4s9cQGzIZguiWn5x+n6vhNfTsU=",
        "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "OSWALD",
      "MiddleName" : "NOAH",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :

```

```

    { "DateOfBirth" :
      { "DOBUUnlockToken" : "KGq7HdpTPBArPKyhu0notloP5dCjD8bMzuZ9/bybmt8=",
        "Year" : "XXXX" },
      "CurrentAge" : "55" },
    "ReportToken" : "969T-QJ3Q",
    "CurrentAge" : "55",
    "DateOfBirth" :
    { "DOBUUnlockToken" : "UXBarJfWjC/FfI4boxoePpyAGEuKTGecGoHdY+o4FnQ=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "CLARENCE",
      "MiddleName" : "XAVIER",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "LmmTPvBHuwuxXeTlee6z3UczlHPVAGiWB0zHFMXQjBs=",
        "Year" : "XXXX" },
      "CurrentAge" : "31" },
    "ReportToken" : "MT67-F944",
    "CurrentAge" : "31",
    "DateOfBirth" :
    { "DOBUUnlockToken" : "6WQklLRJwsr8++mgIcjm+jf/NXnDn3T9SQZk6wU5CYo=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "ETHAN",
      "MiddleName" : "KUSHAN",
      "LastName" : "CLARK",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "Boq/SGdaKFE0qrLGF6b8RzDywm11PnMAkM8zkwtFIEI=",
        "Year" : "XXXX" },
      "CurrentAge" : "58" },
    "ReportToken" : "HLH7-7J3Q",
    "CurrentAge" : "58",
    "DateOfBirth" :
    { "DOBUUnlockToken" : "N6HAzTHgYZTV/HsX/3zjJ0iH03/IY27h0b+js460lkQ=",
      "Year" : "XXXX" } },

  { "Name" :
    { "FirstName" : "PEDRO",
      "MiddleName" : "RUBEN",
      "LastName" : "CLARK DE",
      "NameSuffix" : "" },
    "DateOfBirthRecord" :
    { "DateOfBirth" :
      { "DOBUUnlockToken" : "zaAKezK4fReLIBCv6x2qLVmxUIXn3WZ6B+eNRZ2xQ3g=",
        "Year" : "XXXX" },
      "CurrentAge" : "26" },
    "ReportToken" : "JPND-WL3D",
    "CurrentAge" : "26",
    "DateOfBirth" :
    { "DOBUUnlockToken" : "e9hFQFTguRS3uRHe63mdbp160kgo6wyWi0ZLEGkf9Ug=",
      "Year" : "XXXX" } } ] },
  "NumberOfUtilityRecordsAvailable" : "1",
  "Deceased" : "No" } ] } } },
  "transactionId" : "DEMO-TL01-6E1C-7399-9842857",
  "errorCode" : 0,
  "numberOfRecordsFound" : 1,

```

```
"responseTime" : "0",
"deceased" : "No",
"names" :
[
  { "firstName" : "XAVIER",
    "middleName" : "ZANE",
    "lastName" : "CLARK" },

  { "firstName" : "XAVIER",
    "middleName" : "ZANE",
    "lastName" : "CLARK PUIG" },

  { "firstName" : "XAVIER",
    "middleName" : "ZANE",
    "lastName" : "RODRIGUEZ" },

  { "firstName" : "CLARENCE",
    "middleName" : "XAVIER",
    "lastName" : "CLARK" },

  { "firstName" : "XAVIER",
    "middleName" : "ZANE",
    "lastName" : "CLARK" },

  { "firstName" : "XAVIER",
    "middleName" : "Q",
    "lastName" : "CLARK" },

  { "firstName" : "Z",
    "middleName" : "ISAAC",
    "lastName" : "RODRIGUEZ CARLOS" },

  { "firstName" : "CLARENCE",
    "middleName" : "S",
    "lastName" : "CLARK" },

  { "firstName" : "XAVIER",
    "middleName" : "Z",
    "lastName" : "LOPEZ" },

  { "firstName" : "XAVIER",
    "middleName" : "Z",
    "lastName" : "SCOTT CASELLANOS" },

  { "firstName" : "XAVIER",
    "middleName" : "Z",
    "lastName" : "LOPEZ" },

  { "firstName" : "XAVIER",
    "middleName" : "Z",
    "lastName" : "PEREZ" },

  { "firstName" : "XAVIER",
    "middleName" : "S",
    "lastName" : "CLARK" },

  { "firstName" : "XAVIER",
    "middleName" : "H",
    "lastName" : "CLARK" } ],
"emails" :
[ "xavier.clark01@fantasyisland.com",
  "xavier.clark12@fantasyisland5.com",
```

```
"xavier.clark23@fantasyisland2.com",
"xavier.clark34@fantasyisland.com" ],
"addressPhones" :
[ "5613919369",
  "5613915366",
  "5613919369",
  "5613915366" ],
"otherPhones" :
[ "9546829969",
  "9546829970",
  "3058482659",
  "3051142469",
  "9546829965",
  "3051132469",
  "9543395243",
  "3057640409",
  "3053395243",
  "2703246385",
  "9544724320",
  "9546125638",
  "3051143469" ] }
```

V-Z



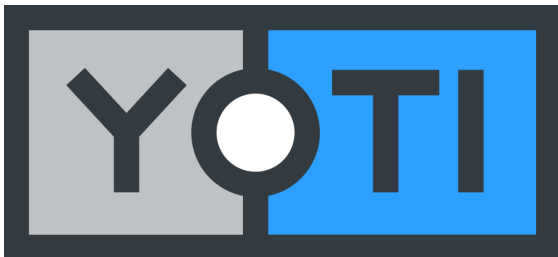
Variable Connector

The Variable connector lets you store and retrieve flow and user attributes as variables in your PingOne DaVinci flow.



Veriff Connector

The Veriff connector lets you verify users with Veriff's artificial intelligence (AI)-powered identity solution for identity fraud prevention in your PingOne DaVinci flow.



Yoti Connector

The Yoti connector lets you provide customers with a safe way to prove who they are through Yoti's identity verification, age estimate, and age verification services in your PingOne DaVinci flow.

Variable Connector

The Variable connector lets you store and retrieve flow and user attributes as variables in your PingOne DaVinci flow.

Setup

Resources

For information and setup help, see the following:

- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Configuring the Variable connector

In DaVinci, add a Variable connector. For more information, see [Adding a connector](#).

Note

This connector doesn't have a configuration at the environment level. You configure it in your flow instead.

Using the connector in a flow

Variables are values that can be read and modified during a flow. In DaVinci, variables allow users to track and adjust values within flows. They can be read and modified during a flow. Variables can be strings, Boolean values, numbers, or objects.

In a flow, variables can be used to track information and a variable's value can be used to determine which nodes are run within the flow. Every variable has a context, which determines how widely its value is shared. There are three types of variables:

Flow Instance Variable

Persists only for a single execution of a flow. This is useful for storing things temporarily for an execution, such as if you want to store a particular value from one node to use it later in the flow.

Flow Variable

Persists across multiple executions of that flow. This is useful for storing common things that are shared across multiple executions of the same flow.

User Variable

A shadow user must be available in order to use this variable. This capability adds a value to the user's details or `userInfo` in DaVinci.

The DaVinci Variable connector has several capabilities that allow you to manage flows, flow instances, and user variables used across flows and instances.

Capabilities

Flow Instance Variable

Add and update flow instance variable

Properties

saveVariables selectNameValueListColumn

Input Schema

- default object
 - properties object

Output Schema

- output object::

Flow Variable

Add and update flow variable

Properties

saveFlowVariables selectNameValueListColumn

Input Schema

- default object
 - properties object

Output Schema

- output object::

Flow Instance variable: Increment by N

Flow instance variables are local to the specific instance of a flow.

Properties

Local Variable Name textField
incrementCounter textField

Input Schema

- default object
 - variables object
 - properties object
 - variable
 - incrementCounter

Output Schema

- output object
 - newValue number

Output Example

```
{ "newValue" : 4 }
```

User Variable

Add and update user variables used across flows and flow instances.

Properties

saveVariables selectNameValueListColumn

Input Schema

- default object
 - userInfo object required
User Information record to which the variable is saved.
 - properties object

Output Schema

- output object::

User variable: Increment by N

If the user is known, variables can contain user context across flows and flow instances.

Properties

Local Variable Name textField
incrementCounter textField

Input Schema

- default object
 - userInfo object required
User Information record to which the variable is saved.
 - properties object
 - variable
 - incrementCounter

Output Schema

- output object
 - newValue number

Output Example

```
{ "newValue" : 4 }
```

Set Language

Set the language to be used for localized content.

Properties

Locale textField required

The language to be used for localized content. This should be a valid locale code, such as "en-US" or "fr-FR".

Input Schema

- default object
 - properties object
 - locale string required

Output Schema

- language string

Veriff Connector

The Veriff connector lets you verify users with Veriff's artificial intelligence (AI)-powered identity solution for identity fraud prevention in your PingOne DaVinci flow.

You can use the Veriff connector to:

- Verify a user's age with user-submitted identity documents
- Redirect to Veriff for age verification
- Make a custom API call

Setup

Resources

For information and setup help, see the following:

- Veriff documentation:
 - [Veriff documentation](#)
 - [Getting started with Veriff](#)
- DaVinci documentation:
 - [Adding a connector](#)
 - [Using connectors securely](#)
 - [Using DaVinci flow templates](#)

Requirements

To use the connector, you'll need:

- A Veriff license
- Your Veriff credentials

Setting up Veriff

Follow the instructions in [Getting started with Veriff](#).

Configuring the Veriff connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

Base URL

The API URL to target, for example, <https://stationapi.veriff.com/>

API Key

Your Veriff API key, for example, 123-456-789

Shared Secret Key

Your Veriff shared secret key, for example, 123-456-789

Using the connector in a flow

Verify a user's age by redirecting to Veriff

The **Redirect to Veriff for Verification** capability provides an alternative to age verification with a custom DaVinci user experience flow, instead redirecting the user to a complete age verification experience hosted by Veriff.

No special configuration is needed. Add the capability and populate its properties according to the help text.

Creating a custom API call

If you want to do something that isn't supported by one of the provided capabilities, you can use the **Make a Custom API Call** capability to define your own action.

This capability uses the credentials from your connector to make an API call with the HTTP method, headers, query parameters, and body you specify.

Capabilities

Create Session

Create a verification session with the user's name and personal details.

Properties

First Name textField required

The user's first name.

Last Name textField required

The user's last name.

Gender textField required

The user's gender, such as 'male' or 'female'.

Date of Birth textField required

The user's date of Birth, formatted as YYYY-MM-DD, such as '1979-01-30'.

National Identification Number textField required

The user's national identification number, such as 'AB123456C'.

Vendor Data textField required

Your organization's unique identifier for the user. This value is returned by Veriff in the Receive Webhook Response capability, which allows you to identify users that submit multiple different photos or documents using the same user identifier.

Output Schema

- output object
 - status string
 - verification object
 - id string
 - url string
 - vendorData string
 - host string
 - status string
 - sessionToken string
 - sessionId string

Upload Images

Submit identity documents and selfie photos.

Properties

Session ID textField required

The user's Veriff session ID. Use the Create Session capability to get a session ID.

Document Front textArea required

The Base64-encoded image of the front of the identity document.

Document Back textArea required

The Base64-encoded image of the back of the identity document.

Selfie Image textArea required

The Base64-encoded image of the user's selfie photo.

Output Schema

- output object
 - documentFront object
 - status string
 - image object
 - context string
 - id string
 - name string
 - timestamp string
 - size integer
 - mimetype string
 - url string
 - documentBack object
 - status string
 - image object
 - context string
 - id string
 - name string
 - timestamp string
 - size integer
 - mimetype string
 - url string
 - face object
 - status string
 - image object
 - context string
 - id string
 - name string
 - timestamp string
 - size integer

- mimetype string
- url string

Submit Session for Review

Submit the session for review after uploading images.

Properties

Session ID textField required

The user's Veriff session ID. Use the Create Session capability to get a session ID.

Output Schema

- output object
 - response object
 - status string
 - verification object
 - id string
 - url string
 - vendorData string
 - host string
 - status string
 - sessionToken string
 - challengeld string

Wait for Session Review Result

Wait for Veriff to send the result of the session review to the DaVinci webhook URL.

Output Schema

- output object
 - response object
 - status string
 - verification object
 - id string
 - code number
 - vendorData string
 - person object
 - status string
 - vendorData string
 - rawResponse object

Redirect to Veriff for Verification

Redirect the browser to a complete user verification experience provided by Veriff.

Properties

First Name textField required

The user's first name.

Last Name textField required

The user's last name.

Vendor Data textField required

Your organization's unique identifier for the user. This value is returned by Veriff in the Receive Webhook Response capability, which allows you to identify users that submit multiple different photos or documents using the same user identifier.

Output Schema

- output object
 - response object
 - status string
 - verification object
 - sessionId object
 - redirectUrl string
 - challenge string

Make Custom API Call

Define and use your own call to the Veriff API.

Properties

Endpoint textField required

The Veriff API endpoint, such as "sessions/:sessionId/media".

Method dropDown required

The method to use for the call.

- GET (Default)
- POST
- DELETE
- PATCH

Query parameters and values to include in the call keyValuePairList

Add query parameters and provide their values.

Headers keyValuePairList

HTTP headers and values to use in the call.

Body textArea

The raw JSON body

Output Schema

- output object
 - rawResponse object
 - status number
 - headers object

Yoti Connector

The Yoti connector lets you provide customers with a safe way to prove who they are through Yoti's identity verification, age estimate, and age verification services in your PingOne DaVinci flow.

You can use the Yoti connector to:

- Estimate a user's age with a selfie photo.
- Verify users with multiple different methods.
- Wait for verification results from Yoti.

Setup

Resources

For information and setup help, see the following:

- Yoti:
 - [Yoti Developer Documentation](#) 
 - [Age Verification Documentation](#) 
- DaVinci documentation:
 - [Adding a connector](#) 
 - [Using connectors securely](#) 
 - [Using DaVinci flow templates](#) 

Requirements

To use the connector, you'll need:

- A Yoti license
- Your Yoti credentials

Setting up Yoti

Follow the instructions in [Yoti Quick Start](#).

Configuring the Yoti connector

Add the connector in DaVinci as shown in [Adding a connector](#), then configure it as follows.

Connector configuration

SDK ID

Your Yoti client SDK ID.

API Key

Your Yoti client API key.

Using the connector in a flow

Age estimation

You can use the **Estimate Age Using Live Photo** capability to prompt the user to take a selfie photo and return an estimated age.

Following your **Estimate Age Using Live Photos** capability, add another Yoti connector node and select the **Wait for Verification Result** result.

Note

You can customize the waiting page HTML or CSS in the **Wait for Verification Result** node.

Age verification

The connector has several capabilities that allow you to verify the user's age:

- **Verify Age Using Digital ID Credential**
- **Verify Age Using Identity Documentation**
- **Verify Age Using Credit Card**
- **Verify Age Using Mobile Carrier Contact**
- **Verify Age with Credit Agency**

Following your age verification capability, for all capabilities except the **Verify Age with Credit Agency** capability, add another Yoti connector node and select the **Wait for Verification Result** capability.

 Note

You can customize the waiting page HTML or CSS in the **Wait for Verification Result** node.

Capabilities

Estimate Age Using Live Photo

Prompt the user to take a selfie photo. Yoti analyzes the photo and returns an estimated age, such as "25".

Properties

Age Check Method dropdown required

Determines whether Yoti returns a true or false response or provides the user's numerical age.

- Must be over Age Threshold (Default)
- Must be under Age Threshold
- Get age from Yoti

Age Threshold textField required

Enter the required age, such as "21". The user must be over or under this age, depending on the Age Check Method.

Check for Liveness toggleSwitch required

When enabled, Yoti uses passive analysis to check the image for signs that it might be a 2D image, mask, or bot.

Display Name button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Input Schema

- default object
 - type string
 - ageEstimation boolean
 - threshold number
 - estimationLevel string

Output Schema

- location string
- output object
 - sessionId string

Verify Age Using Digital ID Credential

Prompt the user to scan a QR code and open a digital ID app, then provide Yoti with a verified age attribute from the app.

Properties

Age Check Method dropDown required

Determines whether Yoti returns a true or false response or provides the user's numerical age.

- Must be over Age Threshold (Default)
- Must be under Age Threshold
- Get age from Yoti

Age Threshold textField required

Enter the required age, such as "21". The user must be over or under this age, depending on the Age Check Method.

Display Name button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - type string
 - ageEstimation boolean
 - threshold number
 - estimationLevel string

Output Schema

- location string
- output object
 - sessionId string

Verify Age Using Identity Document

Prompt the user to scan a photo ID document and take an optional selfie photo. Yoti verifies the document ID and matches the photo to the document.

Properties

Age Check Method dropDown required

Determines whether Yoti returns a true or false response or provides the user's numerical age.

- Must be over Age Threshold (Default)
- Must be under Age Threshold
- Get age from Yoti

Age Threshold textField required

Enter the required age, such as "21". The user must be over or under this age, depending on the Age Check Method.

Additional Authenticity Check dropDown

Determines whether Yoti performs a visual check on the document. For more information, contact your Yoti representative.

- None
- Automatic
- Manual

Country Code textField

The user's three-digit country code, in ISO 3166 Alpha-3 format, such as "USA".

Check for Liveness toggleSwitch required

When enabled, Yoti uses passive analysis to check the image for signs that it might be a 2D image, mask, or bot.

Display Name button

showPoweredBy toggleSwitch

skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - type string
 - ageEstimation boolean
 - threshold number
 - estimationLevel string

Output Schema

- location string
- output object
 - sessionId string

Verify Age Using Credit Card

Prompt the user to enter their credit card number, expiry, postal code, and CV number. Yoti verifies the information to prove that the user is old enough to possess a credit card.

Properties

Display Name button
showPoweredBy toggleSwitch
skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - botton string
 - showPoweredBy boolean
 - skipButtonPress number

Output Schema

- location string
- output object
 - sessionId string

Verify Age Using Mobile Carrier Contract

Prompt the user to enter their name, date of birthday, mobile phone number, and address. Yoti sends an SMS confirmation message to prove the user is old enough to possess a mobile carrier contract.

Properties

Display Name button
showPoweredBy toggleSwitch
skipButtonPress toggleSwitch

Input Schema

- default object
 - properties object
 - botton string
 - showPoweredBy boolean
 - skipButtonPress number

Output Schema

- location string
- output object
 - sessionId string

Verify Age with Credit Agency

Prompt the user to enter their name, address, and date of birth. Yoti verifies the information against credit bureau databases to prove the user's age.

Properties

First Name textField required

The user's first name.

Last Name textField required

The user's last name.

Country textField required

The user's country, in ISO 3166-1 alpha-2 format, such as "US".

Address Line 1 textField required

The first line of the user's address, such as "123 Main Street".

Address Line 2 textField

The second line of the user's address, such as "Unit 10".

Address Line 3 textField

The third line of the user's address.

Postal Code textField required

The user's postal code.

Date of Birth textField required

Date of birth in format "MM/DD/YYYY".

Input Schema

- default object

Output Schema

- output object
 - status string
 - result boolean
 - age number
 - method string
 - type string

Wait for Verification Result

Show a waiting page until Yoti sends the result of the age estimation or verification to the DaVinci webhook URL.

Properties

Session ID textField required

HTML Template textArea

Default:

```
<div
  class="bg-light d-flex flex-column justify-content-center align-items-center position-absolute top-0
start-0 bottom-0 end-0 overflow-auto">
  <div class="mh-100" style="max-width: 400px; width: 100%">
    <div class="card shadow mb-5">
      <div class="card-body p-5 d-flex flex-column">
        
        <p class="text-muted text-center">
          We're processing your request.
        </p>
      </div>
    </div>
  </div>
</div>
```

CSS codeEditor

Default:

```
@import "https://assets.pingone.com/ux/astro-nano/0.1.0-alpha.1/astro-nano.min.css";
@import "https://assets.pingone.com/ux/astro-nano/0.1.0-alpha.1/icons.css";
```

Input Schema

- default object
 - sessionId string
 - customHTML string
 - customCSS string

Output Schema

- output object
 - age number
 - method string
 - id string
 - state string
 - status string
 - sessionId string