Auth node reference

July 4, 2025

AM

Version: 8

Table of Contents

Behavioral nodes

Contextual nodes

Federation nodes

Identity management nodes

Utility nodes

Basic nodes

Data Store Decision node

The **Data Store Decision** node checks that the credentials provided during authentication match the ones stored in the configured data store for the realm.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `realm`, `username`, and `password` properties in the incoming node state.

You can implement the following nodes as inputs to the Data Store Decision node:

Input nodes

- Username Collector node (standalone AM) or Platform Username node (Ping Identity Platform deployment)
- Password Collector node (standalone AM) or Platform Password node (Ping Identity Platform deployment)
- Zero Page Login Collector node

Dependencies

The Data Store Decision node is a basic node used in many authentication application types, such as basic, push, OAuth 2.0, and social provider authentication applications.

Configuration

This node has no configurable properties.

Outputs

This node copies shared and transient state into the outgoing node state.

Outcomes

Returns a boolean outcome:

`True`

The credentials match those found in the data store.

`False`

The credentials do *not* match those found in the data store.

Errors

The following Data Store Decision node warnings and errors can appear in the logs:

Warnings

- "invalid password error"
- "invalid username error"

Errors

- "Exception in data store decision node"

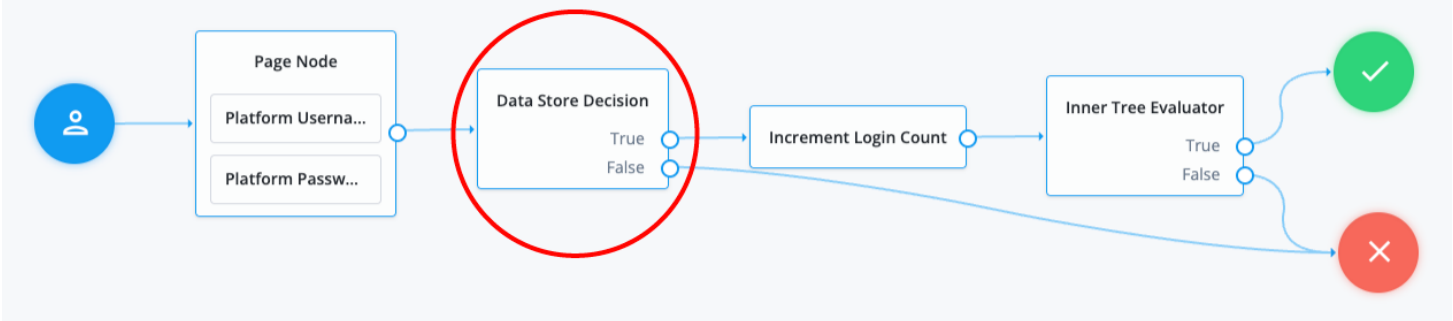
Troubleshooting

Review any errors and warnings this node logged.

- If this node logged a warning, fix the credentials and try again.
- If this node logged an error, review the log messages for the transaction to find the reason for the exception.

Examples

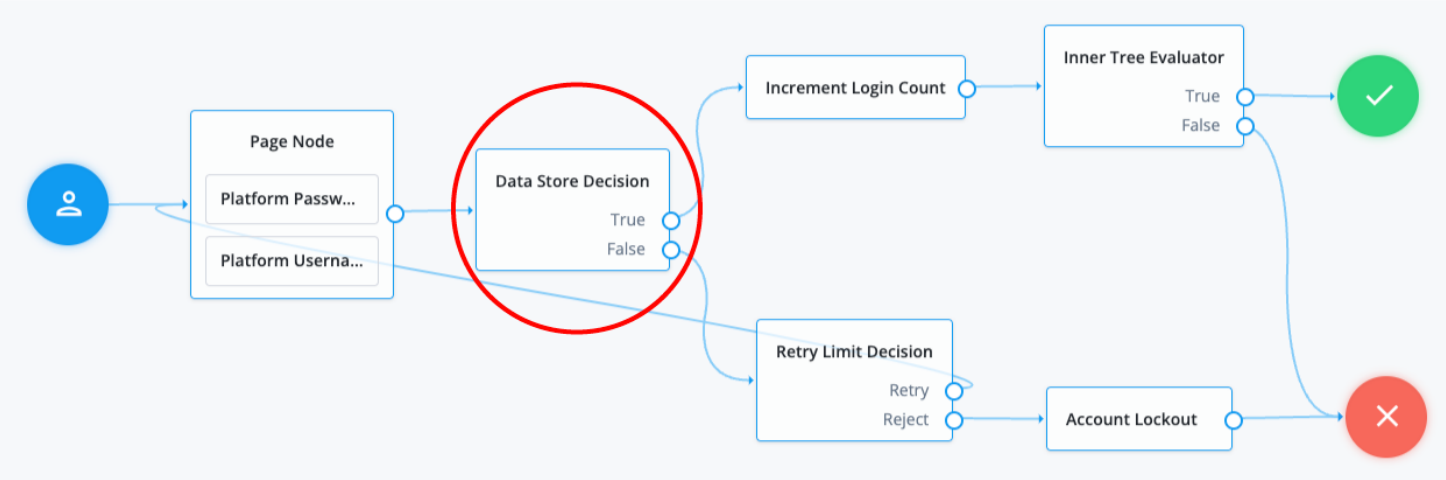
Example 1: Simple username and password collector nodes with Data Store Decision node



This example illustrates a simple login process. The journey involves a Page node that contains two embedded nodes: Platform Username node and Platform Password node. To enhance user experience, the Page node lets users input their username and password on a single page, instead of splitting them across two different pages.

The Data Store Decision node has two outcomes: `True` or `False`. When the outcome is `True`, it triggers a Login Count Decision node. The Increment Login Count node then moves to an Inner Tree Evaluator node, which performs additional login processes. The `False` outcome connects directly to a failure node, indicating a failed state where the username and/or password provided by the user did not match the information stored in the data store.

Example 2: Grant the user several attempts to enter their credentials correctly



In the following example, when an authentication attempt fails at the Data Store Decision node, you can direct it to a Retry Limit Decision node. The Retry Limit Decision node determines the number of retries allowed and either retries the login attempt or rejects it. If the journey rejects the login attempt after reaching the configured limit, for example three attempts, the operation results in an account lockout.

Alternate nodes

The LDAP Decision node supports LDAP Behera Password Policies with separate outcomes for accounts that are locked and passwords that have expired.

Failure node

The **Failure** node is a required element indicating the journey ended in failure.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes

Product	Available?
Ping Identity Platform (self-managed)	Yes

Inputs

The failure outcomes of any preceding nodes.

Dependencies

None.

Configuration

This node has no configurable properties.

Outputs

None. The authentication journey ends in failure.

Outcomes

The authentication journey completes, ending in failure.

AM redirects the user to a failure URL.

Errors

The error depends on the **Authentication > Settings > Account Lockout > Login Failure Lockout Mode** setting for the realm (under **Native Consoles > Access Management**).

Without the setting enabled, by default, the node returns an error with a message such as the following:

```
{"code":401,"reason":"Unauthorized","message":"Login failure"}
```

With the setting enabled, the node checks the invalid attempts property of the user profile and does the following:

- Returns a warning message if the number of failed attempts is equal to or greater than the **Authentication > Settings > Account Lockout > Warn User After N Failures** setting:

```
{
  "code": 401,
  "reason": "Unauthorized",
  "message": "Warning: You will be locked out after 1 more failure(s).",
  "detail": {
    "failureUrl": ""
  }
}
```

- Increments the failure count in the user profile.
- Returns an error message if the account is `Inactive`:

```
{
  "code": 401,
  "reason": "Unauthorized",
  "message": "User Locked Out.",
  "detail": {
    "failureUrl": ""
  }
}
```

To troubleshoot an authentication failure, review the steps in the journey to find what caused the failure.

Examples

All authentication journeys have a **Failure** node as one of their terminals.

Identity Store Decision node

The **Identity Store Decision** node attempts to match the provided username and password with the credentials stored in the identity store.

If the credentials exist, the node checks the following:

- Is the profile locked?
- Has the provided password expired?
- Has the user cancelled a password reset?

Compatibility

Product	Compatible?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	No

Product	Compatible?
Ping Identity Platform (self-managed)	No

Inputs

The node reads the `username` and `password` fields from the node state.

The journey can provide these credentials in a number of ways, for example, with a combination of the Platform Username node and Platform Password node, or by using the Zero Page Login Collector node.

Dependencies

None

Configuration

Property	Usage
Minimum Password Length	For password change requests, the node rejects passwords that are shorter than this value. If you set this value to `0`, the node doesn't check the password length. Default: `8`
Username as Universal Identifier	If you enable this property, the `username` property is set to the value of the `uuid`. For example, `"username": "c636b756-ba6b-481d-ab4a-ab8c064cb24b"`. If this property is false, the value of the `username` property remains unchanged. For example, `"username": "bjensen"`. Default: false
Use mixed case for password change messages	Return password change messages in mixed (sentence) case. By default password reset and password change messages are transformed to upper case. Enable this option to return messages in sentence case. Default: Disabled

Outputs

This node copies shared and transient state into the outgoing node state.

Outcomes

`True`

The credentials match those found in the identity store.

`False`

The credentials don't match those found in the identity store.

`Locked`

The profile associated with the provided credentials is locked.

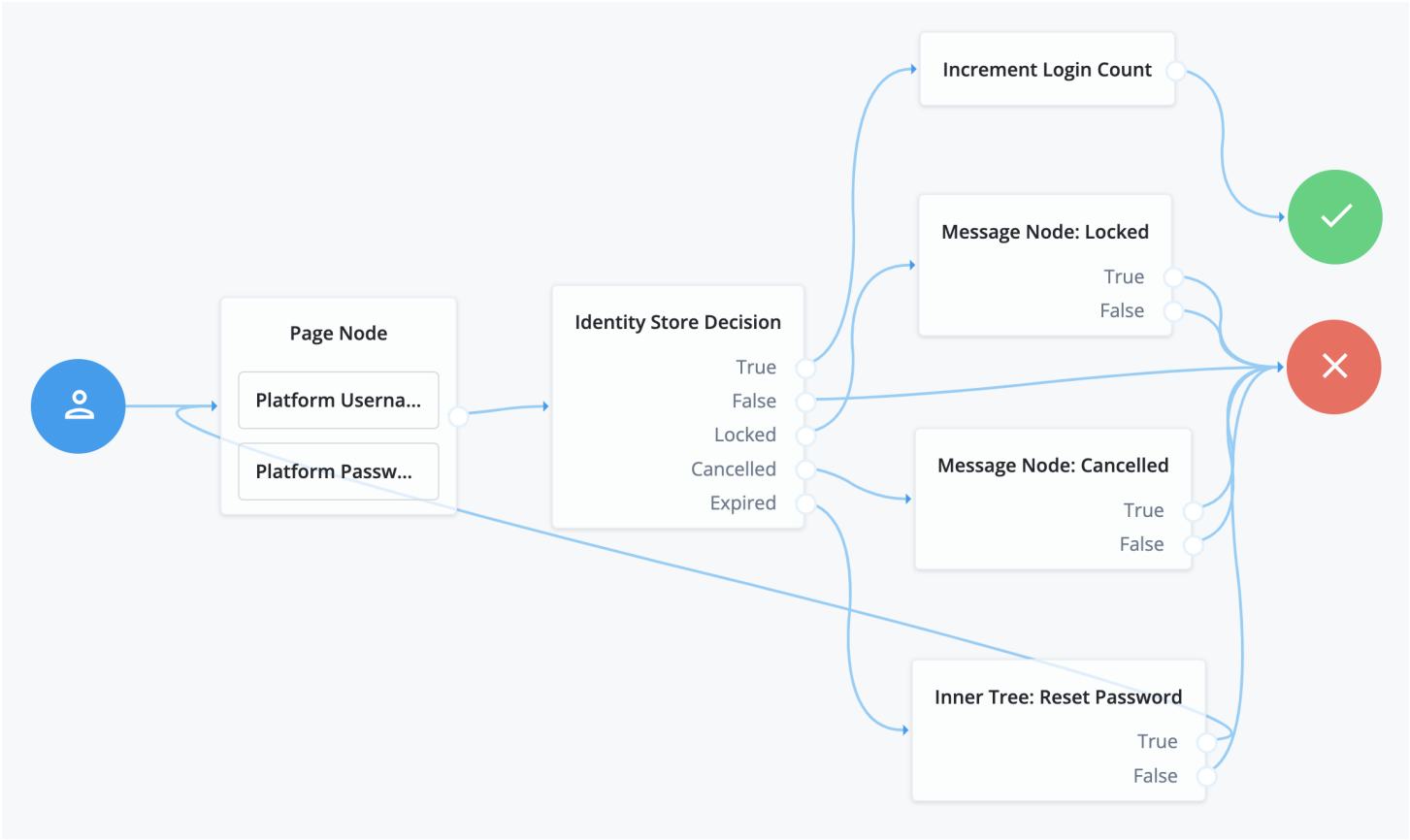
`Cancelled`

The user cancelled a password change request. The example provides a detailed explanation of this outcome.

`Expired`

The credentials match those found in the identity store, but the password has expired.

Example



This example illustrates a simple login process.

- A Page node with the embedded nodes (Platform Username node and Platform Password node) prompts the user for their credentials.
- The Identity Store Decision node assesses the credentials:
  - If it finds the credentials in the data store and the credentials are valid, the journey follows the `True` outcome. An Increment Login Count node increments the login count and the user is authenticated.
  - If the credentials don't exist in the data store, the journey follows the `False` outcome and authentication fails.

- If the credentials exist in the data store but the account is locked, the journey follows the `Locked` outcome. A Message node displays a custom lockout message and authentication fails.
- If the credentials exist in the data store but the user must change their password, the node prompts the user to change their password. If the user cancels this change request, the journey follows the `Cancelled` outcome. A Message node displays a custom message and authentication fails.
- If the credentials exist in the data store but the password has expired, the node follows the `Expired` outcome. The user is routed to an inner tree journey that contains the password reset logic and then routes the user to the start of the journey to authenticate again.

Alternative nodes

- The Data Store Decision node is a simpler node with only two outcomes, `True` and `False`. Use this node if the flow only requires these outcomes.

Kerberos node

Enables desktop single sign-on such that a user who has already authenticated with a Kerberos Key Distribution Center can authenticate to AM without having to provide the login information again.

To achieve this, the user presents a Kerberos token to AM through the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol.

End users may need to set up Integrated Windows Authentication in Internet Explorer or Microsoft Edge to benefit from single sign-on when logged on to a Windows desktop.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

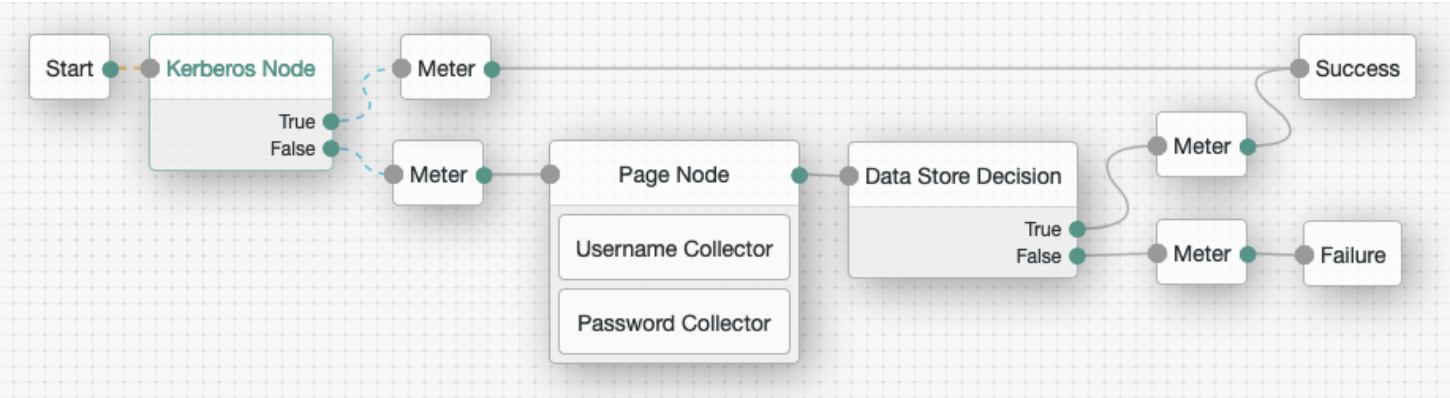
Evaluation continues along the `True` path if Windows Desktop SSO is successful; otherwise, evaluation continues along the `False` path.

Properties

Property	Usage
Service Principal	Specifies the Kerberos principal for authentication in the format `HTTP/AM-DOMAIN@AD-DOMAIN`, where *AM-DOMAIN* corresponds to the host and domain names of the AM instance, and *AD-DOMAIN* is the domain name of the Kerberos realm (the FQDN of the Active Directory domain). *AD-DOMAIN* can differ from the domain name for AM. In multi-instance AM deployments, configure *AM-DOMAIN* as the FQDN or IP address of the load balancer in front of the AM instances. For example, `HTTP/AM-LB.example.com@KERBEROSREALM.INTERNAL.COM`.
Key Tab File Path	Specifies the full, absolute path of the keytab file for the specified Service Principal. **Tip** You generate the keytab file using the Windows `ktpass` utility. For example: `C:\> ktpass -out fileName.keytab -princ HTTP/openam.example.com@AD_DOMAIN.COM -pass +rdnPass -maxPass 256 -mapuser amKerberos@frdpcloud.com -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -kvno 0`
Kerberos Realm	Specifies the name of the Kerberos (Active Directory) realm used for authentication. Must be specified in ALL CAPS.
Kerberos Server Name	Specifies the fully qualified domain name, or IP address of the Kerberos (Active Directory) server.
Trusted Kerberos realms	Specifies a list of trusted Kerberos realms for user Kerberos tickets. If realms are configured, then Kerberos tickets are only accepted if the realm part of the user principal name of the user's Kerberos ticket matches a realm from the list. Each trusted Kerberos realm must be specified in all caps.
Return Principal with Domain Name	When enabled, AM returns the fully qualified name of the authenticated user rather than just the username.
Lookup User In Realm	Validates the user against the configured data stores. If the user from the Kerberos token is not found, evaluation continues along the `False` path. This search uses the `Alias Search Attribute Name` from the core realm attributes. Learn more about this property in User profile.
Is Initiator	When enabled (`true`), specifies that the node is using *initiator* credentials, which is the default. When disabled (`false`), specifies that the node is using *acceptor* credentials.

Example

This flow attempts to authenticate the user with Windows Desktop SSO. If unsuccessful, AM requests the username and password for login. Meter nodes are used to track metrics for the various paths through the flow:



LDAP Decision node

The **LDAP Decision** node verifies that the provided username and password exist in the specified LDAP user data store. The node also checks whether the associated user account has expired or is locked out.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `username` and `password` properties in the incoming node state. Implement the following nodes earlier in the journey:

- Standalone PingAM deployment
  - Username Collector node
  - Password Collector node
- Ping Identity Platform deployment:
  - Platform Username node
  - Platform Password node

You can also use the Zero Page Login Collector node.

Prerequisites

None

Configuration

Property	Usage
Primary LDAP Server *(required)*	Specify one or more primary directory servers. Specify each directory server in the following format: `host:port`. For example, `directory_services.example.com:389`.
Secondary LDAP Server	Specify one or more secondary directory servers. Specify each directory server in the following format: `host:port`. The journey uses the secondary servers when none of the primary servers are available. For example, `directory_services_backup.example.com:389`.
DN to Start User Search *(required)*	Specify the DN from which to start the user search. More specific DNs, such as `ou=sales,dc=example,dc=com`, result in better search performance. If multiple entries with the same attribute values exist in the directory server, make sure this property is specific enough to return only one entry.
Bind User DN, **Bind User Password**	The credentials used to connect to the LDAP user data store.
Attribute Used to Retrieve User Profile *(required)*	The attribute used to retrieve a user profile from the directory server. The user search will have already happened, as specified by the **Attributes Used to Search for a User to be Authenticated** and **User Search Filter** properties.
Attributes Used to Search for a User to be Authenticated *(required)*	The attributes the node uses to match the credentials provided by the user to an entry in the directory server. For example, a value of `uid` forms the search filter `uid=user`. If you specify multiple values, such as `uid` and `cn`, the node forms a complex search filter `(|(uid=user)(cn=user))`. Multiple attribute values let the user authenticate with any one of the values. For example, if you set both `uid` and `mail`, then Barbara Jensen can authenticate with either `bjensen` or `bjensen@example.com`. **Note** If you are using account lockout and you set multiple attribute values here, you must add those attributes to the `Alias Search Attribute Name` property in the User profile.

Property	Usage
User Search Filter	A filter to append to user searches. For example, if your search attribute is `mail` and you set **User Search Filter** to `(objectClass=inetOrgPerson)`, the node uses `(&(mail=address)(objectClass=inetOrgPerson))` as the resulting search filter. In this example, *address* is the mail address provided by the user.
Search Scope	The extent of the search for users in the directory server: • `OBJECT`: The search extends only to the entry specified by the **DN to Start User Search**. • `ONELEVEL`: The search extends to the entries that are direct children of the **DN to Start User Search**. • `SUBTREE`: The search extends to the **DN to Start User Search** and every entry under it. Default: `SUBTREE`
LDAP Connection Mode	Specifies whether to use SSL or StartTLS to connect to the directory server. The node must be able to trust the certificates used. Possible values: `LDAP`, `LDAPS`, and `StartTLS` Default: `LDAP`
mTLS Enabled	Enables mTLS (mutual TLS) between AM and the directory server. This setting applies to *all* configured LDAP servers; that is, AM uses mTLS to authenticate to all LDAP servers configured for this node. When mTLS is enabled, AM ignores the values for **Bind User DN** and **Bind User Password**. If you enable this property, you must: • Set the **LDAP Connection Mode** to `LDAPS` • Provide an **mTLS Secret Label Identifier** Default: Disabled
mTLS Secret Label Identifier	Identifier used to create a secret label for mapping to the mTLS certificate in the secret store. AM uses this identifier to create a specific secret label for this node. The secret label takes the form `am.authentication.nodes.ldap.decision.mtls.identifier.cert`, where `identifier` is the value of **mTLS Secret Label Identifier**. The identifier can only contain alphanumeric characters (`a-z`, `A-Z`, `0-9`) and periods (`.`). It can't start or end with a period. All LDAP servers configured for this node share the same secret label. For more security, you should rotate certificates periodically. When you rotate a certificate, update the corresponding mapping in the realm secret store configuration to reflect this label. When you rotate a certificate, AM closes any existing connections using the old certificate. A new connection is selected from the connection pool and no server restart is required.

Property	Usage
Return User DN to DataStore	When enabled, the node returns the DN rather than the User ID. From the DN value, AM uses the RDN to search for the user profile. For example, if a returned DN value is `uid=demo,ou=people,dc=openam,dc=example,dc=org`, AM uses `uid=demo` to search the directory server. Default: Enabled
User Creation Attributes	This list lets you map (external) attribute names from the LDAP directory server to (internal) attribute names used by AM.
Minimum Password Length	The minimum acceptable password length. Default: `8`
LDAP Behera Password Policy Support	When enabled, support interoperability with servers that implement the Internet-Draft, Password Policy for LDAP Directories. Default: Enabled
Trust All Server Certificates	When enabled, the server blindly trusts server certificates, including self-signed test certificates. Default: Disabled
LDAP Connection Heartbeat Interval	Specifies how often AM should send a heartbeat request to the directory server to ensure that the connection doesn't remain idle. Some network administrators configure firewalls and load balancers to drop connections that are idle for too long. Set the units for the interval in the `LDAP Connection Heartbeat Time Unit` property. **Note** Setting this property to `0` does *not* disable the heartbeat (keepalive) or load balancer availability checks. Disabling these features can only be configured at the global level. Default: `10`
LDAP Connection Heartbeat Time Unit	The time unit for the `LDAP Connection Heartbeat Interval`. Default: `seconds`
LDAP Operations Timeout	The timeout, in seconds, that AM should wait for a response from the directory server. Default: `0` (means no timeout)
Use mixed case for password change messages	Specifies whether the server returns password change messages in mixed (sentence) case or transforms them to uppercase. By default, the server transforms password reset and password change messages to uppercase. Enable this setting to return messages in sentence case. Default: Disabled

Property	Usage
LDAP Affinity Level	Level of affinity used to balance requests across LDAP servers. Affinity-based load balancing means that each request for the same user entry goes to the same DS server. The DS server used for a specific operation is determined by the DN of the identity involved. List the directory server instances that form part of the affinity deployment in the **Primary LDAP Server** and **Secondary LDAP Server** properties. Options are: • `NONE` – no affinity • `BIND` – affinity for BIND requests only • `ALL` – affinity for all requests Default: `NONE`

Outcomes

`True`

The provided credentials match those found in the LDAP user data store.

`False`

The provided credentials don't match those found in the LDAP user data store.

`Locked`

The profile associated with the provided credentials is locked.

`Cancelled`

The user must change their password. When the journey prompts the user to change their password, the user cancels the password change.

`Expired`

The profile is found, but the password has expired.

> **Important**
>
> The LDAP Decision node *requires* specific user attributes in the LDAP user data store. These required attributes are present by default in PingDS. If you are using an alternative identity store, you might need to modify your LDAP schema to use this node.

Password Collector node

Prompts the user to enter their password.

The captured password is transient, persisting only until the authentication flow reaches the next node requiring user interaction.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

Single outcome path.

Evaluation continues after capturing the password.

Properties

This node has no configurable properties.

Success node

The **Success** node is a required element indicating the journey ended successfully.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The success outcomes of any preceding nodes.

Dependencies

None.

Configuration

This node has no configurable properties.

Outputs

None.

Outcomes

The authentication journey completes successfully.

The node resets the failure count in the user profile when reached if the **User Status** property is set to `Active`.

Errors

- Checks the **Status** property of the user profile, when reached, and fails the authentication with an error message if the account is marked as `Inactive`:

```
{
    "code":401,
    "reason":"Unauthorized",
    "message":"User Locked Out.",
    "detail":
    {
        "failureUrl":""
    }
}
```

Examples

All authentication journeys have a **Success** node as one of their terminals.

Username Collector node

Prompts the user to enter their username.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

Single outcome path.

Evaluation continues after capturing the username.

Properties

This node has no configurable properties.

Zero Page Login Collector node

The **Zero Page Login Collector** node verifies the presence of specific HTTP username and password headers in the incoming authentication request. If the headers exist, the node uses their corresponding values as the provided username and password.

The **Zero Page Login Collector** node is commonly used to:

- Connect the `Has Credentials` outcome connector to the input of a Data Store Decision node.
- Connect the `No Credentials` outcome connector to the input of a Username Collector node followed by a Password Collector node (standalone AM) or a Platform Username node followed by a Platform Password node (Ping Identity Platform deployment), and then into the same Data Store Decision node. For an example of this layout, refer to the default `Example` authentication tree provided in AM.

The password collected by this node remains in the node state only until the journey reaches the next node that requires user interaction.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

- HTTP username header
- HTTP password header
- An allowlist of referrers if `Allow Without Referer` property is disabled. When you set the `Allow Without Referer` property to `false`, the request must contain a referrer from the allowlist; otherwise, the journey ends in a failure.

Dependencies

None.

Configuration

Properties

Property	Usage
Username Header name	Enter the name of the header that contains the username value. Default: **X-OpenAM-Username**
Password Header name	Enter the name of the header that contains the password value. Default: **X-OpenAM-Password**
Allow without referer	If enabled, the node accepts incoming requests that do not contain a `Referer` HTTP header. If a `Referer` HTTP header is present, the value is not checked. If disabled, a `Referer` HTTP header must be present in the incoming request, and the value must appear in the Referer allowlist property. Default: `Enabled`
Referer Whitelist	Specify a list of URLs allowed in the `Referer` HTTP header of incoming requests. An incoming request containing a `Referer` HTTP header value not specified in the allowlist causes evaluation to continue along the `No Credentials` outcome path. **Note** You must disable the **Allow Without Referer** property for the referer allowlist property to take effect.

Outputs

The collected credentials from the headers.

Outcomes

- `Has Credentials`
- `No Credentials`

Evaluation continues along the `Has Credentials` outcome path if the specified headers are available in the request, or the `No Credentials` path if the specified headers are not present.

Errors

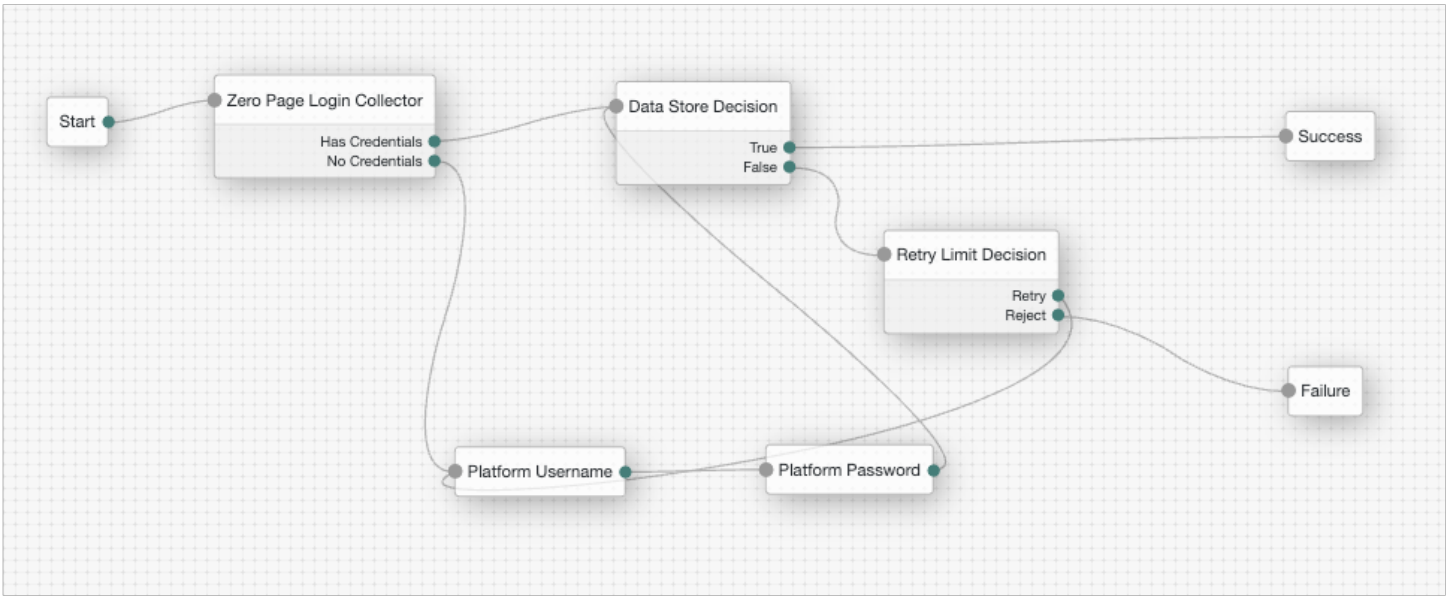
If more than one header value exists for username and/or password, the node returns the following error message

"Expecting only one header value for username and/or password but size is {}."

If the node can't decode the header values, the node returns the following error message

"Could not decode username or password header."

Example



Multi-factor nodes

Combined MFA Registration node

The **Combined MFA Registration node** lets an authenticated user register a device, such as a mobile phone, for multi-factor authentication with a push notification *and* an OATH one-time password in a single step.

This node can make journeys less complex by combining the functionality of the Push Registration node and OATH Registration node.

The node displays a single QR code that users scan to register their device for both push and OATH authentication. Journeys can then use the Push Sender node to verify possession of a registered device. If push does not succeed, for example, the user's device does not have internet access, the journey can fall back to using the OATH Token Verifier node to request a one-time passcode using OATH.

Learn more about push notifications and OATH one-time passwords in MFA: Push authentication and MFA: OATH authentication.]

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires a `username` in the incoming node state to identify which user is registering for MFA.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

Dependencies

You must configure the Push Notification service for the realm to use this node. Optionally, also configure the ForgeRock Authenticator (Push) service.

Find more information in the corresponding documentation for:

- Advanced Identity Cloud

- PingAM

Find information on provisioning the credentials used by the service in How To Configure Service Credentials (Push Auth, Docker) in Backstage.

Configuration

Property	Usage
Issuer	An identifier to appear on the user's device, such as a company name, a website, or a realm. The value is displayed by the authenticator application. For example, `Example Inc.` or the name of your application. Default: `ForgeRock`
Account Name	The profile attribute to display as the username in the authenticator application. If not specified, or if the specified profile attribute is empty, the username is used. Default: `Username`
Background Color	The background color in hex notation that displays behind the issuer's logo within the authenticator application. Default: `032b75`
Logo Image URL	The location of an image to download and display as the issuer's logo within the authenticator application. **Note** The ForgeRock Authenticator supports logos in JPEG and PNG format only. The application resizes your logo automatically, but a maximum image size of one MByte (or 1024 X 1024 pixels) is recommended. Default: none
Generate Recovery Codes	If enabled, recovery codes are generated and stored in the successful outcome's transient state. Use the Recovery Code Display node to display the codes to the user for safekeeping. Default: true **Important** Generating recovery codes overwrites all existing push-specific recovery codes. Only the most recent set of recovery codes can be used for authentication if a device has been lost or stolen.

Property	Usage
QR code message	A custom, localized message with instructions to scan the QR code to register the device. 1. Click **Add**. 2. Enter the message locale in the **Key** field; for example, `en-gb`. 3. Enter the message to display to the user in the **Value** field. Default: none
Registration Response Timeout	The period of time (in seconds) to wait for a response to the registration QR code. If no response is received during this time, evaluation continues along the `Time Out` outcome path. Default: `60`
One Time Password Length	The length of the generated OTP in digits. This value must be at least `6` and compatible with the hardware/software OTP generators you expect end users to use. For example, Google and ForgeRock authenticators support values of `6` and `8`, respectively. Default: `6`
Minimum Secret Key Length	Minimum number of hexadecimal characters allowed for the Secret Key. Default: `32`
OATH Algorithm	The algorithm the device uses to generate the OTP: ***HOTP*** HOTP uses a counter; the counter increments every time a new OTP is generated. When you use this setting, also set the same value in the OATH Token Verifier node. ***TOTP*** TOTP generates a new OTP every few seconds as specified by the `TOTP Time Step Interval` setting. Default: `TOTP`
TOTP Time Step Interval (`totpTimeInterval`)	The length of time that an OTP is valid in seconds. For example, if the time step interval is 30 seconds, a new OTP is generated every 30 seconds and is valid for 30 seconds only. Default: `30` seconds
TOTP Hash Algorithm	The HMAC hash algorithm used to generate the OTP codes. AM supports SHA1, SHA256, and SHA512. Default: `SHA1`
HOTP Checksum Digit	Add a digit to the end of the generated OTP to be used as a checksum to verify the OTP was generated correctly. This is in addition to the actual password length. Only set this if the user devices support it. Default: false

Property	Usage
HOTP Truncation Offset	An option used by the HOTP algorithm that not all devices support. Leave the default value unless you know user devices use an offset. Default: `-1`

JSON Authenticator Policies	Policies to apply to the device being registered, in JSON format. Use the following format to apply policies:
	`{ "[.var]#policyName#" : { "[.var]#policyParameters#" | [.label]#value# } }`
	Supported policies
	The ForgeRock Authenticator app supports enforcement of the following default policies:
	`biometricAvailable`
	Parameters: None
	The device must have a biometric sensor available and enabled in the operating system.
	`deviceTampering`
	Parameters: `score`
	The device must not have been tampered with; for example have root access or be jailbroken.
	This policy applies if the score returned by the device exceeds the provided `score` parameter, which is a number between `0` and `1.0`.
	Example:
	`{ "biometricAvailable": { }, "deviceTampering": { "score": 0.8 } }`

Outputs

- For Push registration, this node updates the shared state with the push device settings, the message ID, and the push challenge.
- For OATH registration, this node records the device profile in the `oathDeviceProfile` shared state attribute and the recovery codes in the `oathEnableRecoveryCode` shared state attribute.

Outcomes

Success

Device registration succeeded.

Failure

AM encountered an issue when attempting to register the authentication device.

Time Out

The node didn't receive a response from the device within the time specified in the configuration.

Errors

No username found

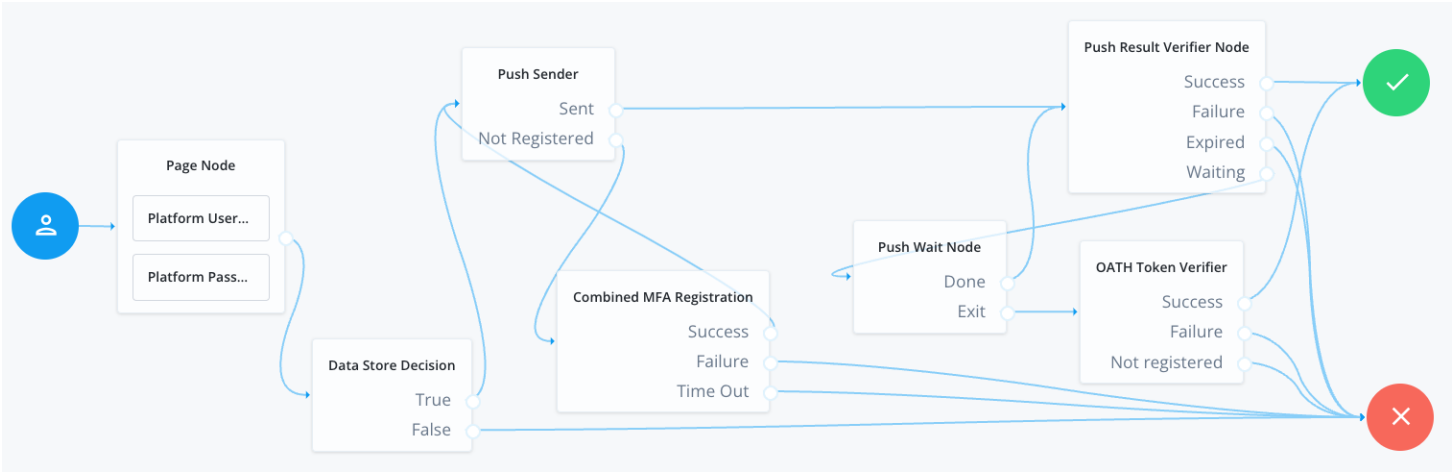
The node failed to read the username from the shared state.

Unable to find push message ID in sharedState

The node failed to read the push message ID from the shared state.

Examples

The following example shows an implementation of combined multi-factor registration in an authentication journey:



- The Page node with the Platform Username node and the Platform Password node prompts for the user credentials.
- The Data Store Decision node confirms the username-password credentials.
- The Push Sender node determines whether the user has a registered device.
    - If the user has a registered device:
        - The Push Sender node sends a push notification to the device.

- The Push Result Verifier node validate the user's response to the push notification, looping through the Push Wait node until authentication succeeds.
- The Push Wait node lets the user cancel the wait for a push notification. In this case evaluation continues to the OATH Token Verifier node, so the user can enter a one-time password instead.

- If the user **doesn't** have a registered device:
  - The Push Sender node routes the user to the Combined MFA Registration node, which displays a QR code to the user to register a device.
  - After successful registration of a device for both push and OATH authentication, evaluation returns to the Push Sender node and continues with the registered device.

Device Binding node

Allows users to register one or more devices to their account. A user can bind multiple devices, and each device can be bound to multiple users.

There are many similarities between WebAuthn and device binding and JWS verification. We provide authentication nodes to implement both technologies in your journeys.

Both can be used for usernameless and passwordless authentication, they both use public key cryptography, and both can be used as part of a multi-factor authentication journey.

One major difference is that with device binding, the private key never leaves the device.

With WebAuthn, there is a possibility that the private key is synchronized across client devices because of Passkey support, which may be undesirable for your organization.

For details of the differences, refer to the following table:

Comparison of WebAuthn and Device Binding/JWS Verification

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Industry-standards based	☑	×	You can refer to the WebAuthn W3C specification. Device binding and JWS verification are proprietary implementations.
Public key cryptography	☑	☑	Both methods use Public key cryptography.
Usernameless support	☑	☑	After registration, the username can be stored in the device and obtained during authentication without the user having to enter their credentials.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Keys are bound to the device	✕	☑	With WebAuthn, if Passkeys are used, they can be shared across devices. With device binding, the private keys do not leave the device.
Sign custom data	✕	☑	With device binding, you can: • Customize the challenge that the device must sign. For example, you could include details of a transaction, such as the amount in dollars. • Add custom claims to the payload when signing a challenge. This gives additional context that the server can make use of by using a scripted node. Refer to Add custom claims when signing.
Format of signed data	WebAuthn authenticator data	JSON Web Signature (JWS)	
Integration	✕	☑	With device binding, after verification, the signed JWT is available in: • Audit Logs • Transient node state This enables the data within to be used for integration into your processes and business logic.
Platform support	☑ Android ☑ iOS ☑ Web browsers	☑ Android ☑ iOS ✕ Web browsers	As it is challenging to store secure data in a browser as a client app, device binding is not supported in web browsers.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Authenticator support	Determined by the platform. Configuration limited to: • Biometric with Fallback to Device Pin	Determined by the authentication node. Full configuration options: • Biometric Authentication • Biometric with Fallback to Device Pin • Application Pin • Silent	With device binding, you can specify what authentication action the user must perform to get access to the private keys. This provides greater flexibility in your security implementation and can reduce authentication friction for your users.
Key storage	Web browsers and iOS synchronize to the cloud. Android has the option to synchronize to the cloud.	***Android*** KeyStore ***iOS*** Secure enclave: hardware-backed and not synchronized to the cloud.	Both technologies store the private keys securely on the client. WebAuthn supports synchronizing the private keys to the cloud for use on other devices. This can reduce authentication friction for your users but may also increase the risk of a breach.
Managing device keys	Managed by the device OS. Apps cannot delete *local* client keys programmatically and do not have a reference to the *remote* server key for deletion.	Managed by the Ping SDKs. Provides an interface to delete local client and remote server keys.	The ability to programmatically delete both client and server keys can greatly simplify the process of registering a new device if an old device is lost or stolen.
Passkey support	☑	×	WebAuthn supports synchronizing the private keys to the cloud for use on other devices. Device binding keeps the private key locked in the device.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
App integrity verification	***Android*** Requires an `assetlinks.json` file. ***iOS*** Requires `apple-app-site-association` file.	Not provided by the device binding or verification nodes. It can be added as part of the journey by using app integrity nodes.	App integrity verification helps ensure your users are only using a supported app rather than a third-party or potentially malicious version.
Key attestation	***Android*** SafetyNet ***iOS*** None	***Android*** Uses hardware-backed key pairs with Key Attestation. ***iOS*** It can be added as part of the journey by using app integrity nodes to support key attestation.	Key attestation verifies that the private key is valid and correct, is not forged, and was not created in an insecure manner.
Complexity	Medium	Low	WebAuthn requires a bit more configuration, for example, creating and uploading the `assetlinks.json` and `apple-app-site-association` files. Device binding only requires the journey and the SDK built into your app.

You must ensure you authenticate the user and obtain their username in the journey before attempting to bind a device.

Registered devices share device data in the form of a public key and a key ID which AM stores in the user's profile, or you can save it in transient state for processing.

The private key of the keypair is kept safely on the device and secured with biometric security or a PIN.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Dependencies

You can verify possession of bound devices by using the Device Signing Verifier node.

You can save the device data to the user's profile by using the Device Binding Storage node.

To use Android Key Attestation, you must also configure the Android Key Attestation Service.

Configuration

Property	Usage
Authentication Type	Specifies how the device should secure access to the private key. The available options are: **`Biometric only`** Request that the client secures access to the cryptography keys with biometric security, such as a fingerprint. **`Biometric with PIN fallback`** Request that the client secures access to the cryptography keys with biometric security, such as a fingerprint, but allow use of a PIN if biometric is unavailable. **`Application PIN`** Request that the client secures access to the cryptography keys with an application-specific PIN. **Important** The PIN is not linked to the user's device PIN and is stored only on the client device. The PIN is not sent to AM, so if the user forgets their PIN, they must bind the device again. **None** Allow the client device to create the cryptography keys without securing access to them.
Application IDs	Specifies a list of Android package names and iOS bundle IDs of applications that are allowed to perform device binding. For example, `com.example.app`.
Title	Specifies a title to display to the user when asking them to bind the device.

Property	Usage
Sub Title	Specifies a subtitle to display to the user when asking them to bind the device.
Description	Specifies descriptive text to display to the user when asking them to bind the device.
Maximum Saved Devices	Specifies the maximum number of devices stored in the user's profile. Set this property to `0` if you do not want to limit the number of devices. When this property is greater than zero, the `Exceed Device Limit` outcome path becomes available.
Timeout	Specify the number of seconds to wait for a response from the client during binding. If the specified time is reached, evaluation continues along the `Timeout` outcome path.
Android Key Attestation	Use Android key attestation to increase confidence that the keys used by the bound device are valid, haven't been revoked, and use hardware-backed security storage. The attestation data is also stored in the transient state of the tree, in a variable named `DeviceBindingCallback.ATTESTATION`, so that you can access and parse the data in a scripted node if required. You can find information on the contents of the attestation data JSON response in Attestation certificate in the Android documentation.

Property	Usage

Store Device Data in Transient State	If enabled, the node *does not save* device data in the user's profile when it completes successfully.
	Instead, the node places the device information into the transient state in a variable named `DeviceBindingNode.DEVICE`. This allows subsequent nodes to use, parse, or alter the information before saving it.
	Use the Device Binding Storage node to save the device data to the user's profile.
	Example device data
	{
	"uuid": "0ea44aa7-ef55-431b-885b-8c3a87e93331",
	"recoveryCodes": [],
	"deviceName": "Pixel 7 Pro",
	"deviceId":
	"aaddfecd9b8b3e2a-153cae31c23bc51a8db6d71bc3a31423a6aca97d",
	"createdDate": 1694787036658,
	"lastAccessDate": 1694787036658,
	"key": {
	"kty": "RSA",
	"kid": "0ea44aa7-ef55-431b-885b-8c3a87e93331",
	"use": "sig",
	"alg": "RS512",
	"n": "n7nn76rmgcOGfuVm8N-wur4GgWW-
	Iek0edwcQR865L3sjKON3XUCHi210tqMyc-PWlCaY-
	dHisyy7TxK0jn4poui_aK3lnGYNzJpuyTU1-
	sunSTRVMW8vDTEJxUNQMZFS086_8hVFiC9OnElkpFllp2jzfgZ7u318bdVMgib2bHlscyMo8
	CZEwA_MHKteIkSD7CZIHMjm-
	JlJIrKlaLIJ3lkZTUG29g2J9LvdGTMXyt206ZLQw3kAQ_QczHpiKieAiLd9sHydjB7BqGpgC
	xjCkmqVi4BEvMl8sEEFnpZG1NzjrCBnGfSWr83dzenr6tbdCh5iew-BIdDXXaDPOXRew",
	"e": "AQAB"
	}
	}

Android key attestation

When binding a device running Android N (`24`) or newer, you can use Android key attestation to increase confidence that the keys used by the bound device are valid, have not been revoked, and use hardware-backed security storage.

The Ping SDK for Android generates attestation data for the cryptographic keys it uses for device binding. Using information provided by Google, including a certificate revocation status list (CRL) and hardware attestation root certificate, the node can verify that the certificates are trustworthy.

If you enable the **Android key attestation** property and the device is running an earlier Android version, evaluation continues down the `Unsupported` outcome path.

Android key attestation *is not* supported if you select `Application PIN` in the **Authentication Type** property. Evaluation continues down the `Unsupported` outcome path in this case.

The node does not attempt attestation when binding non-Android devices.

Outputs

If you enable the **Android Key Attestation** property, the node outputs attestation data in a variable named `DeviceBindingCallback.ATTESTATION`.

If you enable the **Store Device Data in Transient State** property, the node outputs device data in a variable named `DeviceBindingNode.DEVICE`.

Outcomes

- `Success`
- `Failure`
- `Exceed Device Limit`
- `Unsupported` (Client)
- `Abort` (Client)
- `Timeout` (Client)

If the user successfully binds their device, evaluation continues along the `Success` outcome path.

If AM encounters an issue when attempting to register using a device, evaluation continues along the `Failure` outcome path.

If the **Maximum Saved Devices** property is set to an integer greater than zero, and binding a new device would take the number of devices above the specified threshold, then evaluation continues down the `Exceed Device Limit` outcome path. In this case, you need to instruct your users to log in with an existing bound device in order to remove one or more of their registered devices.

If the user's client does not support the requested operation, evaluation continues along the `Unsupported` outcome path. For example, the node is configured to require biometric authentication, but the device does not provide support.

If the user cancels the attempt to bind a device, evaluation continues along the `Abort` outcome path.

If the node does not receive a response from the user's device within the **Timeout** specified in the node configuration, evaluation continues along the `Timeout` outcome path.

Device Binding Storage node

Persists collected device binding data to a user's profile in the identity store.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes

Product	Available?
Ping Identity Platform (self-managed)	Yes

Inputs

The node uses the variable named `DeviceBindingNode.DEVICE` as input from the state.

The node requires that a Device Binding node has gathered device data previously in the journey.

Outcomes

`True`

Device binding data was successfully stored in the user's profile.

`False`

Device binding data was not stored in the user's profile.

Properties

None.

Device Signing Verifier node

Verifies possession of a registered bound device.

There are many similarities between WebAuthn and device binding and JWS verification. We provide authentication nodes to implement both technologies in your journeys.

Both can be used for usernameless and passwordless authentication, they both use public key cryptography, and both can be used as part of a multi-factor authentication journey.

One major difference is that with device binding, the private key never leaves the device.

With WebAuthn, there is a possibility that the private key is synchronized across client devices because of Passkey support, which may be undesirable for your organization.

For details of the differences, refer to the following table:

Comparison of WebAuthn and Device Binding/JWS Verification

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Industry-standards based	☑	×	You can refer to the WebAuthn W3C specification. Device binding and JWS verification are proprietary implementations.
Public key cryptography	☑	☑	Both methods use Public key cryptography.
Usernameless support	☑	☑	After registration, the username can be stored in the device and obtained during authentication without the user having to enter their credentials.
Keys are bound to the device	×	☑	With WebAuthn, if Passkeys are used, they can be shared across devices. With device binding, the private keys do not leave the device.
Sign custom data	×	☑	With device binding, you can: • Customize the challenge that the device must sign. For example, you could include details of a transaction, such as the amount in dollars. • Add custom claims to the payload when signing a challenge. This gives additional context that the server can make use of by using a scripted node. Refer to Add custom claims when signing.
Format of signed data	WebAuthn authenticator data	JSON Web Signature (JWS)	
Integration	×	☑	With device binding, after verification, the signed JWT is available in: • Audit Logs • Transient node state This enables the data within to be used for integration into your processes and business logic.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Platform support	☑ Android ☑ iOS ☑ Web browsers	☑ Android ☑ iOS ✕ Web browsers	As it is challenging to store secure data in a browser as a client app, device binding is not supported in web browsers.
Authenticator support	Determined by the platform. Configuration limited to: • Biometric with Fallback to Device Pin	Determined by the authentication node. Full configuration options: • Biometric Authentication • Biometric with Fallback to Device Pin • Application Pin • Silent	With device binding, you can specify what authentication action the user must perform to get access to the private keys. This provides greater flexibility in your security implementation and can reduce authentication friction for your users.
Key storage	Web browsers and iOS synchronize to the cloud. Android has the option to synchronize to the cloud.	***Android*** KeyStore ***iOS*** Secure enclave: hardware-backed and not synchronized to the cloud.	Both technologies store the private keys securely on the client. WebAuthn supports synchronizing the private keys to the cloud for use on other devices. This can reduce authentication friction for your users but may also increase the risk of a breach.
Managing device keys	Managed by the device OS. Apps cannot delete *local* client keys programmatically and do not have a reference to the *remote* server key for deletion.	Managed by the Ping SDKs. Provides an interface to delete local client and remote server keys.	The ability to programmatically delete both client and server keys can greatly simplify the process of registering a new device if an old device is lost or stolen.
Passkey support	☑	✕	WebAuthn supports synchronizing the private keys to the cloud for use on other devices. Device binding keeps the private key locked in the device.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
App integrity verification	***Android*** Requires an `assetlinks.json` file. ***iOS*** Requires `apple-app-site-association` file.	Not provided by the device binding or verification nodes. It can be added as part of the journey by using app integrity nodes.	App integrity verification helps ensure your users are only using a supported app rather than a third-party or potentially malicious version.
Key attestation	***Android*** SafetyNet ***iOS*** None	***Android*** Uses hardware-backed key pairs with Key Attestation. ***iOS*** It can be added as part of the journey by using app integrity nodes to support key attestation.	Key attestation verifies that the private key is valid and correct, is not forged, and was not created in an insecure manner.
Complexity	Medium	Low	WebAuthn requires a bit more configuration, for example, creating and uploading the `assetlinks.json` and `apple-app-site-association` files. Device binding only requires the journey and the SDK built into your app.

The node requires the device to sign a challenge string using the private key that corresponds to a stored public key.

The user might need to unlock their cryptography keys with biometric security — such as a fingerprint — or a PIN.

Note

This node can be used in usernameless authentication flows.
The Ping SDKs store and provide the identity when handling the callbacks from this node. If the device has been registered by more than one user, the SDK displays a list of the registered keys to choose from on the client device.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

If you want the device to sign a custom challenge, its value must be available in shared state. Enter the variable name in the **Shared state attribute for Challenge** property.

Dependencies

This node requires that you have bound devices by using the Device Binding node.

Configuration

Property	Usage
Sign Random Challenge	Use a random value as the challenge for signing.
Shared state attribute for Challenge	Use the value from the named attribute in shared state as the challenge for signing.
Application IDs	A list of Android package names and iOS bundle IDs of applications allowed to perform device signing verification. For example, `com.example.app`.
Title	A title to display to the user when asking them to bind the device.
Sub Title	A secondary or subtitle to display to the user when asking them to bind the device.
Description	Descriptive text displayed to the user when asking them to bind the device.

Property	Usage
Capture Failure	When enabled, adds the reason for a failure to the shared node state variable `DeviceSigningVerifierNode.FAILURE` and continues evaluation along the "Failure" outcome. If not enabled, the journey halts with an exception, and the journey *does not* continue along an outcome path. Reasons for failure include: **`INVALID_CLAIM`** Failed to validate one or more claims presented in the token. For example, the challenge claim did not match the value set in the node configuration, or the issuer (`ISS`) claim did not match a value in the **Application IDs** list. **`INVALID_SIGNATURE`** Failed to validate the token signature. **`INVALID_USER`** Account does not exist. **`NOT_ACTIVE_USER`** Account is not active or locked out. **`INVALID_SUBJECT`** Failed to validate the token subject.
Timeout	Specify the number of seconds to wait for a response from the client during binding. If the specified time is reached, evaluation continues along the `Timeout` outcome path.

Outputs

If you enable the **Capture Failure** property, the node outputs a failure reason string in a variable named `DeviceSigningVerifierNode.FAILURE` .

Outcomes

- `Success`
- `Failure`
- `No Registered Device`
- `Key Not Found`
- `Unsupported` (Client)
- `Abort` (Client)
- `Timeout` (Client)
- `ClientNotRegistered` (Client)

If the response from the device is verified as coming from a bound device, evaluation continues along the `Success` outcome path.

If AM cannot verify that the response was signed by a bound device, evaluation continues along the `Failure` outcome path.

If the user does not have any bound devices, evaluation continues along the `No Registered Device` outcome path. The user is determined either previously in the authentication journey, or by reading the `sub` claim from the response when doing usernameless flows.

If the client device cannot access the cryptography keys, or the key ID that AM requested cannot be located, evaluation continues along the relevant `Key Not Found` outcome path.

If the user's client does not support the requested operation, evaluation continues along the `Unsupported` outcome path.

If the user cancels authentication, evaluation continues along the `Abort` outcome path.

If the node does not receive a response from the user's device within the **Timeout** specified in the node configuration, evaluation continues along the `Timeout` outcome path.

If the client device does not have the keys present to be able to sign the challenge, evaluation continues along the `ClientNotRegistered` outcome path.

Enable Device Management node

The **Enable Device Management** node controls the restrictions placed on users who want to reset or remove registered multi-factor authentication (MFA) devices.

By default, authenticated users can only remove a registered MFA device if they have authenticated by using a matching device. For example, to delete a device registered for OATH, they must have successfully authenticated by using a journey that includes an OATH Token Verifier node.

You can use this node in a journey to relax or remove this restriction.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Device Check Enforcement Strategy	The MFA authentication method that is required to allow users to remove registered devices. Choose from: **SAME** The user must have authenticated with the same MFA type (WebAuthn, OATH, Device Binding, or PUSH) as the device they want to delete. This matches the default behavior, as if this node were not used. **ANY** The user must have authenticated with any MFA type (WebAuthn, OATH, Device Binding, or PUSH) to be able to delete a device. **NONE** The user does not have to authenticate using WebAuthn, OATH, Device Binding, or PUSH to be able to delete a device. **Caution** If you use this option, ensure you authenticate the user as strongly as possible before allowing them to delete a device. The default is `SAME`.

Outputs

This node adds a flag to the auth session the journey creates, depending on the **Device Check Enforcement Strategy** property.

The flag determines which MFA device types, if any, the user can delete.

Outcomes

Success

Any of the following situations result in the **Success** outcome from this node:

- The **Device Check Enforcement Strategy** is set to `SAME`.

  This setting relies on existing behavior to update the auth session and makes no changes of its own.

- The **Device Check Enforcement Strategy** is set to `ANY`, and at least one MFA type was used previously in the journey.

- The **Device Check Enforcement Strategy** is set to `NONE`, and the node was able to update the auth session.

`Failure`

Any of the following situations result in the **Failure** outcome from this node:

- The `username` property of the identity is not available.
- The user is marked as inactive.
- The **Device Check Enforcement Strategy** is set to `ANY`, but the authentication journey didn't perform MFA.
- The node attempted to update the auth session but did not succeed.

Errors

This node does not output any user-facing error messages.

Example

The following example journey allows users to reset their registered MFA devices without having to authenticate using MFA.

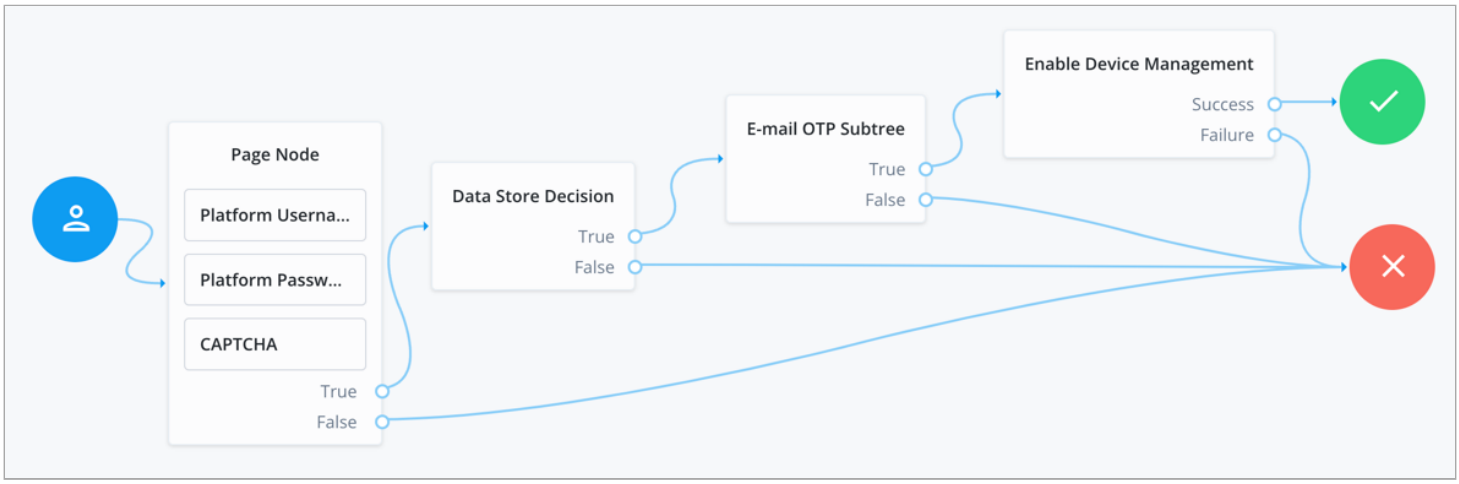


Figure 1. Example Enable Device Management journey

- The user enters their credentials, completes the CAPTCHA, and is verified against the identity store.
- A subtree sends a one-time passcode (OTP) to the user's email address to verify they have access to the address they have in their profile.
- The **Enable Device Management** node, with the **Device Check Enforcement Strategy** property set to `NONE`, upgrades the session the user receives to allow them to delete any of their registered MFA devices.

Get Authenticator App node

The **Get Authenticator App** node displays information to get an authenticator app from the Apple App Store or the Google Play Store.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None. This node doesn't read shared state data.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Get App Authenticator Message	(Optional) Add a custom, localized message to display to the user. You can use the following variables to customize the message: • `{{appleLink}}` • `{{appleLabel}}` • `{{googleLink}}` • `{{googleLabel}}` You can also include HTML elements, for example: `Apple: <a target='_blank' href='{{appleLink}}'>{{appleLabel}}</a>` 1. Click **+**. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Get the app from the {{appleLink}} or on {{googleLink}}.`

Property	Usage
Continue Label	(Optional) Add custom, localized text to display on the button the user can click to continue. 1. Click **+**. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Continue`
Apple App Store URL	The URL to download your authenticator app from the Apple App Store. The default value points to the ForgeRock Authenticator app for iOS. Default: `https://itunes.apple.com/app/forgerock-authenticator/id1038442926`
Google Play URL	The URL to download your authenticator app from the Google Play Store. The default value points to the ForgeRock Authenticator app for Android. Default: `https://play.google.com/store/apps/details?id=com.forgerock.authenticator`

[1] Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

[2] PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Outputs

This node doesn't change the shared state.

Outcomes

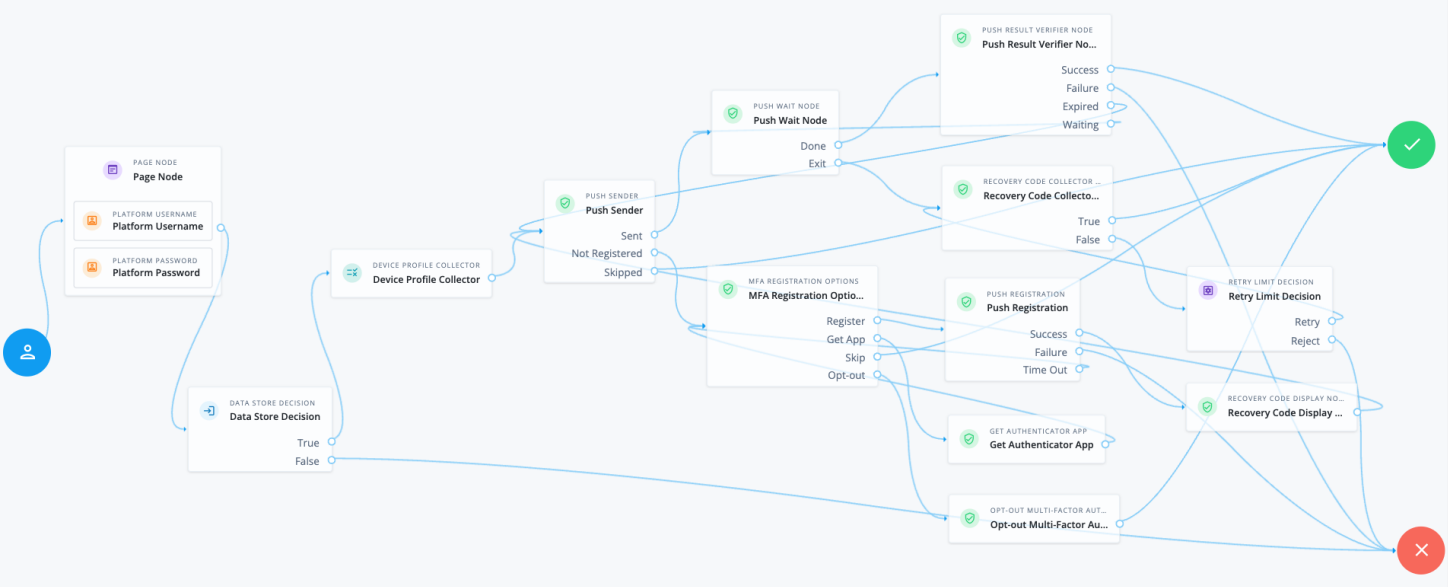
Single outcome path.

Errors

This node doesn't log any error or warning messages of its own.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

HOTP Generator node

Creates a string of random digits of the specified length for use as a one-time passcode.

Passwords are stored in the `oneTimePassword` transient node state property.

Use this node with these nodes to add one-time passcode verification as an additional factor:

- OTP Email Sender node
- OTP SMS Sender node
- OTP Collector Decision node

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

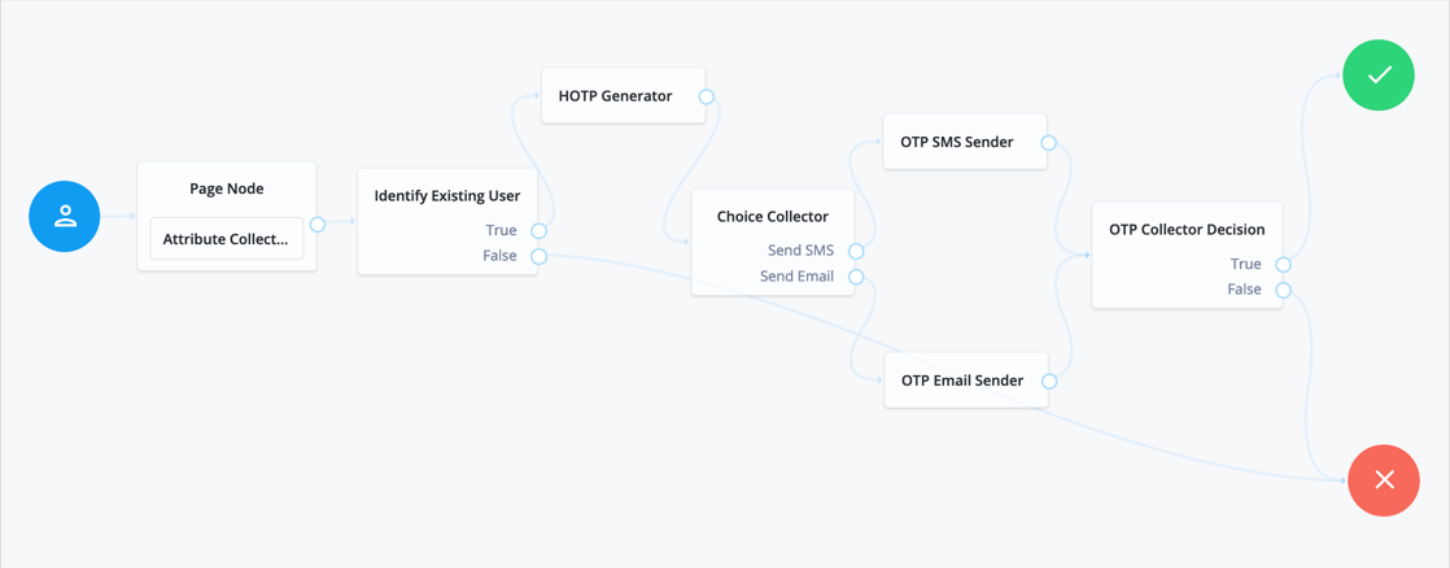
Single outcome path.

Properties

Property	Usage
One-time password length	Specify the number of digits in the one-time passcode. The minimum number of digits is 6, in accordance with the HOTP specification. Default: 8

Example

The following example uses an HOTP generator as part of multi-factor authentication:



MFA Registration Options node

The **MFA Registration Options** node lets the user register a multi-factor authentication (MFA) device or skip the registration process.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

- This node requires a `username` in the incoming node state to identify which user to update.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

- This node requires the `mfaMethod` in the incoming state to know what type of MFA device to register:
  - For push authentication, this node requires the `pushMessageId` in the incoming state, which is a unique ID to identify the push notification request.

    Implement a Push Sender node earlier in the journey.

- For OATH authentication, implement the OATH Token Verifier node earlier in the journey.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Remove 'skip' option	Select this option to make it mandatory for the user to register a device. When selected, the **Skip this Step** and **Opt-out** buttons aren't displayed. When disabled, the user can skip device registration or opt-out if required.
Display Get Authenticator App	Select this option to display the **Get the App** button.
Message	(Optional) Add a custom, localized message to display to the user with instructions on interacting with this node: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.(1) 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.(2) Default: `On this page you can choose to register, skip or opt-out the second factor authentication method selected to protect your account. If you "Skip", an MFA method will not be registered now, but you will be prompted again on your next login. Otherwise, if you "Opt out", an MFA method will not be registered now and you will not be asked again. This choice is not recommended.`
Register Device	(Optional) Add custom, localized text to display on the button the user can click to register their device: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.(1) 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.(2) Default: `Register Device`

Property	Usage
Get Authenticator App	(Optional) Add custom, localized text to display on the button the user can click to get the authenticator app: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Get the App`
Skip this Step	(Optional) Add custom, localized text to display on the button the user can click to skip registering their device: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Skip this step`
Opt-out	(Optional) Add custom, localized text to display on the button the user can click to opt out of registering their device: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Opt-out` **Note** This node doesn't update the user's profile with the opt-out decision. Use the **Opt-out** outcome in an Opt-out Multi-Factor Authentication node to persist the decision in the user's profile.

[1] Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

[2] PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Outputs

This node doesn't change the shared state.

Outcomes

`Register`

The user chooses to register an MFA device.

`Get App`

The user chooses to get the authenticator app.

`Skip`

The user chooses to skip registering an MFA device this time.

`Opt-out`

The user chooses to opt-out of registering an MFA device.

Errors

The node can log the following errors:

- `Expected username to be set`

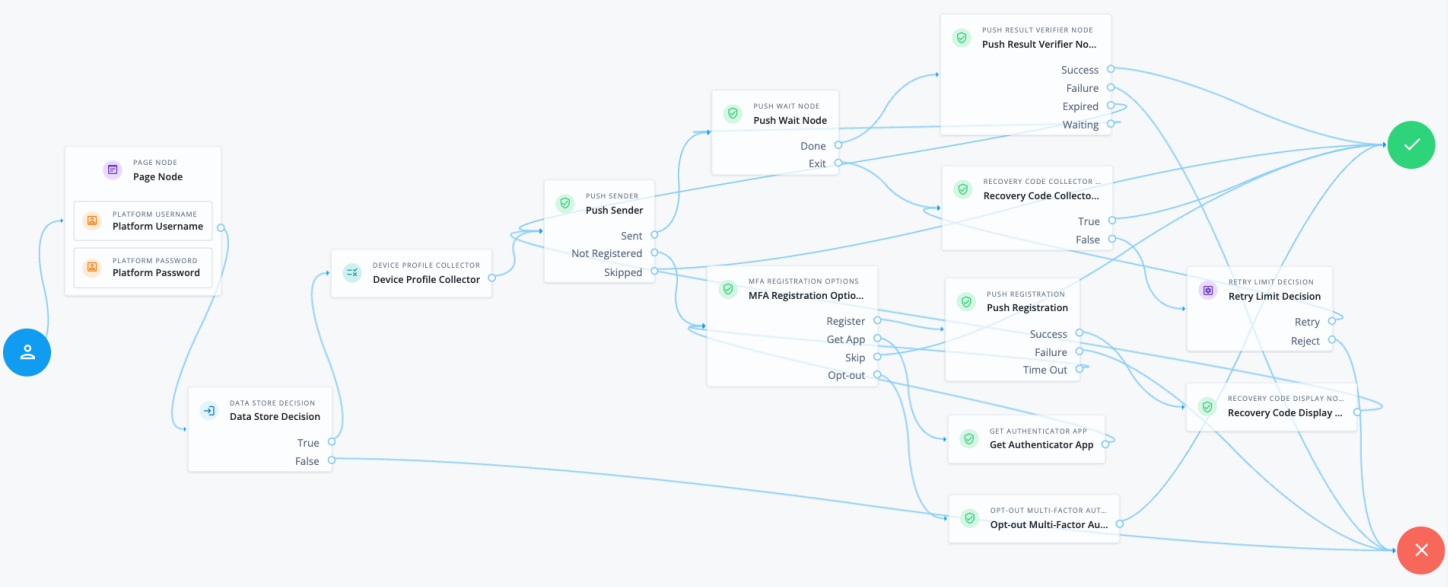
  The node can't identify the user from the shared state.

- `Expected multi-factor authentication method to be set`

  The node can't identify the MFA method from the shared state.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

OATH Device Storage node

The **OATH Device Storage** node stores devices in the user profile after an OATH Registration node records them in the shared state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The OATH-related nodes can integrate with the following authenticator apps:

- The ForgeRock Authenticator app for Android and iOS.
- Third-party authenticator apps that support the following open standards:
  - RFC 4226: HMAC-Based One-Time Password (HOTP)
  - RFC 6238: Time-Based One-Time Password (TOTP)

Inputs

This node reads the device profile as the value of the shared state attribute `oathDeviceProfile`.

Dependencies

Precede this node in the flow with an OATH Registration node with its **Store device data in shared state** setting enabled.

Configuration

This node has no configurable properties.

Outputs

This node doesn't change the shared state.

Outcomes

Success

The node wrote the device profile to the user's account.

`Failure`

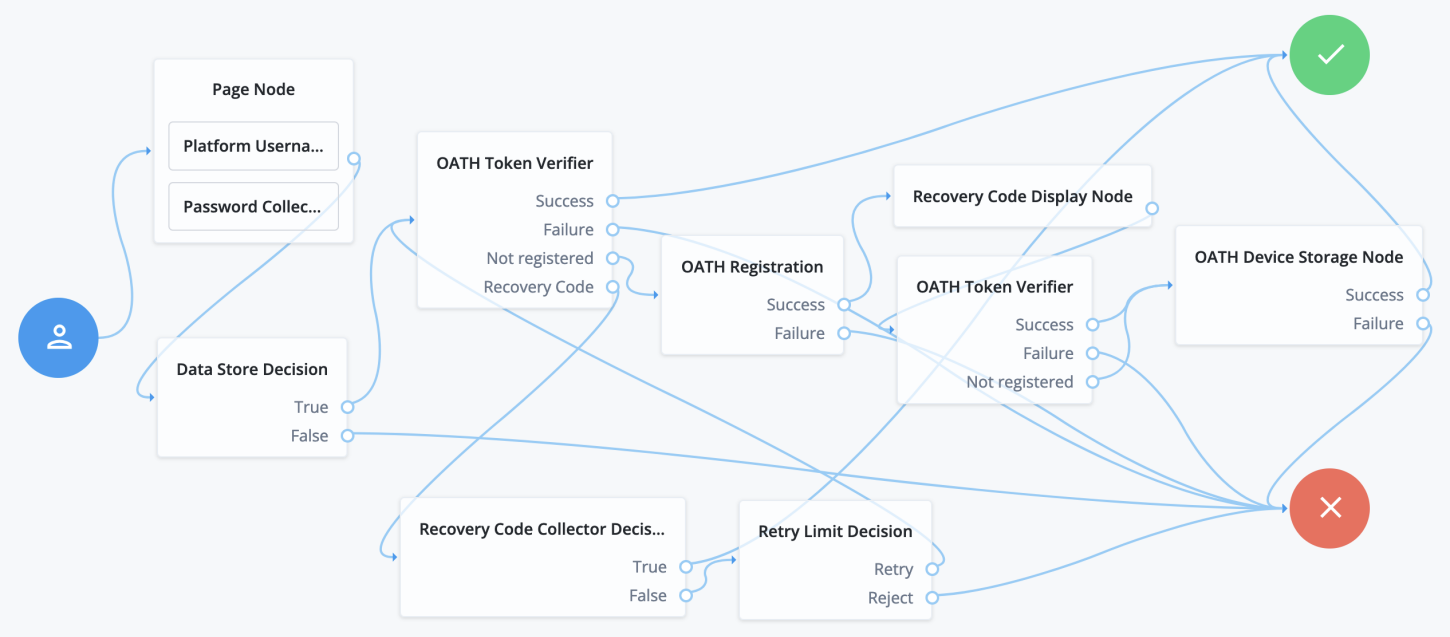
Any other case.

Errors

This node logs a `No device profile found on shared state` error message if it can't get the device profile from the `oathDeviceProfile` shared state attribute.

Example

The following journey includes both username-password and one-time passcode authentication:



- The Page node with the Platform Username node and the Platform Password node prompts for the user credentials.
- The Data Store Decision node confirms the username-password credentials.
- The first OATH Token Verifier node prompts for a one-time passcode with an option to use a recovery code.
- The OATH Registration node prompts the user to register a device and includes its profile in the shared state.
- The Recovery Code Display node shows the recovery codes and prompts the user to keep them safe.

- The second OATH Token Verifier node prompts for a one-time passcode using the newly registered device.
- The OATH Device Storage node writes the device profile to the user's account.
- The Recovery Code Collector Decision node prompts for a recovery code.
- The Retry Limit Decision node lets the user retry another code if they enter one incorrectly.

OATH Registration node

The **OATH Registration** node lets the user register a device for OATH-based multi-factor authentication (MFA).

Based on the node settings, the user device displays a QR code that includes all the details required for registration. If registration is successful, the node stores the device data, and recovery codes (if enabled), and sets the `skippable` attribute to prevent repeat registration at next login.

> **Tip**
>
> You can use the Combined MFA Registration node to register a device for both push notifications and one-time passcode (OATH) verification in a single step.
> Refer to the OATH Token Verifier node example that demonstrates how use to use other MFA nodes to create a complete OATH authentication journey.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The OATH-related nodes can integrate with the following authenticator apps:

- The ForgeRock Authenticator app for Android and iOS.
- Third-party authenticator apps that support the following open standards:
  - RFC 4226: HMAC-Based One-Time Password (HOTP)
  - RFC 6238: Time-Based One-Time Password (TOTP)

Inputs

This node reads the `username` attribute and optionally the `oathDeviceProfile` attribute from the shared state.

Dependencies

Confirm the user credentials before letting them register a device. For example, precede this node with the following nodes earlier in the authentication flow:

- Username Collector node (standalone AM) or Platform Username node (Ping Identity Platform deployment)
- Password Collector node (standalone AM) or Platform Password node (Ping Identity Platform deployment)
- Data Store Decision node

Properties

Property	Usage
Issuer	Specify an identifier to appear on the user's device, such as a company name, a website, or a realm. The authenticator application displays the value. Default: `ForgeRock`
Account Name	Select the profile attribute to display as the username in the authenticator application. If not specified, or if the specified profile attribute is empty, their username is used. Default: **Username**
Background Color	The background color in hex notation that displays behind the issuer's logo within the authenticator application. Default: `032b75`
Logo Image URL	The location of an image to download and display as the issuer's logo within the authenticator application. **Note** The ForgeRock Authenticator supports logos in JPEG and PNG format only. The application resizes your logo automatically, but a maximum image size of one MByte (or 1024 X 1024 pixels) is recommended. Default: none
Generate Recovery Codes	If enabled, recovery codes are generated and stored in the successful outcome's transient state. Use the Recovery Code Display node to display the codes to the user for safekeeping. Default: true

Property	Usage
QR code message	A custom, localized message with instructions to scan the QR code to register the device. 1. Click **Add**. 2. Enter the message locale in the `Key` field. For example, `en-gb`. 3. Enter the message to display to the user in the `Value` field. Default: none
One Time Password Length	The length of the generated OTP in digits. This value must be at least `6`. It must also be compatible with the hardware/software OTP generators you expect end users to use. For example, Google and ForgeRock authenticators support values of `6` and `8` respectively. Default: `6`
Minimum Secret Key Length	Number of hexadecimal characters allowed for the secret key. Default: `32`
OATH Algorithm	Specify the algorithm the device uses to generate the OTP: ***HOTP*** HOTP uses a counter; the counter increments every time a new OTP is generated. When you use this setting, also set the same value in the OATH Token Verifier node. ***TOTP*** TOTP generates a new OTP every few seconds as specified by the **TOTP Time Step Interval** setting. Default: `TOTP`
TOTP Time Step Interval	The length of time that an OTP is valid in seconds. For example, if the time step interval is 30 seconds, a new OTP is generated every 30 seconds and is valid for 30 seconds only. Default: `30` seconds
TOTP Hash Algorithm	The HMAC hash algorithm used to generate the OTP codes. AM supports SHA1, SHA256, and SHA512. Default: `SHA1`
HOTP Checksum Digit	This adds a digit to the end of the OTP generated to be used as a checksum to verify the OTP was generated correctly. This is in addition to the actual password length. Only set this if the user devices support it. Default: false
HOTP Truncation Offset	This is an option used by the HOTP algorithm that not all devices support. Leave the default value unless you know user devices use an offset. Default: `-1`

Property	Usage

Store device data in shared state	If enabled, the device data isn't stored in the user profile on successful completion of the node. Instead, the node adds the device data as a base64-encoded string to the `oathDeviceProfile` property in the shared node state. This string is decoded as an unescaped plain string representation of a JSON object. For example:
	In the shared node state:
	`oathDeviceProfile="eyAidXVpZCI6ICJhNDhiMjUyMS0xYzliLTRiYTct...ja0RyaWZ0U2Vjb25kcyI6IDAgfQ"`
	Decoded value:
	`{ "uuid": "a48b2521-1c9b-4ba7-a45c-8dd855c7397c", "recoveryCodes": [], "sharedSecret": "0CF9910A24CAF84E81CEBA71C2086DE4", "deviceName": "OATH Device", "lastLogin": 0, "counter": 0, "checksumDigit": false, "truncationOffset": -1, "clockDriftSeconds": 0 }`
	Use the OATH Device Storage node to store the device data in the user profile instead.
	Default: false

Outputs

If the **Store device data in shared state** setting is enabled, this node records the device profile in the `oathDeviceProfile` shared state attribute.

If the **Generate Recovery Codes** setting is enabled, this node records the recovery codes in the `oathEnableRecoveryCode` shared state attribute.

Outcomes

Success

Device registration succeeded.

Failure

Any other case.

Errors

This node logs the following error messages:

`No username found.`

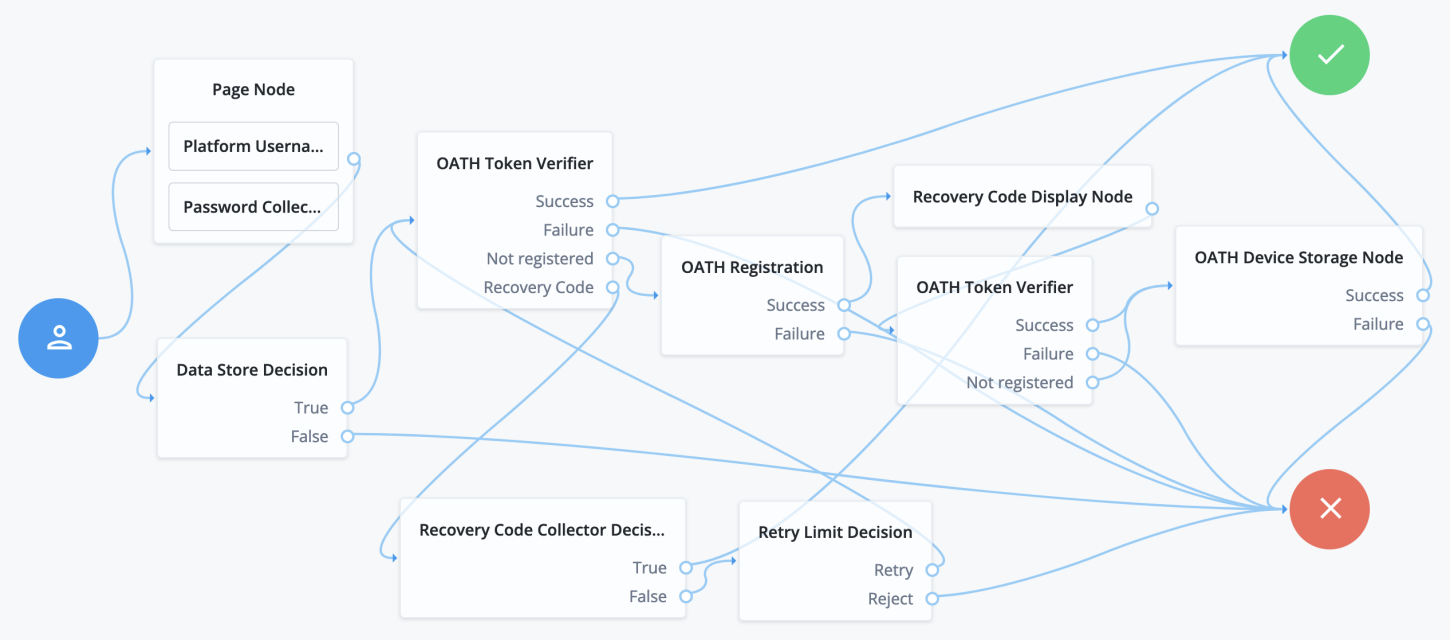
The node failed to read the username from the shared state.

`No device profile found on shared state`

The node failed to read the device profile from the shared state.

Example

The following journey includes both username-password and one-time passcode authentication:



- The Page node with the Platform Username node and the Platform Password node prompts for the user credentials.
- The Data Store Decision node confirms the username-password credentials.
- The first OATH Token Verifier node prompts for a one-time passcode with an option to use a recovery code.
- The OATH Registration node prompts the user to register a device and includes its profile in the shared state.
- The Recovery Code Display node shows the recovery codes and prompts the user to keep them safe.
- The second OATH Token Verifier node prompts for a one-time passcode using the newly registered device.
- The OATH Device Storage node writes the device profile to the user's account.
- The Recovery Code Collector Decision node prompts for a recovery code.
- The Retry Limit Decision node lets the user retry another code if they enter one incorrectly.

OATH Token Verifier node

The **OATH Token Verifier** node requests and verifies a one-time passcode (OTP) generated by a device such as a mobile phone.

The default configuration is time-based OTP (TOTP), but the node also supports HMAC (HOTP).

The node requires prior authentication and a device registered with an OATH Registration node.

> **Note**
>
> You can use the OATH nodes in conjunction with the ForgeRock Authenticator application to register your device, receive notifications, and generate one-time passwords.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The OATH-related nodes can integrate with the following authenticator apps:

- The ForgeRock Authenticator app for Android and iOS.
- Third-party authenticator apps that support the following open standards:
  - RFC 4226: HMAC-Based One-Time Password (HOTP)
  - RFC 6238: Time-Based One-Time Password (TOTP)

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

Dependencies

Confirm the user credentials before letting them authenticate with a device. For example, precede this node with the following nodes earlier in the authentication flow:

- Username Collector node (standalone AM) or Platform Username node (Ping Identity Platform deployment)
- Password Collector node (standalone AM) or Platform Password node (Ping Identity Platform deployment)
- Data Store Decision node

Configuration

Property	Usage
OATH Algorithm	Specify the algorithm the device uses to generate the OTP: ***HOTP*** HOTP uses a counter; the counter increments every time a new OTP is generated. When you use this setting, also set the same value in the OATH Registration node. ***TOTP*** TOTP generates a new OTP every few seconds as specified by the **TOTP Time Step Interval** setting. Default: `TOTP`
HOTP Window Size	Specify how much the OTP device and the server counter can be out of sync. For example, if the window size is 100 and the server's last successful login was at counter value 2, the server accepts an OTP that is generated between counter 3 and 102. Default: `100`
TOTP Time Step Interval	The length of time an OTP is valid in seconds. For example, if the time step interval is 30 seconds, a new OTP is generated every 30 seconds and is valid for 30 seconds only. Default: `30` seconds
TOTP Time Steps	Specify how many time steps the OTP can be out of sync. This applies to codes generated before or after the current code. For example, with a time step of 1, the server accepts the previous, current, and next codes. Default: `2`
TOTP Hash Algorithm	The HMAC hash algorithm used to generate the OTP codes. The ForgeRock Authenticator application supports SHA1, SHA256, and SHA512. Default: `SHA1`
TOTP Maximum Allowed Clock Drift	Specify how many time steps the authenticator application can be out of sync with the server before manual resynchronization is required. For example, with **TOTP Time Steps** of `3` and a **TOTP Time Step Interval** of 30 (seconds), the server treats codes up to 90 seconds from the current time as belonging to the current time step. The drift for a user's device is calculated each time they enter a new code. If the drift exceeds this value, the outcome is `Failure`. Default: `5`
Allow recovery codes	If enabled, lets users provide a recovery code to authenticate. Default: false

Outputs

If the outcome is `Not registered`, this node sets `"mfaMethod": "oath"` in the shared state.

Outcomes

Success

The user has a registered device and the token code was verified.

Failure

The user was not authenticated, or the collected token code can't be verified.

Not registered

The user account has no registered device profiles.

Recovery Code

Allow recovery codes is enabled, and the user chose to provide a recovery code.

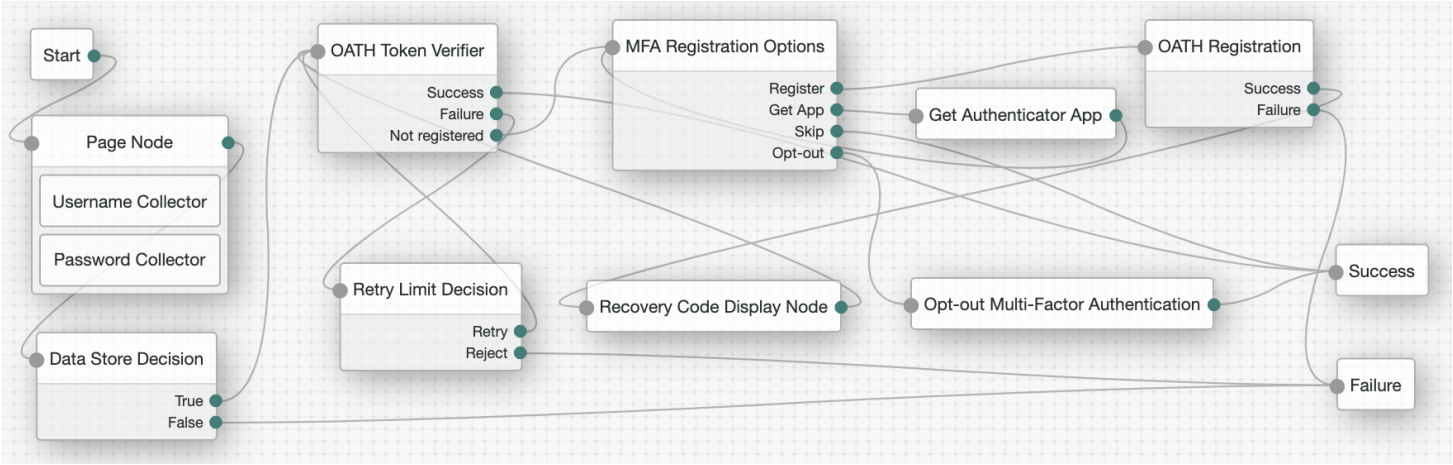
Errors

If this node cannot read the username from the shared state, it logs an error message: `Expected username to be set.`

If processing raises an exception, this node logs the detail as an error message.

Example

The following journey uses this node as part of a flexible multi-factor authentication (MFA) authentication flow:



- The Page node with the Username Collector node and the Password Collector node prompts for the user credentials.
- The Data Store Decision node confirms the username-password credentials.
- The OATH Token Verifier node prompts for a one-time passcode with an option to use a recovery code.

- The Retry Limit Decision node lets the user retry another code if they enter one incorrectly.
- The MFA Registration Options node lets the user choose how to register their device.
- The Get Authenticator App node helps the user install the ForgeRock Authenticator application.
- The OATH Registration node prompts the user to register a device and includes its profile in the shared state.
- The Recovery Code Display node shows the recovery codes and prompts the user to keep them safe.
- The Opt-out Multi-Factor Authentication node lets the user choose to skip the second authentication factor.

OTP Collector Decision node

Requests and verifies one-time passwords.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Evaluation continues along the `True` outcome path if the one-time passcode is valid; otherwise, evaluation continues along the `False` outcome path.

Properties

Property	Usage
One Time Password Validity Length	Specify the length of time, in minutes, that a one-time passcode remains valid. Default: `5`

OTP Email Sender node

The OTP Email Sender node sends an email containing a generated one-time passcode (OTP) to the user.

Send mail requests time out after 10 seconds.

Tip

You can change the timeout in the following advanced AM server properties:

- `org.forgerock.openam.smtp.system.connect.timeout`
- `org.forgerock.openam.smtp.system.socket.read.timeout`
- `org.forgerock.openam.smtp.system.socket.write.timeout`

- To configure advanced server properties for all the instances of the AM environment, go to **Configure > Server Defaults > Advanced** in the AM admin UI.
- To configure advanced server properties for a specific instance, go to **Deployment > Servers > *Server Name* > Advanced**.

If the property you want to add or edit is already configured, click the pencil (✎) button to edit it, then click the checkmark (✓) button.
Save your changes.
For more information, refer to advanced properties.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Prerequisites

- The node requires a configured email provider.

Inputs

This node requires the following input from the shared state:

- The authenticating user's ID. The node queries the user's entry for an email address.

  Implement an Attribute Collector node node before this node to obtain the user's ID.

- The OTP stored in the `oneTimePassword` transient state property.

  Implement the HOTP Generator node before this node in the journey to obtain the OTP.

Configuration

Property	Usage
Mail Server Host Name *(required)*	The hostname of the SMTP email server.
Mail Server Host Port	The outgoing mail server port. Common ports are 25, 465 for SSL/TLS, or 587 for StartTLS.
Mail Server Authentication Username	The username AM uses to connect to the mail server.
Mail Server Authentication Password	The password AM uses to connect to the mail server. **Note** This property is deprecated. Use the **Mail Server Secret Label Identifier** instead. If you set a **Mail Server Secret Label Identifier**, this password is ignored.
Mail Server Secret Label Identifier	An identifier used to create a *secret label* for mapping to a secret in a secret store. AM uses this identifier to create a specific secret label for this node. The secret label takes the form `am.authentication.nodes.otp.mail.identifier.password` where identifier is the value of **Mail Server Secret Label Identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period. If you set a **Mail Server Secret Label Identifier** and AM finds a matching secret in a secret store, the **Mail Server Authentication Password** is ignored.
Email From Address *(required)*	The email address from which the OTP will appear to have been sent.
Email Attribute Name	The attribute in the user profile that contains the email address to which the email with the OTP is sent. Default: `mail`
The subject of the email	Click **Add** to add a new email subject. Enter the locale, such as `en-uk`, in the **Key** field and the subject in the **Value** field. Repeat these steps for each locale that you support.
The content of the email	Click **Add** to add the content of the email. Enter the locale, such as `en-uk`, in the **Key** field and the email content in the **Value** field. Repeat these steps for each locale that you support.

Property	Usage
Mail Server Secure Connection	Set the connection method to the mail server. If you set a secure method here, AM must trust the server certificate of the mail server. The possible values for this property are: • `NON SSL/TLS` • `SSL/TLS` • `Start TLS` Default: `SSL/TLS`
Gateway Implementation Class	The class the node uses to send SMS and email messages. A custom class must implement the `com.sun.identity.authentication.modules.hotp.SMSGateway` interface. Default: `com.sun.identity.authentication.modules.hotp.DefaultSMSGatewayImpl`

Outputs

This node copies shared and transient state into the outgoing node state.

Errors

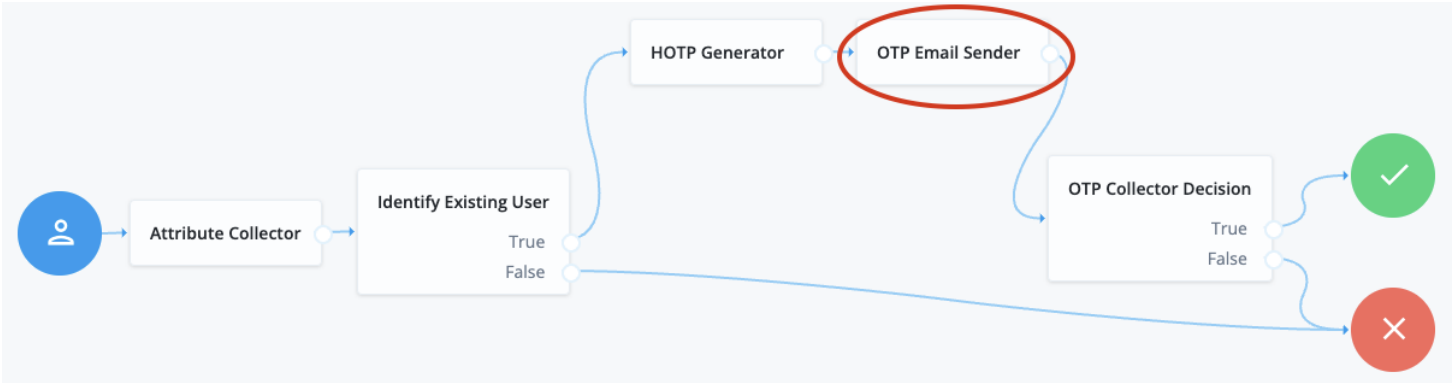
The node throws an `IdRepoException` and an `SSOException` error if it's unable to obtain the user's email address.

Outcomes

Single outcome path.

Implement an OTP Collector Decision node after this node to continue the authentication journey.

Example



OTP SMS Sender node

The OTP SMS Sender node uses an email-to-SMS gateway provider to send an SMS message containing a generated one-time password (OTP) to the user.

The node sends an email to an address formed by joining the following values together:

- The user's telephone number, obtained by querying a specified profile attribute, for example, `telephoneNumber`.
- The `@` character.
- The email-to-SMS gateway domain, obtained by querying the profile attribute specified by the **Mobile Carrier Attribute Name** property.

For example, if configured to use the *TextMagic* email-to-SMS service, the node might send an email through the specified SMTP server to the address: `18005550187@textmagic.com`.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Prerequisites

- The node requires a configured email-to-SMS gateway provider.

Inputs

This node requires the following input from the shared state:

- The authenticating user's ID. The node queries the user's entry for a telephone number.

  Implement an Attribute Collector node node before this node to obtain the user's ID.

- The OTP stored in the `oneTimePassword` transient state property.

  Implement the HOTP Generator node before this node in the journey to obtain the OTP.

Configuration

Property	Usage
Mail Server Host Name *(required)*	The hostname of the SMTP email server.

Property	Usage
Mail Server Host Port	The outgoing mail server port. Common ports are 25, 465 for SSL/TLS, or 587 for StartTLS.
Mail Server Authentication Username	The username AM uses to connect to the mail server.
Mail Server Authentication Password	The password AM uses to connect to the mail server. **Note** This property is deprecated. Use the **Mail Server Secret Label Identifier** instead. If you set a **Mail Server Secret Label Identifier**, this password is ignored.
Mail Server Secret Label Identifier	An identifier used to create a *secret label* for mapping to a secret in a secret store. AM uses this identifier to create a specific secret label for this node. The secret label takes the form `am.authentication.nodes.otp.sms.identifier.password` where identifier is the value of **Mail Server Secret Label Identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period. If you set a **Mail Server Secret Label Identifier** and AM finds a matching secret in a secret store, the **Mail Server Authentication Password** is ignored.
Email From Address *(required)*	The email address from which the OTP will appear to have been sent.
Mobile Phone Number Attribute Name	The attribute in the user profile that contains the mobile phone number to which the SMS with the OTP is sent. Default: `telephoneNumber`
Mobile Carrier Attribute Name	The attribute in the user profile that contains the mobile carrier domain for sending SMS messages. By default, an AM user profile doesn't have an attribute for the mobile carrier domain. You can customize the user profile by adding a new attribute to it, then populate that attribute with users' SMS messaging domains. All mobile carriers and bulk SMS messaging services have associated SMS messaging domains. For example, Verizon uses `vtext.com`, T-Mobile uses `tmomail.net`, and the TextMagic service uses `textmagic.com`. If you plan to send text messages internationally, determine whether the messaging service requires a country code. If you leave the **Mobile Carrier Attribute Name** property empty, AM defaults to sending SMS messages using `txt.att.net` for all users.
The subject of the message	Click **Add** to add a new message subject. Enter the locale, such as `en-uk`, in the **Key** field and the subject in the **Value** field. Repeat these steps for each locale that you support.

Property	Usage
The content of the message	Click **Add** to add the content of the message. Enter the locale, such as `en-uk`, in the **Key** field and the email content in the **Value** field. Repeat these steps for each locale that you support.
Mail Server Secure Connection	Set the connection method to the mail server. If you set a secure method here, AM must trust the server certificate of the mail server. The possible values for this property are: • `NON SSL/TLS` • `SSL/TLS` • `Start TLS` Default: `SSL/TLS`
Gateway Implementation Class	The class the node uses to send SMS and email messages. A custom class must implement the `com.sun.identity.authentication.modules.hotp.SMSGateway` interface. Default: `com.sun.identity.authentication.modules.hotp.DefaultSMSGatewayImpl`

Outputs

This node copies shared and transient state into the outgoing node state.

Errors

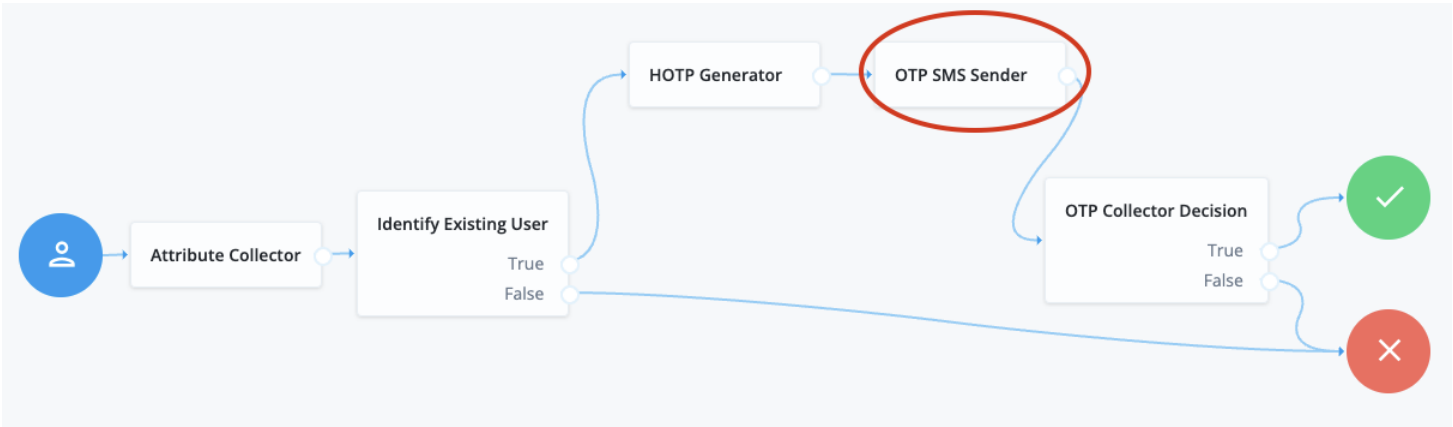
The node throws an `IdRepoException` and an `SSOException` error if it's unable to obtain the user's telephone number.

Outcomes

Single outcome path.

Implement an OTP Collector Decision node after this node to continue the authentication journey.

Example



Opt-out Multi-Factor Authentication node

The **Opt-out Multi-Factor Authentication** node sets an attribute in the user's profile, which records their decision to skip multi-factor authentication (MFA) on the selected device.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

- This node requires the `realm` and `username` properties in the incoming node state.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

- This node requires the `mfaMethod` in the incoming state to know what type of MFA device to update:
  - For push authentication, this node requires the `pushMessageId` in the incoming state, which is a unique ID to identify the push notification request.

    Implement a Push Sender node earlier in the journey.
  - For OATH authentication, implement the OATH Token Verifier node earlier in the journey.

Dependencies

This node has no dependencies.

Configuration

This node has no configurable properties.

Outputs

This node doesn't change the shared state.

This node updates the user's profile with either the `push2faEnabled` or `oath2faEnabled` attribute to record their decision to opt out.

These are the default attributes but they can be changed in the ForgeRock Authenticator (Push) service or the ForgeRock Authenticator (OATH) service.

Outcomes

Single outcome path.

Errors

The node can log the following errors:

- `Expected username to be set`

  The node can't identify the user from the shared state.

- `Expected MFA method to be set`

  The node can't identify the MFA method from the shared state.

- `Unable to set user attribute as skippable`

  The node can't set the relevant attribute for the user's current device.

- `Failed to get the identity object`

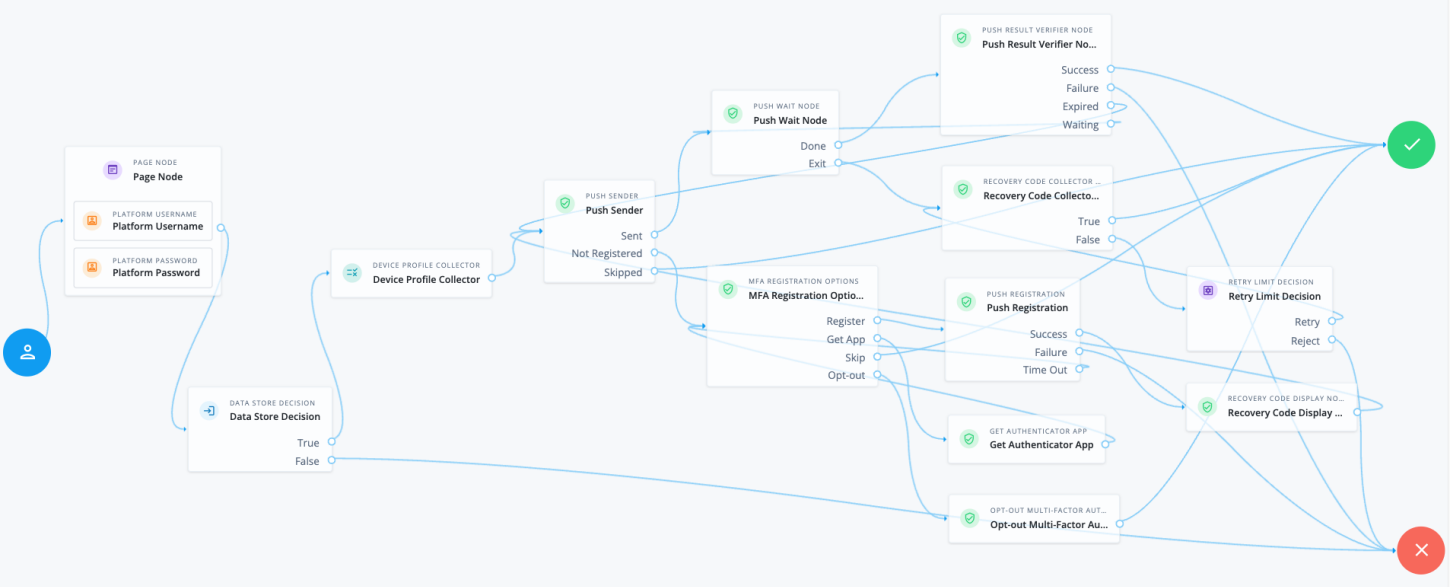
  The node can't read the identity of the account.

- `Unsupported MFA method has been set`

  The node can't retrieve the device profile details or the user has an unsupported MFA method set.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Push Registration node

The **Push registration** node lets a user register their device, such as a mobile phone for multi-factor authentication (MFA) using push notifications.

Learn more in the Push Authentication documentation for:

- Advanced Identity Cloud
- PingAM

> **Tip**
>
> You can use the Combined MFA Registration node to register a device for use with both push notifications and one-time passcode (OATH) verification in a single step.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The push-related nodes integrate with the ForgeRock Authenticator app for Android and iOS.

Third-party authenticator apps aren't compatible with the push notification functionality.

Inputs

This node requires the `realm` and `username` properties in the incoming node state.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

Dependencies

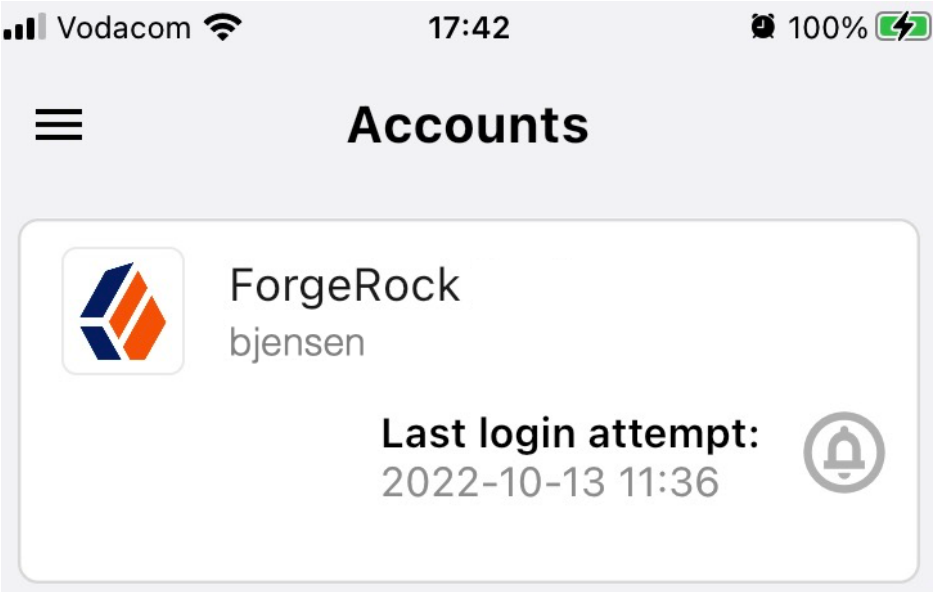
You must configure the Push Notification service for the realm to use this node. Optionally, also configure the ForgeRock Authenticator (Push) service.

Find more information in the corresponding documentation for:

- Advanced Identity Cloud
- PingAM

Find information on provisioning the credentials used by the service in How To Configure Service Credentials (Push Auth, Docker) in Backstage.

Configuration

Property	Usage
Issuer	The name of the issuer or application so the user knows which service their account relates to. This value is displayed in the authenticator app. 
Account Name	The profile attribute to display as the username in the authenticator app. If not specified, or if the specified profile attribute is empty, their username is used.
Background Color	The background color, in hex notation, to display behind the issuer's logo within the authenticator app.
Logo Image URL	The location of an image to download and display as the issuer's logo in the authenticator app.

Property	Usage
Generate Recovery Codes	Select this option to generate push-specific recovery codes. When enabled, recovery codes are generated and stored in the transient state if registration is successful. Use the Recovery Code Display node to display the codes to the user for safe keeping. **Important** Generating recovery codes overwrites all existing push-specific recovery codes. Only the most recent set of recovery codes can be used for authentication if a device is lost or stolen.
QR code message	(Optional) Add a custom, localized message to display to the user with instructions to scan the QR code to register the device: 1. Click **+**. 2. In the **Key** field, enter the locale. For example, `en-gb`.(1) 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.(2) Default: `Open your Authenticator app and tap the number shown to sign-in`
Registration Response Timeout	The number of seconds to wait for a response from the authenticator app. As soon as the specified time is reached, evaluation continues along the `Time Out` outcome path.

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

(2) PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Outputs

- The node adds the `pushDeviceProfiles` attribute to the user's profile with the device details on successful registration.
- The node updates the shared state with the push device settings, the message ID and the push challenge.
- If **Generate Recovery Codes** is enabled, the node records the recovery codes in the `recoveryCodes` shared state attribute. Use the Recovery Code Display node to display the codes to the user for safe keeping.

Outcomes

Success

The user successfully registered their authenticator app.

`Failure`

An issue occurred during device registration.

`Time Out`

A response wasn't received from the user's device within the time specified in the node configuration.

Errors

The node can log the following errors:

- `Unable to find push message ID`

  The node failed to read the `pushMessageId` from the shared state and can't proceed with registration. Make sure you have implemented a Push Sender node earlier in the journey.

- `Expected username to be set`

  The node can't identify the user from the shared state.

- `Unable to read service addresses for Push Notification Service`

  The node can't retrieve the push service URLs. Check that the Push Notification service is set up correctly in the realm.

- `Could not get messageId`

  The node fails to retrieve the messageId and can't proceed with registration.

- `The push message corresponds to <message type> message type which is not registered in the <realm name> realm`

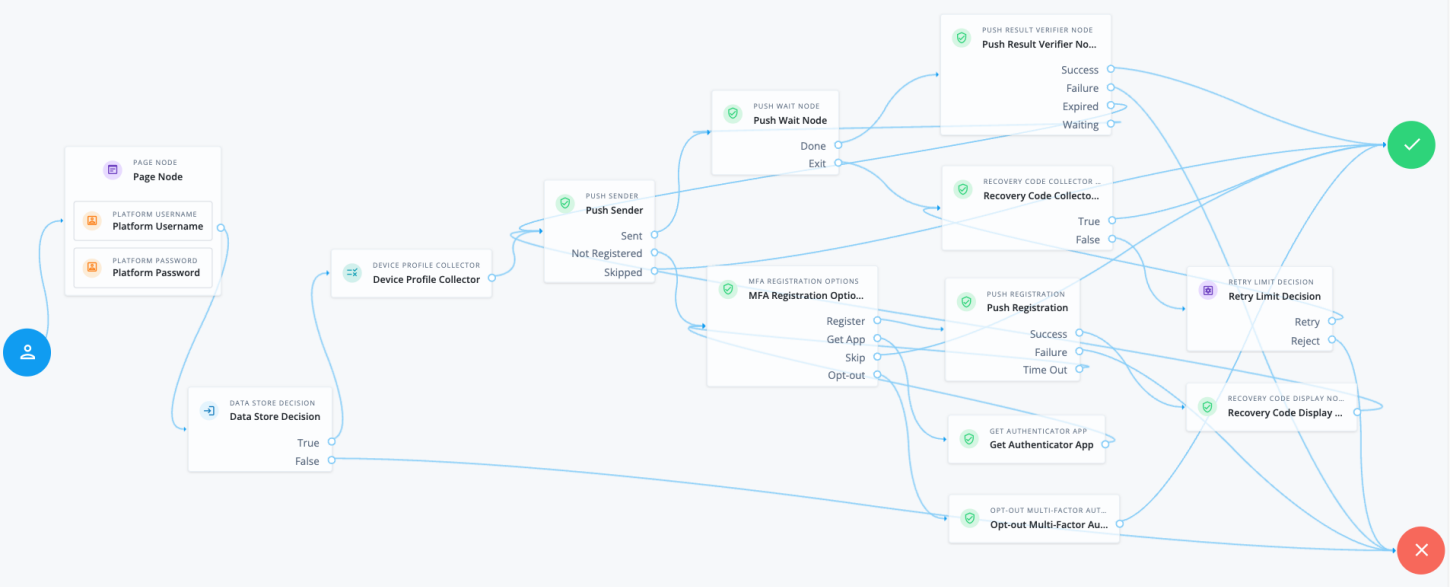
  The node can't start the registration process. Check that the Push Notification service is set up correctly in the realm.

- `Failed to save device to user profile`

  The node can't save the device details to the user's profile.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Push Result Verifier node

The **Push Result Verifier** node validates the user's response to a previously sent push notification message.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The push-related nodes integrate with the ForgeRock Authenticator app for Android and iOS.

Third-party authenticator apps aren't compatible with the push notification functionality.

Inputs

- This node requires the `realm` and `username` properties in the incoming node state.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

- This node also requires the `pushMessageId` in the incoming state, which is a unique ID to identify the push notification request.

  Implement a Push Sender node earlier in the journey.

Dependencies

You must configure the Push Notification service for the realm to use this node. Optionally, also configure the ForgeRock Authenticator (Push) service.

Find more information in the corresponding documentation for:

- Advanced Identity Cloud

- PingAM

Find information on provisioning the credentials used by the service in How To Configure Service Credentials (Push Auth, Docker) in Backstage.

Configuration

This node has no configurable properties.

Outputs

This node doesn't change the shared state.

Outcomes

`Success`

The user approved the push notification.

`Failure`

The user rejected the push notification.

`Expired`

A response wasn't received from the user's device within the time specified in the Push Sender node.

`Waiting`

A response hasn't been received yet.

Errors

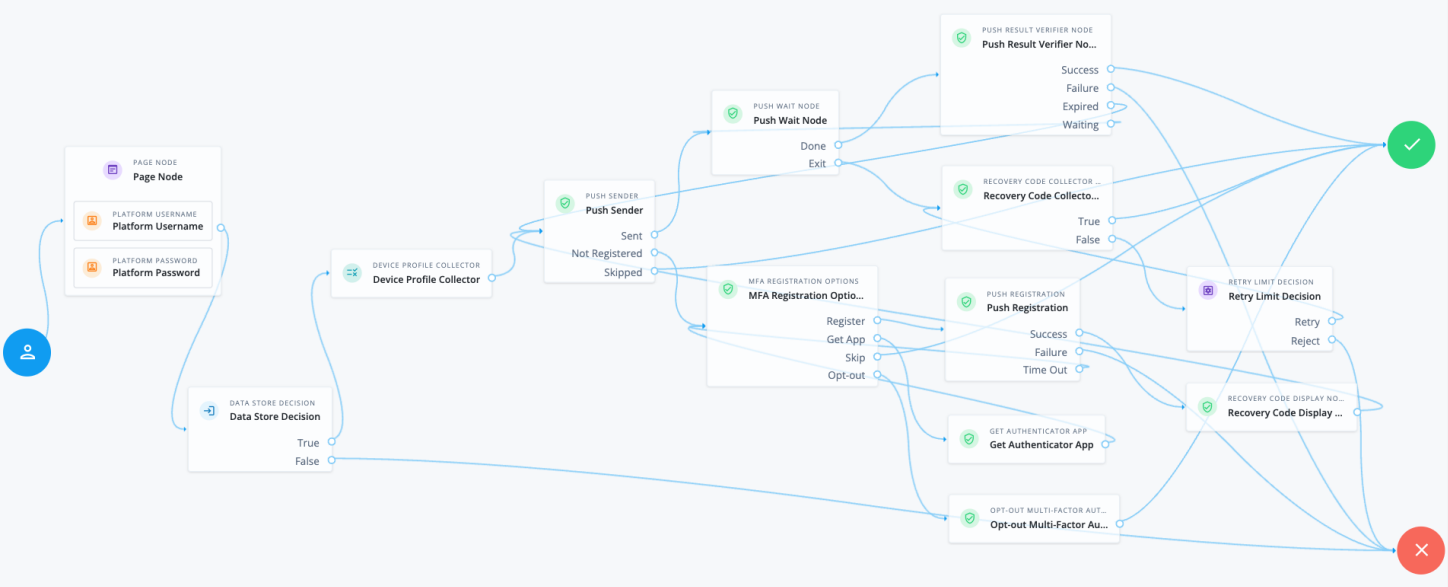
The node can log the following errors:

- `Unable to find push message ID`

  The node failed to read the `pushMessageId` from the shared state and can't verify the user's response. Make sure you have implemented a Push Sender node earlier in the journey.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Push Sender node

The **Push Sender** node sends push notification messages to a device for multi-factor authentication (MFA).

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The push-related nodes integrate with the ForgeRock Authenticator app for Android and iOS.

Third-party authenticator apps aren't compatible with the push notification functionality.

Inputs

- This node requires the `realm` and `username` properties in the incoming node state.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

- This node can read the device location from the incoming node state if it exists.

  The device location only exists when a Device Profile Collector node is implemented earlier in the journey with the **Collect Device Location** option selected.

Dependencies

You must configure the Push Notification service for the realm to use this node. Optionally, also configure the ForgeRock Authenticator (Push) service.

Find more information in the corresponding documentation for:

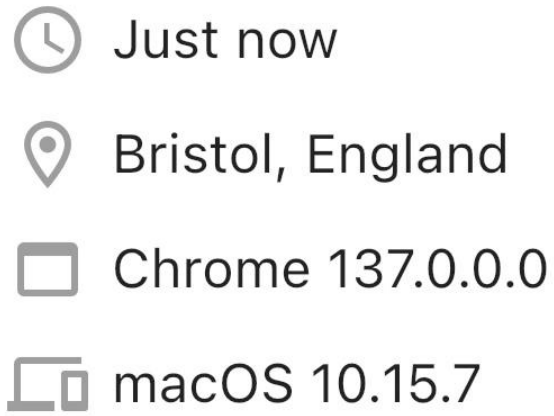
- Advanced Identity Cloud

- PingAM

Find information on provisioning the credentials used by the service in How To Configure Service Credentials (Push Auth, Docker) in Backstage.

Configuration

Property	Usage
Message Timeout	The number of milliseconds that the push notification message remains valid. The Push Result Verifier node rejects responses to push messages that have timed out. Default: `120000`
User Message	(Optional) Add a custom, localized message to send to the user. You can use the following variables in the **Value** field: **`{{user}}`** This variable is replaced with the username value obtained from the shared state, for example, `bjensen`. **`{{issuer}}`** This variable is replaced with the issuer value read from the device profile metadata, which is stored in the `pushDeviceProfiles` attribute by default. 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.(1) 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.(2) Default: `Login attempt from {{user}} at {{issuer}}`
Remove 'skip' option	Select this option to make push authentication mandatory. The `Skipped` outcome is not available when this option is selected. When disabled, the user can skip push authentication if required.

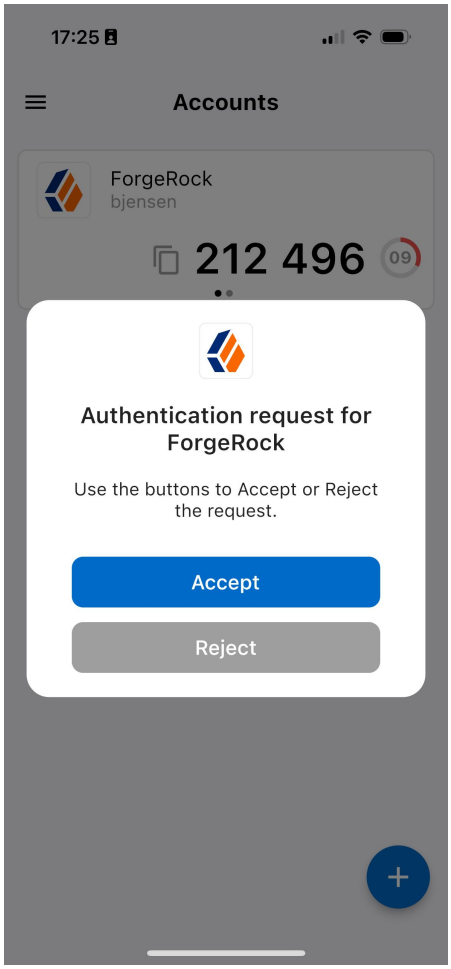
Property	Usage
Share Context Info	Select this option to include context data such as `remoteIp`, `userAgent`, and `location` in the notification payload. `{ "location": { "latitude": 51.454514, "longitude": -2.587910 }, "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36", "remoteIp": "9.9.9.9" }` The ForgeRock Authenticator app displays this additional information to the user to help them verify that the request is genuine and initiated by them. For example:  To include the `location` attribute, the journey must include a Device Profile Collector node with the **Collect Device Location** option selected.
Custom Payload Attributes	(Optional) Enter the names of the shared state objects to include in the message payload sent to the client. Enter each name separately and press Enter to add it. The size of the payload mustn't exceed 3 Kb.

Push Type

Select the type of push authentication the user must perform on their device to continue the journey.
Possible values are:

`Tap to Accept` *(default)*

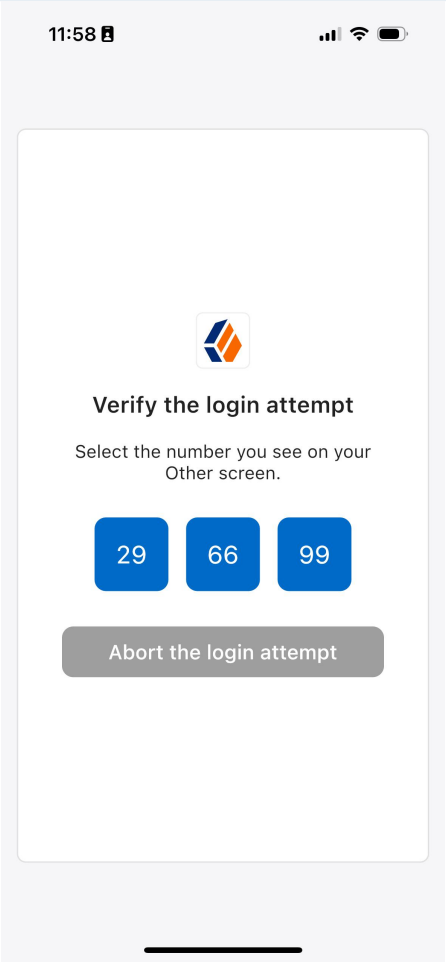
The user must tap `Accept` on their device to verify the request, or tap `Reject`.



> **Note**
> Research shows that users might accept a push authentication without checking it's legitimate. To reduce the chances of a user accepting a malicious push authentication attempt, consider using `Display Challenge Code` or `Use Biometrics to Accept` instead.

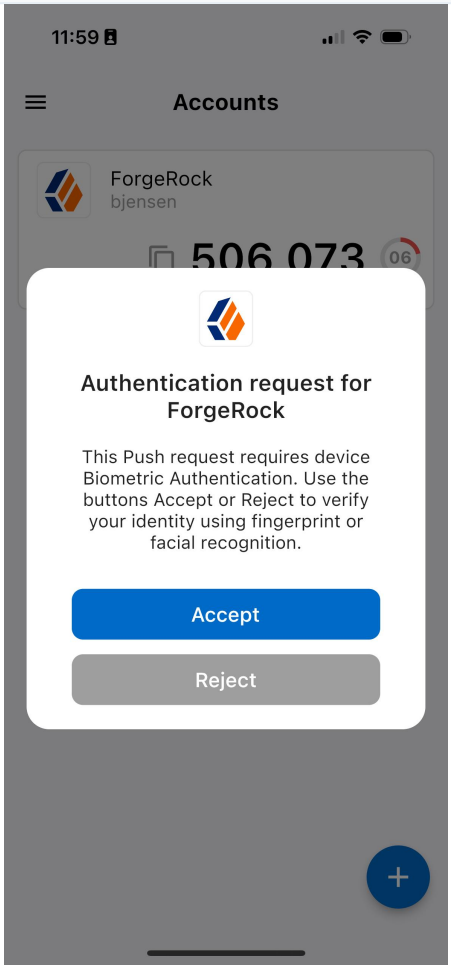
`Display Challenge Code`

The user must select one of three numbers displayed on their device. The number they select must match the code displayed in the browser to verify the request.



`Use Biometrics to Accept`

The user must tap `Accept` on their device and then authenticate using biometrics to verify the request.

Property	Usage
	
Capture failure	Select this option to store the failure reason in the `PushAuthFailureReason` shared state attribute when the node fails to send the push notification. The `Failure` outcome is only available when this option is selected.

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

(2) PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Outputs

- The node adds a unique ID to identify the push notification request to the `pushMessageId` shared state attribute.
- If the outcome is `Not Registered`, this node sets `"mfaMethod": "push"` in the shared state.
- If the node fails to send the push notification and **Capture failure** is enabled, the node adds the failure reason to a property named `PushAuthFailureReason` in the shared state. Other nodes can read this property later in the journey, if required.

Possible failure reasons are:

- `MISSING_USERNAME`
- `SENDER_ALREADY_USED`
- `CTS_ERROR`
- `TRANSMISSION_FAILURE`

Outcomes

`Sent`

The push notification was sent successfully to the device.

`Not Registered`

The user doesn't have a registered device.

`Skipped`

The user chooses to skip push authentication.

`Failure`

An error occurred during node execution.

Errors

The node can log the following errors:

- `Failed to fetch identity`

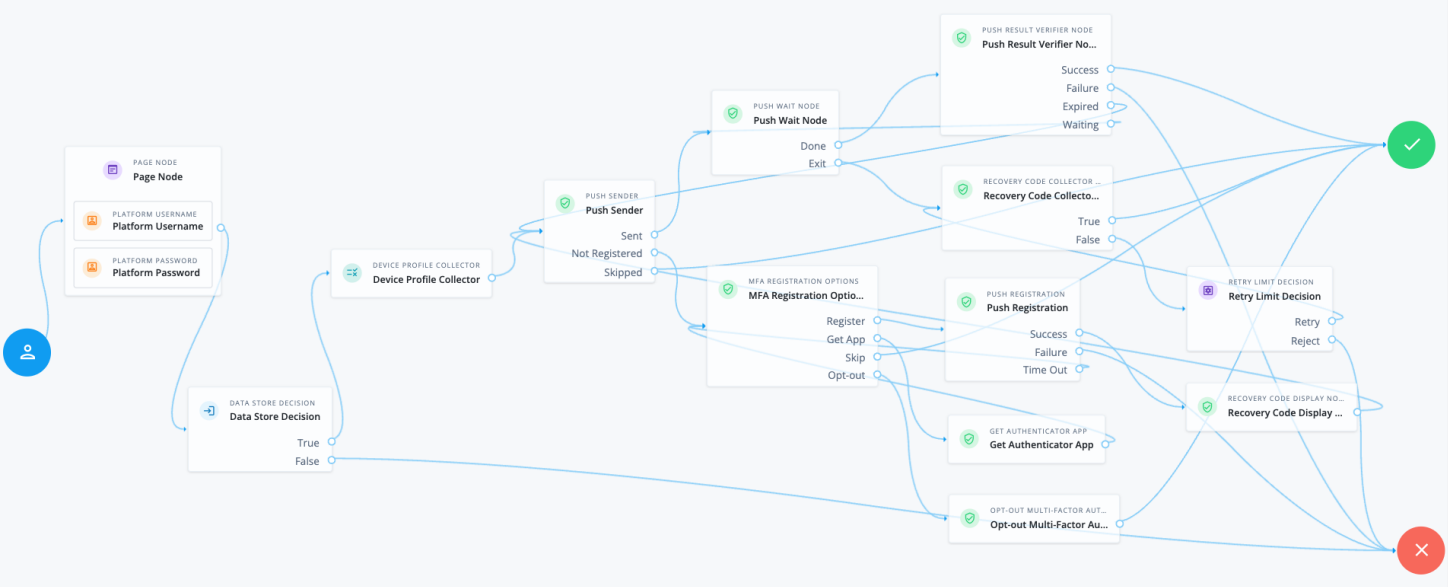
  The node can't identify the user from the shared state.

- `Payload data exceed maximum accepted size`

  The size of the message payload exceeds 3 Kb. Review any custom attributes you've included.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Push Wait node

The **Push Wait** node pauses authentication for the specified number of seconds during the processing of a push authentication request.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Authenticators

The push-related nodes integrate with the ForgeRock Authenticator app for Android and iOS.

Third-party authenticator apps aren't compatible with the push notification functionality.

Inputs

If the push type in the Push Sender node is set to `Display Challenge Code`, this node checks for the `pushNumberChallengeKey` in the incoming state. This value populates the `{{challenge}}` variable if it's included in the message.

Dependencies

Precede this node in the flow with a Push Sender node to send the push authentication request.

Configuration

Property	Usage
Seconds To Wait	The number of seconds to pause authentication. Default: `5`

Property	Usage
Waiting Message	(Optional) Add a custom, localized message to display to the user. You can use the `{{time}}` variable in the **Value** field to include the remaining seconds in the message: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Waiting for response…`
Push Challenge Message	(Optional) Add a custom, localized message to display to the user with the challenge code. You can use the `{{challenge}}` variable in the **Value** field to include the number challenge in the message. This message is displayed only when the **Push Type** in the Push Sender node is set to `Display Challenge Code`: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Open your Authenticator app and tap the number shown to sign-in`
Exit Message	(Optional) Add custom, localized text to display on the button the user can click to exit the node before the waiting period has elapsed. 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done. Leave blank to use the default message.[2] Default: `Cancel`

[1] Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

[2] PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Outputs

This node doesn't change the shared state.

Outcomes

Done

The waiting time has elapsed.

`Exit`

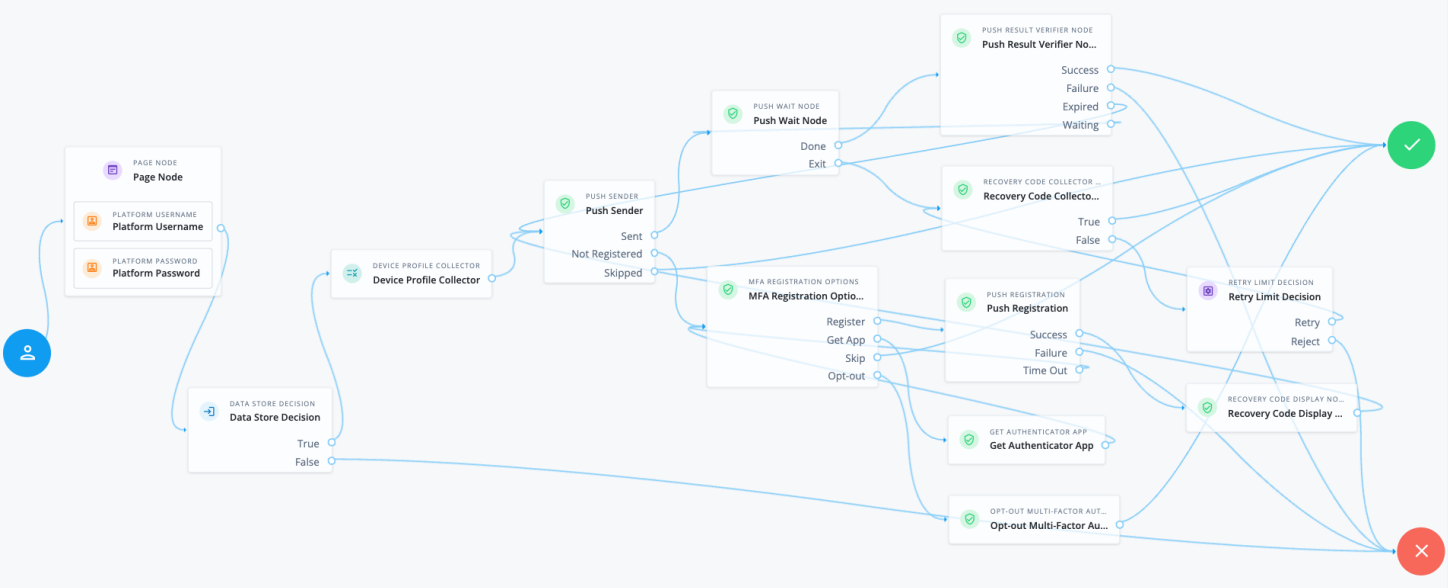
The user clicked the **Cancel** button to exit the node.

Errors

This node doesn't log any error or warning messages of its own.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision

Source node	Outcome path	Target node
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision

Source node	Outcome path	Target node
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

   > **Tip**
   >
   > Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

   A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.
3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   ### *Register Device*

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   ### *Get the App*

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

Skip this step

Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

Opt-out

Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Recovery Code Collector Decision node

The **Recovery Code Collector Decision** node lets users authenticate with a recovery code that was generated when they registered a device for multi-factor authentication (MFA).

Use this node in an authentication journey that includes push notifications or one-time passwords. When the user loses their registered device, they can use a recovery code as an alternative method for authentication.

Find more information on viewing recovery codes when registering a device in the *ForgeRock Authenticator* documentation for:

- PingAM
- Advanced Identity Cloud

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `realm` and `username` properties in the incoming node state.

Implement a Username Collector node (standalone AM) or Platform Username node (Advanced Identity Cloud and Ping Identity Platform deployments) earlier in the journey.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Recovery Code Type	Select the type of recovery code the user will submit for verification. Default: `OATH`

Outputs

This node doesn't change the shared state.

Outcomes

`True`

The user entered a valid recovery code.

`False`

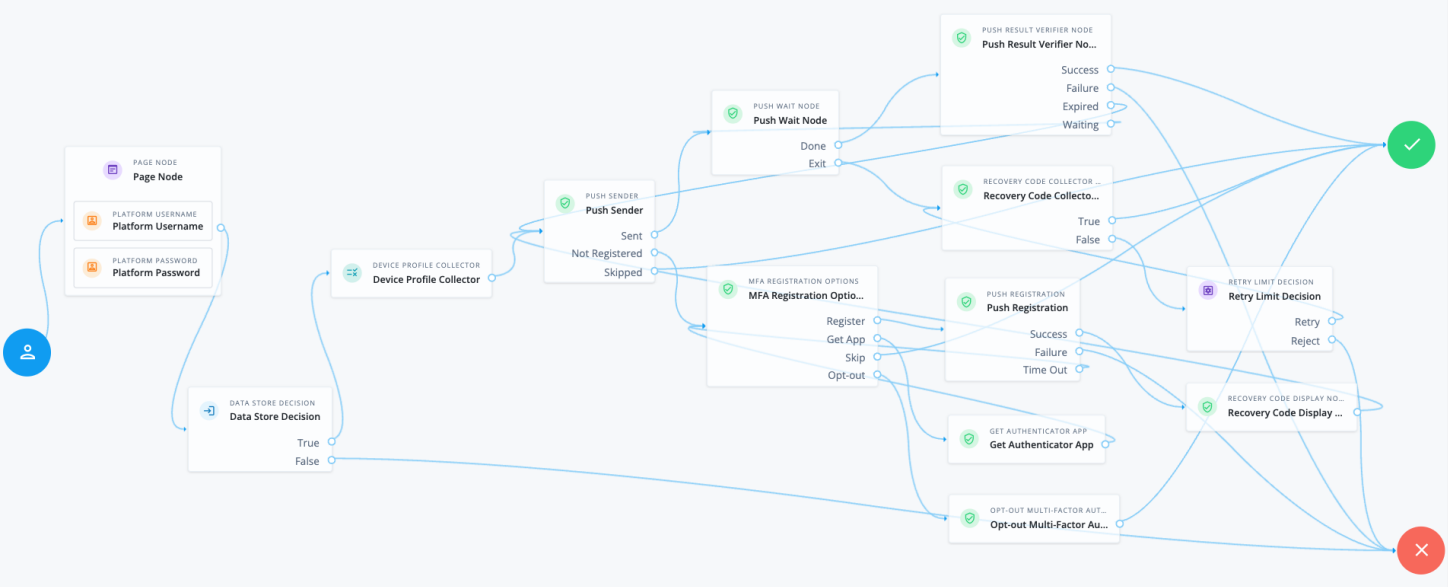
The user didn't enter a valid recovery code.

Errors

This node doesn't log any error or warning messages of its own.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success

Source node	Outcome path	Target node
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

> **Tip**
>
> Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.

3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   Register Device

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   Get the App

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

   Skip this step

   Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

   Opt-out

   Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

Recovery Code Display node

The **Recovery Code Display** node retrieves the generated recovery codes from the transient state and displays them to the user, for safe-keeping. The codes can be used to authenticate if a registered device is lost or stolen.

> **Important**
>
> The generated recovery codes can't be retrieved from the user's profile because they're one-way encrypted.
> This node provides the *only* opportunity to view and save the recovery codes.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `recoveryCodes` attribute in the incoming state so that it can display the recovery codes to the user. If there aren't any recovery codes in the transient state, evaluation continues along the only outcome path and nothing is displayed to the user.

Implement an OATH Registration node, a Push Registration node or a WebAuthn Registration node earlier in the journey, and connect the `Success` outcome path to this node to display the codes.

Dependencies

This node has no dependencies.

Configuration

This node has no configurable properties.

Outputs

This node removes the recovery code details from the shared state.

Outcomes

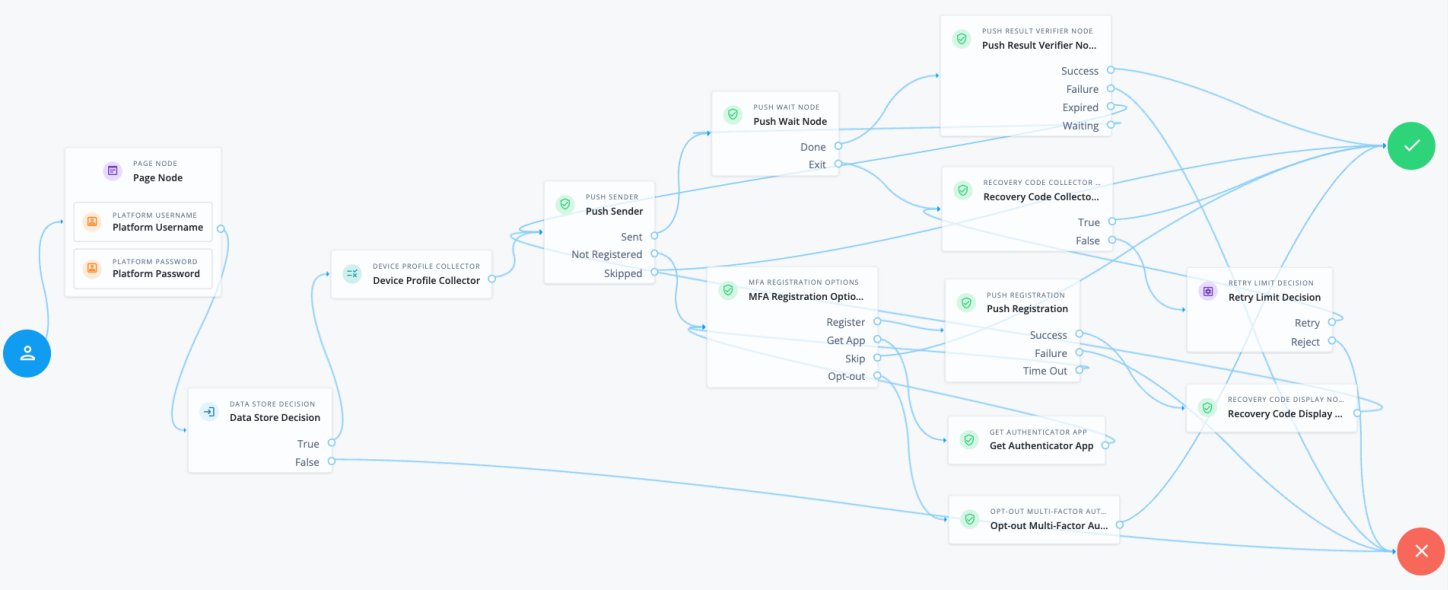
Single outcome path.

Errors

This node doesn't log any error or warning messages of its own.

Examples

The following example shows one possible implementation of multi-factor push authentication, which uses this node:



List of node connections

Source node	Outcome path	Target node
Page Node containing nodes to collect credentials. For standalone AM deployments, implement a Username Collector node and a Password Collector node. For Advanced Identity Cloud and Ping Identity Platform deployments, implement a Platform Username node and a Platform Password node.	→	Data Store Decision
Data Store Decision	True	Device Profile Collector

Source node	Outcome path	Target node
	False	Failure
Device Profile Collector	→	Push Sender
Push Sender	Sent	Push Wait
	Not Registered	MFA Registration Options
	Skipped	Success
Push Wait	Done	Push Result Verifier
	Exit	Recovery Code Collector Decision
Push Result Verifier	Success	Success
	Failure	Failure
	Expired	Push Sender
	Waiting	Push Wait
MFA Registration Options	Register	Push Registration
	Get App	Get Authenticator App
	Skip	Success
	Opt-out	Opt-out Multi-Factor Authentication
Recovery Code Collector Decision	True	Success
	False	Retry Limit Decision
Push Registration	Success	Recovery Code Display Node
	Failure	Failure
	Time Out	MFA Registration Options
Get Authenticator App	→	MFA Registration Options
Opt-out Multi-Factor Authentication	→	Success
Retry Limit Decision	Retry	Recovery Code Collector Decision
	Reject	Failure

Source node	Outcome path	Target node
Recovery Code Display Node	→	Push Sender

After verifying the user's credentials, evaluation continues to the Device Profile Collector node to collect the device's location and then proceeds to the Push Sender node.

If the user *has* a registered device:

1. The Push Sender node sends a push notification to their registered device.
2. The Push Wait node pauses authentication for five seconds. During this time, the user can respond to the push notification on their device using the ForgeRock Authenticator app.

   If the user exits the Push Wait node, they're directed to the Recovery Code Collector Decision node, where they can enter a recovery code to authenticate.

   > **Tip**
   >
   > Configure the **Exit Message** property in the Push Wait node with a message, such as `Lost phone? Use a recovery code` for situations like this.

   A Retry Limit Decision node allows three attempts to enter a recovery code before failing the authentication.
3. The Push Result Verifier node verifies the user's response:
   - If the user responds positively, they're authenticated successfully and logged in.
   - If the user responds negatively, authentication fails.
   - If the push notification expires, the Push Sender node sends a new push notification.

     > **Tip**
     >
     > Use a Retry Limit Decision node to constrain the number of times a new code is sent.

   - If the user hasn't yet responded, the flow loops back a step and the Push Wait node pauses authentication for another 5 seconds.

If the user *doesn't have* a registered device:

1. The MFA Registration Options node presents the user with the following options:

   ### *Register Device*

   The flow continues to the Push Registration node, which displays a QR code for the user to scan with their authenticator app.

   ### *Get the App*

   Displayed only if the node is configured to display Get Authenticator App. The flow continues to the Get Authenticator App node, which displays links to download the authenticator app.

Skip this step

Displayed only if the node is configured to allow users to skip registration. In this example, skipping is linked to the `Success` outcome. However, you could provide an alternative authentication flow using an Inner Tree Evaluator node for example.

Opt-out

Displayed only if the node is configured to allow users to skip registration. Evaluation continues to the Opt-out Multi-Factor Authentication node, which updates the user's profile to skip MFA with push in the future. In this example, after updating the profile, the flow continues to the `Success` outcome.

2. The user registers the device with the Push Registration node.

After registration, the Recovery Code Display node displays the recovery codes to the user and the flow returns to the Push Sender node to continue push authentication.

> **Note**
>
> To manage push devices, the user must log in using either the device or a recovery code.
> Find more information in the MFA documentation for:
>
> - PingAM
> - Advanced Identity Cloud

WebAuthn Authentication node

The **WebAuthn Authentication** node lets users on supported clients authenticate using a registered FIDO device.

There are many similarities between WebAuthn and device binding and JWS verification. We provide authentication nodes to implement both technologies in your journeys.

Both can be used for usernameless and passwordless authentication, they both use public key cryptography, and both can be used as part of a multi-factor authentication journey.

One major difference is that with device binding, the private key never leaves the device.

With WebAuthn, there is a possibility that the private key is synchronized across client devices because of Passkey support, which may be undesirable for your organization.

For details of the differences, refer to the following table:

Comparison of WebAuthn and Device Binding/JWS Verification

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Industry-standards based	☑	×	You can refer to the WebAuthn W3C specification. Device binding and JWS verification are proprietary implementations.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Public key cryptography	☑	☑	Both methods use Public key cryptography.
Usernameless support	☑	☑	After registration, the username can be stored in the device and obtained during authentication without the user having to enter their credentials.
Keys are bound to the device	✕	☑	With WebAuthn, if Passkeys are used, they can be shared across devices. With device binding, the private keys do not leave the device.
Sign custom data	✕	☑	With device binding, you can: • Customize the challenge that the device must sign. For example, you could include details of a transaction, such as the amount in dollars. • Add custom claims to the payload when signing a challenge. This gives additional context that the server can make use of by using a scripted node. Refer to Add custom claims when signing.
Format of signed data	WebAuthn authenticator data	JSON Web Signature (JWS)	
Integration	✕	☑	With device binding, after verification, the signed JWT is available in: • Audit Logs • Transient node state This enables the data within to be used for integration into your processes and business logic.
Platform support	☑ Android ☑ iOS ☑ Web browsers	☑ Android ☑ iOS ✕ Web browsers	As it is challenging to store secure data in a browser as a client app, device binding is not supported in web browsers.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Authenticator support	Determined by the platform. Configuration limited to: • Biometric with Fallback to Device Pin	Determined by the authentication node. Full configuration options: • Biometric Authentication • Biometric with Fallback to Device Pin • Application Pin • Silent	With device binding, you can specify what authentication action the user must perform to get access to the private keys. This provides greater flexibility in your security implementation and can reduce authentication friction for your users.
Key storage	Web browsers and iOS synchronize to the cloud. Android has the option to synchronize to the cloud.	***Android*** KeyStore ***iOS*** Secure enclave: hardware-backed and not synchronized to the cloud.	Both technologies store the private keys securely on the client. WebAuthn supports synchronizing the private keys to the cloud for use on other devices. This can reduce authentication friction for your users but may also increase the risk of a breach.
Managing device keys	Managed by the device OS. Apps cannot delete *local* client keys programmatically and do not have a reference to the *remote* server key for deletion.	Managed by the Ping SDKs. Provides an interface to delete local client and remote server keys.	The ability to programmatically delete both client and server keys can greatly simplify the process of registering a new device if an old device is lost or stolen.
Passkey support	☑	×	WebAuthn supports synchronizing the private keys to the cloud for use on other devices. Device binding keeps the private key locked in the device.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
App integrity verification	***Android*** Requires an `assetlinks.json` file. ***iOS*** Requires `apple-app-site-association` file.	Not provided by the device binding or verification nodes. It can be added as part of the journey by using app integrity nodes.	App integrity verification helps ensure your users are only using a supported app rather than a third-party or potentially malicious version.
Key attestation	***Android*** SafetyNet ***iOS*** None	***Android*** Uses hardware-backed key pairs with Key Attestation. ***iOS*** It can be added as part of the journey by using app integrity nodes to support key attestation.	Key attestation verifies that the private key is valid and correct, is not forged, and was not created in an insecure manner.
Complexity	Medium	Low	WebAuthn requires a bit more configuration, for example, creating and uploading the `assetlinks.json` and `apple-app-site-association` files. Device binding only requires the journey and the SDK built into your app.

Important

To authenticate using WebAuthn on an Android or iOS device without an external keystore, screen lock *must* be enabled. Find more information in the respective device documentation for Android and iOS.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes

Product	Available?
Ping Identity Platform (self-managed)	Yes

Inputs

- This node reads the `username` from the shared state to assess whether the user has a registered device.

  Implement the following node before this node in the journey:

  - Username Collector node (standalone AM)
  - Platform Username node (Ping Identity Platform deployment)

- Optionally, this node can read the contents of the `webAuthnExtensions` shared state property as input.

  You can populate the `webAuthnExtensions` property with any JSON object you choose using a script or in a node that occurs earlier in the journey. If this property is populated, its contents are placed in the `extensions` entry passed to the browser or authenticator. If this property is empty, an empty JSON object is passed to the browser or authenticator.

  You can find more information on WebAuthn extensions in WebAuthn Extensions.

Dependencies

For successful authentication, this node depends on:

- A client that supports web authentication
- A registered FIDO device

Configuration

Property	Usage
Relying party identifier	The domain used as the relying party identifier during web authentication. This is the domain against which to register the device. If you leave this field blank, it defaults to the domain name of the AM instance, for example, `am.example.com`. Specify an alternative domain if your AM instances are behind a load balancer, for example.
Origin domains	A list of fully qualified URLs to accept as the origin of the incoming request. If this field is empty, the accepted origin is the incoming request origin.

Property	Usage
User verification requirement	The required user verification level. The available options are: **`REQUIRED`** The authenticator used must verify the user's identity, for example, by using biometrics. Authenticators that don't verify the user's identity are filtered out and can't be selected by the user. **`PREFERRED`** If multiple authenticators are presented, AM prefers those that verify the user's identity. If none are available, AM accepts any authenticator. **`DISCOURAGED`** AM doesn't require an authenticator that verifies the user's identity. Authenticators that don't verify the user's identity are preferred.
Allow recovery codes	If you select this option, AM lets the user enter a recovery code instead of performing an authentication gesture. Enabling this options adds a `Recovery Code` outcome path to the node. The outcome path should lead to a Recovery Code Collector Decision node to collect and verify the recovery code.
Timeout	The number of seconds to wait for a valid WebAuthn authenticator to be registered before failing. If the specified timeout is reached, evaluation continues along the `Client error` outcome path. AM stores a message in the `WebAuthenticationDOMException` property of the shared state.
Username from device	Specifies whether AM should get the username from the device. If you enable this option and the device is unable to store or provide usernames, the node fails and evaluation continues along the `Failure` path. You can find information on using this property for usernameless authentication with ForgeRock Go in Configure usernameless authentication with ForgeRock Go.

Property	Usage
Return challenge as JavaScript	Choose how the node should return its challenge for consumption by your front-end user interface: ***PingOne Advanced Identity Cloud hosted pages or Ping SDK client apps:*** Deselect this option when using either hosted pages in PingOne Advanced Identity Cloud or a client application built using the Ping SDKs as your authentication user interface. When not enabled the node returns the challenge and associated data in a metadata callback. PingOne Advanced Identity Cloud hosted pages and Ping SDK client apps that might not be able to execute JavaScript use the information from the callback to interact with WebAuthn APIs on AM's behalf. ***PingAM User UI:*** You should only enable this option if you are using the PingAM User UI to authenticate users. Enabling this option causes the node to return its challenge as a fully encapsulated client-side JavaScript that interacts directly with the WebAuthn API.
Detect sign count mismatch	The sign count is useful for detecting potential cloned devices. It's stored in the WebAuthn device profile as `signCount`. If you enable this option, the node compares the authenticator's sign count (signature counter) with the sign count stored in the user's profile. If the authenticator sign count is less than or equal to the stored value, evaluation continues to the Sign Count Mismatch outcome.

Outcomes

`Unsupported`

If the user's client doesn't support web authentication, evaluation continues along the `Unsupported` outcome path. For example, clients connected over the HTTP protocol rather than HTTPS don't support WebAuthn; however, HTTPS may not be required when testing locally on `http://localhost`. Learn more in Is origin potentially trustworthy?.

`No Device Registered`

If the user doesn't have a registered device, evaluation continues along the `No Device Registered` outcome path.

`Success`

If the user successfully authenticates with a device of the type determined by the **User verification requirement** property, evaluation continues along the `Success` outcome path.

`Failure`

If the node encounters an issue when attempting to authenticate the user with the device, evaluation continues along the `Failure` outcome path; for example, if the node can't verify that the response from the authenticator was appropriate for the specific instance of the authentication journey.

`Client Error`

If the user's client encounters an issue when attempting to authenticate using the device, for example, if the timeout was reached, evaluation continues along the `Client Error` outcome path.

The journey takes this path whenever the client throws a `DOMException`, as required by the Web Authentication: An API for accessing Public Key Credentials Level 1 specification.

`Recovery Code`

If **Allow recovery code** is enabled, the node gives the user an option to enter a recovery code rather than authenticate using a device. If the user enters a recovery code, evaluation continues along the `Recovery Code` outcome path.

This outcome path must lead to a Recovery Code Collector Decision node to let AM accept and verify the recovery code.

`Sign Count Mismatch`

If **Detect sign count mismatch** is enabled and the authenticator sign count is less than or equal to the value stored in the user's profile, evaluation continues to the **Sign Count Mismatch** outcome.

This outcome can help to detect cloned or malfunctioning authenticators. A sign count mismatch doesn't necessarily indicate that the operation was performed by a cloned authenticator. Address this situation appropriately for your deployment, for example, by using a scripted decision node.

> **Note**
>
> The node itself is considered to have succeeded even if evaluation leads to this outcome. Therefore, if it suits your deployment, you can design your journey to continue through this outcome.

Outputs

- If a client error occurs, the node adds the error type and description to a property named `WebAuthenticationDOMException` in the shared state. Other nodes can read this property later in the journey, if required.
- PingAM On successful authentication, the node adds the UUID of the device (`webauthnDeviceUuid`) and the name of the device (`webauthnDeviceName`) to the shared state.

  This lets you track the use of biometric authentication and the device used to authenticate.
- PingAM On successful authentication, the node adds a `webauthnAssertionInfo` object to the transient state.

  The `webauthnAssertionInfo` object includes the following information:

```
{
  "authenticatorAttachment": "platform",
  "flags": {
    "UP": true,
    "UV": true,
    "ED": false,
    "AT": false,
    "BE": true,
    "BS": true
  }
}
```

The `authenticatorAttachment` field is only populated when the UI or client application supports sending it. This field lets the journey identify whether the device used to authenticate was a roaming (cross-platform) device or a client-bound (platform) device. Learn more in Authenticator Attachment Modality in the WebAuthn specification.

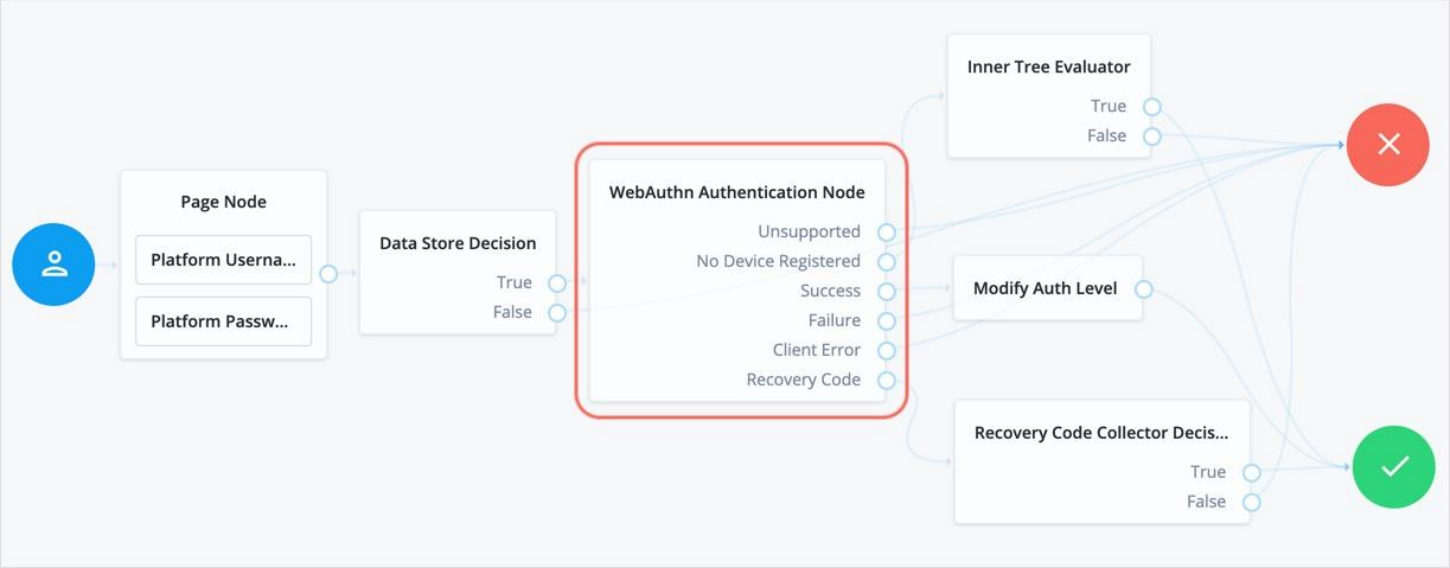
The `flags` provide additional information about the authenticator. Learn more about these flags in Authenticator Data in the WebAuthn specification.

Note

- With the exception of the `webauthnAssertionInfo` object, the contents of the transient state for this node aren't public. Don't rely on them in your scripts.

Example

This example shows one possible implementation of the flow for authenticating with WebAuthn devices:

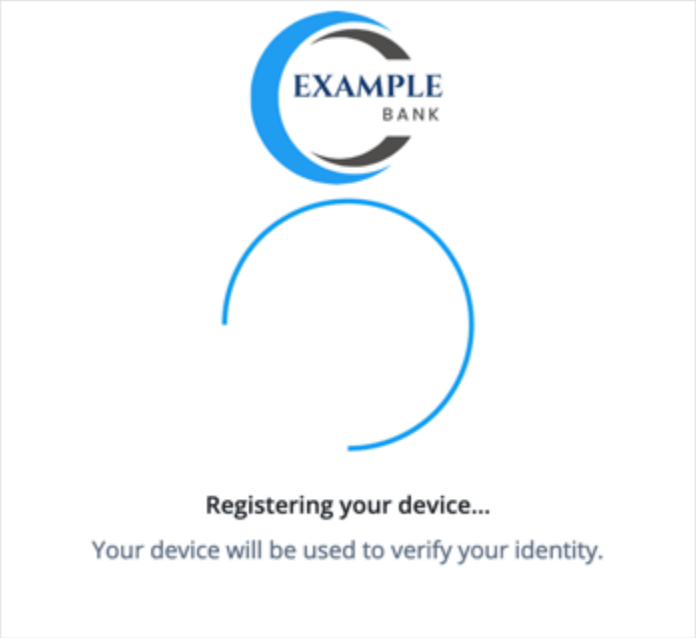


After verifying the users credentials against the configured data store, evaluation continues to the WebAuthn Authentication node.

If the user's client doesn't support WebAuthn, authentication fails and the user doesn't get a session. A more user-friendly approach would be to set a success URL to redirect the user to a page explaining the benefits of multi-factor authentication, and then proceeding to the `Success` node.

If there are no registered WebAuthn devices present in the user's profile, the failure URL is set, pointing to a flow that lets the user register a device. This stage could also be an Inner Tree Evaluator node.

If the user's client supports WebAuthn, and the connection is secured with TLS, the user is prompted to complete an authorization gesture, for example, scanning a fingerprint, or entering a PIN:



The user's browser may present a consent pop-up to allow access to the authenticators available on the client. When consent has been granted, the browser activates the relevant authenticators, ready for authentication.

> **Tip**
>
> The relying party details configured in the node are often included in the consent message to help the user verify the entity requesting access.

The authenticators the client activates for authentication depend on the value of the properties in the node. For example, if the **User verification requirement** property is set to `REQUIRED`, the client **SHOULD** only activate authenticators that verify the identity of the user.

For extra protection, AM **WILL** verify that the response from an authenticator matches the criteria configured for the node, and will reject an authentication attempt by an inappropriate authenticator type by routing it to the `Failure` outcome.

When the user completes an authorization gesture, for example, by scanning a fingerprint or entering a PIN, evaluation continues along the `Success` outcome path. In this example, their authentication level is increased by ten to signify the stronger authentication that has occurred, and the user is taken to their profile page.

If the user clicks the `Use Recovery Code` button, evaluation continues to the Recovery Code Collector Decision node, ready to accept the recovery code. If verified, the user is taken to their profile page.

Any problems encountered during authentication lead to the `Failure` outcome, including a timeout, or to the `Client Error` outcome, resulting in an authentication failure.

WebAuthn Device Storage node

Writes information about FIDO2 devices to a user's profile. The user can subsequently authenticate using the device.

Use this node to store the device data the WebAuthn Registration node places into the transient node state when its **Store device data in transient state** property is enabled.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Success`
- `Failure`
- `Exceed Device Limit`

If AM encounters an issue when attempting to save the device data to the user's profile; for example, the user was not identified earlier, then evaluation continues along the `Failure` outcome path.

If the **Maximum Saved Devices** property is set to an integer greater than zero, and registering a new device would take the number of devices above the specified threshold, then evaluation continues down the `Exceed Device Limit` outcome path. In this case, you may need to instruct your users to log in with an existing device in order to remove one or more of their registered devices.

If the node successfully stores the device data to the user's profile, evaluation continues along the `Success` outcome path.

Properties

Property	Usage
Generate recovery codes	Specify whether WebAuthn device recovery codes should be generated. If enabled, recovery codes are generated and stored in the transient node state, and stored alongside the device profile. Use the Recovery Code Display node to display the codes to the user for safe keeping. **Important** Generating recovery codes overwrites all existing WebAuthn device recovery codes for the device. Only the most recent set of recovery codes can be used for authentication if a device has been lost or stolen.
Maximum Saved Devices	Specify the maximum number of WebAuthn devices to save in a user's profile. Set this property to `0` if you do not want to limit the number of devices. When this property is greater than zero, the `Exceed Device Limit` outcome path becomes available.

WebAuthn Registration node

The **WebAuthn Registration** node lets users of supported clients register FIDO2 devices for use during authentication.

There are many similarities between WebAuthn and device binding and JWS verification. We provide authentication nodes to implement both technologies in your journeys.

Both can be used for usernameless and passwordless authentication, they both use public key cryptography, and both can be used as part of a multi-factor authentication journey.

One major difference is that with device binding, the private key never leaves the device.

With WebAuthn, there is a possibility that the private key is synchronized across client devices because of Passkey support, which may be undesirable for your organization.

For details of the differences, refer to the following table:

Comparison of WebAuthn and Device Binding/JWS Verification

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Industry-standards based	☑	×	You can refer to the WebAuthn W3C specification. Device binding and JWS verification are proprietary implementations.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Public key cryptography	☑	☑	Both methods use Public key cryptography.
Usernameless support	☑	☑	After registration, the username can be stored in the device and obtained during authentication without the user having to enter their credentials.
Keys are bound to the device	✕	☑	With WebAuthn, if Passkeys are used, they can be shared across devices. With device binding, the private keys do not leave the device.
Sign custom data	✕	☑	With device binding, you can: • Customize the challenge that the device must sign. For example, you could include details of a transaction, such as the amount in dollars. • Add custom claims to the payload when signing a challenge. This gives additional context that the server can make use of by using a scripted node. Refer to Add custom claims when signing.
Format of signed data	WebAuthn authenticator data	JSON Web Signature (JWS)	
Integration	✕	☑	With device binding, after verification, the signed JWT is available in: • Audit Logs • Transient node state This enables the data within to be used for integration into your processes and business logic.
Platform support	☑ Android ☑ iOS ☑ Web browsers	☑ Android ☑ iOS ✕ Web browsers	As it is challenging to store secure data in a browser as a client app, device binding is not supported in web browsers.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
Authenticator support	Determined by the platform. Configuration limited to: • Biometric with Fallback to Device Pin	Determined by the authentication node. Full configuration options: • Biometric Authentication • Biometric with Fallback to Device Pin • Application Pin • Silent	With device binding, you can specify what authentication action the user must perform to get access to the private keys. This provides greater flexibility in your security implementation and can reduce authentication friction for your users.
Key storage	Web browsers and iOS synchronize to the cloud. Android has the option to synchronize to the cloud.	***Android*** KeyStore ***iOS*** Secure enclave: hardware-backed and not synchronized to the cloud.	Both technologies store the private keys securely on the client. WebAuthn supports synchronizing the private keys to the cloud for use on other devices. This can reduce authentication friction for your users but may also increase the risk of a breach.
Managing device keys	Managed by the device OS. Apps cannot delete *local* client keys programmatically and do not have a reference to the *remote* server key for deletion.	Managed by the Ping SDKs. Provides an interface to delete local client and remote server keys.	The ability to programmatically delete both client and server keys can greatly simplify the process of registering a new device if an old device is lost or stolen.
Passkey support	☑	×	WebAuthn supports synchronizing the private keys to the cloud for use on other devices. Device binding keeps the private key locked in the device.

Feature	WebAuthn / FIDO	Device Binding / JWS Verifier	Details
App integrity verification	***Android*** Requires an `assetlinks.json` file. ***iOS*** Requires `apple-app-site-association` file.	Not provided by the device binding or verification nodes. It can be added as part of the journey by using app integrity nodes.	App integrity verification helps ensure your users are only using a supported app rather than a third-party or potentially malicious version.
Key attestation	***Android*** SafetyNet ***iOS*** None	***Android*** Uses hardware-backed key pairs with Key Attestation. ***iOS*** It can be added as part of the journey by using app integrity nodes to support key attestation.	Key attestation verifies that the private key is valid and correct, is not forged, and was not created in an insecure manner.
Complexity	Medium	Low	WebAuthn requires a bit more configuration, for example, creating and uploading the `assetlinks.json` and `apple-app-site-association` files. Device binding only requires the journey and the SDK built into your app.

AM interacts with FIDO2/WebAuthn capable browsers, such as `Chrome`, `Firefox` and `Microsoft Edge`.

These browsers interact with the following:

- Client to Authenticator Protocol 2 (CTAP2) authenticators, including Universal 2nd Factor (U2F) and FIDO2 Security Keys
- Platforms such as Windows Hello and Apple Touch ID

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `username` and `password` properties in the incoming node state. Implement the following nodes earlier in the journey:

- Standalone PingAM deployment
  - Username Collector node
  - Password Collector node
- Ping Identity Platform deployment:
  - Platform Username node
  - Platform Password node

Optionally, this node can read the contents of the `webAuthnExtensions` shared state property as input.

You can populate the `webAuthnExtensions` property with any JSON object you choose using a script or in a node that occurs earlier in the journey. If this property is populated, its contents are placed in the `extensions` entry passed to the browser or authenticator. If this property is empty, an empty JSON object is passed to the browser or authenticator.

You can find more information on WebAuthn extensions in WebAuthn Extensions.

Dependencies

You must configure the WebAuthn Profile Encryption service to use this node.

Configuration

Property	Usage
Relying party	The name of the relying party entity that registers and authenticates users by using WebAuthn. This could be the name of the organization, realm, and so on. For example, `Example.com`
Relying party identifier	The domain used as the relying party identifier during WebAuthn. If not specified, AM uses the domain name of the instance, such as `am.example.com`. Specify an alternative domain if your AM instances are behind a load balancer.
Origin domains	A set of fully-qualified URLs of accepted origins, for example `http://app.example.com:443`. If empty, the accepted origin is the incoming request origin.

Property	Usage
User verification requirement	The required level of user verification. The available options are: **`REQUIRED`** The authenticator must verify the identity of the user, for example, by using biometrics. AM filters out authenticators that don't verify user identity and the user can't select them. **`PREFERRED`** AM prefers an authenticator that verifies user identity. If none are available, AM accepts any authenticator. **`DISCOURAGED`** The authenticator doesn't need to verify the identity of the user. Authenticators that don't verify user identity are preferred. Default: `PREFERRED`
Preferred mode of attestation	Indicates whether the authenticator must provide attestation statements. The available options are: **`NONE`** AM doesn't require the authenticator to provide attestation statements. If the authenticator sends attestation statements, AM doesn't verify them and the process doesn't fail. **`INDIRECT`** AM doesn't require the authenticator to provide attestation statements. However, if the authenticator sends attestation statements, AM verifies them and the process fails if the verification fails. **`DIRECT`** AM requires the authenticator to provide attestation statements and verifies them. The process fails if the attestation statements can't be verified. AM supports the following attestation formats: • None • Android SafetyNet • Packed • FIDO U2F • TPM **Important** If your end users use an authenticator that provides attestation statements in a format other than these supported formats, you must set the **Preferred mode of attestation** property to `NONE`. Specifically, AM *does not* support the Android Key Attestation Statement Format.

Property	Usage
Accepted signing algorithms	The algorithms authenticators can use to sign their assertions.
Authentication attachment	If specified, AM filters out authenticators that don't match the attachment type. There are two attachment types: • A `PLATFORM` authenticator is part of the device, for example, a fingerprint scanner built-in to a phone or laptop. • A `CROSS_PLATFORM` authenticator can be removed from a device and used elsewhere, for example, a USB hardware security key. Available options for this property are: **`UNSPECIFIED`** AM accepts any attachment type. **`PLATFORM`** The authenticator must be a *platform* attachment type. The client shouldn't activate other authenticator types for registration. **`CROSS_PLATFORM`** The authenticator must be a *cross-platform* attachment type. The client shouldn't activate other authenticator types for registration.
Trust Store alias	The alias of the realm trust store holding the secrets necessary to validate a supplied attestation certificate. The alias can only contain the characters `a-z` and periods (`.`). This value is appended to the string `am.authentication.nodes.webauthn.truststore.` to form the dynamic secret label used to map certificate chains.
Enforce revocation check	Whether to enforce the checking of revocation entries from certificates. If you enable this setting, any attestation certificate's trust chain *must* have a CRL or OCSP entry that AM can verify. If you disable this setting, AM doesn't check presented certificates for revocation. **Note** Certificates downloaded from the FIDO Metadata Service might not have a CRL or OCSP entry. You must remove expired or revoked certificates manually.
Timeout	The number of seconds to wait for a response from an authenticator. If the specified time is reached, evaluation continues along the `Client error` outcome path and a relevant message is stored in the `WebAuthenticationDOMException` property of the shared state.
Limit registrations	Indicates whether the same authenticator can be registered multiple times. If you enable this property, the client won't activate an authenticator that's already registered for registration.

Property	Usage
Generate recovery codes	Indicates whether AM generates WebAuthn-specific recovery codes. If enabled, AM generates recovery codes and stores them in the transient state if registration is successful. Use the Recovery Code Display node to display the codes to the user for safe-keeping. Don't enable this property if you've enabled the **Store device data in transient state** property (and aren't saving the device data to the user's profile immediately). Enable the **Generate recovery codes** property in the WebAuthn Device Storage node instead. **Important** Generating recovery codes overwrites *all existing* WebAuthn-specific recovery codes. Only the most recent set of recovery codes can be used for authentication if a device has been lost or stolen.
Store data in transient state	If you enable this property, the node stores the following data in transient state: • Information provided by the device is stored in the `webauthnData` property for later analysis by subsequent nodes. • The attestation type achieved (`BASIC` , `CA` , or `SELF`) is stored in the `webauthnAttestationType` property. **Warning** The amount of data received from the device can be large. Only enable this option if you intend to analyze it.
Store device data in transient state	If you enable this property, information about the device required for WebAuthn is stored in transient state instead of saved immediately to the user's profile. Enable this option under the following conditions: • You've enabled the **Store data in transient state** property • You need to make decisions in scripts based on the outcome of the analysis of data in transient state • You don't want to register the device to the user until the analysis is complete **Important** Don't *change* the data while it's in transient state, nor when it's saved to a user's profile. Changing the device data will likely cause the device to be unable to authenticate. If you enable this option, use the WebAuthn Device Storage node to write the device data to the user's profile. If this option is disabled, device data is written automatically to the user's profile when registration is successful.

Property	Usage
Username to device	This option specifies that the device should store the user's username. If you enable this option, devices that don't support storing and providing the username won't be able to use this node. If the device can't store or provide usernames, the node fails and the journey follows the Failure outcome. You can find information on using this property for usernameless authentication with ForgeRock Go in Configure usernameless authentication with ForgeRock Go.
Shared state attribute for display name	The share state property that contains a display name for the user. For example, their full name, or email address. When **Username to device** is enabled, AM writes the value stored in this property to devices in addition to the username. This helps the user select between the accounts they may have on their devices. If you don't set this property, or if the variable isn't found in shared state, the username is used. You can find information on using this property for usernameless authentication with ForgeRock Go in Configure usernameless authentication with ForgeRock Go.
Return challenge as JavaScript	Choose how the node should return its challenge for consumption by your front-end user interface: ***PingOne Advanced Identity Cloud hosted pages or Ping SDK client apps:*** Deselect this option when using either hosted pages in PingOne Advanced Identity Cloud or a client application built using the Ping SDKs as your authentication user interface. When not enabled the node returns the challenge and associated data in a metadata callback. PingOne Advanced Identity Cloud hosted pages and Ping SDK client apps that might not be able to execute JavaScript use the information from the callback to interact with WebAuthn APIs on AM's behalf. ***PingAM User UI:*** You should only enable this option if you are using the PingAM User UI to authenticate users. Enabling this option causes the node to return its challenge as a fully encapsulated client-side JavaScript that interacts directly with the WebAuthn API.

Property	Usage
Maximum Saved Devices	The maximum number of WebAuthn devices that can be stored in the user's profile. Set this property to `0` if you don't want to limit the number of devices. When this property is greater than zero, the `Exceed Device Limit` outcome path becomes available. **Important** You can only limit the number of devices stored in the user's profile. If you enable **Store device data in transient state**, the node can't limit the number of devices and the `Exceed Device Limit` outcome path isn't displayed. In this case, specify the maximum number of saved devices in the WebAuthn Device Storage node.
Validate FIDO-U2F attestation AAGUID	If enabled, the node validates the Authenticator Attestation Global Unique Identifier (AAGUID) for any FIDO-U2F attestation type. The AAGUID must be 16 bytes, initialized with all zeros.
FIDO Certification Level	The minimum FIDO certification level that the device's certification status must satisfy during a registration flow. If this setting is `Off` (the default), AM doesn't check the metadata service for the device's certification level. Other options include: • `Self Assertion Submitted`: Use this setting if your authenticator has been submitted for FIDO certification but has not yet been certified. • `FIDO Certified L1` - `FIDO Certified L3+`: Find information on these levels in Certified Authenticator Levels. **Note** You must configure the WebAuthn Metadata service for the realm to enforce a FIDO certification check.

Outputs

- The node passes the contents of the `webAuthnExtensions` property to the browser or authenticator.
- If a timeout is reached, or any other client error occurs, the error type and description are added to the `WebAuthenticationDOMException` shared state property.
- If **Shared state attribute for display name** is set, the node writes the username or display name to shared state as a value of the specified property.
- If **Store data in transient state** is set, the node writes the following data to transient state on successful registration:
  - Information provided by the device is stored in the `webauthnData` property.
  - The attestation type achieved is stored in the `webauthnAttestationType` property.

- The registered Authenticator Attestation Global Unique Identifier (AAGUID) is stored in the `webauthnDeviceAaguid` property.
- PingAM Additional attestation information is stored in the `webauthnAttestationInfo` object.

  The `webauthnAttestationInfo` object includes the following information:

```
{
  "authenticatorAttachment": "platform",
  "flags": {
    "UP": true,
    "UV": true,
    "ED": false,
    "AT": false,
    "BE": true,
    "BS": true
  }
}
```

  The `authenticatorAttachment` field is added only if **Return challenge as JavaScript** is enabled. This field lets the journey identify whether the end user registered a roaming (cross-platform) device or a client-bound (platform) device. Learn more in Authenticator Attachment Modality in the WebAuthn specification.

  The `flags` provide additional information about the authenticator. Learn more about these flags in Authenticator Data in the WebAuthn specification.

Outcomes

Unsupported

If the user's client doesn't support WebAuthn, evaluation continues along the `Unsupported` outcome path. For example, clients connected over the HTTP protocol rather than HTTPS don't support WebAuthn.

Success

If the user successfully registers an authenticator of the correct type as determined by the node's properties, evaluation continues along the `Success` outcome path.

Failure

If AM encounters an issue when attempting to register a user's device, evaluation continues along the `Failure` outcome path. For example, if AM can't verify that the response from the authenticator was appropriate for the specific instance of the authentication ceremony.

Client Error

If the user's client encounters an issue when attempting to register using a device, for example, if the timeout was reached, evaluation continues along the `Client Error` outcome path. The node follows this outcome whenever the client throws a `DOMException`, as required by the WebAuthn specification.

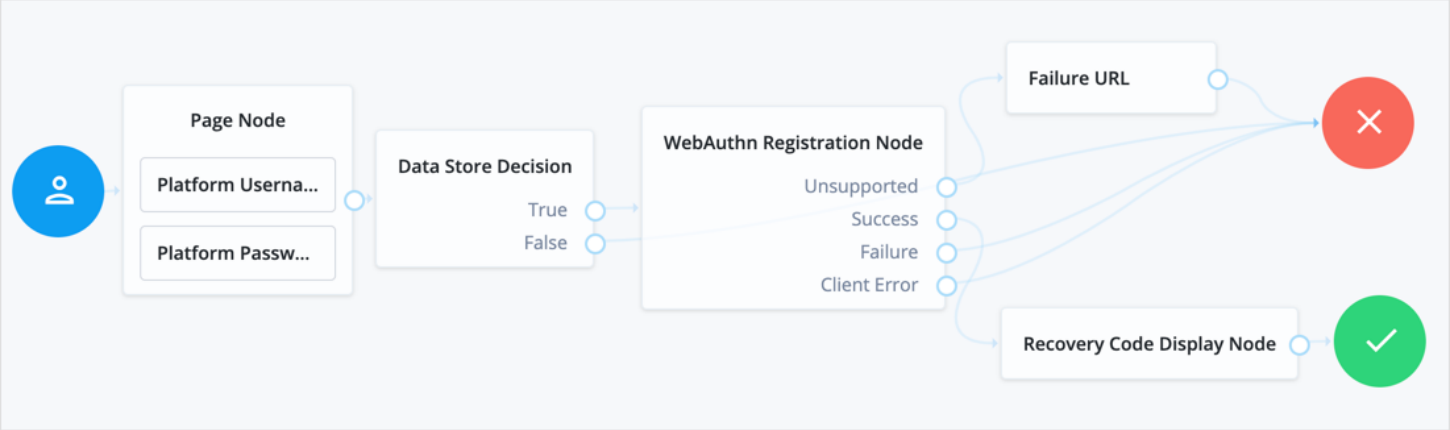
> **Tip**
>
> If a client error occurs, the error type and description are added to the `WebAuthenticationDOMException` shared state property. If required, this property can be read by nodes later in the journey.

Exceed Device Limit

If the **Maximum Saved Devices** property is an integer greater than zero, and registering a new device would take the number of devices above the specified threshold, evaluation continues down the `Exceed Device Limit` outcome path. In this case, you might need to instruct users to log in with an existing device to remove one or more of their registered devices.

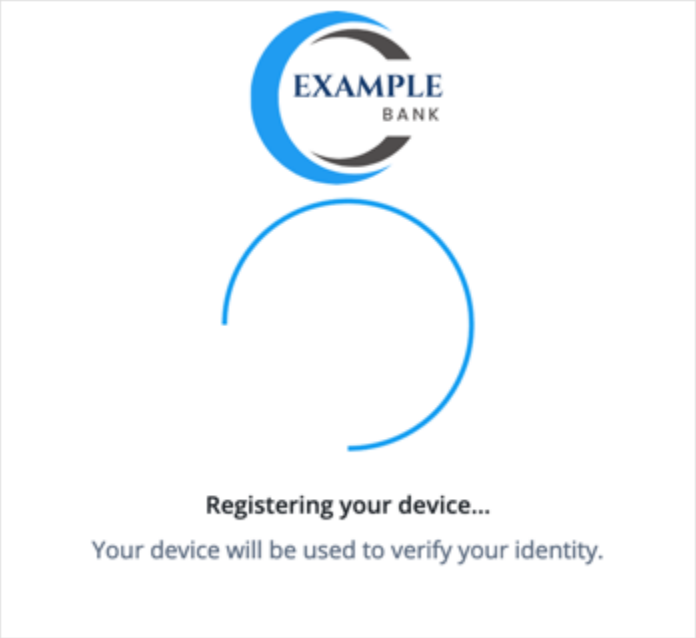
Example

The following sample journey registers WebAuthn devices:



If the user's client doesn't support WebAuthn, the failure URL is altered, for example to redirect the user to a page explaining which clients and operating systems support WebAuthn.

If the user's client does support WebAuthn, and the connection is secured with TLS, AM prompts the user to register an authenticator:



The user's browser may present a consent pop-up to allow access to the authenticators available on the client. When consent has been granted, the browser activates the relevant authenticators, ready for registration.

> **Tip**
>
> The relying party details configured in the node are often included in the consent message to help the user verify the entity requesting access.

The authenticators the client activates for registration depend on the value of the properties in the node. For example, if the **User verification requirement** property is set to `REQUIRED`, the client would not activate a USB hardware security key for registration.

When the user completes an authorization gesture, for example, by scanning a fingerprint or entering a PIN, the evaluation continues along the `Success` outcome path, and in this example will be taken to their profile page.

The registered authenticator appears on the user's dashboard page, with the label *New Security Key*. To rename the authenticator, click its vertical ellipsis context icon, ⋮, and click Rename.

Any problems encountered during the registration, including a timeout, results in the evaluation continuing to the `Failure` outcome.

Risk management nodes

Account Active Decision node

The **Account Active Decision** node determines whether the current account is both active and unlocked, and lets the journey make a decision, based on that check.

An account is considered locked under these conditions:

- The status is inactive.
- The status is active and a duration lockout is set on the account.

An account is considered unlocked under this condition:

- The status is active and no duration lockout is set on the account.

The node determines whether the account has been locked through both persistent (physical) lockout and duration lockout. Learn more in Account lockout for trees.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

Dependencies

This node has no dependencies.

Configuration

This node has no configurable properties.

Outputs

This node doesn't write anything to the shared state.

Outcomes

- `True`

  The journey follows this outcome path if the account is assessed to be `active` and `unlocked`.

- `False`

  The journey follows this outcome path if the account is assessed to be `inactive` or `locked`.

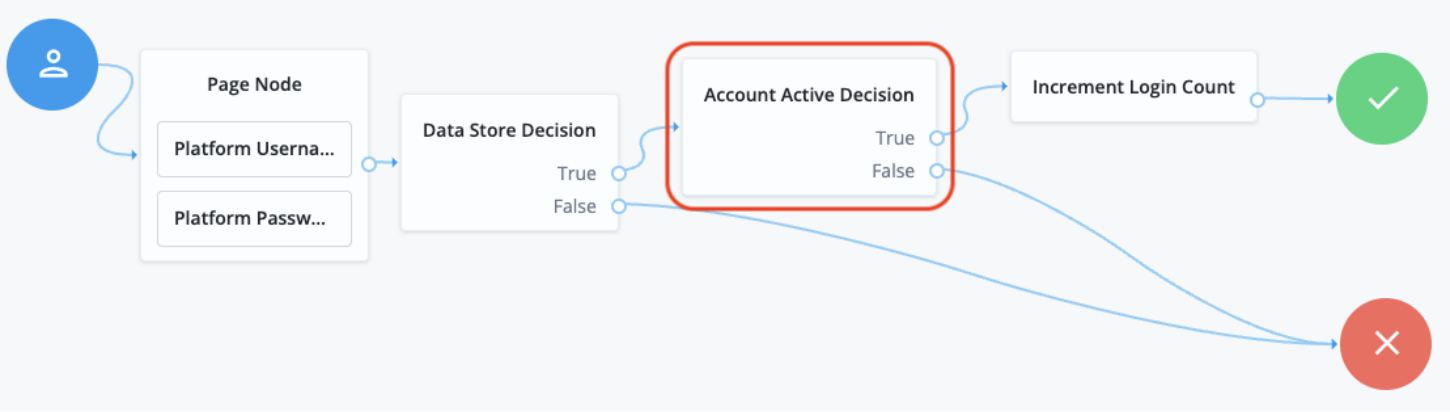
Errors

If the node cannot read the identity of the account, it throws the following exception:

`Failed to get the identity object`

Examples

In this simple login journey, authentication fails if the account is assessed to be `inactive` or `locked`.



This example uses the following nodes:

- The Page node prompts the user to input their username and password:
  - The Platform Username node collects the username and stores it in the shared state.
  - The Platform Password node collects the password and stores it in the shared state.
- The Data Store Decision node uses the username and password to determine whether the account exists.
- The **Account Active Decision** node determines whether the account is active and unlocked.

- If the account is active and unlocked, the Increment Login Count node increments the login count and authentication succeeds.
- If the account is inactive or locked, the authentication fails.

Account Lockout node

The **Account Lockout** node locks or unlocks the authenticating user's account profile.

The node also determines whether the account has been locked through both persistent (physical) lockout and duration lockout. Learn more in Account lockout for trees.

> **Tip**
>
> You can also use the Account Active Decision node to check whether the account is locked at any point in the journey.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

It also requires the `realm` property, which AM sets by default.

Dependencies

This node depends on the underlying identity service that stores the user profile.

Configuration

Property	Usage
Lock Action	Choose whether to `LOCK` or `UNLOCK` the authenticating user's account profile.

Outputs

This node does not change the shared node state.

Outcomes

Single outcome path; the node updates the account status according to the configured **Lock Action**:

`LOCK`

The account is inactive and the user cannot authenticate.

`UNLOCK`

The account is active and the user can authenticate.

Errors

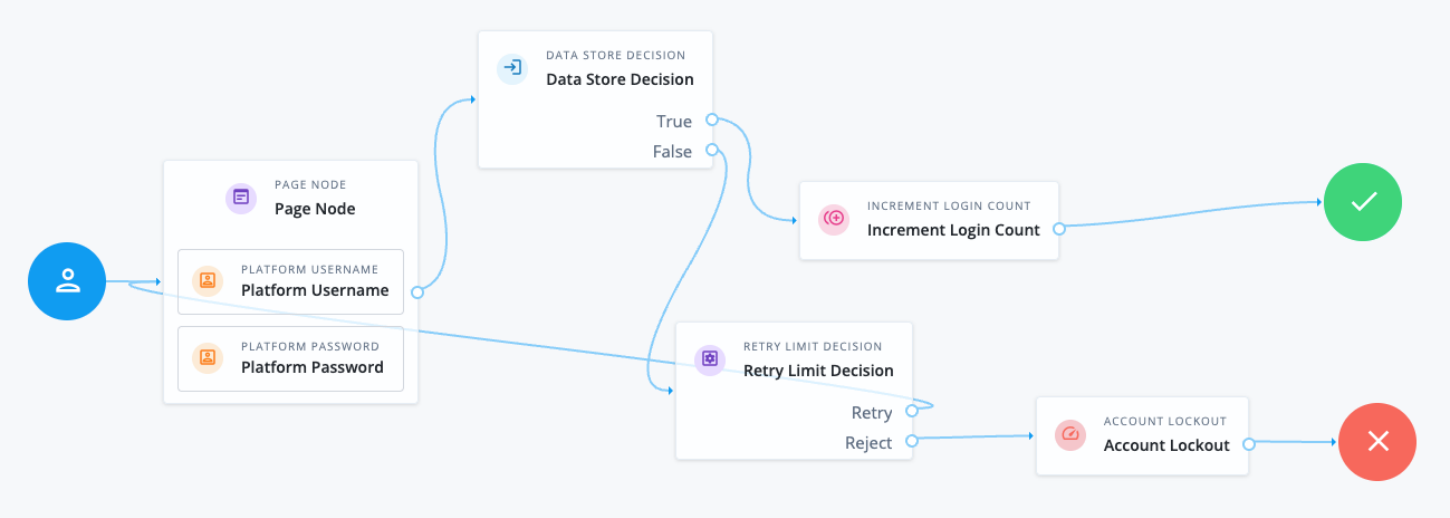
If this node fails to set the account status, it logs a `failed to set the user status inactive` warning.

This node can also throw exceptions with the following messages:

Message	Notes
`Could not get a valid username from the context`	Failed to read the `username` from the shared node state
`Could not get a valid realm from the context`	Failed to read the `realm` from the shared node state
`Could not find the identity based on the information available on context`	Failed to find the account profile with this `username` in this `realm`
`An error occurred when trying to lock out the user account`	Failed to update the account status; applies when locking and unlocking the account

Example

The following simple example uses this node with the Retry Limit Decision node to lock an account after the set number of invalid attempts:



The Retry Limit Decision node **Retry limit** (default: 3) defines the number of failed attempts before lockout.

Before using a journey like this in deployment, adapt it to reset the retry count on successful authentication.

Auth Level Decision node

Compares the current authentication level value against a configured value.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Sufficient Authentication Level	Evaluation continues along the `True` path if the current authentication level is equal to or greater than this integer; otherwise, the evaluation continues along the `False` path.

CAPTCHA node

The **CAPTCHA** node adds CAPTCHA support by verifying the response token received from the CAPTCHA provider and creating a callback for the UI to interact with.

By default, the node is configured for Google's reCAPTCHA v2.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

> **Note**
> This node only supports reCAPTCHA v2 and v3, and hCaptcha.
> For Google reCAPTCHA Enterprise support, use the reCAPTCHA Enterprise node.

Inputs

None. This node doesn't read shared state data.

Dependencies

You need to sign up for access to the reCAPTCHA API to get the API key pair required for configuring the node.

Configuration

Property	Usage
CAPTCHA Site Key *(required)*	The CAPTCHA site key supplied by the CAPTCHA provider when you sign up for access to the API.
CAPTCHA Secret Key	The CAPTCHA secret key supplied by the CAPTCHA provider when you sign up for access to the API. **Important** This property is deprecated and will be removed in a future release. Use the **CAPTCHA Secret Label Identifier** instead. If you set a **CAPTCHA Secret Label Identifier** and AM finds a matching secret in a secret store, the **CAPTCHA Secret Key** is ignored.

Property	Usage
CAPTCHA Secret Label Identifier	An identifier used to create a *secret label* for mapping to a secret in a secret store. AM uses this identifier to create a specific secret label for this node. The secret label takes the form `am.authentication.nodes.captcha.identifier.secret` where identifier is the value of **CAPTCHA Secret Label Identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period. If you set a **CAPTCHA Secret Label Identifier** and AM finds a matching secret in a secret store, the **CAPTCHA Secret Key** is ignored.
CAPTCHA Verification URL	The URL used to verify the CAPTCHA submission. Possible values are: • Google: `https://www.google.com/recaptcha/api/siteverify` • hCaptcha: `https://hcaptcha.com/siteverify`
CAPTCHA API URL *(required)*	The URL of the JavaScript that loads the CAPTCHA widget. Possible values are: • Google: `https://www.google.com/recaptcha/api.js` • hCaptcha: `https://hcaptcha.com/1/api.js`
Class of CAPTCHA HTML Element	The class of the HTML element required by the CAPTCHA widget. Possible values are: • Google: `g-recaptcha` • hCaptcha: `h-captcha`
ReCaptcha V3 node	If you're using Google reCAPTCHA, specify whether it's v2 or v3. Turn on for v3.
Score Threshold	If you're using Google reCAPTCHA v3 or hCaptcha, enter a score threshold. The CAPTCHA provider returns a score for each user request, based on observed interaction with your site. CAPTCHA "learns" by observing real site traffic, so scores in a staging environment or in a production deployment that has just been implemented might not be very accurate. A score of 1.0 is likely a good user interaction, while 0.0 is likely to be a bot. The threshold you set here determines whether to allow or deny access, based on the score returned by the CAPTCHA provider. Start with a threshold of 0.5. Learn more about score thresholds in the Google documentation.
Disable submission until verified	If selected, form submission is disabled until CAPTCHA verification succeeds. Default: Enabled

Outputs

None.

Outcomes

`True`

The CAPTCHA response was successfully verified.

`False`

The CAPTCHA response wasn't verified or failed verification.

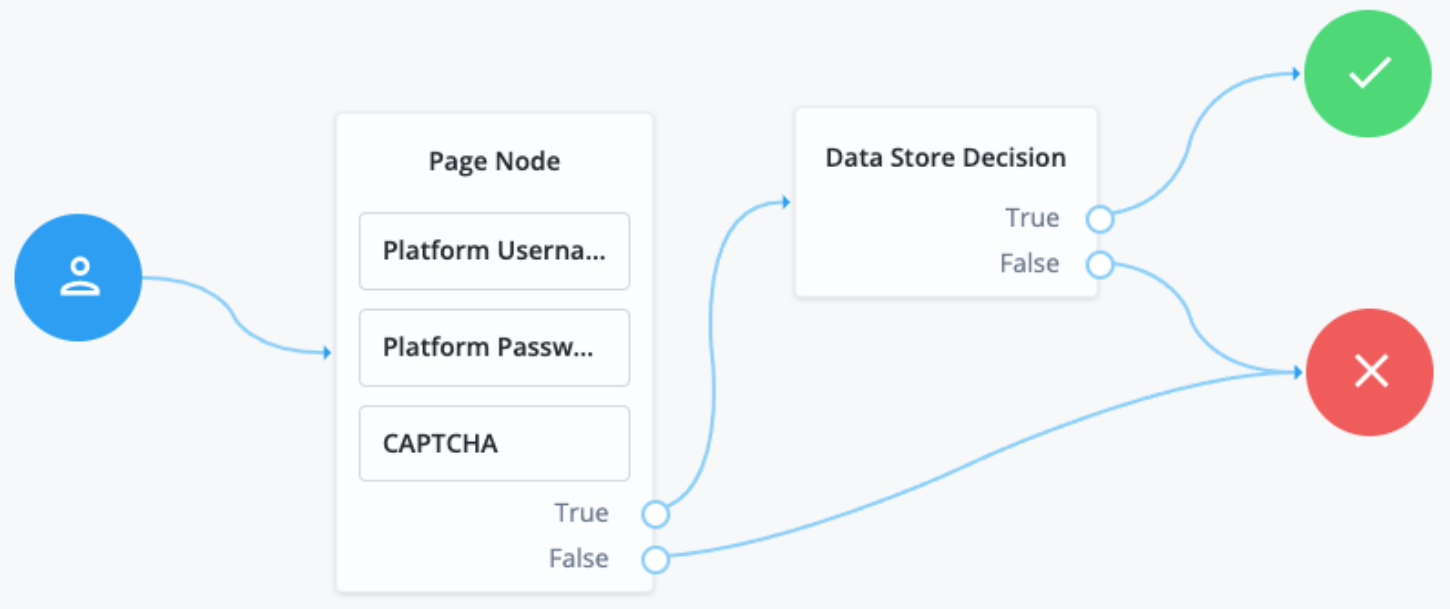
Errors

This node can throw exceptions with the following messages:

- `CAPTCHA response required for verification`
- `Unable to verify CAPTCHA response`
- `Unable to retrieve state from token response`
- `No secret key found`

Example

The following journey uses a Page node and a Data Store Decision node to collect and verify the credentials and a CAPTCHA response:



This example uses the following nodes:

- The Page node prompts the user to input their username and password:
  - The Platform Username node collects the username and stores it in the shared state.
  - The Platform Password node collects the password and stores it in the shared state.
  - The CAPTCHA node collects and verifies the CAPTCHA response.
- The Data Store Decision node uses the username and password to determine whether authentication is successful.

reCAPTCHA Enterprise node

The **reCAPTCHA Enterprise** node adds Google reCAPTCHA Enterprise support to your journeys.

Google reCAPTCHA Enterprise offers improvements over previous versions, including more granular scores, reason codes for events deemed higher risk, Web Application Firewall (WAF) support, and native support for Android and iOS.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

- Only the Ping SDKs support the reCAPTCHA Enterprise functionality this node provides.

  The following user interfaces do not support this node:
  - PingOne Advanced Identity Cloud hosted pages
  - PingAM User UI
- This node only supports Google reCAPTCHA Enterprise.

  For reCAPTCHA v2 and v3 support, and hCaptcha support, use the CAPTCHA node.

Inputs

This node reads an optional `CaptchaEnterpriseNode.PAYLOAD` variable from shared state.

Use this variable to customize the payload the node sends to the Google reCAPTCHA Enterprise server for assessment.

You can set the value by using a Set State node, or by using a Scripted Decision node, using a script similar to the following:

```
var username = nodeState.get("username");
var customPayload =
  JSON.parse(`{"userInfo": {"accountId": "${username}"}}`);
sharedState.put("CaptchaEnterpriseNode.PAYLOAD", customPayload);
outcome = "true";
```

To learn more about the payload, refer to Project Assessments - Event in the Google Developer documentation.

Dependencies

You need to sign up for access to the reCAPTCHA API to get the API key pair required to configure the node.

Configuration

Property	Usage
Google Cloud project ID	The ID of the project that has Google reCAPTCHA enabled. You can get the ID of your project in the Google Cloud console. For example, `my-project-65746-07969469388`.
reCAPTCHA Site Key *(required)*	The ID of the reCAPTCHA key you created in the Google Cloud console. The key can be for any platform type, `Website`, `Android app`, or `iOS app`. Sometimes referred to as a *key ID* in the Google Cloud console and documentation.
reCAPTCHA API key secret identifier	An identifier used to create a secret label for mapping to your Google reCAPTCHA API key in a secret store. Get or create your API key from the **Google Cloud Console** under **APIs and Services > Credentials**. The secret label takes the form `am.authentication.nodes.captchaEnterprise.identifier.secret` where identifier is the value of **reCAPTCHA API key secret identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period.
Score Threshold	The score threshold for determining if a user is likely to be a real person. reCAPTCHA scores are between `0.0` and `1.0`, with higher scores indicating higher confidence that the user is a real person. If the returned score is equal to or greater than the threshold the journey continues along the `true` outcome path. To learn more, refer to Interpret scores in the Google documentation.
Store reCAPTCHA assessment JSON	Stores the assessment response JSON for future reference within the journey. The node stores the JSON response in the `CaptchaEnterpriseNode.ASSESSMENT_RESULT` variable.

Property	Usage
Store reCAPTCHA error messages	Stores the error messages for future reference within the journey. The node stores the error messages in the `CaptchaEnterpriseNode.FAILURE` variable. The error consists of an error code and description of the error. • `INVALID_TOKEN` • `INVALID_PROJECT_ID` • `CLIENT_ERROR` • `INVALID_SECRET_KEY` • `VALIDATION_ERROR` • `API_ERROR` • `IO_ERROR` • `UNKNOWN`
reCAPTCHA CSS class	A CSS class to apply to the HTML elements reCAPTCHA adds to JavaScript apps. The default is `g-recaptcha`.
reCAPTCHA Verification URL	The URL to send the reCAPTCHA to for verification. Only change this if Google updates the URL used for reCAPTCHA verifications. The default is `https://recaptchaenterprise.googleapis.com/v1`.
JavaScript reCAPTCHA API URL	The URL of the JavaScript file containing the reCAPTCHA API. Only change this if Google releases a new version of the JavaScript reCAPTCHA API. The default is `https://www.google.com/recaptcha/enterprise.js`.

Outputs

If you enable the **Store reCAPTCHA assessment JSON** property, the node outputs the reCAPTCHA assessment response JSON in a state variable named `CaptchaEnterpriseNode.ASSESSMENT_RESULT`.

If you enable the **Store reCAPTCHA error messages** property, the node outputs the error response JSON in a state variable named `CaptchaEnterpriseNode.FAILURE`.

Outcomes

`True`

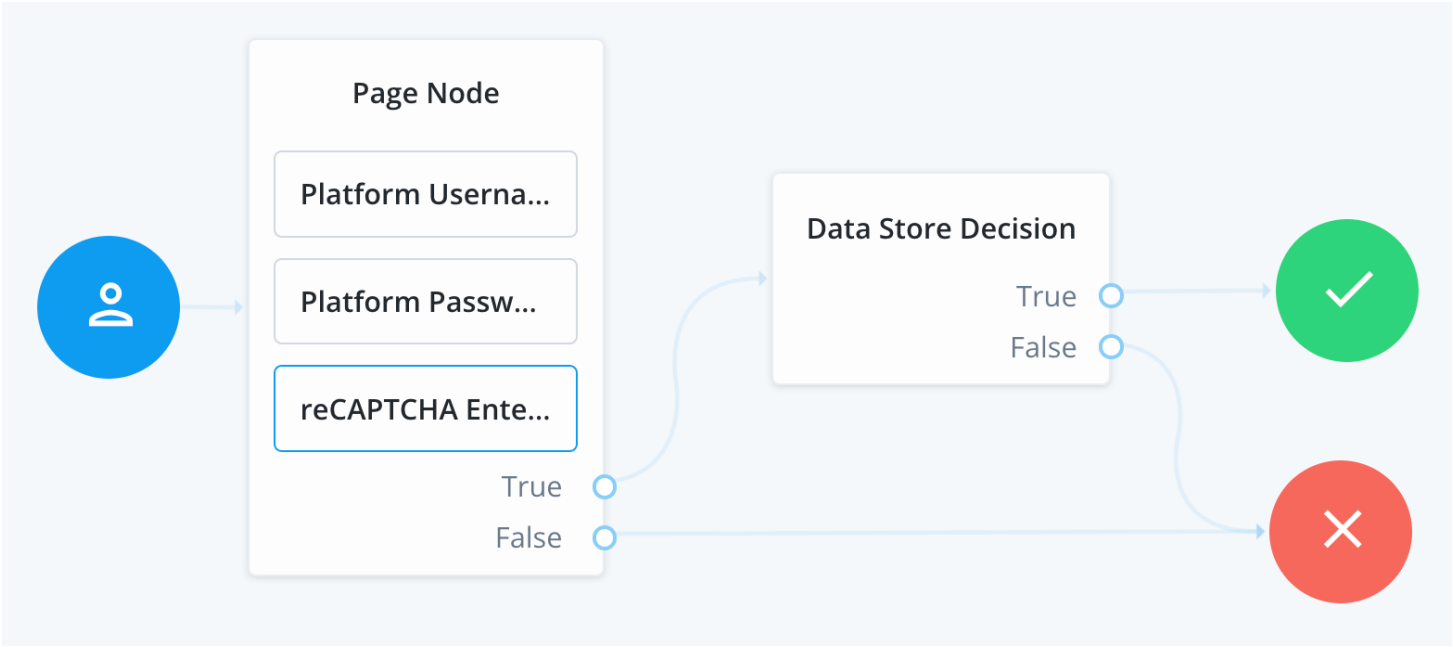
The reCAPTCHA response was successfully verified.

`False`

The reCAPTCHA response wasn't verified or failed verification.

Example

The following journey uses a Page node and a Data Store Decision node to collect and verify the credentials and a CAPTCHA response:



This example uses the following nodes:

- The Page node prompts the user to input their username and password:
  - The Platform Username node collects the username and stores it in the shared state.
  - The Platform Password node collects the password and stores it in the shared state.
  - The reCAPTCHA Enterprise node collects and verifies the reCAPTCHA Enterprise response.
- The Data Store Decision node uses the username and password to determine successful authentication.

Legacy CAPTCHA node

Verifies the response token received from the CAPTCHA verifier, and creates a CAPTCHA callback for the UI to interact with. Default values are for Google ReCAPTCHA.

Important

This node has been superseded by the CAPTCHA node. Use that node instead.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True` *(success)*
- `False` *(failure)*

Properties

Property	Usage
CAPTCHA Site Key *(required)*	The CAPTCHA site key supplied by the CAPTCHA provider when you sign up for access to the API.
CAPTCHA Secret Key *(required)*	The CAPTCHA secret key supplied by the CAPTCHA provider when you sign up for access to the API.
CAPTCHA Verification URL *(required)*	The URL used to verify the CAPTCHA submission. Possible values are: • Google: `https://www.google.com/recaptcha/api/siteverify` • hCaptcha: `https://hcaptcha.com/siteverify`
CAPTCHA API URL *(required)*	The URL of the JavaScript that loads the CAPTCHA widget. Possible values are: • Google: `https://www.google.com/recaptcha/api.js` • hCaptcha: `https://hcaptcha.com/1/api.js`
Class of CAPTCHA HTML Element	The class of the HTML element required by the CAPTCHA widget. Possible values are: • Google: `g-recaptcha` • hCaptcha: `h-captcha`

Modify Auth Level node

Increases or decreases the current authentication level value.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Value To Add	Enter a positive integer to increase the current authentication level, or a negative integer to decrease the current authentication level by the specified value.

PingOne Protect Evaluation node

The **PingOne Protect Evaluation** node contacts PingOne to calculate the risk level and other risk-related details associated with an event.

Depending on how you configure your risk policies in PingOne, the response could return a risk score, a risk level such as high, medium, or low, and recommended actions to take, such as mitigation against bots.

Learn more in PingOne Protect > How it Works.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node can use shared state variables that contain the PingOne `user.id` and `user.name` as input. If these are not available, the node uses the `UserId` and `Username` variables.

This node requires that you've initialized PingOne Protect in your client application. For example, by using a PingOne Protect Initialization node node previously in the journey or by initializing the SDK within the app itself.

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can connect to your PingOne instance and send it the necessary data to make risk evaluations.

The client application must be using Ping SDK 4.4.0 or later.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Target App ID	(Optional) If the user is attempting to access a PingOne application through the journey, add its v4 UUID client ID. This correlates the authentication with the application in PingOne, allowing you to filter by the **Resource Id** that matches the entered Target App ID when viewing the audit log in PingOne. For example, `12345678-abcd-4567-abcd-a123b123c123`.
Risk Policy Set ID	The ID of the risk policy in PingOne. To view risk policies in the PingOne admin console, go to **Threat Protection** > **Risk Policies**. If not specified, the environment's default risk policy set is used.
Flow Type	The type of flow or event for which the risk evaluation is being carried out. Choose from: **`REGISTRATION`** Initial registration of an account. **`AUTHENTICATION`** Standard authentication for login or actions such as password change. **`ACCESS`** Verification of whether the user can access the relevant application. **`AUTHORIZATION`** Verification of whether the user is authorized to perform a specific action such as a profile change. **`TRANSACTION`** Authentication carried out in the context of a purchase or other one-time transaction. The default is `AUTHENTICATION`.

Property	Usage
Device Sharing Type	Whether the device is shared between users or not. Choose from: • `UNSPECIFIED` • `SHARED` • `PRIVATE` The default is `SHARED`.
User Type	The type of user associated with the event. Choose from: **`PING_ONE`** User exists within the PingOne environment. **`EXTERNAL`** User exists outside PingOne, such as a federated user. The default is `EXTERNAL`.
Score Threshold	Scoring higher than this value results in evaluation continuing along the `Exceeds Score Threshold` outcome. The default is `300`.
Recommended Actions	A list of recommended actions the risk evaluation could return. Each entry in the list becomes a node outcome. If the evaluation score does not exceed the **Score Threshold** value, and a recommended action is present in the response from PingOne Protect, the journey continues down the matching entry in this list. Possible values are: **`BOT_MITIGATION`** PingOne suspects the client could be automated or a bot. You should route the journey to a CAPTCHA node or similar next step to mitigate against bots. **`AITM_MITIGATION`** PingOne suspects an adversary-in-the-middle (AitM) attack. You should route the journey to the failure node, and consider locking the account, and force a password change to mitigate against these attacks.
Pause Behavioral Data	After receiving the device signal, instruct the client to pause collecting behavioral data. Default: Selected
Node State Attribute For User ID	The node state variable that contains the `user.id` as it appears in PingOne. If left blank, the node uses the current context `UserId` as the `user.id`.
Node State Attribute For Username	The node state variable that contains the `user.name` as it appears in PingOne. If left blank, the node uses the current context `Username` as the `user.name`.

Property	Usage
Store Risk Evaluation	Stores the risk evaluation response in the transient node state under a key named `PingOneProtectEvaluationNode.RISK`. The default is not enabled. **Note** The key is empty if the node is unable to retrieve a risk evaluation from PingOne.

Outputs

If you enable the **Store Risk Evaluation** property, the node outputs the risk evaluation response JSON in a state variable named `PingOneProtectEvaluationNode.RISK`.

Outcomes

`High`

The risk evaluation level is considered high.

`Medium`

The risk evaluation level is considered medium.

`Low`

The risk evaluation level is considered low.

`Exceeds Score Threshold`

The score returned is higher than the configured threshold.

`Failure`

The risk evaluation could not be completed.

Recommended Actions

The risk evaluation recommended a mitigation action to take, and it matched a value in the **Recommended Actions** list.

Currently, the only value possible is `BOT_MITIGATION`, which recommends you check for the presence of a human, such as by using a CAPTCHA node.

`ClientError`

The client returned an error when attempting to capture the data to perform a risk evaluation.

Outcome precedence

Evaluation of the journey continues along an outcome based on the response received and which fields are present in it, as follows:

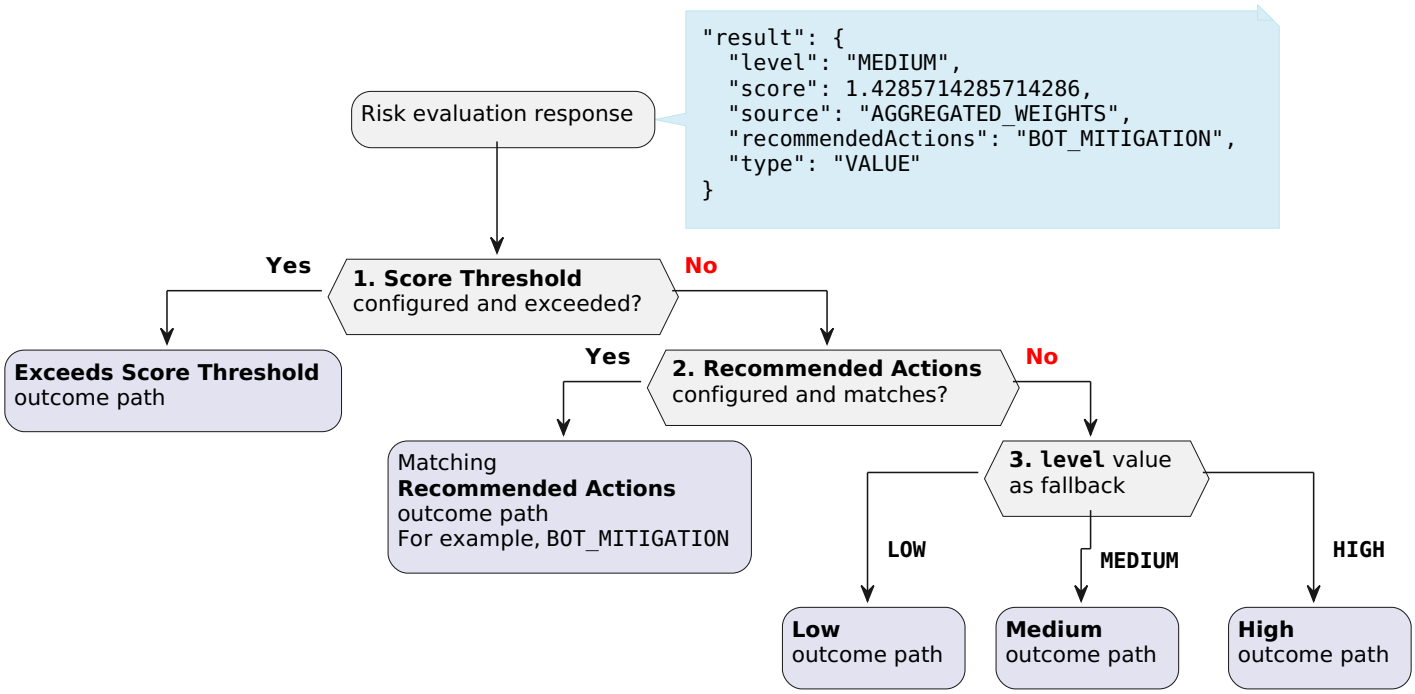


Figure 1. Risk evaluation outcome path precedence

1. If you have configured the **Score Threshold** property and the result contains a score that exceeds it, evaluation continues along the `Exceeds Score Threshold` outcome path.
2. If you have *not* configured the **Score Threshold** property, or the score does not exceed it, but *have* added a value in the **Recommended Actions** list that matches one in the response, evaluation continues along the relevant dynamic outcome path. For example, the `BOT_MITIGATION` outcome path.
3. If you have *not* configured the **Score Threshold** property, or the score does not exceed it, and have *not* added a matching value in the **Recommended Actions** list, then evaluation continues along the relevant `level` path, one of `Low`, `Medium`, or `High`.

Example

The following example journey leverages PingOne Protect functionality to perform a risk evaluation on a client app. The client app is built using the Ping SDKs.

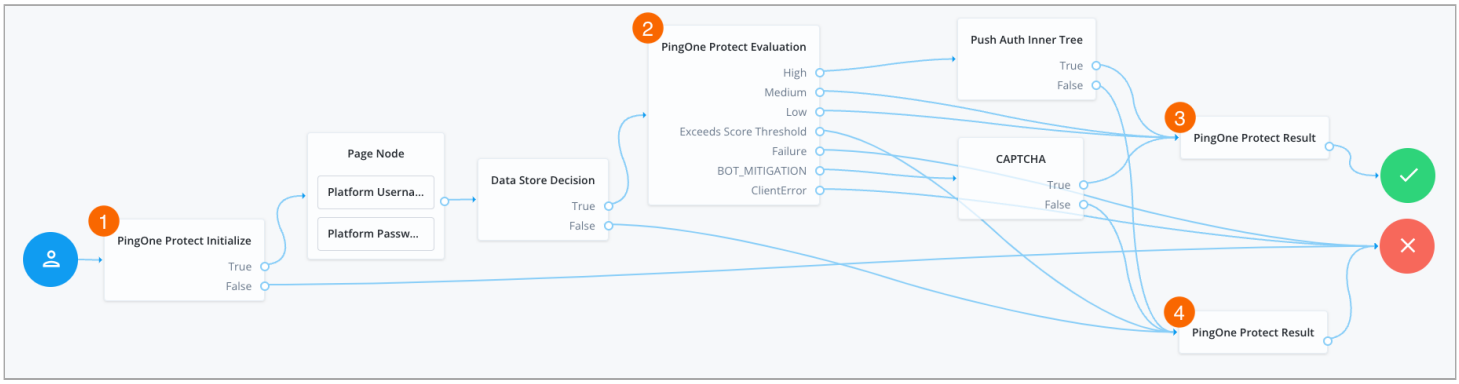


Figure 2. Example PingOne Protect journey

- 1 The PingOne Protect Initialization node instructs the SDK to initialize the PingOne Protect Signals API with the configured properties.

> **Tip**
>
> Initialize the PingOne Protect Signals API as early in the journey as possible, before any user interaction. This enables it to gather sufficient contextual data to make an informed risk evaluation.

- The user enters their credentials, which are verified against the identity store.
- 2 The PingOne Protect Evaluation node performs a risk evaluation against a risk policy in PingOne.

The example journey continues depending on the outcome:

`High`

The journey requests that the user respond to a push notification.

`Medium` *or* `Low`

The risk is not significant, so no further authentication factors are required.

`Exceeds Score Threshold`

The score returned is higher than the configured threshold and is considered too risky to complete successfully.

`Failure`

The risk evaluation could not be completed, so the authentication attempt continues to the **Failure** node.

`BOT_MITIGATION`

The risk evaluation returned a recommended action to check for the presence of a human, so the journey continues to a CAPTCHA node.

`AITM_MITIGATION`

The risk evaluation returned a recommended action regarding the possible presence of an adversary-in-the-middle attack, so the journey continues to the Failure node.

`ClientError`

The client returned an error when attempting to capture the data to perform a risk evaluation, so the authentication attempt continues to the **Failure** node.

- 3 An instance of the PingOne Protect Result node returns the `Success` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.
- 4 A second instance of the PingOne Protect Result node returns the `Failed` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.

PingOne Protect Initialization node

The **PingOne Protect Initialization** node instructs the SDK to initialize the embedded PingOne Protect SDK on the client device using the configuration provided by the node properties.

Learn more in Threat Protection using PingOne Protect.

You can only initialize the PingOne Protect SDK on the client device once. Attempting to initialize the SDK with a different configuration will not override the initial settings.

> **Tip**
>
> You should initialize the PingOne Protect SDK on the client device as early as possible so that it can gather sufficient contextual information to make risk evaluations.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node has no required predecessor nodes.

It does not read from the shared node state.

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can connect to your PingOne instance and send it the necessary data to make risk evaluations as part of the journey.

You can find information on the properties used by the service in PingOne Worker service.

The client application must be using Ping SDK 4.4.0 or later.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Enable SDK Logs	When enabled, output SDK log messages in the developer console. Default: Disabled
Device Attributes To Ignore	A list of device attributes you want to exclude from the results when collecting device signals. These attributes will not be sent to PingOne to perform evaluations, which might limit its ability to create accurate results. Some examples of attributes the client might obtain from the device include: • `BATTERY_LEVEL` • `CPU_ARCHITECTURE` • `DEVICE_MODEL` • `DEVICE_VENDOR` • `GPS_SUPPORTED` • `HAS_CHROME_APP` • `IS_ACCEPT_COOKIES` • `NAVIGATOR_USER_AGENT` • `OS_NAME` • `OS_VERSION` • `RESOLUTION` • `TOUCH_SUPPORT` **Note** The attributes collected vary depending on the OS of the client. For example, an Android device might provide different attributes to a JavaScript app running on Windows.
Custom Host	Deprecated. We recommend that you do not change this property.
Lazy Metadata	When enabled, calculate metadata on demand. When not enabled, metadata is calculated automatically after initialization. Default: Disabled
Collect Behavioral Data	When enabled, collect behavioral data. When not enabled, behavioral data is not collected. Default: Enabled
Disable Hub	When selected, the client stores device data in the browser's `localStorage` only. When not selected, an iframe is used. Default: Not selected

Property	Usage
Device Key Rsync Intervals (days)	Number of days that device attestation can rely upon the device fallback key. Default: `14`
Enable Trust	Tie the device payload to a non-extractable crypto key stored in the browser for content authenticity verification
Disable Tags	When selected, the client does not collect tag data. Tags are used to record the pages the user visited, forming a browsing history. Default: Not selected

Outputs

The node sends a `PingOneProtectInitializeCallback` to the client application.

The Ping SDKs consume this callback and initialize the PingOne Protect functionality so it can start gathering the data it needs to make risk evaluations.

Outcomes

`True`

The client application confirmed successful receipt of the configuration.

`False`

The client application did not confirm successful receipt of the configuration or returned a client error.

Example

The following example journey leverages PingOne Protect functionality to perform a risk evaluation on a client app. The client app is built using the Ping SDKs.

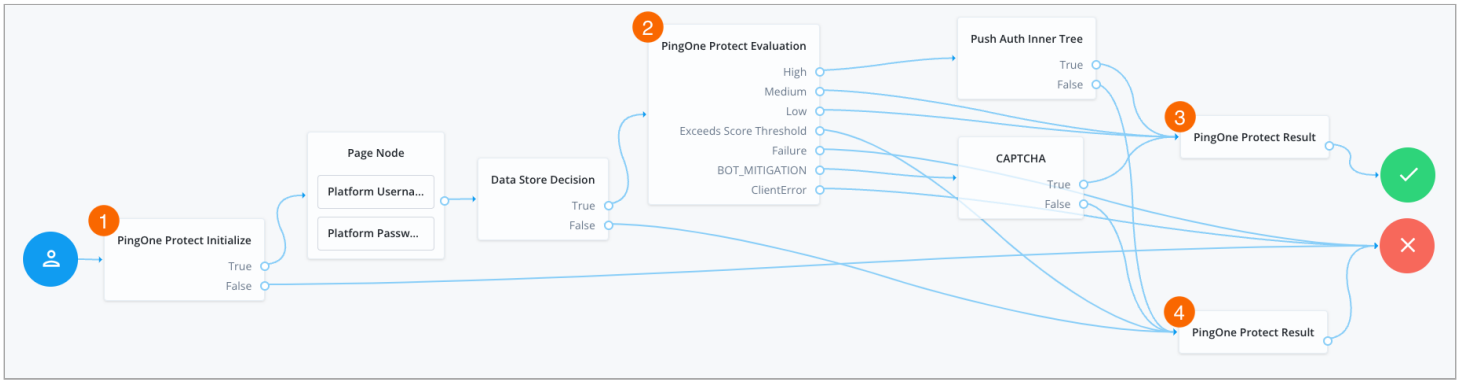


Figure 1. Example PingOne Protect journey

- 1 The PingOne Protect Initialization node instructs the SDK to initialize the PingOne Protect Signals API with the configured properties.

> **Tip**
>
> Initialize the PingOne Protect Signals API as early in the journey as possible, before any user interaction. This enables it to gather sufficient contextual data to make an informed risk evaluation.

- The user enters their credentials, which are verified against the identity store.
- 2 The PingOne Protect Evaluation node performs a risk evaluation against a risk policy in PingOne.

The example journey continues depending on the outcome:

`High`

The journey requests that the user respond to a push notification.

`Medium` *or* `Low`

The risk is not significant, so no further authentication factors are required.

`Exceeds Score Threshold`

The score returned is higher than the configured threshold and is considered too risky to complete successfully.

`Failure`

The risk evaluation could not be completed, so the authentication attempt continues to the **Failure** node.

`BOT_MITIGATION`

The risk evaluation returned a recommended action to check for the presence of a human, so the journey continues to a CAPTCHA node.

`AITM_MITIGATION`

The risk evaluation returned a recommended action regarding the possible presence of an adversary-in-the-middle attack, so the journey continues to the Failure node.

`ClientError`

The client returned an error when attempting to capture the data to perform a risk evaluation, so the authentication attempt continues to the **Failure** node.

- 3 An instance of the PingOne Protect Result node returns the `Success` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.
- 4 A second instance of the PingOne Protect Result node returns the `Failed` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.

PingOne Protect Result node

The **PingOne Protect Result** node updates the risk evaluation configuration or modifies the completion status of the resource while the risk evaluation is still in progress.

You can check the results of the evaluation in the PingOne admin console by filtering for `Risk Evaluation Updated` event types.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires that you've initialized PingOne Protect in your client application. For example, by using a PingOne Protect Evaluation node previously in the journey or by initializing the SDK within the app itself.

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can connect to your PingOne instance and send it the necessary data to make risk evaluations as part of the journey.

Configuration

Property	Usage
Completion Status	Report the status of the journey back to PingOne. Choose from: • `FAILED` • `SUCCESS`

Outputs

This node does not change the shared node state.

Outcomes

Single outcome path.

The node attempts to update the PingOne server but continues along the single outcome without confirming the server received the update.

Example

The following example journey leverages PingOne Protect functionality to perform a risk evaluation on a client app. The client app is built using the Ping SDKs.

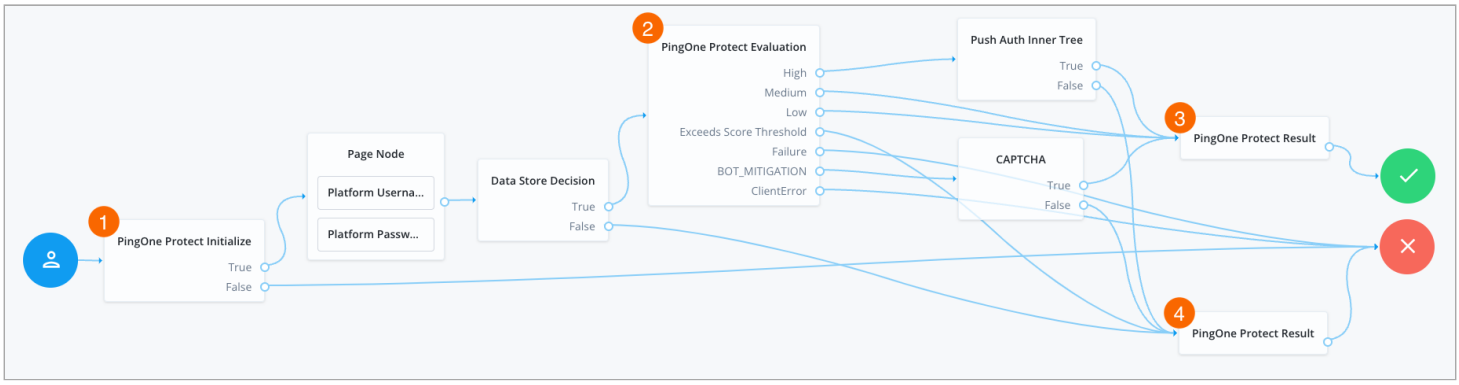


Figure 1. Example PingOne Protect journey

- 1 The PingOne Protect Initialization node instructs the SDK to initialize the PingOne Protect Signals API with the configured properties.

> **Tip**
>
> Initialize the PingOne Protect Signals API as early in the journey as possible, before any user interaction. This enables it to gather sufficient contextual data to make an informed risk evaluation.

- The user enters their credentials, which are verified against the identity store.
- 2 The PingOne Protect Evaluation node performs a risk evaluation against a risk policy in PingOne.

The example journey continues depending on the outcome:

`High`

The journey requests that the user respond to a push notification.

`Medium` *or* `Low`

The risk is not significant, so no further authentication factors are required.

`Exceeds Score Threshold`

The score returned is higher than the configured threshold and is considered too risky to complete successfully.

`Failure`

The risk evaluation could not be completed, so the authentication attempt continues to the **Failure** node.

`BOT_MITIGATION`

The risk evaluation returned a recommended action to check for the presence of a human, so the journey continues to a CAPTCHA node.

`AITM_MITIGATION`

The risk evaluation returned a recommended action regarding the possible presence of an adversary-in-the-middle attack, so the journey continues to the Failure node.

`ClientError`

The client returned an error when attempting to capture the data to perform a risk evaluation, so the authentication attempt continues to the **Failure** node.

- 3 An instance of the PingOne Protect Result node returns the `Success` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.
- 4 A second instance of the PingOne Protect Result node returns the `Failed` result to PingOne, which can be viewed in the console to help with analysis and risk policy tuning.

Behavioral nodes

Increment Login Count node

The **Increment Login Count** node increments the successful login count property of a managed object.

Use the Login Count Decision node to change the flow of the journey based on the count.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node's **Identity Attribute** specifies the property it requires in the incoming node state. It uses this property to access the managed object.

Dependencies

This node depends on IDM to store the managed object.

Configuration

Property	Usage
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

This node does not change the shared node state.

Outcomes

Single outcome path; on success, this node increments the managed object's `loginCount`.

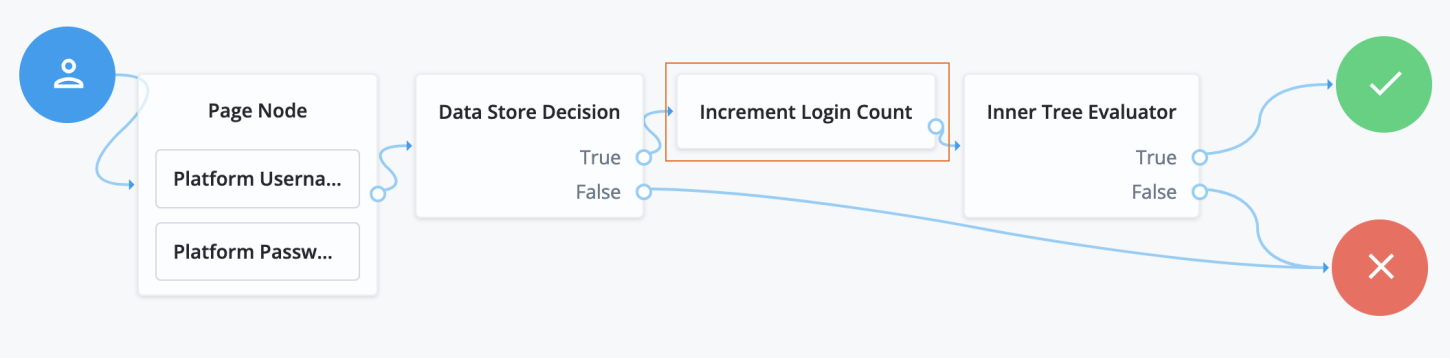
Errors

If this node fails to access the managed object, it throws an exception with a `No object to increment` message.

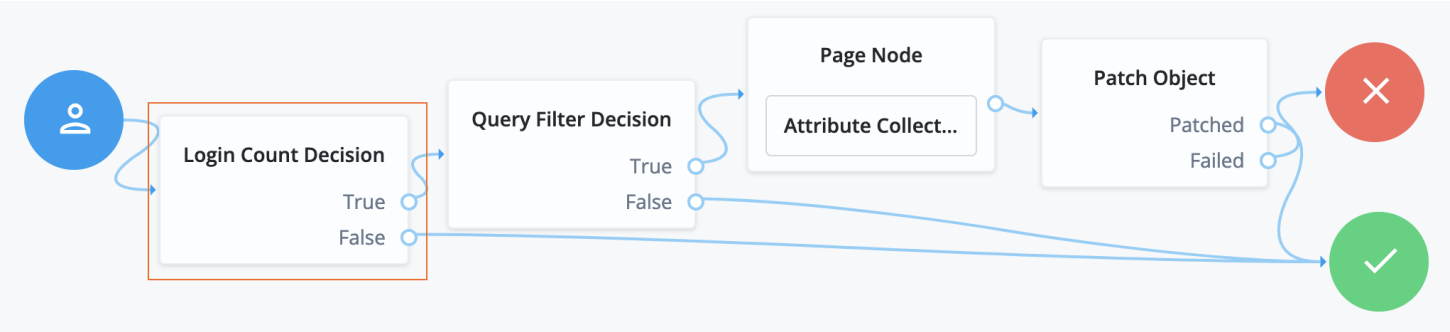
If this node fails to increment the login count, it logs an `Unable to increment login count` warning message.

Example

The following journey uses the Increment Login Count node to update the login count on successful authentication:



- The Platform Username node injects the `userName` into the shared node state.
- The Data Store Decision node determines whether authentication is successful.
- The Increment Login Count node (outlined in the image) updates the login count.
- The Inner Tree Evaluator node invokes the following nested journey for progressive profiling:



- The Login Count Decision node triggers the rest of the journey depending on the login count and its settings.
- The Query Filter Decision node determines whether managed object profile fields are still missing.

- The Page node requests additional input for the profile.
- The Patch Object node stores the additional input in the managed object profile.

Login Count Decision node

The **Login Count Decision** node triggers an action when a user's successful login count property reaches a specified number.

Use the Increment Login Count node to set the login count on successful authentication.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node's **Identity Attribute** specifies the property it requires in the incoming node state. It uses this property to access the managed object.

Dependencies

This node depends on IDM to store the managed object.

Configuration

Property	Usage
Interval	Trigger the `True` outcome depending on this setting, the **Amount**, and the login count: **AT** Proceed to `True` when the login count matches the **Amount** setting. **EVERY** Proceed to `True` every time the login count reaches a multiple of the **Amount** setting. Default: `AT`
Amount	The login count to trigger a `True` outcome depending on the **Interval**. Default: 25
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

This node does not change the shared node state.

Outcomes

`True`

The login count reached **Amount**, and the **Interval** setting triggered this outome.

`False`

All other cases.

Errors

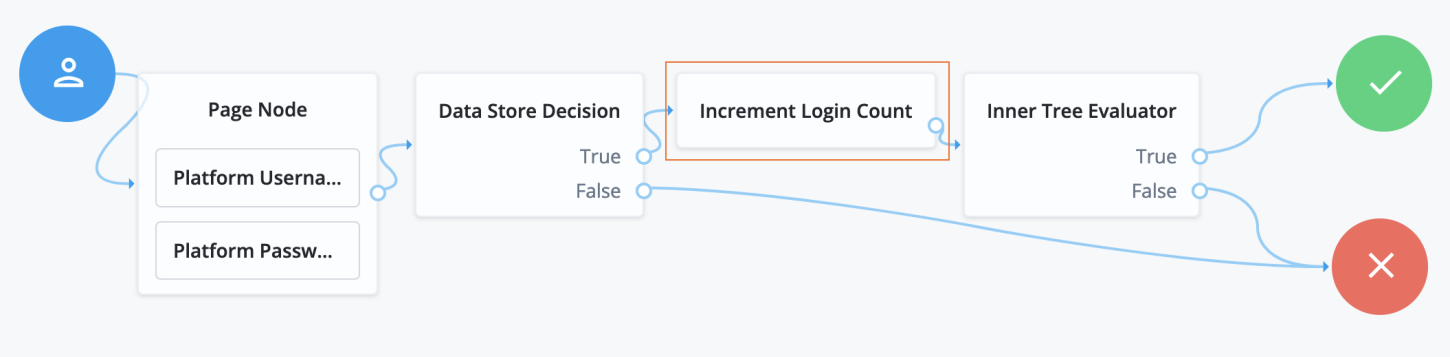
This node can throw exceptions with the following messages:

Message	Notes
`<Identity Attribute> not present in state`	Failed to read the specified **Identity Attribute** in the shared node state
`Failed to retrieve existing object`	Failed to find the managed object using the **Identity Attribute** value from the shared node state

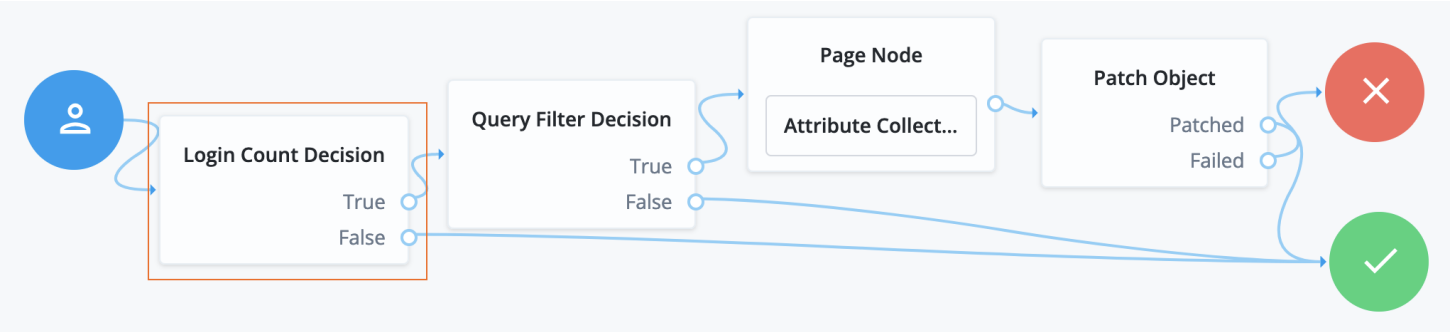
Message	Notes
`Retrieve login not found`	Failed to read the managed object's login count

Example

The following journey uses the Increment Login Count node to update the login count on successful authentication:



- The Platform Username node injects the `userName` into the shared node state.
- The Data Store Decision node determines whether authentication is successful.
- The Increment Login Count node (outlined in the image) updates the login count.
- The Inner Tree Evaluator node invokes the following nested journey for progressive profiling:



- The Login Count Decision node triggers the rest of the journey depending on the login count and its settings.
- The Query Filter Decision node determines whether managed object profile fields are still missing.
- The Page node requests additional input for the profile.
- The Patch Object node stores the additional input in the managed object profile.

Contextual nodes

Certificate Collector node

The **Certificate Collector** node collects an X.509 digital certificate from the request. The journey can use the collected certificate as authentication credentials for a user or OAuth 2.0 client.

PingAM accepts certificates in PEM and DER format.

PingOne Advanced Identity Cloud accepts certificates in DER format.

> **Note**
>
> You can't use this node in isolation because it only *collects* the certificate from the request. It doesn't extract or validate the certificate's content. Use a Certificate Validation node to validate the certificate and a Certificate User Extractor node to extract the user details from the certificate.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the certificate from the request payload or in a request header. It doesn't read anything from the shared state.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Certificate Collection Method	How the node should collect the certificate from the request. Possible values are: **`Request`** The node locates the certificate in the request. Use this option if TLS termination happens at AM. **`Header`** The node locates the certificate in an HTTP header. Specify the header name in the **HTTP Header Name for the Client Certificate** property. Use this option if TLS termination happens in a proxy or load balancer outside AM. **`Either`** The node attempts to locate the certificate in the request. If there's no certificate in the request, the node attempts to locate the certificate in the HTTP header specified in **HTTP Header Name for the Client Certificate**. Default: `Either`
HTTP Header Name for the Client Certificate	The name of the HTTP header that contains the certificate. If you set the **Certificate Collection Method** to `Header` or `Either`, you must set a value here. Default: No value
Trusted Remote Hosts	A list of IP addresses trusted to supply certificates on behalf of the authenticating client, such as load balancers doing TLS termination. If you don't set a value here, AM rejects certificates supplied by remote hosts. If you set a value of `any`, AM trusts certificates supplied by any remote host, on behalf of the authenticating client. Default: No value

Outcomes

`Collected`

The node was able to collect the certificate.

`Not Collected`

The node was unable to collect the certificate.

Outputs

The node outputs the X509 certificate to the transient state to be consumed by the Certificate Validation node.

Errors

- If no certificate is provided in the configured location (either header or request), the node logs the following error:

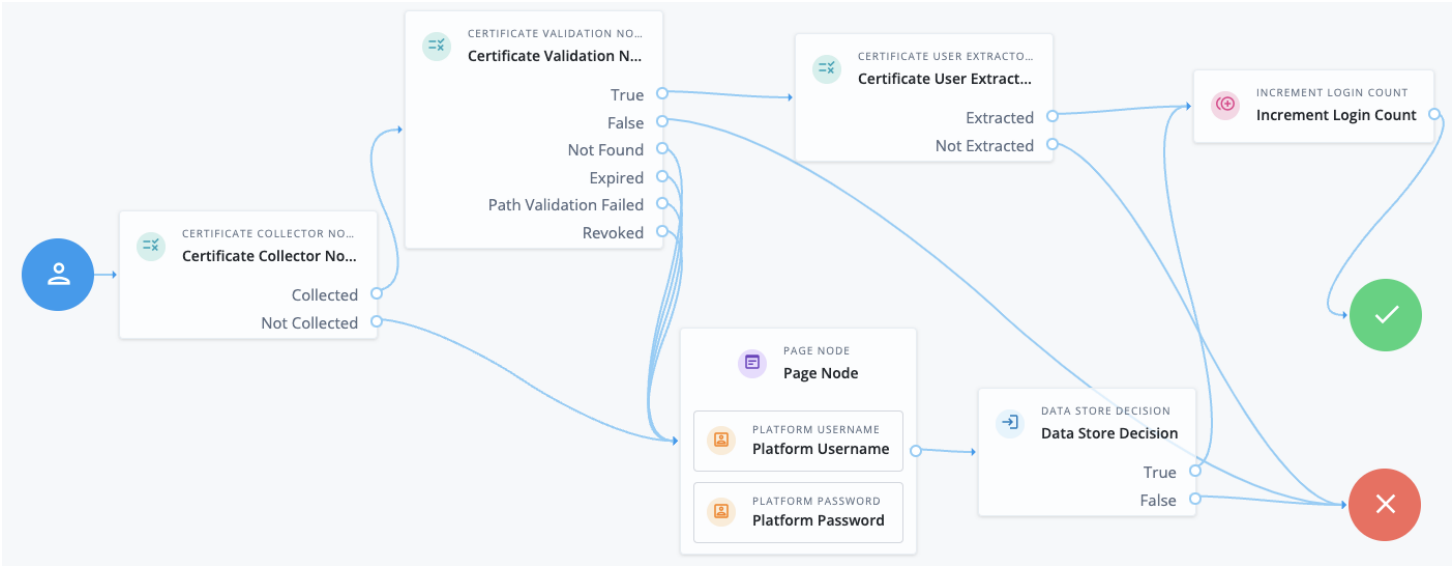
  `Certificate was not successfully collected based on node configuration and client request`

- If there's a problem with the certificate provided in the header or in the request, the node logs the following error:

  `CertificateFromParameter decode failed, possibly invalid Base64 input`

Example

This example shows an authentication journey using a certificate as credentials.



1. The **Certificate Collector** node attempts to collect the certificate from the request body or the header.
   - If the node can collect the certificate, the journey proceeds to the Certificate Validation node.
   - If the node can't collect the certificate, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
2. The **Certificate Validation** node attempts to validate the certificate based on the configuration of that node.
   - If the certificate can be validated, the journey proceeds to the Certificate User Extractor node.
   - If the certificate is invalid, the journey proceeds to the Failure node.
   - In all other cases, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
3. The **Certificate User Extractor** node extracts the user ID from the certificate and attempts to find a match in the identity store.
   - If the username can be extracted and a matching user is found in the identity store, the journey increments the login count and authenticates the user.

- If the username can't be extracted or no matching user is found in the identity store, the journey proceeds to the Failure node.

Certificate User Extractor node

The **Certificate User Extractor** node extracts an identifier from the certificate collected by the Certificate Collector node and searches for that identifier in the identity store. The purpose of this node is to match the collected certificate with a user in the identity store.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the value of the `X509Certificate` property from the transient state.

Implement the Certificate Collector node as input to this node to obtain the `X509Certificate`.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Certificate Field Used to Access User Profile	Specifies the field in the certificate that AM uses to search for the user in the identity store. Possible values are: • `Subject DN` • `Subject CN` • `Subject UID` • `Email Address` • `Other` • `None` If you select `Other`, provide an attribute name in the **Other Certificate Field Used to Access User Profile** property. Select `None` if you want to specify an alternate way of looking up the user profile in the **SubjectAltNameExt Value Type to Access User Profile** property. Default: `Subject CN`
Other Certificate Field Used to Access User Profile	Specifies a custom certificate field to use as the base of the user search.
SubjectAltNameExt Value Type to Access User Profile	Specifies how to look up the user profile: **None** AM uses the value specified in the **Certificate Field Used to Access User Profile** or the **Other Certificate Field Used to Access User Profile** properties when looking up the user profile. **RFC822Name** AM looks up the user profile using the value of the `RFC822Name` field. **UPN** AM looks up the user profile as the User Principal Name attribute used in Active Directory. Default: `None`

Outcomes

`Extracted`

The node extracted the user ID from the certificate and found a match in the identity store.

`Not Extracted`

The node couldn't extract the user ID from the certificate or couldn't match the ID to an identity in the identity store.

Outputs

If the node can extract a value from the certificate, that value is stored in the `username` key in the shared node state.

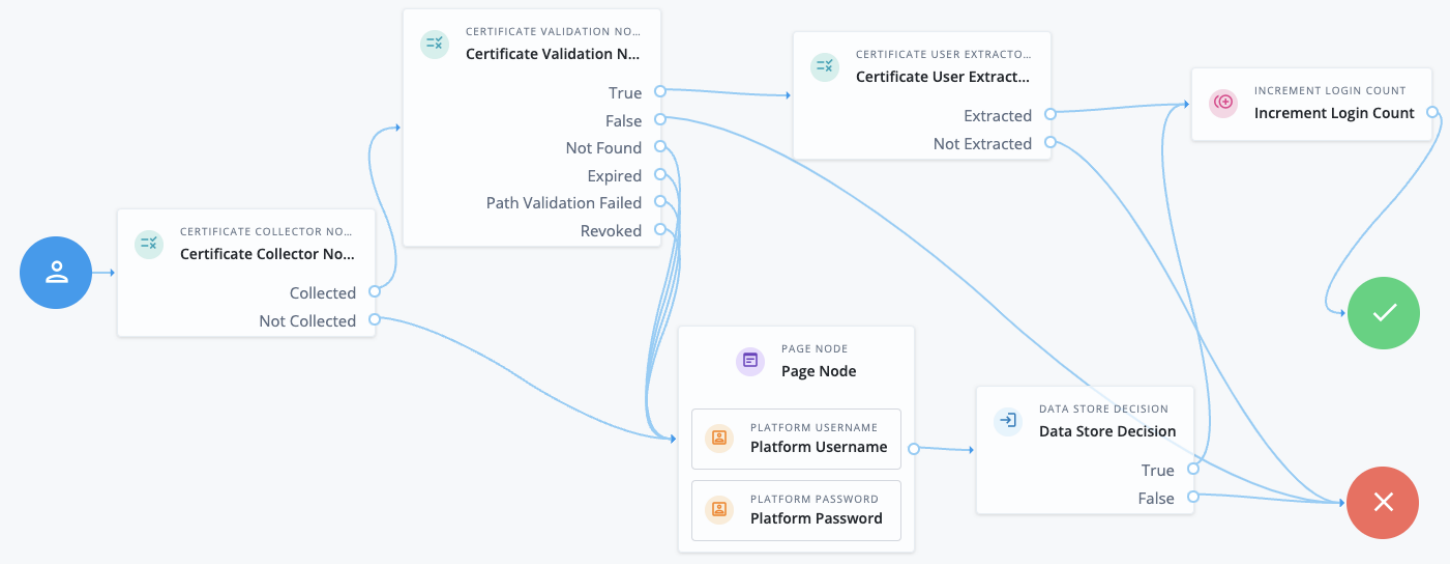
Errors

If the node can't extract the user ID from the certificate, it logs the following error:

```
Unable to parse user token ID from Certificate
```

Example

This example shows an authentication journey using a certificate as credentials.



1. The **Certificate Collector** node attempts to collect the certificate from the request body or the header.
    - If the node can collect the certificate, the journey proceeds to the Certificate Validation node.
    - If the node can't collect the certificate, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
2. The **Certificate Validation** node attempts to validate the certificate based on the configuration of that node.
    - If the certificate can be validated, the journey proceeds to the Certificate User Extractor node.
    - If the certificate is invalid, the journey proceeds to the Failure node.
    - In all other cases, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
3. The **Certificate User Extractor** node extracts the user ID from the certificate and attempts to find a match in the identity store.
    - If the username can be extracted and a matching user is found in the identity store, the journey increments the login count and authenticates the user.

- If the username can't be extracted or no matching user is found in the identity store, the journey proceeds to the Failure node.

Certificate Validation node

The **Certificate Validation** node validates a digital X.509 certificate collected by the Certificate Collector node.

Important

Certificate validation rules

- If you add this node to a journey, you *must* configure it. With no configuration, the node returns `True` as the outcome by default, regardless of the validity of the certificate provided in the journey.
- This node validates the *first* certificate in a certificate chain (the user certificate) and ignores the remaining certificates in the chain.
- If the collected user certificate is a self-signed certificate (test environments only), the self-signed user certificate must be present in the truststore for certificate validation to succeed.
- If the collected user certificate is signed by a valid issuer, the issuing certificates (intermediate, or intermediate and root) must be present in the truststore for certificate validation to succeed.
- If the user certificate is signed by a valid issuer and the issuing certificate (intermediate certificate) is *not* present in the truststore, certificate validation fails.
- The node uses the intermediate and user certificates to verify certificate revocation status.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires an `X509Certificate` property in the incoming node state.

Implement the Certificate Collector node as input to the Certificate Validation node.

Configuration

Property	Usage
Match Certificate in LDAP	When enabled, AM matches the collected certificate with a certificate stored in the identity store. Set the **Subject DN Attribute Used to Search LDAP for Certificates** to specify which LDAP property to search for certificate information. Default: Disabled
Check Certificate Expiration	When enabled, AM checks if the collected certificate has expired. Default: Disabled
Subject DN Attribute Used to Search LDAP for Certificates	The attribute AM uses to search the identity store for the certificate. The search filter is based on this attribute and the value of the Subject DN as it appears in the certificate. Default: `CN`
Match Certificate to CRL	When enabled, AM checks if the collected certificate has been revoked according to a Certificate Revocation List (CRL) in the identity store. Define related CRL properties later in the node configuration. Default: Disabled.
Issuer DN Attribute(s) Used to Search LDAP for CRLs	The name of the attribute or attributes in the issuer certificate that AM uses to locate the CRL in the identity store. • If you specify only one attribute here, the LDAP search filter used is `(attr-name=attr-value-in-subject-DN)`. For example, if the subject DN of the issuer certificate is `C=US, CN=Some CA, serialNumber=123456`, and the attribute specified is `CN`, AM uses a search filter of `(CN=Some CA)` to locate the CRL. • Specify several CRLs for the same CA issuer in a comma-separated list (`,`) where the names are in the same order in which they appear in the subject DN. In this case, the LDAP search filter used is `(attr1=attr1-value-in-subject-DN,attr2=attr2-value-in-subject-DN,…)`, and so on. For example, if the subject DN of the issuer certificate is `C=US, CN=Some CA, serialNumber=123456`, and the attributes specified are `CN,serialNumber`, the LDAP search filter used to find the CRL is `(CN=Some CA,serialNumber=123456)`. Default: `CN`
HTTP Parameters for CRL Update	Parameters AM includes in any HTTP CRL call to the CA that issued the certificate. If the client or CA certificate includes the `IssuingDistributionPoint` extension, AM uses this information to retrieve the CRL from the distribution point. Add the parameters as key-value pairs in a comma-separated list (`,`). For example, `param1=value1,param2=value2`.

Property	Usage
Cache CRLs in Memory	When enabled, AM caches CRLs in memory. If this option is enabled, **Update CA CRLs from CRLDistributionPoint** must also be enabled. Default: Enabled
Update CA CRLs from CRLDistributionPoint	When enabled, AM fetches new CA CRLs from the CRL Distribution Point and updates them in the identity store. If the CA certificate includes either the `IssuingDistributionPoint` or the `CRLDistributionPoint` extensions, AM attempts to update the CRLs when they're out of date. Default: Enabled
OCSP Validation	When enabled, AM checks the validity of certificates using the Online Certificate Status Protocol (OCSP). PingAM If you enable this option, the AM instance must be able to connect to the internet. You must also configure OCSP for AM under **Configure > Server Defaults > Security > Online Certificate Status Protocol Check**. Default: Disabled
Certificate Identity Store	PingAM Select the identity store (configured for the realm) that AM must search for certificates. If you select an identity store here, AM uses the connection details defined for that identity store and ignores all the server settings below this field. PingOne Advanced Identity Cloud Select the default identity store (`OpenDJ`) from the list. You *must* select this identity store to let AM search for the certificate. AM ignores all LDAP server settings below this field.
PingAM **LDAP Server Where Certificates are Stored**	The LDAP server that holds certificates. Enter the server details in the format `ldap-server:port` . To associate multiple AM servers in a site with corresponding LDAP servers, use the format `am_server|ldapserver:_port_` . For example, `am.example.com|ldap1.example.com:636` .
PingAM **LDAP Search Start or Base DN**	Valid base DN for the LDAP search, such as `dc=example,dc=com` . To associate AM servers with different search base DNs, use the format `am_server|base_dn` . For example, `am.example.com|dc=example,dc=com` `openam1.test.com|dc=test,dc=com` .
PingAM **LDAP Server Authentication User** and **LDAP Server Authentication Password**	The credentials used to connect to the LDAP directory that holds the certificates. If you enable mTLS, the node ignores these credentials. Default Authentication User: `cn=Directory Manager`

Property	Usage
PingAM **mTLS Enabled**	Enables mTLS (mutual TLS) between AM and the directory server. When mTLS is enabled, the node ignores the values for **LDAP Server Authentication User** and **LDAP Server Authentication Password**. If you enable this property, you must: • Enable **Use SSL/TLS for LDAP Access**. • Provide an **mTLS Secret Label Identifier**. Default: Disabled
PingAM **mTLS Secret Label Identifier**	An identifier used to create a secret label for mapping to the mTLS certificate in the secret store. AM uses this identifier to create a specific secret label for this node. The secret label takes the form `am.authentication.nodes.certificate.validation.mtls.identifier.cert`, where `identifier` is the value of **mTLS Secret Label Identifier**. The label can only contain alphanumeric characters (`a-z`, `A-Z`, `0-9`) and periods (`.`). It can't start or end with a period. For greater security, you should rotate certificates periodically. When you rotate a certificate, update the corresponding mapping in the realm secret store configuration to reflect this identifier. When you rotate a certificate, AM closes any existing connections using the old certificate. A new connection is selected from the connection pool and no server restart is required.
PingAM Use SSL/TLS for LDAP Access	When enabled, AM uses SSL/TLS to access the LDAP directory. Make sure that AM trusts the certificate from the LDAP server when enabling this option. Default: Disabled

Outputs

This node doesn't put anything into the shared state.

Outcomes

`True`

The node could validate the certificate.

When the outcome is `True`, add a Certificate User Extractor node to extract the values of the certificate.

`False`

The node couldn't validate the certificate. The journey follows this path when the node can't validate the certificate and no more specific outcome is available.

`Not found`

The **Match Certificate in LDAP** property is enabled, but the certificate wasn't found in the LDAP store.

`Expired`

The **Check Certificate Expiration** property is enabled, and the certificate has expired.

`Path Validation Failed`

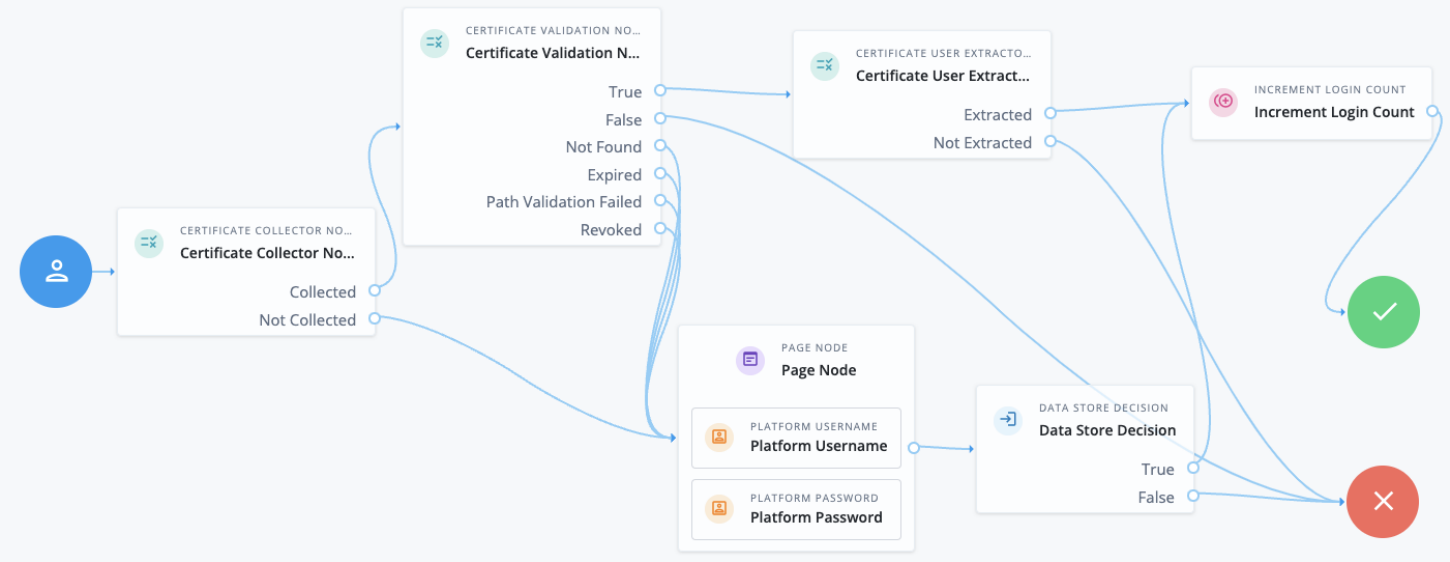
The **Match Certificate to CRL** property is enabled, and the certificate path is invalid.

Revoked

The **OCSP Validation** property is enabled, and the certificate has been revoked.

Example

This example shows an authentication journey using a certificate as credentials.



1. The **Certificate Collector** node attempts to collect the certificate from the request body or the header.
    - If the node can collect the certificate, the journey proceeds to the Certificate Validation node.
    - If the node can't collect the certificate, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
2. The **Certificate Validation** node attempts to validate the certificate based on the configuration of that node.
    - If the certificate can be validated, the journey proceeds to the Certificate User Extractor node.
    - If the certificate is invalid, the journey proceeds to the Failure node.
    - In all other cases, the journey proceeds to a Page node containing a Platform Username node and a Platform Password node to let the user authenticate with username/password credentials.
3. The **Certificate User Extractor** node extracts the user ID from the certificate and attempts to find a match in the identity store.
    - If the username can be extracted and a matching user is found in the identity store, the journey increments the login count and authenticates the user.

- If the username can't be extracted or no matching user is found in the identity store, the journey proceeds to the Failure node.

Cookie Presence Decision node

Checks that a named cookie is present in the incoming authentication request.

This node does not check the value of the named cookie, only that it exists.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Name of Cookie *(required)*	Evaluation continues along the `True` path if the named cookie is present in the incoming authentication request; otherwise, evaluation continues along the `False` path.

Device Geofencing node

Compares any collected device location metadata with the trusted locations configured in the authentication node.

Use this node with the Device Profile Collector node to determine if the authenticating user's device is located within range of configured, trusted locations.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Inside`
- `Outside`

Evaluation continues along the `Inside` path if the collected location is within the specified range of a configured trusted location; otherwise, evaluation continues along the `Outside` path.

Properties

Property	Usage
Trusted Locations *(required)*	Specify the latitude and longitude of at least one trusted location. Separate the values with a comma. For example, `37.7910855,-122.3951663`.
Geofence Radius (km)	Specifies the maximum distance, in kilometers, that a device can be from a configured trusted location. The distance is calculated point-to-point.

Device Location Match node

Compares any collected device location metadata with that stored in the user's profile.

Use this node with the Device Profile Collector node to determine if the authenticating user's device is located within range of somewhere they have authenticated from, and saved, previously.

You must establish the identity of the user before attempting to match locations.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`
- `Unknown Device`

Evaluation continues along the `True` path if the collected location is within the specified range of saved location data; otherwise, evaluation continues along the `False` path.

If the user has no saved device profiles or the identity of the user has not been established, evaluation continues along the `Unknown Device` path.

Properties

Property	Usage
Maximum Radius (km)	Specifies the maximum distance, in kilometers, that a device can be from a previously saved location. The distance is calculated point-to-point.

Device Match node

The **Device Match** node compares collected device metadata with that stored in the user's profile.

Use this node with the Device Profile Collector node to check whether the user is authenticating with a previously saved, trusted device.

The Device Match node supports the following methods of comparison:

- Built-in matching

  The node handles the comparison and matching. You configure the acceptable variance and the maximum age for device profiles.

- Custom matching

  Create scripts to compare captured device data against trusted device profiles.

  AM includes a customizable template script.

  In the AM admin UI, go to **Realms** > ***Realm Name*** > **Scripts**, and click **Device Profile Match Template - Decision Node Script**.

> **Tip**
>
> For a comprehensive sample script with instructions for its use and a development toolkit, go to the GitHub sample repository.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

This node also reads collected device metadata from the shared state. Implement a Device Profile Collector node earlier in the journey to collect metadata for the current device.

If **Use Custom Matching Script** is enabled, the inputs depend on the script.

Uniquely identify devices

The Device Match node looks up a user's stored device profiles using a device identifier as a key.

The client device generates a device identifier as part of the device profile that it returns to the Device Profile Collector node in the JSON payload.

For example:

```
{
  "identifier": "d50cdb5ce8d055a3-86bd35e1b975a14d76b40940112c2380264c8efd",
  ....
}
```

When can identifiers change?

If the identifier changes, the Device Match node can't match any stored device profiles.

If this happens, your journey must collect and store a new device profile that contains the new identifier.

This section explains what can cause an identifier to change on each platform.

Android

In Android, the instance ID is deleted or changes if any of the following occurs:

- An app is restored on a new device.
- The user uninstalls and reinstalls the app.
- The user clears app data.

iOS

On iOS, the device ID is stored in the Keychain. This means the ID persists when the app is removed.

However, the device ID is deleted or changes if any of the following occurs:

- The user wipes or factory resets the phone.
- The user migrates to a new phone.
- The keychain is programmatically deleted from the phone.
- The device ID is programmatically deleted from the Keychain.
- The keychain identifier in the `forgerock_keychain_access_group` configuration property changes.

JavaScript

In JavaScript, the device ID is deleted or changes if any of the following occurs:

- The browser window creates the device ID while in "private" or "incognito" mode. Closing the browser removes the ID.
- The browser removes the ID when cleaning up old data to accommodate new data.
- The browser is uninstalled and reinstalled. The ID is removed.
- The user removes the device ID by clearing the browser data.

Dependencies

If **Use Custom Matching Script** is enabled, the dependencies depend on the script.

Configuration

Property	Usage
Acceptable Variance	The maximum number of acceptable device attribute differences for a match. Default: `0` (all attributes must match)
Expiration	The maximum age in days a saved profile is valid for comparison. The node ignores older device profiles saved to the user's account when comparing device profiles with the collected metadata. Default: `30` (days)
Use Custom Matching Script	Enable this option to use a custom script instead of built-in matching to compare the collected metadata with saved device profiles. When enabled, the node ignores the **Acceptable Variance** and **Expiration** settings. The script type must be `Decision node script for authentication trees` (standalone AM) or `Journey Decision Node` (Ping Identity Platform deployment). Default: false
Custom Matching Script	Select the custom script to use when **Use Custom Matching Script** is enabled. Only scripts of type `Decision node script for authentication trees` (standalone AM) or `Journey Decision Node` (Ping Identity Platform deployment) appear in the list. Default: `Authentication Tree Decision Node Script`

Outputs

This node does not change the shared state on its own.

If the node uses a **Custom Matching Script**, the output is determined by the script.

Outcomes

`True`

The collected device metadata matches a saved profile within the configured variance.

`False`

The collected device metadata doesn't match a saved profile, or another error occurred.

`Unknown Device`

The journey follows this outcome path in the following situations:

- The user has no saved trusted device profiles.
- The user identity hasn't yet been established.
- The acceptable device variance matches, but the device ID no longer matches.

Errors

This node logs the following warning messages:

`script outcome error`

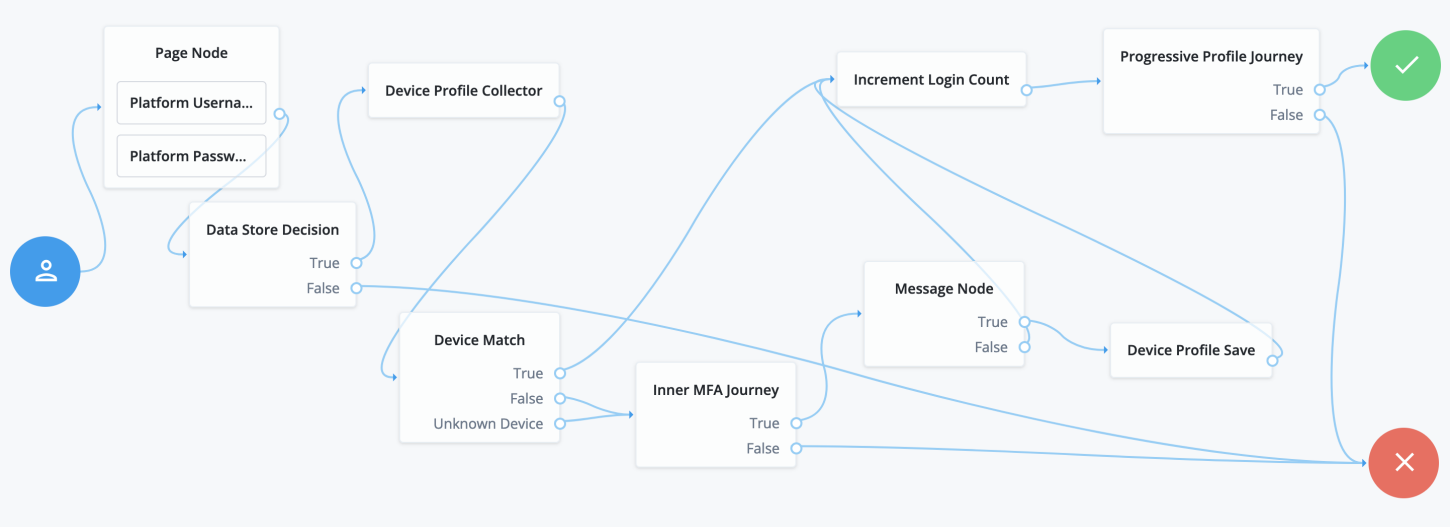
The script failed to set the `outcome` field to a string.

`error evaluating the script`

The script failed to complete. Refer to the logs for details.

Example

The following journey authenticates the user and checks whether the current device is trusted. If the device isn't trusted yet, the journey requires an additional authentication factor and lets the user opt to trust the device:



- The Page node with the Platform Username node and Platform Password node prompt the user for their credentials.
- The Data Store Decision node confirms the user's credentials.
- The Device Profile Collector node collects metadata about the current device.
- The **Device Match** node compares saved device profiles with the current device.
- The **Inner MFA Journey**, an Inner Tree Evaluator node, requires an additional authentication factor.
- The Message node prompts the user with an option to trust the current device.
- The Device Profile Save node saves the current device profile.
- The Increment Login Count node updates the number of successful authentications.
- The **Progressive Profile Journey**, an Inner Tree Evaluator node, invokes a journey to collect additional profile data.

Device Profile Collector node

Gathers metadata about the device used to authenticate.

The node sends a `DeviceProfileCallback` callback. Learn more in Interactive callbacks.

When used with the Ping SDKs, the node can collect the following:

Device Metadata

Information such as the platform, versions, device name, hardware information, and the brand of the device being used.

The captured data is in JSON format, and stored in the authentication shared state in a variable named `forgeRock.device.profile`.

Device Location

Provides the last known latitude and longitude of the device's location.

The captured data is in JSON format, and stored in the authentication shared state in a variable named `forgeRock.device.location`.

The collection of geographical information requires end-user approval. A browser function drives this process. A pop-up displays, prompting for access to share the geographical location. The browser connection must be secure.

Important

It is up to you what information you collect from users and devices.
Always use data responsibly and provide your users with appropriate control over data they share with you.
You are responsible for complying with any regulations or data protection laws.

In addition to the collected metadata, an `identifier` string in the JSON uniquely identifies the device.

Use this node with the Device Profile Save node to create a trusted profile from the collected data. You can use the trusted device profile in subsequent authentication attempts; for example, with the Device Match node and Device Location Match node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Maximum Profile Size (KB)	Specifies the maximum accepted size, in kilobytes, of a device profile. If the collected profile data exceeds this size, authentication fails. Default: `3`
Collect Device Metadata	Specifies whether device metadata is requested.
Collect Device Location	Specifies whether device location is requested.
Message	Specifies an optional message to display to the user while the node collects the requested data. You can provide the message in multiple languages by specifying the locale in the `KEY` field. For example, `en-US`. The locale selected for display is based on the user's locale settings in their browser. Messages provided in the node override the defaults provided by AM.

Device Profile Save node

Persists collected device data to a user's profile in the identity store.

Use this node with the Device Profile Collector node to reuse the collected data in future authentications; for example, with the Device Match node and Device Location Match node.

You must establish the identity of the user before attempting to save to their profile.

A user profile can contain multiple device profiles. Use the **Maximum Saved Profiles** property to configure the maximum number of device profiles to persist per user. Saving a device profile with the same identifier as an existing entry overwrites the original record, and does not increment the device profile count.

In a Ping Identity Platform deployment, the end user UI displays saved device profiles to end users.

In an AM standalone deployment, the PingAM UI **does not** display saved device profiles to end users.

You can manage device profiles over REST, by using the `/json/users/user/devices/profile` endpoint for the realm.

Use the AM API Explorer for detailed information about the parameters supported by the `/devices/profile` endpoint and to test it against your deployed AM instance.

In the AM admin UI, select the **Help** icon, and then go to **API Explorer > /users > /{user} > /devices > /profile**.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Device Name Variable	Specifies the name of a variable in the shared node state that contains an alias label for the device profile.
Maximum Saved Profiles	Specify the maximum number of device profiles to save in a user's profile. When the maximum is reached, saving a new profile replaces the least-recently used profile.
Save Device Metadata	Specifies whether device metadata is saved to the user's profile.
Save Device Location	Specifies whether device location metadata is saved to the user's profile.

Device Tampering Verification node

Specifies a threshold for deciding if the device has been tampered with; for example, if it has been rooted or jailbroken.

The device scores between zero and one, based on the likelihood that is has been tampered with or may pose a security risk. For example, an emulator scores the maximum of `1`.

Use this node with the Device Profile Collector node to retrieve the tampering score from the device.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes

Product	Available?
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Not Tampered`
- `Tampered`

Evaluation continues along the `Not Tampered` path if the device scores less than or equal to the configured threshold; otherwise, evaluation continues along the `Tampered` path.

Properties

Property	Usage
Score Threshold	Specifies the score threshold for determining if a device has been tampered with. Enter a decimal fraction, between `0` and `1`. For example, `0.75`. The higher the score returned from the device, the more likely the device is jailbroken, rooted, or is a potential security risk. Emulators score the maximum; `1`.

Persistent Cookie Decision node

The **Persistent Cookie Decision** node checks for the existence of a specified persistent cookie (default: `session-jwt`).

If the cookie is present, the node verifies the signature of the JWT stored in the cookie with the configured signing key.

If the configured signing key isn't valid, AM checks the signature against all valid signing keys mapped to the configured secret label.

If the signature is valid, the node decrypts the payload of the JWT using the key pair defined in the active secret mapped to the `am.authentication.nodes.persistentcookie.encryption` secret label.

If there isn't a valid secret label mapping in a secret store, AM uses the key pair specified in **Realms** > ***Realm Name*** > **Authentication** > **Settings** > **Security** > **Persistent Cookie Encryption Certificate Alias**. The global setting is found under **Configure** > **Authentication** > **Core Attributes** > **Security**.

The decrypted JSON payload includes information, such as the UID of the identity and the client IP address. Enable **Enforce Client IP** to verify that the current IP address and the client IP address in the cookie are the same.

> **Note**
>
> This node recreates the specified persistent cookie, updating the value for the idle time property and the JWT `kid` header with the stable ID used to sign the JWT.
> Therefore, the node has cookie creation properties similar to the Set Persistent Cookie node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `realm` property, which AM sets by default.

Dependencies

To authenticate successfully, the tree must have set a persistent cookie using a node such as the Set Persistent Cookie node.

Configuration

Property	Usage
Idle Timeout	The maximum idle time allowed before the persistent cookie is invalidated, in hours. If no requests are received and the time is exceeded, the cookie is no longer valid.
Enforce Client IP	When enabled, ensures that the persistent cookie is only used from the same client IP to which the cookie was issued.
Use Secure Cookie	When enabled, adds the `Secure` flag to the persistent cookie. If the `Secure` flag is included, the cookie can only be transferred over HTTPS. When a request is made over HTTP, the cookie is not made available to the application.
Use HTTP Only Cookie	When enabled, adds the `HttpOnly` flag to the persistent cookie. When the `HttpOnly` flag is included, that cookie will not be accessible through JavaScript. According to RFC 6265, the `HttpOnly` flag, "instructs the user agent to omit the cookie when providing access to cookies via 'non-HTTP' APIs (for example, a web browser API that exposes cookies to scripts)."

Property	Usage

HMAC Signing Key	The key to use for HMAC signing of the persistent cookie.
	
	Note
	This property is *deprecated*. Use the **HMAC Signing Key Secret Label Identifier** instead.
	If you set an **HMAC Signing Key Secret Label Identifier**, this signing key is ignored.
	
	Values must be base64-encoded and at least 256 bits (32 bytes) long.
	To generate an HMAC signing key, run one of the following commands:
	`$ openssl rand -base64 32`
	or
	`$ cat /dev/urandom | LC_ALL=C tr -dc 'a-zA-Z0-9' | fold -w 32 | head -n 1|base64`

HMAC Signing Key Secret Label Identifier	An identifier used to create a *secret label* for mapping to a secret in a secret store. AM uses this identifier to create a specific secret label for the signing key for this node. The secret label takes the form `am.authentication.nodes.persistentcookie.identifier.signing` where identifier is the value of **HMAC Signing Key Secret Label Identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period. If you set an **HMAC Signing Key Secret Label Identifier** and AM finds a matching secret in a secret store, the **HMAC Signing Key** is ignored. If **HMAC Signing Key** is empty, AM uses the value configured for `am.default.authentication.nodes.persistentcookie.signing` for the realm, or at the global level if undefined. For greater security, you should rotate signing keys periodically. When you rotate a key, update the corresponding mapping in the realm secret store configuration to reflect this identifier. **Important** To read the persistent cookies generated by the Set Persistent Cookie node, ensure the nodes use the same HMAC signing key.
Persistent cookie name	The name of the persistent cookie to check.

Outputs

The node copies shared state into the outgoing node state. It records the user identity and stores the cookie name as a session property.

The node adds the `UpdatePersistentCookieTreeHook`, which runs when the tree completes.

Outcomes

- `True`
- `False`

Evaluation continues along the `True` outcome path if the persistent cookie is present and all the verification checks are satisfied; otherwise, evaluation continues along the `False` outcome path.

Errors

The node logs the following warning messages:

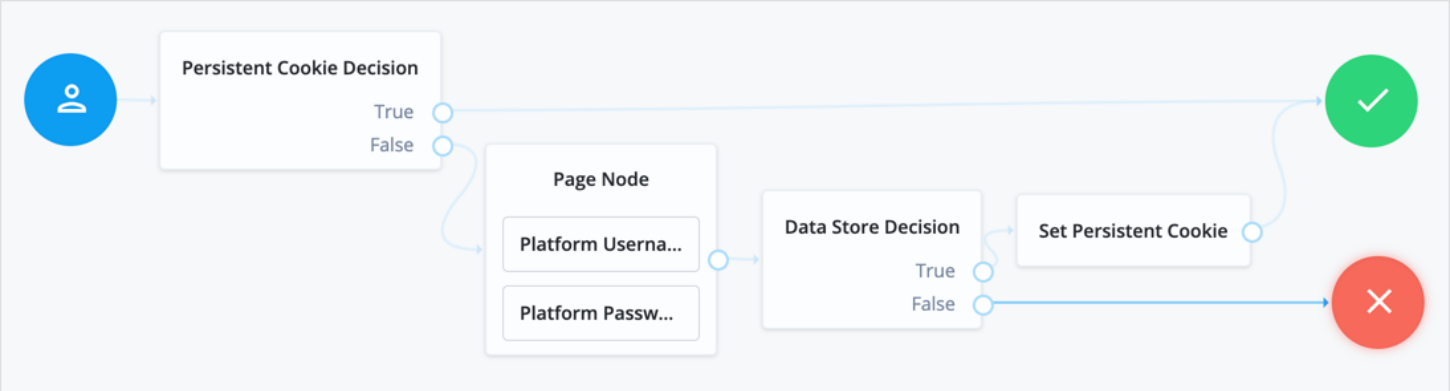
- `Attempt to verify JWT failed, attempting other valid keys`
- `Failed to parse universal id username from claim openam.usr`

The node logs the following error messages:

- `Claims context not found`
- `Failed to find signing key with associated keyID`
- `jwt reconstruction error`
- `Authentication failed. Jwt claim Realm does not match`
- `Authentication failed. Cannot read the user from null claims`
- `Authentication failed. Cannot read the user from empty claims`
- `Failed to parse universal Id from claim: openam.usr`
- `Authentication failed. Client IP is different`

Example

The following example authenticates the user based on a persistent cookie, if possible:



Set Custom Cookie node

The **Set Custom Cookie** node lets you store a custom cookie on the client in addition to the session cookie.

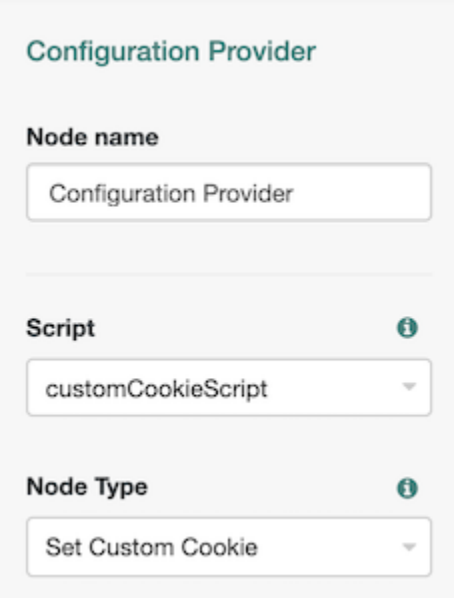
The node uses the specified properties to create a cookie with a custom name and value. It can also set attributes, such as the cookie path, domain, expiry, and security flags.

Use this node with the Configuration Provider node to extend custom capabilities. For example, create a `Config Provider` script to set custom static values or access values from the shared node state.

Include all the attributes in the configuration provider script's `config` map. The following example sets the attributes of the custom cookie to static values:

```
config = {
    "name": "testname",
    "value": "testvalue",
    "maxAge": "60",
    "domain": "am.example.com",
    "path": "/",
    "useSecureCookie": false,
    "useHttpOnlyCookie": false,
    "sameSite": "LAX"
};
```

Reference the script when you create a Configuration Provider node, and set the **Node Type** to `Set Custom Cookie`:



Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the user data from the shared node state.

It requires a predecessor node that gathers the user data.

Configuration

Property	Usage
Custom Cookie Name *(required)*	The name of the custom cookie. The cookie name can contain any US-ASCII characters except for: space, tab, control, or a separator character (`()<>@,;:"/[]?=\{}`).
Custom Cookie Value *(required)*	The value of the custom cookie.
Max Age	The length of time the custom cookie remains valid, in seconds. If that time is exceeded, the cookie is no longer valid. AM sets the `Max-Age` and `Expires` attributes in the cookie to increase compatibility with different browsers. If omitted, the cookie expires at the end of the current session. The precise implementation of this is determined by the specific browser. Refer to RFC 6265 for details.
Custom Cookie Domain	The domain the custom cookie will be sent to. If you specify a value here, AM sets a domain cookie. For example, if you set this property to `am.example.com`, AM sets a cookie on `.am.example.com`. Note the leading `.` indicating a domain cookie rather than a host cookie. If you don't set a value here, AM sets a host level cookie on the FQDN on which the client accessed AM. For example, if the client accesses AM at `https://am.example.com` and this property is empty, AM sets a host cookie on `am.example.com`.
Custom Cookie Path	The path of the custom cookie.
Use Secure Cookie	When enabled, adds the `Secure` flag to the custom cookie. If you include the `Secure` flag, the cookie can only be transferred over HTTPS. When a request is made over HTTP, the cookie isn't made available to the application.
Use HTTP Only Cookie	When enabled, adds the `HttpOnly` flag to the custom cookie. If you include the `HttpOnly` flag, the cookie isn't accessible to scripts.

Property	Usage
Custom Cookie SameSite attribute	Sets the `SameSite` attribute of the custom cookie. The default value is `LAX`, to align with most modern browsers. Learn more in SameSite cookie rules.

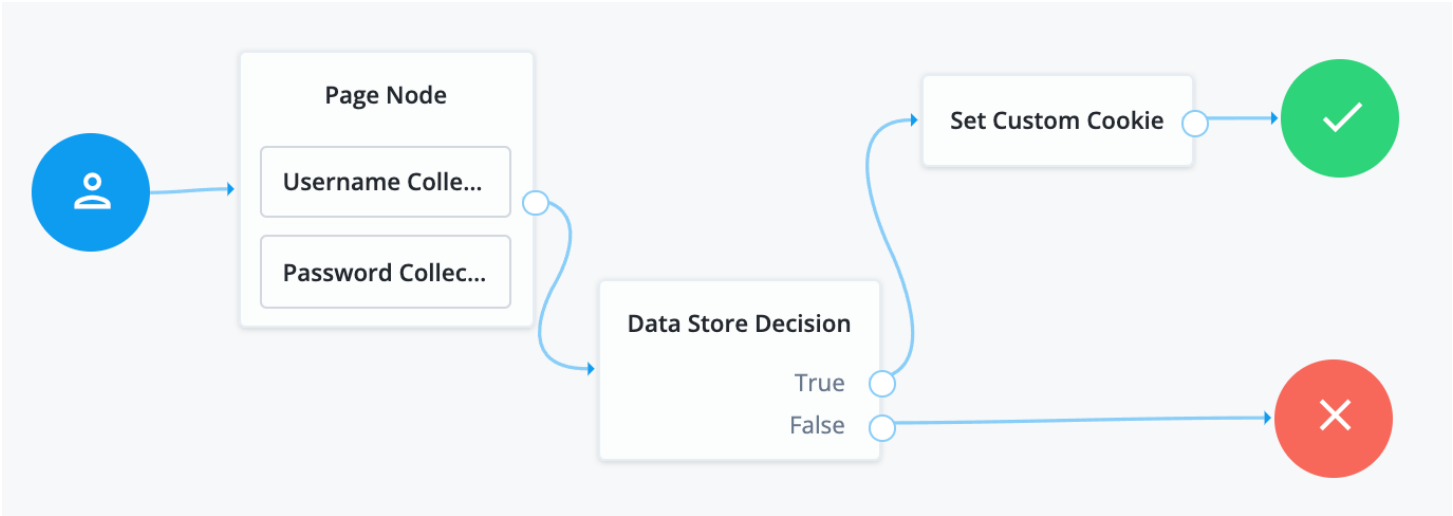
Outcomes

Single outcome path.

The cookie is created when AM next returns to the client.

Example

This example uses this node in a login flow. The node sets the custom cookie in the client browser after the user has successfully authenticated:



Set Persistent Cookie node

Creates the specified persistent cookie, the default being `session-jwt`.

The cookie contains a JWT with a JSON payload including information such as the UID of the identity, and the client IP address.

The node encrypts the payload of the JWT using the key pair defined in the active secret mapped to the `am.authentication.nodes.persistentcookie.encryption` secret label.

If there isn't a valid secret label mapping in a secret store, AM uses the key pair specified in **Realms > *Realm Name* > Authentication > Settings > Security > Persistent Cookie Encryption Certificate Alias**. The global setting is found under **Configure > Authentication > Core Attributes > Security**.

The node signs the cookie with the HMAC signing key defined in the node properties or the secret store with the mapped secret label. Configure nodes that read the persistent cookie such as the Persistent Cookie Decision node with the same HMAC signing key.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

When the authentication tree completes successfully, the `CreatePersistentCookieTreeHook` treehook for this node uses session properties to create the persistent cookie.

Dependencies

A secret store configured for storing the dynamic secret label mapping to the cookie's signing key.

Configuration

Property	Usage
Idle Timeout	The maximum amount of idle time allowed before the persistent cookie is invalidated, in hours. If no requests are received before the timeout, the cookie is no longer valid.
Max life	The length of time the persistent cookie remains valid, in hours. After this time has passed, the cookie is no longer valid.
Use Secure Cookie	When enabled, adds the `Secure` flag to the persistent cookie. If the `Secure` flag is included, the cookie can only be transferred over HTTPS. When a request is made over HTTP, the cookie is not made available to the application.
Use HTTP Only Cookie	When enabled, adds the `HttpOnly` flag to the persistent cookie. When the `HttpOnly` flag is included, that cookie will not be accessible through JavaScript. According to RFC 6265, the `HttpOnly` flag, "instructs the user agent to omit the cookie when providing access to cookies via 'non-HTTP' APIs (for example, a web browser API that exposes cookies to scripts)."

Property	Usage

HMAC Signing Key	A key to use for HMAC signing of the persistent cookie.
	
	Note
	This property is *deprecated*. Use the **HMAC Signing Key Secret Label Identifier** instead. If you set an **HMAC Signing Key Secret Label Identifier**, this signing key is ignored.
	
	Values must be base64-encoded and at least 256 bits (32 bytes) long.
	To generate an HMAC signing key, run one of the following commands:
	`$ openssl rand -base64 32`
	or
	`$ cat /dev/urandom | LC_ALL=C tr -dc 'a-zA-Z0-9' | fold -w 32 | head -n 1|base64`

HMAC Signing Key Secret Label Identifier	An identifier used to create a *secret label* for mapping to a secret in a secret store. AM uses this identifier to create a specific secret label for the signing key for this node. The secret label takes the form `am.authentication.nodes.persistentcookie.identifier.signing` where identifier is the value of **HMAC Signing Key Secret Label Identifier**. The identifier can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period. If you set an **HMAC Signing Key Secret Label Identifier** and AM finds a matching secret in a secret store, the **HMAC Signing Key** is ignored. If **HMAC Signing Key** is empty, AM uses the value configured for `am.default.authentication.nodes.persistentcookie.signing` for the realm, or at the global level if undefined. For greater security, you should rotate signing keys periodically. When you rotate a key, update the corresponding mapping in the realm secret store configuration to reflect this identifier. **Important** To read the persistent cookies this node generates, ensure the nodes use the same HMAC signing key.
Persistent Cookie Name	The name used for the persistent cookie.

Outputs

The node stores the cookie name in the session properties.

The node adds the `CreatePersistentCookieTreeHook` treehook, which runs when the tree completes.

Outcomes

Single outcome path.

Errors

The node logs the following warning messages:

- `Unable to create signing key from provided configuration.`

The node logs the following error messages:

- `Tree hook creation exception`
- `No signing keys available to sign JWT`
- `Error creating jwt string`

Example

Refer to the Persistent Cookie Decision node example.

Federation nodes

OAuth 2.0 node

Lets AM authenticate users of OAuth 2.0-compliant resource servers.

References in this section are to RFC 6749, The OAuth 2.0 Authorization Framework.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

- `Account Exists`
- `No account Exists`

Evaluation continues along the `Account Exists` path if an account matching the attributes retrieved from the social identity provider is found in the user data store; otherwise, evaluation continues along the `No account exists` path.

Properties

Property	Usage
Client ID *(required)*	Specifies the `client_id` parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).
Client Secret *(required)*	Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).

Property	Usage
Authentication Endpoint URL *(required)*	Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Example: `https://accounts.google.com/o/oauth2/v2/auth`
Access Token Endpoint URL *(required)*	Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Example: `https://www.googleapis.com/oauth2/v4/token`
User Profile Service URL *(required)*	Specifies the user profile URL that returns profile information. Example: `https://www.googleapis.com/oauth2/v3/userinfo`
OAuth Scope *(required)*	Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). Ensure you use the correct scope delimiter required by the identity provider, including commas or spaces. The list depends on the permissions that the resource owner, such as the end user, grants to the client application.
Scope Delimiter *(required)*	Specifies the delimiter used to separate scope values. Some authorization servers use non-standard separators for scopes, for example commas.
Redirect URL *(required)*	Specifies the URL the user is redirected to by the social identity provider after authenticating. For authentication trees in AM, set this property to the URL of the UI. For example, `https://am.example.com:8443/am/XUI/`.
Social Provider *(required)*	Specifies the name of the social provider for which this module is being set up. Example: `Google`
Auth ID Key *(required)*	Specifies the attribute the social identity provider uses to identify an authenticated individual. Example: `id`
Use Basic Auth	Specifies that the client uses HTTP Basic authentication when authenticating to the social provider. Default: `true`
Account Provider *(required)*	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

Property	Usage

Account Mapper *(required)*	Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from the social identity provider.
	Provided implementations are:
	`org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
	The Account Mapper classes can take two constructor parameters:
	1. A comma-separated list of attributes
	2. A prefix to apply to their values.
	For example, to prefix all received property values with `facebook-` before searching, specify:
	`org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|facebook-`

Attribute Mapper *(required)*	Specifies the list of fully qualified class names for implementations that map attributes from the OAuth 2.0 authorization server to AM profile attributes.
	Provided implementations are:
	`org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
	The Attribute Mapper classes can take two constructor parameters to help differentiate between the providers:
	1. A comma-separated list of attributes
	2. A prefix to apply to their values.
	For example, to prefix all incoming values with `facebook-`, specify:
	`org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|facebook-`
	To prefix all incoming values use an asterisk (`*`) as the attribute list. This prefixes all values, including email addresses, postal addresses, and so on.

Property	Usage

Account Mapper Configuration	Specifies the attribute configuration used to map the account of the user authenticated in the OAuth 2.0 provider to the local data store in AM.
	Valid values are in the form `provider-attr=local-attr`.
	Examples:
	`email=mail`
	`id=facebook-id`
	
	Tip
	When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation.
	For example, given a JSON payload of:
	`{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }`
	You can create a mapper, such as `name.first_name=cn`.

Property	Usage

Attribute Mapper Configuration	Map of OAuth 2.0 provider user account attributes to local user profile attributes, with values in the form `provider-attr=local-attr`.
	Examples:
	`first_name=givenname`
	`last_name=sn`
	`name=cn`
	`email=mail`
	`id=facebook-id`
	`first_name=facebook-fname`
	`last_name=facebook-lname`
	`email=facebook-email`
	Tip
	When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation.
	For example, given a JSON payload of:
	`{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }`
	You can create a mapper, such as `name.first_name=cn`.

Save attributes in the session	When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.
OAuth 2.0 Mix-Up Mitigation Enabled	Controls whether the OAuth 2.0 authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned as the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter. When this is enabled, set the Token Issuer property so that the validation can succeed. The authorization code response contains an issuer value (`iss`) for the client to validate. **Note** Refer to the authorization server's documentation for the value it uses for the issuer field. Learn more in section 4 of OAuth 2.0 Mix-Up Mitigation Draft.
Token Issuer	Corresponds to the expected issuer identifier value in the `iss` field of the ID token. Example: `https://accounts.google.com`

OpenID Connect node

Lets AM authenticate users of OpenID Connect-compliant resource servers.

As OpenID Connect is an additional layer on top of OAuth 2.0, described in RFC 6749, The OAuth 2.0 Authorization Framework. OpenID Connect is described in the OpenID Connect Core 1.0 incorporating errata set 1 specification.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

The OpenID Connect node implements the Authorization code grant.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

- `Account Exists`
- `No account Exists`

Evaluation continues along the `Account Exists` path if an account matching the attributes retrieved from the OpenID Connect identity provider is found in the identity store; otherwise, evaluation continues along the `No account exists` path.

Properties

Property	Usage
Client ID *(required)*	Specifies the `client_id` parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).
Client Secret *(required)*	Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).
Authentication Endpoint URL *(required)*	Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Example: `https://accounts.google.com/o/oauth2/v2/auth`

Property	Usage
Access Token Endpoint URL *(required)*	Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Example: `https://www.googleapis.com/oauth2/v4/token`
User Profile Service URL *(required)*	Specifies the user profile URL that returns profile information. If not specified, attributes are mapped from the claims returned by the `id_token`, and no call to a user profile endpoint is made. Example: `https://www.googleapis.com/oauth2/v3/userinfo`
OAuth Scope	Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). Ensure you use the correct scope delimiter required by the identity provider, including commas or spaces. The list depends on the permissions that the resource owner, such as the end user, grants to the client application.
Redirect URL	Specifies the URL the user is redirected to by the social identity provider after authenticating. For authentication trees in AM, set this property to the URL of the UI. For example, `https://am.example.com:8443/am/XUI/`.
Social Provider *(required)*	Specifies the name of the OpenID Connect provider for which this node is being set up. Example: `Google`
Auth ID Key	Specifies the attribute the social identity provider uses to identify an authenticated individual. Example: `sub`
Use Basic Auth	Specifies that the client uses HTTP Basic authentication when authenticating to the social provider. Default: `true`
Account Provider	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

Property	Usage
Account Mapper	Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from the social identity provider. The provided implementations is `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper`. The Account Mapper classes can take two constructor parameters: 1. A comma-separated list of attributes 2. A prefix to apply to their values. For example, to prefix all received property values with `openid-` before searching, specify: `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|*|openid-`
Attribute Mapper	Specifies the list of fully qualified class names for implementations that map attributes from the authorization server to AM profile attributes. The provided implementations is `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper`. The Attribute Mapper classes can take two constructor parameters to help differentiate between the providers: 1. A comma-separated list of attributes 2. A prefix to apply to their values. For example, to prefix incoming `iplanet-am-user-alias-list` values with `openid-`, specify: `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper`
iplanet-am-user-alias-list	openid- To prefix all incoming values use an asterisk (`*`) as the attribute list. This prefixes all values, including email addresses, postal addresses, and so on.
Account Mapper Configuration	Specifies the attribute configuration used to map the account of the user authenticated in the provider to the local identity store in AM. To add a mapping, specify the name of the provider attribute as the key, and the local attribute to map to as the value. For example, click **Add**, then specify `sub` in the **Key** field and `iplanet-am-user-alias-list` in the **Value** field, and click +.

Property	Usage

Attribute Mapper Configuration	Specifies how to map provider user attributes to local user profile attributes.
	To add a mapping, specify the name of the provider attribute as the Key, and the local attribute to map to as the Value.
	For example, click **Add**, then specify `id` in the **Key** field and `facebook-id` in the **Value** field, and click +.
	Examples:
	`first_name=givenname`
	`last_name=sn`
	`name=cn`
	`email=mail`
	`id=facebook-id`
	`first_name=facebook-fname`
	`last_name=facebook-lname`
	`email=facebook-email`

Save attributes in the session	When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.
OAuth 2.0 Mix-Up Mitigation Enabled	Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned as the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter. When this is enabled, set the Token Issuer property so that the validation can succeed. The authorization code response contains an issuer value (`iss`) for the client to validate. **Note** Refer to the authorization server's documentation for the value it uses for the issuer field. Learn more in section 4 of OAuth 2.0 Mix-Up Mitigation Draft.
Token Issuer *(required)*	Corresponds to the expected issuer identifier value in the `iss` field of the ID token. Example: `https://accounts.google.com`

Property	Usage
OpenID Connect Validation Type *(required)*	Specifies how to validate the ID token received from the OpenID Connect provider. This ignores keys specified in JWT headers, such as `jku` and `jwe`. The following options are available to validate an incoming OpenID Connect ID token: **`Well Known URL` *(Default)*** Retrieves the provider's keys based on the information provided in its OpenID Connect configuration URL. Specify the provider's configuration URL in the OpenID Connect Validation Value field; for example, `https://accounts.google.com/.well-known/openid-configuration`. **`Client Secret`** Validates the ID token signature with a specified client secret key. Specify the key to use in the OpenID Connect Validation Value field. **`JWK URL`** Retrieve the necessary JSON web key from the URL that you specify. Specify the provider's JWK URI in the OpenID Connect Validation Value field; for example, `https://www.googleapis.com/oauth2/v3/certs`.
OpenID Connect Validation Value	Provide the URL or secret key used to verify an incoming ID token, depending on the value selected in the OpenID Connect Validation Type property.

OIDC ID Token Validator node

The **OIDC ID Token Validator** node lets AM rely on an OIDC provider (OP)'s ID token to authenticate an end user. The node evaluates whether the ID token is valid according to the OIDC specification.

To configure the node, first get an `id_token` from an OIDC client and examine the decoded JWT to view the required claims values.

This example uses an `id_token` from the OAuth 2.0 Playground:

```
{
    "iss": "https://accounts.google.com",
    "azp": "407408718192.apps.googleusercontent.com",
    "aud": "407408718192.apps.googleusercontent.com",
    "sub": "111730983950574648607",
    "at_hash": "kvQJZrGcnNMZqM4w68DFBA",
    "iat": 1677608448,
    "exp": 1677612048
}
```

The `iss`, `azp`, and `aud` claims provide the values for the node's `Token Issuer`, `Authorized parties` and `Audience name` properties respectively.

To use the OIDC ID Token Validator node to authenticate a user, first configure the node to run a transformation script that maps the user attributes from the JWT to local attributes. You can then create a journey with a Scripted Decision node that stores the attributes in the shared node state so that you can authenticate the user with an ID token.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None.

Dependencies

A valid OIDC ID token provided in the HTTP request header.

Configuration

Property	Usage
OpenID Connect Validation Type	To validate the ID token from the OP, the node requires either a URL to get the public keys for the provider, or the symmetric key for an ID token signed with an HMAC-based algorithm. Select one of the following options to determine how the node retrieves the required information: • `Well Known URL` (default): Validate with the keys specified in the OP's `/.well-known/openid-configuration` JSON document. • `Client Secret`: Validate the ID token signature with the provided client secret. • `JWK URL`: Validate with the keys retrieved from the URL to the OP's JSON Web Key Set (JWKS).
OpenID Connect Validation Value	The well-known URL or URL to the JWK location, depending on the value of `OpenID Connect Validation Type`. If the validation type is `Client Secret`, this value is ignored and the `Client Secret Label` is used instead. For example: `https://accounts.google.com/.well-known/openid-configuration`

Property	Usage
Client Secret Label	The secret label to which the OIDC client secret should be mapped. Only required if the validation type is `Client Secret`. You can specify an existing label or AM creates a new one dynamically. The label can only contain alphanumeric characters `a-z`, `A-Z`, `0-9`, and periods (`.`). It can't start or end with a period.
ID Token Header Name	The name of the HTTP request header referencing the ID token. Default: `oidc_id_token`
Token Issuer	The issuer of the OIDC ID token, which is checked against the `iss` claim in the ID token. For example: `https://accounts.google.com`
Audience name	The case-sensitive name of the intended audience for this node, which is checked against the `aud` claim in the ID token.
Authorized parties	The authorized parties from which the node accepts ID tokens, which is checked against the `azp` claim in the ID token. The value can be either a case-sensitive string or a URI.
Transformation Script	Select a `Social Identity Provider Profile Transformation` script that maps ID token attributes to local attributes. For examples of transformation (normalization) scripts, refer to the Example or the `*-profile-normalization.js` sample script.
Script Inputs	A list of state inputs for the script. Default: `*`
Unreasonable Lifetime Limit	Specify the maximum permitted lifetime of the token in minutes. If the `iat` claim is present, the token must expire within the specified duration. Default: `60`

Outputs

The node relies on the transformation script to set profile attributes required later in the journey.

Outcomes

- `True`
- `False`

Evaluation continues along the `True` path if the ID token is valid; otherwise, evaluation continues along the `False` path.

Errors

The node logs the following warnings:

- `No OpenIdConnect ID Token referenced by header value: {}`: if the node can't read the ID token in the HTTP request header.
- `Error evaluating the script`: if there's a problem with the transformation script.

The node logs an error if an `AuthLoginException` occurs during node processing.

Example

This example demonstrates how to use the OIDC ID Token Validator node as part of a journey to validate an ID token and authenticate the user.

Figure 1. Ping Identity Platform deployment

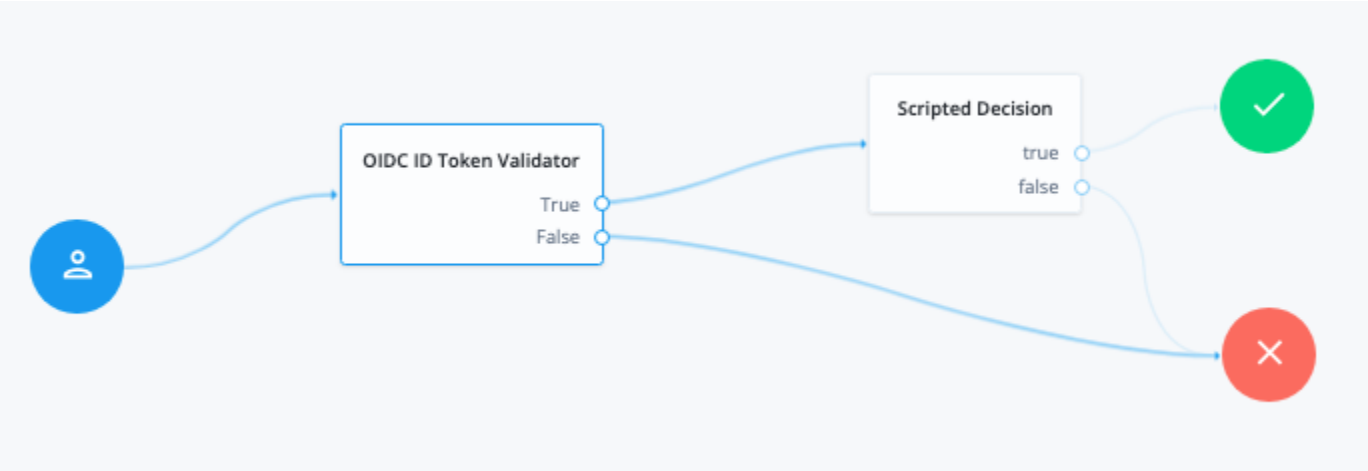


Figure 2. PingAM deployment

You can access all the provided JWT claims through the `jwtClaims` attribute. This JavaScript, configured as the node's transformation script, retrieves the user ID from the JWT.

```
(function () {
    var fr = JavaImporter( org.forgerock.json.JsonValue);

    var identity = fr.JsonValue.json(fr.JsonValue.object());
    identity.put('uid', jwtClaims.get('sub'));

    return identity;
}());
```

Ping Identity Platform

A Scripted Decision node runs this script to find the username from `lookupAttributes` and store it in the shared node state:

Next-generation

```
var attributes = nodeState.get("lookupAttributes");
var userName = attributes.get("uid");

// Add userName in objectAttributes to nodeState for use by Identify Existing User node.
nodeState.putShared("objectAttributes", attributes);

// Add username at the root level so that a session can be created
nodeState.putShared("username", userName);

action.goTo('true');
```

Legacy

```
var attributes = nodeState.get("lookupAttributes");
var userName = attributes.get("uid").asString();

// Add userName in objectAttributes to nodeState for use by Identify Existing User node.
nodeState.putShared("objectAttributes", attributes);

// Add username at the root level so that a session can be created
nodeState.putShared("username", userName);

outcome = "true";
```

The Identify Existing User node then performs a lookup on IDM with the `_id` attribute using the username saved into shared state by the Scripted Decision node.

The following REST call authenticates the user with the example journey, providing the ID token in the header:

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "Accept-API-Version: resource=2.0, protocol=1.0" \
--header "oidc_id_token: <id_token>" \
"https://<tenant-env-fqdn>/am/json/realms/root/realms/alpha/authenticate?
authIndexType=service&authIndexValue=myJourney"
{
    "tokenId": "AQIC5w…NTcy*",
    "successUrl": "/openam/console",
    "realm": "/alpha"
}
```

PingAM

In a standalone AM deployment, a Scripted Decision node runs this script to find the user ID from `lookupAttributes` and store it in the shared node state:

Next-generation

```
var attributeName = "uid";
var attributes = nodeState.get("lookupAttributes");
var uid = attributes.get(attributeName);

// get the identity for the sub claim (stored as uid)
var identity = idRepository.getIdentity(uid);

// verify the identity exists
var userName = identity.getAttributeValues(attributeName);

if (!userName.isEmpty()) {
    nodeState.putShared("username", userName[0]);
    action.goTo('true');
} else {
    action.goTo('false');
}
```

Legacy

```
var attributeName = "uid";
var attributes = nodeState.get("lookupAttributes");
var userName = attributes.get(attributeName).asString();
var identity = idRepository.getAttribute(userName, attributeName);

if (!identity.isEmpty()) {
    nodeState.putShared("username", identity.iterator().next());
    outcome = "true";
} else {
    outcome = "false";
}
```

The following REST call authenticates the user with the example tree, providing the ID token in the header:

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "Accept-API-Version: resource=2.0, protocol=1.0" \
--header "oidc_id_token: <id_token>" \
"https://openam.example.com:8443/openam/json/realms/root/authenticate?
authIndexType=service&authIndexValue=myJourney"
{
    "tokenId": "AQIC5w…NTcy*",
    "successUrl": "/openam/console",
    "realm": "/alpha"
}
```

Provision Dynamic Account node

Provision an account following successful authentication by a SAML2 authentication node or the Social Provider Handler node.

Accounts are provisioned using properties defined in the attribute mapper configuration of a social authentication or SAML2 authentication node earlier in the flow.

If a password has been acquired from the user, for example, by using the Password Collector node, it is used when provisioning the account; otherwise, a 20 character random string is used.

In addition to retrieving the password from the node state, the Provision Dynamic Account node gets the `realm` value, and `attributes` and `userNames` from `userInfo` in the shared state. It sets the `username` attribute in the node's shared state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

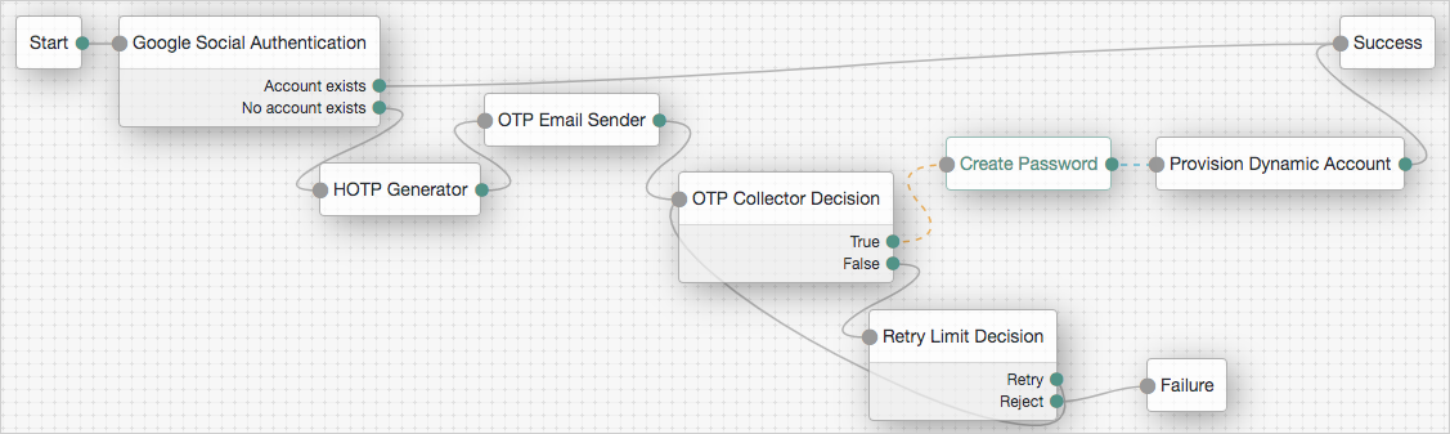
Single outcome path.

Properties

Property	Usage
Account Provider	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

Example

The following example uses this node to let users who have performed social authentication using Google provide a password and provision an account if they do not have a matching existing profile. They must enter a one-time passcode to verify they are the owner of the Google account.



Provision IDM Account node

Redirects users to an IDM instance to provision an account.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Ensure you configured the details of the IDM instance in AM, by navigating to **Configure > Global Services > IDM Provisioning**.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes

Product	Available?
Ping Identity Platform (self-managed)	No

Outcomes

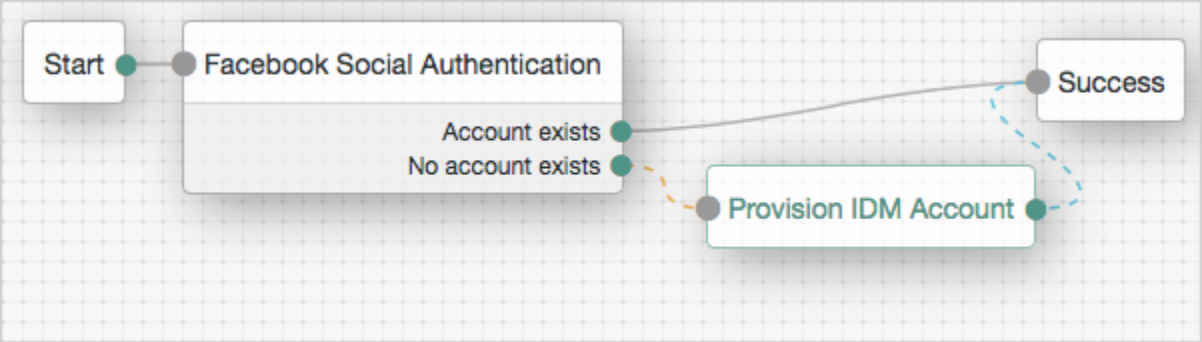
Single outcome path.

Properties

Property	Usage
Account Provider	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

Example

The following example uses this node to let users who have performed social authentication using Facebook provide a password and provision an account if they do not have a matching existing profile:



SAML2 Authentication node

The **SAML2 Authentication** node integrates SAML 2.0 single sign-on into an authentication flow.

Use this node when deploying SAML 2.0 SSO in integrated mode (SP-initiated SSO only). This node doesn't support single logout (SLO).

Implement the Write Federation Information node after this node in the journey to link the remote account to a local account.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Dependencies

This node requires the following configuration in AM:

- A remote identity provider (IdP) and a hosted service provider (SP) in a circle of trust in the same realm where you're configuring the journey.
- You must configure the service provider for integrated mode.

  PingAM Configure AM for integrated mode.

  PingOne Advanced Identity Cloud Configure Advanced Identity Cloud for integrated mode.

Inputs

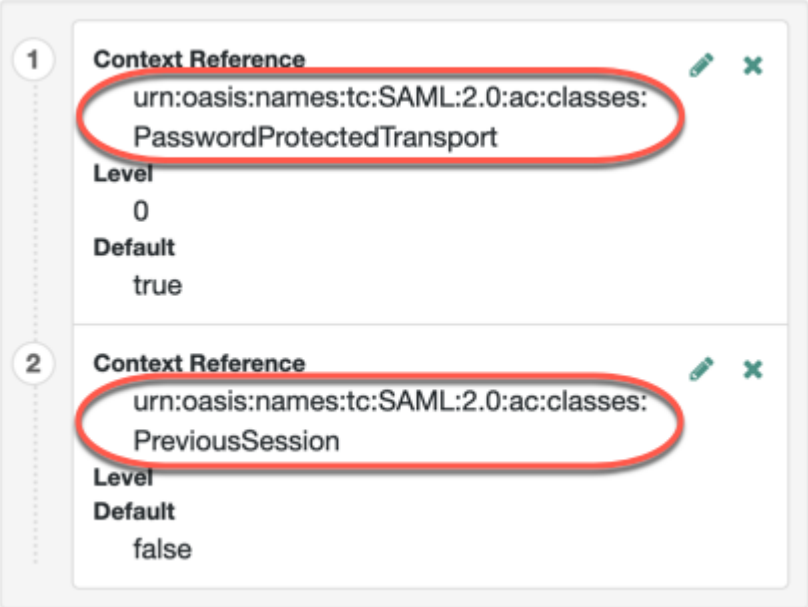
This node sends a SAML Request and processes the incoming SAML assertion.

Configuration

Property	Usage
IdP Entity ID	The name of the remote IdP.
SP MetaAlias	The local alias for the SP in the format `/Realm Name/SP Name`.
Allow IdP to Create NameID	Enable this option if you want the IdP to create a new identifier for the authenticating user if none exists. Learn more in AllowCreate in the SAML Version 2.0 specification. Default: `Enabled`

Property	Usage
Comparison Type	The comparison method to evaluate authentication context classes or statements. This value overrides the value in the SP configuration: PingAM Under **Realms > *Realm Name* > Applications > Federation > Entity Providers > *Service Provider Name* > Assertion Content > Authentication Context > Comparison Type**. PingOne Advanced Identity Cloud Under **Native Consoles > Access Management > Realms > *Realm Name* > Applications > Federation > Entity Providers > *Service Provider Name* > Assertion Content > Authentication Context > Comparison Type**. Valid comparison methods are `exact`, `minimum`, `maximum`, or `better`. Learn more about comparison methods in `Element <RequestedAuthnContext>` in Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. Default: `minimum`

Property	Usage

Authentication Context Class Reference	(Optional) Set one or more URIs for authentication context classes to be included in the SAML request.
	Authentication context classes are unique identifiers for an authentication mechanism. The SAML 2.0 protocol supports a standard set of authentication context classes, defined in Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0.
	You can specify your own authentication context classes in addition to the standard ones.
	Any authentication context class you specify here must be supported for the SP. To add authentication context classes to the SP:
	1. In the AM admin UI, go to **Realms** > ***Realm Name*** > **Applications** > **Federation** > **Entity Providers** > ***Service Provider Name*** > **Assertion Content**.
	2. In the **Authentication Context** section, add the authentication context classes.
	 
	Use the | character to separate multiple authentication context classes, for example:
	`urn:oasis:names:tc:SAML:2.0:ac:classes:Password|`
	`urn:oasis:names:tc:SAML:2.0:ac:classes:TimesyncToken`

Authentication Context Declaration Reference	(Optional) One or more URIs that identify authentication context declarations. Use the | character to separate multiple URIs. Learn more in the section on the `<RequestedAuthnContext>` element in Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.
Request Binding	The format of the authentication request that the SP sends to the IdP. Valid values are `HTTP-Redirect` and `HTTP-POST`. Default: `HTTP-Redirect`

Property	Usage
Response Binding	The format of the response that the IdP sends to the SP. Valid values are `HTTP-POST` and `HTTP-Artifact`. Default: `HTTP-Artifact`
Force IdP Authentication	Indicate whether the IdP should force authentication or if it can reuse existing security contexts. Default: Disabled
Passive Authentication	Indicate whether the IdP should use passive authentication. When this setting is enabled, the IdP can only use authentication methods that don't require user interaction, such as authenticating with an X.509 certificate. Default: Disabled

NameID Format	The SAML name ID format that's requested in the SAML authentication request.
	Valid values are:
	`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
	`urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
	`urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`
	Default: `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`

Outputs

This node updates the shared state with the SAML 2.0 assertion data as follows:

- It adds a `userInfo` key with two child keys: `attributes` and `userNames`.
- The `attributes` object contains a map of SAML 2.0 attributes, each of which is stored as an array.
- The `attributes` object also stores the SAML 2.0 identity attributes `sun-fm-saml2-nameid-info` and `sun-fm-saml2-nameid-infokey`.

  These attributes are required by the Write Federation Information node.
- The `userNames` object contains the user's UUID.

```
{
    "realm" : "/",
    "authLevel" : 0,
    "username" : "22fe07c3-ac8b-4e84-9016-b55f1c009924",
    "userInfo" : {
      "attributes" : {
        "uid" : [ "bjensen" ],
        "mail" : [ "bjensen@example.com" ],
        "sun-fm-saml2-nameid-info" : [ "serviceprovider2|identityprovider1|sAdI2i7LT2YL0rbJC/QqsRt5SABV|
identityprovider1|urn:oasis:names:tc:SAML:2.0:nameid-format:persistent|null|serviceprovider2|SPRole|false" ],
        "sun-fm-saml2-nameid-infokey" : [ "serviceprovider2|identityprovider1|sAdI2i7LT2YL0rbJC/QqsRt5SABV" ]
      },
      "userNames" : {
        "username" : [ "22fe07c3-ac8b-4e84-9016-b55f1c009924" ],
        "uid" : [ "22fe07c3-ac8b-4e84-9016-b55f1c009924" ]
      }
    },
    "emailAddress" : "bjensen@example.com"
  }
```


Tip

You can use a script to read the SAML 2.0 attributes, for example:

```
nodeState.get("userInfo").get("attributes").get("uid").get(0)
```

The updated shared state depends on the node outcome:

- If the outcome is `Account exists`, the shared state is updated with `nodeState.userNames` as follows:

```
userNames={username=[bjensen], uid=[bjensen]}}
```

- If the outcome is `No account exists`, the shared state is updated with `nodeState.userNames` as follows:

```
userNames={username=[null], uid=[null]}}
```

- If the `mail` attribute exists in the `attributes` map, the shared state is updated with `nodeState.emailAddress`.
- If the `RelayState` attribute exists in the `attributes` map, the shared state is updated with `nodeState.successUrl`.
- The `username` is added to the shared state, regardless of outcome.

The node also sets the following session properties:

- `SessionIndex`: the session index
- `NameID`: the NameID of the Assertion XML
- `isTransient`: if the NameId is `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
- `cacheKey`: for internal use only

Outcomes

`Account exists`

The node found a user account that matches the federated account.

`No account exists`

Any other case.

Errors

This node can log the following errors:

Message	Notes
`Unable to complete SAML2 authentication, IDP descriptor not found for entity with id: ID`	The node was unable to find the remote IdP descriptor.
`Unable to complete SAML2 authentication, SP descriptor not found for entity with id: ID`	The node was unable to find the SP descriptor.
`Unable to retrieve SAML2 state from SFO`	The node was unable to retrieve the SAML 2.0 state from the second-factor authentication.
`Unable to complete SAML2 authentication, response data not found`	The node was unable to read the SAML 2.0 response data.
`Failed to remove data for responseKey starting with keyname`	The node was unable to remove the SAML 2.0 response data.
`AuthConsumer endpoint reported error code: code`	The `AuthConsumer` endpoint (Assertion Consumer Service URL) on the SP reported an error.

Example

Read the following sections for examples that show this node in a SAML 2.0 authentication journey:

PingAM SSO and SLO in integrated mode.

PingOne Advanced Identity Cloud Configure Advanced Identity Cloud for integrated mode.

Social Facebook node

Duplicates OAuth 2.0 node but is preconfigured to work with Facebook. You specify only the `Client ID` and `Client Secret`.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

- `Account exists`
- `No account exists`

Evaluation continues along the `Account Exists` path if an account matching the attributes retrieved from Facebook are found in the user data store; otherwise, evaluation continues along the `No account exists` path.

Properties

Property	Usage
Client ID	Specifies the `client_id` parameter as provided by Facebook.
Client Secret	Specifies the `client_secret` parameter as provided by Facebook.
Authentication Endpoint URL	Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: `https://www.facebook.com/dialog/oauth`
Access Token Endpoint URL	Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: `https://graph.facebook.com/v2.12/oauth/access_token`
User Profile Service URL	Specifies the user profile URL that returns profile information. Default: `https://graph.facebook.com/v2.6/me?fields=name%2Cemail%2Cfirst_name%2Clast_name`

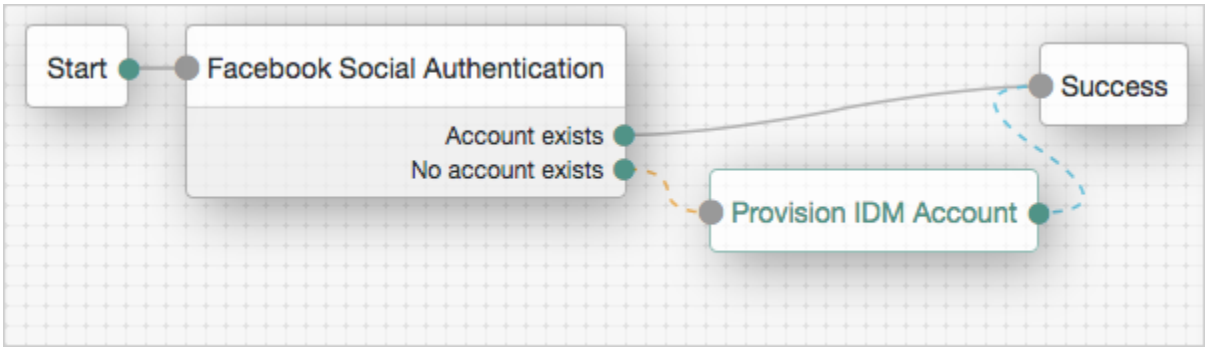
Property	Usage
OAuth Scope	Specifies a comma-separated list of user profile attributes the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions the resource owner, such as the end user, grants to the client application.
Redirect URL	Specifies the URL the user is redirected to by Facebook after authenticating to continue the flow. Set this property to the URL of the AM UI. For example, `https://am.example.com:8443/am/XUI/`. **Tip** If the tree is not in the Top Level Realm, you can specify the realm in the redirect URL. Use a DNS alias for the realm, or add the realm as a query parameter, for example, `https://am.example.com:8443/am/XUI/?realm=/mySubRealm`. Learn more in Configure DNS aliases to access a realm.
Social Provider	Specifies the name of the social provider for which this node is being set up. Default: `facebook`
Auth ID Key	Specifies the attribute the social identity provider uses to identify an authenticated individual. Default: `id`
Use Basic Auth	Specifies that the client uses HTTP Basic authentication when authenticating to the social provider. Default: `true`
Account Provider	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`
Account Mapper	Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from Facebook. Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
Attribute Mapper	Specifies the list of fully qualified class names for implementations that map attributes from Facebook to AM profile attributes. Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|facebook-`

Property	Usage
Account Mapper Configuration	Specifies the attribute configuration used to map the account of the user authenticated in the Social Facebook provider to the local data store in AM. Valid values are in the form `provider-attr=local-attr`. Default: `id=uid`. **Tip** When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation. For example, given a JSON payload of: `{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }` You can create a mapper, such as `name.first_name=cn`.
Attribute Mapper Configuration	Map of Facebook user account attributes to local user profile attributes, with values in the form `provider-attr=local-attr`. Default: `name=cn`, `last_name=sn`, `id=uid`, `first_name=givenname`, `email=mail`. **Tip** When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation. For example, given a JSON payload of: `{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }` You can create a mapper, such as `name.first_name=cn`.
Save attributes in the session	When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session. Default: `true`.

Property	Usage
OAuth 2.0 Mix-Up Mitigation Enabled	Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned as the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter. The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response contains an issuer value (`iss`) for the client to validate. Learn more in section 4 of OAuth 2.0 Mix-Up Mitigation Draft.
Token Issuer	Corresponds to the expected issuer identifier value in the `iss` field of the ID token. Example: `https://graph.facebook.com`

Example

The following example shows the node in context:



Social Google node

Duplicates OAuth 2.0 node, but is preconfigured to work with Google. You specify only the `Client ID` and `Client Secret`.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

- `Account exists`
- `No account exists`

Evaluation continues along the `Account Exists` path if an account matching the attributes retrieved from Google are found in the user data store; otherwise, evaluation continues along the `No account exists` path.

Properties

Property	Usage
Client ID *(required)*	Specifies the `client_id` parameter as provided by Google.
Client Secret *(required)*	Specifies the `client_secret` parameter as provided by Google.
Authentication Endpoint URL	Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: `https://accounts.google.com/o/oauth2/v2/auth`
Access Token Endpoint URL	Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: `https://www.googleapis.com/oauth2/v4/token`
User Profile Service URL	Specifies the user profile URL that returns profile information. Default: `https://www.googleapis.com/oauth2/v3/userinfo`
OAuth Scope	Specifies a space-separated list of user profile attributes the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions the resource owner, such as the end user, grants to the client application. Default: `profile email`.

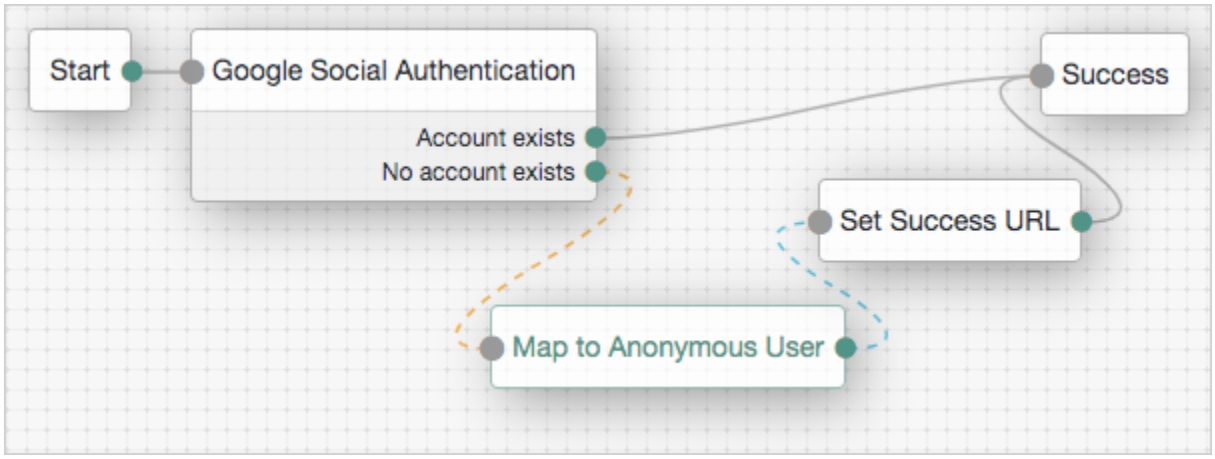
Property	Usage
Redirect URL	Specifies the URL the user is redirected to by Google after authenticating to continue the flow. Set this property to the URL of the AM UI. For example, `https://am.example.com:8443/am/XUI/`. **Tip** If the tree is not in the Top Level Realm, you can specify the realm in the redirect URL. Use a DNS alias for the realm, or add the realm as a query parameter; for example, `https://am.example.com:8443/am/XUI/?realm=/mySubRealm`. Learn more in Configure DNS aliases to access a realm.
Social Provider	Specifies the name of the social provider for which this node is being set up. Default: `google`
Auth ID Key	Specifies the attribute the social identity provider uses to identify an authenticated individual. Default: `sub`
Use Basic Auth	Specifies that the client uses HTTP Basic authentication when authenticating to Google. Default: `true`
Account Provider	Specifies the name of the class that implements the account provider. Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`
Account Mapper	Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from Google. Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
Attribute Mapper	Specifies the list of fully qualified class names for implementations that map attributes from Google to AM profile attributes. Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|iplanet-am-user-alias-list|google-`

Property	Usage
Account Mapper Configuration	Specifies the attribute configuration used to map the account of the user authenticated in the Social Google provider to the local data store in AM. Valid values are in the form `provider-attr=local-attr`. Default: `sub=uid`. **Tip** When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation. For example, given a JSON payload of: `{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }` You can create a mapper, such as `name.first_name=cn`.
Attribute Mapper Configuration	Map of Google user account attributes to local user profile attributes, with values in the form `provider-attr=local-attr`. Default: `sub=uid`, `name=cn`, `given_name=givenName`, `family_name=sn`, `email=mail`. **Tip** When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings using dot notation. For example, given a JSON payload of: `{ "sub" : "12345", "name" : { "first_name" : "Demo", "last_name" : "User" } }` You can create a mapper, such as `name.first_name=cn`.
Save attributes in the session	When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session. Default: `true`.

Property	Usage
OAuth 2.0 Mix-Up Mitigation Enabled	Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned as the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter. The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response contains an issuer value (`iss`) for the client to validate. Learn more in section 4 of OAuth 2.0 Mix-Up Mitigation Draft.
Token Issuer	Corresponds to the expected issuer identifier value in the `iss` field of the ID token. Example: `https://accounts.google.com`

Example

The following example shows the node in context:



Social Ignore Profile node

Specifies whether to ignore a local user profile.

If evaluation flows through this node after successful social authentication, AM issues an SSO token regardless of whether a user profile exists in the data store. AM does not check for whether a user profile is present.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

Single outcome path.

Properties

This node has no configurable properties.

Social Provider Handler node

The **Social Provider Handler** node attempts to authenticate a user with an identity provider they select in the Select Identity Provider node. The **Social Provider Handler** node collects relevant profile information from the provider, transforms the profile information into the appropriate attributes, and returns the user to the journey.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the user's selected social identity provider from shared state.

Implement the Select Identity Provider node before this node to capture the social provider name.

Dependencies

- The Social Identity Provider service must be configured with the details of at least one social identity provider.
- The user must have selected a social identity provider in a previous node in the journey.

Configuration

Property	Usage
Transformation Script *(required)*	The *normalization* script of each provider maps that provider's attributes to a profile format AM can use. The *transformation* script then transforms the normalized social profile to an identity (standalone AM) or a managed object (Ping Identity Platform deployment). *In standalone AM deployments*, select `Normalized Profile to Identity` or a custom script that transforms the profile to an identity object. Review the sample script (normalized-profile-to-identity.js) for a list of bindings. *In Ping Identity Platform deployments*, select `Normalized Profile to Managed User` (default) or a custom script to transform the profile to a managed object. Review the sample script (normalized-profile-to-managed-user.js) for a list of bindings. **Important** Don't use normalization scripts (`<Identity provider>-profile-normalization.*`) for this purpose.
Username Attribute	( ) The attribute in IDM that contains the username for this object.
Client Type	The client type you're using to authenticate to the provider. Select one of the following: • `BROWSER` (default) Select this type for Ping Identity-provided user interfaces or the Ping SDKs for JavaScript. With this setting, the node returns the RedirectCallback. • `NATIVE` Select this type for the Ping SDKs for Android or iOS. With this setting, the node returns the IdPCallback.
Store Tokens	When `true`, the node stores access and refresh tokens in the transient state for use by subsequent nodes in the journey. In some cases, the social provider requires these tokens, for example, to revoke user authorization. If you choose to store tokens, you can configure a Scripted Decision node later in the journey to handle your social provider use case. Default: `false`

Outputs

- If no profile information is returned from the social provider, the journey follows the `Social auth interrupted` outcome.
- If the node retrieves profile information from the social identity provider, it transforms a normalized version of the profile and stores it in `objectAttributes` in transient state.
- *In Ping Identity Platform deployments*, the `aliasList` is updated and saved to `objectAttributes` in transient state to link existing users.

- The node stores the social identity subject as the `username` both directly in shared state and in its `objectAttributes`.
- The node also updates `socialOAuthData` in transient state with all existing node state, social provider data, and associated tokens.

> **Note**
>
> Make sure you copy required transient data to shared state because all transient data is removed if the node is followed by an interactive page later in the journey.

Outcomes

`Account exists`

Social authentication succeeded, and a matching Ping Identity account exists.

`No account exists`

Social authentication succeeded, but no matching Ping Identity account exists.

> **Note**
>
> *In standalone AM deployments*, to ensure existing users are dynamically linked, complete these additional steps:
>
> 1. Connect the `No account exists` outcome to a Scripted Decision node.
> 2. Write a Scripted Decision node script and use the `idRepository` binding's `get-` and `setAttribute` methods to check for an existing account and add a link by updating the account-linking attribute, `iplanet-am-user-alias-list`.
>
>   For multiple OIDC providers, add links to the existing list. For example:
>
>    ```
>    "iplanet-am-user-alias-list": [
>        "google_IDP-123456789",
>        "amazon_IDP-987654321"
>    ],
>    ```
> 3. Connect the Scripted Decision node to a Provision Dynamic Account node to update the account.
>
> *In Ping Identity Platform deployments*, to ensure existing users are dynamically linked, connect the `No account exists` outcome to an Identify Existing User node followed by a Patch Object node to create the link.

`Social auth interrupted`

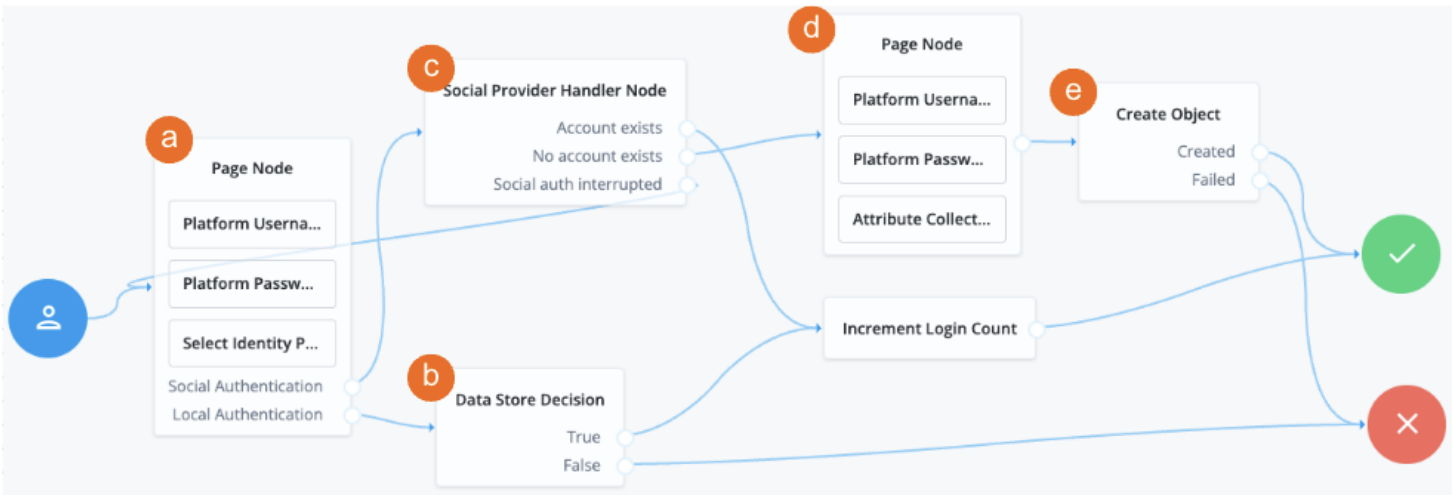
The user interrupted the social authentication journey after the node requested profile information from the social identity provider. This can happen in the following situations:

- The user clicks the **Back** button in their browser from the social identity provider's login page
- The user clicks the **Cancel** button on the social identity provider's login page
- The user re-enters the journey URL in the same browser window

In this case, the node routes the user back to the Select Identity Provider node to select a social identity provider again.

Example

This example shows the **Social Provider Handler** node in a social authentication journey.



a The Page node containing the Select Identity Provider node prompts the user to select a social identity provider or to authenticate with a username and password.

b If the user selects local authentication, the Data Store Decision node takes care of the authentication.

c If the user selects social authentication, the **Social Provider Handler** node does the following:

- Routes the user to the selected social provider to authenticate there
- Retrieves the user's profile information, and transforms it into a format that AM can use
- Assesses whether the user has an existing identity in AM
  - If the user has an existing identity, authenticates that identity
  - If the user doesn't have an identity, routes the user to another page node
  - If the user interrupts the social authentication, routes the user back to the Select Identity Provider node

d The nodes on the page node request the information required to *register* a new identity.

e The Create Object node creates the new identity in AM.

Legacy Social Provider Handler node

This legacy node is similar to the newer Social Provider Handler node. It takes a provider selection from the Select Identity Provider node and attempts to authenticate the user. The node collects relevant profile information from the provider, transforms the profile information into the appropriate attributes and returns the user to the journey.

This node remains supported in existing journeys. For new journeys, use the Social Provider Handler node instead.

Implement this node with the Select Identity Provider node to use the Social Identity Provider Service.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

`Account exists`

Social authentication succeeded, and a matching AM account exists.

`No account exists`

Social authentication succeeded, but no matching AM account exists.

Properties

Property	Usage
Transformation Script *(required)*	This script is used after the configured provider's *normalization* script has mapped the social identity provider's attributes to a profile format compatible with AM. The *transformation* script then transforms a normalized social profile to an identity (standalone AM) or a managed object (Ping Identity Platform deployment). Select `Normalized Profile to Identity`, `Normalized Profile to Managed User`, or a script you've created to transform the profile to an identity object. To view the scripts and bindings, refer to normalized-profile-to-identity.js. Normalization scripts (`<Identity provider>-profile-normalization.*`) are not suitable for this purpose.
Username Attribute	(Ping Identity Platform deployments only.) The attribute in IDM that contains the username for this object.
Client Type	Specify the client type you are using to authenticate to the provider. Use the default, `BROWSER`, with ForgeRock-provided user interfaces or the Ping SDK for JavaScript. This causes the node to return the RedirectCallback. Select `NATIVE` with the Ping SDKs for Android or iOS. This causes the node to return the IdPCallback.

Property	Usage
Store Tokens	When `true`, the node stores access and refresh tokens in the transient state for use by subsequent nodes in the journey. In some cases, the social provider requires these tokens, for example, to revoke user authorization. If you choose to store tokens, you can configure a Scripted Decision node later in the journey to handle your social provider use case. Default: `false`

Write Federation Information node

Creates a persistent link between a remote IdP account and a local account in the SP, if none exists yet. If a transient link exists, it is persisted. Existing account links with different IdPs are not lost.

Use this node with the SAML2 Authentication node, and ensure that the NameID Format is `persistent`.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

This node has no configurable properties.

Find examples of its use in SSO and SLO in integrated mode.

Identity management nodes

Accept Terms and Conditions node

The **Accept Terms and Conditions** node prompts the user to accept the currently active terms and conditions.

You set terms and conditions in the Ping Identity Platform admin UI. Learn more in Terms and conditions.

Use this node for registration, or combined with the Terms and Conditions Decision node for progressive profiling or log in.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None.

Dependencies

This node depends on IDM for the active terms and conditions.

Configuration

This node has no configurable properties.

Outputs

The node writes a `termsAccepted` object to the shared node state. The object contains these fields:

- `acceptDate`: A timestamp string indicating when the user accepted the terms.

- `termsVersion`: A string indicating the version of the accepted terms.

Outcomes

Single outcome path; the user accepted the terms and conditions.

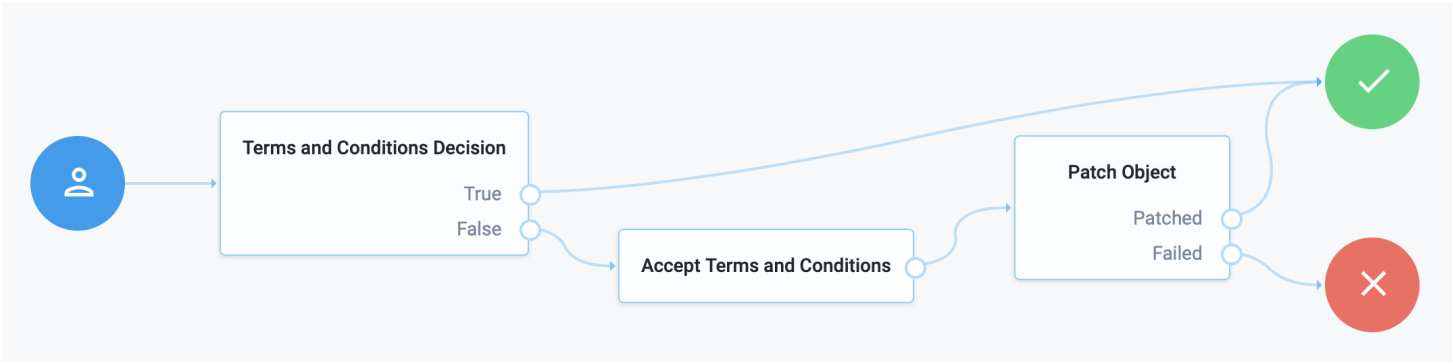
Errors

This node does not log error or warning messages of its own.

Example

For progressive profiling, include this node after a Terms and Conditions Decision node. If the user has not accepted the latest version of the terms and conditions, evaluation takes them to a page that requires them to accept the current terms and conditions.

The Patch Object node stores the acceptance response in IDM if the user accepts:



Attribute Collector node

The **Attribute Collector** node collects the values of attributes for use later in the flow; for example, to populate a new account during registration.

This node supports three types of attributes:
`string`
`boolean`
`number`

To request a value, the attribute must be present in the IDM schema of the current identity object.

The node lets you configure whether the attributes are required to continue and whether to use a policy filter of IDM to validate them.

Use the node alone or within a Page node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

For validation, this node reads the **Identity Attribute** (default: `userName`) from the shared node state. It uses the value to look up the identity object.

It prompts the user for the attributes to collect.

Dependencies

This node depends on IDM to store the user profile and perform validation.

Configuration

Property	Usage
Attributes to Collect	A list of the attributes to collect based on those in the IDM schema for the current identity object. Default: none
All Attributes Required	When enabled, all attributes collected in this node are required in order to continue. Default: false

Property	Usage
Validate Input	When enabled, validate the content against any policies specified in the IDM schema for each collected attribute. Learn more in Use policies to validate data in the IDM documentation. If you enable this property, the collected identity attributes must be *User Editable*. To make an attribute user-editable in the IDM admin UI: 1. Go to **Configure > Managed Objects > *object-name***. 2. Click the pencil (✎) icon, then click **Show advanced options**. 3. Select the **User Editable** toggle. Learn more in [Property Configuration Properties in the IDM documentation. Default: false
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

The node writes the attributes and their values to the shared node state.

Outcomes

Single outcome path; on success, downstream nodes can read the attributes from the shared node state.

Errors

This node does not log error or warning messages of its own.

Examples

Add date and datetime fields to a journey

> **Note**
>
> This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.

The **Attribute Collector** node lets you add properties (attributes) that follow a date or datetime (date and time of day). The format of the date comes from the locale set in your browser.

The following table displays the differences between date and datetime:

Display format	Managed object field format	Notes
Date only	String format	The format of the date comes from the locale set in your browser. For example, if the locale is English, then the format presented to the end user is `MM-DD-YYYY`. If the local is French, the format is `DD-MM-YYYY`.
Date and time	String format (date and time of day)	The format of the date comes from the locale set in your browser. For example, if the locale is English (United States), then the format presented to the end user is `MM-DD-YYYY`. If the local is French, the format is `DD-MM-YYYY`.

Note

While the rendering of the date to the end user changes depending on the locale set in the browser, Ping Identity Platform *stores* the date value in UTC format as `YYYY-MM-DDHH:MM:SS`. For example, `2023-09-13T08:01:00Z`.

To render the date or datetime UI element to an end user with the **Attribute Collector** node, you must:

1. Specify the IDM property:
   - In the Ping Identity Platform admin UI, go to **Configure** > **Managed Objects** > *Select object*, for example, **User**.
   - Use an existing `string` property or create your own string property. Learn more in Property Configuration Properties in the IDM documentation.
2. Apply formatting and policies to the property in the IDM admin UI for `Date` or `Datetime`.

Apply formatting and policies

1. In the Advanced Identity Cloud admin UI, go to **Configure** > Managed Objects > *Select object*, for example, **User**.
2. Select the property to use.
3. To select the format of the attribute, on the **Details** tab, click the **Format** field, and select one of the following:
   - For date property — `Date`
   - For datetime property — `Datetime`
4. Click **Save**.
5. On the **Validation** tab, click **+ Add Policy**.
6. In the **Policy Id** field, enter one of the following:
   - For date property — `valid-formatted-date`
   - For datetime property — `valid-datetime`

   Learn more about applying policies to properties in Default policy reference.

7. Click **Add**.

8. In your journey, in the **Attribute Collector** node, add the property name to the **Attributes to Collect** field.

For an in-depth use case, add the date or datetime property to an **Attribute Collector** node in a registration flow. Learn more in User self-registration.

The following video shows an example of a journey collecting the datetime from an end user using the Attribute Collector node:

Your browser does not support the video tag.

Attribute Present Decision node

The **Attribute Present Decision** node checks whether an attribute is present on an object, including private attributes. There is no need to specify the value of the attribute.

Use this node during an update password flow to check whether the local account has a password, for example.

This node is similar to the Attribute Value Decision node when that node is set to use the `PRESENT` operator, except it can't return the value of the attribute, but can work with private attributes.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the **Identity Attribute** from the shared node state. If it can't read the **Identity Attribute**, it reads the `userName` from the shared node state.

It uses the value to look up the identity object.

Dependencies

This node depends on IDM to look up the user object.

Configuration

Property	Usage
Present Attribute	The attribute whose presence you want to verify in the IDM object. This can be an otherwise private attribute, such as `password`. **Note** This field is case-sensitive and must match the IDM object attribute. For example, `givenName`, not `givenname`. Default: `password`
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

None.

Outcomes

`True`

The node found the attribute in the managed identity object.

`False`

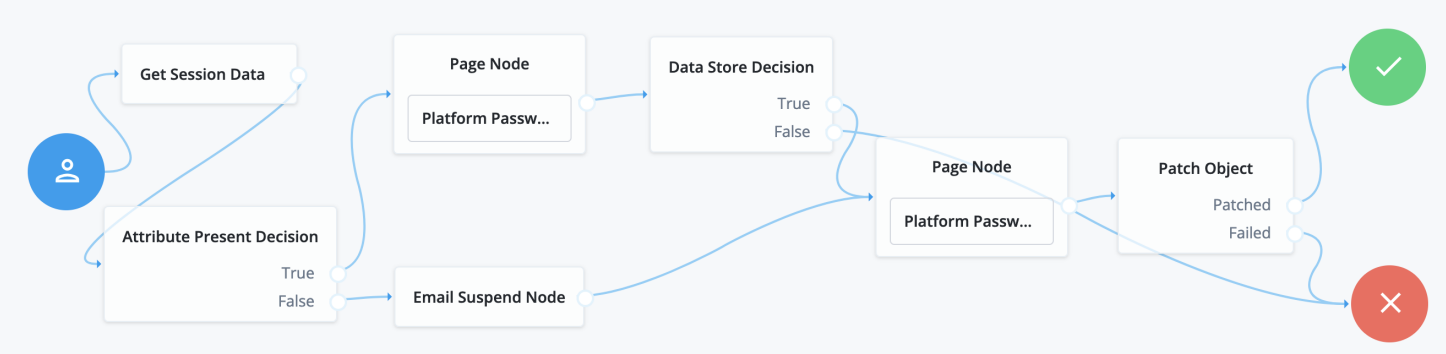
Any other case.

Errors

This node does not log error or warning messages of its own.

Example

This journey to update a password uses the **Attribute Present Decision** node to check whether the account has a password:



The user has already authenticated before beginning this journey:

- The Get Session Data node stores the `userName` from the session.
- The **Attribute Present Decision** node checks whether the user object has a password attribute.
- If so, the first Page node with the Platform Password node prompts the user for the current password.
- Otherwise, the Email Suspend node sends an email to the user and suspends the flow until the user follows the link in the message.
- The Data Store Decision node confirms the username-password credentials.
- The second Page node with the Platform Password node prompts the user for the new password.
- The Patch Object node updates the user object with the new password.

Attribute Value Decision node

Verifies that the specified attribute satisfies a specific condition.

Use this node to check whether an attribute's expected value is equal to a collected attribute value, or to validate that the specified attribute was collected.

Examples:

- To validate that a user provided the country attribute during registration, set the comparison operation to `PRESENT`, and the comparison attribute to `country`.
- To validate that the country attribute is set to the United States, set the comparison operation to `EQUALS`, the comparison attribute to `country`, and the comparison value to `United States`.

Use Attribute Present Decision node instead when you need to check for the presence of a private attribute, such as `password`.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Properties

Property	Usage
Comparison Operation	The operation to perform on the object attribute: **PRESENT** Checks the existence of an attribute regardless of its value. **EQUALS** Checks if the object's attribute value equals the configured comparison value.
Comparison Attribute	The object attribute to compare.
Comparison Value	When **Comparison Operation** is `EQUALS`, compare this value to the provided attribute value.
Identity Attribute	The attribute used to identify the managed object in IDM.

Consent Collector node

Prompts the user for consent to share their profile data.

A consent notice is listed for each identity mapping that has consent enabled. If an identity mapping is not created, or the mappings do not have privacy and consent enabled, AM does not show a consent message to the user.

This node is primarily used in progressive profile and registration flows.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Properties

Property	Usage
All Mappings Required	If enabled, all mappings listed by this node require consent in order to move forward.
Privacy & Consent Message	Localized message providing the privacy and consent notice. The key is the language, such as `en` or `fr`, and the value is the message to display.

Create Object node

The **Create Object node** lets you create a new object in IDM based on information collected during authentication, such as user registration.

Any managed object attributes that are marked as required in IDM must be collected during authentication in order to create the new object.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the managed object attributes marked as required

Configuration

Property	Usage
Identity Resource	The type of managed identity resource object that this node creates. It must match the identity resource type for the current flow. **Tip** To check for the available managed identity resource types, go to the IDM admin UI, and open the **Manage** drop-down list in the upper right corner of the screen. Identity managed object types are preceded by the icon. Default: `managed/user`

Outputs

This node doesn't change the shared state.

Outcomes

This node has the following outcomes:

- Created
- Failed

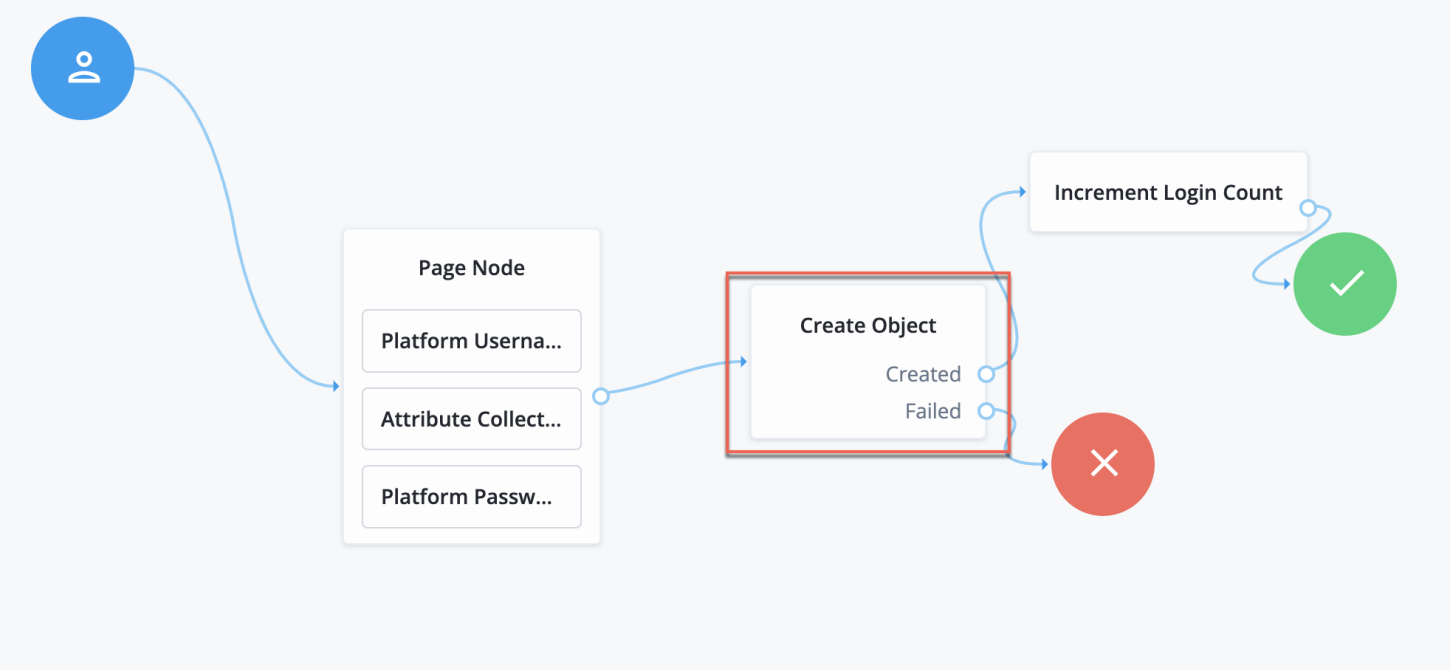
Errors

This node can log the following warning messages:

Message	Notes
Failed to create object	The preceding nodes don't provide all the fields required to create the object.
Failed to retrieve object's schema	The node failed to get the list of required attributes from the **Identity Resource** schema.

Example

The following example uses this node with the Increment Login Count node to create a new user object.



- The Page node includes various nodes that collect attributes and store them in the shared node state.
- The Create Object node uses these attributes to create the new user.
- The Increment Login Count node resets the retry count on successful authentication of the new user.

Create Password node

Lets users create a password when provisioning an account.

> **Note**
>
> This node and its related services are deprecated.
> You can find information on the new methods for implementing social authentication in Social authentication.

Social identity providers do not provide a user's password. Use this node to provide a password to complete the user's credentials before provisioning an account.

> **Important**
>
> The flow must provision an account after prompting the user for a password, for example, by using the Provision Dynamic Account node. If no account is provisioned, the flow does not save the password.
> Do not place any nodes that request additional input from the user between this node and the provisioning node; otherwise, the password is lost.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

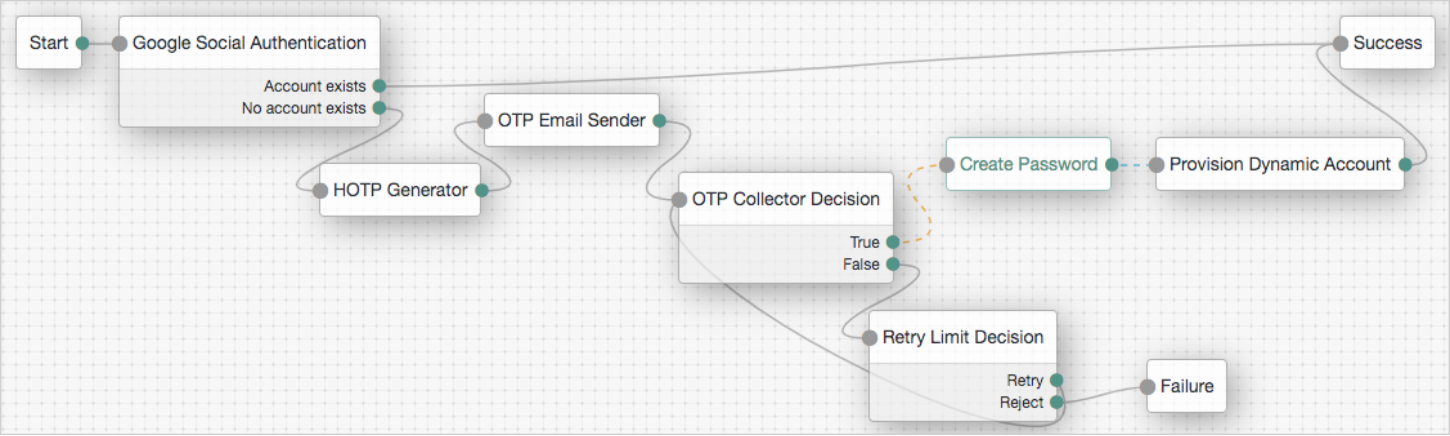
Single outcome path.

Properties

Property	Usage
minPasswordLength	Specifies the minimum number of characters the password must contain.

Example

The following example lets users who have performed social authentication using Google provide a password and provision an account when they don't have one. They must enter a one-time passcode to verify they are the owner of the Google account.



Display Username node

Fetches a username based on a different identifying attribute, such as an email address, then displays it.

To email the username to the user instead, use the Identify Existing User node combined with a Email Suspend node or Email Template node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Properties

Property	Usage
User Name	The attribute used to identify the username in an IDM object.
Identity Attribute	The attribute used to identify the managed object in IDM. When this node serves to recover a username, the identity attribute should be some other attribute that is unique to a user object, such as the email address. The node raises an exception when more than one value exists for this attribute. Make sure the value of whatever attribute you select is unique for each user.

Identify Existing User node

The **Identify Existing User** node verifies if a user exists based on an identifying attribute, such as an email address, then makes the value of a specified attribute available in the shared node state.

Use this node in a forgotten password flow to fetch a username to email to the user. To display the username on the screen, use the Display Username node instead.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the **Identity Attribute** (default: `mail`) from the shared node state.

If the **Identity Attribute** is not available, it reads the `userName` from the shared node state.

Dependencies

This node depends on IDM to store the user profile.

Configuration

Property	Usage
Identifier	The attribute to collect from a managed identity object. Default: `userName`
Identity Attribute	The attribute used to identify the managed object in IDM. When this node serves to recover a username, the identity attribute should be some other attribute that is unique to a user object, such as the email address. Default: `mail`

Outputs

The node writes the **Identifier** and the user account `_id` to the shared node state.

If the **Identifier** differs from `userName`, this node also writes the `userName` to the shared node state.

Outcomes

True

The node successfully identified the user and updated the shared node state.

`False`

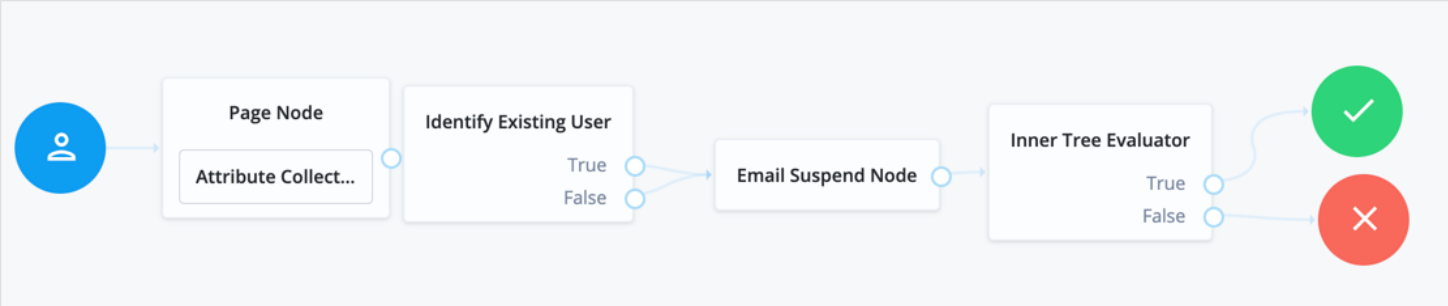
Any other case.

Errors

This node does not log error or warning messages of its own.

Example

The following example shows a flow to reset a forgotten password:



- The user enters their email in the Attribute Collector node of the Page node.
- The **Identify Existing User** node uses the email address to look up the username of the user's account. If it finds the user account, it adds the username to the shared node state.
- The Email Suspend node emails the user and suspends authentication.
- Once authentication resumes, the Inner Tree Evaluator node sends the user to a different flow to reset their password.

KBA Decision node

Checks whether the user account has the required minimum number of KBA questions.

To set the number of KBA questions, edit **Configure > Security Questions > Questions > Number** in the IDM admin UI.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes

Product	Available?
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Evaluation continues along the `True` path if the user profile holds at least the minimum number of KBA questions; otherwise, evaluation continues along the `False` path.

Properties

Property	Usage
Identity Attribute	The attribute used to identify the managed object in IDM.

KBA Definition node

The **KBA Definition** node collects knowledge-based authentication (KBA) questions and answers.

Use this node when creating or updating a user with KBA enabled. Learn more in Security questions.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None. This node doesn't require any attributes from the shared node state.

Dependencies

This node depends on IDM for the KBA configuration.

Configuration

Property	Usage
Purpose Message	A localized message describing the purpose of the data requested from the user. Default: none
Allow User-Defined Questions	When enabled, users can create their own KBA questions. Disable this setting to restrict users to select from predefined questions only. Default: Enabled
Questions	Create or modify custom localized questions that the user can choose from when defining security questions. To add a localized security question: 1. Click **+** to open the **Add a Security Question** form. 2. Select from the list of existing locales or add a new locale, type a question into the text field, and click **Done**. 3. Repeat to add further questions, and click **Save** when complete. To edit an existing security question, click the edit icon, make your changes, and click **Save**. Default: `What's your favorite color?` (locale: `en`)

Outputs

The node writes the KBA questions and answers in the transient shared node state.

Outcomes

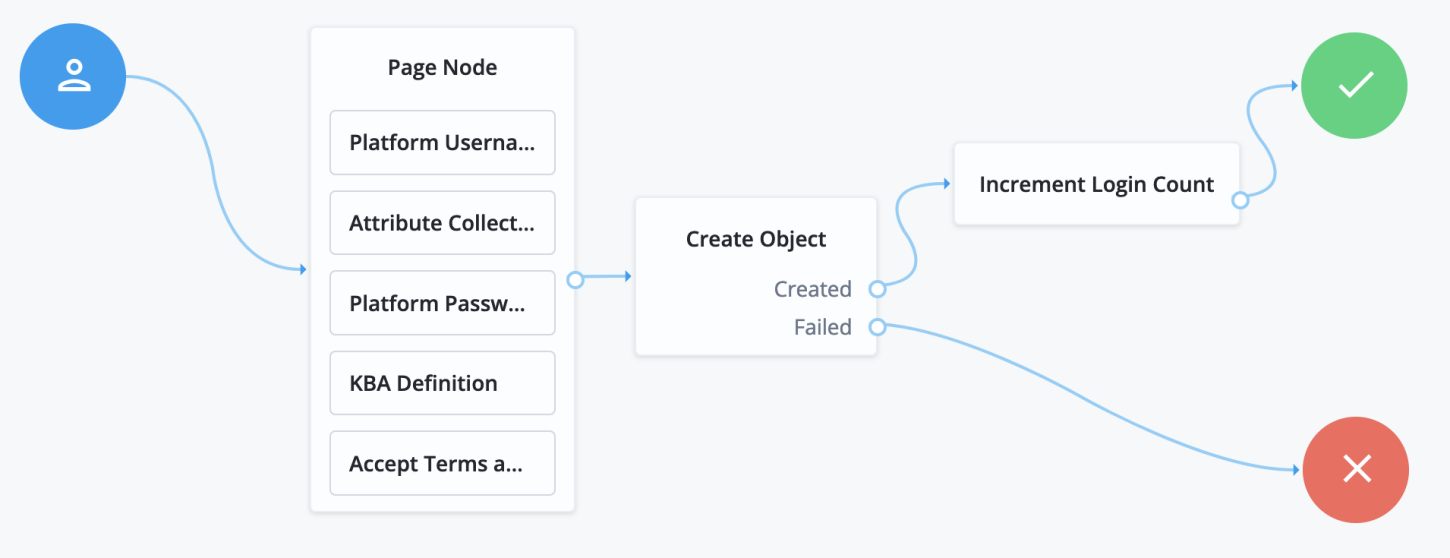
Single outcome path; on success, the transient state holds the questions and answers.

Errors

This node logs a `Failed to retrieve kba configuration` warning message when it can't read the configuration.

Example

The following registration journey prompts for questions and answers when creating an account:



- The Page node collects registration information:
  - The Platform Username node prompts for and collects a username for the new account.
  - The Attribute Collector node prompts for a given name, a surname, an email address, and profile preferences.
  - The Platform Password node prompts for and collects a password.
  - The **KBA Definition** node collects questions and answers.
  - The Accept Terms and Conditions node prompts the user to accept the active terms and conditions.
- The Create Object node stores the collected information in the new account object.
- The Increment Login Count node updates the number of successful authentications.

KBA Verification node

Presents KBA questions to the user, collects answers to those questions, and verifies the input against the user's stored answers.

Use this node for additional authentication when resetting a forgotten password or username.

To set the number of KBA questions, edit **Configure > Security Questions > Questions > Number** in the IDM admin UI.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Properties

Property	Usage
KBA Attribute	The managed object attribute in which KBA questions and answers are stored.
Identity Attribute	The attribute used to identify the managed object in IDM.

Pass-through Authentication node

Authenticates an identity through a connector to a third-party service.

This lets you migrate user profiles without forcing users to reset their passwords, or retain a third-party service indefinitely as the canonical store for authentication credentials.

Before you use the node:

- Configure the connector to the third-party service.

  Learn more in the OpenICF documentation.

- If you plan to collect credentials in the identity repository for users, synchronize accounts from the third-party service.

  Learn more in Synchronization in the IDM documentation.

Inputs

This node requires the `username` and `password` properties in the incoming node state. Implement the following nodes earlier in the journey:

- Standalone PingAM deployment
  - Username Collector node
  - Password Collector node

- Ping Identity Platform deployment:
  - Platform Username node
  - Platform Password node

Pass the credentials to this node to authenticate the identity against the service.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Connectors that support pass-through authentication

The following connectors support pass-through authentication using the `AuthenticateOp` interface by default:

- LDAP connector
- CSV file connector
- Database Table connector
- Microsoft Graph API Java connector
- Scripted SQL connector

Note

All Scripted Groovy-based connectors are capable of pass-through authentication if the `AuthenticateScript.groovy` script is implemented, but the only default implementation is the ScriptedSQL connector. Learn more in Authenticate script and Authenticate operation.

Outcomes

- `Authenticated`
- `Missing Input`
- `Failed`

Properties

Property	Usage
System Endpoint	Required. Name of the connector to the third-party service that performs authentication.
Object Type	The OpenICF object type for the object being authenticated. Default: `account`
Identity Attribute	The username attribute for authentication. Default: `userName`
Password Attribute	The password attribute for authentication. Default: `password`

Example

The following example requires a Ping Identity Platform deployment.

Before trying this example, synchronize accounts from the third-party service. The example shows a login flow that tries pass-through authentication when local authentication fails, and stores the user password when authentication with the third-party service succeeds.

In this example, the user enters their credentials with the Platform Username node and Platform Password node. The Data Store Decision node authenticates against the platform directory service. On failure, authentication passes through to the third-party service. If authentication with the third-party service is successful, the Identify Existing User node and Required Attributes Present node check for a valid user profile. The Patch Object node updates the user's profile with the successful password:

List of node connections

Source node	Outcome path	Target node
Page Node containing: • Platform Username • Platform Password	→	Data Store Decision
Data Store Decision	True	Increment Login Count
	False	Pass-through Authentication
Pass-through Authentication	Authenticated	Identify Existing User
	Missing Input	Page Node
	Failed	Failure
Identify Existing User	True	Required Attributes Present
	False	Increment Login Count
Required Attributes Present	True	Patch Object
	False	Increment Login Count
Patch Object	Patched	Increment Login Count
	Failed	Increment Login Count
Increment Login Count	→	Inner Tree Evaluator
Inner Tree Evaluator	True	Success
	False	Failure

Patch Object node

The **Patch Object** node updates the attributes of an existing managed identity object.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the **Identity Attribute** and the managed object fields to patch from the shared node state. If it can't read the **Identity Attribute**, it reads the `userName` from the shared node state.

Dependencies

This node depends on IDM to find and patch the managed object.

Configuration

Property	Usage
Patch as Object	If enabled, update the object as its subject—for example, update a managed user object as the user; otherwise, update the object as the client application. Enable this property to patch fields of the current, authenticated user's account the client application can't update. Default: false
Ignored Fields	Omit the specified shared state fields from the patch. If no fields are specified, the node attempts to update all the shared state fields as part of the patch. Default: none
Identity Resource	The type of managed identity resource object this node patches. This must match the identity resource type for the current flow. **Tip** To check for the available managed identity resource types, go to the IDM admin UI, and open the **Manage** drop-down list in the upper right corner of the screen. Identity managed object types are preceded by the icon. Default: `managed/user`
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

None.

Outcomes

`Patched`

The node updated the managed object.

`Failed`

Any other case.

Errors

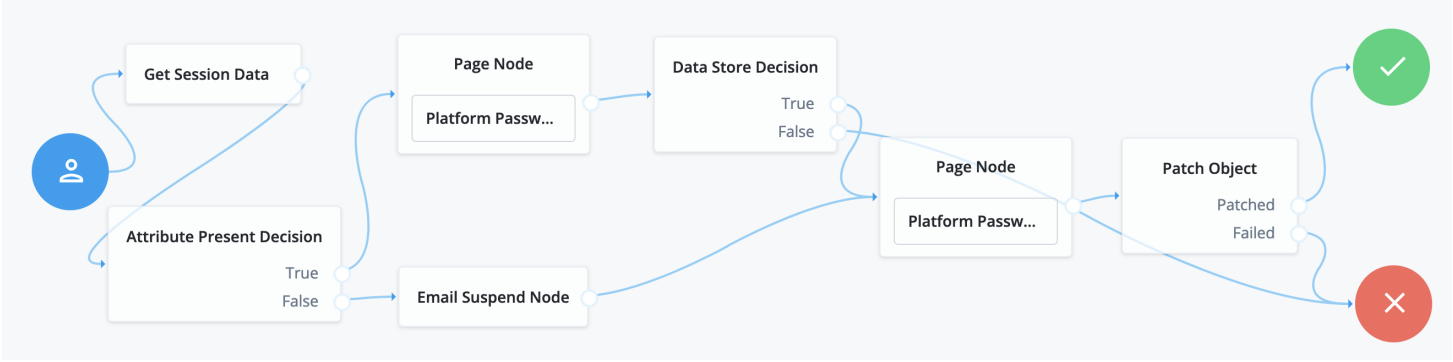
This node logs the following warning messages when an update fails:

- `Failed to create object`
- `Failed to patch object`

Review the logs for additional messages describing the problem.

Example

This journey uses the **Patch Object** node to update a user's password:



The user has already authenticated before beginning this journey:

- The Get Session Data node stores the `userName` from the session.
- The Attribute Present Decision node checks whether the user object has a password attribute.
- If so, the first Page node with the Platform Password node prompts the user for the current password.
- Otherwise, the Email Suspend node sends an email to the user and suspends the flow until the user follows the link in the message.
- The Data Store Decision node confirms the username-password credentials.

- The second Page node with the Platform Password node prompts the user for the new password.
- The **Patch Object** node updates the user object with the new password.

PingOne Create User node

The **PingOne Create User** node can create new users in the PingOne platform.

You can configure the node to create a user including their profile data or to create an anonymized user.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

You must also verify the user's identity by using a Data Store Decision node.tity-store-decision.adoc[].]

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can authenticate to your PingOne instance.

You can find information on the properties used by the service in PingOne Worker service.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Population ID	The ID of the population in PingOne to check for users or provision new ones. If not specified, the node uses the environment's default population ID.

Property	Usage
Anonymized user	When enabled, the node creates a user in PingOne with only a unique identifier and a language attribute. It does not add any other profile attributes, helping prevent any personally identifiable information (PII) from being shared.
AM Identity Attribute	The attribute from the user's AM profile that the node uses as the username for the account created in PingOne. **Tip** When creating anonymized users, choose a profile attribute that does not contain PII. Default: `uid`
Capture failure	Capture the details in shared state if a failure occurs. The node stores the details in a variable named `pingOneCreateUserFailureReason`. Default: `False` Example: `{ "code": "MISSING_ATTRIBUTE_FROM_PROFILE", "message": "Could not get attribute from user profile.", "exception": "", }`

Outputs

The node is non-interactive and does not send a callback to the client.

If the node was able to create a new user in PingOne it stores the PingOne user identifier in a state variable named `pingOneUserId`. For example `a648aaac-ch15-b357-457b-8d2e714180ff`.

If you select **Capture failure**, the node stores any error response in a shared state variable named `pingOneCreateUserFailureReason`.

Outcomes

`True`

The node created an account in PingOne.

`False`

The node did not create an account in PingOne.

The journey also uses this outcome if any error occurs. Enable **Capture Failure** to store the details in node state.

Example

The following example journey leverages PingOne Verify to perform user identity verification.

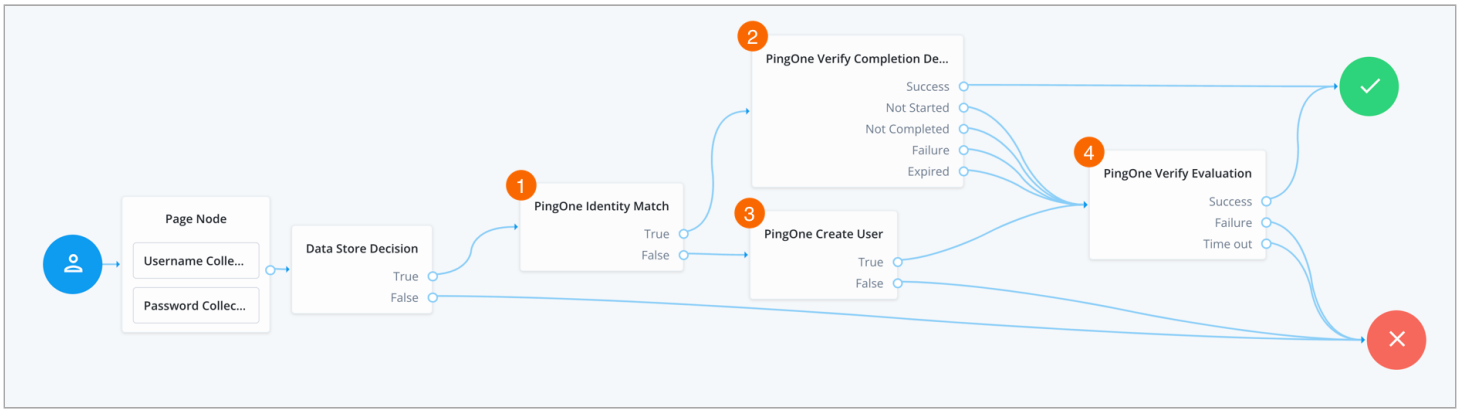


Figure 1. Example PingOne Verify journey

- The user enters their credentials, which the Data Store Decision node then verifies against the identity store.
- 1 The PingOne Identity Match node checks PingOne for a matching user.
- 2 If a user is found, the PingOne Verify Completion Decision node checks the user's most recent verification transaction to determine the status:

Success

The user successfully completed the most recent PingOne Verify transaction, so continue directly to the **Success** node, completing the authentication journey.

Not Completed

The user has an existing PingOne Verify transaction in progress, so continue the journey to resume the existing verification transaction.

The node adds the user's existing transaction ID to the shared node state in a variable named `pingOneVerifyTransactionId`.

Not Started / Failure / Expired

The user either does not have an existing transaction (`Not Started`), or did not successfully complete the most recent PingOne Verify transaction, or it expired, so continue the journey to start a new verification transaction.

- 3 If a user is not found, the PingOne Create User node creates a new user in PingOne.
- 4 The PingOne Verify Evaluation node starts a new PingOne Verify evaluation, or continues an existing one if `pingOneVerifyTransactionId` is present in the shared node state, and either completes or fails the journey based on the result.

PingOne Delete User node

The **PingOne Delete User** node can delete users from the PingOne platform.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `pingOneUserId` variable from node state. The variable must contain the identifier of the user to delete from PingOne. For example, `a648aaac-ch15-b357-457b-8d2e714180ff`.

Use either of the following nodes to populate the `pingOneUserId` variable in shared state:

- PingOne Identity Match node
- PingOne Create User node

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can authenticate to your PingOne instance.

You can find information on the properties used by the service in PingOne Worker service.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Capture failure	Capture the details in shared state if a failure occurs. The node stores the details in a variable named `pingOneDeleteUserFailureReason`. Default: `False` Example: `{ "code": "MISSING_PINGONE_USER_ID", "message": "Expected PingOne User ID to be set in sharedState or user's profile.", "exception": "", }`

Outputs

The node is non-interactive and does not send a callback to the client.

If you select **Capture failure**, the node stores any error response in a shared state variable named `pingOneDeleteUserFailureReason`.

Outcomes

`True`

The node deleted the account from PingOne.

`False`

The node did not delete the account from PingOne.

The journey also uses this outcome if any error occurs. Enable **Capture Failure** to store the details in node state.

PingOne Identity Match node

The **PingOne Identity Match** node checks that users that exist in the ForgeRock platform also exist in the PingOne platform.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

You must also verify the user's identity by using a Data Store Decision node.

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can authenticate to your PingOne instance.

Find information on the properties used by the service in PingOne Worker service.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Population ID	The ID of the population in PingOne to check for users or provision new ones. If not specified, the node uses the environment's default population ID.
AM Identity Attribute	The attribute from the user's ForgeRock profile that the node uses to match their account in PingOne. Default: `uid`
Ping Identity Attribute	The attribute from the user's PingOne profile that the node uses to search for a matching account. If there are multiple entries with the same attribute value in the PingOne directory server, ensure that this property is specific enough to retrieve only one entry. Default: `username`
Capture failure	Capture the details in shared state if a failure occurs. The node stores the details in a variable named `pingOneIdentityMatchFailureReason`. Default: `False` Example: `{ "code": "ACCESS_TOKEN", "message": "Unable to get access token for PingOne Worker.", "exception": "", }`

Outputs

The node is non-interactive and does not send a callback to the client.

If the node was able to find a unique match in PingOne it stores the PingOne user identifier in a state variable named `pingOneUserId`. For example `a648aaac-ch15-b357-457b-8d2e714180ff`.

If you select **Capture failure**, the node stores any error response in a shared state variable named `pingOneIdentityMatchFailureReason`.

Outcomes

`True`

The node found a unique matching account in PingOne.

`False`

The node did not find a unique match in PingOne.

Example

The following example journey leverages PingOne Verify to perform user identity verification.

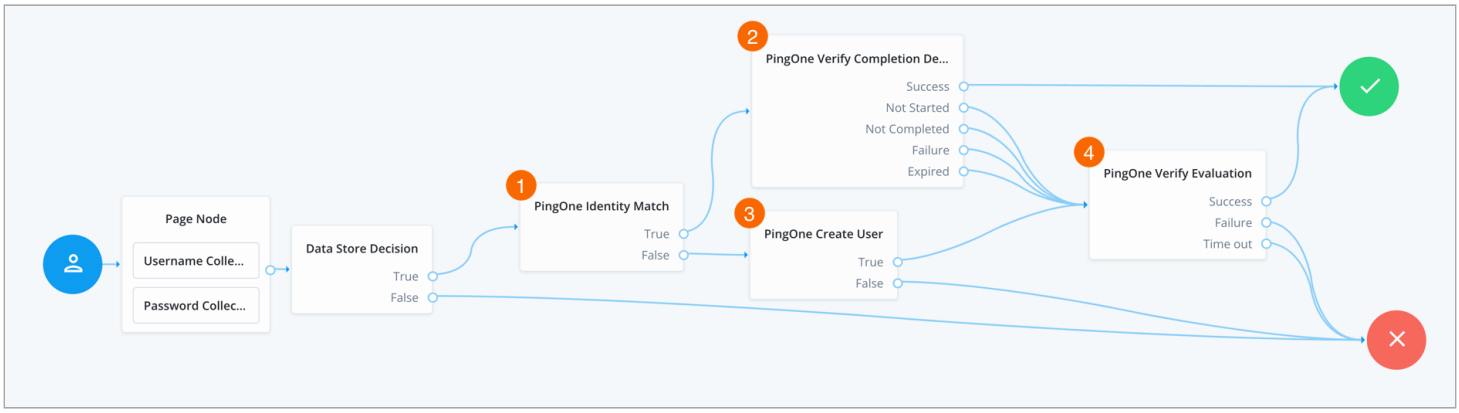


Figure 1. Example PingOne Verify journey

- The user enters their credentials, which the Data Store Decision node then verifies against the identity store.
- 1 The PingOne Identity Match node checks PingOne for a matching user.
- 2 If a user is found, the PingOne Verify Completion Decision node checks the user's most recent verification transaction to determine the status:

Success

The user successfully completed the most recent PingOne Verify transaction, so continue directly to the **Success** node, completing the authentication journey.

Not Completed

The user has an existing PingOne Verify transaction in progress, so continue the journey to resume the existing verification transaction.

The node adds the user's existing transaction ID to the shared node state in a variable named `pingOneVerifyTransactionId`.

Not Started / Failure / Expired

The user either does not have an existing transaction (`Not Started`), or did not successfully complete the most recent PingOne Verify transaction, or it expired, so continue the journey to start a new verification transaction.

- 3 If a user is not found, the PingOne Create User node creates a new user in PingOne.
- 4 The PingOne Verify Evaluation node starts a new PingOne Verify evaluation, or continues an existing one if `pingOneVerifyTransactionId` is present in the shared node state, and either completes or fails the journey based on the result.

PingOne Verify Completion Decision node

The **PingOne Verify Evaluation** node determines the completion status of the most recent identity verification transaction for a PingOne user.

The node checks the previous identity verification transaction for the user and returns an outcome based on the verification status.

You can use this node to prevent users from repeatedly having to verify their identity by checking their most recent verification transaction. You can also determine if a transaction is already in progress, to prevent multiple ongoing transactions.

For further customization of behavior, use a **PingOne Verify Completion Decision** script to evaluate the verification transactions started for the specified PingOne user, and the associated metadata. The script can then add additional context to the journey, or perform additional business logic, dependent on the verification metadata.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires that the user has an account in the PingOne environment. It requires that the journey stores the PingOne user ID for the account in the shared state variable named `pingOneUserId`.

Use a PingOne Identity Match node to populate the shared state with the user's PingOne ID.

The shared state data must also include all required **Script Inputs** properties.

You can restrict available inputs using the **Script Inputs** field when configuring the node.

Dependencies

This node requires a **PingOne Worker Service** configuration so that it can connect to your PingOne instance and send it the necessary data to perform PingOne Verify evaluations as part of the journey.

You can find information on the properties used by the service in PingOne Worker service.

Configuration

Property	Usage
PingOne Worker service ID	The ID of the PingOne worker service for connecting to PingOne.

Use a script to process Verify transactions	When enabled, use a **PingOne Verify Completion Decision** script to process verification transaction data relating to the user.

```
{
    "_links": {
        "self": {
            "href": "https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-
a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/verifyTransactions"
        }
    },
    "_embedded": {
        "verifyTransactions": [
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/029ea878-2618-4067-b7e3-922591e6b55f"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "029ea878-2618-4067-b7e3-922591e6b55f",
                "transactionStatus": {
                    "status": "APPROVED_NO_REQUEST"
                },
                "createdAt": "2022-02-17T20:32:22.052Z",
                "updatedAt": "2022-02-17T20:32:58.711Z",
                "expiresAt": "2022-02-17T21:02:58.711Z"
            },
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/cca479e7-d130-4e3c-b888-74ba1920f59a"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "cca479e7-d130-4e3c-b888-74ba1920f59a",
                "transactionStatus": {
                    "status": "REQUESTED"
                },
                "qrUrl": "https://api.pingone.com/v1/idValidations/shortcode/
086645084110/qr",
                "verificationCode": "086645084110",
                "createdAt": "2022-02-17T20:23:58.662Z",
                "updatedAt": "2022-02-17T20:23:58.662Z",
                "expiresAt": "2022-02-17T20:53:58.662Z"
            },
```

```
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/52c9bf9a-0687-4e01-85d1-9caa9bb387ee"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "52c9bf9a-0687-4e01-85d1-9caa9bb387ee",
                "transactionStatus": {
                    "status": "REQUESTED"
                },
                "qrUrl": "https://api.pingone.com/v1/idValidations/shortcode/
008299320746/qr",
                "verificationCode": "008299320746",
                "createdAt": "2022-02-17T20:23:08.887Z",
                "updatedAt": "2022-02-17T20:23:08.887Z",
                "expiresAt": "2022-02-17T20:53:08.887Z"
            },
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/dd5a6d4f-a999-4819-b107-85a0a10138c6"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "dd5a6d4f-a999-4819-b107-85a0a10138c6",
                "transactionStatus": {
                    "status": "REQUESTED"
                },
                "createdAt": "2021-12-09T13:45:34.882Z",
                "updatedAt": "2021-12-09T13:45:34.882Z",
                "expiresAt": "2022-12-09T14:15:34.882Z"
            },
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/bfc414cb-a1b4-46b8-b622-3d806a85002f"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
```

```
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "bfc414cb-a1b4-46b8-b622-3d806a85002f",
                "transactionStatus": {
                    "status": "REQUESTED"
                },
                "createdAt": "2021-12-08T21:34:52.424Z",
                "updatedAt": "2021-12-08T21:34:52.424Z",
                "expiresAt": "2022-12-08T22:04:52.424Z"
            },
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/b21db4c4-01c5-47b5-a2a9-3d8df21d189b"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "b21db4c4-01c5-47b5-a2a9-3d8df21d189b",
                "transactionStatus": {
                    "status": "APPROVED_NO_REQUEST"
                },
                "createdAt": "2021-12-07T21:33:22.088Z",
                "updatedAt": "2021-12-07T21:45:22.944Z",
                "expiresAt": "2022-12-07T22:15:22.944Z"
            },
            {
                "_links": {
                    "self": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
verifyTransactions/e44ebfe2-6a76-4ffa-ac35-d71ee9365e57"
                    },
                    "environment": {
                        "href": "https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
                    },
                    "user": {
                        "href": "https://api.pingone.com/v1/users/36ff33da-
cba7-4d46-bedc-8b242889d461"
                    }
                },
                "id": "e44ebfe2-6a76-4ffa-ac35-d71ee9365e57",
                "transactionStatus": {
                    "status": "APPROVED_NO_REQUEST"
                },
                "createdAt": "2021-12-07T19:55:16.630Z",
                "updatedAt": "2021-12-07T21:31:26.835Z",
                "expiresAt": "2022-12-07T22:01:26.835Z"
```

Property	Usage

	{
	            },
	            {
	                "_links": {
	                    "self": {
	                        "href": "https://api.pingone.com/v1/environments/
	abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/36ff33da-cba7-4d46-bedc-8b242889d461/
	verifyTransactions/fc695b11-93a4-48bb-9ec3-ff5738e3818c"
	                    },
	                    "environment": {
	                        "href": "https://api.pingone.com/v1/environments/
	abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
	                    },
	                    "user": {
	                        "href": "https://api.pingone.com/v1/users/36ff33da-
	cba7-4d46-bedc-8b242889d461"
	                    }
	                },
	                "id": "fc695b11-93a4-48bb-9ec3-ff5738e3818c",
	                "transactionStatus": {
	                    "status": "REQUESTED"
	                },
	                "createdAt": "2021-12-07T18:36:48.156Z",
	                "updatedAt": "2021-12-07T18:36:48.156Z",
	                "expiresAt": "2021-12-07T19:06:48.153Z"
	            }
	        ]
	    },
	    "size": 8
	}
	For more information on verification transaction data, refer to Read All Verify Transactions.

Manage Verify transactions script	The name of the script to process the JSON containing verification transactions relating to the user. The script must be of type **PingOne Verify Completion Decision**. Refer to Example scripts.
Script Inputs	Optionally, list the shared state data properties required by the script. Declare each required property, enter `null` for no properties, or set to `*` for access to all shared and transient state data. Default: `*`.

Capture failure	Capture the details in shared state if a failure occurs.
	The node stores the details in a variable named `pingOneVerifyCompletionFailureReason`.
	Default: `False`
	Example:
	{
	  "code": "VERIFY_COMPLETION_SCRIPT_ERROR",
	  "message": "Error evaluating the verify completion decision script.",
	  "exception": "",
	}

Outputs

The node is non-interactive and doesn't send a callback to the client.

If the node discovers that the user's most recent Verify transaction isn't yet complete, it adds the ID of the transaction to the shared state, in a variable named `pingOneVerifyTransactionId`. The PingOne Verify Evaluation node can use this value to continue the existing Verify evaluation, rather than start a brand new one.

If you select **Capture failure**, the node stores any error response in a shared state variable named `pingOneVerifyCompletionFailureReason`.

If you enable the **Use a script to process Verify transactions** property, the script you specify can add values to the shared state, as required.

Outcomes

`Success`

The user successfully completed their most recent PingOne Verify evaluation.

`Failure`

The user did not successfully complete their most recent PingOne Verify evaluation, or an error occurred.

`Expired`

The user's most recent PingOne Verify evaluation timed out. Usually this happens when a user starts a verification transaction, but does not complete it within the time limit.

`Not Started`

The user's most recent PingOne Verify evaluation has not yet started.

`Not Completed`

The user's most recent PingOne Verify evaluation has started, but not yet completed.

Examples

Example journey

The following example journey leverages PingOne Verify to perform user identity verification.

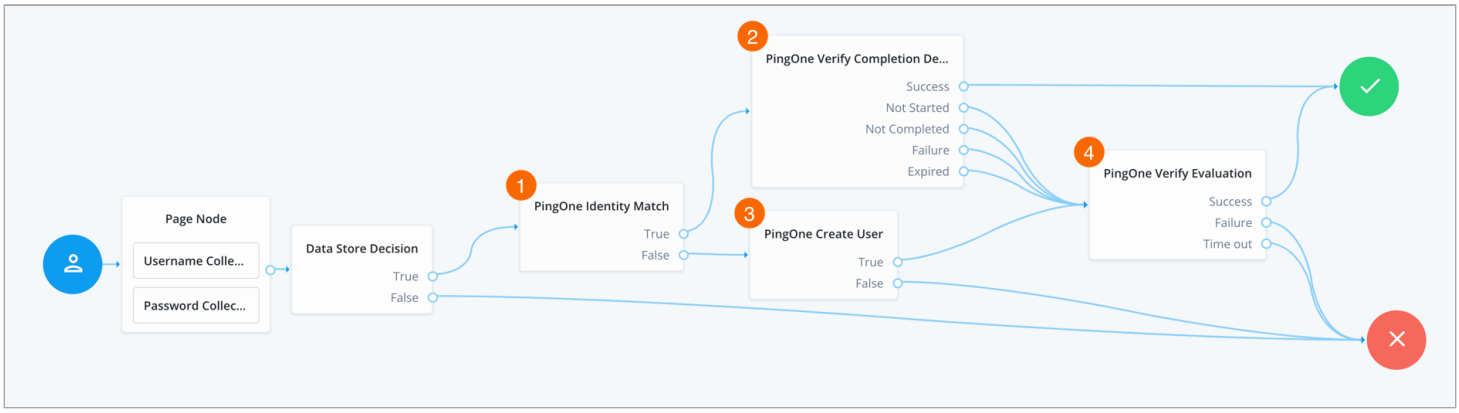


Figure 1. Example PingOne Verify journey

- The user enters their credentials, which the Data Store Decision node then verifies against the identity store.
- 1 The PingOne Identity Match node checks PingOne for a matching user.
- 2 If a user is found, the PingOne Verify Completion Decision node checks the user's most recent verification transaction to determine the status:

Success

The user successfully completed the most recent PingOne Verify transaction, so continue directly to the **Success** node, completing the authentication journey.

Not Completed

The user has an existing PingOne Verify transaction in progress, so continue the journey to resume the existing verification transaction.

The node adds the user's existing transaction ID to the shared node state in a variable named `pingOneVerifyTransactionId`.

Not Started / Failure / Expired

The user either does not have an existing transaction (`Not Started`), or did not successfully complete the most recent PingOne Verify transaction, or it expired, so continue the journey to start a new verification transaction.

- 3 If a user is not found, the PingOne Create User node creates a new user in PingOne.
- 4 The PingOne Verify Evaluation node starts a new PingOne Verify evaluation, or continues an existing one if `pingOneVerifyTransactionId` is present in the shared node state, and either completes or fails the journey based on the result.

Example scripts

These example scripts demonstrate some use cases for the **PingOne Verify Completion Decision** node. They use the `verifyTransactionsHelper` next-generation script binding, which gives access to the data used during a PingOne Verify transaction.

Learn more about the binding in Access PingOne Verify transactions and manage associated use.

Example 1

Check the status of the user's most recent PingOne Verify transaction and that the ID used was a driving license.

```
/** ***************************************************************
 *
 * The following script checks the status of the user's most recent
 * identity check, and ensures the ID used was a driver's license.
 *
 * Global node variables accessible within this scope:
 * 1. `nodeState` provides access to auth tree state attributes
 * 2. `verifyTransactionsHelper` provides access to verify transactions
 * 3. `outcome` variable maps to auth tree node outcomes; values are
 *    'successOutcome', 'notStartedOutcome', 'notCompletedOutcome',
 *    'expiredOutcome', or 'failureOutcome'.
 * ***************************************************************/

// Retrieve the user's latest verified transaction.
var result = verifyTransactionsHelper.getLastVerifyTransaction();
if (result != null) {
    var lastTransaction = JSON.parse(result);
    if (lastTransaction.hasOwnProperty("transactionStatus")) {
        // Get the status of the transaction.
        var status = lastTransaction.transactionStatus.status;
        // Determine the document type and verify if it is a Driver's License.
        var verifiedDocuments = lastTransaction.verifiedDocuments;
        if (status == "SUCCESS" && verifiedDocuments.includes("driver_license")) {
            outcome = "successOutcome";
        } else {
            outcome = "failureOutcome";
        }
    } else {
        outcome = "notStartedOutcome";
    }
}
```

Example 2

Check the ID used in the user's most recent PingOne Verify transaction and that their age is 18 or over.

> **Note**
>
> This data is available for a short timeframe after the verification.
> Usually 30 minutes after PingOne Verify reaches its verification decision.

```
/** *****************************************************************
 *
 * The following script checks the ID used in the user's most recent
 * identity check, and that their age is 18 or over.
 *
 * Note:
 * This data is available for a short timeframe after the verification.
 * Usually 30 minutes after a verification decision is reached.
 *
 * Global node variables accessible within this scope:
 * 1. `nodeState` provides access to auth tree state attributes
 * 2. `verifyTransactionsHelper` provides access to verify transactions
 * 3. `outcome` variable maps to auth tree node outcomes; values are
 *    'successOutcome', 'notStartedOutcome', 'notCompletedOutcome',
 *    'expiredOutcome', or 'failureOutcome'.
 * *****************************************************************/

// Retrieve the user's latest verified transaction.
var result = verifyTransactionsHelper.getLastVerifyTransaction();
if (result != null) {
    var lastTransaction = JSON.parse(result);
    if (lastTransaction.hasOwnProperty("id")) {
        // Obtain the ID of the last transaction.
        var lastTransactionId = lastTransaction.id;
        // Get the verified data for the Government ID provided by the user.
        var verifiedDataResult = verifyTransactionsHelper.getVerifiedDataByType(lastTransactionId,
"GOVERNMENT_ID");
        // Determine the age of the user.
        if (verifiedDataResult != null) {
            var verifiedData = JSON.parse(verifiedDataResult);
            var dateString = verifiedData._embedded.verifiedData[0].data.birthDate;
            if (dateString != null && dateString.trim() != "") {
                var birthDate = new Date(dateString + "T00:00:01");
                var currentDate = new Date().getTime();
                var difference = currentDate - birthDate;
                var currentAge = Math.floor(difference / (1000 * 60 * 60 * 24 * 365.25));
                if (currentAge >= 18) {
                    outcome = "successOutcome";
                } else {
                    outcome = "failureOutcome";
                }
            } else {
                outcome = "failureOutcome";
            }
        } else {
            outcome = "notCompletedOutcome";
        }
    } else {
        outcome = "notStartedOutcome";
    }
} else {
    outcome = "notStartedOutcome";
}
```

Example 3

Check the user’s most recent PingOne Verify transaction to obtain the expiration date for the Government ID provided.

The node stores this information in a variable named `governmentIdExpireDate` in the shared state, but you could also store it in a user attribute to determine when to perform the next identity verification.

> **Note**
>
> This data is available for a short timeframe after the verification.
> Usually 30 minutes after PingOne Verify reaches its verification decision.

```
/** ********************************************************************
 *
 * The following script checks the user's most recent Verify transaction
 * to obtain the expiration date for the Government ID provided.
 *
 * This information is stored in a variable named `governmentIdExpireDate`
 * in the shared state, but could also be stored as a user attribute
 * to determine when to perform the next identity verification.
 *
 * Note:
 * This data is available for a short timeframe after the verification.
 * Usually 30 minutes after a verification decision is reached.
 *
 * Global node variables accessible within this scope:
 * 1. `nodeState` provides access to auth tree state attributes
 * 2. `verifyTransactionsHelper` provides access to verify transactions
 * 3. `outcome` variable maps to auth tree node outcomes; values are
 *    'successOutcome', 'notStartedOutcome', 'notCompletedOutcome',
 *    'expiredOutcome', or 'failureOutcome'.
 * ********************************************************************/

// Retrieve the user's latest verified transaction.
var result = verifyTransactionsHelper.getLastVerifyTransaction();
if (result != null) {
    var lastTransaction = JSON.parse(result);
    if (lastTransaction.hasOwnProperty("id")) {
        // Obtain the ID of the last transaction.
        var lastTransactionId = lastTransaction.id;
        // Get the verified data for the Government ID provided by the user.
        var verifiedDataResult = verifyTransactionsHelper.getVerifiedDataByType(lastTransactionId,
"GOVERNMENT_ID");
        // Get the expire date and set on shared state.
        if (verifiedDataResult != null) {
            var verifiedData = JSON.parse(verifiedDataResult);
            var expireDate = verifiedData._embedded.verifiedData[0].data.expirationDate;
            if (expireDate != null && expireDate.trim() != "") {
                nodeState.putShared("governmentIdExpireDate", expireDate);
                outcome = "successOutcome";
            } else {
                outcome = "failureOutcome";
            }
        } else {
            outcome = "notCompletedOutcome";
        }
    } else {
        outcome = "notStartedOutcome";
    }
} else {
    outcome = "notStartedOutcome";
}
```

Example 4

Check that the user has at least one successful identity verification in the past 365 days.

```
/** ****************************************************************
 *
 * The following script checks that the user has at least one successful
 * identity verification in the past 365 days.
 *
 * Global node variables accessible within this scope:
 * 1. `nodeState` provides access to auth tree state attributes
 * 2. `verifyTransactionsHelper` provides access to verify transactions
 * 3. `outcome` variable maps to auth tree node outcomes; values are
 *    'successOutcome', 'notStartedOutcome', 'notCompletedOutcome',
 *    'expiredOutcome', or 'failureOutcome'.
 * ****************************************************************/

// Retrieve all transactions for the user
var result = verifyTransactionsHelper.getAllVerifyTransactions();
if (result != null) {
    var allTransactions = JSON.parse(result);
    if (allTransactions != null) {
        // Loop through the transactions to find a successful verification within the last 12 months.
        var verifyTransactions = allTransactions._embedded.verifyTransactions;
        var found = false;
        for (var i = 0; i < verifyTransactions.length; i++) {
            var transaction = verifyTransactions[i];
            // Get the status of the transaction.
            var status = transaction.transactionStatus.status;
            // If status is success, verify if it is still valid
            if (status == "SUCCESS") {
                found = true;
                // Calculate the number of days
                var dateString = transaction.createdAt;
                var createdDate = new Date(dateString);
                var currentDate = new Date().getTime();
                var difference = Math.abs(createdDate - currentDate);
                var numDaysBetween = difference / (1000 * 60 * 60 * 24);
                if (numDaysBetween <= 365) {
                    outcome = "successOutcome";
                    break;
                } else {
                    outcome = "expiredOutcome";
                }
            }
        }
        // No successful transaction found
        if (found == false) {
            outcome = "failureOutcome";
        }
    } else {
        outcome = "notStartedOutcome";
    }
} else {
    outcome = "notStartedOutcome";
}
```

Example 5

Check the user's most recent PingOne Verify transaction to review the biographic match results.

The script uses the **Failure** outcome if the match confidence for any attribute is anything other than `HIGH`.

```
/** ********************************************************************
 *
 * The following script checks the user's last identity verification to
 * review the "Biographic Match" results.
 *
 * The script uses the failure outcome if the match confidence for any
 * attribute is below `HIGH`.
 *
 * Global node variables accessible within this scope:
 * 1. `nodeState` provides access to auth tree state attributes
 * 2. `verifyTransactionsHelper` provides access to verify transactions
 * 3. `outcome` variable maps to auth tree node outcomes; values are
 *    'successOutcome', 'notStartedOutcome', 'notCompletedOutcome',
 *    'expiredOutcome', or 'failureOutcome'.
 * *********************************************************************/

// Retrieve the user's latest verified transaction.
var result = verifyTransactionsHelper.getLastVerifyTransaction();
if (result != null) {
    var lastTransaction = JSON.parse(result);
    if (lastTransaction.hasOwnProperty("id")) {
        // Obtain the ID of the last transaction.
        var lastTransactionId = lastTransaction.id;
        // Get all the metadata.
        var allMetadataResult = verifyTransactionsHelper.getAllMetadata(lastTransactionId);
        // Loop through the metadata to find the biographic match results.
        var biographicMatchResults;
        if (allMetadataResult != null) {
            var allMetadataJson = JSON.parse(allMetadataResult);
                        var allMetadata = allMetadataJson._embedded.metaData;
            for (var i = 0; i < allMetadata.length; i++) {
                var metadata = allMetadata[i];
                var type = metadata.type;
                var status = metadata.status;
                if (type == "BIOGRAPHIC_MATCH" && status == "SUCCESS") {
                    biographicMatchResults = metadata.data.biographic_match_results;
                    break;
                }
            }
        } else {
            outcome = "failureOutcome";
        }
        // Validate the biographic match results
        if (biographicMatchResults != null && biographicMatchResults.length > 0) {
            var success = true;
            for (var j = 0; j < biographicMatchResults.length; j++) {
                var match = biographicMatchResults[j].match;
                if (match != "HIGH") {
                                        success = false;
                                        break;
                }
            }
            if (success) {
                outcome = "successOutcome";
            } else {
                outcome = "failureOutcome";
            }
        } else {
            outcome = "failureOutcome";
        }
```

```
    } else {
        outcome = "notStartedOutcome";
    }
} else {
    outcome = "notStartedOutcome";
}
```

PingOne Verify Evaluation node

The **PingOne Verify Evaluation** node leverages the PingOne Verify Service to initiate a new or continue an existing verification transaction.

It offers a range of delivery methods, such as a QR code, email, or SMS to start the identity verification process.

You can customize the verification types users can perform in the PingOne Verification Policy.

Learn more in Verify policies.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires that the user has an account in the PingOne environment. It requires that the journey stored the PingOne user ID for the account in a shared state variable named `pingOneUserId`.

Use a PingOne Identity Match node to populate the shared state with the user's PingOne ID.

If there's a transaction ID in the shared state variable named `pingOneVerifyTransactionId`, this node continues that evaluation, rather than starting a new one.

Use a PingOne Verify Completion Decision node to determine the status of any previous transactions and populate the shared state with an in-progress transaction ID.

Dependencies

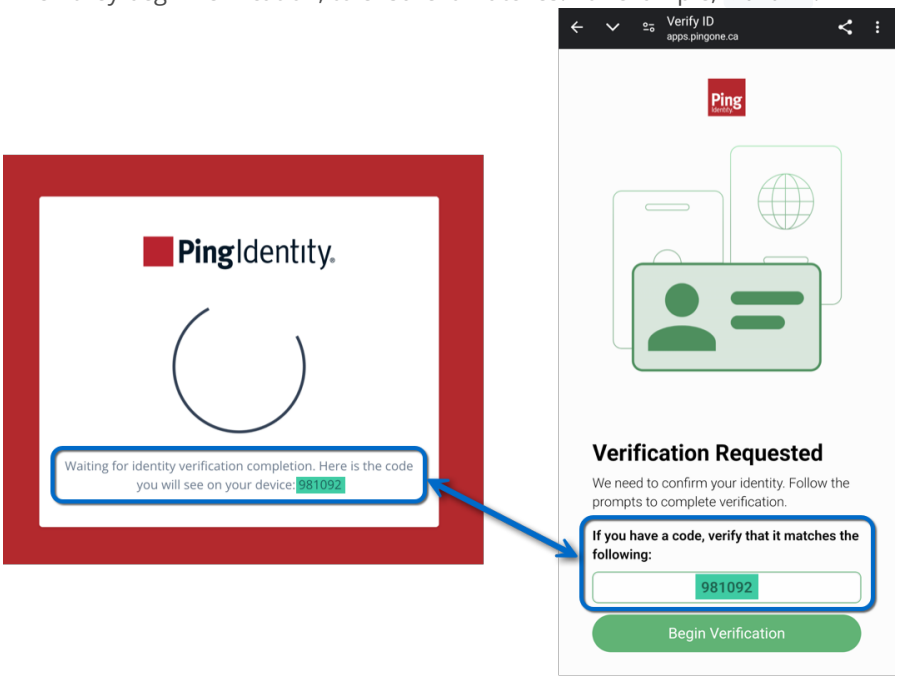
This node requires a **PingOne Worker Service** configuration so that it can connect to your PingOne instance and send it the necessary data to perform PingOne Verify evaluations as part of the journey.

You can find information on the properties used by the service in PingOne Worker service.

Configuration

Property	Usage
PingOne Worker Service ID	The ID of the PingOne worker service for connecting to PingOne.
Verify Policy ID	The ID of the policy to use for the PingOne Verify evaluation. If not specified, the node uses the environment's default Verify policy.
Verify URL delivery method	How the user will receive the URL they need to start a PingOne Verify evaluation. Choose from: **`QR Code`** Display the URL as a QR code. **`Email`** Send an email containing the URL to the email address in the user's AM identity profile. **`SMS`** Send an SMS containing the URL to the phone number in the user's AM identity profile. **`Redirect`** Redirect the user to the PingOne Verify web app for identity verification. On completion, redirect the user back to AM to continue the authentication journey. Default: `QR Code`
Allow user to choose the URL delivery method	When enabled, the node prompts the user to choose the URL delivery method.
Delivery method message	Add the text per locale to display when prompting the user to choose their delivery method: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] If the incoming HTTP request does not include the header or the preferred locales do not match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. If you leave this blank, the node displays a localized version of the following text: `Select the delivery method to start the identity verification process.` To edit an entry, click its pencil icon (✎). To remove an entry, click its delete icon (🗑).

Property	Usage
QR code message	Add the text per locale to display when you select QR code as the delivery method: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] If the incoming HTTP request does not include the header or the preferred locales do not match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. If you leave this blank, the node displays a localized version of the following text: `Scan the QR code to initiate the identity verification process.` To edit an entry, click its pencil icon (✎). To remove an entry, click its delete icon (🗑).
Redirect message	Add the text per locale to display when you select **Redirect** as the delivery method, and the node redirects the user back to AM to continue the journey: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] If the incoming HTTP request does not include the header or the preferred locales do not match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. To edit an entry, click its pencil icon (✎). To remove an entry, click its delete icon (🗑).

Property	Usage
Waiting message	Add the text per locale to display while waiting for the user to respond to the Verify transaction, when using the SMS or Email delivery methods: 1. Click **Add**. 2. In the **Key** field, enter the locale.[(1)] If the incoming HTTP request does not include the header or the preferred locales do not match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. You can use the following variable in the `Value` field: **`{{verificationCode}}`** Replaced with a 6-digit code that the user can compare with the code displayed when they begin verification, to ensure it matches. For example, `981092`.  ***Figure 1. Compare the code displayed on screen with the code presented during verification.*** If you leave this blank, the node displays a localized version of the following text: `Waiting for identity verification completion. Here is the code you will see on your device: {{verificationCode}}` To edit an entry, click its pencil icon (✎). To remove an entry, click its delete icon (🗑).

Property	Usage
Biographic Matching	Require that the specified data obtained from the user's identity documents match the paired attribute in the user's profile. To create a pairing: 1. Click **Add**. 2. In the **Key** field, enter the biographic matching requirement. One of: **`referenceSelfie`** The photo the user took of themselves, in base64 encoded data form. **`phone`** The phone number obtained from the user's identification. **`email`** The email address obtained from the user's identification. **`given_name`** The first, or given name obtained from the user's identification. For example, `Babs`. **`family_name`** The last, surname, or family name obtained from the user's identification. For example, `Jensen`. **`name`** The full name obtained from the user's identification. For example, `Babs Jensen`. **`address`** The address obtained from the user's identification, as a single string. For example, `123 Any Street, London, United Kingdom, CH15 1EE`. **`birth_date`** The date of birth obtained from the user's identification. 3. In the **Value** field, enter the attribute in the user's AM profile that should match. For example, you could pair the `family_name` biographic key to the `sn` profile attribute. To edit an entry, click its pencil icon (✎). To remove an entry, click its delete icon (🗑).

Store Verification Metadata	When enabled, store the verification metadata returned from PingOne Verify in shared state under a key named `pingOneVerifyMetadata`.

```
{
    "_links":{
        "self":{
            "href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-
a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/verifyTransactions/
7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData"
        },
        "user":{
            "href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-
a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94"
        },
        "environment":{
            "href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-
a5d9-80ad5c98f9f6"
        },
        "verifyTransaction":{
            "href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-
a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/verifyTransactions/
7668563d-0226-4ca5-8401-03f6dc5bcdc6"
        }
    },
    "_embedded":{
        "metaData":[
            {
                "_links":{
                    "self":{
                        "href":"https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/
verifyTransactions/7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData/
4ebb9165-4e5c-4270-94e4-d50d7b17ecb4"
                    }
                },
                "id":"4ebb9165-4e5c-4270-94e4-d50d7b17ecb4",
                "provider":"IDRND",
                "type":"LIVENESS",
                "status":"SUCCESS",
                "data":{
                    "score":6.4909873,
                    "probability":0.99848527,
                    "quality":0.94462675
                },
                "retry":{
                    "attempt":2
                }
            },
            {
                "_links":{
                    "self":{
                        "href":"https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/
verifyTransactions/7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData/546d3a8e-
f606-4078-92f1-96a5c2d003e9"
                    }
                },
                "id":"546d3a8e-f606-4078-92f1-96a5c2d003e9",
                "provider":"AMAZON",
                "type":"FACIAL_COMPARISON",
                "status":"SUCCESS",
                "data":{
                    "similarity":99.37002,
```

```
                    "confidence":99.99767,
                    "quality":{
                        "brightness":36.77353,
                        "sharpness":20.92731
                    }
                }
            },
            {
                "_links":{
                    "self":{
                        "href":"https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/
verifyTransactions/7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData/96315a69-
fb46-4d28-9b0d-c79927e59df1"
                    }
                },
                "id":"96315a69-fb46-4d28-9b0d-c79927e59df1",
                "provider":"BIOGRAPHIC_MATCHER",
                "type":"BIOGRAPHIC_MATCH",
                "status":"SUCCESS",
                "data":{
                    "biographic_match_results":[
                        {
                            "identifier":"address",
                            "match":"NOT_APPLICABLE"
                        },
                        {
                            "identifier":"given_name",
                            "match":"NONE"
                        },
                        {
                            "identifier":"family_name",
                            "match":"HIGH"
                        },
                        {
                            "identifier":"birth_date",
                            "match":"HIGH"
                        }
                    ]
                }
            },
            {
                "_links":{
                    "self":{
                        "href":"https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/
verifyTransactions/7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData/
fba13756-8c24-49ff-9b42-ff1a3661d0ae"
                    }
                },
                "id":"fba13756-8c24-49ff-9b42-ff1a3661d0ae",
                "provider":"MITEK",
                "type":"DOCUMENT_AUTHENTICATION",
                "status":"SUCCESS",
                "data":{
                    "mitekVerifications":[
                        {
                            "name":"Document Ensemble Authenticator",
                            "judgement":"Authentic",
                            "verificationType":202,
                            "probability":753,
```

```
            "version":"3.47.0.7114",
            "documentId":"048f28f1-a7fe-42a5-9722-f10977606719"
        },
        {
            "name":"Black And White Copy",
            "judgement":"Authentic",
            "verificationType":102,
            "probability":717,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"Image Classification",
            "judgement":"Authentic",
            "verificationType":105,
            "probability":1000,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"Data Comparison",
            "judgement":"Authentic",
            "verificationType":700,
            "probability":1000,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"Ensemble Authenticator",
            "judgement":"Authentic",
            "verificationType":201,
            "probability":753,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"ID Document Blacklist",
            "judgement":"Authentic",
            "verificationType":101,
            "probability":1000,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"Generic Font",
            "judgement":"Authentic",
            "verificationType":104,
            "probability":926,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"MRZ Check Digit",
            "judgement":"Authentic",
            "verificationType":601,
            "probability":1000,
            "version":"3.47.0.7114",
            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
        },
        {
            "name":"MRZ Font Type Authentication",
```

```
                            "judgement":"Authentic",
                            "verificationType":600,
                            "probability":1000,
                            "version":"3.47.0.7114",
                            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
                        },
                        {
                            "name":"Image Processing",
                            "judgement":"Authentic",
                            "verificationType":710,
                            "probability":1000,
                            "version":"1.0",
                            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
                        },
                        {
                            "name":"Document Liveness",
                            "judgement":"Authentic",
                            "verificationType":108,
                            "probability":999,
                            "version":"1.0",
                            "documentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856"
                        }
                    ],
                    "frontImageDocumentId":"e290d74d-bf9c-4116-9fe7-9b6fb909c856",
                    "documentEvidenceId":"048f28f1-a7fe-42a5-9722-f10977606719",
                    "retry":{
                        "attempt":1
                    }
                }
            }
        ]
    },
    "previousAttempts":[
        {
            "_links":{
                "self":{
                    "href":"https://api.pingone.com/v1/environments/
abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/03df72b1-b80b-4449-8eef-ee8f85f48d94/
verifyTransactions/7668563d-0226-4ca5-8401-03f6dc5bcdc6/metaData/
06aebfbd-0053-4860-8b59-4f3cb7371dcb"
                }
            },
            "id":"06aebfbd-0053-4860-8b59-4f3cb7371dcb",
            "provider":"IDRND",
            "type":"LIVENESS",
            "status":"FAIL",
            "data":{
                "score":2.4509223,
                "probability":0.40062885,
                "quality":0.40874674
            },
            "retry":{
                "attempt":1
            }
        }
    ],
    "size":4
}
```

Property	Usage
	Note The key is empty if the node is unable to retrieve the verification metadata from PingOne. Default: Disabled

Property	Usage

Store Verified Data	When enabled, store a list of the verified data submitted by the user in shared state under a key named `pingOneVerifyVerifiedData`.
	
	{
	"_links":{
	"self":{
	"href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/a27dec16-1e80-4f10-a261-2cac46a12b78/verifyTransactions/0e2ed48f-6c3a-46c4-bcb5-3a6bd791348b/verifiedData/34613a50-672c-428f-8db9-c67fe09fc4cc"
	},
	"environment":{
	"href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6"
	},
	"user":{
	"href":"https://api.pingone.com/v1/users/a27dec16-1e80-4f10-a261-2cac46a12b78"
	},
	"transaction":{
	"href":"https://api.pingone.com/v1/environments/abfba8f6-49eb-49f5-a5d9-80ad5c98f9f6/users/a27dec16-1e80-4f10-a261-2cac46a12b78/verifyTransactions/0e2ed48f-6c3a-46c4-bcb5-3a6bd791348b"
	}
	},
	"id":"84170421-62c6-49a5-b343-496bee93c206",
	"type":"GOVERNMENT_ID",
	"createdAt":"2022-02-23T15:51:01.603Z",
	"data":{
	"addressCity":"this city",
	"addressState":"this state",
	"addressZip":"11111",
	"birthDate":"1970-01-01",
	"country":"USA",
	"expirationDate":"1970-01-01",
	"firstName":"given",
	"gender":"",
	"idNumber":"11111",
	"issueDate":"1970-01-01",
	"issuingCountry":"",
	"lastName":"surname",
	"nationality":"",
	"weight":""
	},
	"retry":{
	"attempt":1
	}
	}
	
	Note
	The key is empty if the node is unable to retrieve the verified data from PingOne.
	
	Default: Disabled

Property	Usage
Capture failure	Capture the details in shared state if a failure occurs. The node stores the details in a variable named `pingOneVerifyEvaluationFailureReason`. Default: `False` Example: `{ "code": "IDENTITY_VERIFICATION_FAILED", "message": "Identity verification failed.", "exception": "", }`

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

Outputs

- If **Allow user to choose the URL delivery method** is selected, the node sends the following callbacks:

  `TextOutputCallback`

  Contains the **Delivery method message**.

  `ConfirmationCallback`

  Contains the options available to the client application.

- When using the `QR Code` URL delivery method, the node sends the following callbacks:

  `TextOutputCallback`

  Contains the **QR Code message**.

  `ScriptTextOutputCallback`

  Contains JavaScript script to run to display the QR code.

  `HiddenValueCallback`

  Contains the actual URL to start the verification. The client might display this to users on a mobile device that cannot scan a QR code, or to render their own QR code, for example.

  `PollingWaitCallback`

  Waits for the user to complete the verification, and the **Waiting message**.

- When using the `Email` or `SMS` URL delivery method, the node sends the following callbacks:

  `PollingWaitCallback`

  Waits for the user to complete the verification, and contains the **Waiting message**.

- When using the `Redirect` delivery method, the node sends the following callbacks:

  `RedirectCallback`

  Contains the URI to redirect the user to for identity verification, using the PingOne Verify web application.

- If you select **Store Verification Metadata**, the node outputs the verification metadata JSON in a state variable named `pingOneVerifyMetadata`.

  To learn more about verification metadata, refer to Read All Verification Metadata.

- If you select **Store Verified Data**, the node outputs the verified information gathered from the user's ID in a state variable named `pingOneVerifyVerifiedData`.

  To learn more about verified data, refer to Read One User Verified Data.

- If you select **Capture failure**, the node stores any error response in a shared state variable named `pingOneVerifyEvaluationFailureReason`.

Outcomes

Success

The user successfully completed the PingOne Verify evaluation.

`Failure`

The user did not successfully complete the PingOne Verify evaluation, or an error occurred.

`Time Out`

The node did not receive a response from the user performing the verification before the timeout specified in the **Verify Transaction Timeout** property.

Example

The following example journey leverages PingOne Verify to perform user identity verification.

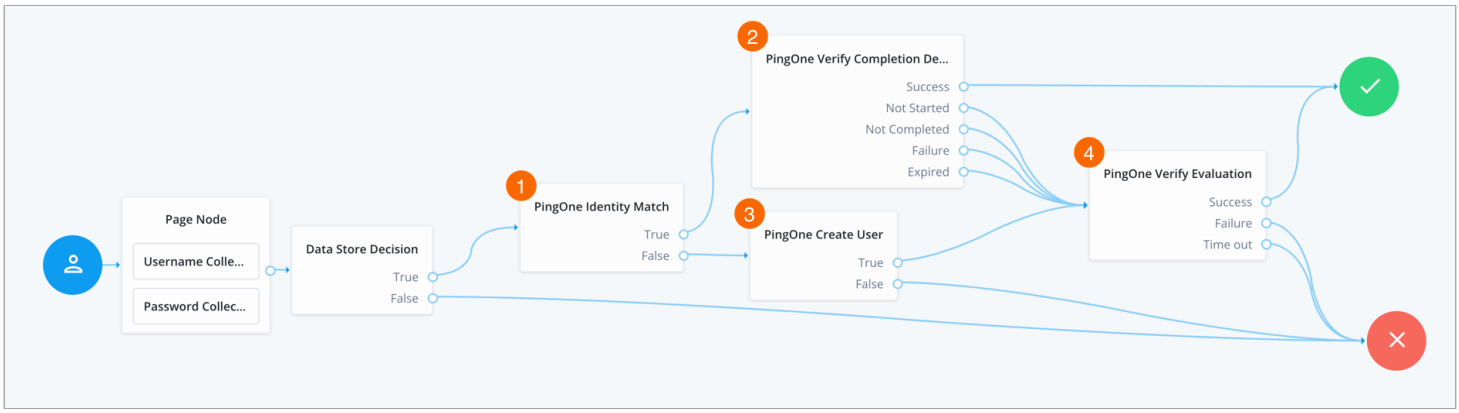


Figure 2. Example PingOne Verify journey

- The user enters their credentials, which the Data Store Decision node then verifies against the identity store.

- 1 The PingOne Identity Match node checks PingOne for a matching user.
- 2 If a user is found, the PingOne Verify Completion Decision node checks the user's most recent verification transaction to determine the status:

Success

The user successfully completed the most recent PingOne Verify transaction, so continue directly to the **Success** node, completing the authentication journey.

Not Completed

The user has an existing PingOne Verify transaction in progress, so continue the journey to resume the existing verification transaction.

The node adds the user's existing transaction ID to the shared node state in a variable named `pingOneVerifyTransactionId`.

Not Started / Failure / Expired

The user either does not have an existing transaction (`Not Started`), or did not successfully complete the most recent PingOne Verify transaction, or it expired, so continue the journey to start a new verification transaction.

- 3 If a user is not found, the PingOne Create User node creates a new user in PingOne.
- 4 The PingOne Verify Evaluation node starts a new PingOne Verify evaluation, or continues an existing one if `pingOneVerifyTransactionId` is present in the shared node state, and either completes or fails the journey based on the result.

Platform Password node

The **Platform Password** node prompts the user to enter their password and stores it in a configurable property of the shared node state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node uses the `_id` of the object for policy evaluation.

For existing users, the user's `_id` must be in the shared state to evaluate user-specific policies, such as password history, cannot-contain-others, and so on. No `_id` is available for new users.

Dependencies

If this node's **Validate Password** setting is enabled, the node relies on IDM for password policies.

Configuration

Property	Usage
Validate Password	When enabled, this node uses the password policies in IDM to validate the user's input. It returns any policy failures as errors. For example, if you submitted an invalid password on registration, the response from this node would include a list of failed policies: `{ "name": "failedPolicies", "value": [ "{ \"params\": { \"minLength\": 8 }, \"policyRequirement\": \"MIN_LENGTH\" }", "{ \"params\": { \"numCaps\": 1 }, \"policyRequirement\": \"AT_LEAST_X_CAPITAL_LETTERS\" }", "{ \"params\": { \"numNums\": 1 }, \"policyRequirement\": \"AT_LEAST_X_NUMBERS\" }" ] }` Default: disabled
Password Attribute	The attribute used to store a password in the managed identity object. Default: `password`
Confirm Password	Enable this option to require the user to enter the password identically in a second field. **Note** This property only displays when the node is placed within a Page node in a Ping Identity Platform deployment. Default: disabled

Property	Usage
Checkmark Policy Display	Enable this option to show a checkmark instead of faded bullet points on successful password validation. **Note** This property only displays when the node is placed within a Page node in a Ping Identity Platform deployment. Default: disabled

Outputs

On success, this node updates the **Password Attribute** property in the shared node state with the password.

The captured password is transient, persisting only until the authentication flow reaches the next node requiring user interaction. It may be persisted to the secure state if required later in the journey.

Outcomes

Single outcome path.

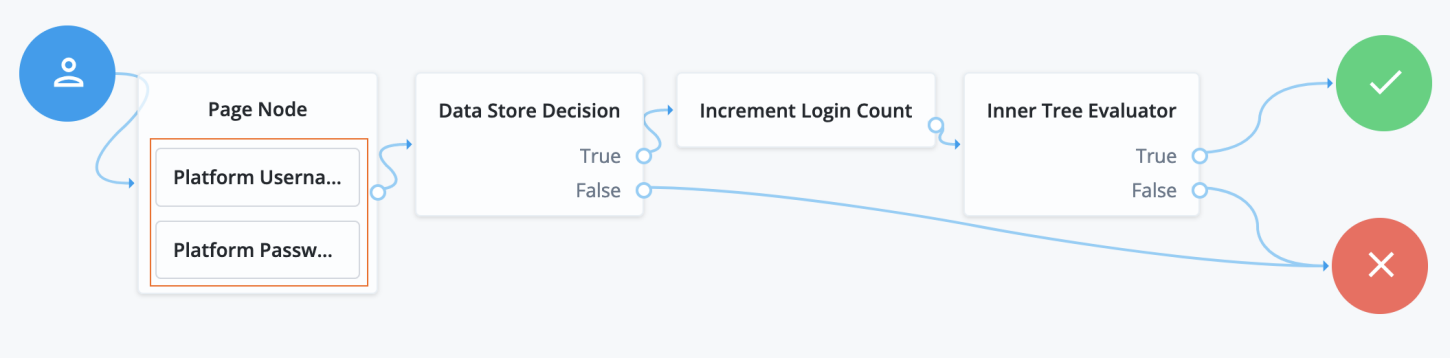
Errors

This node does not log error or warning messages of its own.

If it fails to get the result from IDM for a validation request, this node throws an exception with a `Communication failure` message.

Example

The following journey uses a Page node containing the Platform Username node and Platform Password node to collect the username and password and set their values in the shared node state:



- The Page node presents a page with input fields to prompt for the username and password.
  - The Platform Username node collects and injects the `userName` into the shared node state.
  - The Platform Password node collects and injects the `password` into the shared node state.

- The Data Store Decision node uses the username and password to determine whether authentication is successful.
- The Increment Login Count node updates the login count on successful authentication.
- The Inner Tree Evaluator node invokes a nested journey for progressive profiling.

Platform Username node

The **Platform Username** node prompts the user to enter their username and stores it in a configurable property of the shared node state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None.

Dependencies

If this node's **Validate Username** setting is enabled, the node relies on IDM for username policies.

Configuration

Property	Usage
Validate Username	When enabled, this node uses the username policies in IDM to validate the user's input. It returns any policy failures as errors. **Important** Only enable this field if you're using this node as part of a *registration* journey. Don't enable this field in an *authentication* journey because the validation includes verifying that the provided username doesn't exist in the identity store. Default: disabled
Username Attribute	The attribute used to store a username in the managed identity object. Default: `userName`

Outputs

On success, this node updates the **Username Attribute** property in the shared node state with the username.

Outcomes

Single outcome path.

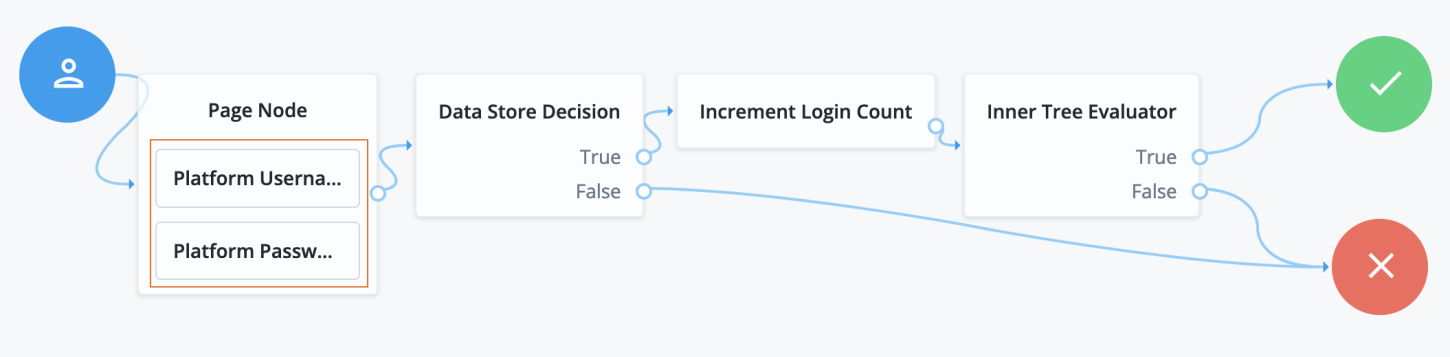
Errors

This node does not log error or warning messages of its own.

If it fails to get the result from IDM for a validation request, this node throws an exception with a `Communication failure` message.

Example

The following journey uses a Page node containing the Platform Username node and Platform Password node to collect the username and password and set their values in the shared node state:



- The Page node presents a page with input fields to prompt for the username and password.
  - The Platform Username node collects and injects the `userName` into the shared node state.
  - The Platform Password node collects and injects the `password` into the shared node state.
- The Data Store Decision node uses the username and password to determine whether authentication is successful.
- The Increment Login Count node updates the login count on successful authentication.
- The Inner Tree Evaluator node invokes a nested journey for progressive profiling.

Profile Completeness Decision node

Use progressive profile flows to check how much of a user's profile has been completed, where the completeness of a profile is expressed as a percentage of user-viewable, and user-editable fields that are not `null`.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Profile Completeness Threshold	Percentage of user-viewable and user-editable fields in a profile that must be filled for the node to pass. Express this as a number between 0 and 100.
Identity Attribute	The attribute used to identify the managed object in IDM.

Query Filter Decision node

The **Query Filter Decision** node checks if the contents of a user's profile match the specified query filter.

Use this node to check whether an attribute of the user profile matches a specific pattern. For instance, use this in progressive profile flows to check if marketing preferences are set on a user's profile.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the **Identity Attribute** from the shared node state. If it can't read the **Identity Attribute**, it reads the `userName`.

It uses the value to look up the identity object.

Dependencies

This node depends on IDM to look up the user object.

Configuration

Property	Usage
Query Filter	A query filter used to check the contents of an object. Learn more about constructing effective query filters in Construct queries in the IDM documentation. Default: none
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

None.

Outcomes

`True`

The node user profile matched the query.

`False`

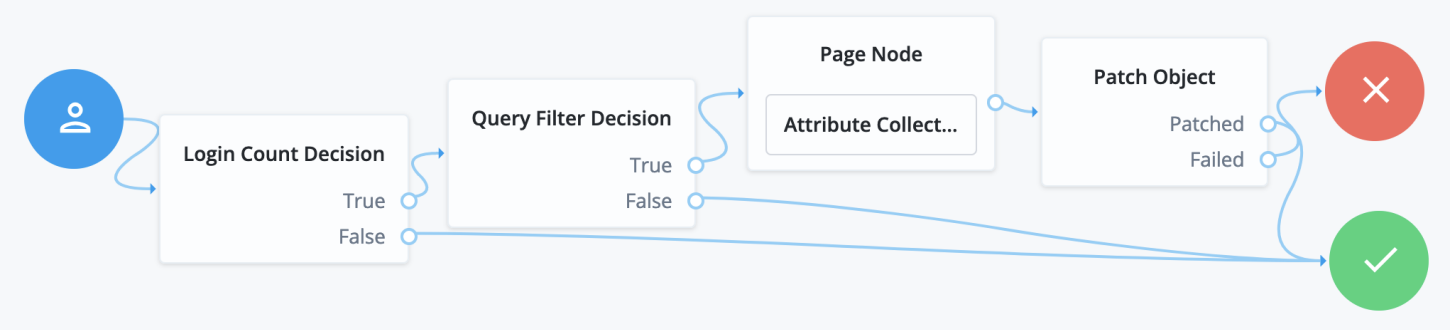
Any other case.

Errors

This node doesn't log error or warning messages of its own.

Example

Other journeys invoke the following progressive profile journey to capture missing profile attributes:



- The Login Count Decision node triggers the rest of the journey depending on the login count and its settings.
- The **Query Filter Decision** node determines whether managed object profile fields are missing.

- The Attribute Collector node in the Page node requests additional input for the profile.
- The Patch Object node stores the additional input in the managed object profile.

Required Attributes Present node

Checks the specified identity resource in IDM, by default, `managed/user`, and determines if all attributes required to create the specified object exist within the shared node state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Identity Resource	The type of managed identity resource object this node creates. It must match the identity resource type for the current flow. **Tip** To check for the available managed identity resource types, go to the IDM admin UI, and open the **Manage** drop-down list in the upper right corner of the screen. Identity managed object types are preceded by the icon.

Select Identity Provider node

Presents the user with a list of configured, enabled, social identity providers to use for authentication.

Use this node with the Social Provider Handler node to use the Social Identity Provider Service.

In a Ping Identity Platform deployment, you can configure this node to only show identity providers the user has already associated with their account, such as in account claiming flows, where a user wishes to associate a new social identity provider with an account that is being authenticated with social authentication.

The node has two possible outputs: social authentication and local authentication. Local authentication can be turned off by disabling **Include local authentication**.

In cases such as account claiming, where the user has already authenticated once and is associating a new identity provider, the node only displays a local sign in option if it detects that the user's account has a `password` attribute.

This node returns the SelectIdPCallback when more than one social identity provider is enabled, or a single provider is enabled as well as the **Local Authentication** option, It then requires a choice from the user. If no choice from the user is required, authentication proceeds to the next node in the flow.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Social Authentication`
- `Local Authentication`

To turn off local authentication, disable **Include local authentication**.

Properties

Property	Usage
Include local authentication	Whether local authentication is included as a method for authenticating.

Property	Usage
Offer only existing providers	Ping Identity Platform deployments only. Enable this when the social identity provider choices offered should be limited to those already associated with a user object. Use this when a user is authenticating using a new social identity provider, and an account associated with that user already exists (also known as "account claiming").
Password attribute	Ping Identity Platform deployments only. The attribute in the user object that stores a user's password for use during local authentication.
Identity Attribute	Ping Identity Platform deployments only. The attribute used to identify an existing user. Required to support the offer of only existing providers.
Filter Enabled Providers	By default, the node displays all identity providers marked as **Enabled** in the Social Identity Provider Service as a selectable option. Specify the name of one of more providers to filter the list. **Tip** View the names of your configured social identity providers in AM admin UI under **Realms > *Realm name* > Services > Social Identity Provider Service > Secondary Configurations**. If this field is not empty, providers must be in the list and must be enabled in the Social Identity Provider service to appear. If left blank, the node displays all enabled providers.

Terms and Conditions Decision node

Verifies the user has accepted the active set of terms and conditions.

You set up terms and conditions in the Ping Identity Platform admin UI. Learn more in Terms and conditions.

Use this node to verify the user has accepted terms and conditions before proceeding, for example, during login or progressive profile data collection.

You can use this node with the Accept Terms and Conditions node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Identity Attribute	The attribute used to identify the managed object in IDM.

Time Since Decision node

Checks if a specified amount of time has passed since the user was registered.

For example, to prompt users to review your terms and conditions after the account is a week old, set the **Elapsed Time** property to `1 week`. After that time has elapsed, the next time the user logs in, they are prompted to review your terms and conditions.

Use this node for progressive profile completion.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `True`
- `False`

Properties

Property	Usage
Elapsed Time	The amount of time since the user was created, in minutes, that needs to elapse before this node is triggered. This property also supports specifying basic time units. For example, when setting the property to `10080` minutes, writing `7 days` or `1 week` also works.
Identity Attribute	The attribute used to identify the managed object in IDM.

Utility nodes

Agent Data Store Decision node

The **Agent Data Store Decision** node authenticates the agent using the data store for agent profiles and sets its authentication identifier if successful.

> **Note**
>
> This node only authenticates agents, such as PingGateway and AM Java and web agents.
> Use the Data Store Decision node for other identities.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node requires the `username` and `password` properties in the incoming node state.

Obtain the agent credentials from the user or with a Zero Page Login Collector node.

Dependencies

This node depends on the underlying data store for agent profiles.

Configuration

This node has no configurable properties.

Outputs

This node copies the shared and transient states into the outgoing node state.

Outcomes

`True`

The credentials match those found in the data store for agent profiles.

`False`

The credentials do *not* match those found in the data store for agent profiles.

Errors

This node can log the following warnings:

`Exception in data store decision node`

The node couldn't connect to the data store, or another error occurred.

`invalid password error`

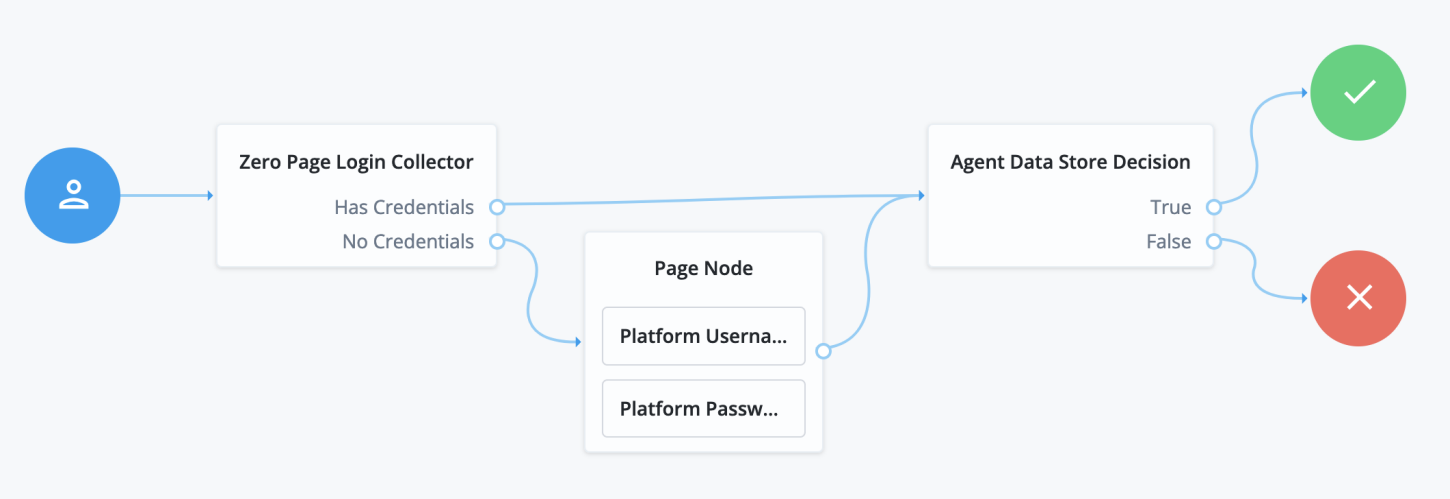
The password doesn't match.

`invalid username error`

The username doesn't match any profiles found in the data store.

Example

The following example uses this node to authenticate an agent with the credentials provided:



- The Zero Page Login Collector node collects the username and password from HTTP headers if provided.
- The Page node collects the username and password interactively from the user.
- The **Agent Data Store Decision** node verifies the agent credentials match those in the data store.

Amster Jwt Decision node

PingAM

The **Amster Jwt Decision** node lets AM authenticate Amster connections using SSH keys.

The Amster client signs the JWT using a local private key. AM verifies the signature using the list of public keys in the `authorized_keys` file. Specify the path to the `authorized_keys` file in the node configuration.

If the entry in the authorized keys file contains a `from` parameter, only connections originating from a qualifying host are permitted.

Find more information in Private key connections in the Amster documentation.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `NONCE_STATE_KEY` from the Amster client.

Dependencies

None.

Configuration

Property	Usage
Authorized Keys	Location of the `authorized_keys` file used to validate remote Amster connections. This file has the same format as an OpenSSH `authorized_keys` file.

Outputs

This node doesn't change the shared state.

Outcomes

True

The journey follows this outcome if the node can validate the incoming private key against the public keys in the `authentication_keys` file. Successful authentication creates an `amAdmin` session in AM.

False

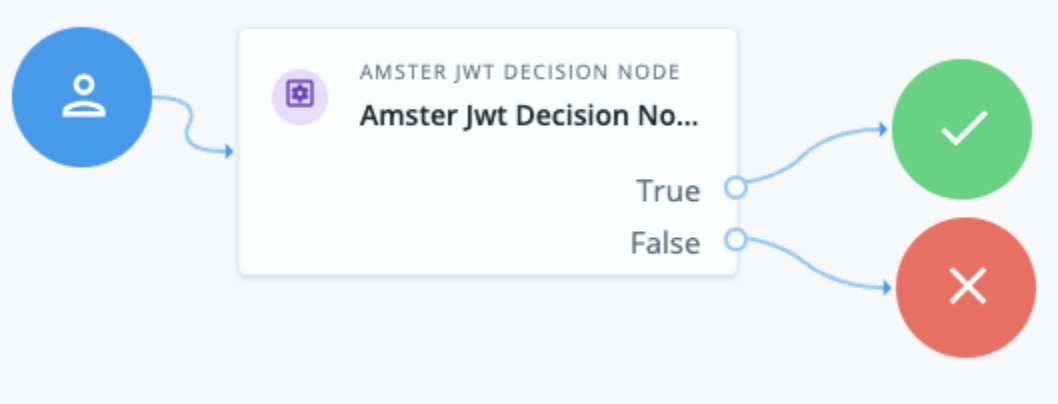
The journey follows this outcome if the node can't validate the incoming private key against the public keys in the `authentication_keys` file, either because the incoming key is invalid, or because the `authentication_keys` file is inaccessible.

Errors

If the node can't read the `authorized_keys` file, it returns the error `AmsterJwtDecisionNode: Could not read authorized keys file filename`.

Examples

This node is used only by the `amsterService` authentication tree:



Caution

Changing or removing this tree could prevent Amster from connecting to AM.

Anonymous Session Upgrade node

Upgrades an anonymous session to a non-anonymous session.

Use this as the first node in the flow.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

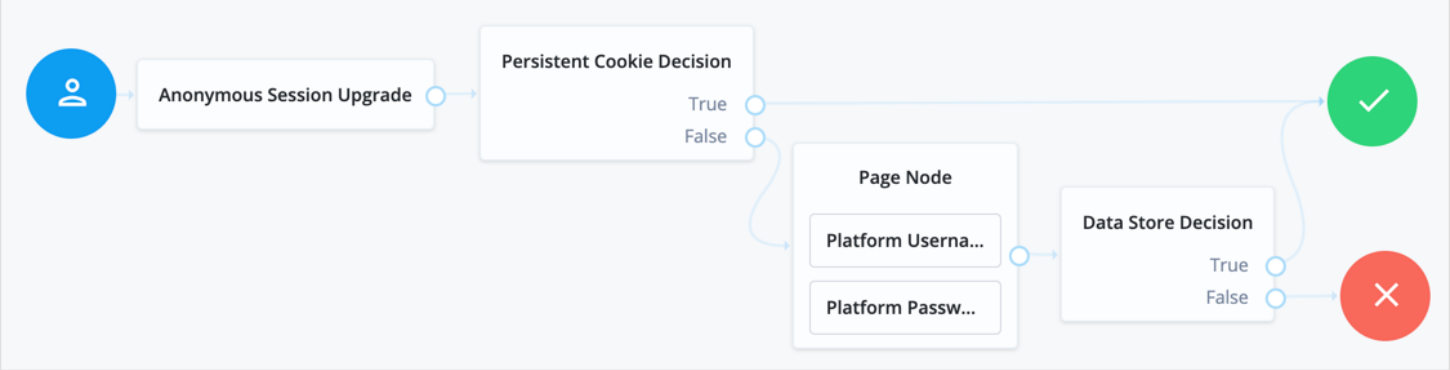
Single outcome path.

Properties

This node has no configurable properties.

Example

After using the Anonymous User Mapping node to access AM as an anonymous user, this node lets users upgrade their session to a non-anonymous one:



Anonymous User Mapping node

Lets users log in to an application or website without providing credentials, by assuming the identity of a specified existing user account. The default user for this purpose is named `anonymous`.

Take care to limit access for such users. For example, grant anonymous users access to public downloads on your site.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

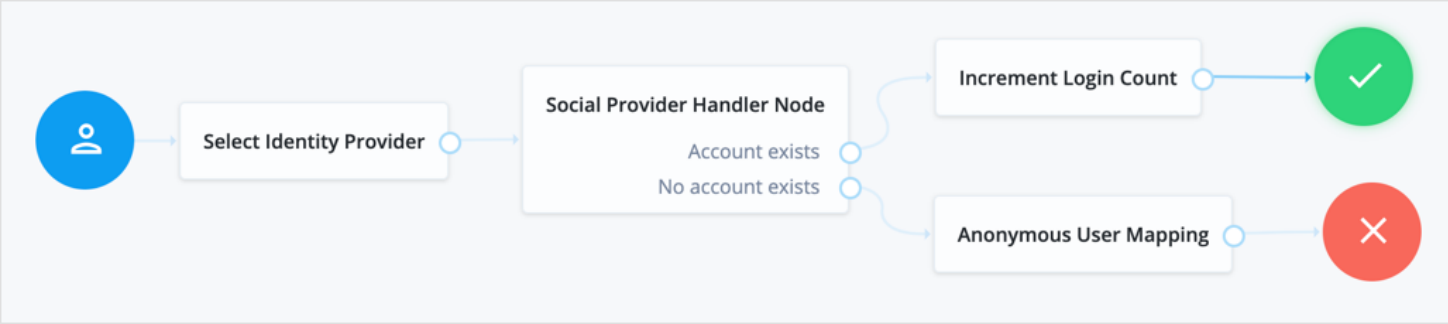
Single outcome path.

Properties

Property	Usage
Anonymous User Name	Specifies the username of an account that represents anonymous users. This user must already exist in the realm, and its user status must be `active`.

Example

The following example uses this node to grant access as an anonymous user to users who have performed social authentication access and do not have an existing profile:



Choice Collector node

Define two or more options to present to the user when authenticating.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- *Choice 1*

  ...

- *Choice n*

Properties

Property	Usage
Choices	Enter two or more choice strings to display to the user. To remove a choice, select its **Delete** icon ✕. To delete all choices, select the **Clear all** button in the **Choices** field.
Default Choice *(required)*	Enter the value of the choice to be selected by default. **Important** If you do not specify a default choice, the first choice in the list becomes the default.
Prompt *(required)*	Enter the prompt string to display to the user when presenting the choices.

Property	Usage

Field Display Type	The format of the options presented to the user.
	
	Note
	• This property only displays when the node is placed within a Page node.
	• This property is not visible in the AM admin UI. It requires the Platform UI (Advanced Identity Cloud admin console).
	
	Possible values are:
	
	`select`
	Lets the user select one or more options from a selection (default).
	`radio`
	Lets the user select a single option from a group of radio buttons.

Configuration Provider node

The **Configuration Provider** node is a scripted node that dynamically imitates another node and replaces it in the journey.

The script builds a map of configuration properties matching settings for the imitated node. The **Configuration Provider** node uses the settings to imitate the other node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The specific shared state inputs depend on your script and the configuration it builds. The shared state data must include all required **Script Inputs** properties.

In other words, shared state data must include whatever the **Script** requires to prepare configuration data for the imitated node.

Dependencies

To use this node, you need to prepare a script that provides values for the settings of the imitated node.

1. Choose the type of node to imitate
2. Get a template script
3. Configure the script

Choose the type of node to imitate

The imitated node must have a *defined set of outcomes*.

This can be a variable set of outcomes from a predefined list, such as the Polling Wait node, or a fixed set of outcomes, such as the Message node.

You can't use a node type whose outcomes are defined *entirely* by configuration, such as the Scripted Decision node.

Get a template script

Use the REST API to get the required configuration properties for the imitated node.

1. Call the following API endpoint with the `configProviderScript` action to get a template script for the type of node you want to imitate:

   ```
   /realm-config/authentication/authenticationtrees/nodes/node-type?_action=configProviderScript
   ```

   Learn more about the node endpoint in the API explorer.

2. Specify the language as `JAVASCRIPT` or `GROOVY` in the request body. If omitted, the default is JavaScript.

   For example, the following request returns a base64-encoded JavaScript template script for a Polling Wait node:

   ```
   $ curl \
   --request POST \
   --header "iPlanetDirectoryPro: admin-tokenId" \
   --header "Content-Type: application/json" \
   --data '{"language":"JAVASCRIPT"}' \
   "https://am.example.com:8443/am/json/realm-config/authentication/authenticationtrees/nodes/PollingWaitNode?
   _action=configProviderScript"
   {
     "script":"LyoqCiAqIFRoZSBmb2xsb3dpbmcgc2.."
   }
   ```

3. Decode the `script` value, for example, by using an online base64 decoder.

   The decoded output shows the required properties. For example, a request for the **Polling Wait node** generates the following template script:

```
config = {
  "secondsToWait" : 8,
  "spamDetectionEnabled" : false,
  "spamDetectionTolerance" : 3,
  "waitingMessage" : { },
  "exitable" : false,
  "exitMessage" : { }
};
```

Configure the script

Use the imitated node's properties to create a **Config Provider** or **Config Provider Node (Next-Gen)** type script.

Learn more in Manage scripts (UI).

1. Base your script on the `config-provider-node.js` sample.

   Your script must have a `config` object. This object must define the configuration properties that match the settings of the imitated node.

   For example, a script for the Email Suspend node has the following structure:

   ```
   config = {
     "emailTemplateName" : "registration",
     "emailAttribute" : "mail",
     "emailSuspendMessage" : {
       "en" : "An email has been sent to the address you entered. Click the link in that email to proceed."
     },
     "objectLookup" : false,
     "identityAttribute" : "userName"
   };
   ```

   A Configuration Provider node script can use either the next-generation or legacy script engine. It has access to all the common bindings available for its script type. You can use these to help you set the values of the configuration properties.

   Refer to the example for a script that uses shared state data to set the node configuration.

2. Save your script, and select it from the list when you configure the node's **Script** property.

Configuration

Property	Usage
Script	Select the script you created for this node. The list displays legacy and next-generation Configuration Provider scripts.
Node Type	Select the type of node to imitate. The list is restricted to node types with outcomes that are fixed or variable based on predefined values.

Property	Usage
Script Inputs	Optionally, limit the shared state data properties in the shared state input to the selected **Script**. Default: `*` (Any available shared state property)

Outputs

The outputs match those of the imitated node.

Outcomes

The **Configuration Provider** node inherits the outcomes of its configured **Node Type**. Connect these as you would the outcomes of the imitated node.

Nodes with a variable set of outcomes inherit all the possible outcomes even if runtime configuration makes them unreachable. Connect these outcomes to the Failure node.

This node also has a **Configuration failure** outcome. The **Configuration failure** outcome arises when:

- The **Configuration Provider** node failed to build the configuration map.
- The configuration map is missing required values.
- The configuration map is invalid.

Errors

In addition to the messages from the imitated node, this node can log the following:

Warnings

- `Failed to collect inputs of contained node: node-type`

  A required input property was missing.

- `Failed to get outcome provider for node type.`

  The **Node Type** outcomes were missing.

Errors

- `Failed to configure node: node-type`

  This corresponds to the **Configuration failure** outcome.

To troubleshoot HTTP errors this node causes, refer to the *Errors* section of the imitated node.

Examples

Example 1: Imitate the Message node

In the following example, the **Configuration Provider** node imitates a Message node.

The **Configuration Provider** settings are the following:

Script

A script to configure a Message node dynamically.

The script assigns values to the required properties, accessing the `username` from shared state data to set the message:

```
config = {
    "message": {"en-GB": `Hi ${nodeState.get("username")}. Please confirm you are over 18.`},
    "messageYes": {"en-GB": "Confirm"},
    "messageNo": {"en-GB": "Deny"},
    "stateField" : null
}
```

Node Type

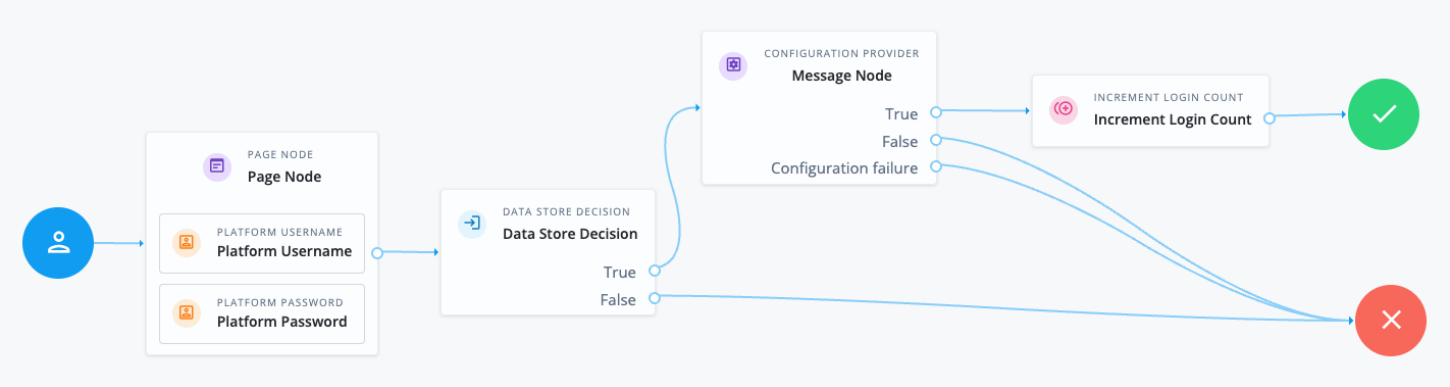
`Message Node`

Script Inputs

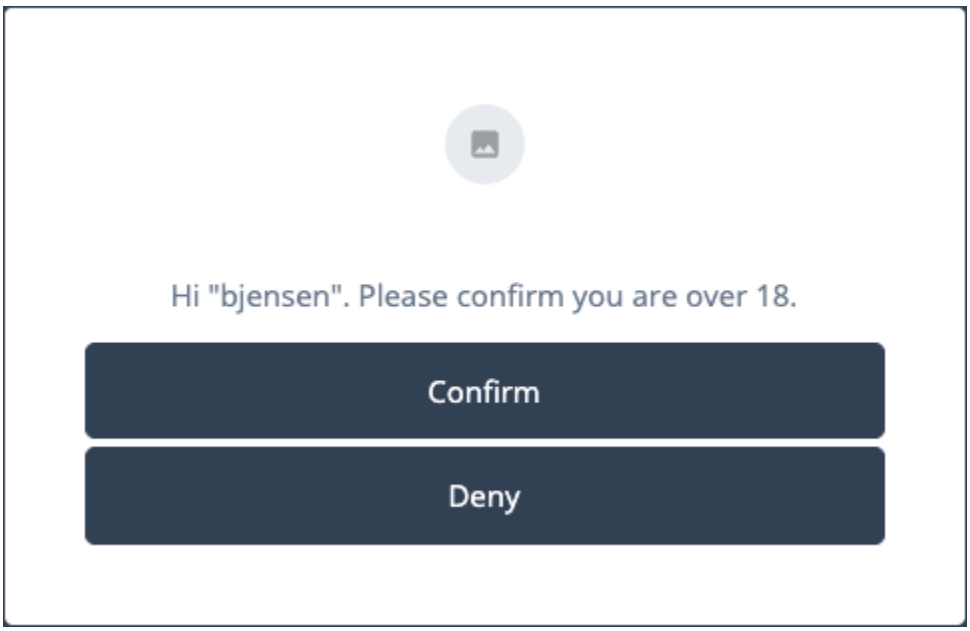
`username`

The default, `*`, also works because `username` is one of the available shared state properties.

The **Configuration Provider** node is part of a journey where the user enters their username and password before getting the message screen, so their username is in the shared state data. Notice the outcomes of the node include those of the Message node (**True**, **False**):



When the journey reaches the **Configuration Provider** node, the script for the node retrieves the `username` and dynamically configures the node. The **Configuration Provider** node, imitating a Message node, prompts the user with the message:

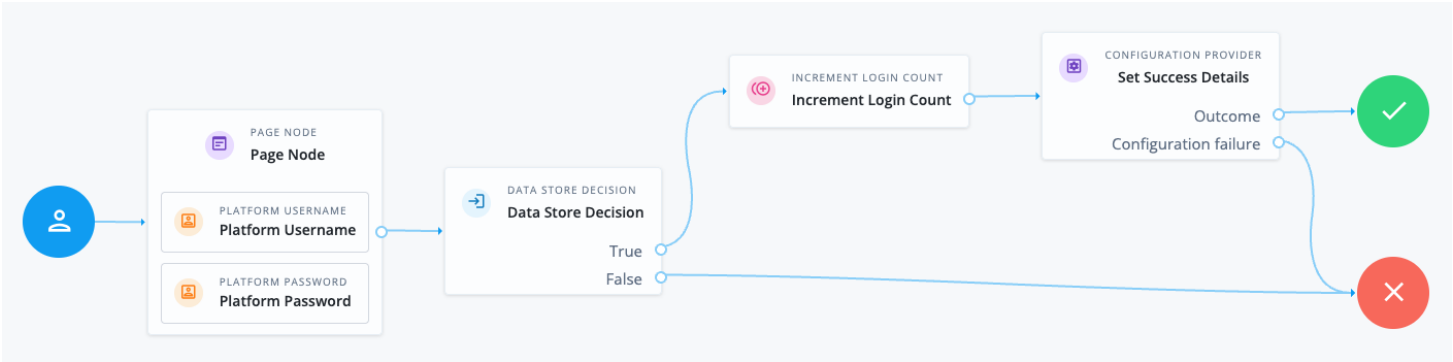


- When the user clicks **Confirm**, the journey continues to the Increment Login Count node.
- When the user clicks **Deny**, the journey continues to the Failure node.
- If the configuration process fails, the node triggers the **Configuration failure** outcome and the journey continues to the Failure node. In this case, you can find the reason for the failure in the logs.

Example 2: Imitate the Set Success Details node

This example uses the **Configuration Provider** node to imitate a Set Success Details node and add the following additional details to the JSON response:

- A dynamic `apiResponse` field, which returns the response from the `monitoring/health` endpoint.
- A static `authMethod:password` field.
- A `universalId` session property, which returns the corresponding value from the session when the user authenticates.



- The Page node containing the Platform Username node and Platform Password node prompts for credentials.
- The Data Store Decision node validates the username-password credentials.
- The Increment Login Count node updates the number of successful authentications in the user profile.

- The **Configuration Provider** node, imitating a Set Success Details node, adds the additional configured details to the JSON response upon successful authentication. This example uses the following configuration:

Script

The following next-generation script calls the `monitoring/health` endpoint and dynamically configures the node by setting the required properties. It includes the API response in the JSON response if authentication is successful along with the static field and session property:

```
var requestAPI = "https://example.com/monitoring/health";

var response = httpClient.send(requestAPI).get();

var apiResponse = response.json();

config = {
    "successDetails": {
        "authMethod": "password",
        "apiResponse": apiResponse
    },
    "sessionProperties": {
        "universalId": "sun.am.UniversalIdentifier"
    }
};
```

Node Type

`Set Success Details`

Script Inputs

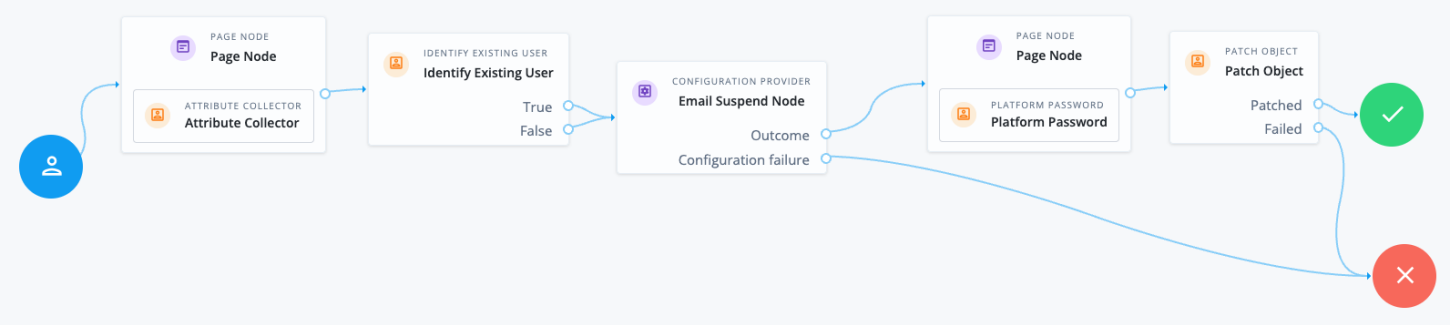
`*`

When the user authenticates successfully using this journey, the JSON response includes the additional details you configured. For example:

```
{
    "tokenId": "AQIC5wM…TU3OQ*",
    "successUrl": "/enduser/?realm=/alpha",
    "realm": "/alpha",
    "universalId": "id=bjensen,ou=user,o=alpha,ou=services,ou=am-config",
    "apiResponse": {
       "status": "OK"
     },
    "authMethod": "password"
}
```

Example 3: Imitate the Email Suspend node

This example extends the default `resetPassword` journey to include the user's email address in the email suspend message. This is achieved by using the **Configuration Provider** node to imitate the Email Suspend node.



The **Configuration Provider** node in this example uses the following configuration:

Script

The following next-generation script dynamically configures the node by setting the required properties. It retrieves the user's email address from the shared state and includes it in the email suspend message:

```
var attributes = nodeState.getObject("objectAttributes");

config = {
  "emailTemplateName" : "resetPassword",
  "emailAttribute" : "mail",
  "emailSuspendMessage" : {
    "en" : `An email has been sent to ${attributes.get("mail")}. Click the link in that email to reset your
password.`
  },
  "objectLookup" : true,
  "identityAttribute" : "mail"
};
```

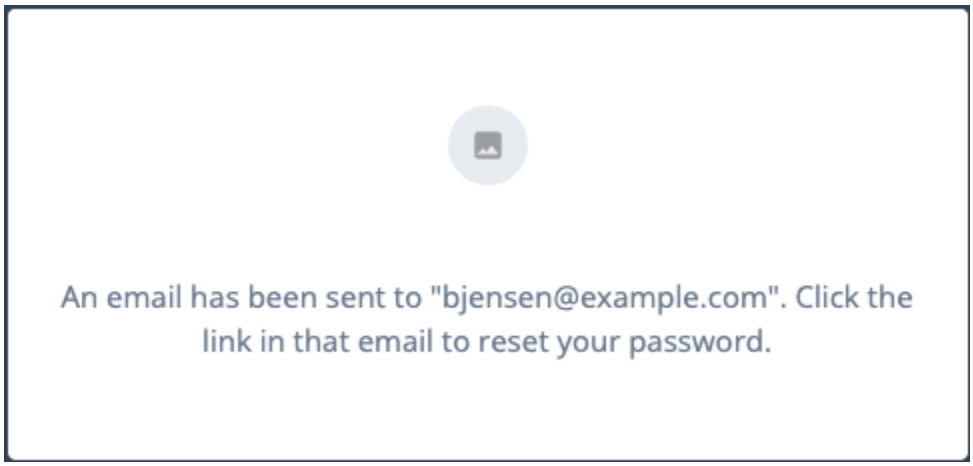
Node Type

`Email Suspend Node`

Script Inputs

`*`

When the journey is suspended, the updated suspend message is shown. For example:



Email Suspend node

The **Email Suspend** node generates and sends an email, such as an address verification email based on an email template. This node relies on the email service configured in IDM to send the email.

This node generates a unique link and passes it as the `resumeURI` property for the template.

The **External Login Page URL** is used as the base of the `resumeURI` if it's been configured. Otherwise, the **Base URL Source** service is used to construct the base of the `resumeURI`.

Learn more in Core authentication attributes > General and Configure the Base URL source service.

The journey is suspended until the end user clicks the link in the email to resume it. Make sure the journey session is long enough for the end user to complete the journey so that it doesn't time out. Learn more in Configure suspended journeys.

If you don't need to suspend a journey and wait for a reply, use the Email Template node instead.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The **Email Suspend** node either uses the identity profile in the shared state data or looks up the user profile. In either case, the node uses any applicable profile properties to populate the email template, omitting missing values from the populated template.

If **Object Lookup** is *not* enabled for the node (default), the shared state data must hold the **Email Attribute** with the recipient's email address and any properties the email template uses.

If **Object Lookup** is enabled for the node, the shared state data must hold the profile value to match the configured **Identity Attribute**. The **Email Suspend** node uses the **Identity Attribute** to look up the profile, and its **Email Attribute** to get the recipient's email address from the profile.

Dependencies

Before you use the **Email Suspend** node:

- Configure IDM integration in AM.
- Configure outbound email in IDM.

- Prepare an email template in IDM.

Record the email template name for use when configuring the **Email Suspend** node.

> **Tip**
>
> You can find the email template name in the required format in the URL when you're configuring the template. For example, the **Forgotten Username** email template's name is `forgottenUsername`:
>
> ```
> https://<tenant-env-fqdn>/?realm=alpha#/email/templates/edit/forgottenUsername
> ```

Configuration

Property	Usage
Email Template Name	The name of the email template prepared as a dependency. Default: `registration`
Email Attribute	The shared state data property or profile attribute for the recipient's email address. Default: `mail`
Email Suspend Message	The localized message to display when the node suspends the journey. According to OWASP authentication recommendations, the message should be the same regardless of the validity of the recipient's email address. You can use plain text or HTML code in this message. Default: `An email has been sent to the address you entered. Click the link in that email to proceed.`
Object Lookup	Whether to look up the managed identity profile. Default: disabled
Identity Attribute	The attribute used to identify the managed object in IDM. The node uses this when **Object Lookup** is enabled. Default: `userName`
PingAM **Suspend Duration**	(Optional) The length of time a journey session can be suspended in minutes. The time allowed for suspending the journey must be the same as or less than the maximum duration of the journey session. If set, this overrides the suspend duration set in the core authentication settings. Learn more in Suspend duration. Values from `1` to `2147483647` are allowed.

Outputs

This node doesn't add to the shared state data.

Outcomes

The **Email Suspend** node has a single outcome path.

Evaluation continues when the end user clicks the link in the email to resume the flow.

Errors

This node doesn't log any error or warning messages of its own.

Examples

The following default journeys use the **Email Suspend** node:

- `ForgottenUsername`
- `ResetPassword`
- `UpdatePassword`

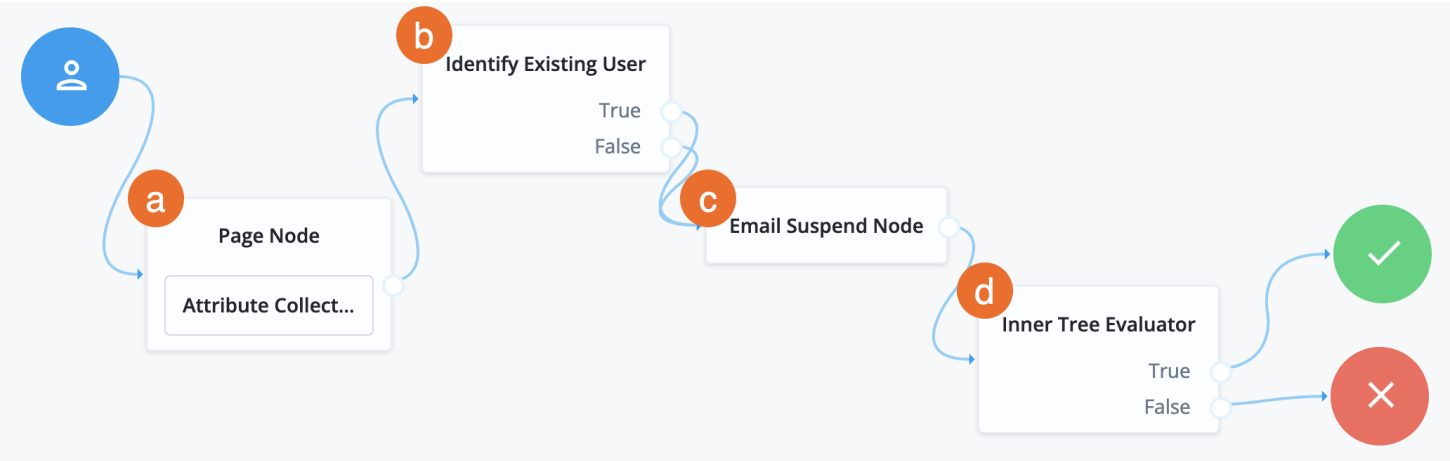
Example 1: Forgotten username

In the default journey for recovering a forgotten username, the end user enters their email address to recover their username.

Before you start

- Configure the email service.
- Optionally use the email template editor to modify the `forgottenUsername` template.

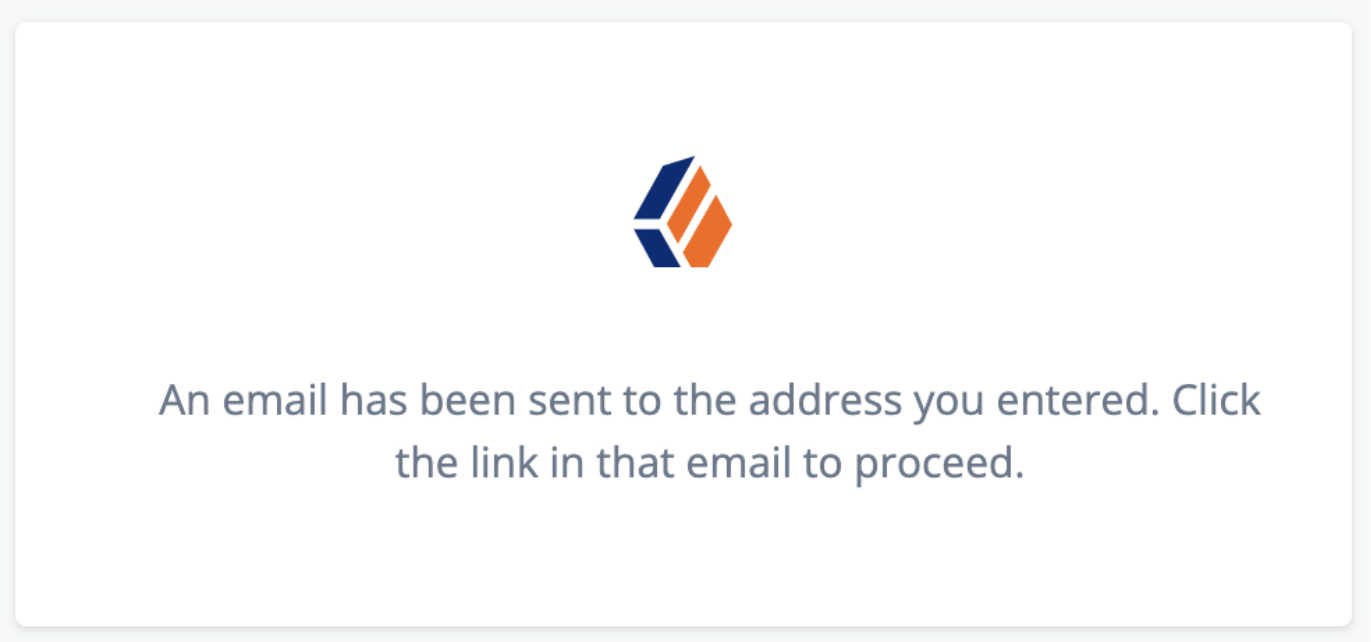
The journey



1. The Page node with an Attribute Collector node prompts for the end user's email address.
2. The Identify Existing User node attempts to look up the username by matching the email address to the email address in an identity profile.

   The lookup fails if more than one user profile uses the same email address.

3. The **Email Suspend** node reads the user profile, generates a unique `resumeURI` link to resume the journey, and populates the `forgottenUsername` email template. On success, the node makes a request to the email service to send the email. In any case, it displays the suspend message:



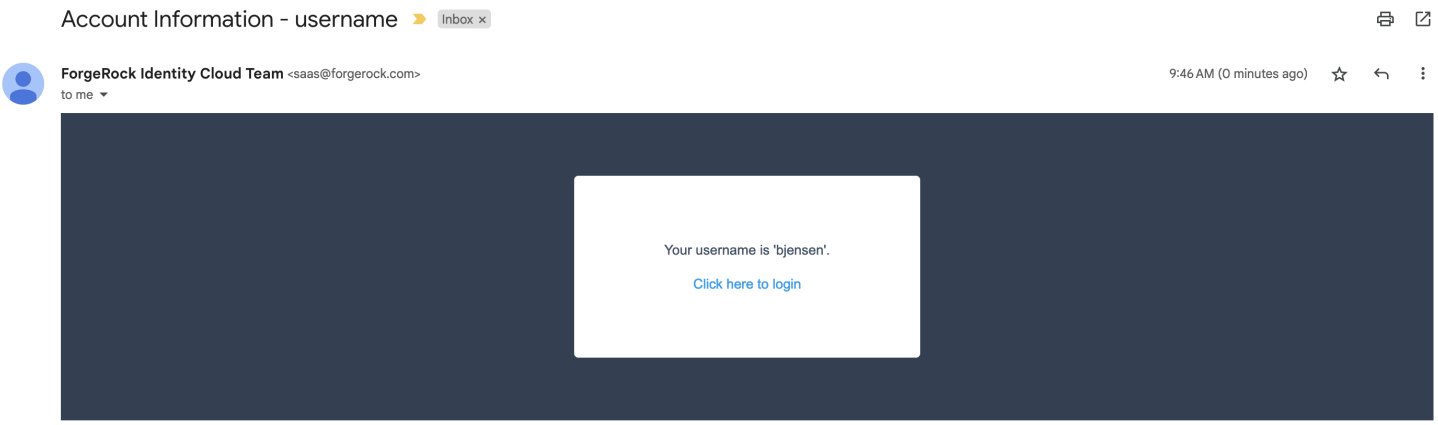
The node's settings are:

Email Template Name	`forgottenUsername`
Email Attribute	`mail` (default)
Email Suspend Message	`An email has been sent to the address you entered. Click the link in that email to proceed.` (default)
Object Lookup	Enabled
Identity Attribute	`mail`

4. When the end user clicks the link to resume the journey, the Inner Tree Evaluator node starts the `Login` journey.

Try the journey

Use the journey to recover the username for an account whose email you have access to. For example, if Babs Jensen's account has your email address, the **Email Suspend** node sends you a message such as the following:



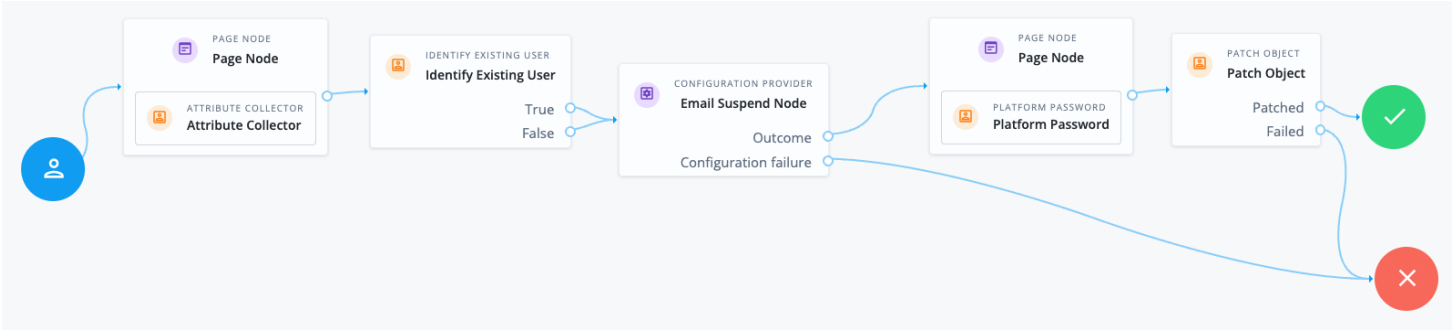
Follow the link to continue the journey and log in as Babs Jensen.

Example 2: Registration

For an example registration journey showing how to use the **Email Suspend** node and the Email Template node, read the **Email Template** node examples.

Example 3: Add dynamic user data to the email suspend message

This example uses the Configuration Provider node to imitate the **Email Suspend** node. Using the **Configuration Provider** node lets you include dynamic user data, such as their email address, in the email suspend message.



Find more information in Example 3: Imitate the Email Suspend node.

Email Template node

The **Email Template** node generates and sends an email, such as a welcome email based on an email template. This node relies on the email service configured in IDM to send the email.

This node doesn't wait for a reply. If authentication should pause and wait for a reply to the email, use the Email Suspend node instead.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed) **Note** This functionality requires that you configure AM as part of a sample Ping Identity Platform deployment.	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The **Email Template** node uses the identity in the shared state data to get the profile, meaning the journey must have successfully authenticated or at least identified the recipient. When the journey reaches this node, the shared state must hold the profile value to match the configured **Identity Attribute**. The value can be in the `username` property or in a property having the same name as the **Identity Attribute**.

The **Email Template** node uses its **Identity Attribute** to look up the profile, and its **Email Attribute** to get the recipient's email address from the profile. In other words, the node finds the recipient's address and other properties in the *profile*, not the shared state data.

For example, if the node uses default configuration settings and Babs Jensen authenticated to the journey, the shared state includes `"username": "bjensen"`. The node looks for a profile with `"userName": "bjensen"`. It gets the recipient address from the profile's `mail` attribute, such as `"mail": "bjensen@example.com"`. The node uses any applicable profile attributes to populate the email template, omitting missing values from the populated template.

Dependencies

Before you use the **Email Template** node:

- Configure IDM integration in AM.
- Configure outbound email in IDM.
- Prepare an email template in IDM.

  Record the email template name for use when configuring the **Email Template** node.

  Tip

  You can find the email template name in the required format in the URL when you're configuring the template. For example, the **Forgotten Username** email template's name is `forgottenUsername`:

  ```
  https://<tenant-env-fqdn>/?realm=alpha#/email/templates/edit/forgottenUsername
  ```

Configuration

Property	Usage
Email Template Name	The name of the email template prepared as a dependency. Default: `welcome`
Email Attribute	The profile attribute for the recipient's email address. Default: `mail`
Identity Attribute	The attribute used to identify the managed object in IDM. Default: `userName`

Outputs

This node doesn't add to the shared state data.

If the outcome is `Email Sent`, this node has sent the templated message to the recipient through the email service.

Outcomes

`Email Sent`

The node completed a request to send the message to the recipient.

If the message doesn't reach its destination, the problem is with the delivery, not with the node.

`Email Not Sent`

The node failed to complete a request to send the message.

This outcome arises, for example, when one of the following happens:

- The node can't get the user profile.
- The template doesn't match the user profile.
- The specified **Email Attribute** doesn't contain an address.

According to OWASP authentication recommendations, any messages displayed in the journey should be the same in both cases.

Errors

This node doesn't log any error or warning messages of its own.

Examples

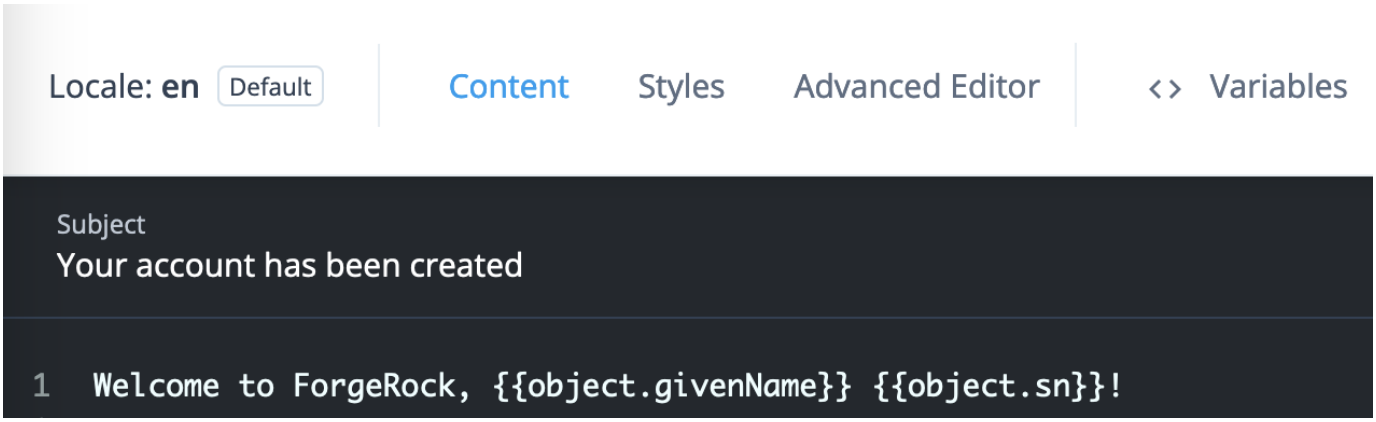
Use the **Email Template** node to send an email message when the journey doesn't depend on a reply. For example, send a welcome message when a user completes registration.

This example augments the default **Registration** journey and sends a welcome email.

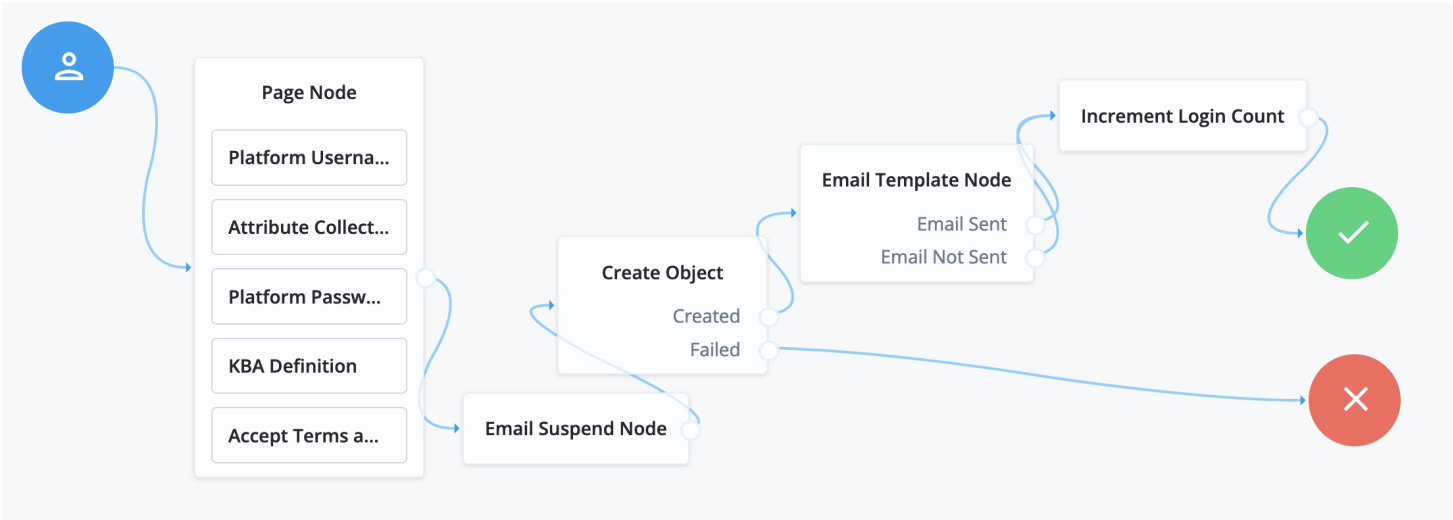
Before setting up the journey:

- Configure the email service.
- Create an email template for the **Email Template** node.

  Use the platform email template editor to duplicate the `Welcome` template and customize your copy:



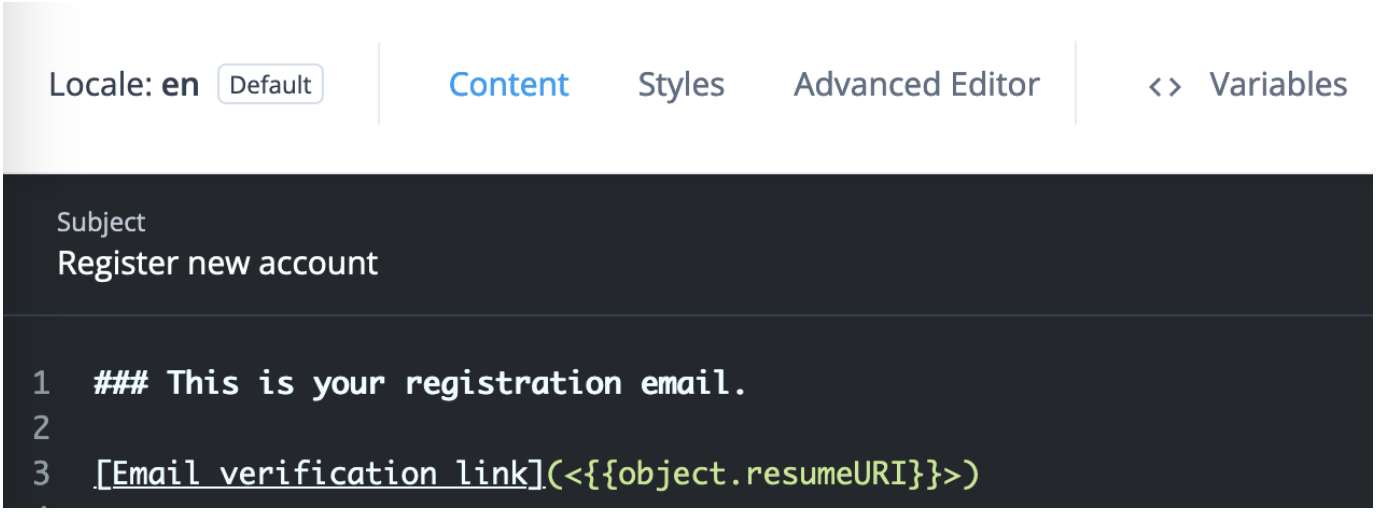
The journey is as follows:



1. The Page node prompts for the same information as the default **Registration** journey.
2. The Email Suspend node sends a message to the registered email address with a link for the user to click.

   The journey proceeds when the user clicks the link, confirming their email address.

   It has default settings and uses the default `Registration` email template:



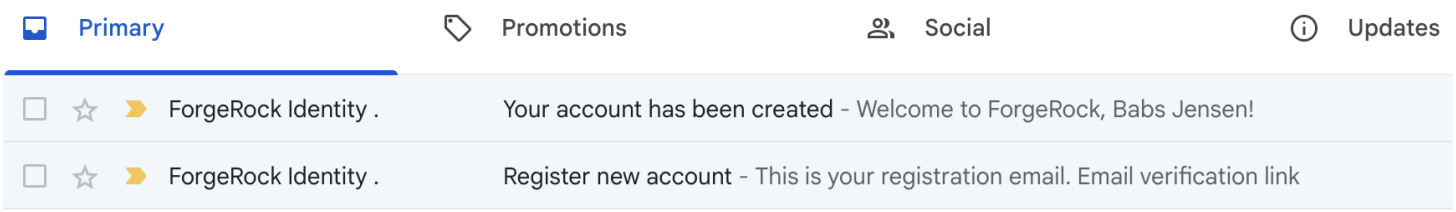
3. The Create Object node stores the newly registered user's profile.
4. The **Email Template** node reads the user profile and populates the template from profile attribute values. It makes a request to the email service to send the message.

   Its settings are:

Email Template Name	The name of your welcome email template
Email Attribute	`mail` (default)
Identity Attribute	`userName` (default)

5. The Increment Login Count node updates the count on successful authentication.

Use the journey to register an account for Babs Jensen with your email as the address. You receive two messages:



- The `Register new account` message has a link to click to continue the journey, confirming you can access the registered email account.
- The `Your account has been created` welcomes you on successful registration.

This demonstrates you have successfully used the **Email Template** node in a journey.

Failure URL node

Sets the redirect URL when authentication fails.

> **Note**
>
> Specifying a failure URL overrides any `gotoOnFail` query string parameters.

For more information on how AM determines the redirection URL, and to configure the Validation Service to trust redirection URLs, refer to Configure success and failure redirection URLs.

> **Tip**
>
> The URL is also saved in the shared `nodeState` object on the `failureUrl` key.
> Learn more in Customize authentication trees.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Failure URL *(required)*	Specify the full URL to redirect to when authentication fails.

Flow Control node

The **Flow Control** node lets you control the authentication flow by randomly sending traffic down different paths of a journey. This means you can use the node to evaluate changes before rolling out changes to a production environment. For example, configure the node to direct a percentage of requests to a new authentication journey to observe the user experience and check for potential failures.

Inputs

None. This node doesn't read shared state data.

Dependencies

This node has no specific dependencies.

Configuration

Property	Usage
Path A Percentage	The percentage of requests to send down path A. The remaining percentage follows path B.
Path A Name	The display name for the outcome of path A.
Path B Name	The display name for the outcome of path B.

Outputs

None

Outcomes

- `Path A Name` *(configured display name)*
- `Path B Name` *(configured display name)*

Errors

This node doesn't log any errors or warnings.

Example

The following sample journey lets an administrator phase in a new authentication path by initially routing a small number of incoming requests to the new login journey for monitoring.

The **Flow Control** node is configured with the following values:

Path A Percentage

`90`

Path A Name

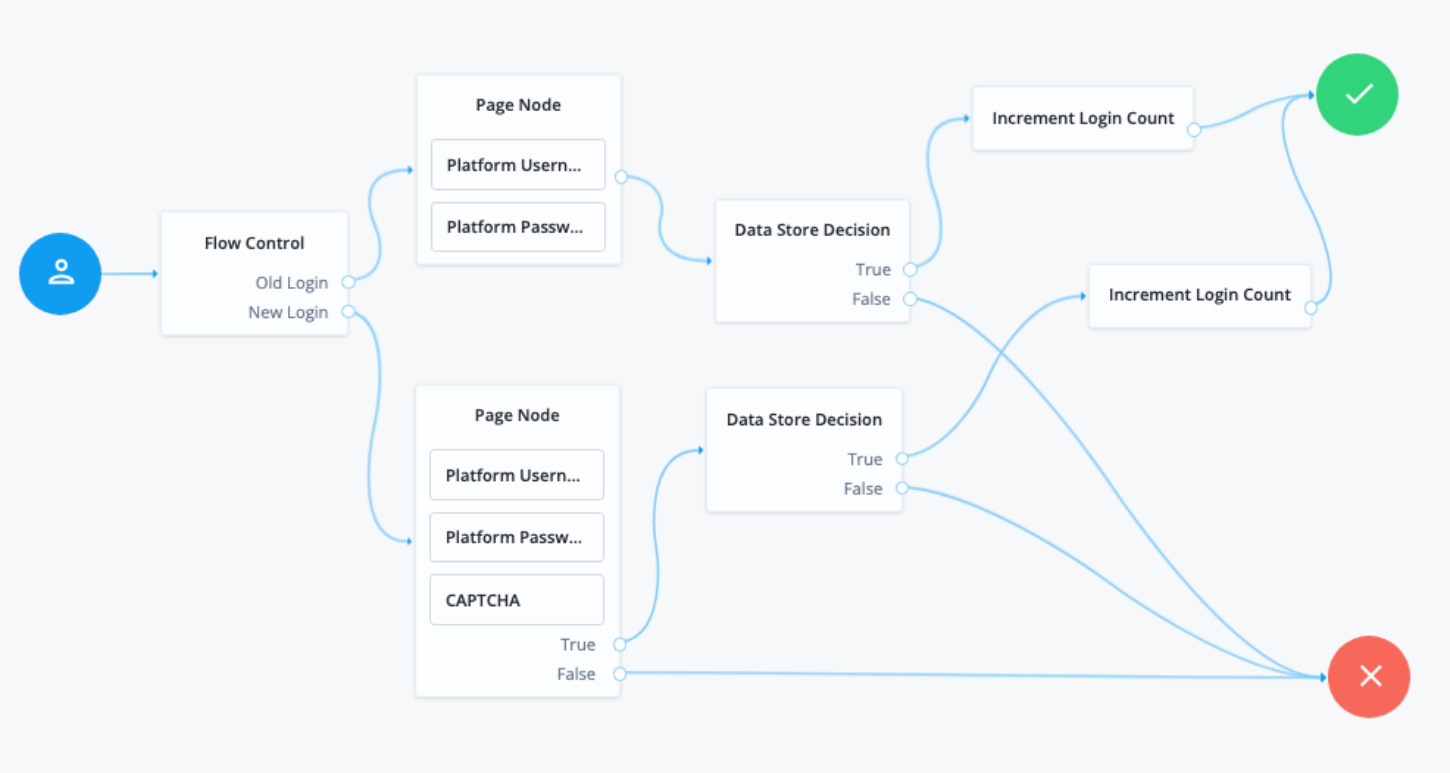
`Old Login`

Path B Name

`New Login`

The **Flow Control** node randomly assigns 90% of authentication requests to path A (`Old Login`) and the remaining 10% to path B (`New Login`).

The user follows the allocated path to complete authentication.



Get Session Data node

The **Get Session Data** node retrieves the value of a specified key from a user's session data, and stores it in the specified key of the shared state (in scripts, the `nodeState` object).

Use this node only during session upgrade—when the user has already successfully authenticated previously and is now upgrading their session for additional access. For more information on upgrading a session, refer to Session upgrade.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads values from the user's session data.

Dependencies

This node can complete its function only when the user has an existing session. Precede this node in the flow with a Scripted Decision node using a script to determine whether an existing session is present:

```
if (typeof existingSession !== 'undefined') {
  outcome = "hasSession";
} else {
  outcome = "noSession";
}
```

Configuration

All the configuration properties are required:

Property	Usage
Session Data Key	Specify the session data key whose value the node reads. Default: none
Shared State Key	Specify the name of the shared node state field to hold the session data. Default: none

Outputs

This node writes the **Session Data Key** value in the **Shared State Key** field of the shared node state.

It also writes the field and its value to the `objectAttributes` object in the shared node state.

Outcomes

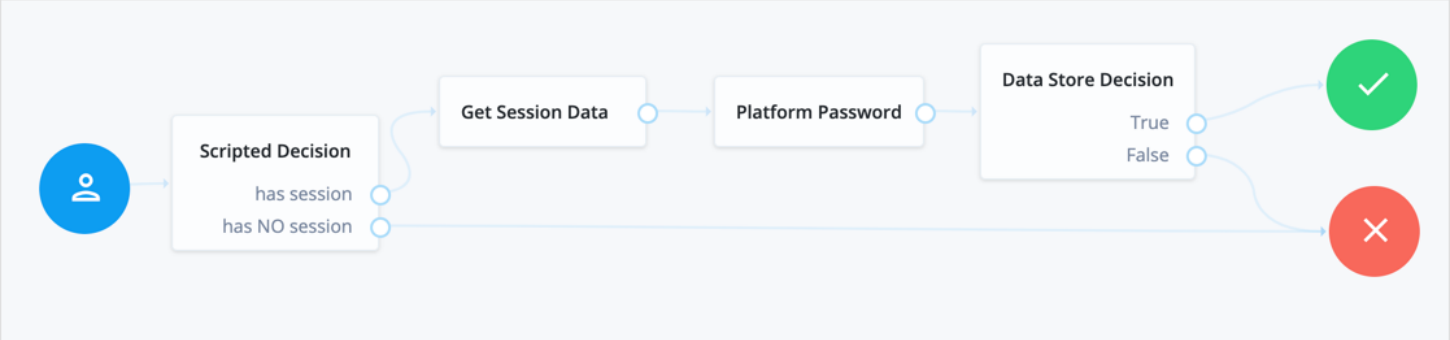
Single outcome path; on success, the **Shared State Key** in the shared node state holds the session data.

Errors

If it cannot read the **Session Data Key** value, this node logs an `Exception occurred trying to get data (<session-data-key>) from existing session` error message.

Example

When the user has an active session, the following example gets the username from the session, collects the password, and confirms the username-password credentials:



The following table includes example keys from an existing session with their corresponding sample values:

Key	Sample value
`AMCtxId`	`e370cca2-02d6-41f9-a244-2b107206bd2a-122934`
`amlbcookie`	`01`
`authInstant`	`2023-04-04T09:19:05Z`
`AuthLevel`	`0`
`CharSet`	`UTF-8`
`clientType`	`genericHTML`
`FullLoginURL`	`/am/XUI/?realm=alpha#login/`
`Host`	`34.117.172.39`
`HostName`	`am.forgeblocks.com`
`Locale`	`en_US`
`Organization`	`dc=openam,dc=forgerock,dc=org`
`Principal`	`uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org`
`Principals`	`amAdmin`
`Service`	`ldapService`
`successURL`	`/openam/console`
`sun.am.UniversalIdentifier`	`uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org`
`UserId`	`amAdmin`
`UserProfile`	`Required`

Key	Sample value
`UserToken`	`amAdmin`
`webhooks`	`myWebHook`

Inner Tree Evaluator node

The **Inner Tree Evaluator** node lets you nest authentication journeys as children within a parent. There is no limit to the depth of nesting.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

Any information collected or set by the parent journey, such as a username or the authentication level, is available in the child journeys.

Learn more about shared state data in Access shared state data.

Dependencies

None.

Configuration

Property	Usage
Tree Name	Select or enter the name of the authentication journey to evaluate. You must set this value; there's no default.

Outputs

Shared node state data collected by child journeys is available to the parent when evaluation of the child is complete, but data stored in transient and secure state is not. For instance, if a child journey collects and stores the user's password in transient state, it cannot be retrieved by a node in the parent journey when evaluation continues.

Learn more about shared state data in Access shared state data.

Outcomes

`True`

Successfully reached the `Success` node of the child.

`False`

Any other case.

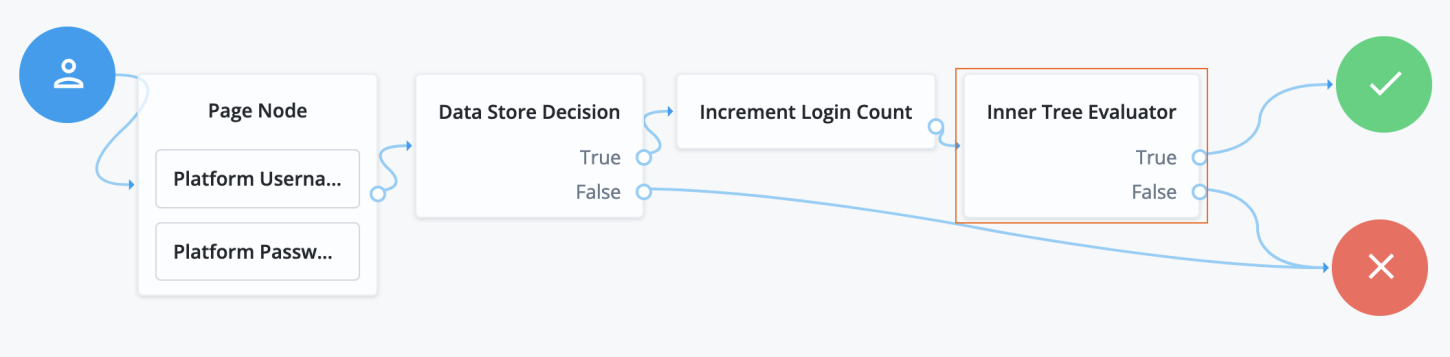
Errors

If it cannot get the shared node state from the child, this node logs an `Exception when gathering inner tree inputs` message.

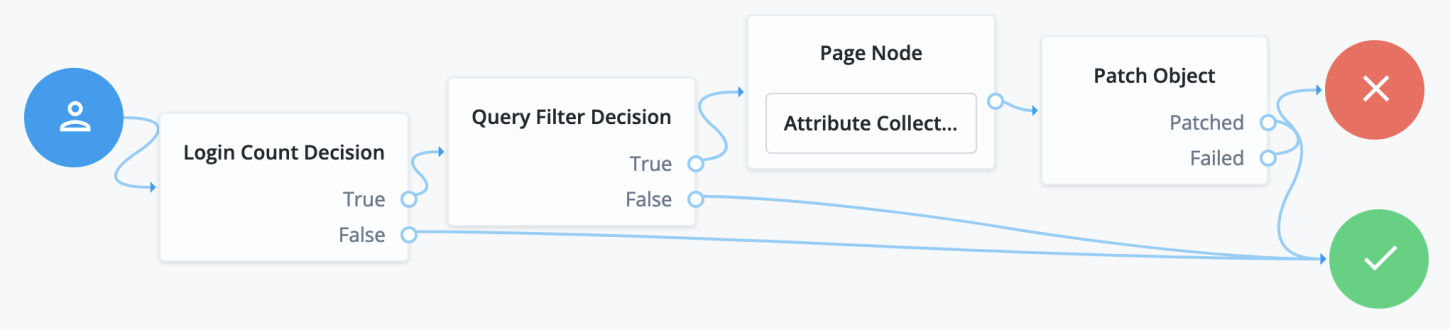
If the **Tree Name** doesn't match an existing journey, this node throws an exception with a `Configured tree does not exist: <tree-name>` message.

Example

The following journey uses an Inner Tree Evaluator node for progressive profiling:



- The Page node presents a page with input fields to prompt for the username and password.
  - The Platform Username node collects and injects the `userName` into the shared node state.
  - The Platform Password node collects and injects the `password` into the shared node state.
- The Data Store Decision node uses the username and password to determine whether authentication is successful.
- The Increment Login Count node updates the login count on successful authentication.
- The Inner Tree Evaluator node (outlined) invokes a nested journey:



- The Login Count Decision node triggers the rest of the journey depending on the login count and its settings.
- The Query Filter Decision node determines whether managed object profile fields are still missing.
- The Attribute Collector node in the Page node requests additional input for the profile.
- The Patch Object node stores the additional input in the managed object profile.

Message node

The **Message** node presents a custom, localized message to the user with customizable, localized positive and negative answer buttons the user must click to proceed.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads preferred locales from the incoming request context.

It doesn't read from the shared node state.

This node has no required predecessor nodes.

Dependencies

None.

Configuration

Property	Usage
Message	Add a custom, localized message per locale: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] The incoming HTTP request can include an `Accept-Language` header indicating the user's preferred locales. If the incoming HTTP request doesn't include the header or the preferred locales don't match any configured locales, the node uses default settings. It uses the **Realms > *Realm Name* > Authentication > Settings > General > Default Authentication Locale** setting from the AM admin UI. If there's no default authentication locale, the node uses **Deployment > Servers > *Server Name* > General > System > Default Locale**. 3. In the **Value** field, enter the message to display to the user. If you leave this blank, the message node displays a localized version of `Default message` to the user. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).
Positive answer	Add the text per locale for the positive answer button that triggers a **True** outcome: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] If the incoming HTTP request doesn't include the header or the preferred locales don't match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. If you leave this blank, the button displays a localized version of `Yes`. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).
Negative answer	Add the text per locale for the negative answer button that triggers a **False** outcome: 1. Click **Add**. 2. In the **Key** field, enter the locale.[1] If the incoming HTTP request doesn't include the header or the preferred locales don't match any configured locales, the node uses the first text in the list. 3. In the **Value** field, enter the text to display to the user. If you leave this blank, the button displays a localized version of `No`. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).

Property	Usage
Shared State Property Name	The name of the node state property. If set, the node adds the property to shared node state, setting its value to the numeric value of the outcome: ***0*** The user clicked the positive answer button. ***1*** The user clicked the negative answer button. For example, if you set this to `messageNodeOutcome` and the user clicks the positive answer button, the node adds `"messageNodeOutcome": 0` as a shared node state property.
Only Positive Answer	(Platform UI only) When enabled, the node displays only the positive answer button. **Note** This property only displays when the node is placed within a Page node in a Ping Identity Platform deployment.
Show buttons as links	When enabled, the node shows the buttons as links instead. **Note** This property only displays when the node is placed within a Page node in a Ping Identity Platform deployment.

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

Outputs

When the **Shared State Property Name** setting has a value, the node adds the property to the shared node state. The property's value is the numeric value of the outcome:

`0`

The user clicked the positive answer button.

`1`

The user clicked the negative answer button.

Outcomes

Returns a boolean outcome:

True

The user clicked the positive answer button.

False

The user clicked the negative answer button.

Errors

This node doesn't cause authentication to fail unless you connect one of the outcomes to a Failure node.

If the message or answer button settings specify a locale Java doesn't support, the node throws a configuration exception with an `Invalid locale provided` message. If this happens, fix the locale setting.

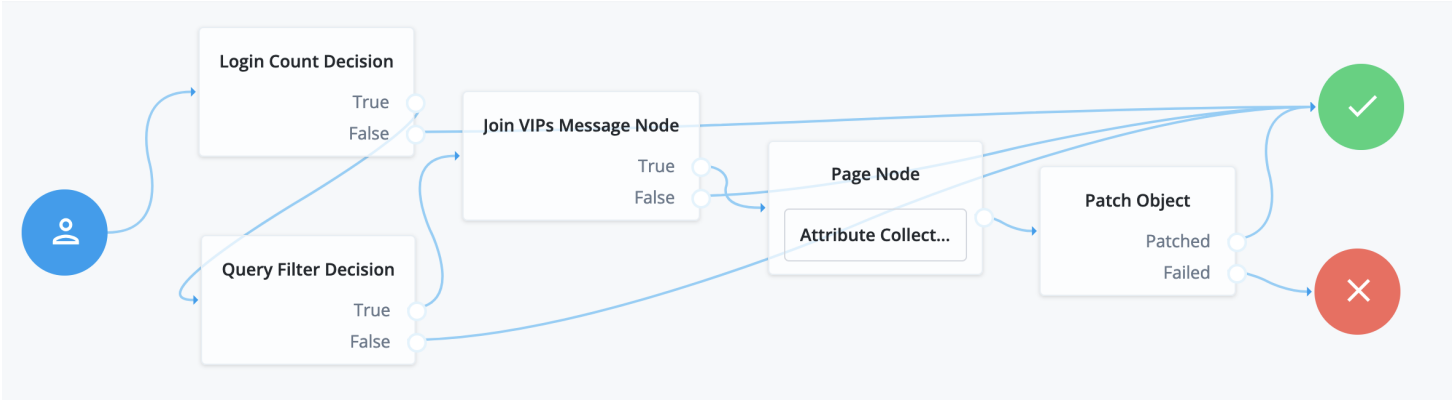
If this node encounters an internal configuration issue, it logs a warning message `Error attempting to retrieve the realm/global default locale`. If the warning persists, contact Ping Identity Support.

Examples

Use a **Message** node to:

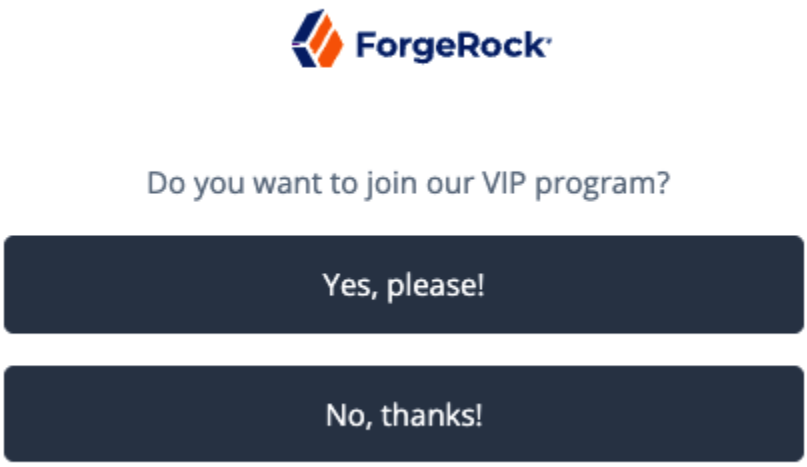
- Communicate an important message for the user to acknowledge.
- Ask a question with a yes/no answer.

The following journey uses the `Join VIPs Message Node` to prompt the user to join the VIP program:



- The Login Count Decision node triggers the Query Filter Decision node after every tenth authentication.
- The Query Filter Decision node queries the user profile to determine whether they have signed up for the VIP program.

  If the user hasn't signed up yet, the **True** outcome triggers the `Join VIPs Message Node`, which prompts the user to join the program:



Node property settings:

Message

`en-gb` ; `Do you want to join our VIP program?`

Positive answer

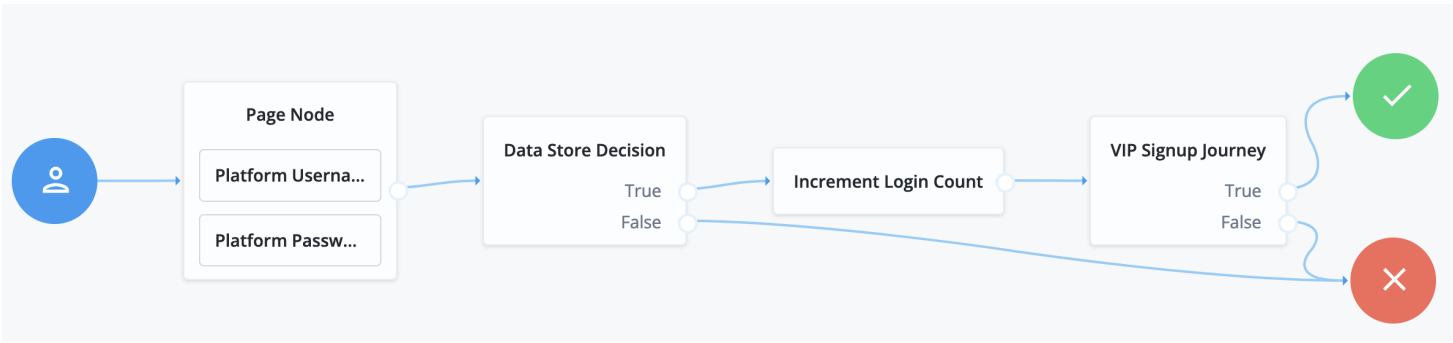
`en-gb` ; `Yes, please!`

Negative answer

`en-gb` ; `No, thanks!`

- If the user clicks **Yes, please!** the Page node with an embedded Attribute Collector node collects opt-in choices to store in user profile attributes.
- The Patch Object node updates the user profile with the attributes collected.

Call the journey using an Inner Tree Evaluator node from another authentication journey directly after an Increment Login Count node note:



The `VIP Signup Journey` uses the login count from the Increment Login Count node in the Login Count Decision node to decide whether to prompt the user to join the VIP program.

Meter node

Increments a specified metric key each time evaluation passes through the node.

You can find information on the `Meter` metric type in Monitoring metric types. The metric is exposed in all available interfaces, as described in Monitor AM instances.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Metric Key *(required)*	Specify the name of a metric to increment when evaluation passes through the node. Example: `authentication.success` For the list of available metrics, refer to Monitoring metrics.

Page node

The **Page** node lets you combine multiple nodes that request input onto a single page for display to the user.

Drag and drop nodes onto the Page node to combine them. Only add nodes that use callbacks to request input. Don't add other nodes, such as the Data Store Decision node and the Push Sender node to this node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The inputs are determined by the collective inputs of the contained nodes.

Dependencies

None.

Configuration

Property	Usage
Page Header	Optional. A localized title for the Page node and the nodes contained within it. Use this when components of an authentication journey need a title. For example, dividing a registration flow into labeled sections.
Page Description	Optional. A localized description for the Page node and the nodes contained within it. Use this when you need additional descriptive text in an authentication journey. In a Ping Identity Platform deployment, you can use HTML code to format the description.
Stage	Optional. A stage name to pass to the client to aid in rendering. NOTE: You can't configure a **Stage** for this node if you configure a **Page Footer**, **Theme** or **Submit Button Text**. These properties overwrite the value of the **Stage** property.
Submit Button Text	Optional. Use the **Key** and **Value** fields to set the text of the **Submit** button.
Page Footer	Optional. A localized footer for the page node and the nodes contained within it. Use this when you need additional descriptive text in an authentication journey. In a Ping Identity Platform deployment, you can use HTML code to format the footer.
Theme	Optional. If using hosted pages, specify a theme to override this journey's UI theme.

> **Note**
>
> This node's optional properties are passed in the response, but a self-hosted or custom UI must support these properties to make them visible to the end user.

Outputs

The outputs are determined by the collective outputs of the contained nodes.

Outcomes

The outcomes are determined by the last node in the Page node. Only the last node in the page can have more than one outcome path.

Errors

This node can log the following error messages:

Message	Notes
`Failed to collect inputs of contained node: <node-name>`	The <node-name> could not retrieve required properties from the shared node state
`Failed to collect outputs of contained node: <node-name>`	The <node-name> could not retrieve required properties to include in the shared node state
`Could not find the identity based on the information available on context`	Failed to find the account profile with this `username` in this `realm`
`An error occurred when trying to lock out the user account`	Failed to update the account status; applies when locking and unlocking the account

This node can throw exceptions with the following messages during operation:

Message	Notes
`This page has no nodes in it, so cannot proceed`	A Page node must contain at least one other node
`No outcome and only metadata callbacks found`	Failed to get to an outcome while processing the contained nodes
`Node properties cannot be fetched`	Failed to access the properties of a contained node

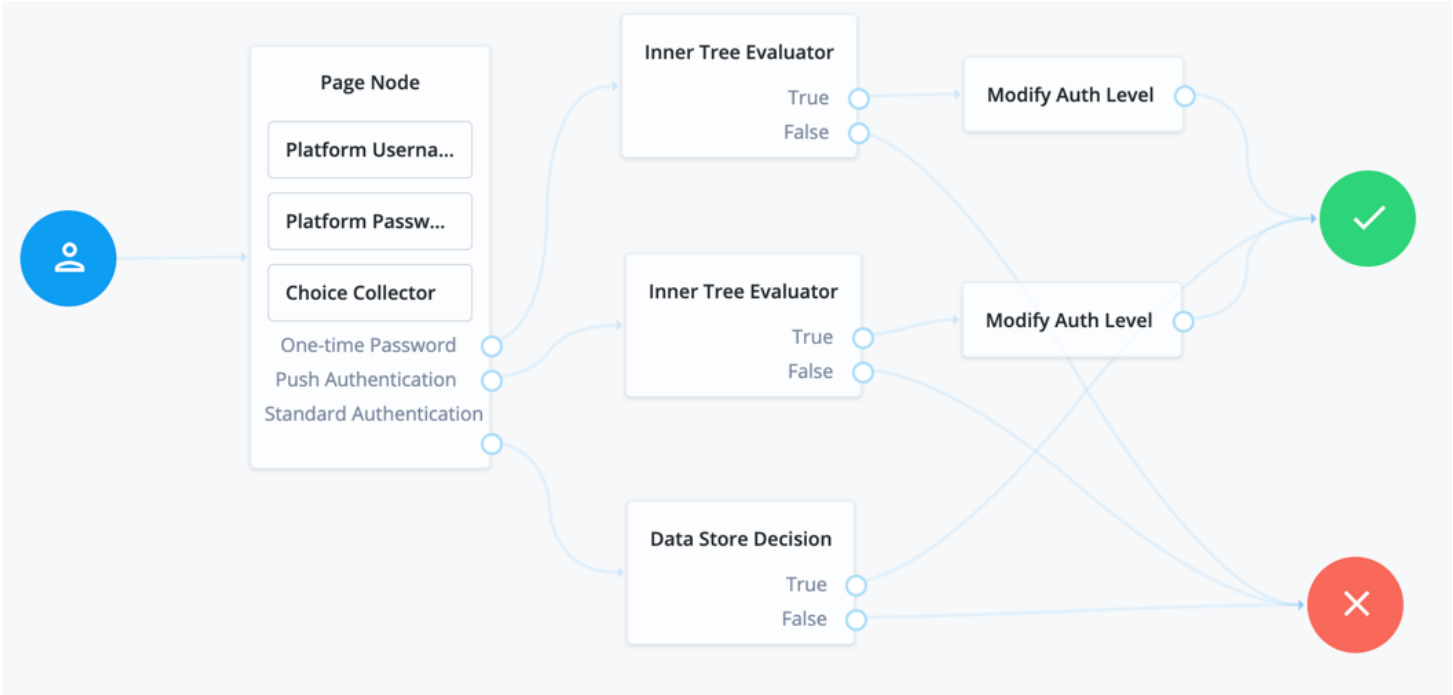
This node can throw exceptions with the following messages when saving the journey:

Message	Notes
`Illegal child node type: <node-type>`	A Page node can’t contain a <node-type>
`Node does not have any outcomes: <node-type>`	The contained nodes must have at least a single outcome path

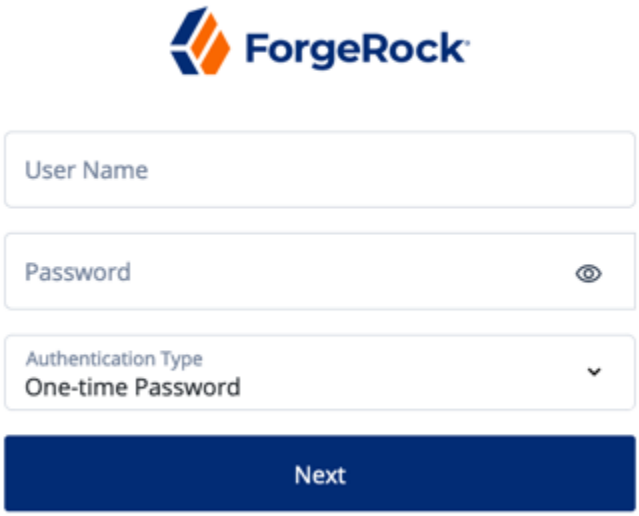
Message	Notes
`Only the last node in a page can have more than one outcome`	Consider rearranging the contained nodes
`Node does not exist: <node-id>`	Use the journey editor to fix the problem
`Could not load child node: <node>`	Use the journey editor to fix the problem
`Could not obtain outcomes for node: <node>`	Use the journey editor to fix the problem

Example

The following example uses a Page node containing a Platform Username node, Platform Password node, and Choice Collector node:



The flow prompts the user for all input on a single page:



Polling Wait node

Pauses authentication progress for a specified number of seconds, for example, to wait for a response to a one-time passcode email or push notification.

Requests made during the wait period are sent a `PollingWaitCallback` callback and an authentication ID. For example, the following callback indicates a wait time of 10 seconds:

```
{
    "authId": "eyJ0eXAiOiJK...u4WvZmiI",
    "callbacks": [
        {
            "type": "PollingWaitCallback",
            "output": [
                {
                    "name": "waitTime",
                    "value": "10000"
                },
                {
                    "name": "message",
                    "value": "Waiting for response..."
                }
            ]
        }
    ]
}
```

The client must wait 10 seconds before returning the callback data, including the `authId`:

```
$ curl \
--request POST \
--header "Accept-API-Version: resource=2.0, protocol=1.0" \
--header "Content-Type: application/json" \
--data '{
  "authId": "eyJ0eXAiOiJK…u4WvZmiI",
  "callbacks": [
      {
          "type": "PollingWaitCallback",
          "output": [
              {
                  "name": "waitTime",
                  "value": "10000"
              },
              {
                  "name": "message",
                  "value": "Waiting for response…"
              }
          ]
      }
  ]
}' \
'https://am.example.com:8443/am/json/realms/root/realms/alpha/authenticate?
authIndexType=service&authIndexValue=Example'
```

The end user UI automatically waits for the required amount of time and resubmits the page to continue evaluation. The message displayed during the wait is configurable with the **Waiting Message** property.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Done`
- `Exited` (configurable)
- `Spam` (configurable)

Evaluation continues along the `Done` outcome path when the next request is received after the wait time has passed.

Enabling Spam detection adds a `Spam` outcome path to the node. Evaluation continues along the `Spam` outcome path if more than the specified number of requests are received during the wait time.

Enabling the user to exit without waiting adds an `Exited` outcome path to the node. Evaluation continues along the `Exited` outcome path if the user clicks the button that appears when the option is enabled. The message displayed on the exit button is configurable by using the **Exit Message** property.

Properties

Property	Usage
Seconds To Wait	Specify the number of seconds to pause authentication. Default: `8`
Enable Spam Detection	Specify whether to track the number of responses received during the wait time, and continue evaluation along the `Spam` outcome path if the number specified in the **Spam Tolerance** property is exceeded. Default: Disabled
Spam Tolerance	Specify the number of responses to allow during the wait time before continuing evaluation along the `Spam` outcome path. This property only applies if spam detection is enabled. Default: `3`
Waiting Message	Specifies the optional message to display to the user. Provide the message in multiple languages by specifying the locale in the **KEY** field. For example, `en-gb`.[(1)] The locale selected for display is based on the user's locale settings in their browser. Leave blank to use the default message.[(2)]
Exitable	Whether the user can exit the node during the wait period. Enabling this option adds a button with a configurable message to the page. Clicking the button causes evaluation to continue along the `Exited` outcome path. Default: Disabled
Exit Message	Specifies the optional message to display to the user on the button used to exit the node before the wait period has elapsed. For example, `Cancel` or `Lost phone? Use Recovery Code`. This property only applies if the **Exitable** property is enabled. Provide the message in multiple languages by specifying the locale in the **KEY** field. For example, `en-gb`.[(1)] The locale selected for display is based on the user's locale settings in their browser. Leave blank to use the default message.[(2)]

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

(2) PingAM only: Learn more about customizing and translating default messages in Internationalize nodes.

Query Parameter node

The **Query Parameter** node lets you insert query parameter values from a journey URL into configurable node state properties. This lets you customize journeys based on the query parameter values.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node takes its inputs from the journey URL and maps each query parameter to a property in the node state. For multi-valued parameters, the node delimits the parameters by a comma (`,`) symbol. In this case, the value assigned to the node state property is a comma-delimited list of items.

The node doesn't read input from the state.

The node has no required predecessor nodes.

Dependencies

None.

Configuration

Property	Usage
Allowed query parameters	List the query parameters the node can obtain from the URL and map them to a property in the node state: 1. Click **Add**. 2. In the **Key** field, enter the query parameter name. 3. In the **Value** field, enter the node state property that will hold the value of this query parameter. This field sets an allow list of parameters the node can pull into the node state. Exercise caution when you create this list to avoid injecting harmful data into the node state. If a query parameter in the URL isn't in this list, the node ignores it. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).

Property	Usage
Allowed query parameters to be delimited	Specify the allowed query parameters that can take multiple values and whose values you want to store in the node state in a comma-delimited list. For example, `["yellow", "green", "red"]`. Enter the query parameter name in the **Add value** field and click **Add**. If you don't delimit the values of a multi-valued query parameter, the node stores the values in the node state as a single string value. For example, `["yellow, green, red"]`. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).

Outputs

- If the **Allowed query parameters** setting has one or more values, the node adds the values of the listed URL parameters to the corresponding properties in the node state.
- If the **Allowed query parameters** setting has a value but that query parameter isn't present in the URL, the node sets an empty list (`[]`) in the corresponding node state property.
- If an allowed query parameter is also listed in the **Allowed query parameters to be delimited**, the node sets the values of the listed URL parameter in the node state as a comma-delimited list.

Important

- The node URL-decodes query parameters before putting them into the node state.
  If a query parameter includes `%2C`, the node puts this value into the node state as a comma (`,`). If the query parameter is included in the **Allowed query parameters to be delimited** the node interprets `%2C` as a comma delimiter.
  The node decodes the plus symbol (`+`) as a *space*. If you need a `+` in a query parameter value, encode it as `%2B` in the URL.
- Values stored in the node state can override values in the authentication journey.
  Take special care when you configure this node so that you don't unintentionally override parameters such as usernames and passwords.
  The output of this node isn't under the control of the node itself. Encode sensitive values appropriately, either at node output or before the values are used later in the journey.

Outcomes

Single outcome that passes an updated node state to the next node in the journey.

Errors

- `No parameters configured - this node is redundant`

  The node logs this error if you include it in a journey but don't configure any **Allowed query parameters**.

- `Cannot delimit parameter if it is not configured as a parameter to be stored in node state`

The node logs this error if you add a parameter to the list of **Allowed query parameters to be delimited** but not to the list of **Allowed query parameters**.

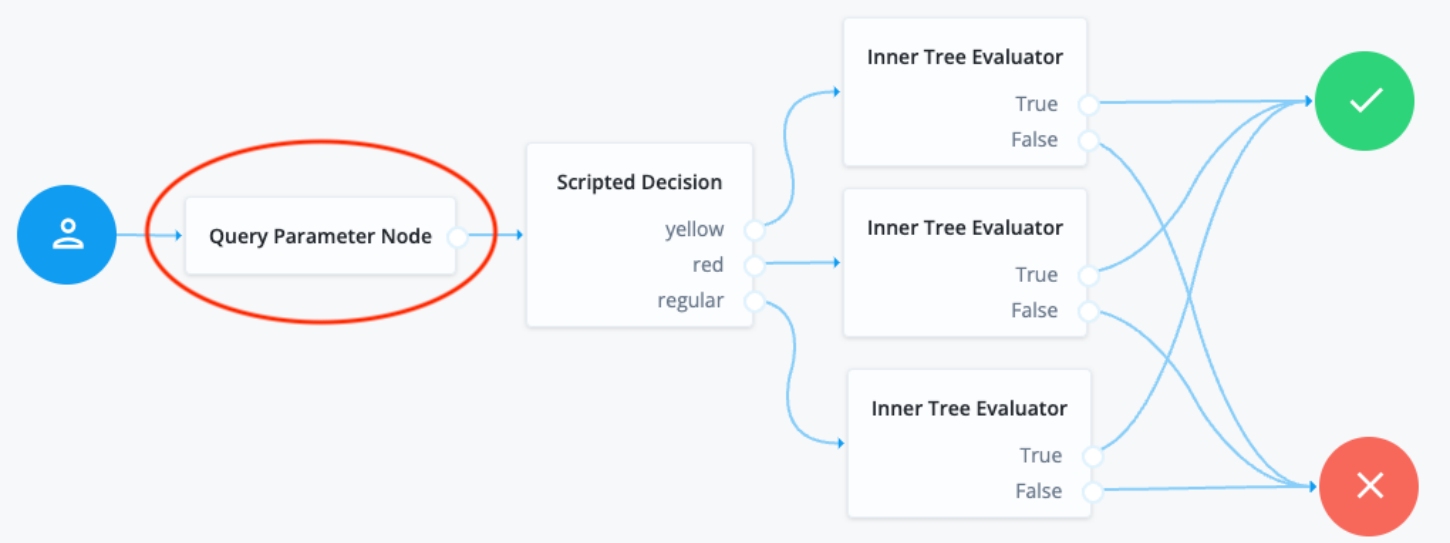
Examples

Use the Query Parameter node to customize a journey based on query parameters in the URL. The following scenarios illustrate how this node could be used:

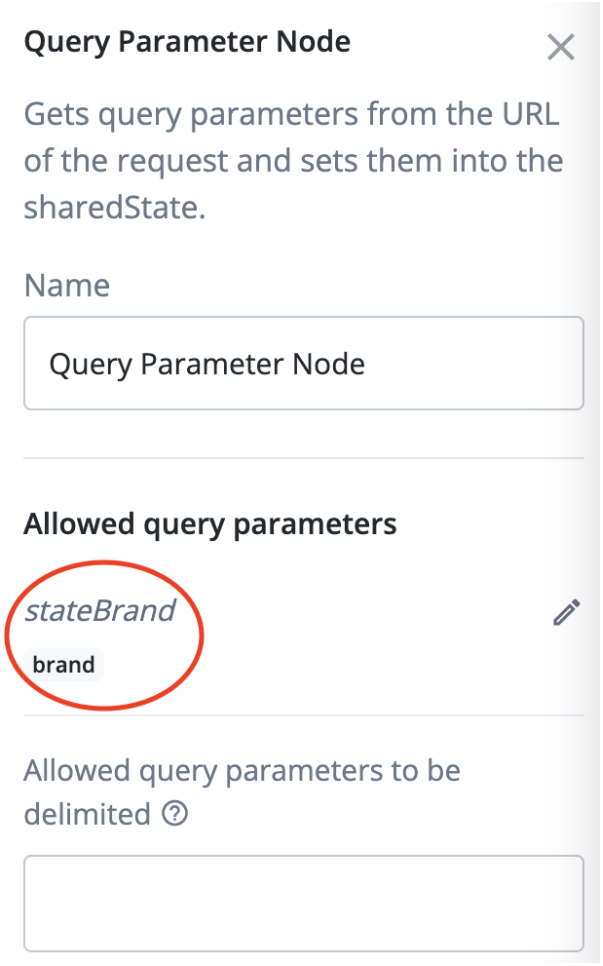
Customized branding

An organization has several brands that use the same journey. Use this node to customize the brand the user sees, based on the query parameters.

Consider the following authentication journey:



1. The configuration of the Query Parameter node maps the `brand` query parameter to a property in the node state named `stateBrand`

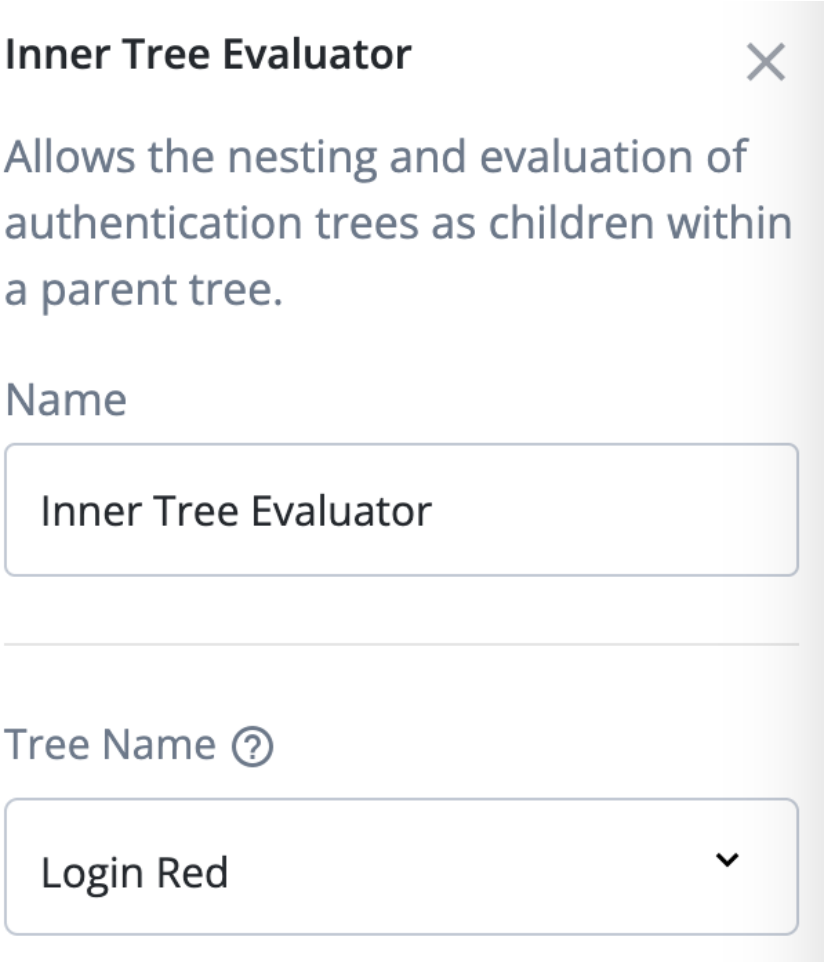


2. The user accesses the journey at a URL that can be one of the following:
   - `https://<tenant-env-fqdn>/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=Login`
   - `https://<tenant-env-fqdn>/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=Login&brand=yellow`
   - `https://<tenant-env-fqdn>/am/XUI/?realm=alpha&authIndexType=service&authIndexValue=Login&brand=red`
3. The Query Parameter node obtains the value of `brand` from the URL and sets that value in the `stateBrand` property in the node state. For example, `stateBrand=yellow`
4. The journey progresses to the scripted decision node that includes the following script:

```
var brand = JSON.parse(nodeState.get('stateBrand'));

if (brand.indexOf("yellow") >= 0) {
  outcome = "yellow";
} else if (brand.indexOf("red") >= 0) {
  outcome = "red";
} else {
  outcome = "regular";
}
```

5. The script routes the journey to one of three outcomes; `yellow`, `red`, or `regular`, depending on the value of the `stateBrand` property.
6. The outcomes direct the user to a custom branded Login journey configured in an Inner Tree Evaluator node. For example:



7. Each Inner Tree Evaluator node routes the end user to a login journey that uses a custom brand.

Redirection from an external system

An external system redirects a user to this authentication journey. The external system must share information about the user with the journey. Use this node to obtain the relevant query parameters and inform the journey of their values.

Register Logout Webhook node

Registers the specified webhook to trigger when a user's session ends. The webhook triggers when a user explicitly logs out or the maximum idle time or expiry time of the session is reached.

The webhook is only registered if evaluation passes through this node. You can register multiple webhooks during the authentication process, but they must be unique.

Find more information on webhooks in Configure authentication webhooks.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Webhook name	Specify the name of the webhook to register.

Remove Session Properties node

Removes properties from the session. The session properties may have been set by a Set Session Properties node elsewhere in the flow.

If a specified key is not found in the list of session properties it is added to the session upon successful authentication, no error is thrown, and evaluation continues along the single outcome path.

If a specified key is found, the evaluation continues along the single outcome path after setting the value of the property to `null`.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Property Names *(required)*	Enter one or more key names of properties to remove from the session.

Request Header node

The **Request Header** node lets you insert values from request headers into configurable node state properties. This lets you customize journeys based on the request header values.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node takes its inputs from one or more request headers and maps these values to properties in the node state. For multi-valued headers, the node delimits headers with a comma (`,`) and assigns the value to the node state property as a comma-delimited list.

The node doesn't read input from the state.

The node has no required predecessor nodes.

Dependencies

None.

Configuration

Property	Usage
Allowed headers	List the header names the node can obtain from the URL and map them to a property in the node state: 1. Click **Add**. 2. In the **Key** field, enter the query parameter name. 3. In the **Value** field, enter the node state property that will hold the value of this request header. This field sets an allow list of headers the node can pull into the node state. Exercise caution when you create this list to avoid injecting harmful data into the node state. If a provided request header isn't in this list, the node ignores it. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).
Allowed headers to be delimited	The allowed headers that can take multiple values and whose values you want to store in the node state in a comma-delimited list. For example, `["yellow", "green", "red"]`. Enter the header name in the **Add value** field and click **Add**. If you don't delimit the values of a multi-valued header, the node stores the values in the node state as a single string value. For example, `["yellow, green, red"]`. To edit an entry, click the **Pencil** icon (✎). To remove an entry, click the **Delete** icon (🗑).

Outputs

- If the **Allowed headers** setting has one or more values, the node adds the values of the listed request headers to the corresponding properties in the node state.
- If the **Allowed headers to be delimited** setting has a value but that header isn't provided in the request, the node sets an empty list (`[]`) in the corresponding node state property.
- If an allowed header is also listed in the **Allowed headers to be delimited**, the node sets the values of that header in the node state as a comma-delimited list.
- The node performs no decoding or sanitization on the header value. It simply passes the value into the node state as a string.

Important

Values stored in the node state can override values in the authentication journey.
Take special care when you configure this node so that you don't unintentionally override parameters such as usernames and passwords.
The output of this node isn't under the control of the node itself. Encode sensitive values appropriately, either at node output or before the values are used later in the journey.

Outcomes

Single outcome that passes an updated node state to the next node in the journey.

Errors

- `No headers configured — this node is redundant`

  The node logs this error if you include it in a journey but don't configure any **Allowed headers**.

- `Cannot delimit header if it is not configured as a header to be stored in node state`

  The node logs this error if you add a header to the list of **Allowed headers to be delimited** but not to the list of **Allowed headers**.

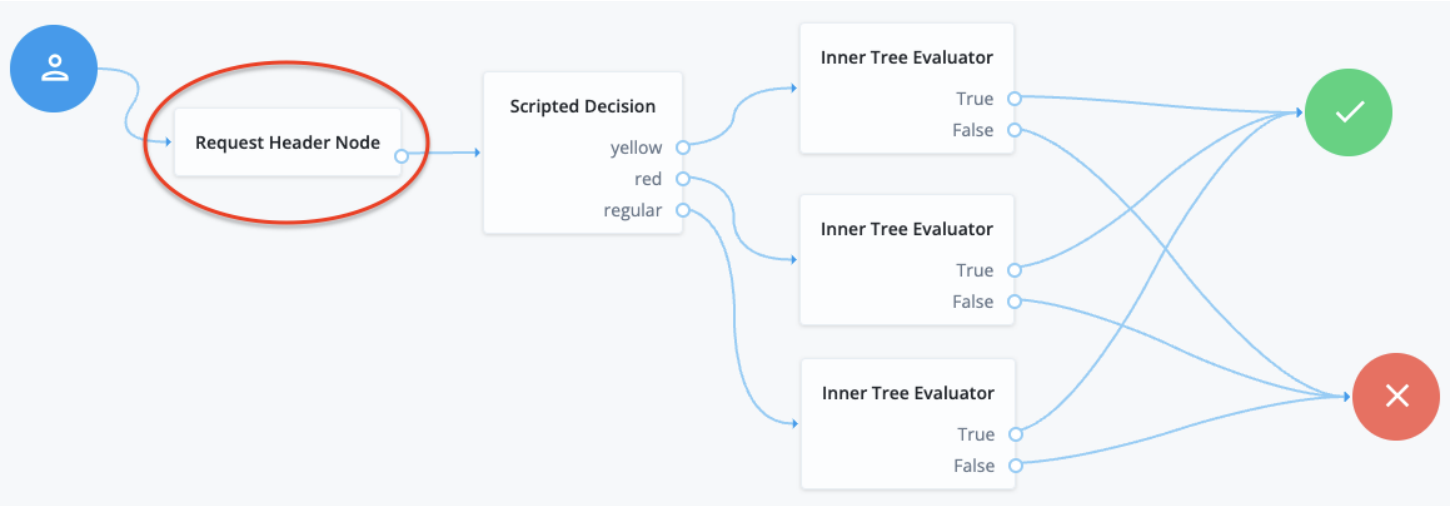
Examples

Use the Request Header node to customize a journey based on the values of specific request headers. The following scenarios illustrate how this node could be used:

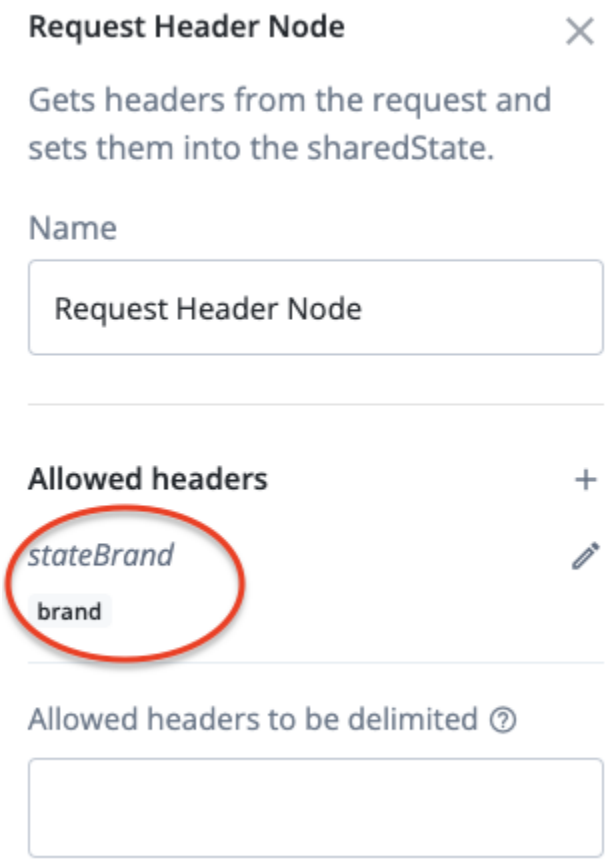
Customized branding

An organization has several brands that use the same journey. Use this node to customize the brand the user sees, based on the request header.

Consider the following authentication journey:



1. The configuration of the Request Header node maps the `brand` header to a property in the node state named `stateBrand`



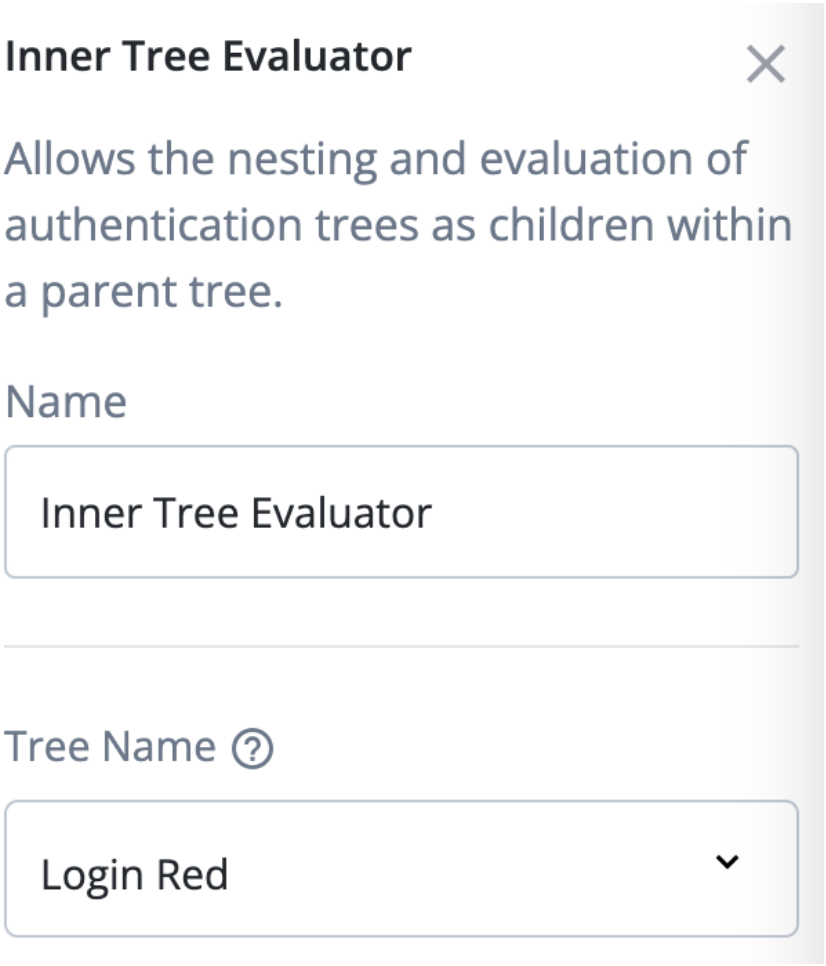
2. The REST request to access the journey includes one of the following headers:
    - `--header "brand: yellow"`
    - `--header "brand: red"`
    - `--header "brand: regular"`
3. The Request Header node obtains the value of the `brand` header and sets that value in the `stateBrand` property in the node state. For example, `stateBrand=yellow`
4. The journey progresses to the scripted decision node that includes the following script:

```
var brand = JSON.parse(nodeState.get('stateBrand'));

if (brand.indexOf("yellow") >= 0) {
  outcome = "yellow";
} else if (brand.indexOf("red") >= 0) {
  outcome = "red";
} else {
  outcome = "regular";
}
```

5. The script routes the journey to one of three outcomes; `yellow`, `red`, or `regular`, depending on the value of the `stateBrand` property.

6. The outcomes direct the user to a custom branded Login journey configured in an Inner Tree Evaluator node. For example:



7. Each Inner Tree Evaluator node routes the end user to a login journey that uses a custom brand.

Redirection from an external system

An external system redirects a user to this authentication journey. The external system must share information about the user with the journey. Use the Request Header node to obtain the relevant request headers and inform the journey of their values.

Retry Limit Decision node

The **Retry Limit Decision** node tracks failed authentications. If the number of failed authentications is below a specified **Retry Limit**, the user can attempt authentication again. Otherwise, the node continues evaluation along the `Reject` outcome path.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

The node reads the `username` from the shared state. Implement the following node before this node in the journey:

- Username Collector node (standalone AM)
- Platform Username node (Ping Identity Platform deployment)

The node also reads the `realm` from the incoming node state.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Retry limit	Specify the number of retries to allow. Default: `3`
Save Retry Limit to User	Specify whether the number of failed login attempts persists across multiple journeys until authentication is successful. Possible values are: ***Enabled*** The node saves the number of failed login attempts to the `retryLimitNodeCount` attribute in the user's profile. New flows using this node start with the stored value and continue to the retry limit. AM resets the count after the user authenticates successfully with an authentication journey that contains this node. If AM can't find the user's profile, authentication ends with an error. ***Disabled*** The node saves the number of failed login attempts in a shared state property named `nodeId.retryCount` and discards the value when the authentication journey ends. For security reasons, you should enable this setting. Default: Enabled.

Outputs

If **Save Retry Limit to User** is enabled, the node increments the retry count and saves the number of failed attempts to the `retryLimitNodeCount` attribute in the user's profile. If the user can't be identified during the journey, the journey ends with an error.

If **Save Retry Limit to User** is disabled, the node increments the retry count and saves the number of failed attempts to a shared state property named `nodeId.retryCount`. The count is lost if the journey is restarted.

Outcomes

`Retry`

The user hasn't exceeded the number of allowed retries and can attempt authentication again.

`Reject`

The user has exceeded the number of allowed retries.

Errors

This node can log the following:

Warnings

- `Error clearing attribute`

  The node can't reset the `retryLimitNodeCount` user attribute after the user has successfully authenticated.

Errors

- `Error getting current retry count`

  The node can't retrieve the current retry count.

- `Failed to save retryLimitNodeCount to user: Identity Repo has not been upgraded.`

  The node can't save retry count details to the `retryLimitNodeCount` user attribute during the authentication flow.

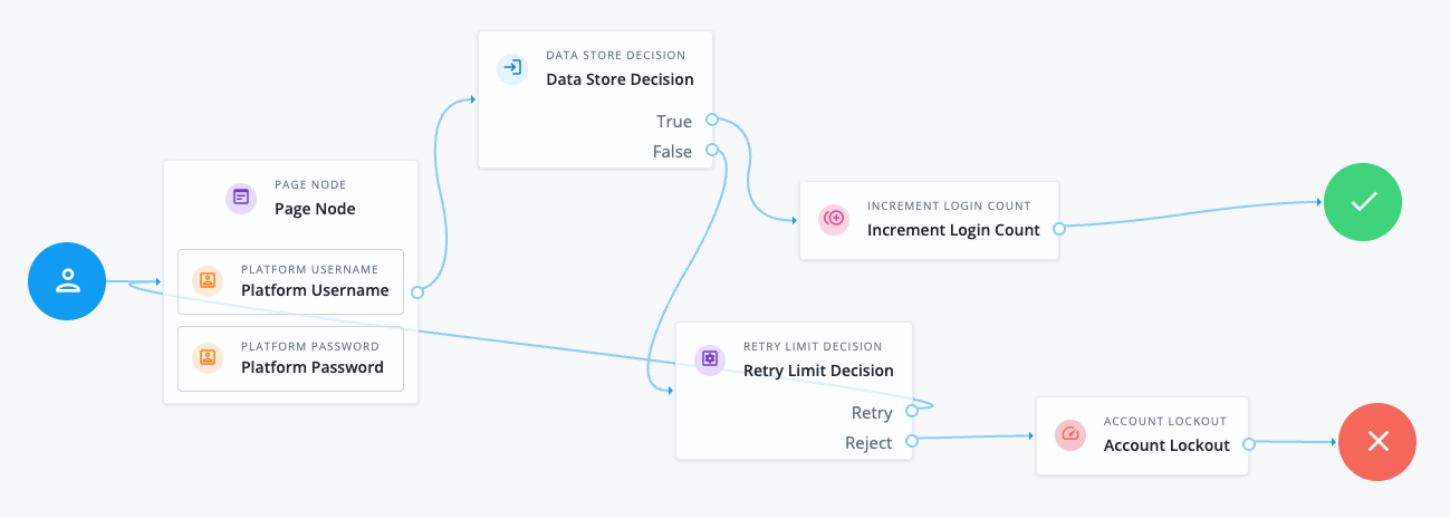
- `Error setting retry count on user attribute`

  The node can't increment the retry count on the `retryLimitNodeCount` user attribute during the authentication flow.

These warnings and errors typically occur if the identity store is unreachable or the user no longer exists.

Examples

This example uses the **Retry Limit Decision** node to allow a user three attempts to authenticate. Otherwise, their account is locked.



- The Page node containing the Platform Username node and Platform Password node prompts for credentials.
- The Data Store Decision node validates the username-password credentials.
- The Increment Login Count node updates the number of successful authentications in the user profile.
- The **Retry Limit Decision** node is configured to allow three login attempts and either retries the login attempt or rejects it depending on the number of failed attempts.
- The Account Lockout node locks the user's account on their fourth failed attempt.

Scripted Decision node

The **Scripted Decision** node lets you run a server-side script in an authentication journey. It exists to let you connect the script to other nodes with the journey editor.

The script makes a decision to set the outcome for the node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

Scripted Decision node inputs depend entirely on the node's server-side script.

The script has access to the authentication context including:

- Headers from the request
- Query string parameters from the request
- Secrets configured for the realm
- Shared state data
- User profile data

The script can use callbacks to prompt the user for information.

Find details about the inputs available to the script in Scripted decision node API.

You can restrict available inputs using the **Script Inputs** field when configuring the node.

Dependencies

A **Scripted Decision** node depends on a **Decision node for authentication trees** script you create before you configure the node.

Configuration

Property	Usage
Script	Select the script to run from the drop-down list.
Outcomes	Enter one string for each `outcome` the script can set. The node shows only the outcomes you configure. If you omit an `outcome` string, you can't connect it in the journey editor. When the script sets an `outcome` you omitted in the configuration, it logs a warning. This can prevent the journey from completing successfully.

Property	Usage
Script Inputs	Optionally, list the shared state data properties required by the script. If you change the setting, you must declare each property or `null` for no properties. Default: `*`. The script has access to all shared and transient state data. **Important** Sensitive data in transient state upgrades to *secure* state if: • The node sends a callback to the user. • The node detects a downstream node requesting the transient state data as input. Unless the downstream node explicitly requests the secure state data by name, the authentication journey removes it from the node state after processing the next callback. For example, a node in a registration journey stores a user's password in transient state. The node sends a callback to the user before an inner tree node, downstream in the journey, consumes that password. As part of the callback, the journey assesses what to add to the secure state. It does this by checking the state inputs that downstream nodes in the journey require. Nodes that *only* request `*` are ignored, as this would result in putting everything in transient state into secure state, and retaining sensitive information longer than necessary. If a downstream node requires the password, it must explicitly request it as state input, even if it lists the `*` wildcard as input.
Script Outputs	Optionally, list the shared state data properties the node expects the script to set. If you change the setting, you must declare each property or `null` for no properties. Default: `*`. The node doesn't validate the script outputs at all.

Outputs

Scripted Decision node outputs, such as updates to shared state data, depend entirely on the node's server-side script.

You can restrict available outputs using the **Script Outputs** field when configuring the node.

Outcomes

The script defines the outcomes by setting its `outcome` variable to an outcome string before returning.

You include all possible `outcome` strings from the script in the **Outcome** field when configuring the node.

The authentication journey continues along the outcome path from the script.

Errors

The server-side script can log messages.

The node logs the following warning messages:

Warnings:

- `Found an action result from scripted node, but it was not an Action object`: An action in a legacy script didn't return an object with type `Action`.
- `Found an action result from scripted node, but it was not an ActionWrapper object`: An action in a next generation script didn't return an object with type `ActionWrapper`.
- `invalid script outcome <outcome>`: The <outcome> is missing in the **Outcome** field of the node configuration.
- `invalid script outcome <action-outcome> in action`: The <action-outcome> is missing in the **Outcome** field of the node configuration.
- `script outcome error`: The script set an outcome not found in the **Outcome** field of the node configuration.

Examples

You use a **Scripted Decision** node when no other available node does what you need.

In this example, the node depends on the following JavaScript **Decision node for authentication trees** script. The script gets the user's names from their profile and stores a message in a shared state property:

Next-generation

```
// Get the username from shared state data:
var username = nodeState.get('username')

// Get the given name(s) and surname(s) from the user profile:
var profile = idRepository.getIdentity(username)
var givenname = profile.getAttributeValues('givenName')
var surname = profile.getAttributeValues('sn')
if (!(givenname && surname)) {
  var error = `Failed to get names for ${username}: ${givenname} ${surname}`
  action.goTo('Failure').withErrorMessage(error);
} else {
  // Record who authenticated in the shared state data:
  var firstGivenName = givenname[0]
  var firstSurname = surname[0]
  var now = new Date().toLocaleString()
  var message = `${firstGivenName} ${firstSurname} logged in at ${now}.`
  nodeState.putShared('message', message)
  action.goTo('Success');
}
```

Legacy

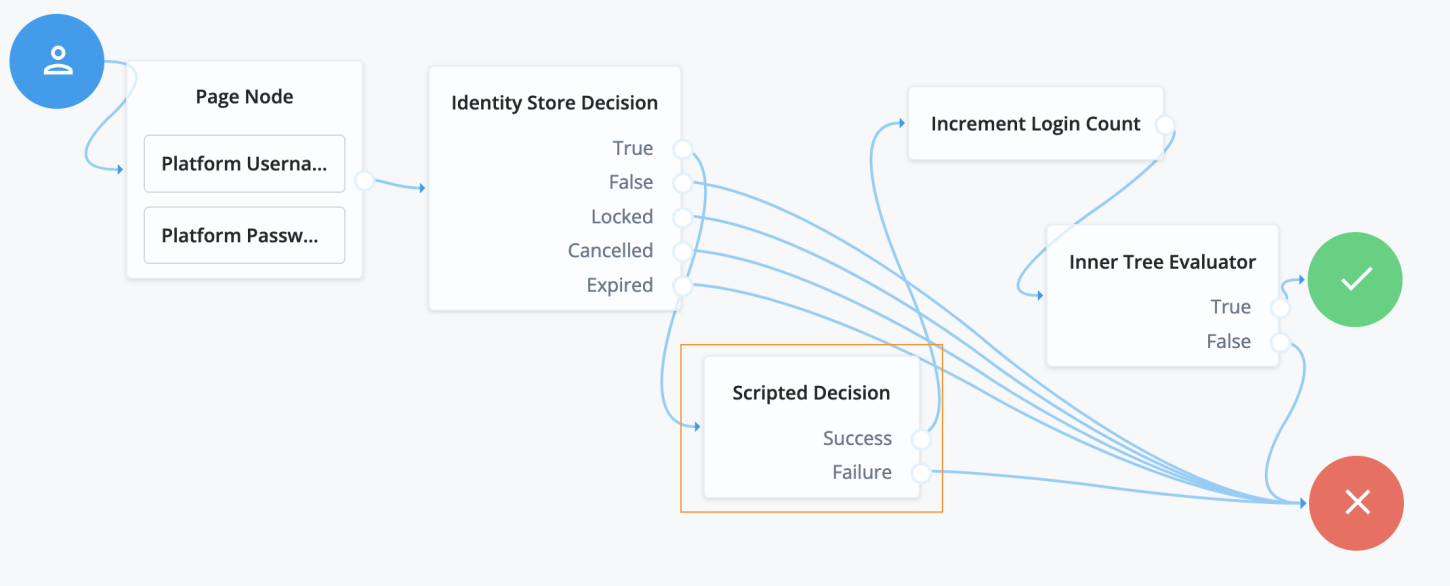
```
var goTo = org.forgerock.openam.auth.node.api.Action.goTo

// Get the username from shared state data:
var username = nodeState.get('username').asString()

// Get the given name(s) and surname(s) from the user profile:
var profile = idRepository.getIdentity(username)
var givenname = profile.getAttributeValues('givenName')
var surname = profile.getAttributeValues('sn')
if (!(givenname && surname)) {
  var error = `Failed to get names for ${username}: ${givenname} ${surname}`
  action = goTo('Failure').withErrorMessage(error).build()
} else {
  // Record who authenticated in the shared state data:
  var firstGivenName = givenname[0]
  var firstSurname = surname[0]
  var now = new Date().toLocaleString()
  var message = `${firstGivenName} ${firstSurname} logged in at ${now}.`
  nodeState.putShared('message', message)
  action = goTo('Success').build()
}
```

Notice the script sets the outcomes using the `Action.goTo(outcome)` function.

The journey is as follows:



1. The Page node prompts the user for their username and password.
2. Replace the Identity Store Decision node with a Data Store Decision node to check the username and password.
3. The **Scripted Decision** node runs the script and has the following settings:

Script	The name of the script
Outcomes	`Success`, `Failure`
Script Inputs	`username`
Script Outputs	`*`

Notice the **Outcomes** setting lists all outcome strings from the script.

4. The Increment Login Count node updates the count on successful authentication.
5. The Inner Tree Evaluator node refers to another journey to perform more steps.

   This node is optional.

If you activate debug mode for the journey and select **Enable Debug Popup**, you find the message in the debug popup window when authenticating:

```
{
  "universalId": "id=<_id>,ou=user,o=alpha,ou=services,ou=am-config",
  "transactionId": "<transaction-id>",
  "password": "<password>",
  "pageNodeCallbacks": {
    "0": 0,
    "1": 1
  },
  "realm": "/alpha",
  "message": "Babs Jensen logged in at August 16, 2023 9:55:33 AM UTC.",
  "authLevel": 0,
  "objectAttributes": {
    "password": "<password>"
  },
  "username": "id=<_id>"
}
```

Set Error Details node

PingAM

The **Set Error Details** node adds details to the JSON response when a journey ends in an error. You can configure the node properties to return an error message and extra information in the form of static `key:value` fields.

Place the **Set Error Details** node before the node that errors in the journey.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No

Product	Available?
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None. This node doesn't read shared state data.

Dependencies

None.

Configuration

Property	Usage
Error Message	The message to add to the JSON response when a journey ends in an error. Add a custom, localized message per locale: 1. Click **+**. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. For example, `Invalid outcome from script`. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done.

<table>
<tr><th>Property</th><th>Usage</th></tr>
<tr><td>Error Details</td><td>The details to add to the JSON response when a journey ends in an error:

1. Click +.
2. In the Key field, enter a name to identify the details. For example, <code>redirect_url</code>.
3. In the Value field, enter the details to return. For example, <code>https://example.com</code>.
The value can be a simple text string, a boolean value, or a JSON formatted value. The value is formatted appropriately when output in the JSON response.
For example:

<table><tr><th>Key</th><th>Value</th><th>Output</th></tr><tr><td><code>example</code></td><td><code>this is a test value</code></td><td><pre>"example": "this is a test value"</pre></td></tr><tr><td><code>boolean</code></td><td><code>true</code></td><td><pre>"boolean": true</pre></td></tr><tr><td><code>field</code></td><td><code>{ "nested": "nested value" }</code></td><td><pre>"field": {
  "nested": "nested value"
}</pre></td></tr></table>
4. Click Done.
5. Click + Add to repeat and add more messages.
6. Save your changes.</td></tr>
</table>

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

Outputs

This node doesn't change the shared state.

Outcomes

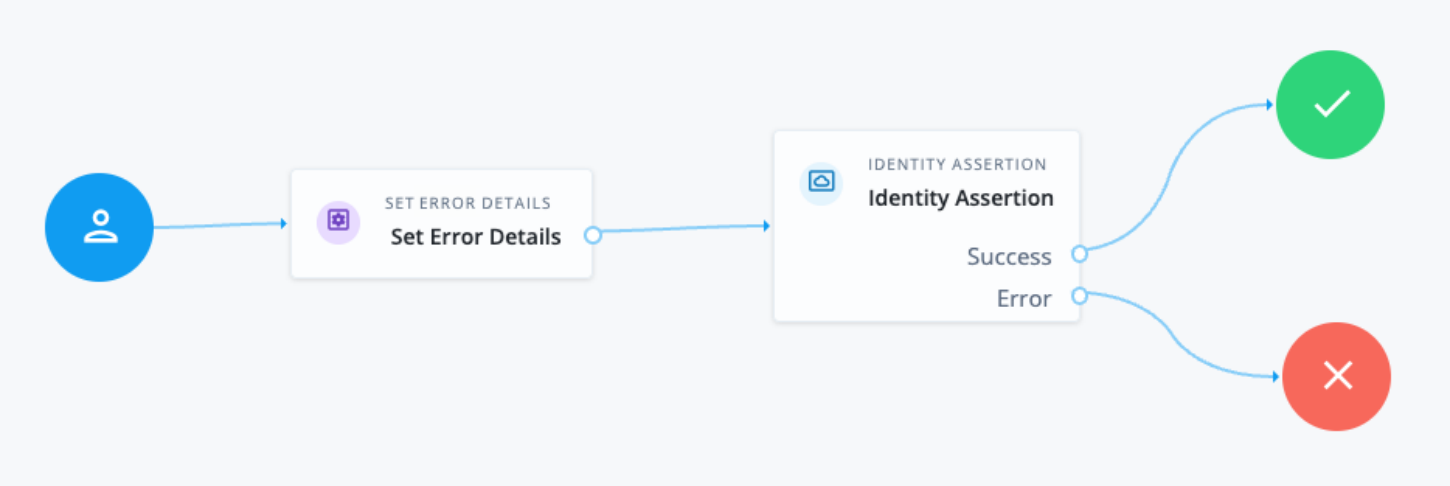
Single outcome path: when the journey ends in an error, this node adds the configured details to the JSON response.

Errors

This node doesn't log messages of its own.

Examples

This example uses the **Set Error Details** node to handle errors from the Identity Assertion node when the journey ends in an error.



- The **Set Error Details** node adds details to the JSON response when the journey ends in an error. This example uses the following configuration:

  ### *Error Message*

  - **Key**: `en-gb`
  - **Value**: `Identity assertion failure`

  ### *Error Details*

  - **Key**: `errorUrl`
  - **Value**: `https://example.com/error`

- The **Identity Assertion** node is configured as described in the documentation.

  If an error is encountered, the **Set Error Details** node displays the configured message to the user and adds both the message and the details to the JSON response.

  For example:

```
{
    "code": 401,
    "reason": "Unauthorized",
    "message": "Identity assertion failure",
    "detail": {
      "errorUrl": "https://example.com/error"
    }
}
```

Set Failure Details node

The **Set Failure Details** node adds details to the JSON response when a journey ends in failure. You can configure the node properties to return a failure message and extra information in the form of static `key:value` fields.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None. This node doesn't read shared state data.

Dependencies

None.

Configuration

Property	Usage
Failure Message	The message to add to the JSON response when authentication fails: Add a custom, localized message per locale: 1. Click +. 2. In the **Key** field, enter the locale. For example, `en-gb`.[1] 3. In the **Value** field, enter the message. For example, `Your account has been locked`. 4. Click **Done**. 5. Repeat to add more messages and save your changes when you're done.
Failure Details	The details to add to the JSON response on journey failure: 1. Click +. 2. In the **Key** field, enter a name to identify the details. For example, `Reason`. 3. In the **Value** field, enter the details to return. For example, `Exceeded max retries`. The value can be a simple text string, a boolean value, or a JSON formatted value. The value is formatted appropriately when output in the JSON response. For example: 4. Click **Done**. 5. Click + **Add** to repeat and add more messages. 6. Save your changes.

Key	Value	Output
`example`	`this is a test value`	`"example": "this is a test value"`
`boolean`	`true`	`"boolean": true`
`field`	`{ "nested": "nested value" }`	`"field": { "nested": "nested value" }`

(1) Specify a locale that Java supports, such as `en-gb`. Otherwise, the node throws a configuration exception with an `Invalid locale provided` message.

Outputs

This node doesn't change the shared state.

Outcomes

Single outcome path: when the journey ends in failure, this node adds the configured details to the JSON response.

Errors

This node doesn't log messages of its own.

Examples

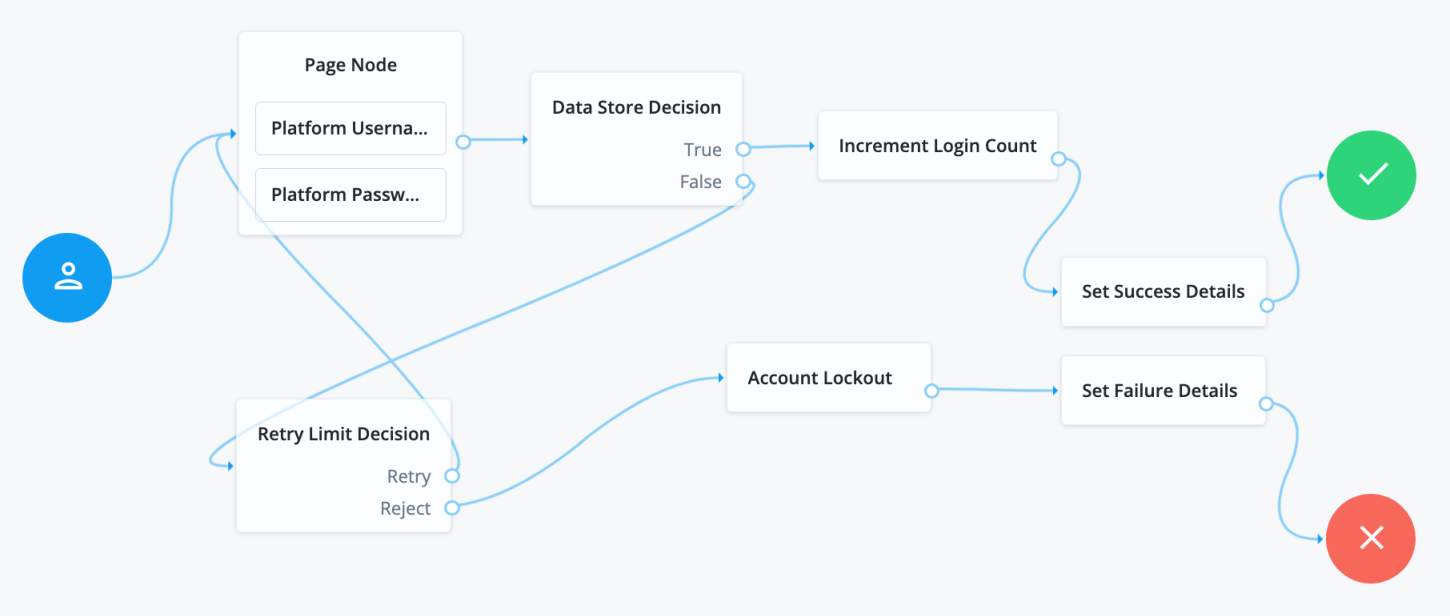
This example uses the **Set Failure Details** node and assumes the following configuration:

Failure Message

- **Key**: `en-gb`
- **Value**: `Your account is locked`

Failure Details

- **Key**: `Reason`
- **Value**: `Exceeded max retries`



- The Page node containing the Platform Username node and Platform Password node prompts for credentials.

- The Data Store Decision node validates the username-password credentials.
- If authentication is successful:
  - The Increment Login Count node updates the number of successful authentications in the user profile.
  - The Set Success Details node adds any configured details to the JSON response.
- If authentication fails:
  - The Retry Limit Decision node checks the number of failed authentications against the configured limit. If the retry limit is reached, the journey continues on the `Reject` outcome path.
  - The Account Lockout node locks the account.
  - The **Set Failure Details** node displays the configured message to the user and adds both the message and the details to the JSON response.

    For example:

```
{
  "code":401,
  "reason":"Unauthorized",
  "message":"Your account is locked",
  "detail":{
    "Reason":"Exceeded max retries"
  }
}
```

Set Session Properties node

The **Set Session Properties** node lets you change details in the resulting authenticated session. You can do one or both of the following:

Set session properties

Use this node to add `key:value` properties to the user's authenticated session on successful authentication.

> **Tip**
>
> You can access session properties using a variable in a webhook. Learn more in Configure authentication webhooks.

Update the authenticated session timeouts

PingAM Use this node to update the authenticated session timeout settings. For example, you could have different session settings for different branches within the journey based on factors such as which region the user was authenticating from or the authentication methods being used.

Consider the following when updating authenticated session timeout settings:

- If a journey has multiple nodes that set session timeouts, AM uses the settings associated with the last executed node to determine the timeouts for the resulting authenticated session.
- If an inner journey includes nodes that set session timeouts, AM uses the updated timeouts in the parent journey.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the authenticated session timeout settings from the user, journey or the Session service. Learn more in Configure authenticated session timeout settings.

Dependencies

Make sure the user can successfully authenticate and get a session.

This node is ignored unless the user gets an authenticated session.

Configuration

Property	Usage
Properties	The session properties to set. • To add a session property: 1. Click +, then + **Add** in the **Properties** modal. 2. Enter the session property name in the **Key** field and the value to set in the **Value** field. 3. Click **Done**. • To edit a property: 1. Click the **Pencil** icon (✎). 2. Update the **Key** and **Value** as when adding properties. • To remove a property, click the **Delete** icon (🗑). When finished, click **Save** to keep your settings.

Property	Usage
PingAM **Maximum Session Time**	The maximum authenticated session time in minutes. If set, this overrides the maximum authenticated session time set in the journey or the Session service. Learn more in Configure authenticated session timeout settings. **Note** If a user has session timeouts set, the user-specific settings are always used.
PingAM **Maximum Idle Time**	The maximum idle time for the authenticated session in minutes. If set, this overrides the maximum idle time set in the journey or the Session service. Learn more in Configure authenticated session timeout settings. **Note** If a user has session timeouts set, the user-specific settings are always used.

Outputs

This node sets *session* properties. It doesn't change the shared state data.

This node can't override system session properties, such as the principal or the authentication level. Use a different journey to re-authenticate the user rather than trying to change such properties with this node.

Additionally, this node updates the authenticated session timeouts if new values are provided.

Outcomes

Single outcome path.

Errors

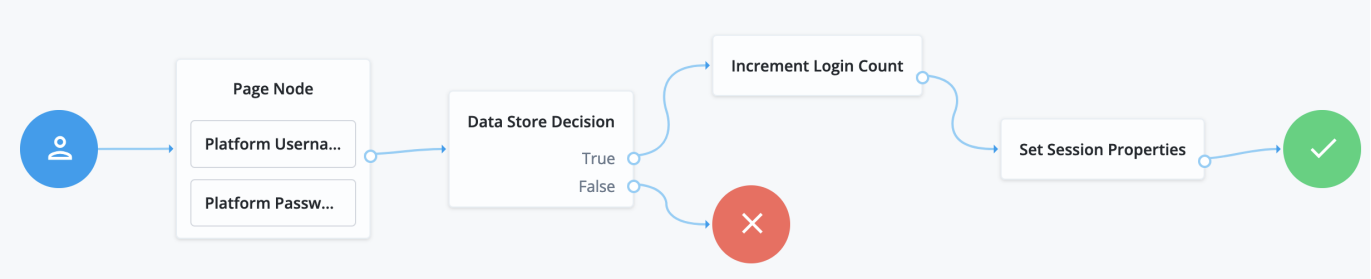
This node doesn't log messages of its own.

Examples

Example 1: Update the `successURL` session property

This example uses the **Set Session Properties** node to update the `successURL` session property.

- A first platform journey updates the session property on successful authentication:

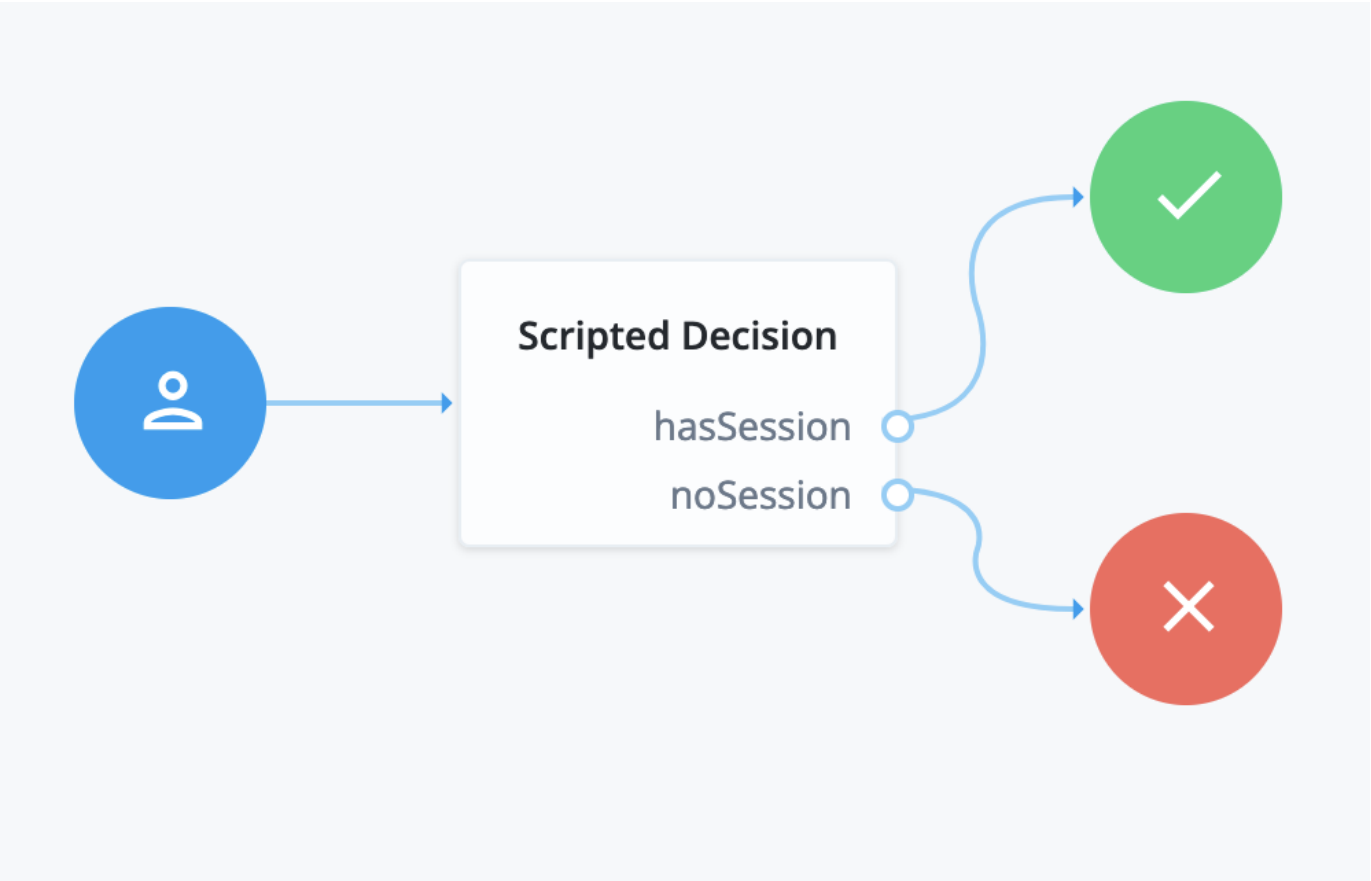


- The Page node containing the Platform Username node and Platform Password node prompts for credentials.
- The Data Store Decision node validates the username-password credentials.
- The Increment Login Count node updates the number of successful authentications in the user profile.
- The **Set Session Properties** node, sets the `successURL` session property.

  Configure the **Properties** to add a `successURL` property with the URL of your choice.

When the journey completes successfully, AM updates the `successURL` in the user's session data.

- A second journey uses a script to display the session properties after the user authenticates:



The Scripted Decision node calls the following script to inject the session properties into the shared state data so the journey can display them though a debug popup:

```
if (typeof existingSession !== 'undefined') {
  nodeState.putShared('session', existingSession)
  action.goTo('hasSession')
} else {
  nodeState.putShared('session', null)
  action.goTo('noSession')
}
```

The second journey has **Debug mode** and **Enable Debug Popup** selected.

Follow these steps to try the example:

1. Create both journeys using the journey editor.
2. Sign in through the first journey with a test user account.

   The browser shows the user profile page.
3. In the same browser window, browse to the URL for the second journey.

   The debug popup window displays the shared state data including session properties:

   ```
   {
       "transactionId": "...",
       "session": {
           "successURL": "<your-success-url>",
           "...": "..."
       },
       "realm": "/alpha",
       "authLevel": 0,
       "username": "test"
   }
   ```

   The `successURL` property is set to <your-success-url>, the one you configured as the value in **Properties** of the **Set Session Properties** node.
4. Sign out as the test user.
5. Sign in through the *default* journey as the test user.

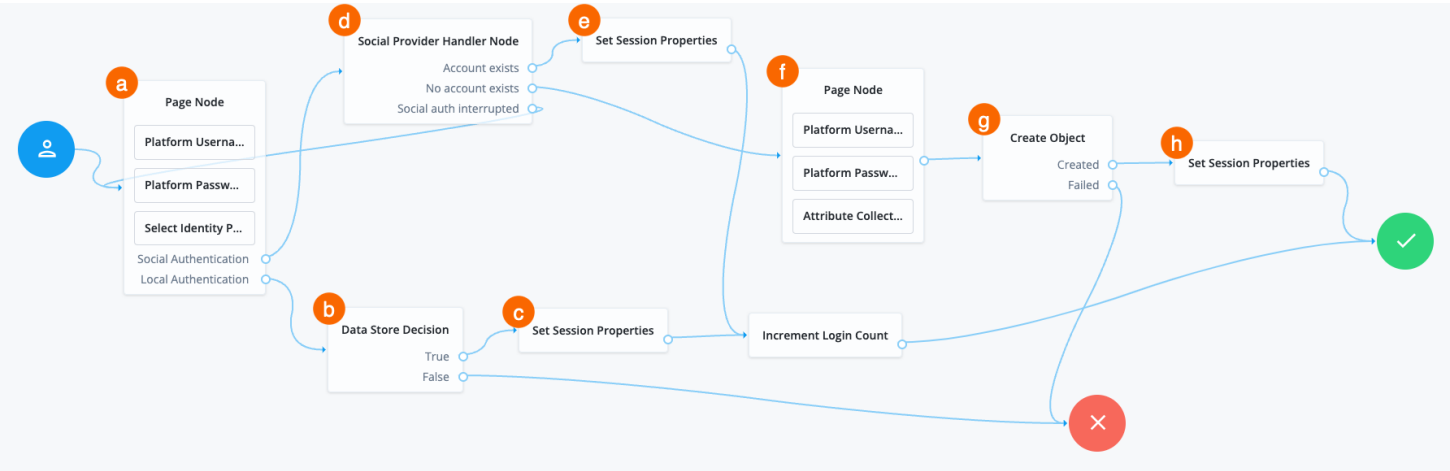
   The default journey doesn't use the **Set Session Properties** node with your configuration, so it uses the default value for the `successURL` session property.
6. In the same browser window, browse to the URL for the second journey again.

   The debug popup window displays the shared state data, including session properties with the default `successURL` value.

Example 2: Update the authenticated session timeouts

PingAM This example uses the **Set Session Properties** node to set different session timeouts depending on the authentication method used. If the user chooses to authenticate with a username and password, the resulting authenticated session will have a shorter lifetime than if they use a social provider to authenticate. For both authentication methods, the idle timeout will be lower than the default.

> **Note**
>
> Instead of setting the same maximum session idle timeout in each node, you could set it at the journey level and leave the node setting blank. They have been set in the nodes in this example for demonstration purposes.



a The Page node containing the Select Identity Provider node prompts the user to select a social identity provider or to authenticate with a username and password.

b If the user selects local authentication, the Data Store Decision node takes care of the authentication.

c The **Set Session Properties** node for local authentication updates the session timeout values with the following settings:

- **Maximum Session Time**: 60
- **Maximum Idle Time**: 20

d If the user selects social authentication, the Social Provider Handler node does the following:

- Routes the user to the selected social provider to authenticate there
- Retrieves the user's profile information and transforms it into a format that AM can use
- Assesses whether the user has an existing identity in AM
  - If the user has an existing identity, authenticates that identity
  - If the user doesn't have an identity, routes the user to another page node
  - If the user interrupts the social authentication, routes the user back to the Select Identity Provider node

e The **Set Session Properties** node for social authentication updates the session timeout values with the following settings:

- **Maximum Session Time**: 180
- **Maximum Idle Time**: 20

f The nodes on the page node request the information required to *register* a new identity.

g The Create Object node creates the new identity in AM.

h The **Set Session Properties** node for social authentication updates the session timeout values with the following settings:

- **Maximum Session Time**: 180
- **Maximum Idle Time**: 20

Set State node

The **Set State** node lets you set the values of any configured attributes in the shared state. The node removes any previous values of the specified attributes from all states (transient, secure, and shared) and resets them to the configured values in the shared state.

> **Caution**
>
> Don't use this node to add sensitive data, such as passwords, to the shared state.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads any attributes stored in the shared state by previous nodes in the journey.

Dependencies

This node has no specific dependencies.

Configuration

Property	Usage
Attributes	Add the attributes you want to set in the shared state. For each attribute: 1. Click +. 2. In the **Key** field, enter the attribute name. 3. In the **Value** field, enter the value of the attribute you want to set. 4. Click **Save** when you have finished.

Outputs

This node writes any configured attributes and their values to the shared state.

Outcomes

None

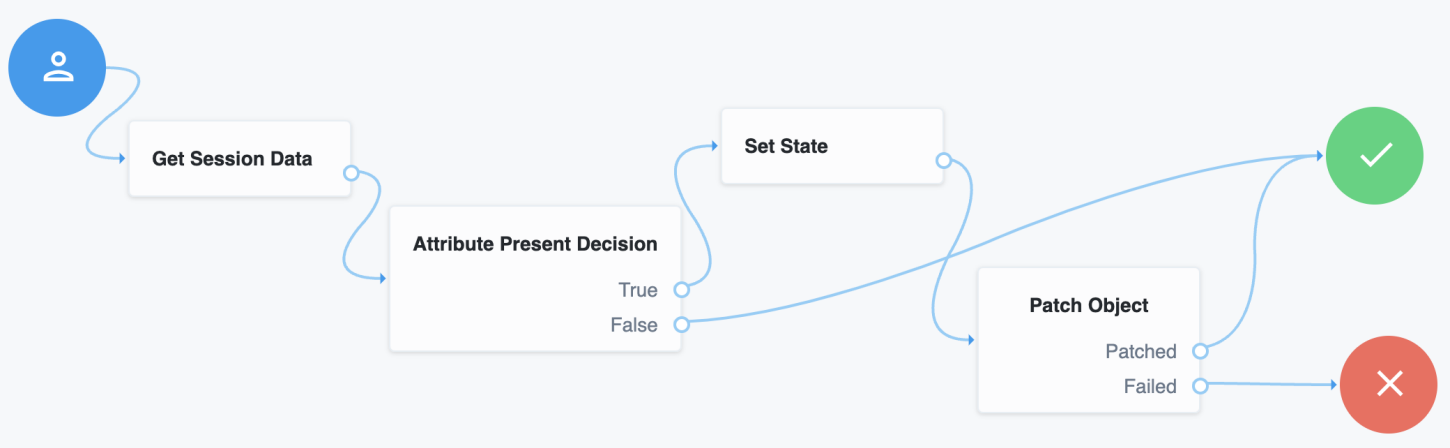
Errors

This node doesn't log any errors or warnings.

Example

The following sample journey assumes that an organization wants to overwrite the `costCenter` of specific employees when they authenticate.

- If an employee doesn't have a `costCenter` attribute in their profile, the journey proceeds without changing the user object.
- If the user does have a `costCenter` attribute, the journey uses the **Set State** node to overwrite the value of that attribute.



The user has already authenticated before beginning this journey:

- The Get Session Data node gets the `userName` from the session.
- The Attribute Present Decision node checks the user object to determine whether the user has a `costCentre` attribute.
  - If the user doesn't have a `costCentre` attribute, the journey proceeds to the success outcome.
  - If the user does have a `costCentre` attribute, the Attribute Present Decision node stores its value in the shared state.
- The **Set State** node overwrites the value of the `costCentre` attribute with the value set in the node configuration.
- The Patch Object node node updates the user object with the new `costCentre`.

- If the patch of the user object is successful, the journey proceeds to the success outcome; otherwise, the journey follows the failure outcome.

Set Success Details node

The **Set Success Details** node adds additional details to the JSON response on successful authentication. You can add either or both of the following:

- **Success details**: Lets you add static `key:value` fields to the JSON response.
- **Session properties**: Lets you add `key:value` fields to the JSON response, where `value` corresponds to the value of the specified session property.

  This lets you retrieve session properties in the journey without needing additional post-authentication processing.

> **Note**
>
> You can't override the `tokenId`, `successUrl`, and `realm` fields returned in the JSON response by default.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

None. This node doesn't read shared state data.

Dependencies

Make sure the user can successfully authenticate and get a session.

If this node is added to a no session journey or the `noSession` query parameter is used during authentication, this node has no effect.

Configuration

<table>
<tr><th>Property</th><th>Usage</th></tr>
<tr><td>Success Details</td><td>The success details to add:
• To add a static field:
1. Click + Add in the Success Details modal.
2. Enter the field name to display in the Key field and the corresponding value to display in the Value field.
The value can be a simple text string, a boolean value, or a JSON formatted value. The value is formatted appropriately when output in the JSON response.
For example:
<table><tr><th>Key</th><th>Value</th><th>Output</th></tr><tr><td><code>example</code></td><td><code>this is a test value</code></td><td><pre>"example": "this is a test value"</pre></td></tr><tr><td><code>boolean</code></td><td><code>true</code></td><td><pre>"boolean": true</pre></td></tr><tr><td><code>field</code></td><td><code>{ "nested": "nested value" }</code></td><td><pre>"field": {
  "nested": "nested value"
}</pre></td></tr></table>3. Click Done.
• To edit a field:
1. Click the Pencil icon (✎).
2. Update the Key and Value as when adding fields.
• To remove a field, click the Delete icon (🗑).

When finished, click Save to keep your settings.</td></tr>
</table>

Property	Usage
Session Properties	The session properties to add. **Note** Session property details are only added to the JSON response if the session property exists in AM and it's available in the authenticated session. You can find a list of the default session properties in Session properties. • To add a session property: 1. Click + **Add** in the **Session Properties** modal. 2. Enter the field name to display in the **Key** field and the session property name in the **Value** field. 3. Click **Done**. • To edit a property: 1. Click the **Pencil** icon (✎). 2. Update the **Key** and **Value** as when adding properties. • To remove a property, click the **Delete** icon (🗑). When finished, click **Save** to keep your settings.

Outputs

This node doesn't change the shared state.

Outcomes

Single outcome path: when the journey completes successfully, this node adds the additional configured details to the JSON response.

Errors

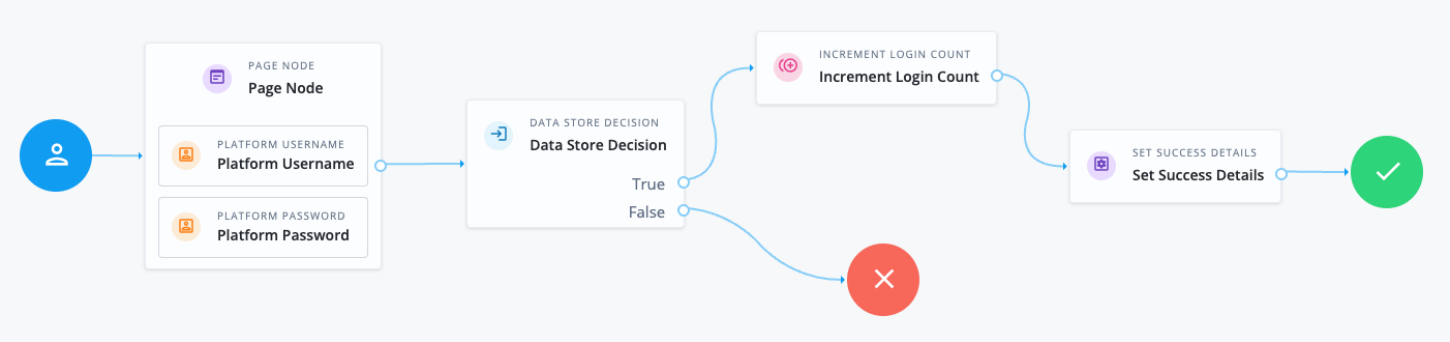
This node doesn't log messages of its own.

Examples

Example 1: Add static content and session properties

This example uses the **Set Success Details** node to add the following additional details to the JSON response:

- A static `authMethod:password` field.
- A `universalId` session property, which returns the corresponding value from the session when the user authenticates.



- The Page node containing the Platform Username node and Platform Password node prompts for credentials.
- The Data Store Decision node validates the username-password credentials.
- The Increment Login Count node updates the number of successful authentications in the user profile.
- The **Set Success Details** node adds the additional configured details to the JSON response upon successful authentication. This example uses the following configuration:

Success Details

Key: `authMethod`

Value: `password`

Session Properties

Key: `universalId`

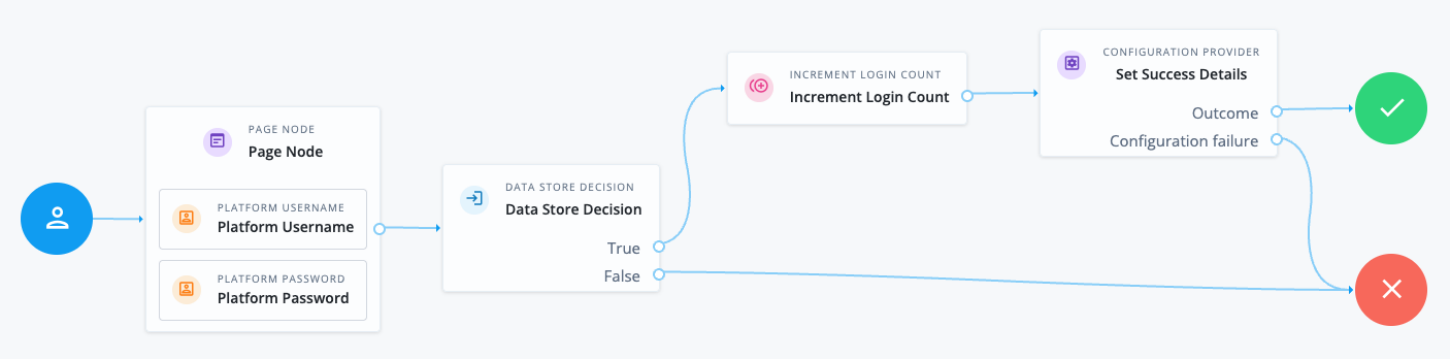
Value: `sun.am.UniversalIdentifier`

When the user authenticates successfully using this journey, the JSON response includes the additional details you configured. For example:

```
{
    "tokenId": "AQIC5wM…TU3OQ*",
    "successUrl": "/enduser/?realm=/alpha",
    "realm": "/alpha",
    "universalId": "id=bjensen,ou=user,o=alpha,ou=services,ou=am-config",
    "authMethod": "password"
}
```

Example 2: Add dynamic content

This example uses the Configuration Provider node to imitate the **Set Success Details** node. Using the **Configuration Provider** node lets you add dynamic content to the JSON response, such as an API response, in addition to static content and session properties.



Find more information in Example 2: Imitate the Set Success Details node.

State Metadata node

The **State Metadata** node returns selected attributes from the shared node state as metadata.

This node sends a `MetadataCallback` to retrieve shared state values, which it adds to the JSON response from the `/authenticate` endpoint. This example shows how a shared state attribute, `mail`, is returned:

```
{
    "callbacks": [
        {
            "type": "MetadataCallback",
            "output": [
                {
                    "name": "data",
                    "value": {
                        "mail": "bjensen@example.com"
                    }
                }
            ]
        }
    ]
}
```

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads its configured **Attributes** from the shared node state.

Dependencies

None.

Configuration

Property	Usage
Attributes	Specify one or more shared state attribute names for return. Default: none

Outputs

This node only sends the callback. It does not modify the shared node state.

Outcomes

Single outcome path.

Evaluation continues after the callback.

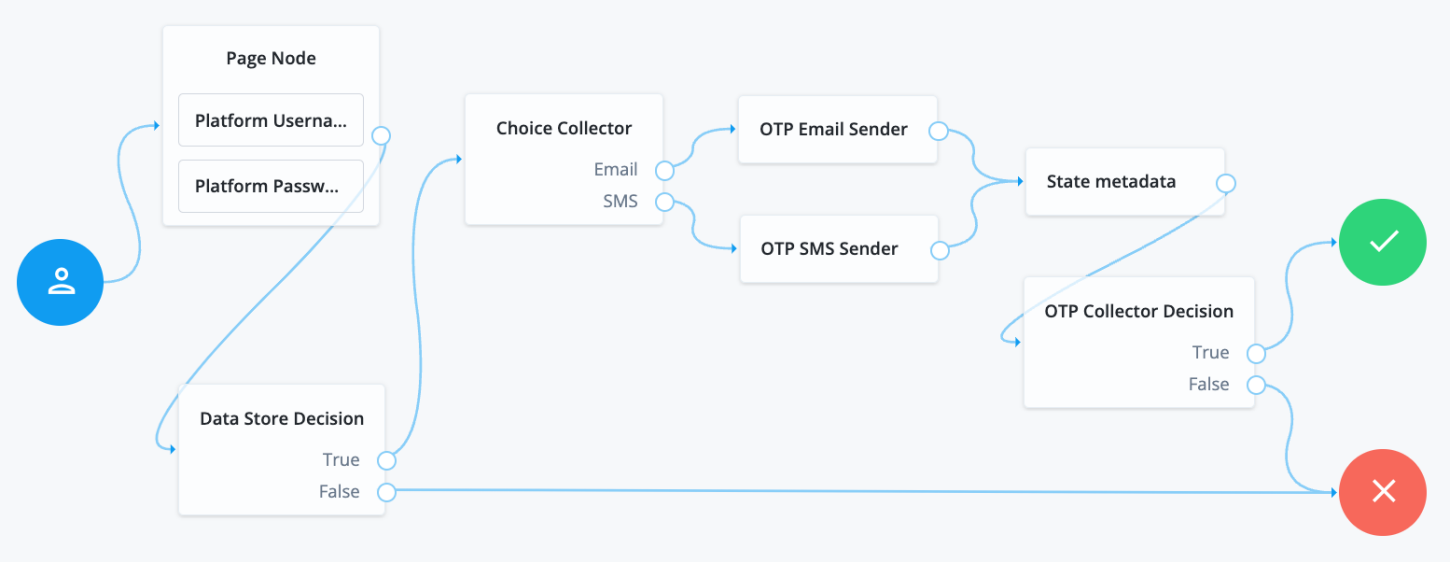
Errors

This node does not log error or warning messages of its own.

Example

Use this node to display custom information that includes user attributes without having to alter the existing flow.

For example, for OTP authentication with a choice of email or SMS, use this node to return the user's email address or phone number. You can use the attributes with an OTP Collector Decision node, and optionally, a Scripted Decision node, to customize the data for display later.



- The Page node with a Platform Username node and Attribute Collector node prompts for the credentials.
- The Data Store Decision node confirms the user's credentials.
- The Choice Collector node lets the user opt for notification through email or a text message.
- The OTP Email Sender node sends the one-time passcode (OTP) as email.
- The OTP SMS Sender node sends the OTP as a text message.
- The **State Metadata** node injects attributes for additional information.
- The OTP Collector Decision node displays the additional information when collecting the OTP to verify.

Success URL node

Sets the redirect URL when authentication succeeds.

> **Note**
>
> Specifying a success URL overrides any `goto` query string parameters.

For more information on how AM determines the redirection URL, and to configure the Validation Service to trust redirection URLs, refer to Configure success and failure redirection URLs.

> **Tip**
>
> The URL is also saved in the `nodeState` object on the `successUrl` key.
> Learn more in Customize authentication trees.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Properties

Property	Usage
Success URL *(required)*	Specify the full URL to redirect to when the authentication succeeds.

Timer Start node

Starts a named timer metric, which you can stop with a Timer Stop node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Start Time Property	Specify a property name into which to store the current time. Specify the same value in any instances of the Timer Stop node that measure the time elapsed since evaluation passed through this node.

Timer Stop node

Records the time elapsed since evaluation passed through the Timer Start node in the specified metric name.

You can find information on the `Timer` metric type in Monitoring metric types.

Note that this node does not reset the time stored in the specified **Start Time Property** property. Other Timer Stop nodes can also calculate the time elapsed since evaluation passed through the same Timer Start node.

The metric is exposed in all available interfaces, as described in Monitor AM instances.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

Single outcome path.

Properties

Property	Usage
Start Time Property	Specify the property name containing the time from which to calculate the elapsed time.
Metric Key *(required)*	Enter the name for a new metric that stores the calculated elapsed time. The name you select is used to identify the metric that exposes the data collected by this node. For example, if you enter `calculated.time`, AM exposes a new metric with this name to the Common REST, JMX, or Graphite interfaces. If you use Prometheus, the name is prefixed with `am_` and appended with `_seconds` to become `am_calculated_time_seconds`.] **Tip** Metrics collate data from multiple invocations of a journey. To record the time it takes for a particular journey to complete, use a Scripted Decision node to store the start time in shared state. Use a script at the end of the journey to capture the end time and output the calculated journey time to the authentication audit logs. Learn more in Audit information.

Update Journey Timeout node

PingAM

The **Update Journey Timeout** node updates the maximum duration of the journey session. You can either set a new timeout value to override the maximum duration or specify a timeout adjustment to modify the maximum duration.

You can use multiple instances of this node in a journey if required. For example, you could increase the maximum duration to allow the end user sufficient time to fetch a document, such as their passport. You could then increase it again to allow them to fetch a second document after they complete that step. Or you could have different timeouts for separate branches within the journey to accommodate different authentication requirements.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

This node reads the maximum duration of the journey session from the journey or the core authentication settings. Learn more in Maximum duration.

Dependencies

This node has no dependencies.

Configuration

Property	Usage
Operation	The timeout update operation. Possible values are: • `Set` : This operation overrides the maximum duration of the journey session with the new value specified. • `Modify` : This operation modifies the maximum duration of the journey session by adding or subtracting the value specified. ⚠ **Warning** Make sure you consider the impact of modifying the journey session duration in all possible scenarios. For example, if a journey loops back through this node multiple times, it could be possible to end up with an infinite length session.
Value	Enter the required value in minutes as follows: • If you're using the `Set` operation, enter a positive integer to set the new maximum journey session duration. • If you're using the `Modify` operation, enter a positive integer to increase the maximum journey session duration or a negative integer to decrease the maximum session duration by the specified value. Values up to `2147483647` are allowed.

Outputs

This node updates the maximum duration of the journey session and stores it in the shared state.

Outcomes

Single outcome path.

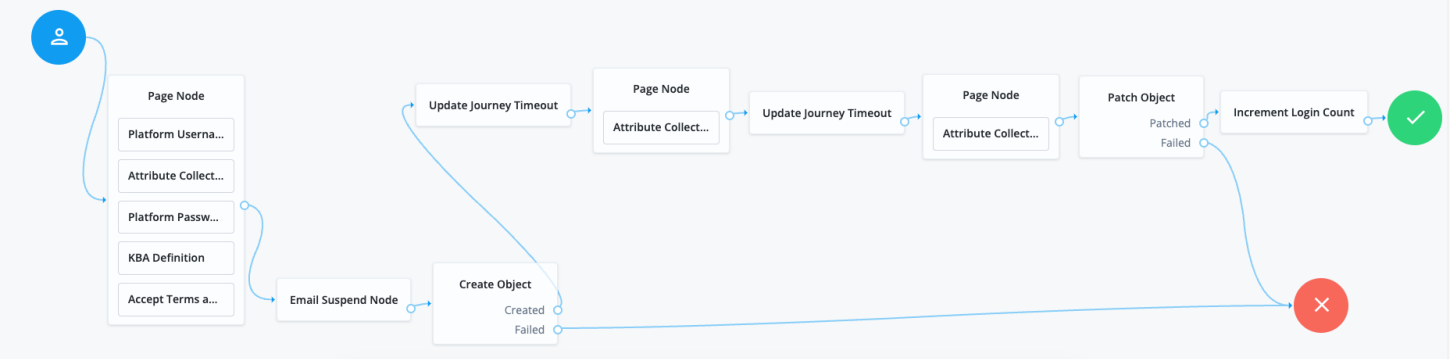
Errors

If the node can't validate the configuration successfully, it logs `An error occurred validating the update journey timeout node configuration`.

Examples

This example uses the **Update Journey Timeout** node to increase the maximum journey session duration to give the end user time to fetch their passport. It then increases it further to allow them time to fetch another document after they've entered their passport details.

This example extends the default **Registration** journey to verify the end user's email address, collect their passport details and collect details from an additional supporting document.



- The Page node prompts for the same information as the default **Registration** journey.
- The Email Suspend node sends an email to the user to verify their email address and suspends the journey.

  The journey proceeds when the user clicks the link, confirming their email address.
- The Create Object node stores the newly registered user's profile.
- The first **Update Journey Timeout** node increases the maximum session duration to `10` minutes with the following settings (this assumes the default of `5` minutes is unchanged):
  - **Operation**: `Modify`
  - **Value**: `5`
- The first Page node containing the Attribute Collector node prompts the user to input their passport details.
- The second **Update Journey Timeout** node increases the maximum session duration to `14` minutes with the following settings:
  - **Operation**: `Modify`
  - **Value**: `4`
- The second Page node containing the Attribute Collector node prompts the user to input details from their supporting document.
- The Patch Object node updates the user object with the collected details.
- The Increment Login Count node updates the count on successful authentication.

Thing nodes

Authenticate Thing node

This node authenticates a *thing*. A thing represents an IoT device, service, or the IoT Gateway.

Before you configure this node, make sure the IoT Service is configured for the realm.

> **Important**
>
> Support for this node is provided by the IoT SDK.

The node supports two methods of authentication:

1. Proof of Possession JWT

   The node collects a proof-of-possession JWT from the request and does the following:

   - Checks that the claims are valid.
   - Checks that an identity with the same ID as the name of the JWT subject exists.
   - Checks that the identity contains a confirmation key that matches the JWT `kid`.
   - Validates the JWT signature, using the confirmation key stored in the identity.

2. Client Assertion

   The node collects a JWT Bearer token from the request for authentication and validates the request according to the JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Success`
- `Failure`

- `Requires Registration`

If all checks are successful, evaluation continues through the `Success` path, and adds the username and the verified claims to the shared node state.

If the identity does not exist, or AM cannot match the identity with the confirmation key, evaluation continues through the `Requires Registration` outcome.

If any other check fails, evaluation continues through the `Failure` outcome.

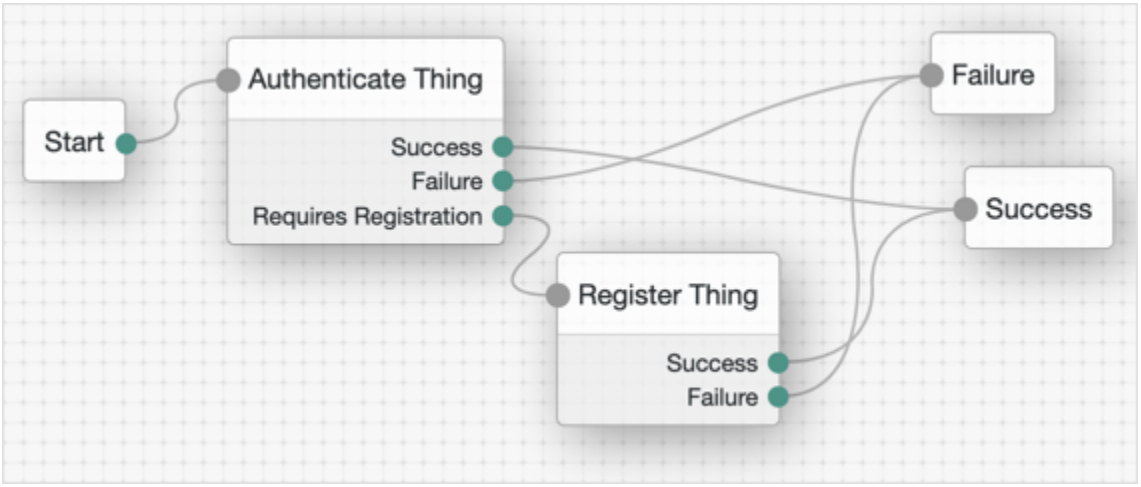
Properties

Property	Usage
JWT Authentication Method	Choose the required JWT authentication method: ***Proof of Possession*** Prove that the signer of the JWT is the owner of the key by including a challenge nonce in the JWT. Validation is according to the JWT Proof of Possession specification. ***Client Assertion*** Present a JWT Bearer token for authentication and validate the request according to the JWT Profile for OAuth 2.0 Client Authentication and Authorization Grants.
Issue Restricted Token	If this setting is enabled, the node adds a Proof of Possession restriction to the session token issued on successful authentication. Any requests accompanied by the token must be signed with the key that was used to sign the authentication JWT.
Additional Audience Values	Specify any additional audience values that will be permitted when verifying JWTs. These audience values are in addition to the AM base, issuer and token endpoint URIs for the Client Assertion authentication method or the realm path for Proof of Possession.

Examples

The following example shows how to authenticate a thing when the identity already exists in the identity store and when its profile contains a confirmation key:

The following example shows how to authenticate a thing when the identity does not exist, or when it needs to refresh its confirmation key:



Register Thing node

This node authenticates a *thing*. A thing represents an IoT device, service, or the IoT Gateway.

Before you configure this node, make sure the IoT Service is configured for the realm.

> **Important**
>
> Support for this node is provided by the IoT SDK.

The node collects a JWT from the request and validates the JWT according to the configured JWT registration method.

If the JWT is valid, the node uses the claims in the JWT to create an identity for the thing and register (or rotate) a confirmation key for it. Then, evaluation continues through the `Success` outcome.

If the node cannot validate the JWT, evaluation continues through the `Failure` outcome.

For an example on how to use this node, refer to Authenticate Thing node.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Outcomes

- `Success`

- `Failure`

Properties

Property	Usage
JWT Registration Method	Choose the method to validate the JWT: ***Proof of Possession & Certificate*** Register using a Proof of Possession JWT that includes an X.509 certificate for providing trust. A challenge nonce is presented in the callback and must be included in the signed JWT. ***Proof of Possession & Software Statement*** Register using a Proof of Possession JWT and a Software Statement for providing trust. A challenge nonce is presented in the callback and must be included in the signed Proof of Possession JWT. The claims in the Software Statement take precedence over the claims in the Proof of Possession JWT. ***Proof of Possession*** Register using a Proof of Possession JWT without using a trusted third party. A challenge nonce is presented in the callback and must be included in the signed JWT. ***Software Statement*** Register using a Software Statement, without doing proof of possession. If you select this registration method, the resultant session token will not include a proof of possession restriction. Default: Proof of Possession & Certificate
Verify Certificate Subject	If the configured JWT registration method is `Proof of Possession & Certificate`, this option verifies that the subject provided in the JWT is the same as the X.509 certificate subject CN or UID. Default: Enabled
Create Identity	Specifies whether AM will create an ID for the thing if one does not exist. Default: Disabled
Rotate Confirmation Key	Specifies whether multiple confirmation keys can be registered for a thing. Disable this setting to allow only one key per thing. Default: Disabled
Default Attribute Values	Lets you set default values for the thing's attributes, where **KEY** is the name of the attribute in the data store, and **VALUE** is the default value of the attribute.
Claim to Attribute Mapping	If **Create Identity** is enabled, this property lets you map verified claims in the JWT to attributes in the thing identity. **KEY** is the claim name and **VALUE** is the name of the attribute in the data store.

Property	Usage
Overwrite Attributes	Specifies whether the node overwrites the value for an existing profile attribute when a claim with a different value is provided in the JWT. Default: Disabled

Uncategorized nodes

Debug node

Displays debug information about the current authentication tree.

This node collects information, such as the shared node state, the identity object's `universalId`, and the transaction ID, which are useful for reference in log messages.

Availability

Product	Available?
PingOne Advanced Identity Cloud	No
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	No

Outcomes

Single outcome path.

Properties

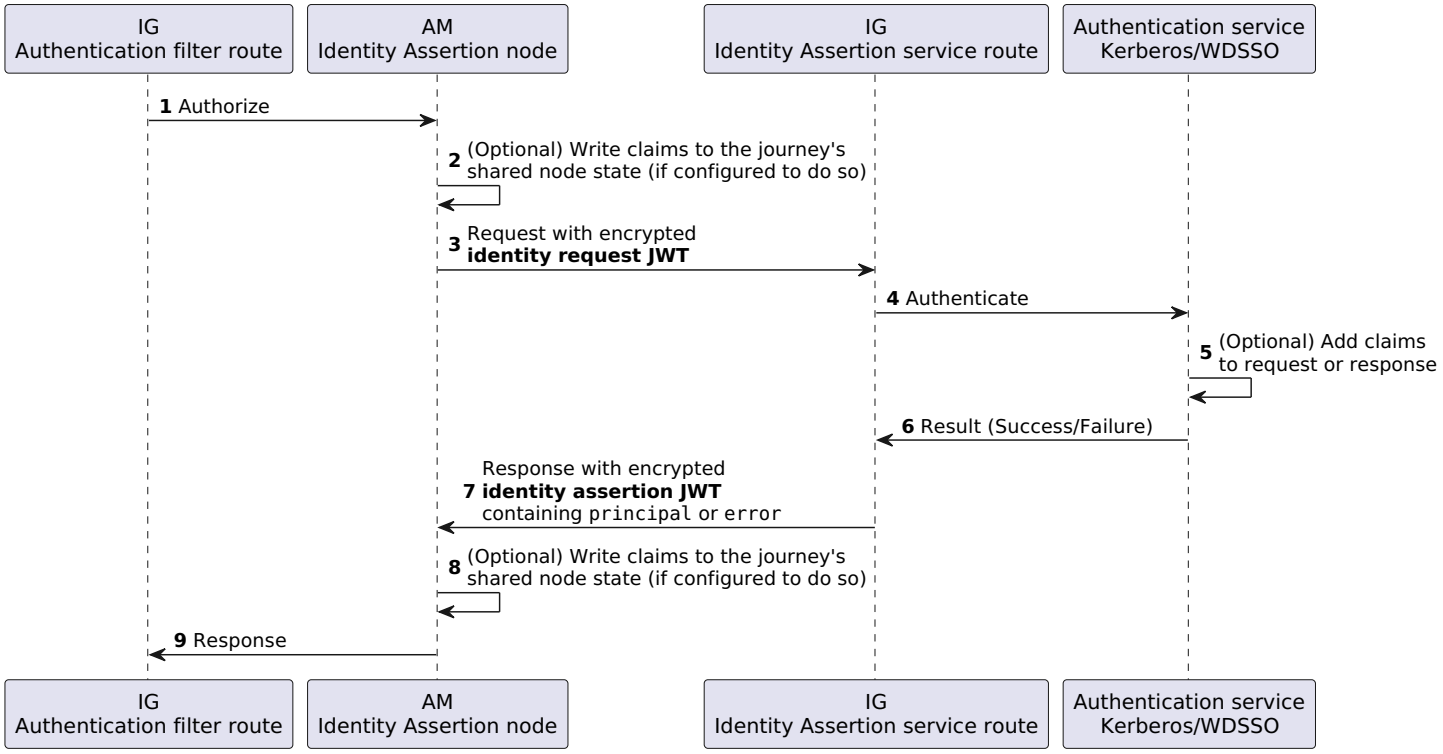
Property	Usage
Enable Debug Popup	If enabled, a popup window displays debug logs as you step through the flow in a browser.

Identity Assertion node

The **Identity Assertion** node provides a secure communication channel for authentication journeys to communicate directly with PingGateway.

The node extends AM by adding PingGateway's routing capabilities and supporting identity assertion with third-party authentication services. Authentication services include Windows Desktop SSO and Kerberos.

The following image shows the flow of an authentication request:



AM and PingGateway share a symmetric key for encryption and decryption at both ends of the flow.

Availability

Product	Available?
PingOne Advanced Identity Cloud	Yes
PingAM (self-managed)	Yes
Ping Identity Platform (self-managed)	Yes

Inputs

All shared node state properties listed in `Mapping to server claims` are valid optional inputs to this node.

To allow the node to validate that an Identity Assertion JWT is the result of an identity request, the nonce must be present in the shared node state as `identityAssertionNonce`. This isn't required for the initiating authentication request.

Dependencies

The Identity Assertion node relies on the following prerequisites:

- An Identity Assertion service must be configured globally or in the same realm, with at least one server configuration that can be selected for use with the Identity Assertion node.
- The Identity Assertion service server must have a valid shared secret encryption key configured in a secret store.

- The Identity Assertion server must be deployed, running, and accessible to the Identity Assertion node.

  It must also be configured with the shared secret encryption key.

  PingGateway can fulfil the role of the Identity Assertion server.

To use the Identity Assertion node in your AM environment, you must complete the following steps, as described in detail in the worked Example :

- Create and import a secret encryption key
- Configure the Identity Assertion service
- Map the secret label to the encryption key
- Configure PingGateway as an Identity Assertion Server

Configuration

The configurable properties for this node are:

Property	Usage
Node name	The name given to this node in the Journey. Default: `Identity Assertion`.
Identity Assertion server ID	The ID of the Identity Assertion server that handles assertion requests. The ID is composed of the server's ID and realm (if realm-scoped).
Mapping to server claims (optional)	Mapping of: • Key: Shared node state key • Value: Identity request JWT claim Required only if the server requires additional data. When a shared node state attribute has a value for a mapped key, the value is added to the identity request JWT claims according to the corresponding claim.
Mapping from server result (optional)	Mapping of: • Key: Identity Assertion JWT claim • Value: Shared node state key Required only if the server requires additional data. Default: the JWT `principal` claim is mapped to the shared node state `username` attribute. When an Identity Assertion JWT claim has a value for a mapped claim, the value is added to the shared node state according to the corresponding shared node state key.

Outputs

Any data mapped from the claims returned by the Identity Assertion server stored in the shared node state of the journey.

Successful Identity Assertion

The configuration `Mapping from server result (optional)` determines the shared node state property to set for the mandatory claim `principal`. The value of the shared node state property is set with the value of the `principal` claim.

For example, if `principal` is mapped to `usernameReceived`, the attribute `usernameReceived` is set in the shared node state. By default, `principal` is mapped to `username`.

Other values mapped in `Mapping from server result (optional)` are set in the shared node state only if the claim exists in the resulting Identity Assertion JWT.

Failed Identity Assertion

The shared node state property `error` is set with the value of the `error` claim in the resulting Identity Assertion JWT.

Outcomes

Success

The Identity Assertion server indicates that authentication was successful. It provides the authenticated `principal`.

`Error`

The Identity Assertion server indicates that authentication failed. It provides information about the error.

Troubleshooting

If the node logs an error, review the log to find the reason for the error.

Example

The following worked example describes how to use the Identity Assertion node to authenticate internal access.

Create and import a secret encryption key

Identity Assertion in AM and PingGateway uses a single secret for all encryption and decryption:

- AM uses the key to encrypt the identity request JWT; PingGateway uses it to decrypt the identity request JWT.
- PingGateway uses the key to encrypt the resulting Identity Assertion JWT; AM uses it to decrypt the Identity Assertion JWT.

Provide the encryption key in PEM format, as a JWK, or in a keystore. For example, create and import an AES PEM key into a secret store.

Configure the Identity Assertion service

Enable the service

1. In the AM admin UI, go to **Configure > Global Services > Identity Assertion Service**. Alternatively, to add the service for a realm, go to **Realms** > ***Realm name*** > **Services**, click **+Add a Service** and select **Identity Assertion Service** to create.
2. In the Identity Assertion Service page, ensure **Enable** is selected.

Configure a server

1. In the `Secondary Configurations` tab, click **+Add a Secondary Configuration** and enter the following information:
   - **Name**: A unique name for the Identity Assertion server. For example, use `IG01`.
   - **Identity Assertion server URL**: The Identity Assertion server URL. For example, enter `https://ig.ext.com:8443`.
   - **Shared Encryption Secret**: AM uses this identifier to create a secret label for encrypting the identity request JWT and resulting Identity Assertion JWT.

     The secret label takes the form `am.services.identityassertion.service.identifier.shared.secret` where identifier is the value of **Shared Encryption Secret**. For example, use identifier `idassert` to create a label called `am.services.identityassertion.service.idassert.shared.secret`.
2. Click **Create**.
3. Keep the default values for **JWT TTL (seconds)** and **Skew Allowance (seconds)** and save your changes.

Learn more about the service configuration in Identity Assertion service.

Map the secret label to the encryption key

To map the encryption key in the secret store, follow the steps in Map and rotate secrets using these values:

- **Secret Label**: Find the secret label to map by entering the value of the **Shared Encryption Secret** you used in the service configuration.

  For example, enter `idassert` to find `am.services.identityassertion.service.idassert.shared.secret`.

  You can find and configure the secret only after you have entered it in the **Shared Encryption Secret**.
- **Aliases**: Enter the alias to the encryption key secret you created earlier.

Configure PingGateway as an Identity Assertion Server

Configure PingGateway to:

- Validate the identity request JWT.
- Create an encrypted Identity Assertion JWT to send back to AM.

The PingGateway configuration includes two routes:

Authentication filter route

Directs unauthenticated requests to an authentication journey in AM.

For testing purposes, configure AM and PingGateway as described in Cross-domain single sign-on. The setup configures a demo user and validation service required for the example.

In `cdsso.json`, the CrossDomainSingleSignOnFilter uses AM's default authentication service. Add the property `authenticationService` to the CrossDomainSingleSignOnFilter to direct requests to the journey.

The following example redirects unauthenticated requests to a journey called `IgCallout`.

```
{
  "name": "CrossDomainSingleSignOnFilter-1",
  "type": "CrossDomainSingleSignOnFilter",
  "config": {
    ...
    "authenticationService" : "IgCallout",
    ...
  }
```

Identity Assertion service route

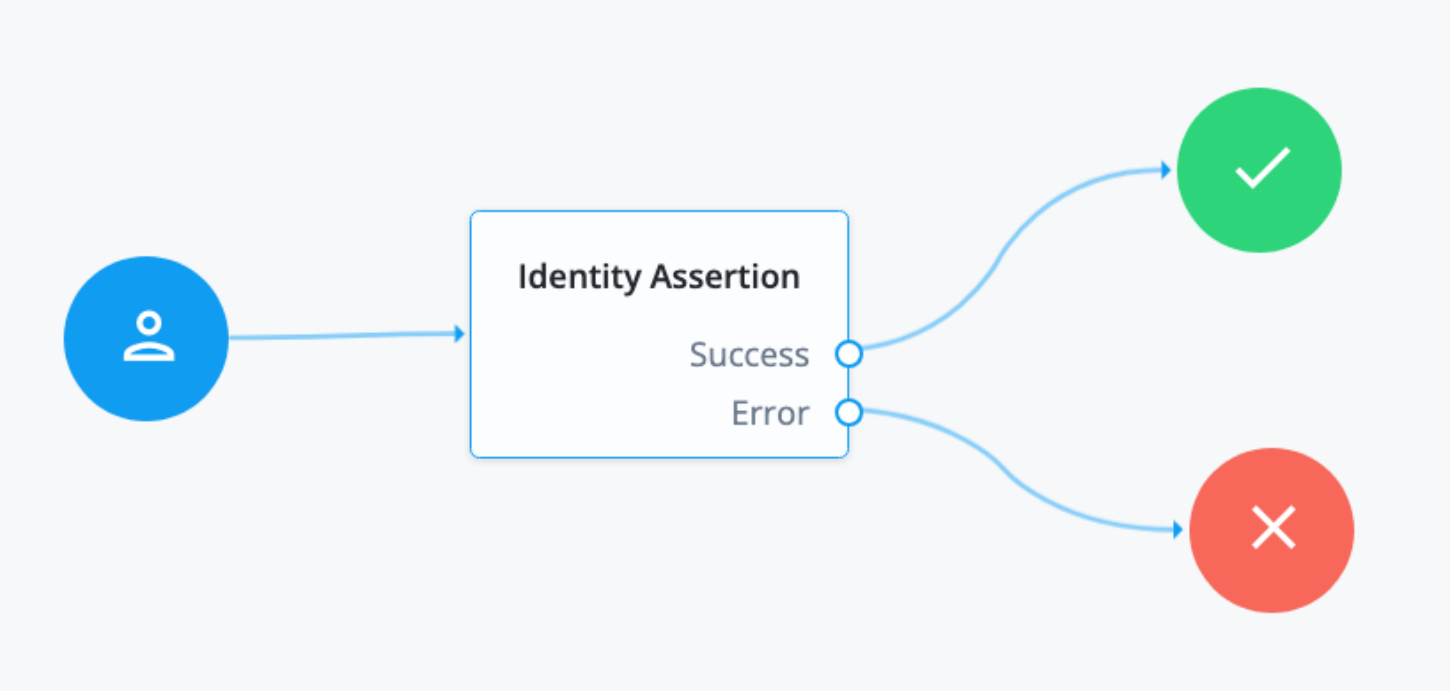
Directs unauthenticated requests to a local authentication service such as Kerberos or Windows Desktop SSO.

Consider the example in PingGateway's Example Identity Assertion service route for Identity Assertion node. The route contains an `IdentityAssertionHandler` that calls a `ScriptableIdentityAssertionPlugin` to manage local authentication.

The route requires the following:

- The key and AM setup described in this worked example.
- That the `IdentityAssertionHandler`'s `peerIdentifier` property refers to the host:port part of the deployment URL.
- That the `IdentityAssertionHandler`'s `condition` refers to the same path as the `Route` configured in the node. In this example, it refers to `/idassert`.

Configure the example authentication journey



Configure the Identity Assertion node as follows:

- **Identity Assertion server ID**: Select the ID and realm configured for the PingGateway server that supports Identity Assertion. For example, enter `IG01 [/alpha]`, where `IG01` is the name of the server created in the Configure the Identity Assertion service.
- **Route**: Enter the value of the `condition` property in the PingGateway route that will handle Identity Assertion requests. For example, enter `/idassert`, as used for the example route in Configure PingGateway as an Identity Assertion Server.

  When a request matches the path `/idassert`, the journey accesses the PingGateway route in PingGateway's Example Identity Assertion service route for IdentityAssertionNode.