Getting Started Guide

Configure ForgeRock with LexisNexis ThreatMetrix Nodes Guide for ForgeRock Identity Cloud

Version 1.0

May 2023

LexisNexis® RISK SOLUTIONS

Table of Contents

SCOPE 3

Document Organization 3
Intended Audience 3

LEXISNEXIS THREATMETRIX NODES 4

ThreatMetrix Profiler Node 4
ThreatMetrix Query Node 4
ThreatMetrix Review Status Node 5
ThreatMetrix Reason Code Node 5
ThreatMetrix Update Review Node 5

LEXISNEXIS THREATMETRIX PORTAL 7

Retrieve OrgID and API Key 7
ThreatMetrix Policy 8

FORGEROCK JOURNEY CONFIGURATION 10

Journey: Login-ThreatMetrix 10
Journey: StepUp-OTP 16

SCOPE

This document contains the detailed steps and supporting information required to install and configure the ForgeRock Identity Cloud with LexisNexis ThreatMetrix Authentication Nodes. This guide is quick start guide to configure the Identity Cloud with LexisNexis ThreatMetrix for a authentication/login use case combined with risk assessment to detect suspicious activity associated to the login event.

The following are architecture assumptions and limitations:

- ForgeRock Identity Cloud tenant is configured
- Default configuration for ForgeRock Identity Cloud with respect to Identity Store where the Alpha realm will be utilized for the test user
- A test account has been configured via Identities that includes first name, last name, email address, and login username

Document Organization

This document is divided into four sections as follows:

- **Scope.** Defines the purpose of this document.
- **LexisNexis ThreatMetrix Nodes**. Provides on overview of the nodes available for ForgeRock journeys.
- **LexisNexis ThreatMetrix Portal.** Provides detailed information regarding the configuration of ThreatMetrix to include configuration of a simple policy and how to access configuration parameters required for the ForgeRock journey.
- **ForgeRock Journey Configuration.** Provides detailed steps to configure a ForgeRock journey with LexisNexis ThreatMetrix for a authentication/login use case combined with risk assessment to detect suspicious activity associated to the login event.

Intended Audience

Table 1 contains a list of the different readers to whom this documentation is directed and how they will use this document.

Table 1: Intended Audience and Reading Suggestions

Reader Type	Use of this document
Developers	This guide is intended for software developers to be able to install and configure ForgeRock for testing and integration.
Administrators	This guide is also intended for administrator to be able to install and configure ForgeRock for testing and integration.

LEXISNEXIS THREATMETRIX NODES

The LexisNexis ThreatMetrix Authentication Nodes are available in the Marketplace to be included within any new or existing Journey configurations. To include a LexisNexis ThreatMetrix node in a journey, enter ThreatMextrix into the Filter nodes to get a listing of available capabilities. For risk assessment, the following nodes are available:

- ThreatMetrix Profiler
- ThreatMetrix Query
- ThreatMetrix Review Status
- ThreatMetrix Reason Code
- ThreatMetrix Update Status

ThreatMetrix Profiler Node

This node will integrate the ThreatMetrix device intelligence and fingerprinting JavaScript Tags onto a ForgeRock Page Node. This is typically placed onto a Login Page, Payment Page, or Account Creation page as part of a risk assessment use case.

The ThreatMetrix Profiler node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated with ThreatMetrix generated for your organization.
- **Page ID** - The Page ID is an identifier to be used if you place the ThreatMetrix tag on multiple pages.
- **Profiler URI** - ThreatMetrix Profiler URI. This can be the Basic Profiling URL or the Enhanced Profiling vis Hosted SSL URL. The default configuration is the Basic Profiling URL.
- **Use Client Generated Session IDs** - If ThreatMetrix JavaScript Tags have been separately integrated onto an application webpage external to the ForgeRock platform, activate this property toggle. When activated, this node will fetch the SessionID from the application via a ForgeRock Read-Only callback, mainly a `HiddenValueCallback`.

ThreatMetrix Query Node

This node makes a request LexisNexis ThreatMetrix API Request to either: (i) Session Query API, or (ii) Attribute Query API. The main difference is that Session Query API requires the TMX Profiler Node to perform device intelligence, whereas the Attribute Query does not involve device intelligence. Attribute query is helpful in situations where a LexisNexis product such as Emailage or InstantID can be invoked for a risk assessment without any device intelligence.

The ThreatMetrix Query Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated with ThreatMetrix generated for your organization.
- **API Key** - This is the unique API key generated by ThreatMetrix associated to the Org ID.
- **Service Type** - Defines the API Response output fields returned from the API Request. The default configuration is session-policy. See the ThreatMetrix Portal KB for a full list of service types.
- **Event Type** - Specifies the type of transaction or event. The default configuration is login. See the ThreatMetrix Portal KB for a full list of event types.
- **Policy** - The policy to be used for the query.
- **Unknown Session Action** - If an "unknown session" is encountered at runtime, this allows the system administrator to define the behavior in the unlikely event this occurs at runtime. Unknown sessions occur for a variety of reasons where the device profiling has failed.

- **Query Type** - Defines the query type to send to ThreatMetrix. Session Query requires device profile information and Attribute Query does not require device profile information.
- **Session Query URI** - ThreatMetrix Session Query URI. This is used when the **Query Type** is set to Session Query, otherwise ignored.
- **Attribute Query URI** - ThreatMetrix Attribute Query URI. This is used when the **Query Type** is set to Attribute Query, otherwise ignored.
- **Add Shared State Variables To Request** - If you'd like to add additional parameters to the ThreatMetrix API Request, enable this option. In general, it is preferred to add as much data as possible to the API Requests as this will improve the fidelity of the risk assessment.
- **Session Query Parameters** - This is a list of ThreatMetrix attribute "key" to ForgeRock "value" attributes. The ForgeRock values are read from the authenticated user identity store.

ThreatMetrix Review Status Node

This node analyzes the response from the ThreatMetrix Query Node and routes based on the API Response `review_status`. The possible outcomes to route are `Pass`, `Challenge`, `Review` or `Reject` node outcomes. If an unknown session occurred as a result of profiling and the ThreatMetrix query reported unknown session condition, the ThreatMetrix Review Status Node will follow the configured Unknown Session Action.

ThreatMetrix Reason Code Node

This node analyzes the response from the ThreatMetrix Query Node and routes based on the API Response `reason_code`. The reason codes are required to be configured so that appropriate outcome routing can occur. The reason codes correspond to the ThreatMetrix Portal policy configuration for possible outcomes. Reason codes are generally utilized when the 4 default outcomes for review status are not sufficient for branching in the ForegeRock authentication tree.

The outcome for Unknown Session Action does need to be configured in the list of outcomes, otherwise the default `Error` outcome will be utilized.

The ThreatMetrix Reason Code Node has the following configuration parameters:

- **Reason Code Outcomes** - A list of Reason Codes that to check from a Query API Response. When a Reason Code is added to this list, a new outcome will be presented on the node. The node will iterate through the configured Reason Code list until a Reason code match is found and will return that outcome. Otherwise, the None Triggered outcome will be returned. Reason Code outcomes are case sensitive and must match the ThreatMetrix Portal policy.

ThreatMetrix Update Review Node

The ThreatMetrix Update Node provides retrospective trusth data to ThreatMetrix for an event. The typical ForgeRock Authentication Tree will perform a ThreatMetrix Query and if step-up authentication is involved, the ThreatMetrix Update Node is integrated to provide additional details on the event. Truth data is incredibly beneficial for tuning of the policy and overall fraud detection.

The ThreatMetrix Update Review Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated with ThreatMetrix generated for your organization.
- **API Key** - This is the unique API key generated by ThreatMetrix associated to the Org ID.
- **Update URI** - ThreatMetrix Update URI.
- **Event Tag** - This represents the event disposition and outcome of the ThreatMetrix Query. Generally, the `challenge_init` is configured prior to sending a Step-Up authentication request in the event the transaction is abandoned. Following a step-up authentication, either `challenge_pass` or `challenge_fail` is sent to the ThreatMetrix platform.
- **Step-Up Method** - This is the authentication challenge method used within the ForgeRock authentication tree to report retrospective truth data for the overall transaction.
- **Notes** - An optional notes parameter that allows you to append any notes such as why the review status is being updated.

LEXISNEXIS THREATMETRIX PORTAL

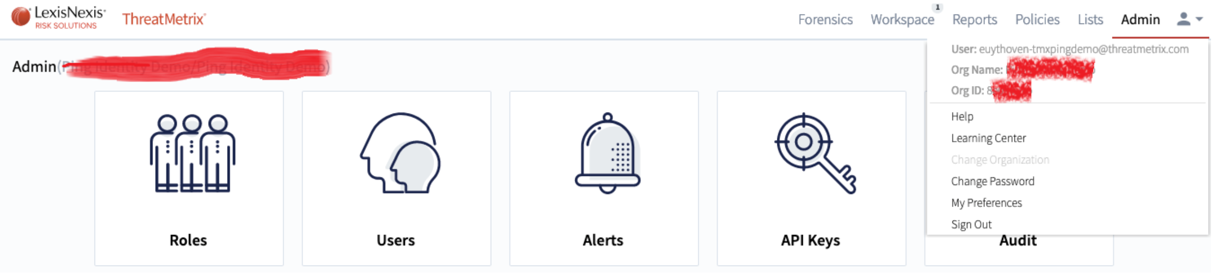
This section defines the high-level LexisNexis ThreatMetrix configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- Organization ID and API Key for the REST API interfaces. This information is needed by the ThreatMetrix Authentication Nodes and will be entered as part of configuration.
- ThreatMetrix Policy. The configured policy within ThreatMetrix provides real-time contextual risk assessment. For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the “default” policy will be configured to detect variations in the user browser agent that is used for testing, mainly Chrome, Firefox, Safari, Microsoft Edge and Internet Explorer.

Retrieve OrgID and API Key

To retrieve the ThreatMetrix values for Organization ID and API Key, perform the following steps.

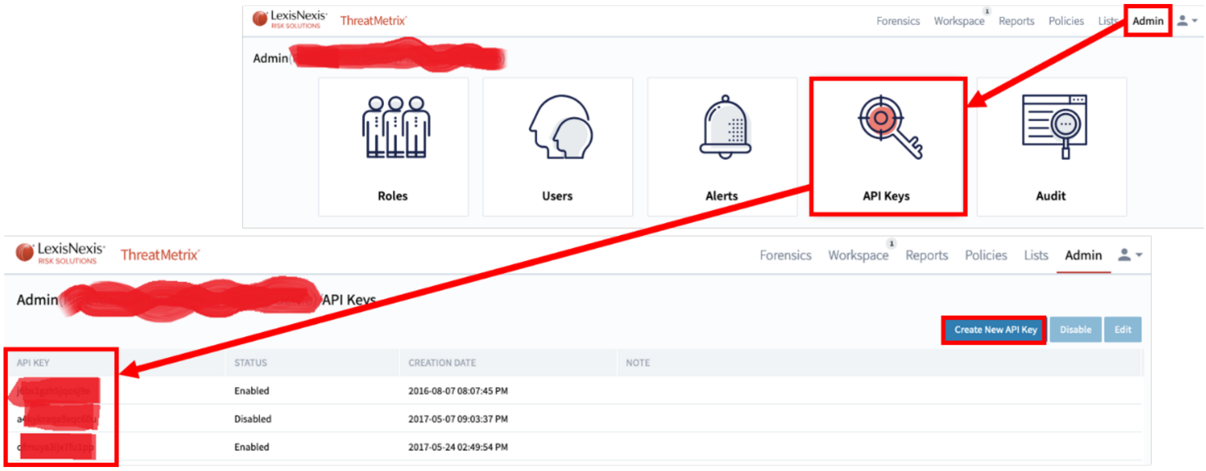
1. Access **ThreatMetrix Portal** over the internet by logging into your administrative account with credentials provided by ThreatMetrix.
2. From the **ThreatMetrix Portal** home page, select the user information dropdown that will display username, OrgName and OrgID. This will be the OrgID to enter into the configuration of the LexisNexis ThreatMetrix Authentication Nodes.



Admin [redacted]

User: euythoven-tmxpingdemo@threatmetrix.com
Org Name: [redacted]
Org ID: [redacted]

3. Within the **ThreatMetrix Portal** home page, select **Admin** followed by selecting the **API Keys** tile. Retrieve the value for API Key. In the event no API Key is listed, select the **Create New API Key** button to generate a new key. This will be the API Key to enter into the configuration of the LexisNexis ThreatMetrix Authentication Nodes. The API Key is to be protected. Do not email or keep this value in cleartext on any computer system.



Admin [redacted]

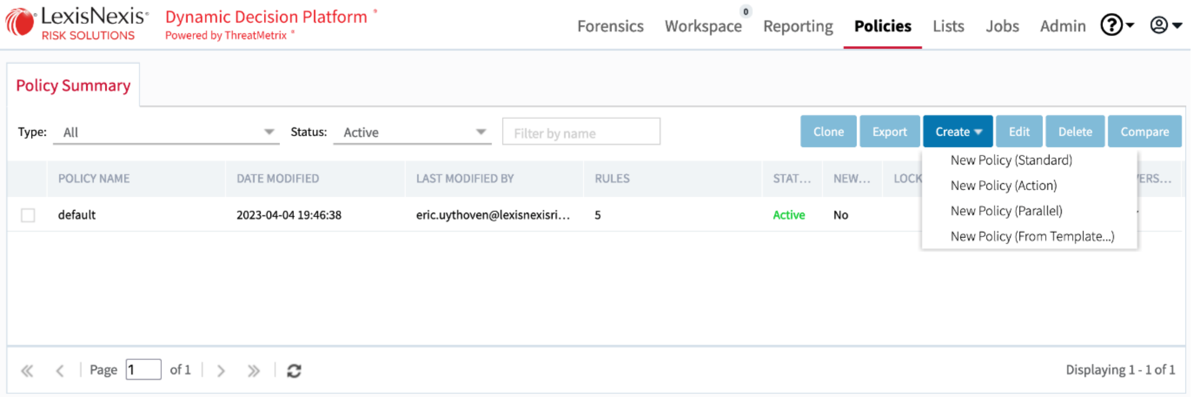
Admin [redacted] API Keys

API KEY	STATUS	CREATION DATE	NOTE
[redacted]	Enabled	2016-08-07 08:07:45 PM	
[redacted]	Disabled	2017-05-07 09:03:37 PM	
[redacted]	Enabled	2017-05-24 02:49:54 PM	

ThreatMetrix Policy

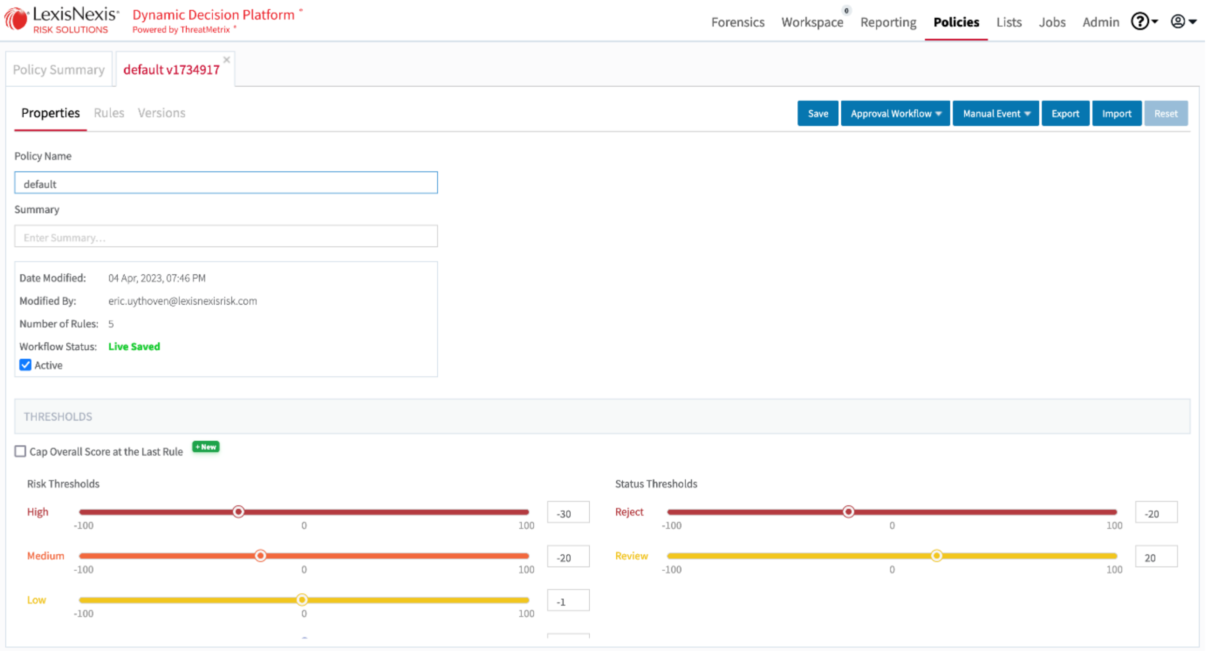
For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the "default" policy will be configured to detect variations in the user browser agent that is used for testing, mainly Chrome, Firefox, Safari, Microsoft Edge and Internet Explorer. Perform the following steps.

1. Access **ThreatMetrix Portal** over the internet by logging into your administrative account with credentials provided by ThreatMetrix.
2. From the **ThreatMetrix Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies that can be configured within the LexisNexis ThreatMetrix Query Node. If a new policy is desired to be created, the instructions here assume the name is **default**. The first step is to select the **Create** dropdown menu followed by **New Policy (Standard)**.



POLICY NAME	DATE MODIFIED	LAST MODIFIED BY	RULES	STAT...	NEW...	LOCK	ERS...
default	2023-04-04 19:46:38	eric.uythoven@lexisnexisri...	5	Active	No		

3. On the Policy Summary, the **Properties** interface tab will be displayed. Enter Policy Name = default, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



Policy Name: default

Summary: Enter Summary...

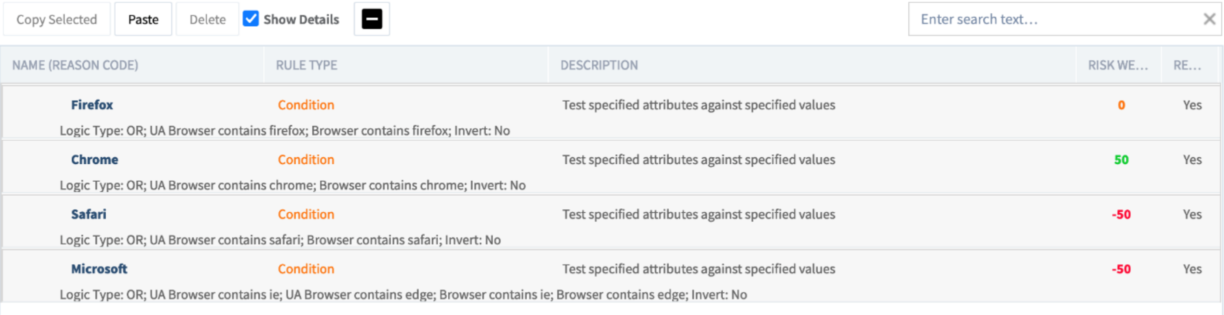
Date Modified: 04 Apr, 2023, 07:46 PM
Modified By: eric.uythoven@lexisnexisrisk.com
Number of Rules: 5
Workflow Status: Live Saved
☑ Active

□ Cap Overall Score at the Last Rule

Risk Thresholds: High -30, Medium -20, Low -1

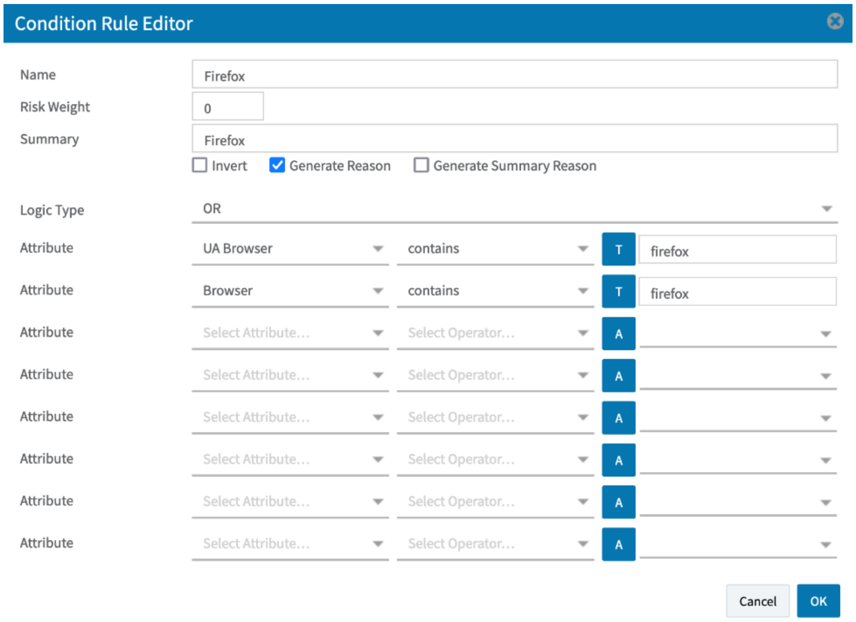
Status Thresholds: Reject -20, Review 20

4. To create the policy rules, select the **Rules** interface tab. The default policy will be a series of **Condition** rules to detect the user browser agent and fulfill the risk weights as follows.



NAME (REASON CODE)	RULE TYPE	DESCRIPTION	RISK WE...	RE...
Firefox	Condition	Test specified attributes against specified values	0	Yes
Logic Type: OR; UA Browser contains firefox; Browser contains firefox; Invert: No				
Chrome	Condition	Test specified attributes against specified values	50	Yes
Logic Type: OR; UA Browser contains chrome; Browser contains chrome; Invert: No				
Safari	Condition	Test specified attributes against specified values	-50	Yes
Logic Type: OR; UA Browser contains safari; Browser contains safari; Invert: No				
Microsoft	Condition	Test specified attributes against specified values	-50	Yes
Logic Type: OR; UA Browser contains ie; UA Browser contains edge; Browser contains ie; Browser contains edge; Invert: No				

5. Each individual rule can follow the template shown here.



Condition Rule Editor

Name: Firefox
Risk Weight: 0
Summary: Firefox
□ Invert ☑ Generate Reason □ Generate Summary Reason

Logic Type: OR
Attribute: UA Browser | contains | T | firefox
Attribute: Browser | contains | T | firefox
Attribute: Select Attribute... | Select Operator... | A |
Attribute: Select Attribute... | Select Operator... | A |
Attribute: Select Attribute... | Select Operator... | A |
Attribute: Select Attribute... | Select Operator... | A |
Attribute: Select Attribute... | Select Operator... | A |
Attribute: Select Attribute... | Select Operator... | A |

6. Save the policy.

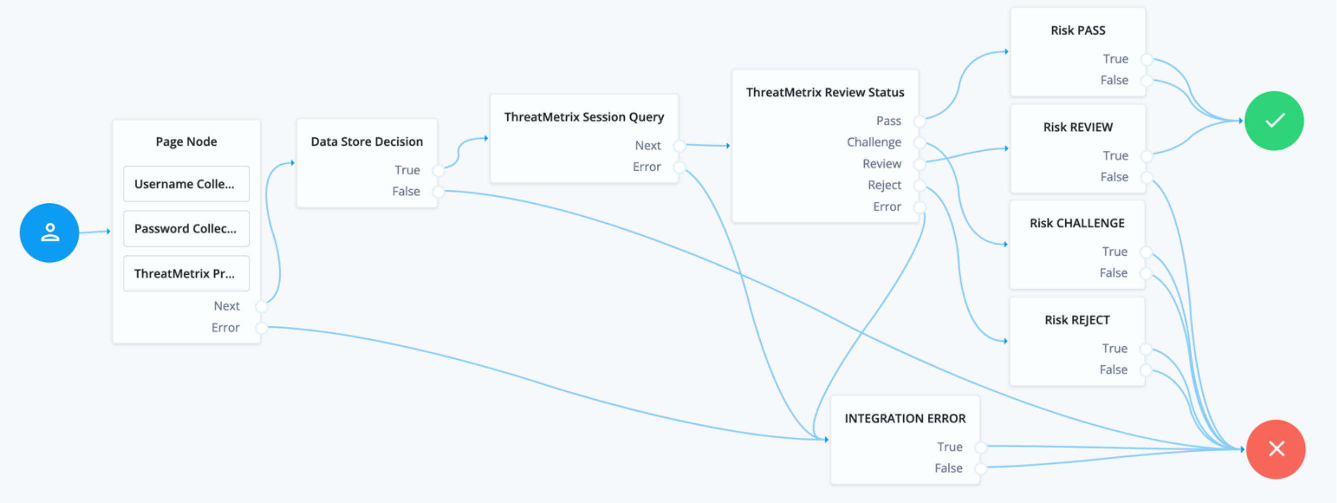
7. Consult with ThreatMetrix services for a more comprehensive policy configuration.

   Another simple test policy configuration can focus on Condition rules that interpret the Account Email attribute for test accounts.

FORGEROCK JOURNEY CONFIGURATION

Journey: Login-ThreatMetrix

This section provides the steps to configure a ForgeRock journey with LexisNexis ThreatMetrix nodes from the ForgeRock Identity Cloud Marketplace. This section will create a Login ThreatMetrix journey that performs device intelligence and profiling followed by a risk assessment via the ThreatMetrix session query. The objective is to have a journey as depicted below.

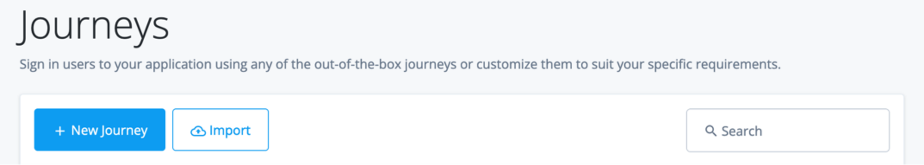


The flow is as follows:

- Page Node to display the Login user interface that will also contain the ThreatMetrix Page Profiling
- Data Store decision, which is to validate the users credentials against the default ForgeRock Identity Cloud user directory
- ThreatMetrix risk assessment via the session query
- ThreatMetrix risk decision based on the output of the risk assessment
- Message Nodes that will display the result of the ThreatMetrix Review Status

Perform the following to configure the journey:

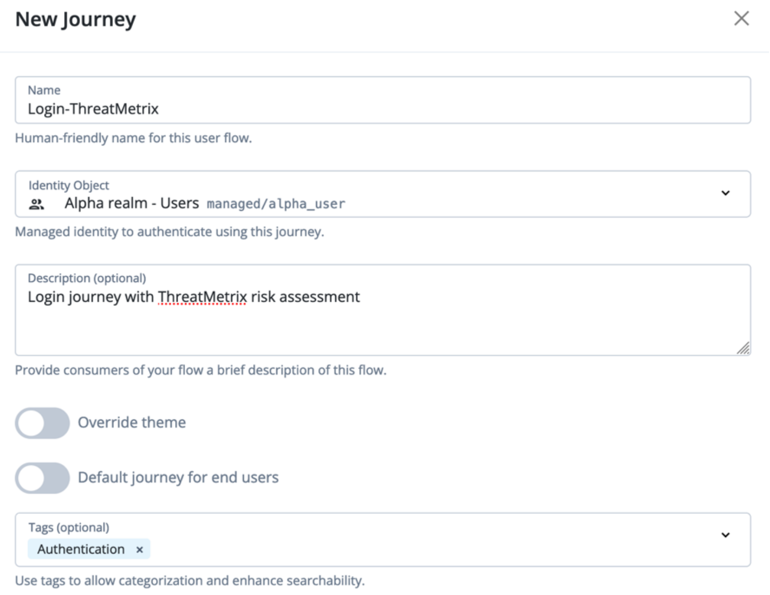
1. From a workstation, launch a browser and navigate to the ForgeRock Identity Cloud:
2. Login with administrator credentials for a user that has permission to configure journeys
3. Upon login, select the realm to configure the journey. For the purposes of this instruction the default realm of **alpha** is assumed.
4. On the main dashboard display, select **Journeys** on the left-hand side of the display.
5. On the **Journeys** display, click the **+New Journey** button.



Journeys

Sign in users to your application using any of the out-of-the-box journeys or customize them to suit your specific requirements.

6. On the **New Journey** display, enter information as shown followed by the **Save** button.



New Journey

Name: Login-ThreatMetrix
Human-friendly name for this user flow.

Identity Object: Alpha realm - Users `managed/alpha_user`
Managed identity to authenticate using this journey.

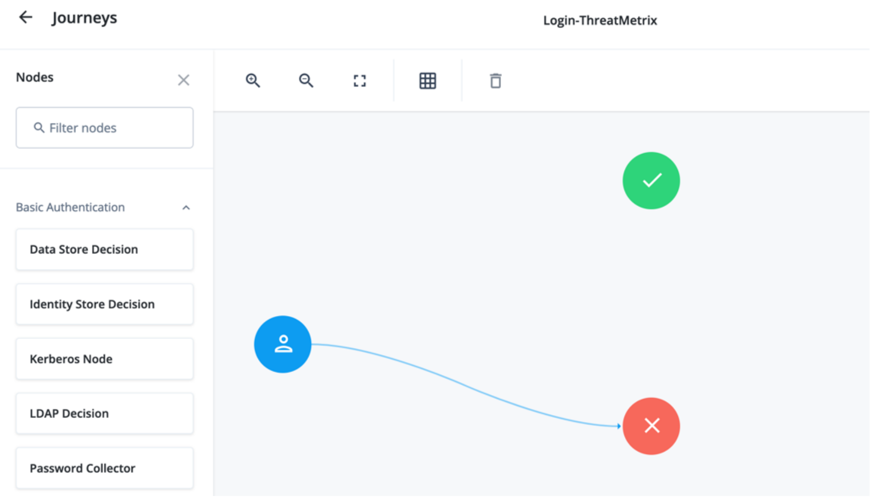
Description (optional): Login journey with ThreatMetrix risk assessment
Provide consumers of your flow a brief description of this flow.

Override theme

Default journey for end users

Tags (optional): Authentication ×
Use tags to allow categorization and enhance searchability.

7. The result is the **Journeys > Login-ThreatMetrix** display. This is the interface to build up the journey. At this point, the journey will be built by drag-n-drop of Components on the left side of the screen. Each node in the policy will then be configured.



8. Build the Login Screen (e.g. Page Node), do the following:

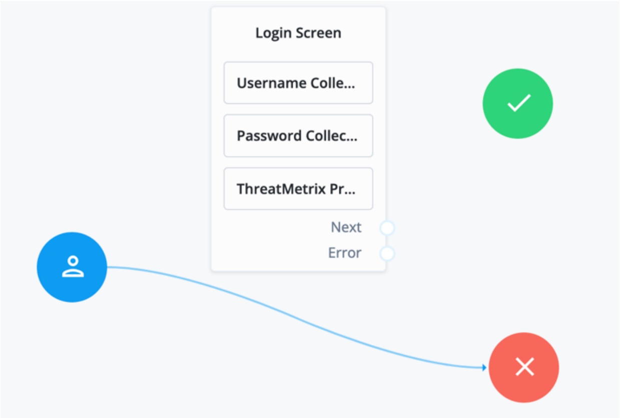
- On the **Components Filter** on the left side of the interface, enter **page**. When the **Page Node** is displayed as a component, drag and drop the node into the journey.
- When the **Page Node** properties are displayed on the right side of the interface, enter the following property values:

Node name	Login Screen
Page Header	(en) Sign In to ThreatMetrix Login Demo
Page Description	(en) New here? <a href="#/service/Registration">Create an account</a> <a href="#/service/ForgottenUsername">Forgot username?</a><a href="#/service/ResetPassword"> Forgot password?</a>

- On the **Components Filter** on the left side of the interface, enter **username**. When the **Username Collector** is displayed as a component, drag and drop the **Username Collector** into the journey into the **Login Screen** page node.
- On the **Components Filter** on the left side of the interface, enter **password**. When the **Password Collector** is displayed as a component, drag and drop the **Password Collector** into the journey into the **Login Screen** page node.
- On the **Components Filter** on the left side of the interface, enter **threatmetrix**. When the **ThreatMetrix Profiler** is displayed as a component, drag and drop it into the journey into the **Login Screen** page node.
- Select the ThreatMetrix Profiler Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Node name	ThreatMetrix Profiler
Org ID	<ENTER ORG ID FROM TMX PORTAL>
Page ID	login-page
Profiler URI	https://h.online-metrix.net/fp/tags.js
Client generated Session ID	Off

- At this point you should have the following



9. Build the Data Store Decision (e.g. login user credential validation), do the following:

   - On the **Components Filter** on the left side of the interface, enter **data**. When the **Data Store Decision** is displayed as a component, drag and drop it into the journey. The data decisions for user credential binding will utilize the Identity Store configure, which is the default user directory. The user identities are created and managed via the Identities capability.

10. Build Message Node for Integration Error to support testing, do the following:

    - On the **Components Filter** on the left side of the interface, enter **message**. When the **Message Node** is displayed as a component, drag and drop an instance into the journey. This node will be used to display an integration error message from any of the nodes. Enter the following property values.

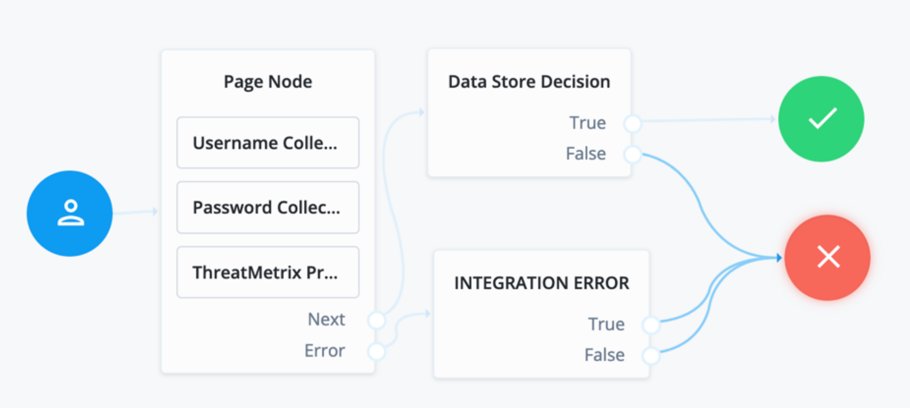
Node name	INTEGRATION ERROR
Message	(en) An integration error has occurred in the journey
Positive answer	(US) OK
Negative answer	(US) OK

11. Link together the nodes of the authentication policy

    - To connect the nodes of the journey, click on the output dot of one node and then drag it to the input dot of another node. The following connections should be made.

Start	Login Screen
Login Screen (Next)	Data Store Decision
Login Screen (Error)	INTEGRATION ERROR
Data Store Decision (True)	Success
Data Store Decision (False)	Failure
INTEGRATION ERROR (True)	Failure
INTEGRATION ERROR (False)	Failure

- At this point you should have the following



NOTE: At this point, the journey can be tested to validate the login screen and user directory credential store. The Journeys interface provides a Preview URL that can be cut and pasted into an incognito browser window.
This URL can be saved as a bookmark as it will be used to test the journey repeatedly.

12. Build the ThreatMetrix Session Query Node, do the following:

- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Session Query** is displayed as a component, drag and drop it into the journey. This node will get the SessionID calculated by the **ThreatMetrix Profiler** to perform the session_query API for risk assessment.
- Select the **ThreatMetrix Session Query Node** component to display the configuration properties on the right side of the interface. Enter the following property values.

Node name	ThreatMetrix Session Query
Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>
Service Type	Session Policy
Event Type	Login
Policy	default
Unknown Session Action	Challenge (This allows knowing if condition is encountered)
Query Type	Session Query
Session Query URI	https://h-api.online-metrix.net/api/session-query
Attribute Query URI	https://h-api.online-metrix.net/api/attribute-query
Add Shared State Variable	Selected

Session Query Parameters	Key=account_email, Value=mail
	Key=account_last_name, Value=sn
	Key=account_first_name, Value=givenName

NOTE: The session query parameters will attempt to discover the values based on the user directory credential store for the authenticated user. Be sure that the **Identities** has been configured with a test user that has the appropriate fields populated.

NOTE: The Query Type configuration allows the integrator to define if the API includes device profiling (e.g. Session Query) or the API is basic (e.g. Attribute Query). In the case of the Session Query configuration, the ThreatMetrix Profiler Node is required that will create the Session ID.

NOTE: The Unknown Session Action configuration allows the administrator to define an outcome when ThreatMetrix Profiling fails to process correctly. Having this outcome configuration can avoid users from being denied access based on issues with ThreatMetrix. For the purposes of this instruction, the values are set the “Challenge”.

13. Build the ThreatMetrix Review Status Node, do the following:

- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Review Status** is displayed as a component, drag and drop it into the journey. This node will get the result of risk assessment from the **ThreatMetrix Session Query** to perform decision logic on how to branch based on the review_status attribute in the API Response.
- Select the **ThreatMetrix Review Status** component to display the configuration properties on the right side of the interface. Enter the following property values.

Node name	ThreatMetrix Review Status

14. Build Message Nodes for the outcomes to support testing, do the following:

- On the **Components Filter** on the left side of the interface, enter **message**. When the **Message Node** is displayed as a component, drag and drop four instances into the journey. These nodes will be used to display the outcome of the **ThreatMetrix Review Status**.
- Name the four nodes as follows:

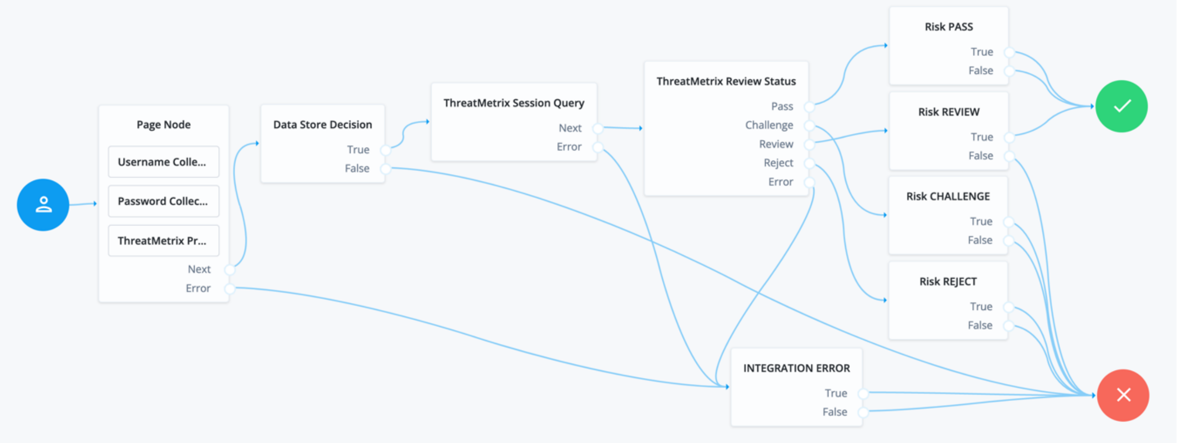
Node name	Risk PASS
Node name	Risk CHALLENGE
Node name	Risk REVIEW
Node name	Risk REJECT

15. Link together the nodes of the authentication policy

- To connect the nodes of the journey, click on the output dot of one node and then drag it to the input dot of another node. The following connections should be made.

Start	Login Screen
Login Screen (Next)	Data Store Decision
Login Screen (Error)	INTEGRATION ERROR
Data Store Decision (True)	ThreatMetrix Session Query
Data Store Decision (False)	Failure
INTEGRATION ERROR (True)	Failure
INTEGRATION ERROR (False)	Failure
ThreatMetrix Session Query (Next)	ThreatMetrix Review Status
ThreatMetrix Session Query (Error)	INTEGRATION ERROR
ThreatMetrix Review Status (Pass)	Risk PASS
ThreatMetrix Review Status (Challenge)	Risk CHALLENGE
ThreatMetrix Review Status (Review)	Risk REVIEW
ThreatMetrix Review Status (Reject)	Risk REJECT
ThreatMetrix Review Status (Error)	INTEGRATION ERROR
Risk PASS (True)	Success
Risk PASS (False)	Success
Risk REVIEW (True)	Success
Risk REVIEW (False)	Failure
Risk CHALLENGE (True)	Failure
Risk CHALLENGE (False)	Failure
Risk REJECT (True)	Failure
Risk REJECT (False)	Failure

- At this point you should have the following



Journey: StepUp-OTP

This section provides the steps to configure a ForgeRock journey with LexisNexis ThreatMetrix nodes from the marketplace, specifically a One-Time Passcode (OTP) integration with ThreatMetrix retrospective truth data via the ThreatMetrix Update Review nodes.

This section will create a journey that is meant to be called from a ForgeRock **Inner Tree Evaluator** node from another authentication tree that has the ThreatMetrix risk assessment, in this case the **Login-ThreatMetrix** journey from the previous section.

The shared state is assumed to have the request_id from the risk assessment result which is used to link together the ThreatMetrix Update Review for retrospective truth data to the risk event.

For the purposes of brevity, the OTP nodes will not be documented here, rather a simple Message node to direct the outcome will be used.

Perform the following to configure the journey:

1. From a workstation, launch a browser and navigate to the ForgeRock Identity Cloud:
2. Login with administrator credentials for a user that has permission to configure journeys
3. Upon login, select the realm to configure the journey. For the purposes of this instruction the default realm of **alpha** is assumed.
4. On the main dashboard display, select **Journeys** on the left-hand side of the display.
5. On the **Journeys** display, click the **+New Journey** button.
6. On the **New Journey** display, enter information as shown followed by the **Save** button.

Name	StepUp-OTP
Identity Object	Alpha realm - Users
Description	Step-Up Authentication workflow with OTP
Override theme	Not selected
Default journey for end users	Not selected
Tags	Authentication

7. The result is the **Journeys > StepUp-OTP** display. This is the interface to build up the authentication policy. At this point, the journey will be built by drag-n-drop of Components on the left side of the screen. Each node in the policy will then be configured.
8. Build the **ThreatMetrix Update Review** nodes, do the following:

- There are going to be three (3) nodes in the journey to handle the different outcomes from the review status node. So be sure to have an “init”, “pass” and “fail” node.
- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Update Review** is displayed as a component, drag and drop it into the journey. This node will add retrospective truth data to a Session Query event that indicates step-up authentication is being initialized. Once the node has been placed on the journey graph, select the component and enter the following configuration:

Node name	Update Review INIT
Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>
Update URI	https://h-api.online-metrix.net/api/update
Event Tag	Step-Up Initialize
Step-Up Method	OTP SMS
Notes	<BLANK>

- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Update Review** is displayed as a component, drag and drop it into the journey. This node will add retrospective truth data to a Session Query event that indicates step-up authentication is being initialized. Once the node has been placed on the journey graph, select the component and enter the following configuration:

Node name	Update Review PASS
Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>
Update URI	https://h-api.online-metrix.net/api/update
Event Tag	Step-Up Pass
Step-Up Method	OTP SMS
Notes	<BLANK>

- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Update Review** is displayed as a component, drag and drop it into the journey. This node will add retrospective truth data to a Session Query event that indicates step-up authentication is being initialized. Once the node has been placed on the journey graph, select the component and enter the following configuration:

Node name	Update Review FAIL
Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>
Update URI	https://h-api.online-metrix.net/api/update
Event Tag	Step-Up Fail
Step-Up Method	OTP SMS
Notes	<BLANK>

9. Build Message Node for Integration Error to support testing, do the following:

- On the **Components Filter** on the left side of the interface, enter **message**. When the **Message Node** is displayed as a component, drag and drop an instance into the journey. This node will be used to display an integration error message from any of the nodes. Enter the following property values.

Node name	INTEGRATION ERROR
Message	(en) An integration error has occurred in the Journey
Positive answer	(en) OK
Negative answer	(en) OK

10. Build Message Node to simulate OTP to support testing, do the following:

- On the **Components Filter** on the left side of the interface, enter **message**. When the **Message Node** is displayed as a component, drag and drop an instance into the journey. This node will simulate the success or failure of Step-Up Authentication. Enter the following property values.

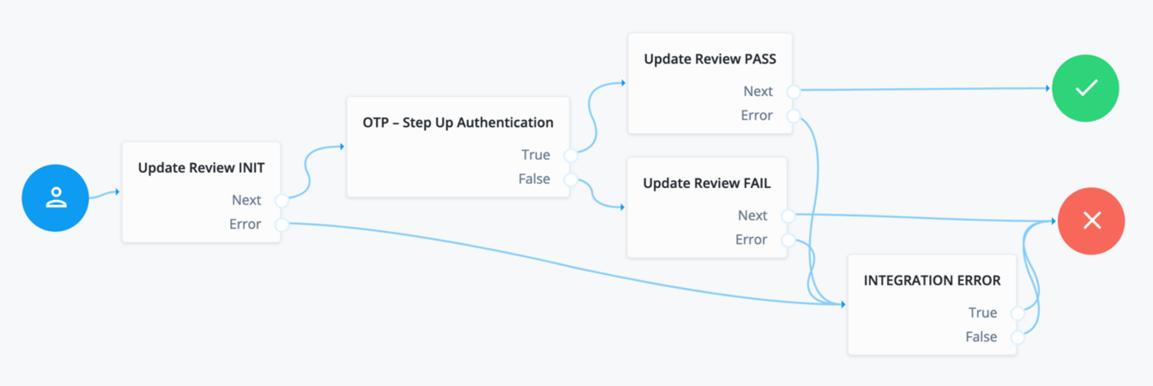
Node name	OTP – Step Up Authentication
Message	(en) OTP – Step Up Authentication
Positive answer	(en) Step Up PASS
Negative answer	(en) Step Up FAIL

11. Link together the nodes of the authentication policy

- To connect the nodes of the journey, click on the output dot of one node and then drag it to the input dot of another node. The following connections should be made:

Start	Update Review INIT
Update Review INIT (Next)	OTP – Step Up Authentication
Update Review INIT (Error)	INTEGRATION ERROR
OTP – Step Up Authentication (True)	Update Review PASS
OTP – Step Up Authentication (False)	Update Review FAIL
Update Review PASS (Next)	Success
Update Review PASS (Error)	INTEGRATION ERROR
Update Review FAIL (Next)	Failure
Update Review FAIL (Error)	INTEGRATION ERROR
INTEGRATION ERROR (True)	Failure
INTEGRATION ERROR (False)	Failure

- At this point you should have the following



12. At this point the OTP journey is ready to be called from any other ForgeRock journey. Click **Save**.
13. To leverage the OTP flow from the journey with ThreatMetrix, add an **Inner Tree Evaluator** node.

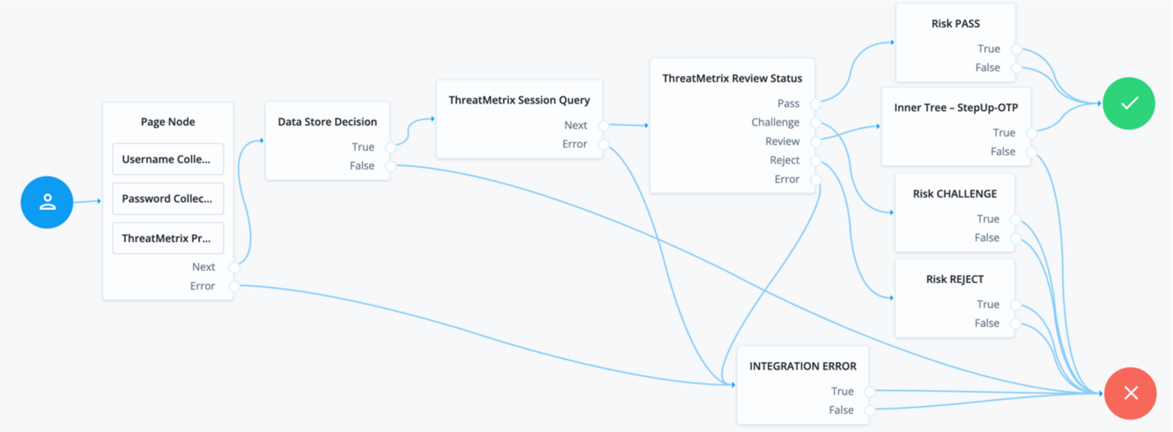
- Open the Authentication Tree named **Login-ThreatMetrix**
- On the **Components Filter** on the left side of the interface, enter **inner**. When the **Inner Tree Evaluator** node is displayed as a component, drag and drop an instance into the authentication tree. This node will be used to display call the OTP Step Up authentication tree. Enter the following property values.

Node name	Inner Tree – StepUp-OTP
Tree Name	StepUp-OTP

- To connect the nodes of the authentication tree, click on the output dot of one node and then drag it to the input dot of another node. The following connections should be made and/or updated:

ThreatMetrix Review Status (Review)	Inner Tree - OTP StepUp
Inner Tree - OTP StepUp (True)	Update Review PASS
Inner Tree - OTP StepUp (False)	Update Review FAIL

- At this point you should have the following



14. Complete and ready for testing

- To Using an incognito browser window, enter the Preview URL and test with the demo user as created in **Identities**.