Getting Started Guide

Configure Ping Access Management (PingAM) / ForgeRock Access Management with LexisNexis ThreatMetrix Nodes

Version 1.3.0

August 2025

LexisNexis®
RISK SOLUTIONS

Table of Contents

SCOPE

LexisNexis Risk Solutions (LNRS) Dynamic Decision Platform (DDP) hosts the ThreatMetrix (TMX) product for risk assessment. This document contains the detailed steps and supporting information required to install and configure Ping Access Management (PingAM), formerly ForgeRock Access Management (AM) with LexisNexis ThreatMetrix Authentication Nodes. This guide is intended to install a simple configuration to support testing.

The following are architecture assumptions and limitations:

- PingAM / ForgeRock Access Management server has been previously installed
- PingAM / ForgeRock Access Management server has an Identity Store configured
- 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 authentication tree integration.
- **LexisNexis Nodes Installation.** Provides information to install the LexisNexis ThreatMetrix nodes upon an on-premise PingAM / ForgeRock Access Management server.
- **LexisNexis ThreatMetrix Portal.** Provides detailed information regarding the configuration of the Dynamic Decision Platform (DDP) / ThreatMetrix (TMX) product to include configuration of a simple policy and how to access configuration parameters required for the authentication tree.
- **Authentication Tree Configuration.** Provides detailed steps to configure an authentication tree with LexisNexis ThreatMetrix for an 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 PingAM / ForgeRock for testing and integration.
Administrators	This guide is also intended for administrator to be able to install and configure PingAM / ForgeRock for testing and integration.

LEXISNEXIS THREATMETRIX NODE OVERVIEW

The LexisNexis ThreatMetrix Nodes provides the capability for administrators to integrate advanced risk assessment capability through integration with the LexisNexis Risk Solutions (LNRS) Dynamic Decision Platform (DDP) / ThreatMetrix (TMX) product. The nodes are available for both PingOne Advanced Identity Cloud (PingOne AIC), formerly ForgeRock Identity Cloud, and Ping Access Management (PingAM), formerly ForgeRock Access Management.

The nodes provide production ready connectivity and orchestration of all LexisNexis products to include ThreatMetrix, BehavioSec, Emailage, PhoneFinder, InstantID, FlexID and more. The nodes also support a wide variety of use cases to include login, password change, account creation, and payment to name a few. When the nodes are integrated, the risk assessment policy hosted within the LexisNexis DDP/TMX cloud returns a risk score mapped to defined outcomes such as step-up authentication, passing without further friction, or rejecting resulting in blocking the transaction.

To include LexisNexis ThreatMetrix nodes in an authentication tree, enter ThreatMetrix 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 fingerprinting/profiling JavaScript Tags within a Page Node to collect device intelligence which will be used as part of risk assessment. The ThreatMetrix Profiler node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated with DDP/TMX generated for your organization.
- **Page ID** - The Page ID is an identifier to be used if you place the profiling on multiple page nodes. This is an optional parameter and can be left blank.
- **Profiler URI** - ThreatMetrix Profiler URI. This can be the Basic Profiling URL or the Enhanced Profiling via Hosted SSL URL. The default configuration is the Basic Profiling URL for the global region.
- **Use Client Generated Session IDs** - If ThreatMetrix JavaScript Tags have been separately integrated onto an customer hosted webpage or mobile device, this configuration allows for sending the unique Session ID to Ping AIC / ForgeRock through HiddenValueCallback as part of an API Request.

ThreatMetrix Query Node

This node makes a DDP/TMX API Request to either: (i) Session Query API, or (ii) Attribute Query API. The main difference is that Session Query API requires the 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 DDP/TMX generated for your organization.
- **API Key** - This is the unique API key generated by DDP/TMX 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 DDP/TMX Knowledge Base (KB) for a full list of service types.
- **Event Type** - Specifies the type of transaction or event. The default configuration is login. See the DDP/TMX KB for a full list of event types.
- **Policy** - The policy to be used for the query. The policy is configured in the DDP/TMX Portal which is a set of decision policy rules that together generate the risk assessment policy score and outcome.
- **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 as the DDP/TMX API Request. Session Query requires device intelligence to be collected previously by the Profiler Node and Attribute Query does not require device profile information.
- **Base URL** - Defines the domain URL for the DDP/TMX region where API Requests are to be sent. The default value is the global region.
- **Add Attributes to API Request** - If you'd like to add additional parameters to the DDP/TMX 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.
- **Attribute Source** - Defines where additional attributes (if configured) are to be fetched at runtime. This is a dropdown list that contains the options User Directory and Shared State. User Directory will look for attributes in the Identity Store, and Shared State looks in the shared memory of the authentication journey.
- **Query Attributes** - This is a list of DDP/TMX attributes (e.g. "key") to authentication journey attributes (e.g. "value"). The Attribute Source configuration defines where the values will be fetched. If the values cannot be fetched, the API Request will not include the DDP/TMX attribute.

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 defined in the ThreatMetrix Query Node.

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 DDP/TMX 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 authentication journey.

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 DDP/TMX Portal policy.

ThreatMetrix Update Review Node

The ThreatMetrix Update Node provides retrospective truth data to ThreatMetrix for an event. The typical authentication journey 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 DDP/TMX generated for your organization.
- **API Key** - This is the unique API key generated by DDP/TMX associated to the Org ID.
- **Base URL** - Defines the domain URL for the DDP/TMX region where API Requests are to be sent. The default value is the global region.
- **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 authentication journey 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.

NODES INSTALLATION

This section describes how to deploy the LexisNexis ThreatMetrix Authentication Nodes to PingAM / ForgeRock Access Management hosted on Apache Tomcat. The server will need to be stopped and restarted for the nodes to be properly deployed. This instruction assumes an Apache Tomcat application web server.

1. Stop the Tomcat server
2. Remove any previously installed versions of LexisNexis ThreatMextrix Nodes from the server:

   Directory: `<fgrkinstall>/tomcat/webapps/openam/WEB-INF/lib`
3. Copy the LexisNexis ThreatMetrix Nodes media as follows:

   Filename: `lexisnexis-threatmetrix-1.3.0.jar`

   Directory: `<fgrkinstall>/tomcat/webapps/openam/WEB-INF/lib`
4. Restart Tomcat server from command line

The latest release of the LexisNexis ThreatMetrix Authentication Nodes does have new configuration parameters that differ from the previous version 1.2.0 release. The new release will handle backwards compatibility for any existing authentication trees. If there is an existing authentication tree, be sure to update configuration and validate the workflows.

DDP / TMX PORTAL CONFIGURATION

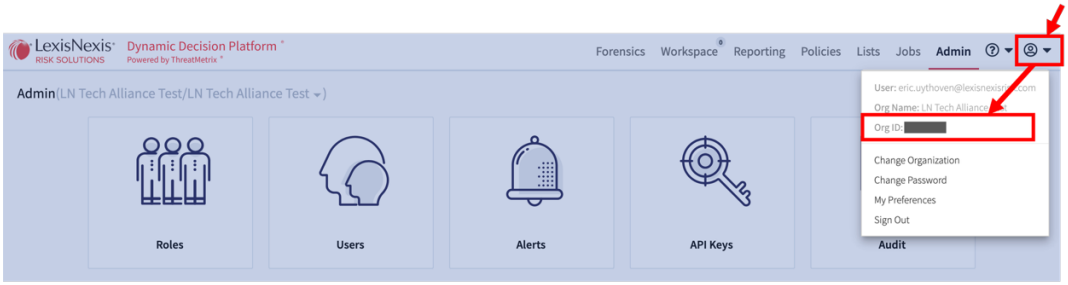
This section defines the high-level DDP / TMX configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- Organization ID and API Key for the REST API interfaces. This information is needed by the LexisNexis ThreatMetrix Authentication Nodes and will be entered as part of configuration.
- DDP/TMX Policy. The configured policy within DDP / TMX 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.

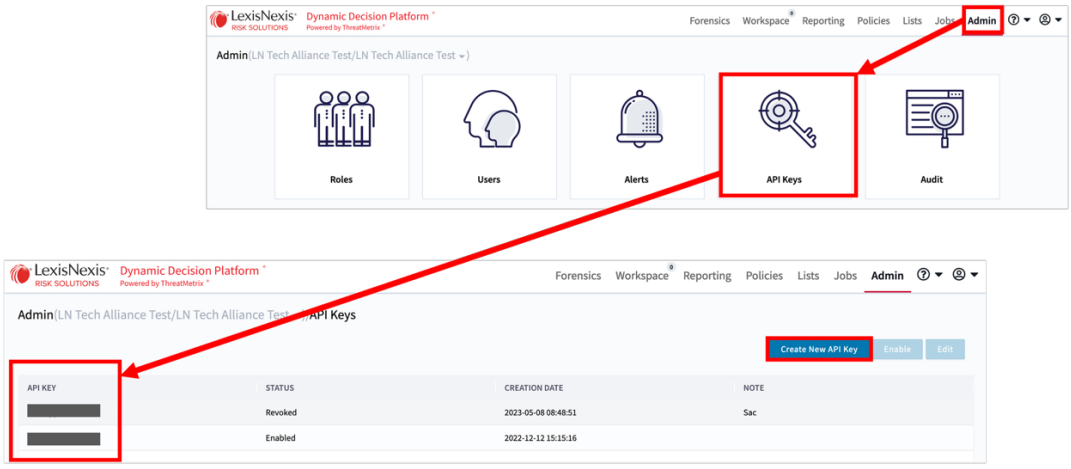
Retrieve OrgID and API Key

To retrieve the DDP / TMX values for Organization ID and API Key, perform the following steps.

1. Access **DDP/TMX Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis Risk Solutions.
2. From the **DDP/TMX 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.



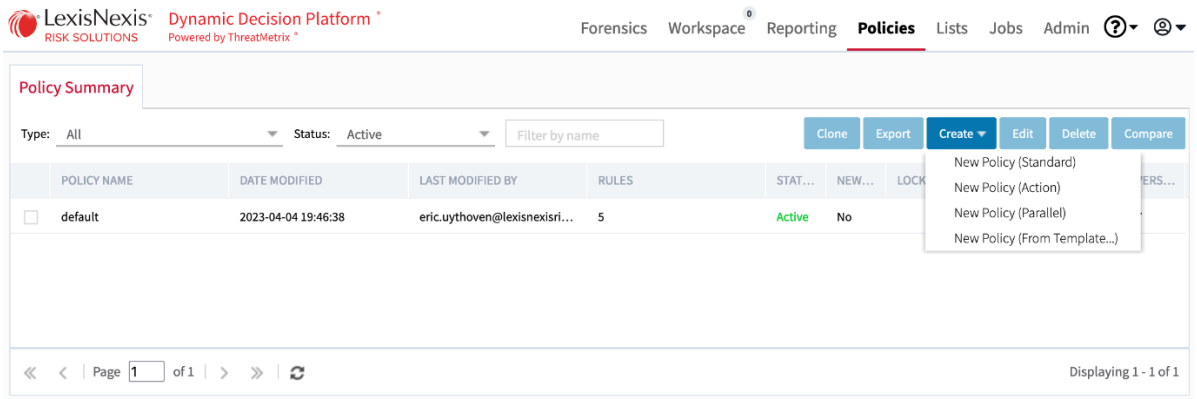
3. Within the **DDP/TMX Portal** home page, select **Admin** followed by selecting the **API Keys** tile. Retrieve the value for API Key. In the event no API Key is listed, select the **Create New API Key** button to generate a new key. This will be the API Key to enter into the configuration of the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



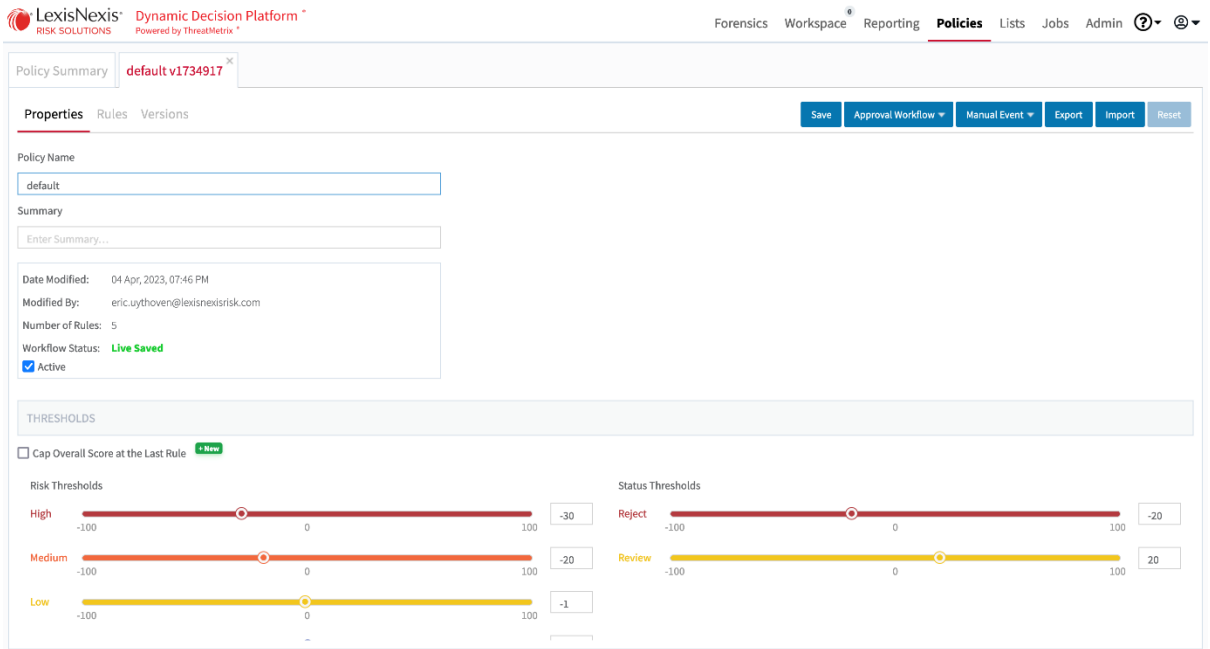
Risk Assessment Policy

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.

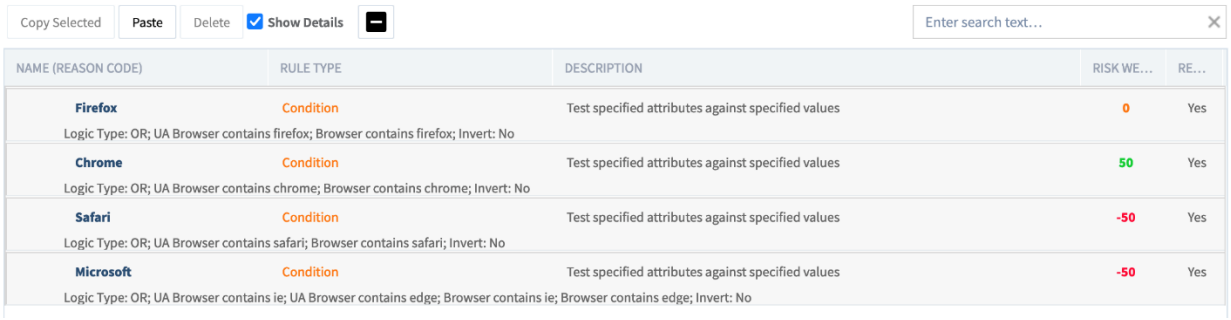
1. Access **DDP/TMX Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis Risk Solutions.
2. From the **DDP/TMX Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies that can be configured 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)**.



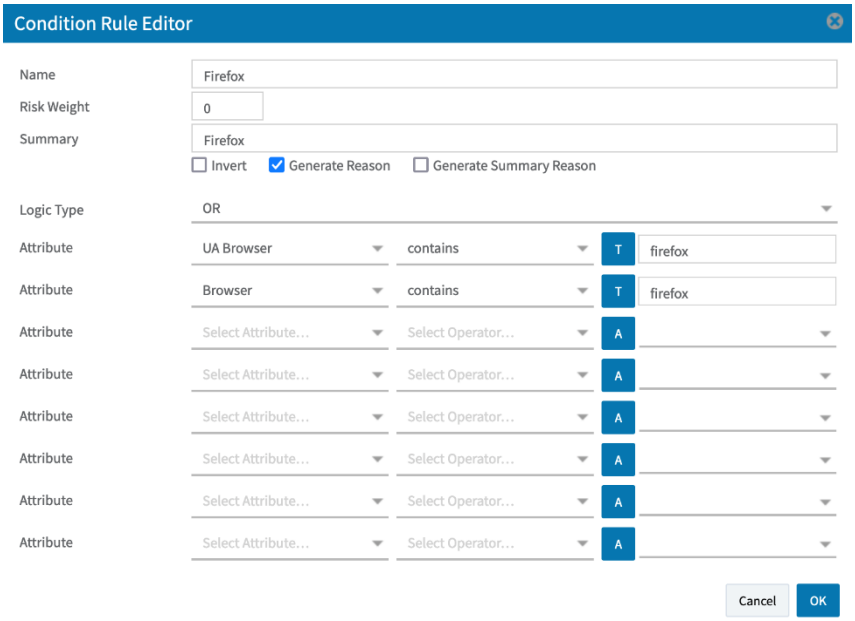
3. On the Policy Summary, the **Properties** interface tab will be displayed. Enter Policy Name = default, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



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.



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



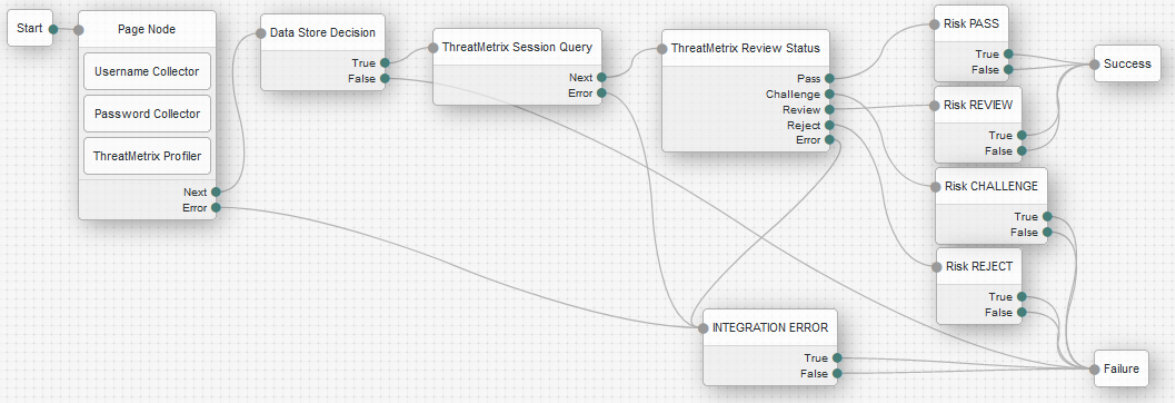
6. Save the policy.
7. Consult with LexisNexis professional services for a more comprehensive policy configuration.

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

AUTHENTICATION TREE CONFIGURATION

Authentication Tree: ThreatMetrix

This section provides the steps to configure a PingAM / ForgeRock Authentication Tree with LexisNexis ThreatMetrix nodes from the marketplace. This section will create an authentication tree that performs device intelligence via the LexisNexis ThreatMetrix Profiler Node followed by a risk assessment via the LexisNexis ThreatMetrix Query Node. The objective is to have a tree as depicted below.



The flow is as follows:

- Page Node to display the Login user interface that will also contain the page profiling
- Data Store decision, which is to validate the users credentials against the Identity Store directory
- Risk assessment via the DDP/TMX session query
- Authentication Tree decision based on the review status output of the risk assessment
- Message Nodes that will display the result of the risk assessment

The steps here will establish the Authentication Tree to be used for authentication of the user. Perform the following to configure the server:

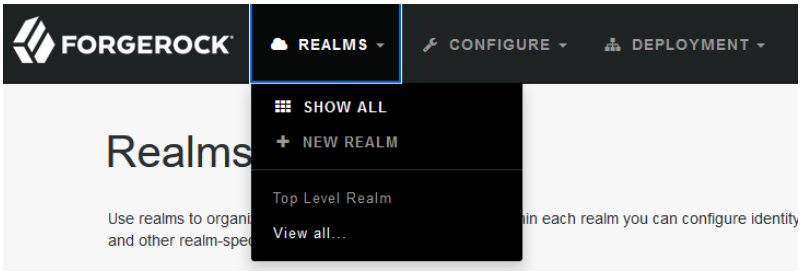
1. From a workstation, launch a browser and enter the URL for the Administration Console:

   Example: `https://sso.threatmetrix.com:8443/openam`

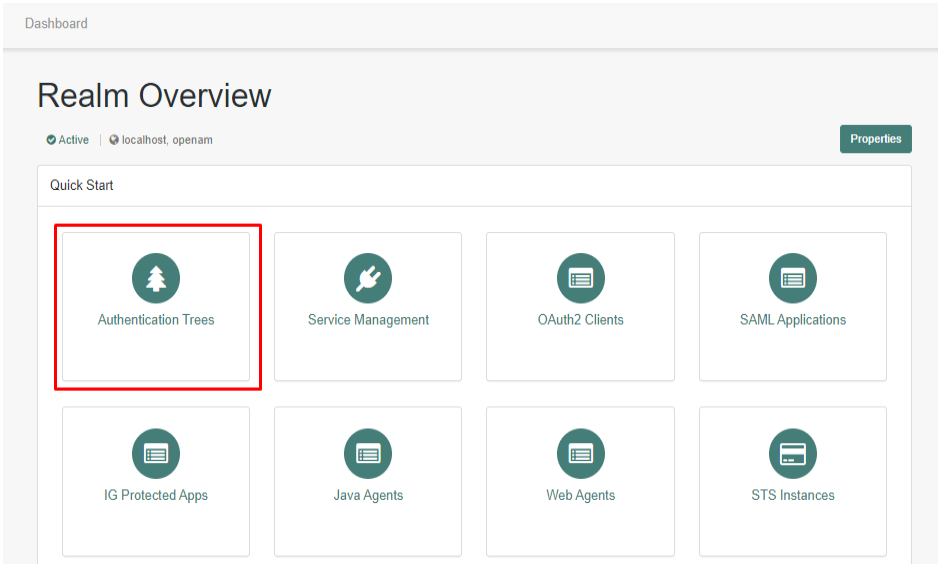
   > **NOTE:** In this example, communications proceed over the HTTPS protocol to a FQDN (`sso.threatmetrix.com`), over a standard Java web container port number (8443), to a specific deployment URI (/openam).

2. Login as Administrator, for example amadmin and credentials

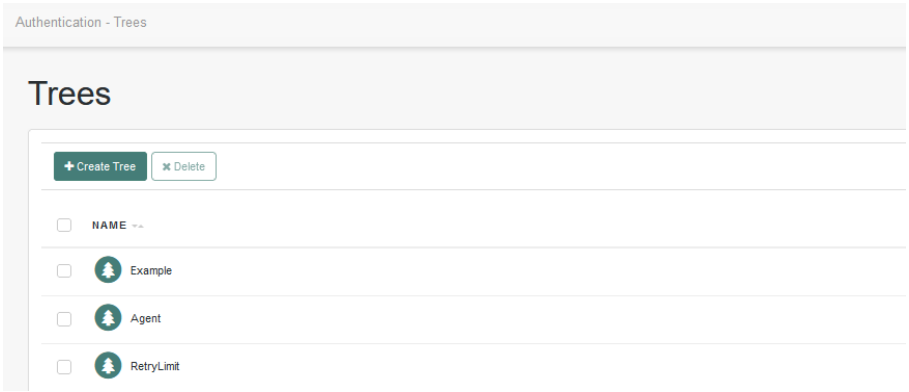
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**. For the remainder of this simple quick start configuration, the top-level root realm is assumed.



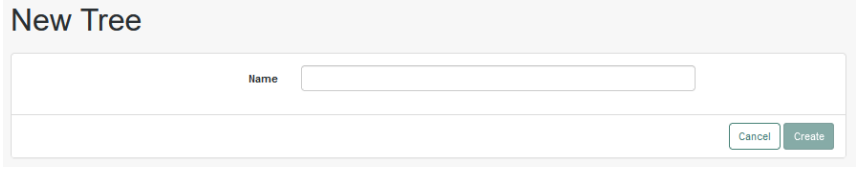
4. On the **Realm Overview** display, click the **Authentication Trees** tile.



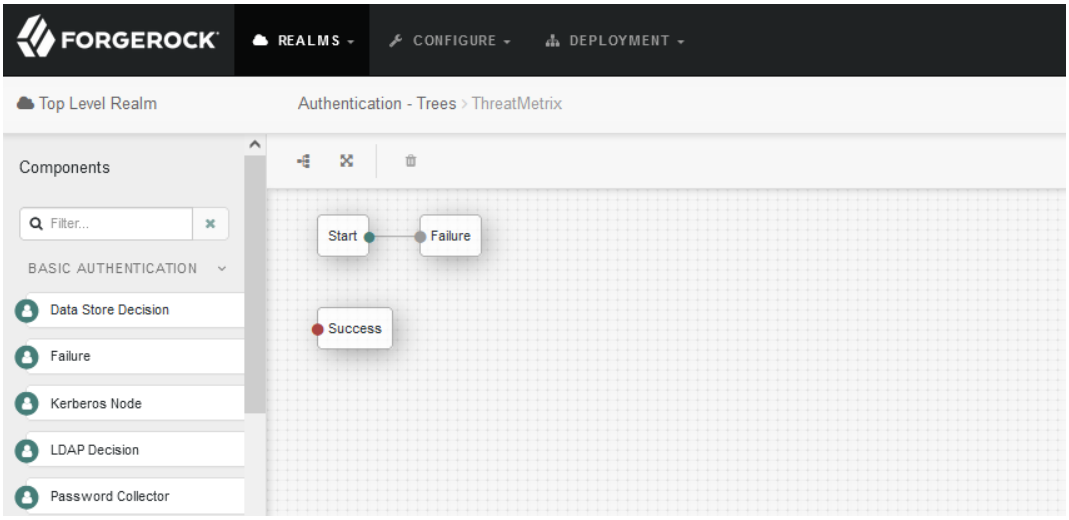
5. On the **Authentication Trees** display, click the **Create Tree** tile.



6. On the **New Tree** display, enter “ThreatMetrix” followed by the **Create** button.



7. The result is the **Authentication Trees > ThreatMetrix** display. This is the interface to build up the authentication policy as a tree depiction showing the nodes in the policy. At this point, the tree 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.

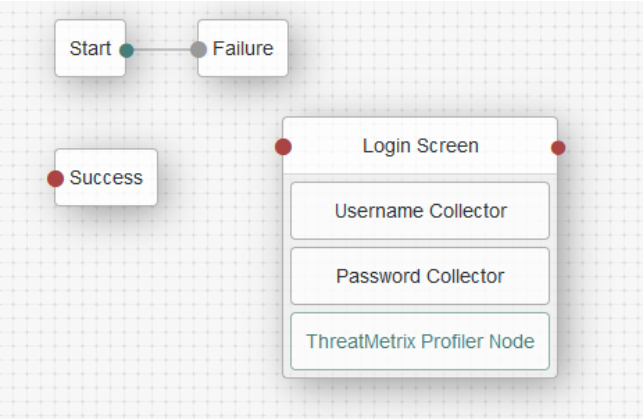


8. Build the Login Screen (e.g. Page Node), do the following:

- 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 authentication tree.
- When the **Page Node** properties are displayed on the right side of the interface, enter **Login Screen** as the **Node Name**.
- 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 authentication tree 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 authentication tree into the **Login Screen** page node.
- On the **Components Filter** on the left side of the interface, enter **threat**. When the **ThreatMetrix Profiler** is displayed as a component, drag and drop it into the authentication tree 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	Leave Blank – This is optional parameter
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 authentication tree. The data decisions for user credential binding will utilize the Identity Store configuration. 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 authentication tree. This node will be used to display an integration error message from any of the nodes. Enter the following property values.

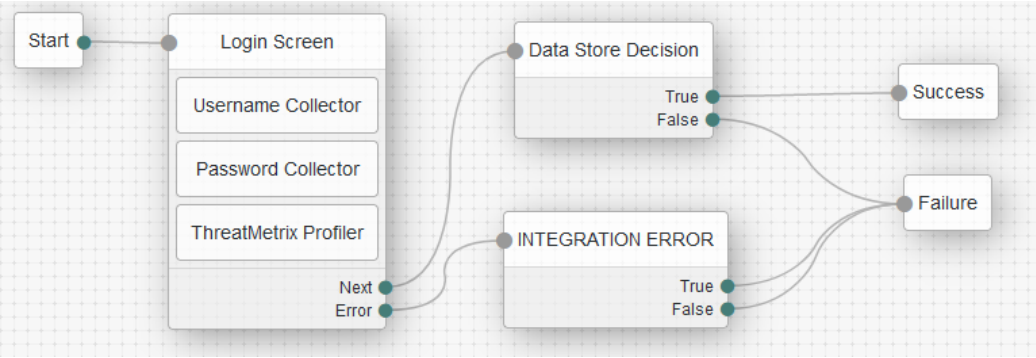
Node name	INTEGRATION ERROR
Message	(en_US) An integration error has occurred in the Auth Tree
Positive answer	(en_US) OK
Negative answer	(en_US) OK

11. Link together the nodes of the authentication policy

    - 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.

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 authentication tree policy can be tested to validate the login screen and core authentication via Data Store Decision. Using an incognito browser window, enter the following URL and test with the demo user as created in **Identities**.
> URL: https://<DOMAIN>:<PORT>/<ADMIN-URI>/XUI/?realm=/&service=ThreatMetrix
> EX: https://sso.threatmetrix.com:8443/openam/XUI/?realm=/&service=ThreatMetrix
> This URL can be saved as a bookmark as it will be used to test the authentication tree 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 Query** is displayed as a component, drag and drop it into the authentication tree. This node will get the SessionID calculated by the **ThreatMetrix Profiler** to perform the session_query API for risk assessment.
- Select the **ThreatMetrix Query Node** component to display the configuration properties on the right side of the interface. Enter the following property values.

Node name	ThreatMetrix 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
Base URL	https://h-api.online-metrix.net/
Add Attributes to API Request	Selected
Attribute Source	User Directory
Query Attributes	Key=account_email, Value=mail Key=account_last_name, Value=sn Key=account_first_name, Value=givenName

> **NOTE:** The Query Attributes will attempt to discover the values as configured by the Attribute Source. This is a list of DDP/TMX attributes (e.g. "key") to authentication journey attributes (e.g. "value"). If the values cannot be fetched, the API Request will not include the DDP/TMX attribute.

NOTE: The Attribute Source defines where the Query Attributes will be searched. User Directory will look for attributes in the Identity Store, and Shared State looks in the shared memory of the authentication tree.

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 authentication tree. This node will get the result of risk assessment from the **ThreatMetrix 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 authentication tree. 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

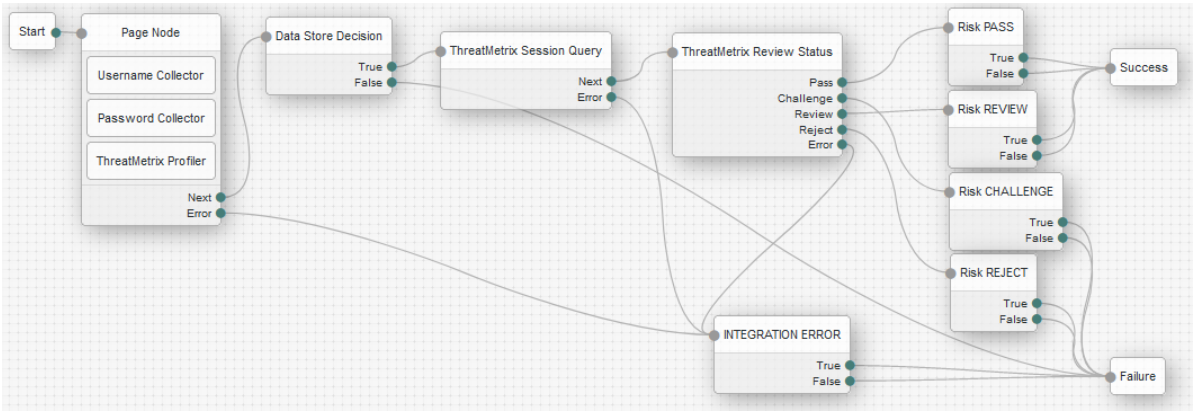
15. Link together the nodes of the authentication policy

    - To connect the nodes of the 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.

Start	Login Screen
Login Screen (Next)	Data Store Decision
Login Screen (Error)	INTEGRATION ERROR
Data Store Decision (True)	ThreatMetrix 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 Assessment REVIEW (True)	Success
Risk Assessment REVIEW (False)	Success
Risk Assessment CHALLENGE (True)	Failure
Risk Assessment CHALLENGE (False)	Failure
Risk Assessment REJECT (True)	Failure
Risk Assessment REJECT (False)	Failure

- At this point you should have the following



16. The risk assessment Authentication Tree with LexisNexis ThreatMetrix nodes is complete and ready for testing. In order to test, ensure a test user is configured via **Identities**. The configured tree will utilize the **Identity Store** to authenticate the user and pull any additional query attributes.
    - URL: https://<DOMAIN>:<PORT>/<ADMIN-URI>/XUI/?realm=/&service=ThreatMetrix
    - EX: https://sso.threatmetrix.com:8443/openam/XUI/?realm=/&service=ThreatMetrix

Authentication Tree: TMX-StepUpOTP

This configuration in this section of the quick start guide is optional. This section provides the steps to configure an Authentication Tree with LexisNexis ThreatMetrix nodes from the marketplace, specifically how to provide truth data and final review status. This integration is performed when the review status indicates a step-up authentication is needed based on the risk assessment. For this simple example, a Message Node will be used to simulate One-Time Passcode (OTP).

This section will create an Authentication Tree that is meant to be called from an Inner Tree Evaluator node. The objective is to package the functionality of the step-up authentication into a separate Authentication Tree that is then invoked from the primary risk assessment Authentication Tree, which in this case is the ThreatMetrix authentication tree from the previous section.

Perform the following to configure:

1. From a workstation, launch a browser and navigate to the Access Management Admin Console.
2. Login with amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.
4. On the **Realm Overview** display, click the **Authentication Trees** tile.
5. On the **Authentication Trees** display, click the **Create Tree** tile.
6. On the **New Tree** display, enter "TMX-StepUpOTP" followed by the **Create** button.
7. The result is the **Authentication Trees > TMX-StepUpOTP** display. At this point, the tree 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 tree 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 authentication tree. This node will add retrospective truth data to a DDP/TMX query event that indicates step-up authentication is being initialized. Once the node has been placed on the Authentication Tree 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>
Base URL	https://h-api.online-metrix.net/
Event Tag	Step-Up Initialize
Step-Up Method	OTP SMS
Notes	<BLANK> - This is an optional parameter

   - 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 authentication tree. 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 Auth Tree 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>
Base URL	https://h-api.online-metrix.net/
Event Tag	Step-Up Pass
Step-Up Method	OTP SMS
Notes	<BLANK> - This is an optional parameter

- 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 authentication tree. 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 Auth Tree 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>
Base URL	https://h-api.online-metrix.net/
Event Tag	Step-Up Fail
Step-Up Method	OTP SMS
Notes	<BLANK> - This is an optional parameter

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 authentication tree. 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_US) An integration error has occurred in the Auth Tree
Positive answer	(en_US) OK
Negative answer	(en_US) 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 authentication tree. Theis node will simulate the success or failure of Step-Up Authentication. Enter the following property values.

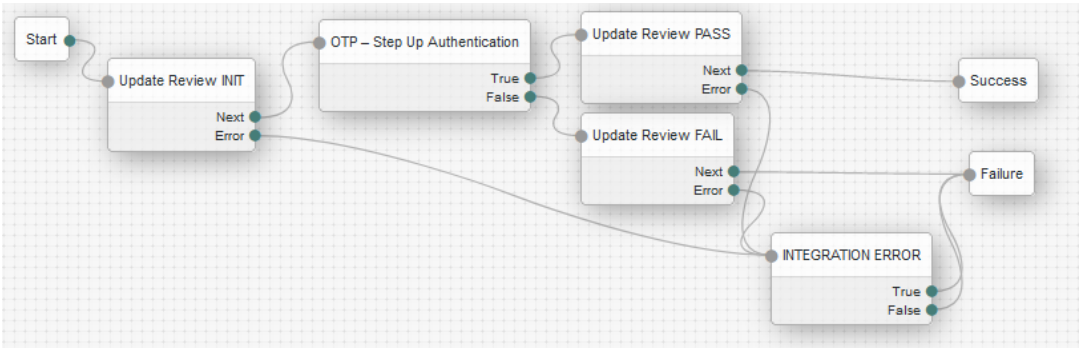
Node name	OTP – Step Up Authentication
Message	(en_US) OTP – Step Up Authentication
Positive answer	(en_US) Step Up PASS
Negative answer	(en_US) Step Up FAIL

11. Link together the nodes of the authentication policy

- 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:

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



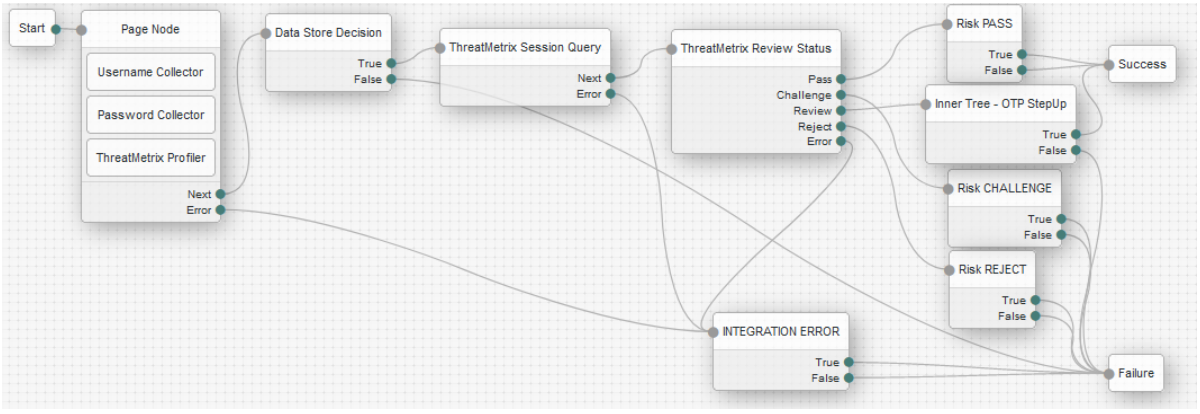
12. At this point the OTP Authentication Tree is ready to be called from any other ForgeRock Authentication Tree. Click **Save**.
13. To leverage the OTP flow from the Login authentication tree with ThreatMetrix, add an Inner Tree Evaluator node.
    - Open the Authentication Tree named ThreatMetrix
    - 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 - OTP StepUp
Tree Name	TMX-StepUpOTP

    - 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. The risk assessment and step-up truth data Authentication Trees with LexisNexis ThreatMetrix nodes are complete and ready for testing. In order to test, ensure a test user is configured via **Identities**. The configured tree will utilize the **Identity Store** to authenticate the user and pull any additional query attributes.

    - URL: https://<DOMAIN>:<PORT>/<ADMIN-URI>/XUI/?realm=/&service=ThreatMetrix
    - EX: https://sso.threatmetrix.com:8443/openam/XUI/?realm=/&service=ThreatMetrix