Getting Started Guide

Configure ForgeRock with LexisNexis ThreatMetrix Nodes

Guide for On Premise with Access Manager

Version 1.0

May 2023

LexisNexis®
RISK SOLUTIONS

Table of Contents

SCOPE

This document contains the detailed steps and supporting information required to install and configure the ForgeRock Access Management (AM) Single Sign-On (SSO) server with LexisNexis ThreatMetrix Authentication Nodes. This guide is intended to install a simple configuration to support testing.

The following are architecture assumptions and limitations:

- ForgeRock Access Manager server has been previously installed
- Default configuration for ForgeRock SSO Server with a default configuration for OpenDJ as the Identity Store
- 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.
- **Nodes Installation.** Provides information to install the LexisNexis ThreatMetrix nodes upon an on-premise ForgeRock Access Management (AM) server.
- **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 authentication tree.
- **ForgeRock Authentication Tree Configuration.** Provides detailed steps to configure a ForgeRock authentication tree 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.

NODES INSTALLATION

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

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

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

   Filename: `ThreatMetrixAuthNode-1.2.0.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 1.1.0 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.

THREATMETRIX PORTAL CONFIGURATION

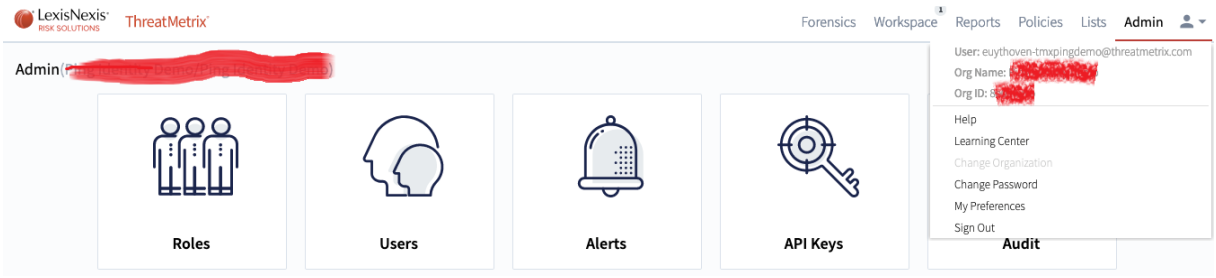
This section defines the high-level LexisNexis ThreatMetrix configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- 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.

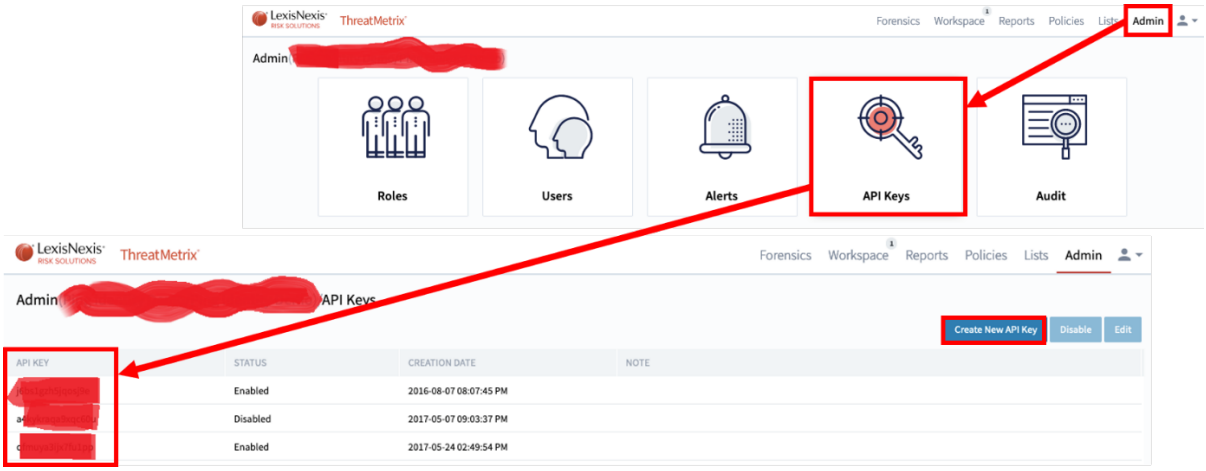
Retrieve OrgID and API Key

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.



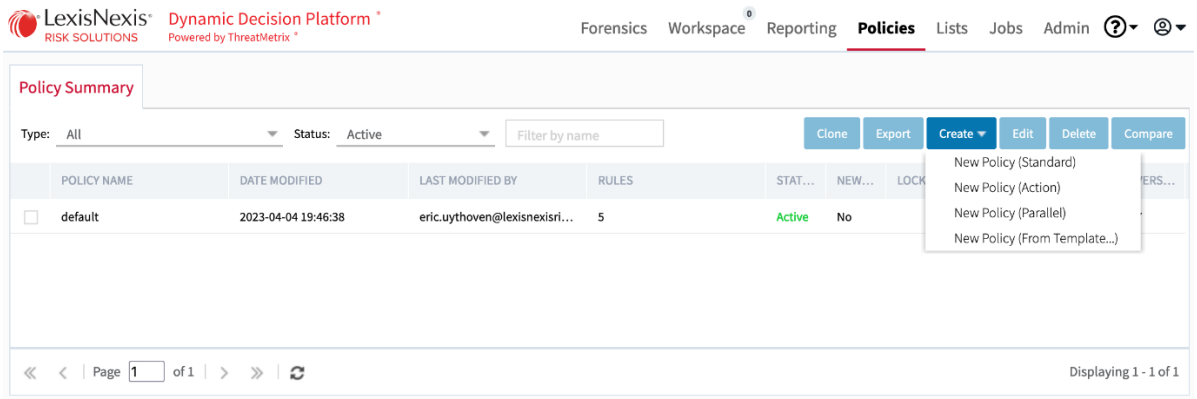
3. Within the **ThreatMetrix Portal** home page, select **Admin** followed by selecting the **API Keys** tile. Retrieve the value for API Key. In the event no API Key is listed, select the **Create New API Key** button to generate a new key. This will be the API Key to enter into the configuration of 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.



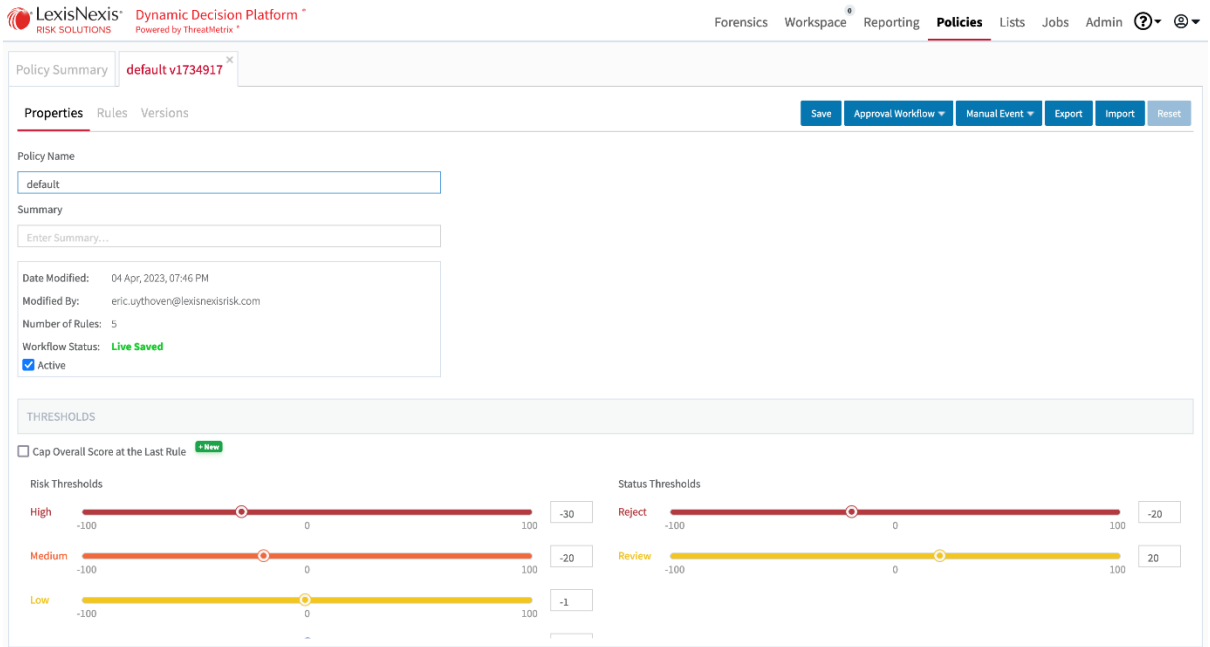
ThreatMetrix Policy

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.

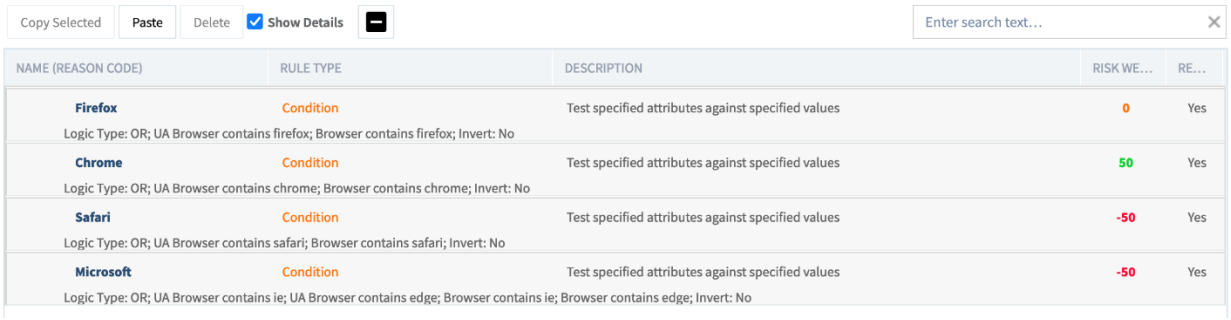
1. Access **ThreatMetrix Portal** over the internet by logging into your administrative account with credentials provided by ThreatMetrix.
2. From the **ThreatMetrix Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies that can be configured within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



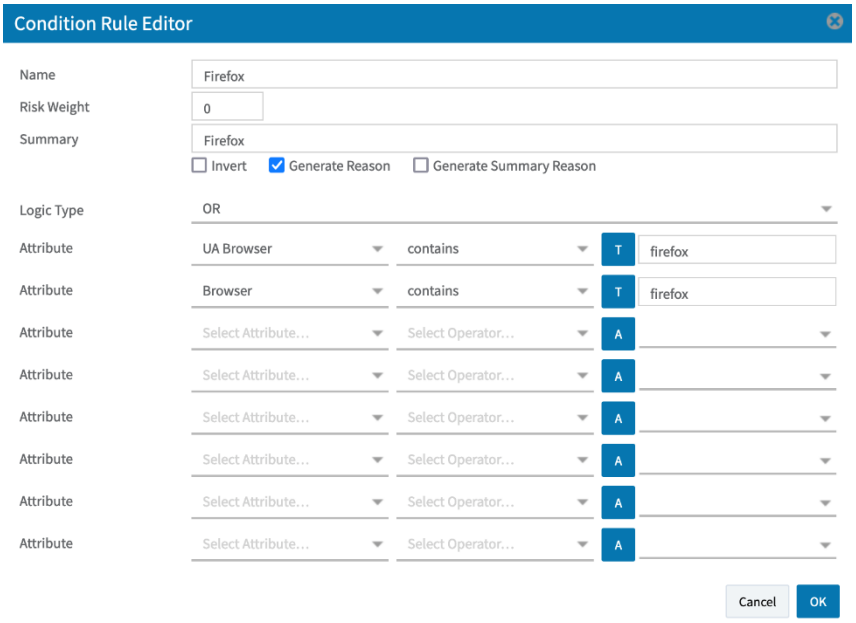
3. On the Policy Summary, the **Properties** interface tab will be displayed. Enter Policy Name = default, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



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.



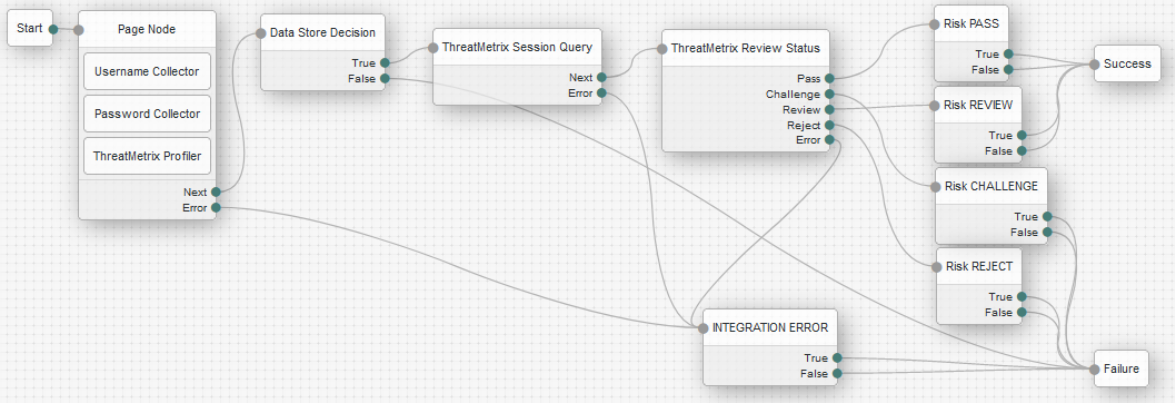
6. Save the policy.
7. Consult with ThreatMetrix services for a more comprehensive policy configuration.

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

FORGEROCK-THREATMETRIX AUTHENTICATION TREE

Authentication Tree: ThreatMetrix

This section provides the steps to configure a ForgeRock Authentication Tree with LexisNexis ThreatMetrix nodes from the marketplace. This section will create a ThreatMetrix authentication tree that performs device intelligence and profiling followed by a risk assessment via the ThreatMetrix session query. 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 ThreatMetrix Page Profiling
- Data Store decision, which is to validate the users credentials against the embedded OpenDJ local user directory as configured in the core settings
- 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

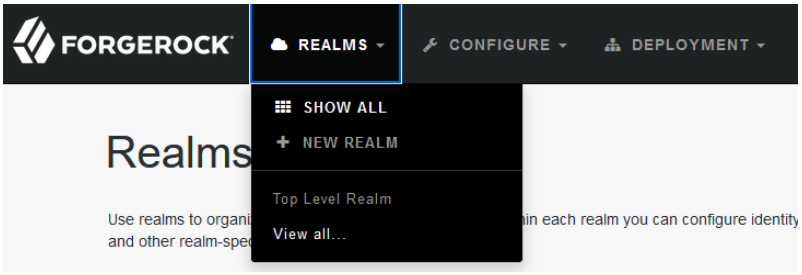
This configuration of the Authentication Tree occurs after the server has completed the core server settings. The steps here will establish the SSO Connection and Authentication Tree to be used for authentication of the user. Perform the following to configure the server:

1. From a workstation, launch a browser and enter the following URL:

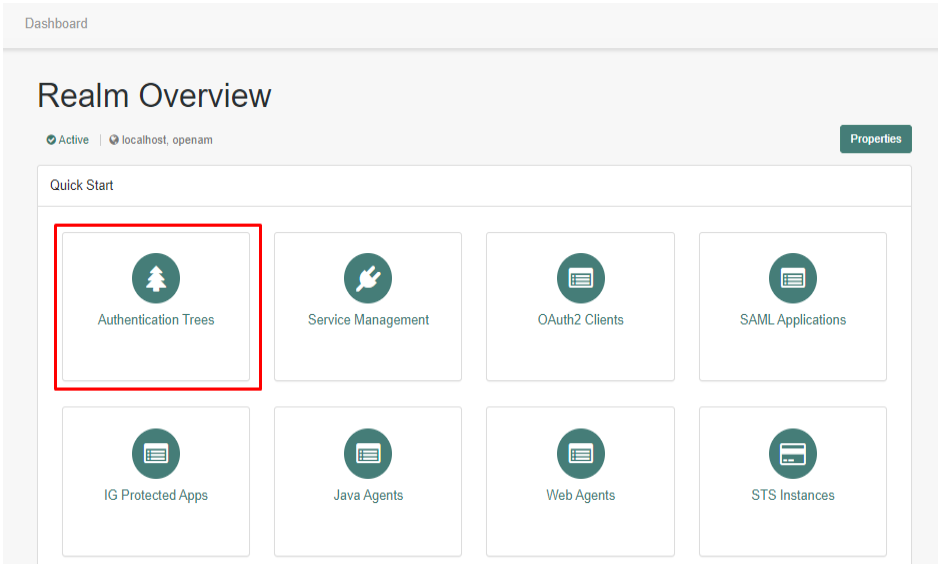
   `https://<SSO-SVR-NAME>:<SSO-SVR-HTTPS-PORT>/openam`

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

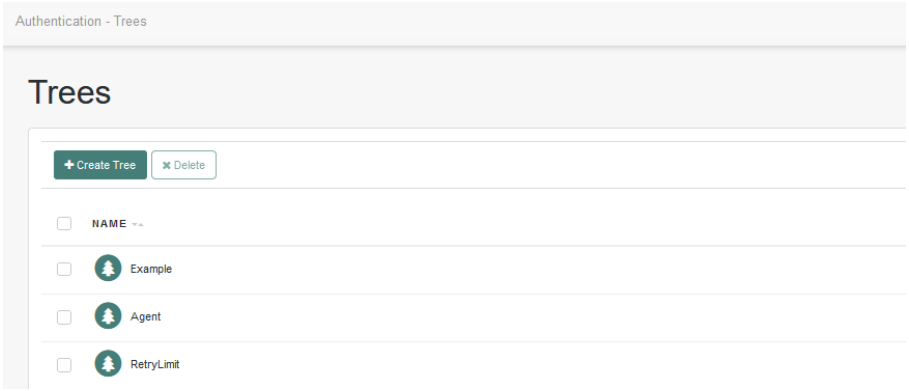
2. Login with amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.



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

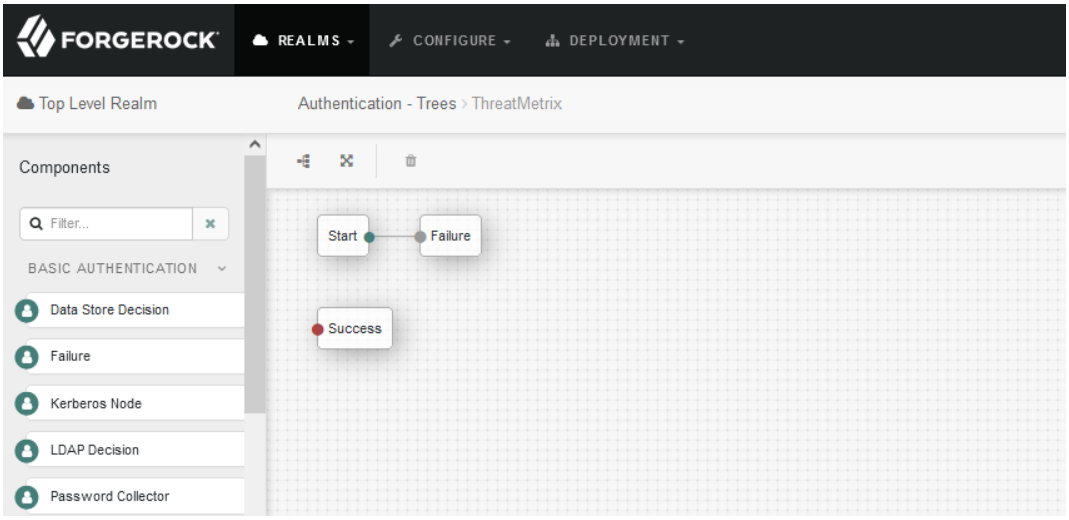


5. On the **Authentication Trees** display, click the **Create Tree** tile.



6. On the **New Tree** display, enter “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.

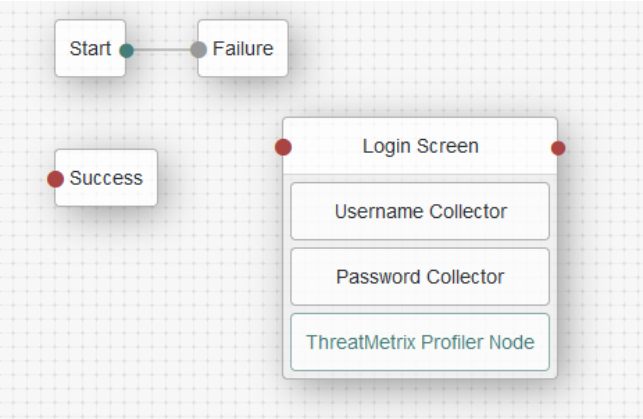


8. Build the Login Screen (e.g. Page Node), do the following:

- 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 **threatmetrix**. 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 Node
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 authentication tree. The data decisions for user credential binding will utilize the Identity Store configure, which is the local embedded OpenDJ. 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. These node will be used to display an integration error message from any of the nodes. Enter the following property values.

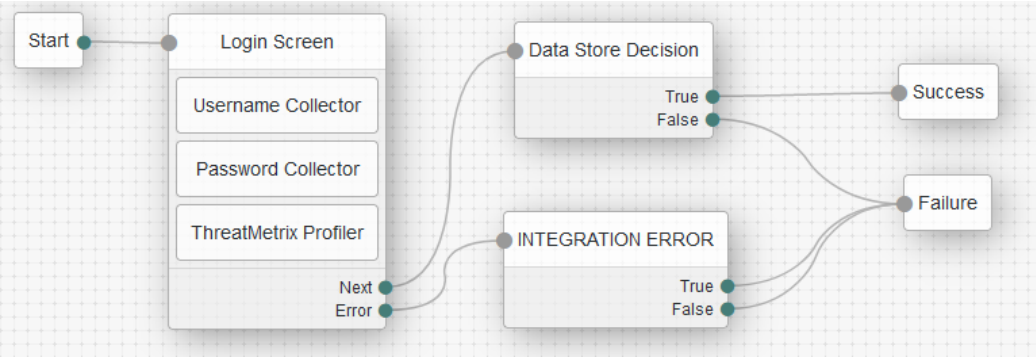
Node name	INTEGRATION ERROR
Message	(en_US) An integration error has occurred in the Auth Tree
Positive answer	(en_US) OK
Negative answer	(en_US) OK

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 embedded OpenDJ credential store. Using an incognito browser window, enter the following URL and test with the demo user as created in **Identities**.
> URL: https://<FGRK-DOMAIN>:<FGRK-PORT>/openam/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 Session 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 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 embedded OpenDJ 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 authentication tree. 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 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

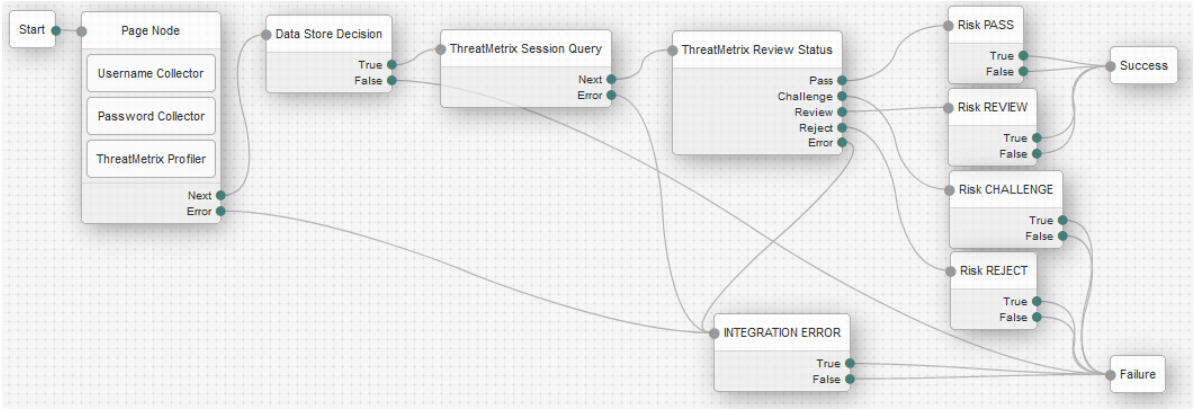
15. Link together the nodes of the authentication policy

- 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 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 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



Authentication Tree: TMX-StepUpOTP

This section provides the steps to configure a ForgeRock Authentication Tree 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 ThreatMetrix authentication tree 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 ThreatMetrix authentication tree 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.

1. From a workstation, launch a browser and navigate to the Access Manager 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 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 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 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>
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 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>
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 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.

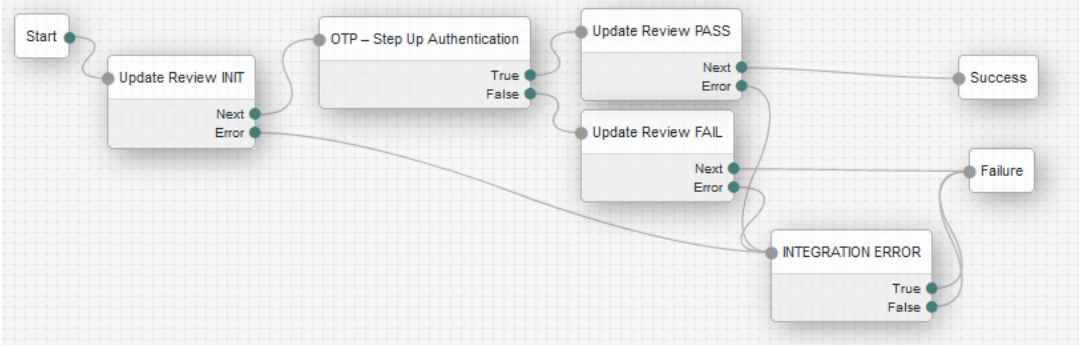
Node name	OTP – Step Up Authentication
Message	(en_US) OTP – Step Up Authentication
Positive answer	(en_US) Step Up PASS
Negative answer	(en_US) Step Up FAIL

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



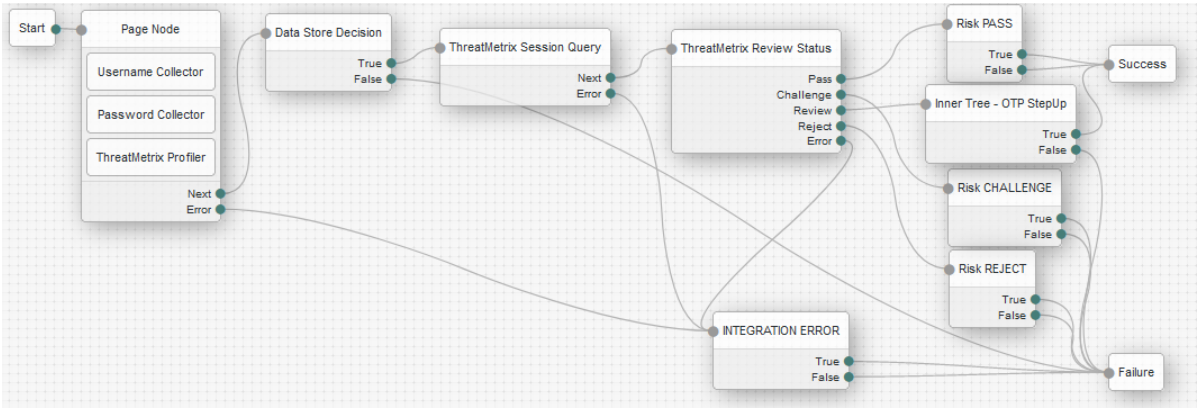
12. At this point the OTP Authentication Tree is ready to be called from any other ForgeRock Authentication Tree. Click **Save**.
13. To leverage the OTP flow from the Login authentication tree with ThreatMetrix, add an Inner Tree Evaluator node.
    - Open the Authentication Tree named ThreatMetrix
    - 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. Complete and ready for testing
    - To Using an incognito browser window, enter the following URL and test with the demo user as created in **Identities**.
      - URL: https://<FGRK-DOMAIN>:<FGRK-PORT>/openam/XUI/?realm=/&service=ThreatMetrix
      - EX: https://sso.threatmetrix.com:8443/openam/XUI/?realm=/&service=ThreatMetrix