Getting Started Guide

Configure ForgeRock with LexisNexis One-Time Passcode (OTP) Nodes

Guide for On Premise with Access Manager

Version 1.0

November 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 One-Time Passcode (OTP) 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, mobile phone, home phone, and login username
- An existing ForgeRock Authentication Tree is configured that can be modified to integrate the OTP Nodes as an Inner Tree Evaluator Node

Document Organization

This document is divided into four sections as follows:

- **Scope.** Defines the purpose of this document.
- **LexisNexis OTP Nodes**. Provides on overview of the nodes available for ForgeRock authentication tree integration.
- **Nodes Installation.** Provides information to install the LexisNexis OTP nodes upon an on-premise ForgeRock Access Management (AM) server.
- **LexisNexis Dynamic Decision Platform Portal.** Provides detailed information regarding the configuration of LexisNexis Dynamic Decision Platform (DDP) 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 OTP Nodes to perform Multi-Factor Authentication (MFA) in support of an existing ForgeRock journey tree.

LEXISNEXIS ONE-TIME PASSCODE NODES

The LexisNexis OTP Nodes are available in the Marketplace to be included within any new or existing ForgeRock authentication tree configurations. To include a LexisNexis OTP node in a journey, enter LexisNexis into the Filter nodes to get a listing of available capabilities. For OTP, the following nodes are available:

- LexisNexis OTP Sender
- LexisNexis OTP Collector
- LexisNexis OTP Decision

LexisNexis OTP Sender

This node will display a list of selections to the user for available methods to send an OTP code. LexisNexis OTP Nodes provide for email/OTP, SMS/OTP and voice/OTP. The methods displayed depend upon two factors, mainly whether the capability is activated in the node and secondarily if the attribute is available from the user directory for the specific user identity.

The LexisNexis OTP Sender does assume that the username is contained in shared state from a previous node in the authentication tree/journey. Specifically the attribute username as provided by ForgeRock Nodes (e.g. Username Collector). At runtime, the username will be used to query the user directory to fetch the attributes as configured in the node.

The LexisNexis OTP Sender Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated your organization on the Dynamic Decision Platform (DDP).
- **API Key** - This is the unique API key generated via DDP Portal associated to the Org ID.
- **OTP URL** - This is the URL for the DDP Authentication Hub API endpoint. The default URL is the Worldwide endpoint. This should be modified for specific regions such as EU, US or India.
- **Policy** - The DDP Portal policy to be used to integate the DDP Authentication Hub with OTP
- **OTP Length** - Length of the OTP
- **OTP Expire** - Expiration time in minutes for the OTP
- **Send Email** - Configuration toggle to enable/disable the method of delivery for Email/OTP
- **Email Title** - When Email/OTP is triggered, this will be the title of the email sent to the user
- **Email Message** -When Email/OTP is triggered, this will be the message body of the email
- **Email Attribute** - When Email/OTP is enabled, the attribute defined in this configuration parameter will be inspected in the user directory to pull the email address for sending OTP code at runtime. If the value is present, then the method will be displayed to the user, otherwise the method will not be displayed.
- **Send SMS Text** - Configuration toggle to enable/disable the method of delivery for SMS/OTP
- **SMS Message** - When SMS/OTP is triggered, this will be the message body of the SMS text message sent to the user

- **SMS Attribute** - When SMS/OTP is enabled, the attribute defined in this configuration parameter will be inspected in the user directory to pull the mobile phone number for sending OTP code at runtime. If the value is present, then the method will be displayed to the user, otherwise the method will not be displayed.
- **Send Voice** - Configuration toggle to enable/disable the method of delivery for Voice/OTP
- **Voice Attribute** - When Voice/OTP is enabled, the attribute defined in this configuration parameter will be inspected in the user directory to pull the user's phone number to call and convery the OTP code via automated voice. If the value is present, then the method will be displayed to the user, otherwise the method will not be displayed.

The LexisNexis OTP Sender Node has the following outcomes:

- **Success** - This outcome is triggered when the OTP code is successfully generated for the user. It is worth mention that generation does not guarantee delivery to the users device. Thus, the LexisNexis OTP Collector Node allows for retry in the event the user never receives the OTP code.
- **None Available** - This outcome is triggered when no OTP delivery methods are available for a user at runtime. This would mean that the attributes required at runtime are not configured for the user and would need to be provisioned.
- **API Error** - This outcome is triggered when there is an issue with the API Request such as a network timeout or the service is unavailable.
- **OTP Fail** - This outcome is triggered when the API Request is rejected by the LexisNexis DDP Authentication Hub service. Within the debug logging for the node, the actual error codes will be written for offline analysis and triage of the issue.
- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

LexisNexis OTP Collector

This node collects the OTP code sent to the user. The interface allows for submitting a OTP code for decision and validation, as well as the user can request the OTP code to be resent.

The LexisNexis OTP Collector Node has the following configuration parameters:

- **Message Body** - This is the message displayed to the user on the collector interface. The variable ${otpDestination} will contain either a email address or phone number depending on the method selected by the user via the Lexis OTP Sender.
- **Help Text** - This is the help text displayed in the OTP text entry box for the user.
- **OTP Error Message** - Message displayed if user enters an incorrect OTP code
- **OTP Blank Message** - Message displayed if user attempts to submit a blank OTP code

The LexisNexis OTP Collector Node has the following outcomes:

- **Submit** - This outcome is triggered when the user selects the "Submit" button. When selected, this should then link to the LexisNexis OTP Decision node to validate the OTP Code being submitted. IF the LexisNexis OTP Decision node detects a blank or invalid OTP code, then this node will be linked and the appropriate message will be displayed. The outcomes review and challenge from the LexisNexis OTP Decision are to link back to the LexisNexis OTP Collector.
- **Retry** - This outcome is triggered when the user wants to get a new OTP code by selecting the "Retry" button on the interface.
- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

LexisNexis OTP Decision

This node verifies OTP codes entered by the user. In a typical authentication tree, the LexisNexis OTP Collector will precede this node. The collector places the user entered and submitted OTP in shared state. Additionally, the LexisNexis OTP Sender will precede this node and the LexisNexis Collector Node that places the characteristics of the type of OTP into shared state.

The LexisNexis OTP Decision Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated your organization on DDP.
- **API Key** - This is the unique API key generated via DDP Portal associated to the Org ID.

The LexisNexis OTP Decision Node has the following outcomes:

- **Pass** - This outcome is triggered when the OTP code submitted by the user is validated so that MFA via OTP has passed.
- **Challenge** - This outcome is triggered when the OTP code fails to validate, and the number of retires has not been violated.
- **Review** - This outcome is triggered when the OTP code fails to validate due to blank OTP code entered.
- **Reject** - This outcome is triggered when OTP code validation is failed.
- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

NODES INSTALLATION

This section describes how to deploy the LexisNexis OTP 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 LexisNexis OTP Nodes from the server:

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

   Filename: `lexisnexis-otp-1.0.0.jar`

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

DYNAMIC DECISION PLATFORM PORTAL CONFIGURATION

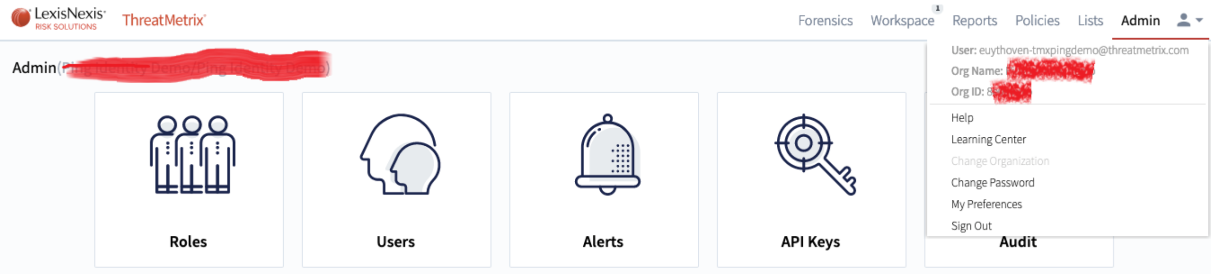
This section defines the high-level LexisNexis Dynamic Decision Platform (DDP) Portal configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- Organization ID and API Key for the REST API interfaces. This information is needed by the LexisNexis OTP Nodes and will be entered as part of configuration.
- LexisNexis DDP Portal Policy. The configured policy within DDP provides the configuration for the Authentication Hub to access OTP services. For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the "OTP" policy will be configured to directly integrate the Authentication Hub without any further policy rules.

Retrieve OrgID and API Key

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

1. Access **DDP Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis.
2. From the **DDP 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 OTP Nodes.



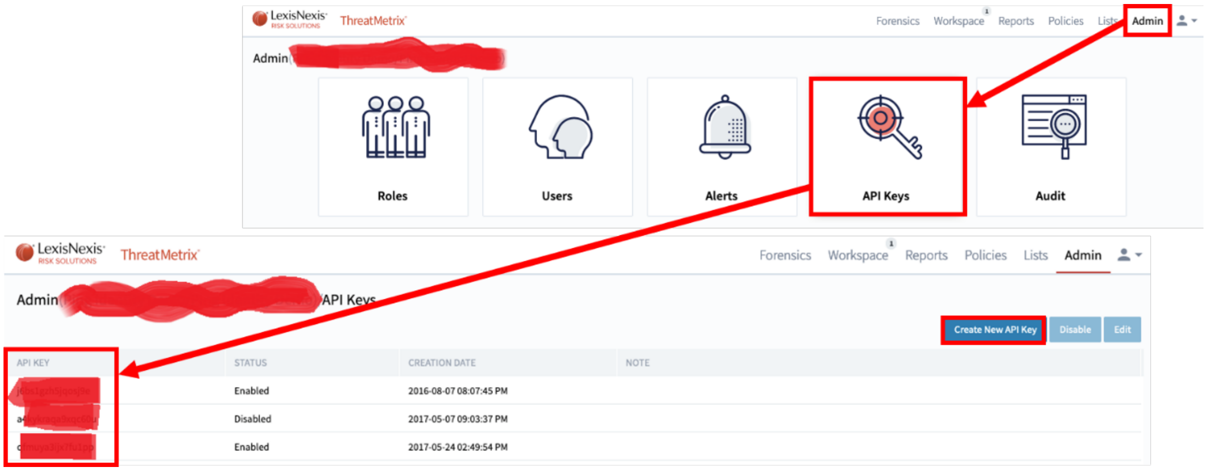
Admin([redacted]

User: euythoven-tmxpingdemo@threatmetrix.com

Org Name: [redacted]

Org ID: [redacted]

3. Within the **DDP 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 OTP Nodes. The API Key is to be protected. Do not email or keep this value in cleartext on any computer system.



Admin [redacted]

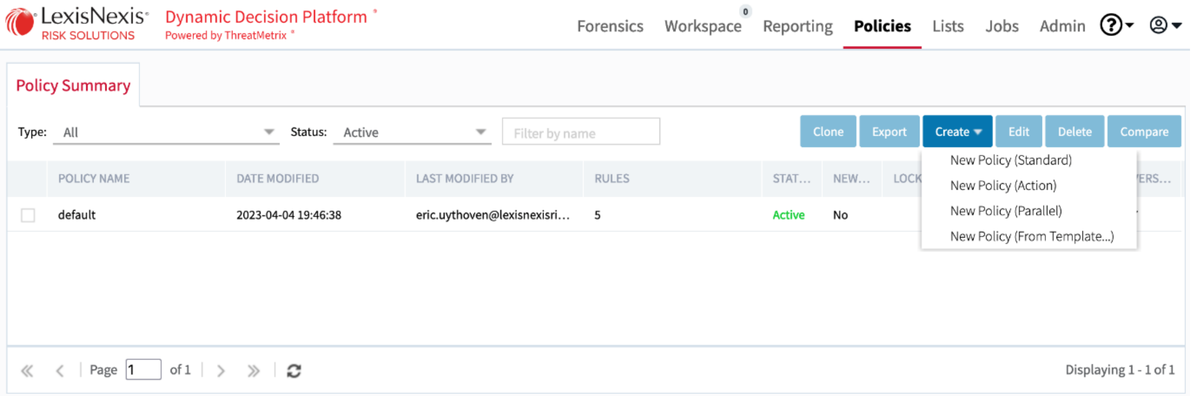
Admin [redacted] /API Keys

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	

Dynamic Decision Platform Portal Policy

For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the "OTP" policy will be configured to directly integrate the Authentication Hub without any further policy rules. Perform the following steps.

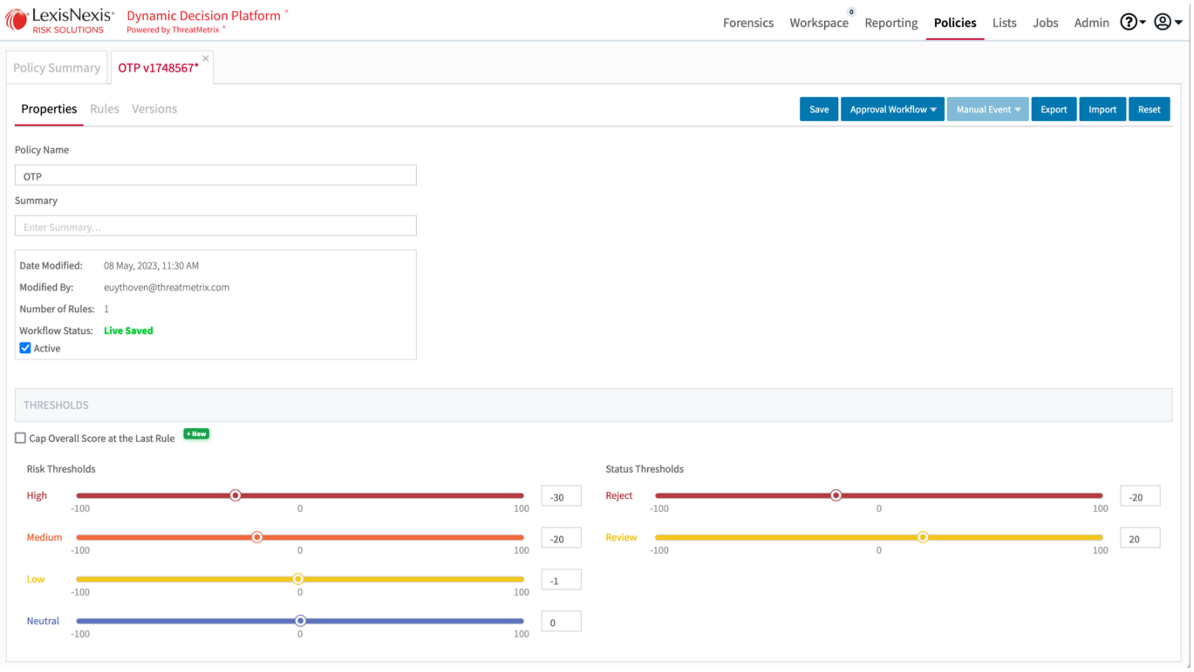
1. Access **DDP Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis.
2. From the **DDP Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies that can be configured with the LexisNexis OTP Nodes. The first step is to select the **Create** dropdown menu followed by **New Policy (Standard)**.



Type: All Status: Active Filter by name

	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 = OTP, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



Policy Name: OTP

Summary: Enter Summary...

Date Modified: 08 May, 2023, 11:30 AM
Modified By: euythoven@threatmetrix.com
Number of Rules: 1
Workflow Status: Live Saved
☑ Active

□ Cap Overall Score at the Last Rule

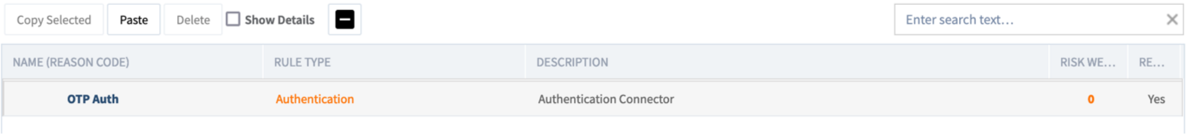
Risk Thresholds

High	-30
Medium	-20
Low	-1
Neutral	0

Status Thresholds

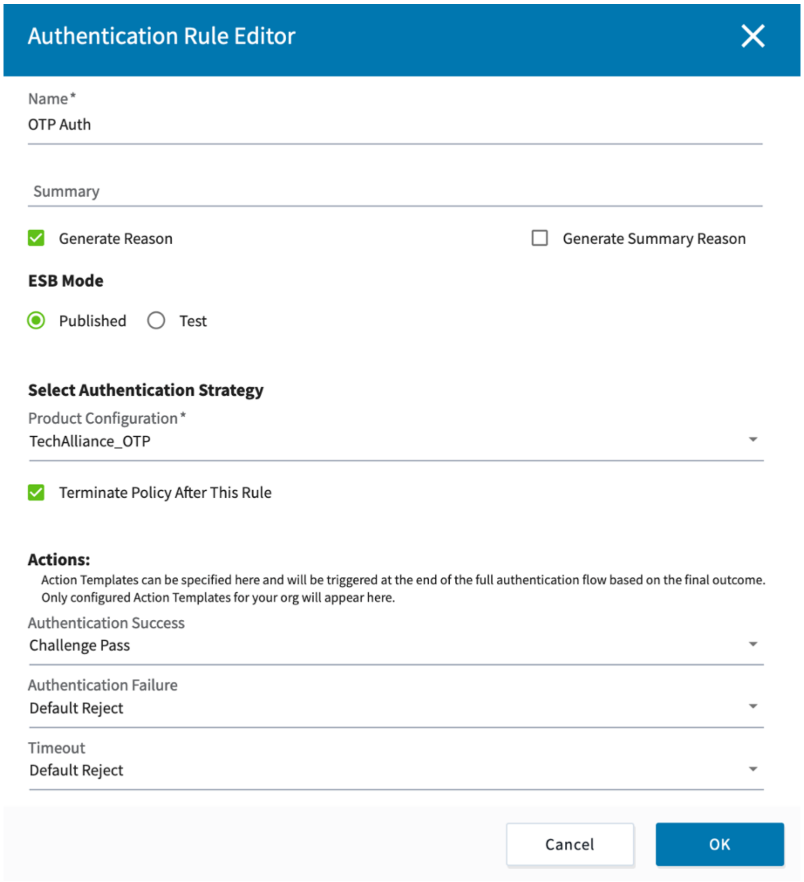
Reject	-20
Review	20

4. To create the policy rules, select the **Rules** interface tab. The OTP policy will be a single **Authentication** rule to integrate the Authentication Hub as follows.



NAME (REASON CODE)	RULE TYPE	DESCRIPTION	RISK WE…	RE…
OTP Auth	Authentication	Authentication Connector	0	Yes

5. The **Authentication Rule Editor** can follow the template shown here. Within this interface, the **Product Configuration** is the Authentication Hub configuration that is established via LexisNexis ThreatMetrix Professional Services. The services configure the LexisNexis OTP service as an interface associated to the customer account.



Authentication Rule Editor

Name*
OTP Auth

Summary

☑ Generate Reason □ Generate Summary Reason

ESB Mode

● Published ○ Test

Select Authentication Strategy

Product Configuration*
TechAlliance_OTP

☑ Terminate Policy After This Rule

Actions:
Action Templates can be specified here and will be triggered at the end of the full authentication flow based on the final outcome. Only configured Action Templates for your org will appear here.

Authentication Success
Challenge Pass

Authentication Failure
Default Reject

Timeout
Default Reject

6. Save the policy.

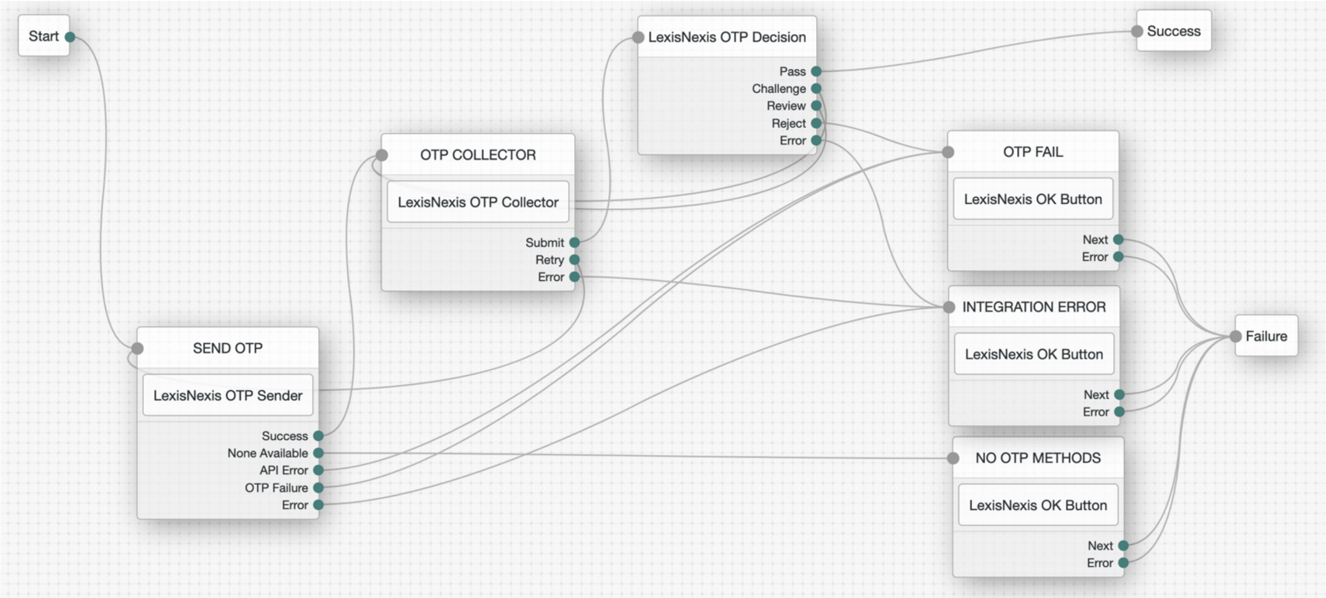
7. Consult with LexisNexis ThreatMetrix services for a more comprehensive policy configuration.

FORGEROCK-LEXISNEXIS AUTHENTICATION TREE

Authentication Tree: LNRS-StepUp-OTP

This section provides the steps to configure a ForgeRock Authentication Tree with LexisNexis OTP nodes from the marketplace.

LexisNexis OTP Nodes are used for Identity proofing as well as a multi-factor authentication (MFA) of a user. The workflow starts with the LexisNexis OTP Sender node that has a dependency upon the attribute “username” being in shared state from another authentication tree workflow. The orchestration allows the user to define the method of OTP delivery, generate the OTP code, enter the OTP code and submit for validation.



The flow is as follows:

- Page Node to display the OTP Method selection interface using the LexisNexis OTP Sender Node
- Page Node to display the OTP Collection interface using the LexisNexis OTP Collector Node
- LexisNexis OTP Decision Node to determine if the OTP collected from the user is valid
- Page Nodes with messages and a single OK button that will display the results and/or error conditions

To configure the Authentication Tree, perform the following to configure the server:

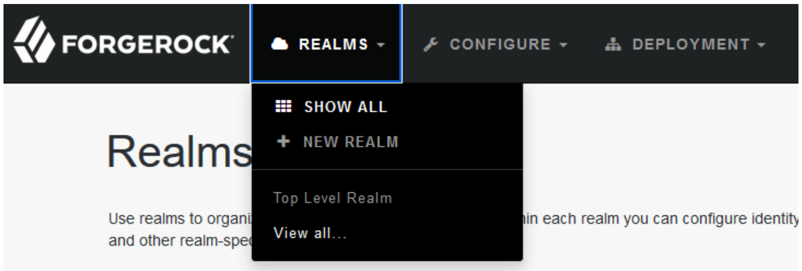
1. From a workstation, launch a browser and enter the following URL:

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

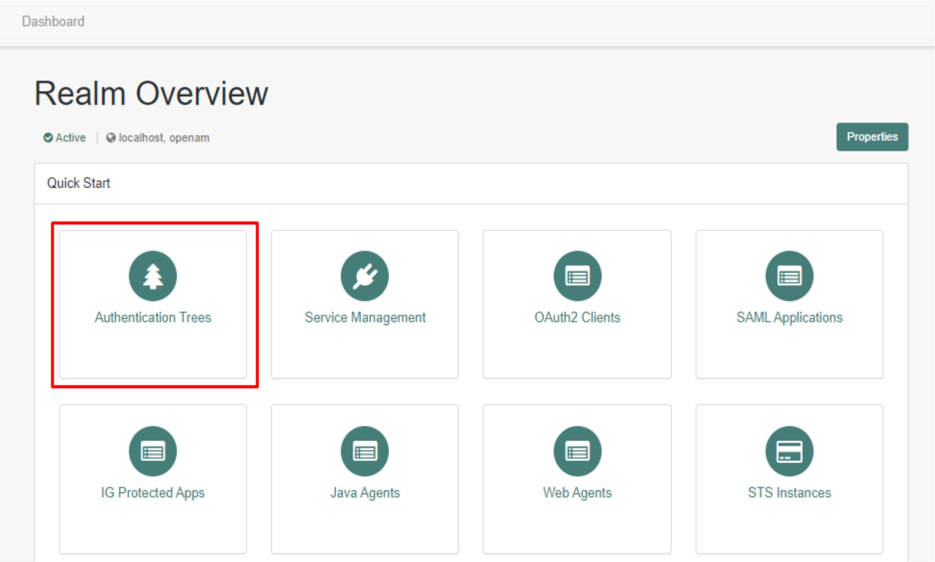
   Example: `https://sso.threatmetrix.com:8443/openam`

2. Login with amadmin and credentials

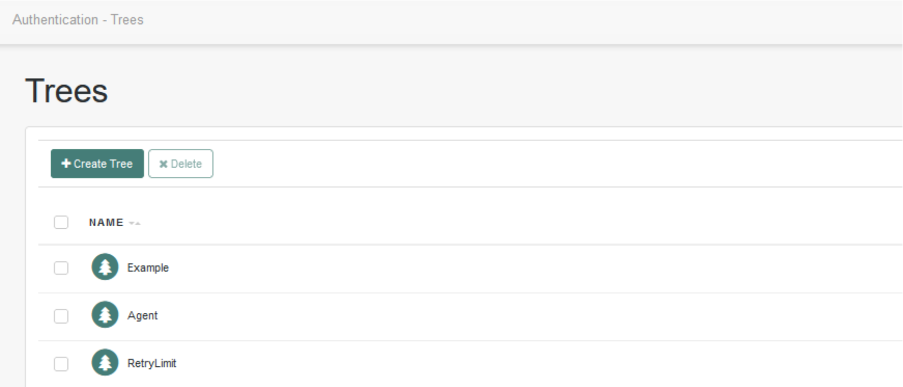
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.



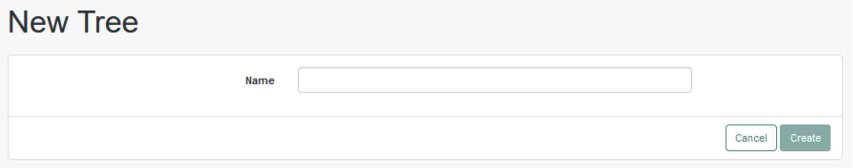
4. On the **Realm Overview** display, click the **Authentication Trees** tile.



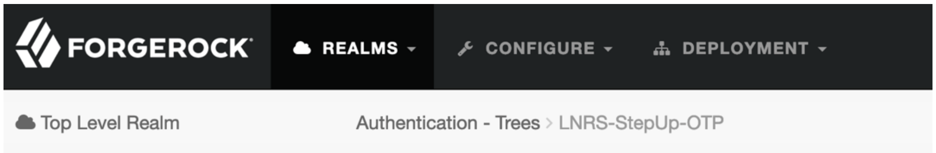
5. On the **Authentication Trees** display, click the **Create Tree** tile.



6. On the **New Tree** display, enter “LNRS-StepUp-OTP” followed by the **Create** button.



7. The result is the **Authentication Trees > LNRS-StepUp-OTP** 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 OTP Method Selection 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 the following property values:

Node name	SEND OTP
Page Header	We do not recognize this device
Page Description	We will send you a one time passcode. Please choose a delivery method.

- On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis OTP Sender** is displayed as a component, drag and drop it into the authentication tree into the **SEND OTP** page node.
- Select the **LexisNexis OTP Sender** Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>
OTP URL	https://h-api.online-metrix.net/authentication/v1/otp/
Policy	OTP [NOTE: This is the configured policy name in DDP Portal]
OTP Length	6
OTP Expire	3
Send Email	Toggle as needed [NOTE: This activates email as a method]
Email Title	Please, check out this email! It's your one time passcode.
Email Message	Your One Time Password is ${OTP}.${LineBreak}We will never call you for this code.${LineBreak}Your passcode will expire in ${ExpirePeriod} minutes.
Email Attribute	mail [NOTE: This is the OpenDJ attribute]
Send SMS	Toggle as needed [NOTE: This activates SMS Text as a method]
SMS Message	Your One Time Password is ${OTP}.${LineBreak}We will never call you for this code.${LineBreak}Your passcode will expire in ${ExpirePeriod} minutes.
SMS Attribute	telephoneNumber [NOTE: This is the OpenDJ attribute]
Send Voice	Toggle as needed [NOTE: This activates voice call as a method]
Voice Attribute	phone [NOTE: This is the OpenDJ attribute]

> **Note:** The toggles for the delivery methods are selected by the customer as methods to allow for all users to perform Multi-Factor Authentication via the LexisNexis OTP Nodes. At runtime, the attribute defined will be inspected for a valid value, which if present will display the OTP method to the user. If the attribute is null, then the method will not be displayed. The outcome “None Available” will trigger if all attributes are null for the selected methods.

> **Note:** The outcome API Error means that an issue occurred with the API request, such as API timeout or a service unavailable over the internet. The outcome OTP Failure means that the API Request was rejected by the LexisNexis DDP Authentication Hub service.

9. Build the OTP Collector 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 the following property values:

Node name	OTP COLLECTOR
Page Header	We do not recognize this device
Page Description	Please enter your one-time passcode.

    - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis OTP Collector** is displayed as a component, drag and drop it into the authentication tree into the **OTP COLLECTOR** page node.
    - Select the **LexisNexis OTP Collector** Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Message Body	Passcode was sent to ${otpDestination}. Please enter it below.
Help Text	One Time Passcode
OTP Error Message	Incorrect passcode entered, please try again.
OTP Blank Message	Blank passcode entered, please try again.

10. Build the OTP Decision, do the following:
    - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis OTP Decision** is displayed as a component, drag and drop it into the authentication tree into the authentication tree.
    - Select the **LexisNexis OTP Decision** Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Org ID	<ENTER ORG ID FROM TMX PORTAL>
API Key	<ENTER API KEY FROM TMX PORTAL>

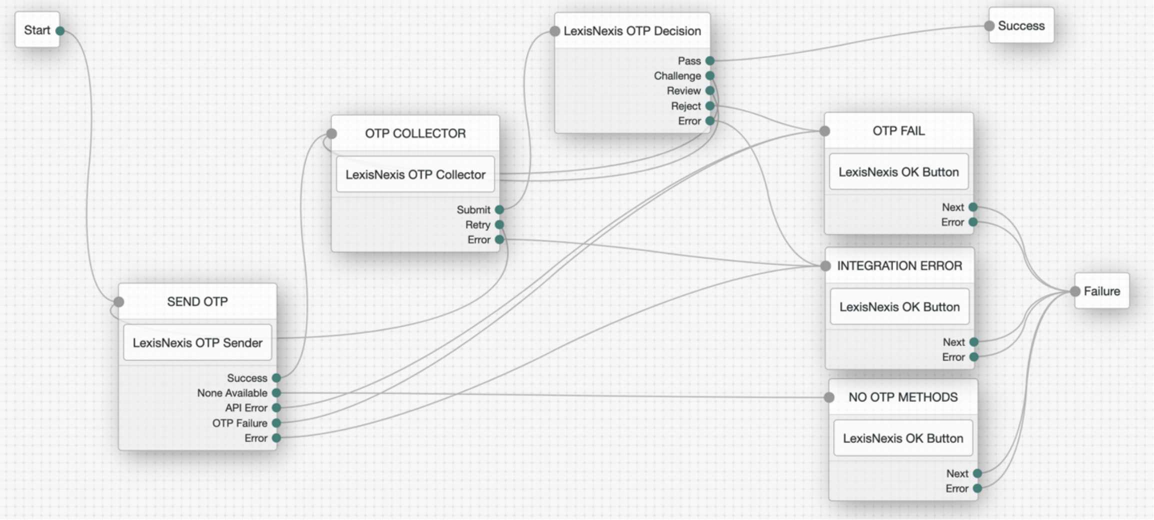
11. Build Message Nodes for OTP Failure, No OTP Methods, and Integration Error to support testing. This can be accomplished with Message Nodes or Page Nodes with an OK Button Node. The nodes are meant to display outcomes to the user.

12. Link together the nodes of the authentication tree

    - 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	SEND OTP
SEND OTP (Success)	OTP COLLECTOR
SEND OTP (None Available)	NO OTP METHODS
SEND OTP (API Error)	OTP FAIL
SEND OTP (OTP Failure)	OTP FAIL
SEND OTP (Error)	INTEGRATION ERROR
OTP COLLECTOR (Submit)	LexisNexis OTP Decision
OTP COLLECTOR (Retry)	SEND OTP
OTP COLLECTOR (Error)	INTEGRATION ERROR
LexisNexis OTP Decision (Pass)	Success
LexisNexis OTP Decision (Challenge)	OTP COLLECTOR
LexisNexis OTP Decision (Review)	OTP COLLECTOR
LexisNexis OTP Decision (Reject)	OTP FAIL
LexisNexis OTP Decision (Error)	INTEGRATION ERROR
NO OTP METHODS (Next)	Failure
NO OTP METHODS (Error)	Failure
OTP FAIL (Next)	Failure
OTP FAIL (Error)	Failure
INTEGRATION ERROR (Next)	Failure
INTEGRATION ERROR (Error)	Failure

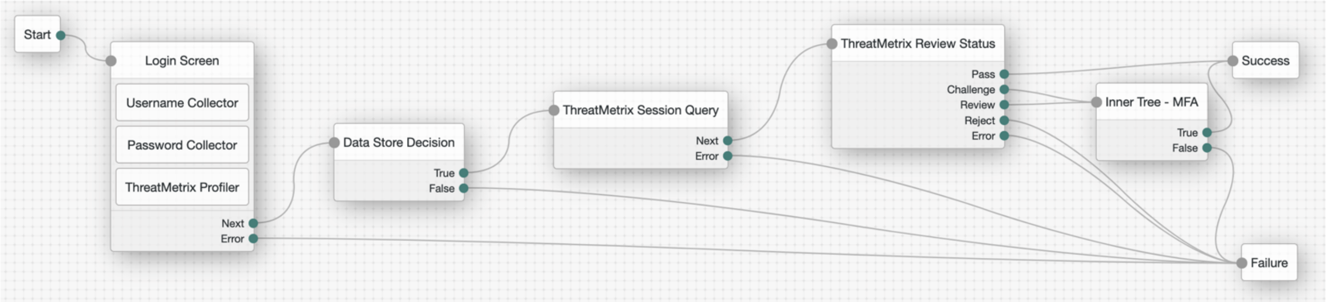
    - At this point you should have the following



Authentication Tree: Integrate OTP into Existing Workflow

One-Time Passcode (OTP) technology is typically used to augment an orchestration for Identity Proofing or user MFA. The authentication tree in the section **Authentication Tree: LNRS-StepUp-OTP** provides an example of the OTP workflow, which is an orchestrated workflow where the LexisNexis OTP Sender node has a dependency upon the attribute "username" being in shared state.

One typical use case for OTP is to integrate the nodes for step-up authentication following a risk assessment where the policy has rated the user as potential level of risk, thus requiring a second factor (e.g. step-up) authentication. Within ForgeRock authentication trees, this can be accomplished by inserting an Inner Tree Evaluator Node. In the example depicted below, there is a first factor authentication performed using the ForgeRock username/password collectors with a decision node, as well as LexisNexis ThreatMetrix Risk Assessment. The Inner Tree Evaluator Node is configured to handle risk assessment with an outcome of review or challenge.



For the purposes of brevity, the entire login workflow authentication tree will not be documented here, rather a simple documentation of the inner tree evaluator to integrate the LNRS-StepUp-OTP tree from the previous section.

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, select the existing authentication tree to modify.
6. To leverage the OTP authentication tree, add an Inner Tree Evaluator node.
   - 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.

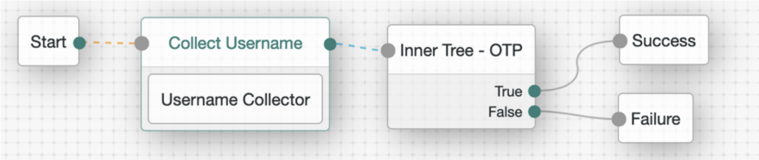
Node name	Inner Tree - MFA
Tree Name	LNRS-StepUp-OTP

   - Connect the nodes of the authentication tree and save the authentication tree.

Authentication Tree: Simple OTP Authentication

One-Time Passcode (OTP) technology is typically used to augment an orchestration for Identity Proofing or user MFA. The authentication tree in the section **Authentication Tree: LNRS-StepUp-OTP** provides an example of the OTP workflow, which is an orchestrated workflow where the LexisNexis OTP Sender node has a dependency upon the attribute “username” being in shared state.

A simple framework to exercise the authentication tree is to configure a page node with a username collector which will fulfill the dependency to have the attribute “username” being in shared state. Then an Inner Tree Evaluator Node can integrate the OTP journey/tree for a final outcome of authentication.



Perform the following.

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 “Login-OTP” followed by the **Create** button.
7. Build the Collector Username 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 the following property values:

Node name	Collect Username
Page Header	OTP Authentication

    - 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.
8. To leverage the OTP authentication tree, add an Inner Tree Evaluator node.
    - 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 - MFA
Tree Name	LNRS-StepUp-OTP

    - Connect the nodes of the authentication tree and save the authentication tree.