Getting Started Guide

Configure Ping Access Management (PingAM) / ForgeRock Access Management with LexisNexis One-Time Passcode (OTP) Nodes

Version 1.1.2

December 2025

LexisNexis®
RISK SOLUTIONS

Table of Contents

SCOPE

LexisNexis Risk Solutions (LNRS) Dynamic Decision Platform (DDP) hosts the Authentication Hub's one-time passcode (OTP) product. LexisNexis OTP is an out-of-band authentication method that provides business and government organizations the ability to have stronger authentication during a high risk, high value transaction with a customer. 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 OTP 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, mobile phone, home phone, and login username, which is used when testing the OTP attribute source configured for user directory.

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 authentication tree integration.
- **LexisNexis Nodes Installation.** Provides information to install the LexisNexis OTP nodes upon an on-premise PingAM / ForgeRock Access Management 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 authentication tree.
- **Authentication Tree Configuration.** Provides detailed steps to configure an authentication tree with LexisNexis OTP Nodes to perform Multi-Factor Authentication (MFA).

LEXISNEXIS ONE-TIME PASSCODE NODES OVERVIEW

LexisNexis One Time Password is an out-of-band authentication method that provides business and government organizations the ability to have stronger authentication during a high risk, high value transaction with a customer. It offers a time-sensitive, unique random passcode via SMS text, email or phone and is ideal for companies that are interested in providing a multi-factor authentication solution for their customers. No hardware (electronic fob, etc.) other than the user's existing phone or personal computer is required.

To include a LexisNexis OTP node in an authentication tree, enter LexisNexis into the Filter nodes to get a listing of available capabilities. For OTP, the following nodes are available:

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

LexisNexis OTP Selector

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. Upon user selection, the node will place the selected value into shared state variable `otp_type_select`. By default, this is the shared state variable that the LexisNexis OTP Send node accepts to determine which type of OTP to send to the end user. If only a single OTP type is configured, the node just sends the otp_type_select without any user interaction.

The LexisNexis OTP Selector node has the following configuration parameters:

- **Send Email** - When selected, this will display an Email Button on the selector interface.
- **Send SMS** - When selected, this will display an SMS Button on the selector interface.
- **Send Voice** - When selected, this will display an Voice Button on the selector interface.

The LexisNexis OTP Selector node has the following outcomes:

- **Success** - This outcome is triggered when a valid OTP Type is selected by the user.
- **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 Risk Solutions.

LexisNexis OTP Sender

This node will send an API request to the LexisNexis Dynamic Decision Platform (DDP) authentication hub to send an OTP code to the end user. The node will inspect shared state for `username` and `otp_type_select`. This combination of information defines the type of OTP to send to the defined user. The configuration of the node will define how additional attributes for the API request are fulfilled.

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.
- **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.
- **Policy** - The DDP Portal policy to be used to integrate the DDP Authentication Hub with OTP
- **OTP Length** - Length of the OTP. Valid values are between 6 and 10 characters.
- **OTP Expire** - Expiration time in minutes for the OTP. Valid values are between 1 and 60 minutes.
- **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
- **SMS Message** - When SMS/OTP is triggered, this will be the message body of the SMS text message sent to the user. The SMS message has a maximum length of 160 characters.
- **Attribute Source** - Defines where the attributes for sending the OTP code is fetched at runtime. This is a dropdown list that contains the options User Directory and Shared State. User Directory will look for attribute in the Identity Store, and Shared State looks in the shared memory.
- **Email Attribute** - When Email/OTP is defined by the OTP Type, the attribute defined in this configuration parameter will be fetched by the name of the attribute provided based on the Attribute Source defined.
- **SMS Attribute** - When SMS/OTP is defined by the OTP Type, the attribute defined in this configuration parameter will be fetched by the name of the attribute provided based on the Attribute Source defined.
- **Voice Attribute** - When Voice/OTP is defined by the OTP Type, the attribute defined in this configuration parameter will be fetched by the name of the attribute provided based on the Attribute Source defined.

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.
- **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 Risk Solutions.

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 an 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 Risk Solutions.

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 Risk Solutions.

NODES INSTALLATION

This section describes how to deploy the LexisNexis OTP 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 a Apache 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-1.1.0.jar`

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

The latest release of the LexisNexis OTP Nodes does have new configuration parameters that differ from the previous version 1.0.0 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.

DYNAMIC DECISION PLATFORM PORTAL CONFIGURATION

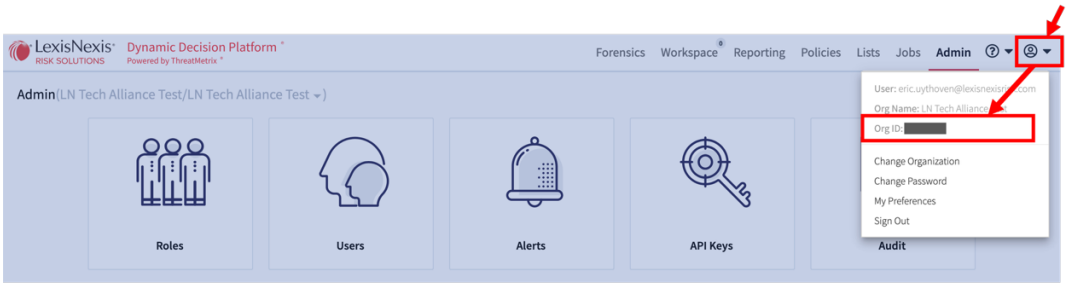
This section defines the high-level LexisNexis Dynamic Decision Platform (DDP) Portal configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- 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.

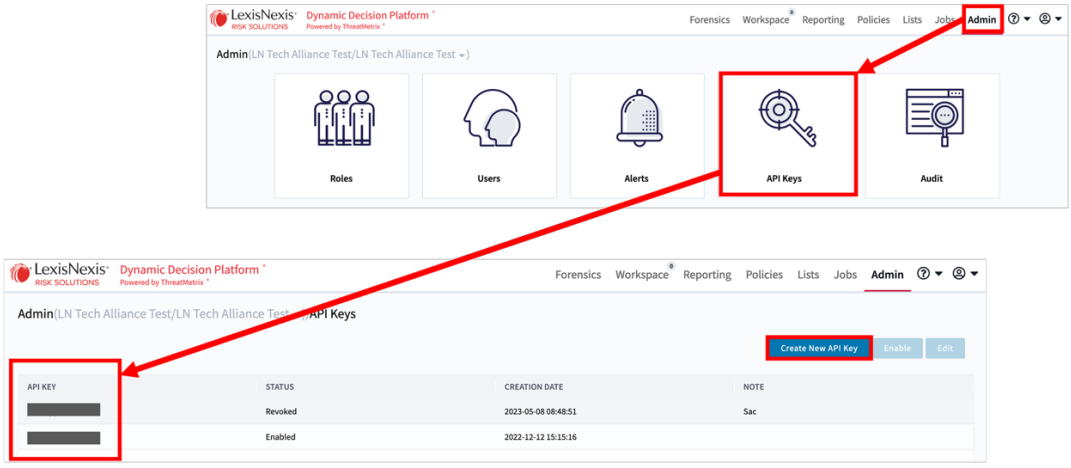
Retrieve OrgID and API Key

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 Risk Solutions.
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.



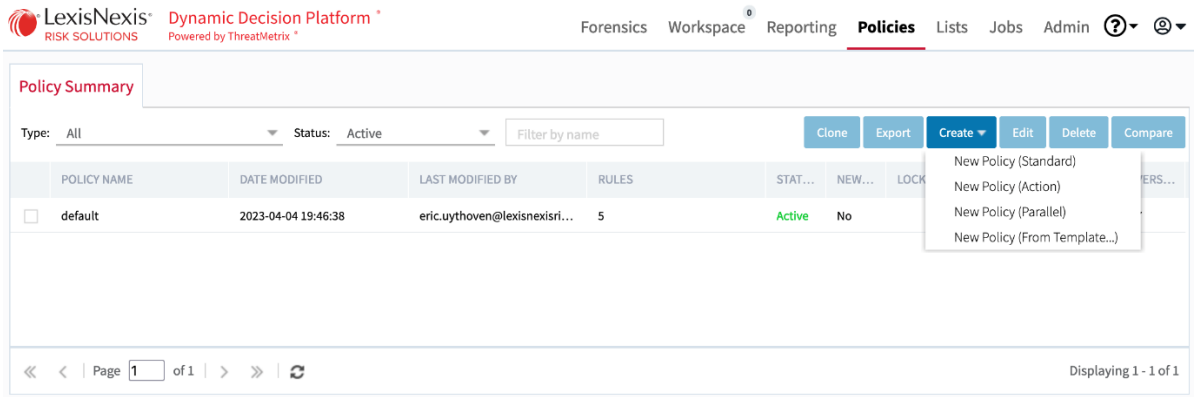
3. Within the **DDP Portal** home page, select **Admin** followed by selecting the **API Keys** tile. Retrieve the value for API Key. In the event no API Key is listed, select the **Create New API Key** button to generate a new key. This will be the API Key to enter into the configuration of the LexisNexis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



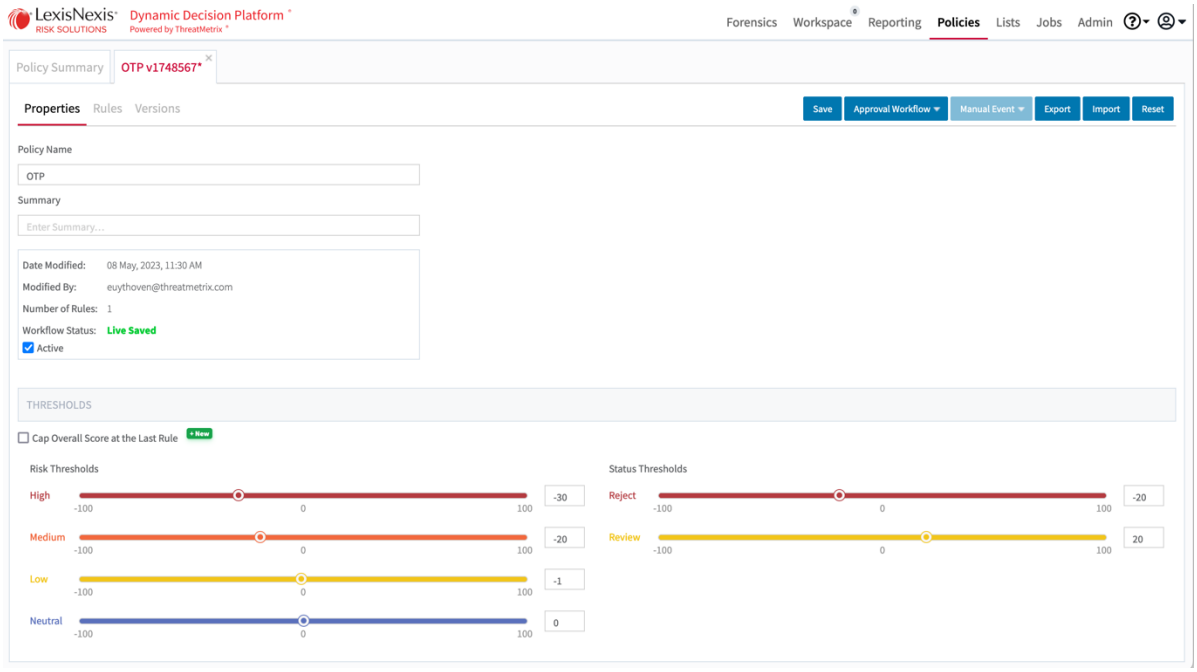
Dynamic Decision Platform Portal Policy

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.

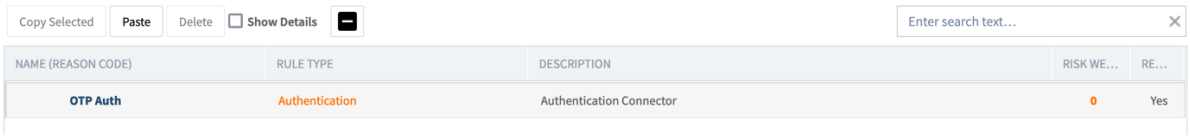
1. Access **DDP Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis.
2. From the **DDP Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies that can be configured with the LexisNexis OTP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



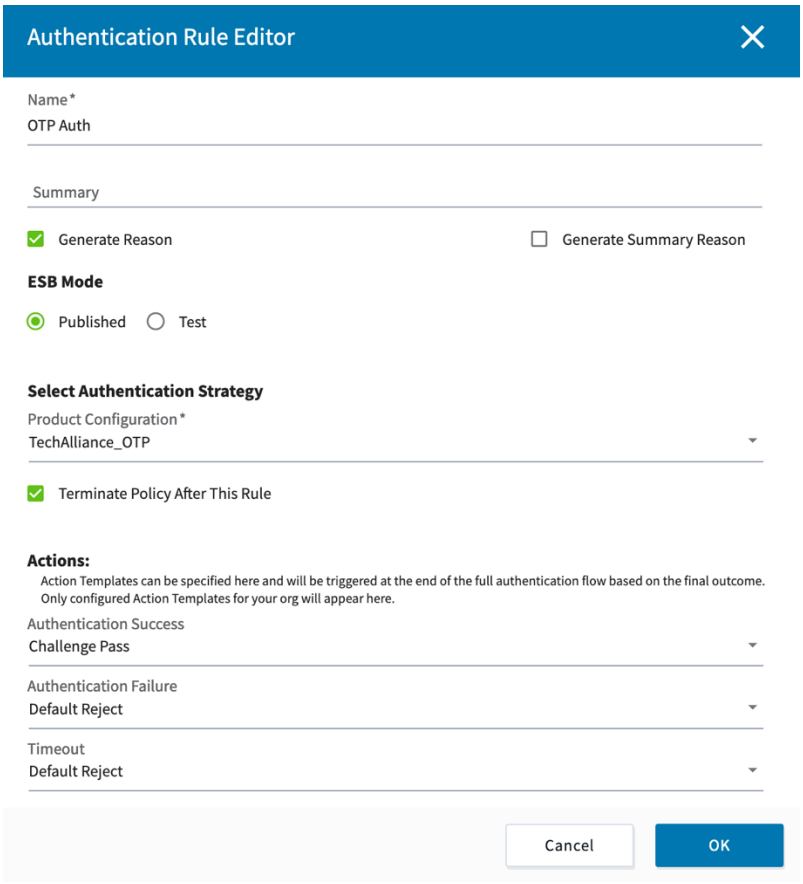
3. On the Policy Summary, the **Properties** interface tab will be displayed. Enter Policy Name = OTP, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



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.



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 Professional Services. The services configure the LexisNexis OTP service as an interface associated to the customer account.

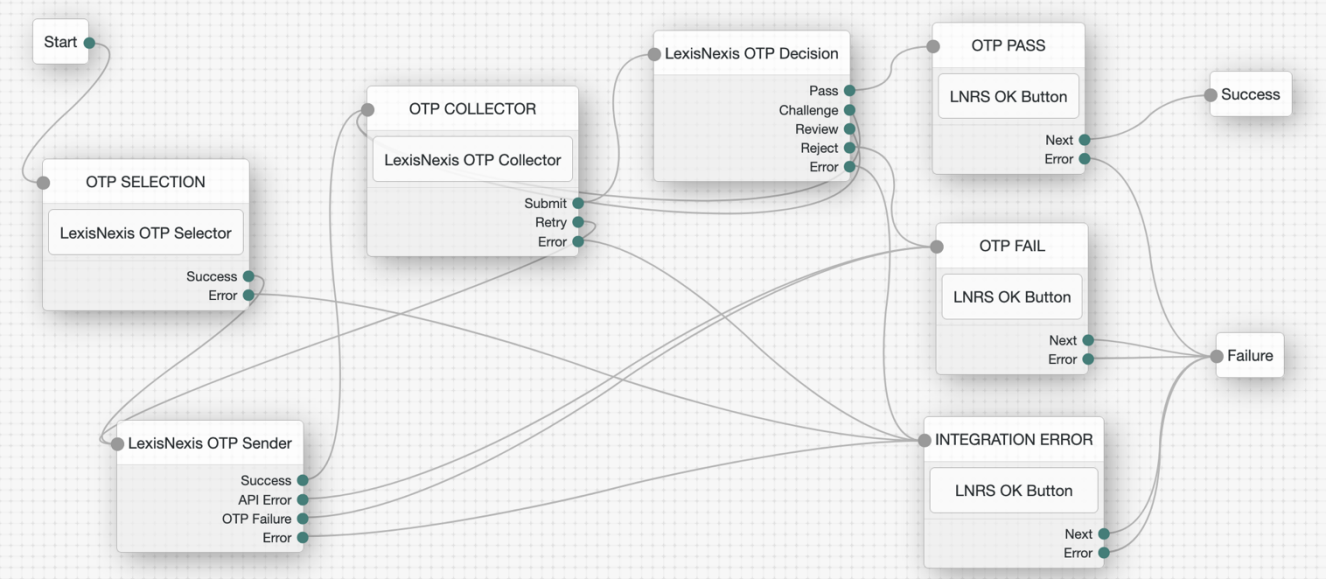


6. Save the policy.
7. Consult with LexisNexis professional services for a more comprehensive policy configuration.

AUTHENTICATION TREE CONFIGURATION

Authentication Tree: LNRS-StepUp-OTP

This section provides the steps to configure a PingAM / 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. This example workflow displays the OTP Selector to the user, sends the OTP code, collects the OTP code value from the user and then validates if the value is correct.



The flow is as follows:

- Page Node to display the OTP selection interface using the LexisNexis OTP Selector node. This configuration wraps the selector with page node so that detailed messages can be displayed to the user as part of the interface. Success from the selector will place the variable `otp_type_select` into shared state.
- LexisNexis OTP Sender node will generate the OTP code to the end user. This node will inspect shared state for `username` and `otp_type_select`. This combination of information defines the type of OTP to send to the defined user. The configuration of the node will define how additional attributes for the API request are fulfilled. For example, if the OTP type is email, then the Email Attribute will be fetched from either the User Directory or Shared state based on the configuration of the Attribute Source.
- Page Node to display the OTP Collection interface using the LexisNexis OTP Collector Node. This configuration wraps the selector with page node so that detailed messages can be displays to the user as part of the interface.
- 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.

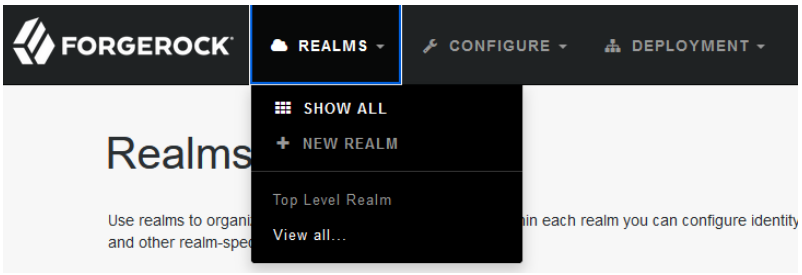
To configure the Authentication Tree, perform the following to configure the server:

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

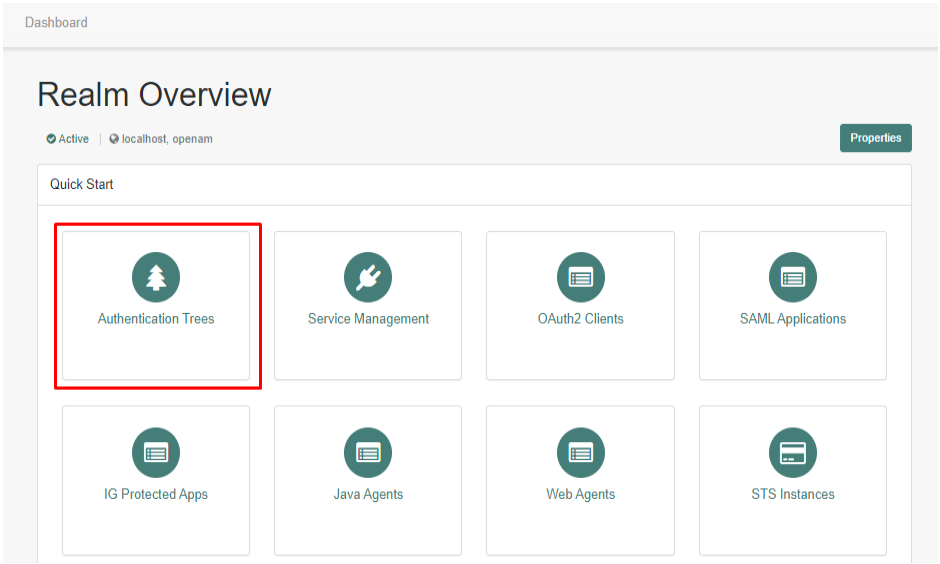
   Example: `https://sso.threatmetrix.com:8443/openam`

   > **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).

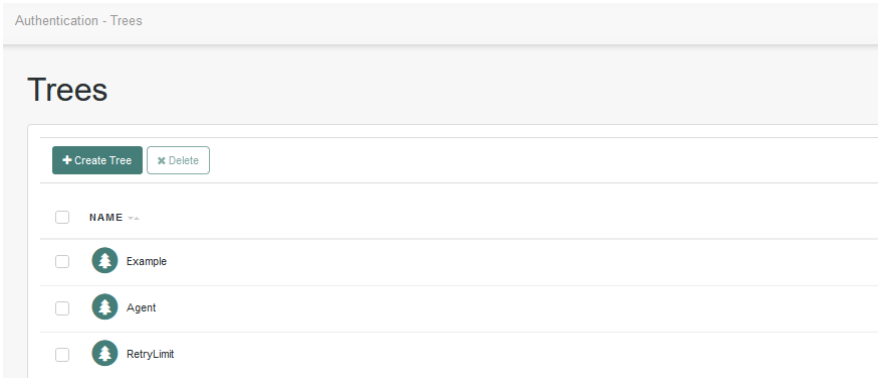
2. Login as Administrator, for example amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**. For the remainder of this simple quick start configuration, the top-level root realm is assumed.



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

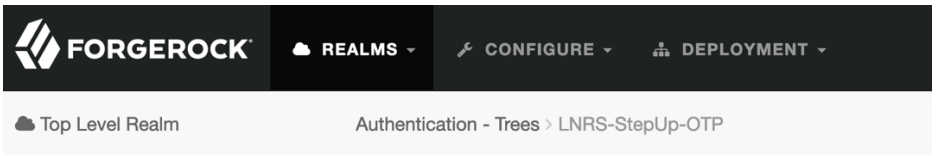


5. On the **Authentication Trees** display, click the **Create Tree** tile.



6. On the **New Tree** display, enter "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	OTP SELECTION
Page Header	Two-Factor Authentication
Page Description	When ready, click the button below to receive a code to your device.

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

Send Email	Selected
Send SMS	Selected
Send Voice	Selected

9. Build the OTP Sender, do the following:

   - 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.
   - 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 DDP PORTAL>
API Key	<ENTER API KEY FROM DDP PORTAL>
Base URL	https://h-api.online-metrix.net/
Policy	OTP [NOTE: This is the configured policy name in DDP Portal]
OTP Length	6
OTP Expire	3
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.
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.
Attribute Source	User Directory
Email Attribute	mail
SMS Attribute	telephoneNumber
Voice Attribute	telephoneNumber

> **Note:** In this example, the OTP Selector will fulfill the `otp_type_select` shared state variable needed by the OTP Sender node. This variable defines the type of OTP that will be sent by the OTP Sender node.

> **Note:** In this example, the authentication is assumed to be called via an inner tree evaluator. The tree that invokes this example authentication tree will insert the variable `username` into shared memory. The OTP Sender node requires this value.

> **Note:** The attribute source is set to look in the user directory at runtime for the attribute to send to OTP. For example, if the OTP type is Email, then the OTP Sender node will look in the Identity Store, for the defined `username`, for the LDAP attribute `mail`.

10. 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	Identity Verification
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.

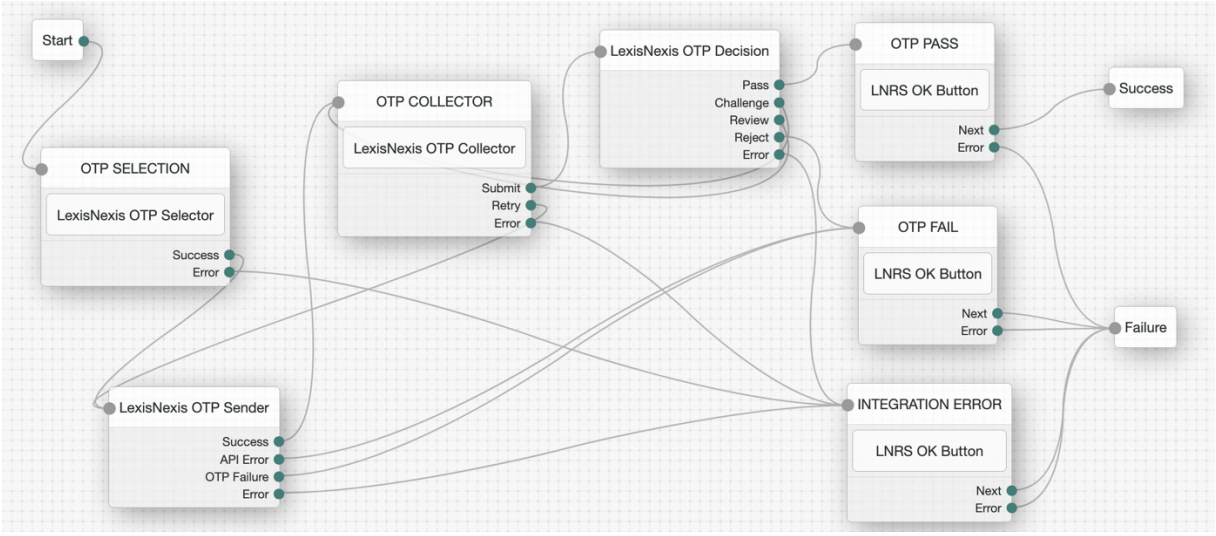
11. Build the OTP Decision, do the following:
    - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis OTP Decision** is displayed as a component, drag and drop it into the authentication tree into the authentication tree.
    - Select the **LexisNexis 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>

12. Build Message Nodes for OTP Pass, OTP Fail, 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.
13. 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	OTP SELECTION
OTP SELECTION (Success)	LexisNexis OTP Sender
OTP SELECTION (Error)	INTEGRATION ERROR
LexisNexis OTP Sender (Success)	OTP COLLECTOR
LexisNexis OTP Sender (API Error)	OTP FAIL
LexisNexis OTP Sender (OTP Failure)	OTP FAIL
LexisNexis OTP Sender (Error)	INTEGRATION ERROR
OTP COLLECTOR (Submit)	LexisNexis OTP Decision
OTP COLLECTOR (Retry)	OTP SELECTION
OTP COLLECTOR (Error)	INTEGRATION ERROR
LexisNexis OTP Decision (Pass)	OTP PASS
LexisNexis OTP Decision (Challenge)	OTP COLLECTOR
LexisNexis OTP Decision (Review)	OTP COLLECTOR
LexisNexis OTP Decision (Reject)	OTP FAIL
LexisNexis OTP Decision (Error)	INTEGRATION ERROR
OTP PASS (Next)	Success
OTP PASS (Error)	Failure
OTP FAIL (Next / Error)	Failure
INTEGRATION ERROR (Next / Error)	Failure

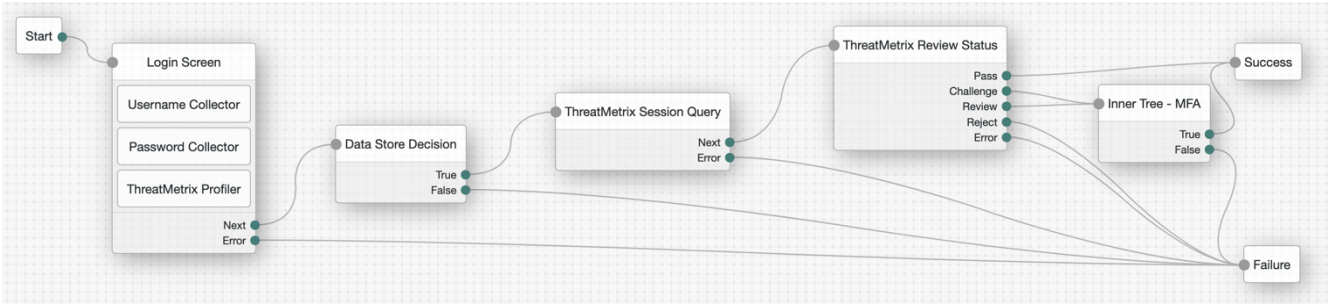
- At this point you should have the following



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.

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

1. From a workstation, launch a browser and navigate to the admin console.
2. Login as Administrator, for example 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 authentication final outcome.

Perform the following.

1. From a workstation, launch a browser and navigate to the admin console.
2. Login as Administrator, for example 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.