

**Configuring for Multiple Environments in MuleSoft**

**Course Number:** MULE-116
**Duration:** 1.5 days

**Overview**

This instructor-led, online Configuring for Multiple Environments in MuleSoft training course teaches attendees how to develop a professional Mule application that is configured for each deployment environment. Students learn how to deploy and promote an application in multiple environments. Attendees also learn how to encrypt sensitive data, like passwords, using the Secure Properties Tool.

**Prerequisites**

Students must have experience with Anypoint Studio and Anypoint Platform. Some experience with organizing a Mule application for a team of developers is helpful but not required.

**Materials**

All MuleSoft training students receive comprehensive courseware.

**Software Needed on Each Student PC**

Students will not need to install any software on their computers for this class. The class will be conducted in a remote environment. Students need a local computer with a web browser (preferably Chrome), stable internet, two monitors, and a headset/microphone.

**Objectives**

* Set up a new Mule application with multiple Mule configuration files
* Create Environment properties in a Mule application
* Add .yaml configuration files and secure properties files for each environment
* Set the environment property in Studio and Runtime Manager
* Explore the features of the Secure Configuration Properties
* Encrypt/decrypt properties using the Secure Properties Tool
* Identify the proper syntax for encrypted values saved in secure config files
* Pass the encryption key in Studio and Runtime Manager

**Outline**

* Application Setup - Our API & Your API
	+ Create a New Mule Application
	+ Import RAML Spec
	+ Add Multiple .xml Files
	+ Create Global Elements
* Configure Environment Properties - Our API & Your API
	+ Add .yaml Files – Local Environment
	+ Create env Global Variable
	+ Create Global Configuration for ${env} File
	+ Deploy/Test in Studio
* Add Dev Environment - Our API & Your API
	+ Add .yaml Files
	+ Deploy/Test in Studio
	+ Deploy/Test via Runtime Manager
* Add Test Environment - Our API & Your API
	+ Add .yaml Files
	+ Deploy/Test in Studio
	+ Deploy/Test via Runtime Manager
* Secure Configuration Properties
	+ Download Secure Properties Tool
	+ Encrypt/Decrypt Files and Fields
	+ Secure Properties Generator
	+ Syntax for Encrypted Values
	+ Secure Encryption Key
* Secure Configuration Properties Files
	+ Add Secure Properties Files per Environment
	+ Encrypt Sensitive Data
	+ Deploy/Test in Each Environment
	+ Set Values from Runtime Manager
* Conclusion