Innovar SSL Settings Plugin

Introduction

Welcome to the SSL Settings plugin documentation for Mirth Connect. This plugin is designed to allow you to use SSL/TLS on the HTTP Connector in Mirth Connect.

Why SSL?

Mirth does not natively support TLS/SSL on the HTTP Connector. Encrypting your traffic is essential for transmitting data, especially patient health information. Using the SSL Settings Plugin, it would allow you to enable SSL/TLS both when receiving and sending messages over HTTP.

Key Features

Keystore: Specify the path to your keystore. This will contain your certificate to identify who you are, and your private key for decrypting messages received. The path can be on the file system or S3.

Truststore: Specify the path to the truststore. The truststore will contain the certificate for all trusted systems. This is needed if want to do mutual TLS authentication.

Verify Hostname: When using SSL to send data, you can enable/disable “verify hostname”. This will validate that the certificate presented by the server matches the url.

Getting Started

Before you dive into the documentation, make sure to review the installation prerequisites and check compatibility with your existing Mirth Connect setup. The subsequent sections will guide you through the configuration, usage, and optimization of the SSL Settings plugin.

Let's get started!

Installation

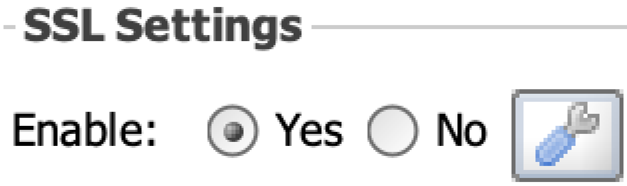
If you are using Mirth Connect packaged by Innovar Healthcare from the AWS Marketplace, the extension should be pre-installed on “Advanced with SSL” and “Advanced with SSL Autoscaling” versions.

If, for some reason, you need to reinstall or update the plugin, you can do this from the Mirth Connect Administrator application. While logged into Mirth Connect Administrator, click on

“Extensions”, then at the bottom of the screen, click “Browse”. A new window will pop up to allow you to browse for your plugin zip file on your local machine. Browse to the appropriate zip file and click “Open”. Once back on the Extensions screen, your file path should be filled in. Click “Install” to upload the file. Once completed, you will need to restart the Mirth Connect Service on the remote server.

Plugin Configuration

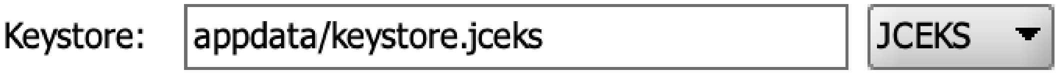
With the SSL Settings Plugin installed, there is an option to enable/disable SSL on both the HTTP Receiver and Sender. With SSL enabled, the tool button is enabled allowing you to configure the SSL Connection.



SSL Settings

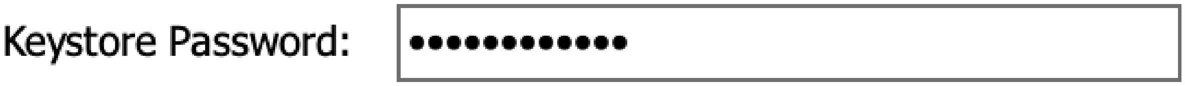
Enable: ● Yes ○ No

The **Keystore** field is for specifying the path to the keystore. It can be a full, or relative path to the Mirth installation directory. You can also specify a S3 path using the following format: s3://<region>.<bucketname>/<objectkey>. Make sure to select the appropriate keystore type in the dropdown field.



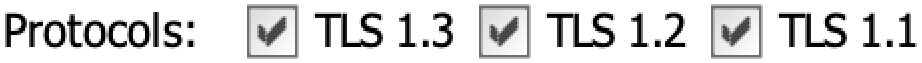
Keystore: appdata/keystore.jceks JCEKS

In the **Keystore Password** field, enter the password for the keystore.



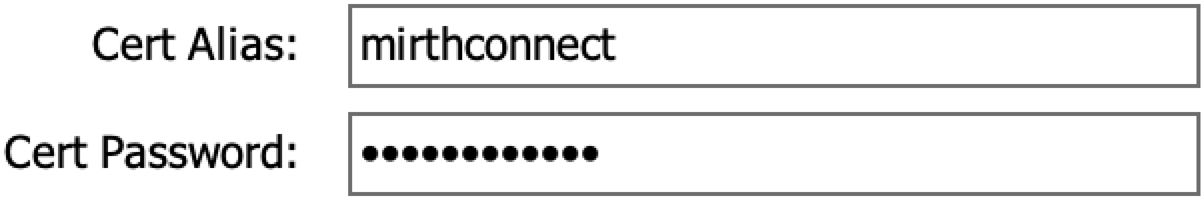
Keystore Password: •••••••••••••

In **Protocols**, you can select which version of TLS you want to support.



Protocols: ☑ TLS 1.3 ☑ TLS 1.2 ☑ TLS 1.1

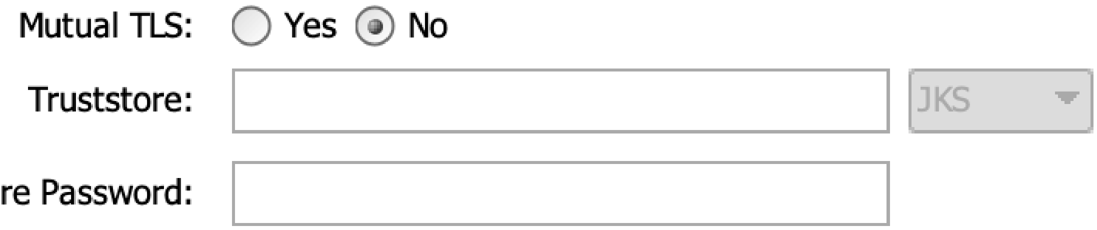
In the **Cert Alias and Cert Password** fields, enter the certificate alias and the password for the associated private key.



Cert Alias: mirthconnect

Cert Password: •••••••••••••

To enable **Mutual TLS (mTLS)**, click the Yes radio box, and enter the trust store path and password. Similar to the KeyStore field, you need to select a truststore type in the drop down, and enter a password for the truststore. You can use a relative or absolute file path, or a S3 location using format: s://<region>.<bucketname>/<objectkey>

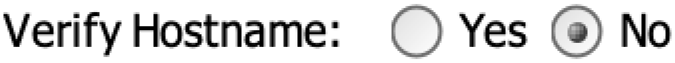


Mutual TLS: ○ Yes ● No

Truststore: JKS

Truststore Password:

When using SSL with the HTTP Sender, you can validate the certificate alias matches the url by enabling **Verify Hostname**



Verify Hostname: ○ Yes ● No