Innovar Cognito Single Sign On (SSO) Plugin

Introduction

Welcome to the Cognito Single Sign On (SSO) plugin documentation for Mirth Connect. This plugin is designed to allow you to login using credentials stored in Amazon Cognito. This would allow you to use the same credentials for multiple different Mirth Connect instances across your organization.

Why SSO?

Managing different user credentials in a different environments can become a maintenance challenge and also open you up to security risk. Managing the user credentials in a single place, can help reduce the maintenance of users.

Key Features

Settings Panel: A user interface is included as part of the plugin to allow you to configure your Cognito User Pool information.

Fallback to Local Authentication: If desired, users can enable “Fallback to Local Auth”. This option would utilize local user authentication if authentication fails against the Cognito User Pool.

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 Cognito SSO 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.

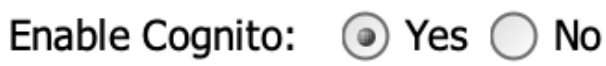
If, for some reason, you need to reinstall or update the plugin, you can do this from the Mirth Connect Administrator application. While logged into Mirth Connect Administrator, click on “Extensions”, then at the bottom of the screen, click “Browse”. A new window will pop up to allow you to browse for 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

In the Mirth Connect Administrator window, click on Settings. You will see a new tab for “Cognito”. See below for explanation for each setting.

Enable Cognito



Select Yes/No to enable/disable Cognito Authentication.

Fallback to Local Authentication

Select Yes to use local user credentials if Cognito Authentication fails.

Test Connection

Click the “Test Connection” button to validate your Cognito settings.

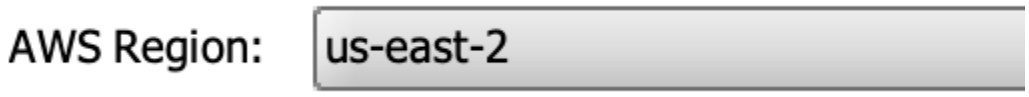
User Pool ID

Enter the User Pool ID. This is a required field.

Cognito Application ID

Enter the Cognito application ID. This is the Client ID of the App Client for the user pool.

Region



Select the region for your Cognito User Pool.

AWS Access ID and Key (optional)

Optionally, you can provide access ID and Key to connect to your AWS Cognito Service. It is recommended to not store access ID and Keys in Mirth Connect so it is better to authenticate using role based permissions.

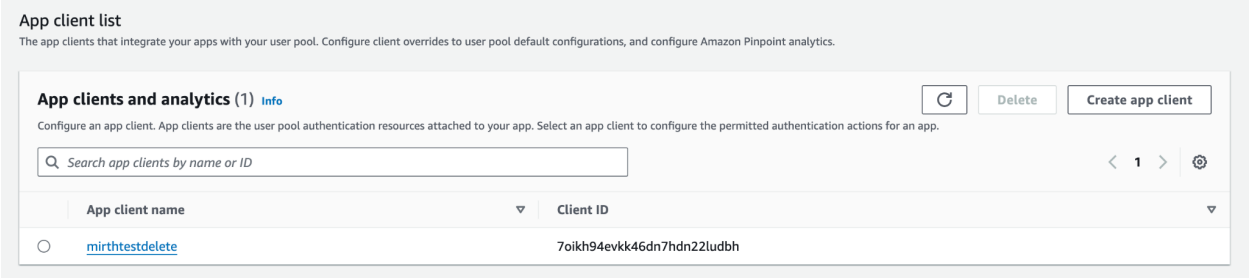
Cognito User Pool Setup

Here are the steps to create a user pool in Cognito using the AWS Console.

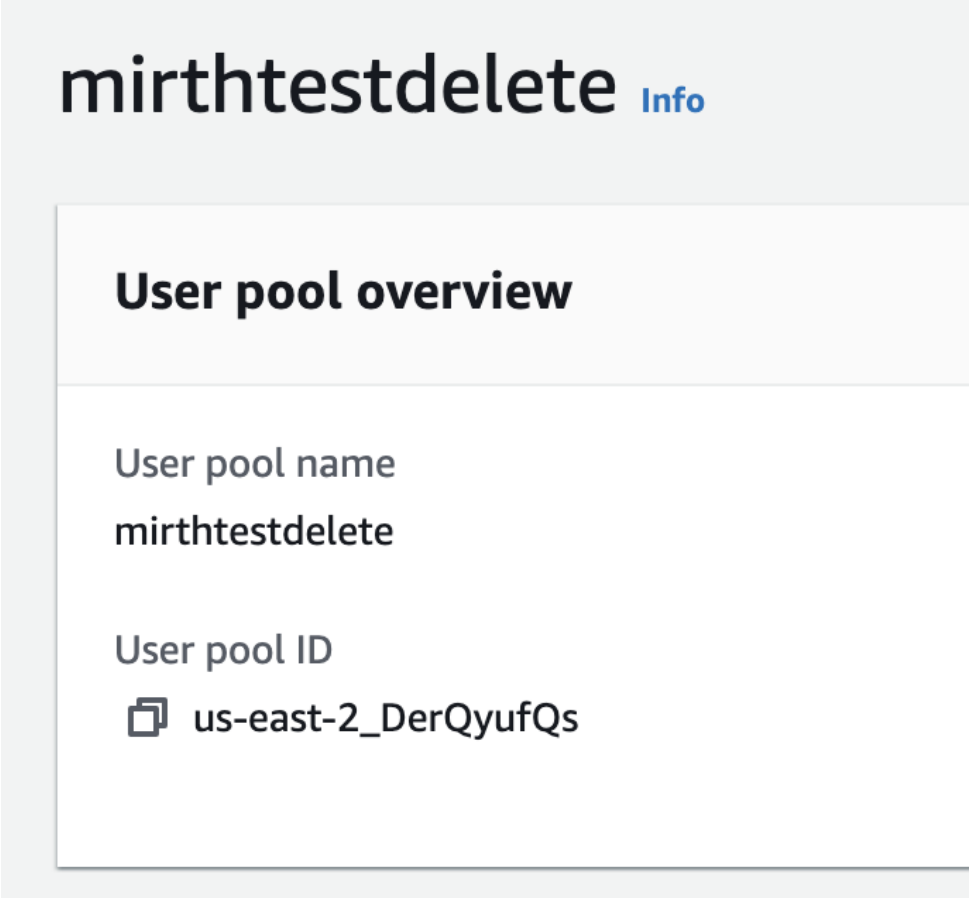
1. Login to your AWS Console.
2. Goto Cognito by searching for Cognito in the search bar.
3. Click User Pools on the left navigation bar.
4. Click Create user pool.
5. Do not check “Federated identity providers”.
6. Check User name under “Cognito user pool sign-in options”.
7. Click Next.
8. Select your password policy as you see fit.
9. Under “Multi-factor authentication, select “No MFA”
10. Under “User account recovery”, uncheck “Enable self-service account recovery”
11. Under “Self-service sign-up”, uncheck “enable self-registration”
12. Under “Cognito-assisted verification and confirmation”, uncheck “Allow Cognito to automatically send messages to verify and confirm”
13. Select required field as you see fit under “Required attributes”
14. Under “User pool name”, enter a user pool name.
15. Under “initial app client”, select “public client”, and enter a app client name.
16. Select “don’t generate a client secret

17. Under “Authentication flows”, select “ALLOW_USER_PASSWORD_AUTH” and “ALLOW_USER_SRP_AUTH”.
18. Click next, then click Create user pool
19. You now should have a user pool that you can use with the Cognito plugin. Take note of the User pool ID and the App Client ID. The app client ID can be found by going to the App integration tab, scrolling to the bottom of the screen, under the Client ID column.

App Client ID:



User Pool ID:



EC2 Role Permissions required for Cognito Access

Here is an example permission statement for the ec2 role to allow access to Cognito. Put your specific user pool ID in the resource field, or use a wildcard for all Cognito resources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cognito-idp:DescribeUserPool",
                "cognito-idp:DescribeUserPoolClient"
            ],
            "Resource": [
                    "arn:aws:cognito-idp:us-east-2:403214344436:userpool/<UserPoolID>"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "cognito-idp:GetUser",
                "cognito-idp:ListUserPools",
                "cognito-idp:InitiateAuth"
            ],
            "Resource": "*"
        }
    ]
}
```