Innovar Role-Based Access Control Plugin

Introduction

Why Role-Based Access Control(RBAC)?

Healthcare systems handle sensitive patient data that must be protected in compliance with regulations like HIPAA (Health Insurance Portability and Accountability Act) in the U.S. RBAC ensures that only authorized users can access or modify specific data. By assigning roles with specific permissions, you can control who has access to which parts of the system and data, minimizing the risk of unauthorized access or breaches.

Key Features

Data Security and Privacy:Healthcare organizations must adhere to strict regulatory requirements concerning data access and protection. RBAC helps in meeting these compliance requirements by enforcing access controls and maintaining audit trails. It ensures that only individuals with appropriate roles can access certain features or data, which is essential for maintaining compliance.
Audit and Accountability: RBAC supports auditing by clearly defining who has access to what and why. This makes it easier to track actions within the system, investigate issues, and ensure accountability. If a data breach or error occurs, having detailed role-based access logs can be crucial for forensic analysis.
Reduced Risk of Errors: By defining clear roles and associated permissions, RBAC helps in reducing the risk of accidental or intentional misuse of the system. For example, a user who only needs to view data shouldn't have permissions to modify or delete it. This minimizes the potential for errors or malicious actions.

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 and how to use the Role-Based Access Control plugin.

Let's get started!

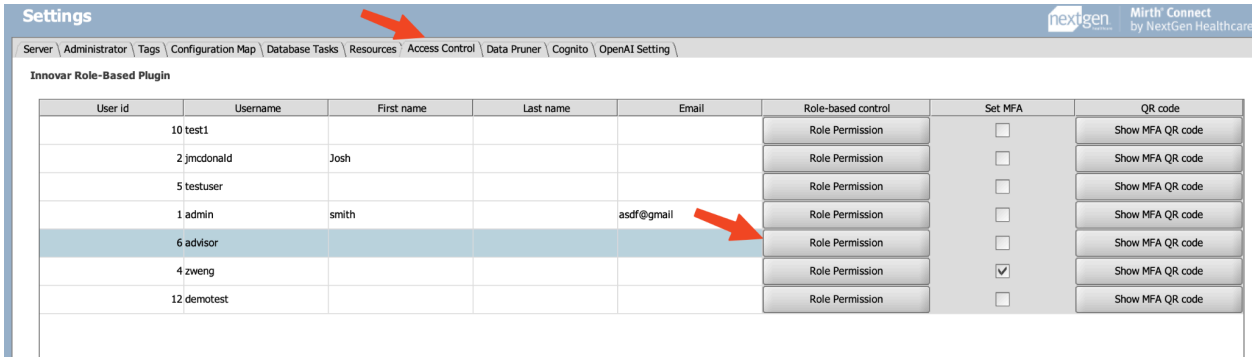
Installation

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

1.Please go to the setting panel > “Access Control” tab, and double click the “Role Permission” button.



2.Please select the permission to every Mirth Connect section.

Editor:the user has the privilege to view, edit and save the modification under the section

Viewer:the user can only view the details, but can not save any modification under the section

No permission:the user is not able to view, edit any details under the section.

For example: this user are not allowed to view any details under Alerts and Events. In the Mirth Connect launcher dashboard ,the user can not view the Alerts and Events.