Part 3 - Manual Deployment and Post-deployment of MedTech service

- Article
- 10/04/2022
- 4 minutes to read

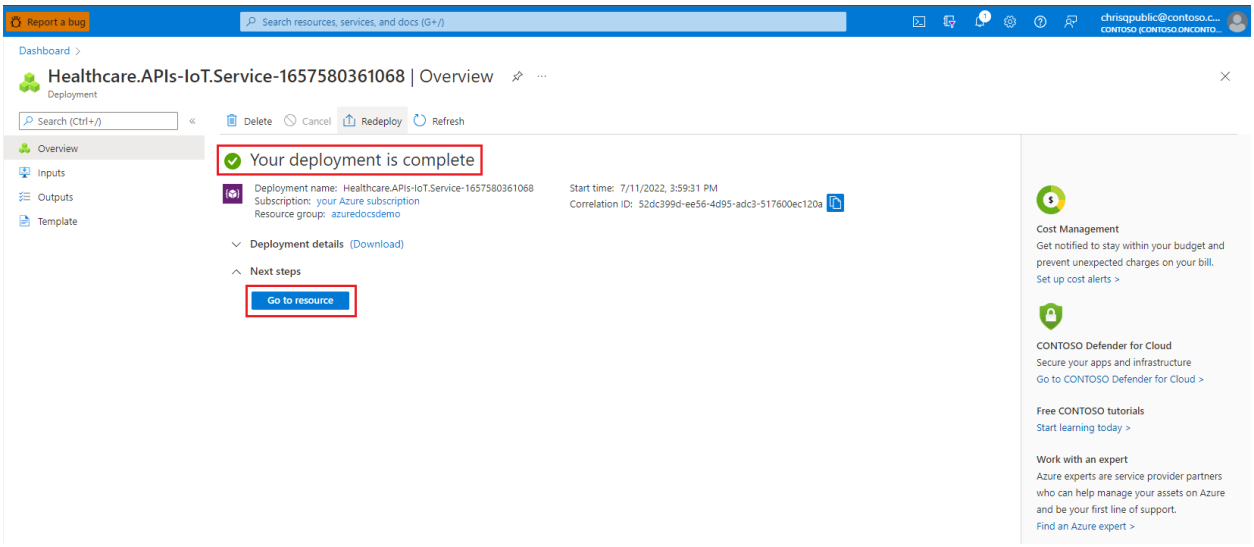
When you are satisfied with your configuration and it has been successfully validated, you can complete the deployment and post-deployment process.

Create your manual deployment

1. Select the **Create** button to begin the deployment.
2. The deployment process may take several minutes. The screen will display a message saying that your deployment is in progress.
3. When Azure has finished deploying, a message will appear will say, "Your Deployment is complete" and will also display the following information:

- Deployment name
- Subscription
- Resource group
- Deployment details

Your screen should look something like this:



Manual Post-deployment requirements

There are two post-deployment steps you must perform or the MedTech service can't read device data from the device message event hub, and it also can't read or write to the FHIR service. These steps are:

1. Grant access to the device message event hub.
2. Grant access to the FHIR service.

These two additional steps are needed because MedTech service uses Azure role-based access control (Azure RBAC) and a system-assigned managed identity for extra security and control of your MedTech service assets.

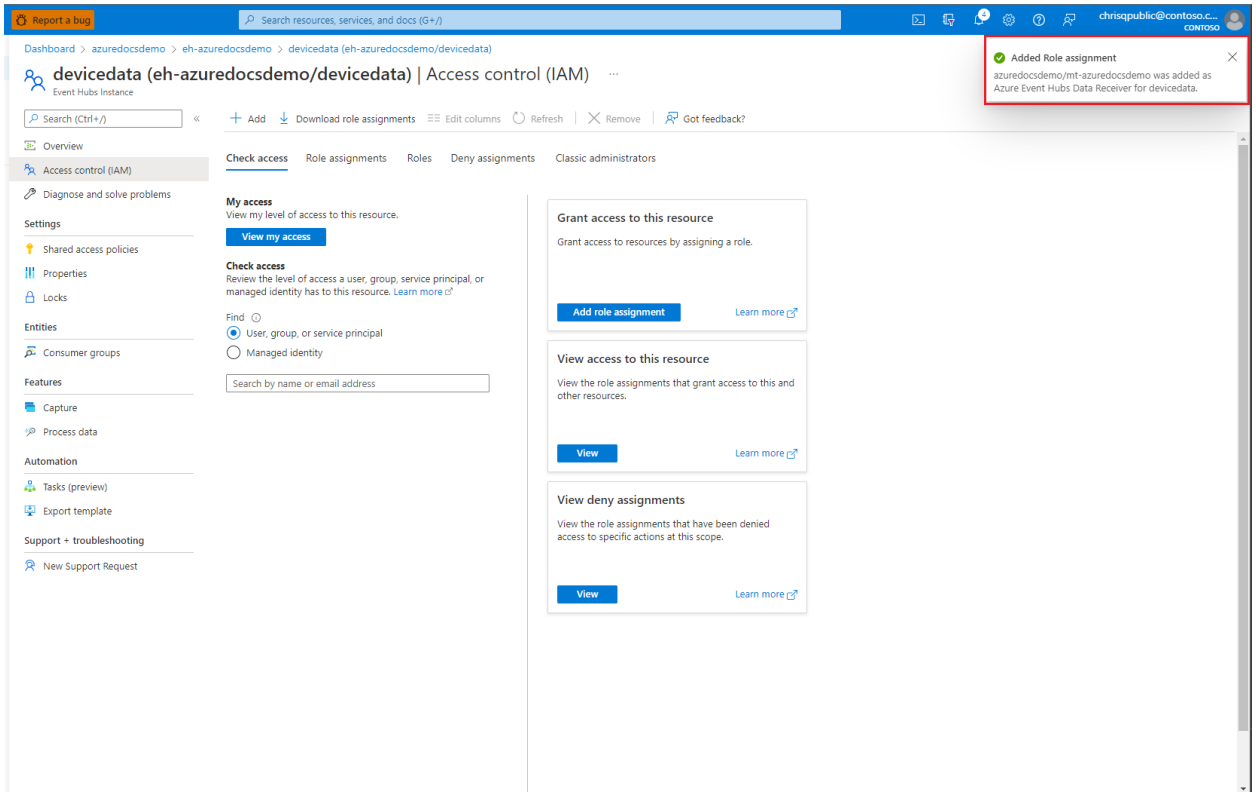
Grant access to the device message event hub

Follow these steps to grant access to the device message event hub:

1. In the **Search** bar at the top center of the Azure portal, enter and select the name of your **Event Hubs Namespace** that was previously created for your MedTech service device messages.
2. Select the **Event Hubs** button under **Entities**.
3. Select the event hub that will be used for your MedTech service device messages. For this example, the device message event hub is named `devicedata'.
4. Select the **Access control (IAM)** button.
5. Select the **Add role assignment** button.
6. On the **Add role assignment** page, select the **View** button directly across from the **Azure Event Hubs Data Receiver** role. The Azure Event Hubs Data Receiver role allows the MedTech service to receive device message data from this event hub. For more information about application roles, see Authentication & Authorization for Azure Health Data Services.
7. Select the **Select role** button.
8. Select the **Next** button.
9. In the **Add role assignment** page, select **Managed identity** next to **Assign access to** and **+ Select members** next to **Members**.
10. When the **Select managed identities** box opens, under the **Managed identity** box, select **MedTech service,** and find your MedTech service system-assigned managed identity under the **Select** box. Once the system-assigned managed identity for your MedTech service is found, select it, and then select the **Select** button.

The system-assigned managed identify name for your MedTech service is a concatenation of the workspace name and the name of your MedTech service, using the format: **"your workspace name"/"your MedTech service name"** or **"your workspace name"/iotconnectors/"your MedTech service name"**. For example: **azuredocsdemo/mt-azuredocsdemo** or **azuredocsdemo/iotconnectors/mt-azuredocsdemo**.

11. On the **Add role assignment** page, select the **Review + assign** button.
12. On the **Add role assignment** confirmation page, select the **Review + assign** button.
13. After the role assignment has been successfully added to the event hub, a notification will display on your screen with a green check mark. This notification indicates that your MedTech service can now read from your device message event hub. It should look like this:



For more information about authorizing access to Event Hubs resources, see Authorize access with Azure Active Directory.

Grant access to the FHIR service

The process for granting your MedTech service system-assigned managed identity access to your FHIR service requires the same 13 steps that you used to grant access to your device message event hub. The only exception will be a change to step 6. Your MedTech service system-assigned managed identity will require you to select the **View** button directly across from **FHIR Data Writer** access instead of the button across from **Azure Event Hubs Data Receiver**.

The **FHIR Data Writer** role provides read and write access to your FHIR service, which your MedTech service uses to access or persist data. Because the MedTech service is deployed as a separate resource, the FHIR service will receive requests from the MedTech service. If the FHIR service doesn't know who's making the request, it will deny the request as unauthorized.

For more information about assigning roles to the FHIR service, see Configure Azure Role-based Access Control (RBAC).

For more information about application roles, see Authentication & Authorization for Azure Health Data Services.

Now that you have granted access to the device message event hub and the FHIR service, your manual deployment is complete and MedTech service is ready to receive data from a medical device and process it into a FHIR Observation resource.