

Telehealth Management Platform (TMP)

5.2.6

Deployment, Installation, Back-Out, and Rollback Guide



November 2024

**Department of Veterans Affairs
Office of Information and Technology (OI&T)**

Introduction

This document describes how to deploy and install Telehealth Management Platform (TMP) 5.2.6 as well as the plan to roll back to a previous version or data set if necessary. 5.2.6 includes updates to App Services as well as manual configuration updates. The instructions have been customized for this release.

For more information on TMP dependencies, deployment environments, site readiness, resources, and roles and responsibilities, please see Standard DIBR Content on Confluence.

Please see TMP 5.2.6 Release Notes for updates included in this release.

TMP 5.2.6 Deployment Instructions

This section provides steps to deploy the TMP related changes in the Production environment, including backup and solution deployment. Complete the steps in the following sections.

Step 1: Perform Backups

Prior to beginning the deployment, it is important to make backups in the environments. For 5.2.6, you will need to back up the App Services, Plugins, and TMP Dynamics Solution. Backup Instructions

Change Request: Begin Implementation

CHG0569466 | Change Request | ServiceNow

Step 2: Deploy the Solution

1. Backup TMP Dynamics
2. Location for the Solution file: GitHub TMP Release 5.2.6 Solution and Backup Files
3. Import solution file into the environment.
4. **Publish All Customizations**

The following Jira issues are included in the solution file.

- TMP-1716: Cancel Reason not populating on VistA Bookings tab (**manual configuration**)
- TMP-2577: INC29789006 Auto Save occurs after selecting Consults or RTCs
- TMP-2612: Update iCal attachment for Appointment notification emails
- TMP-2742: Last Name field on Patient Search is not 508 compliant
- TMP-2884: Clean up old VIA login code and settings (**manual configuration**)
- TMP-3067: INC32183177 TMP is not handling the MVI identifier response status correctly (**manual configuration**)
- TMP-3081: INC35168772 Enable/Disable buttons showing up on Resource: User (**manual configuration**)

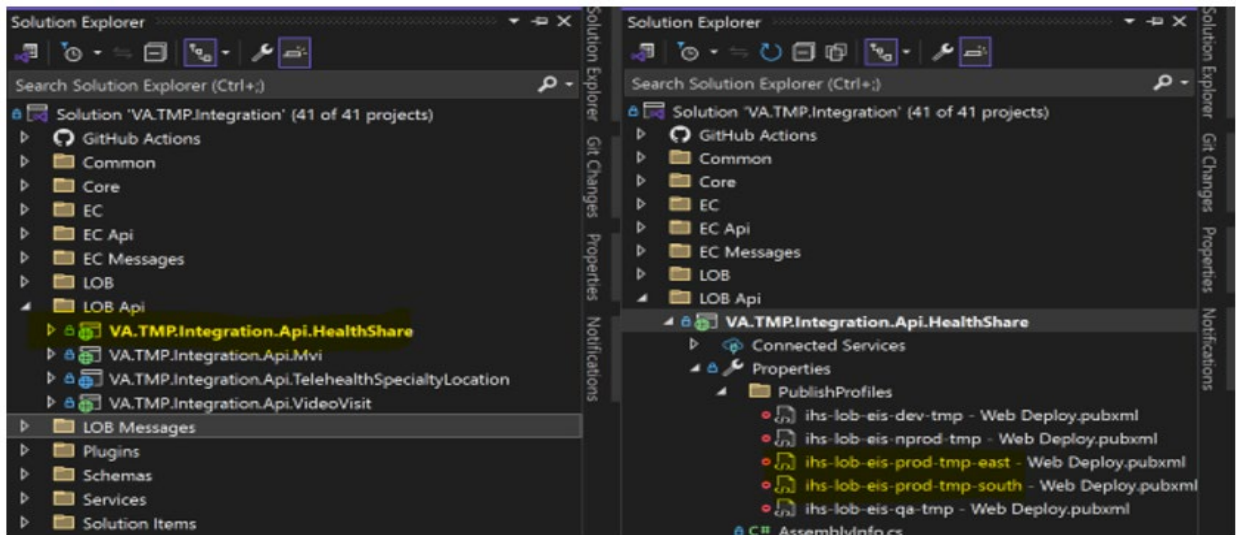
Step 3: Complete Manual Configuration

Publish Changes for API

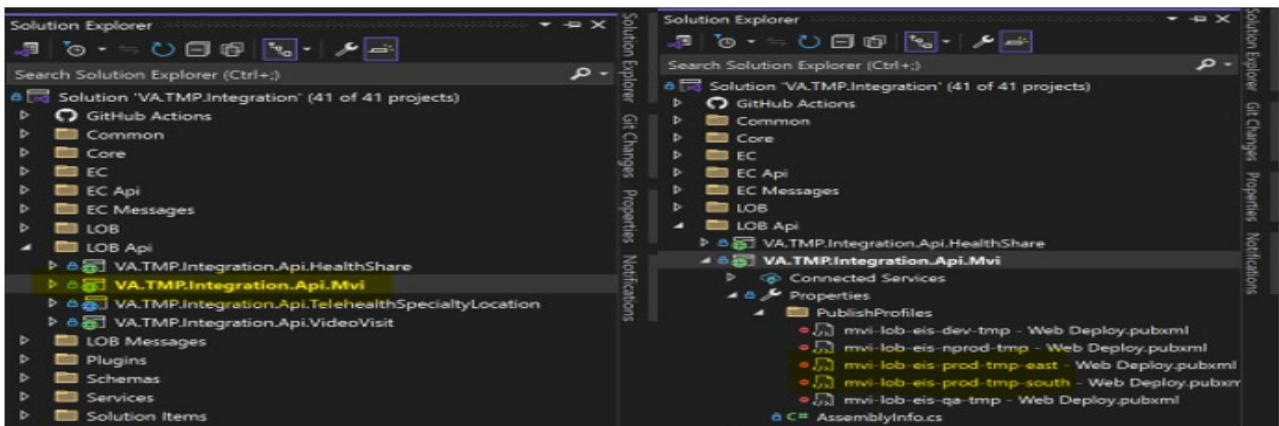
- a. **IHS_LOB - VA.TMP.Integration.Api.HealthShare**
TMP-1716: Cancel Reason not populating on VistA Bookings tab
TMP-2423: Cancelled appointments not sending the correct Cancellation Reason
TMP-2613: INC30109282 Do not update Inactive Sites during Clinic Updates
TMP-3067: INC32183177 TMP is not handling the MVI identifier response status correctly
- b. **MVI_LOB - VA.TMP.Integration.Api.Mvi**
TMP-3067: INC32183177 TMP is not handling the MVI identifier response status correctly

Steps to Publish

1. Open Visual Studio Integration Solutions Project in the **Release Branch**. (Make sure you have the latest changes)
2. Locate the HealthShare API Project and Publish Profiles in the LOB Api Folder (**VA.TMP.Integration.Api.HealthShare**).



3. Either right-click on the Project and select the **Publish** option or select the **Publish** option from the Build Menu.
4. Select either the Prod East or Prod South **EIS** Publish Profile from the menu. If you do not currently have those Profiles as seen ABOVE you'll need to download them from Azure and Import them into Visual Studio, first. **Deploy using existing profiles in Visual Studio. Downloaded publish profiles are for username/password.**
5. Verify the correctly Publish Profile is selected based upon the environment you wish to deploy to, then click Publish.
6. Repeat Steps 2 thru 5 for the other remaining Region (i.e. East or Southwest).
7. Verify Published correctly by logging into KUDO ->Dubug Console->CMD->site->wwwroot->bin dll's dates have been updated
8. Repeat Steps 2 thru 7 for the **VA.TMP.Integration.Api.Mvi** Project for **both** the East and Southwest Regions. Locate the MVI API Project and Publish Profiles in the LOB Api Folder (**VA.TMP.Integration.Api.Mvi**).

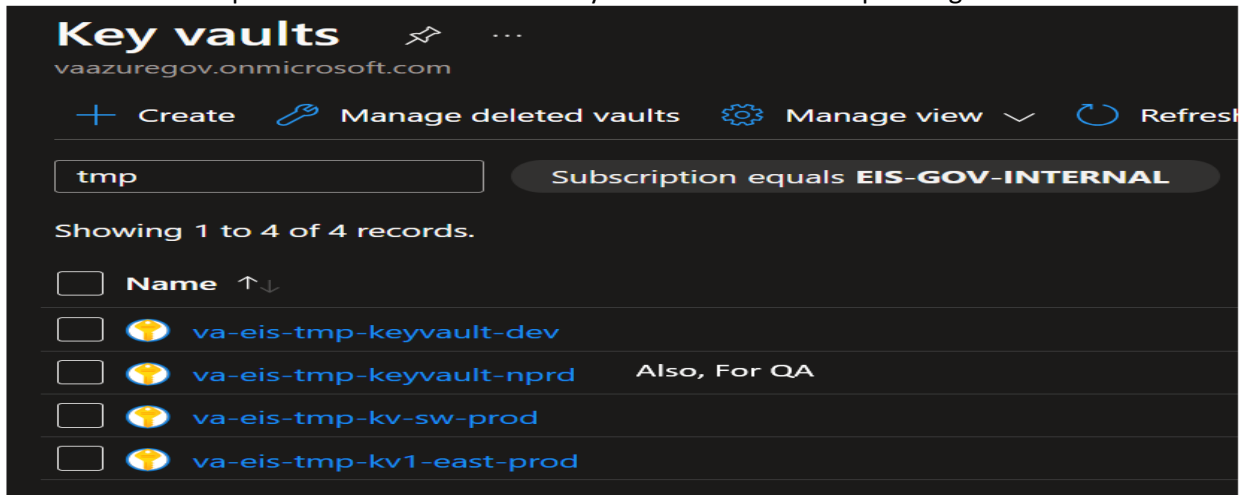


TMP-2938: Implement changes to use Mobile OAuth to retrieve a JWT token - Ec.Jwt.Api

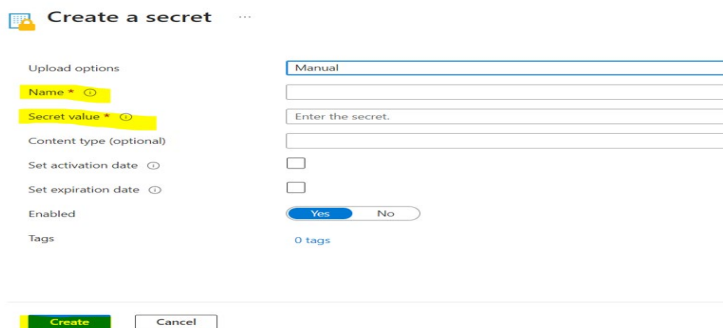
Publish Changes for Azure Key Vault in the Release Branch

1. Log into the Azure Portal.
2. Navigate to Azure Key Vaults.

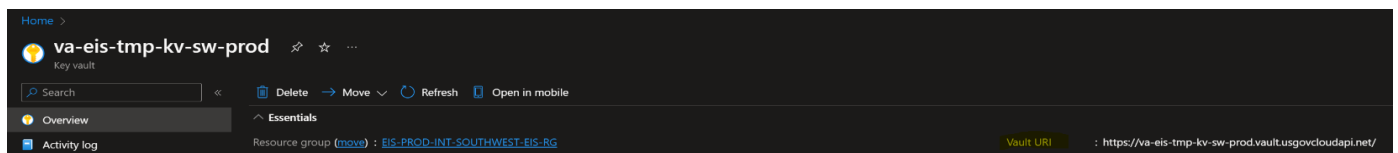
- Filter on EIS Subscription and select one of the Key Vaults below based upon target environment.



- Select **Secrets** from the Left Navigation. **(under objects)**
- Confirm that there's no entry for client-private-key.
- Verify your permission by clicking Access policies search your name. If no permission, Create New Policy->Select All Permissions->Next->Search Zero Account->Next->Leave Blank->Click Create
- Select Secrets, Click the **+Generate/Import** button to create a new entry.
- Enter client-private-key in the **Name field** and the contents of the Private Key certificate file (private.pkcs8) in the **Secret value field** and click **Create**.



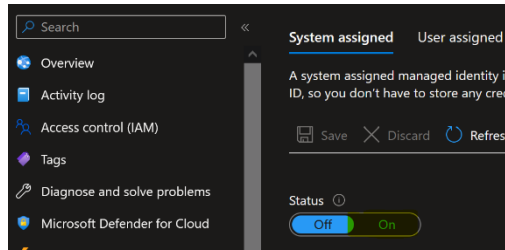
- Switch back to Overview and copy the value from the Vault URI. (Example below)



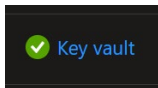
- Navigate to App Services then locate JWT EC App Service.
- Select Environment Variables from the Left Nav.
- Add a new Setting. Enter **Client_Private_Key** in the **Name field** and enter **@Microsoft.KeyVault(VaultName=(Vault Uri from Step 9 above (va-eis-tmp-kv-sw-prod);SecretName=(KeyVault Secret Name(client-private-key))** in the **Value field**.
- Confirm the KeyVault setting is valid indicated by a green check mark, if you do not see a check mark in the Source Column for the new setting then you'll need to complete the following Steps to fix it.



- Switch to the Identity Section and if found **copy the Object Id** for comparison in an upcoming Step. If one doesn't exist or it's not enabled complete the following Steps.
 - Switch the Status from Off to **On**.



- ii. Click **Save**.
 - iii. **Copy the new Object Id**.
 - iv. NOTE: if you had to perform this Step you'll need to **copy the Name of the App Service** for use in an upcoming Step.
- b. Navigate to the Key vaults in Azure and find the Key Vault from Step 3.
 - c. Navigate to the Access Policies Section of that vault. If you had to create the Identity in Step (a) above then enter the Name of the App Service in the Search field, otherwise enter the Object Id and/or Name of the App Service in the Search field. If found, validate that it has List and Get permissions for Secrets selected. If not then delete it and start over. If NOT found, continue.
 - d. Click the **Create** button to create the Access Policy.
 - e. Select the Get and List check boxes in the Secret Permissions column, then click **Next**.
 - f. Enter the Object Id from Step (a) above. Select the App Service found and click **Next**.
 - g. Click **Next** to skip the Application step.
 - h. Make sure the Object Id in the Principal section matches then click **Create**.
 - i. Switch back over to the Environment Variables section of the App Service.
 - j. After refreshing the Environment Variables check on the Key Value for the Client_Private_Key. If there is no green checkmark then you may need to reload the page again. If it still does not appear then make sure you have the correctly formatted value in the setting.



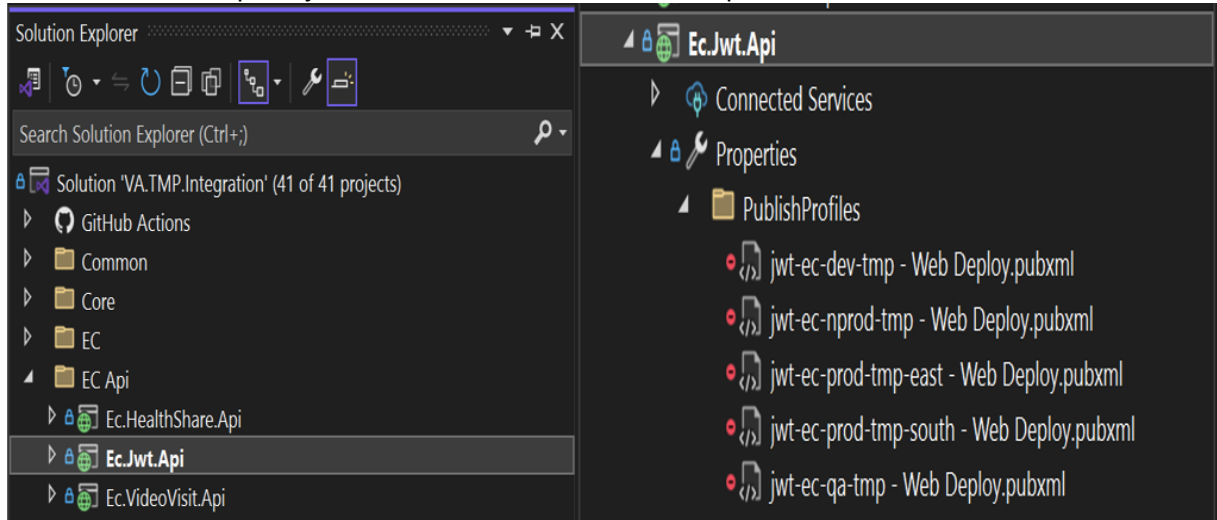
- k. Update the value using the following value **@Microsoft.KeyVault(VaultName= (Vault Uri from Step 9 above (va-eis-tmp-kv-sw-prod));SecretName= (KeyVault Secret Name(client-private-key))** then click **Apply**. Then click the **Apply** again, then click **Confirm**.
- l. Repeat these Steps for the South Region.

Publish Changes for API - Ec.Jwt.Api Project

Steps to Publish

14. Open Visual Studio Integration Solutions Project. (Make sure you have the latest changes)

15. Locate the Ec.Jwt.Api Project and Publish Profiles in the EC Api Folder.



16. Either right-click on the Project and select the **Publish** option or select the **Publish** option from the Build Menu.

17. Select either the Prod East or Prod South **EIS** Publish Profile from the menu. If you do not currently have those Profiles as seen ABOVE you'll need to download them from Azure and Import them into Visual Studio, first.

Deploy using existing profiles in Visual Studio. Downloaded publish profiles are for username/password.

18. Verify the correctly Publish Profile is selected based upon the environment you wish to deploy to, then click Publish.

19. Repeat Steps 2 thru 5 for the other remaining Region (i.e. East or Southwest).

20. Verify Publish.

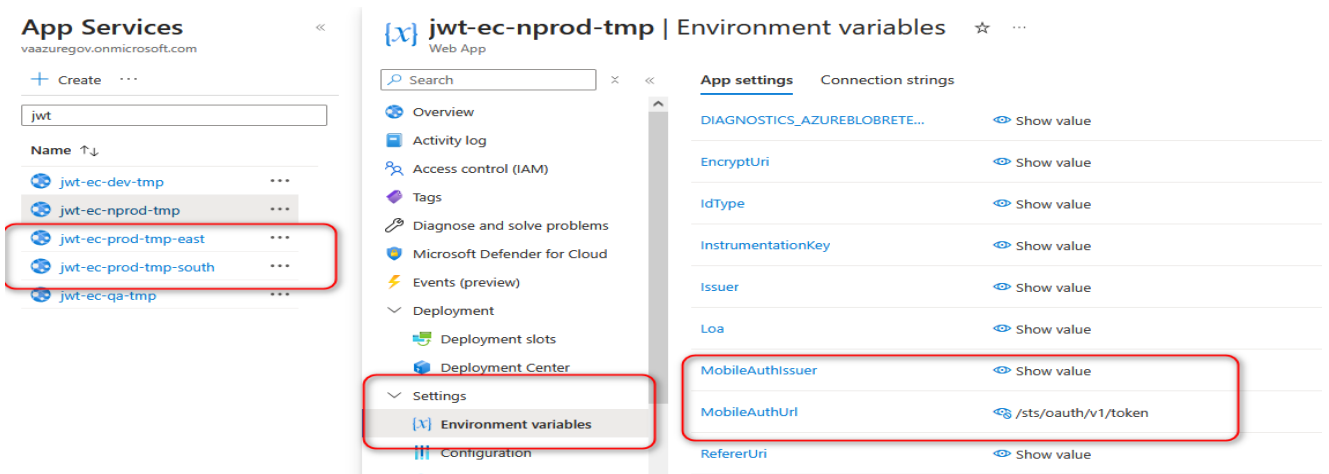
Update the log4net section of the Web.Config file. Set the value for the "level" element in the root section to "ERROR" and SAVE.

21. Repeat Steps 2 thru 20 for the other remaining Region (i.e. East or South).

22. Modify App Services EC_JWT to add the following environment variables in both Region (i.e. East or South).

- a. MobileAuthIssuer: 4716e8cc1bdf88cd
- b. MobileAuthUrl: /sts/oauth/v1/token

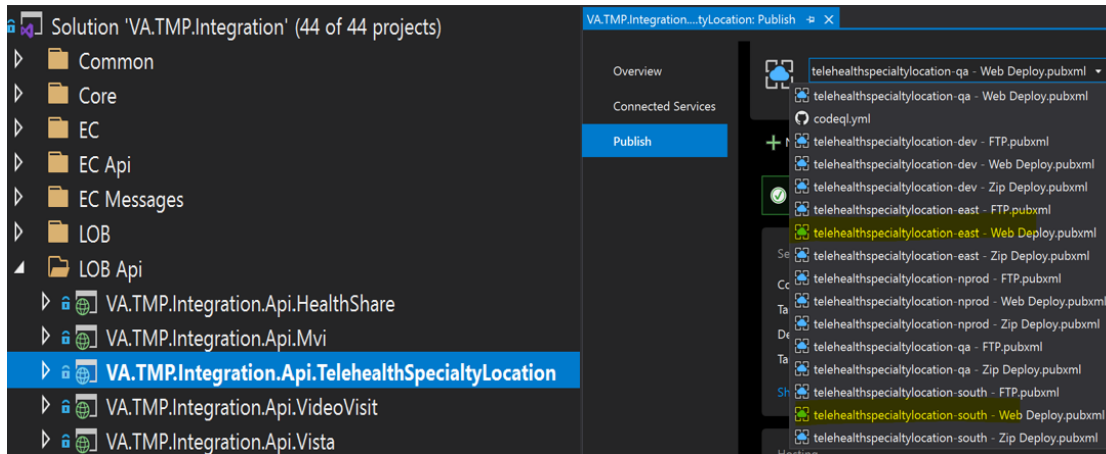
23. Modify App Services EC_JWT to add the following environment variables in both Region (i.e. East or South).



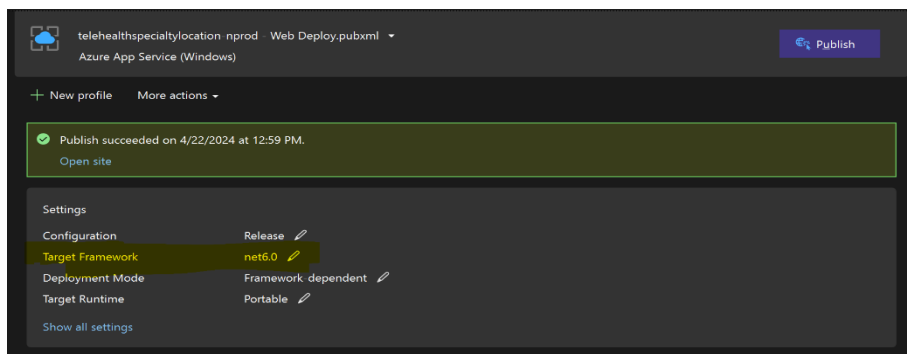
III. Publish Changes for API - Telehealth Specialty Location App Service

TMP-2794: Update TA API to return Patient Location Type and Group Appointment indicators

1. Open Visual Studio Integration Solutions Project. (Make sure you have the latest changes)
2. Locate the TelehealthSpecialtyLocation API Project and Publish Profiles in the LOB Api Folder (VA.TMP.Integration.Api.TelehealthSpecialtyLocation).



3. Either right-click on the Project and select the **Publish** option or select the **Publish** option from the Build Menu.
4. Select either the Prod East or Prod South **EIS** Publish Profile from the menu. If you do not currently have those Profiles as seen ABOVE you'll need to download them from Azure and Import them into Visual Studio, first. **Deploy using existing profiles in Visual Studio. Downloaded publish profiles are for username/password.**
5. Verify the correctly Publish Profile is selected based upon the environment you wish to deploy to, then click Publish.
6. Repeat Steps 2 thru 5 for the other remaining Region (i.e. East or Southwest).
7. Make sure the Target Framework is set to net6.0.



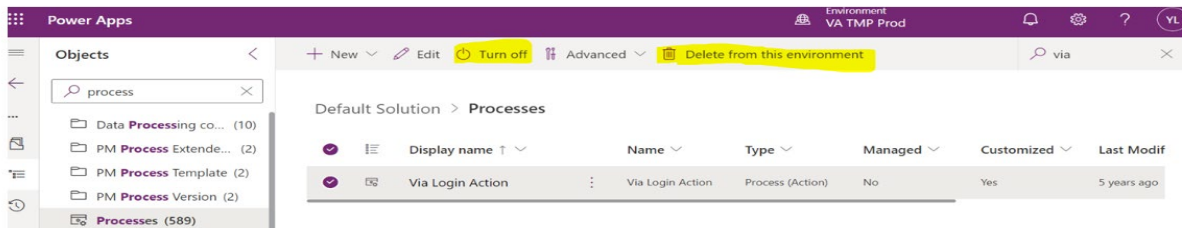
8. Click Publish.
9. Verify Publish
10. Log into <https://portal.azure.us>
11. Go to App Services and find the TelehealthSpecialtyLocation API Project.
12. Click Development Tools → Advanced Tools → GO →
13. Kudo → Debug console → CMD → site → wwwroot (Click download arrow to backup folder)
 - a. Confirm the correct appSettings.json files were deployed via Kudu. There should only be 2, one named appSettings.json and one named appSettings.Prod.json.
 - b. Confirm appSettings.Prod.json values: both BaseUrl and Scope should contain TMP Prod Url, and the AppId should have the correct AppId for the Production Environment. This value can be found in several locations such as the Web.Config Settings in any of the TMP App Services that send Data to TMP such as IHS. Use the value from CrmAppId setting for confirmation. Update the Default Log Level to "ERROR" in the Logging section.

- c. Open the web.config file and confirm the EnvironmentName attribute contains "Prod". This is used by the App Service to determine the correct appSettings.json to use.
- d. Update the Log Level in the log4net.config file. Set the value for the "level" element in the root section to "ERROR" and Save.

14. Repeat Steps 2 thru 9 for the other remaining Region (i.e. East or South).

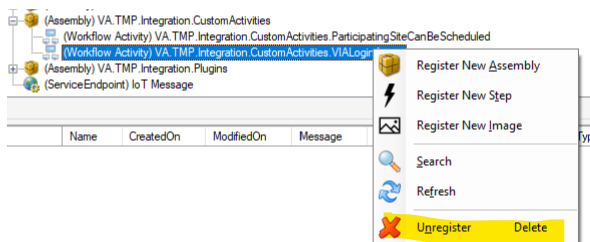
IV. TMP-2884: Clean up old VIA login code and settings

1. Login To Power Apps | Home
2. Search Default Solution ->Left Nav -> Processes -> Search Via Login Action
3. Select Process -> Turn off -> Delete from this environment

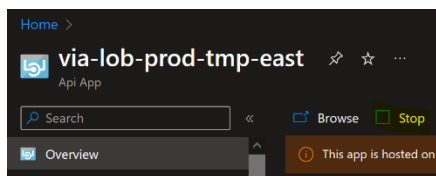


Open Plugin Registration Tool and Connect to Target Environment.

1. Locate the VA.TMP.Integration.CustomActivities Plugin.
2. Unregister the VIALoginAction Workflow Activity.



3. Log into Azure.
4. Navigate to the via-lob-prod-tmp-east App Service in the EIS Subscription. Click the **Stop** button to stop the App Service.



5. Repeat Step 4 - 5 for the other remaining Region (i.e. East or South).

V. TMP-3081: INC35168772 Enable/Disable buttons showing up on Resource: User

Verify that the Enable and Disable buttons from the Resource: User ribbon have been REMOVED, if not follow steps below

1. Create a solution with the Resource:User entity.
2. Open the solution in the Ribbon Workbench.
3. Locate both the Enable and Disable buttons on the Mscrm.HomepageGrid.systemuser.MainTab.
4. Right-click and select **Hide** for each button.
5. Confirm that each button has been added to the Hide Actions section of the Solution Elements window.
6. Publish the form changes.
7. Navigate to **TMP > Metadata & Configuration > Resource: User**.
8. Navigate to **Resources > Users**.

- Click on a User and confirm that the Enable and Disable buttons do not show.

VI. TMP-3194: The VA logo is not 508 compliant

To modify the alt text for the VA logo:

- Log in to TMP.
- Select **Settings > Advanced settings**.
- Select **Customizations**.
- Select **Themes**.
- Select **VA TMP** under All Themes.
- Replace the existing text in the Logo Tooltip field with the following.
VA Seal U.S. Department of Veterans Affairs
- Click **Save**.
- Click **Publish Theme**.
- Verify the logo has been updated by hovering your cursor over the logo.

VII. TMP-3269/TMP-3274: Delete expired secrets

- Login Azure - <https://portal.azure.us/vaazuregov.onmicrosoft.com>
- Click App Registration.
- Click All Applications.
- Search TMP-MAG-P (TMP-MAG-Prod-Server-SP and TMP-MAG-Prod-SP).
- Click application.
- Click Manage.
- Click Certificates and Secrets.
- Click Delete on secret expire(d) 29 Nov 2024.

VIII. TMP-3067: INC32183177 TMP is not handling the MVI identifier response status correctly

- Log in to TMP.
- Select **I from the Left Bottom Nav**
- Select **Integration**
- Select **Integration Settings**
- Select **SelectedPersonFakeResponseType** under Active Integration Settings.
- Replace the existing value field with 1



The screenshot shows a configuration page titled "SelectedPersonFakeResponseType - Saved" under the "Integration Setting" section. There are two tabs: "General" (selected) and "Related". The "General" tab contains a form with the following fields:

Name	SelectedPersonFakeResponseType
Value	1

At the bottom of the form, there is a search bar containing the text "Schafer, Bryan" with a magnifying glass icon on the left and a close button (X) on the right.

- Click **Save**.

Deployment Verification & Testing Procedure

Testing for 5.2.6 will be done in 3 phases.

- SQA: The SQA team will complete regression testing and testing all updates in the SQA environment, using Postman to test the API updates.
- Preprod: Users identified in the MOUs will perform regression testing and test the updates, excluding the API updates. The CCST team and their UAT testers will test the API updates.

3. Production: Business will perform regression testing and test the updates. The CCST team and their UAT testers will test the API updates.

Test cases can be found in the following Teams folder.

TMP 5.2.6

TMP 5.2.6 Backout and Rollback Plan

Redeploy the backups taking prior to deployment.

Rollback Verification Procedure

Manual confirmation of the environment. Confirm any modifications made during the deployment are no longer present and compare file dates to confirm the backups are deployed. Some smoke testing may be required.

Deployment, Testing, and Rollback Checklist

This section will be completed once each task is complete.

Activity	Date	Individual who completed activity
SQA Deployment	12/16/2024	
SQA Testing Completed	1/21/2025	
Preprod Deployment	1/21/2025	
Preprod Testing Completed	TBD	
Production Backup	TBD	
Production Deploy	TBD	
Production Testing	TBD	
Production Go/No Go	TBD	
Production Rollback	TBD	