



Beneficiary Travel

Release Notes

DGBT*1.0*32

October 2018

Department of Veterans Affairs
Office of Information and Technology (OIT)
Product Development

Revision History

Change	Date	Tech Writer, Project Manager
Original document.	March 2017	redacted
Some technically significant updates.	February 2018	redacted
Updated process based on IAM Requirements change	October 2018	redacted

Table of Contents

Overview	4
Web Server/Regional Configuration.....	5
Install the CA SiteMinder WebAgent.....	5
Export the Web Server Certificate to .pfx File in IIS 7	5
Separate the Private Key and SSL Certificate	6
Cache/Site Configuration	7
Cache SSL/TLS Configuration	7
Import the XML file.....	8

Overview

The Beneficiary Travel (BT) Dashboard is a web-based application designed to be used along with the existing VistA Beneficiary Travel Claim option in concurrent sessions for a patient. BT Dashboard calculates the driving mileage from the patient's address to a configured set of institutions. Using the Beneficiary Travel Claim menu, the application automatically synchronizes with travel claims as claims are created in VistA. BT Dashboard also displays patient appointments, claims, notes, orders, and consults. Patch DGBT*1.0*32 upgrades the existing BT Dashboard login methodology by allowing users to authenticate using their PIV card, rather than Access/Verify codes.

Before the BT Dashboard PIV authentication can be used on a workstation, the CA SiteMinder WebAgent must be installed and the Cache Instance must be configured. This involves:

1. Installing the CA SiteMinder WebAgent
2. Exporting the Web Server certificate (.pfx)
3. Separating the Private Key and SSL Certificate
4. Configuring SSL/TLS in Cache
5. Importing the XML file

Web Server/Regional Configuration

Install the CA SiteMinder WebAgent

This part will need to be done at each Web Server (which means that this will probably be done once per Region).

As a part of the Identity Access Management (IAM) teams [VistA Integrated Web Applications](#) integration pattern, the [CA SiteMinder WebAgent](#) must be installed on the Beneficiary Travel Dashboard web server. Upon verifications that the required IP addresses and ports are open on the web server, the IAM team will provide a separate CA SiteMinder WebAgent Installation Guide as well as configuration instructions.

Export the Web Server Certificate

You will need to export the web server certificate and private key, used to encrypt your Beneficiary Travel Dashboard URLs, to a .pfx file.

Export the Web Server Certificate to .pfx File in IIS 7

Instructions from: <https://www.digicert.com/ssl-support/pfx-import-export-iis-7.htm>

1. On the Web Server in the Start menu click **Run** and then type *mmc*.
2. Click **File > Add/Remove Snap-in**.
3. Click **Certificates > Add**.
4. Select **Computer Account** and then click **Next**. Select **Local Computer** and then click **Finish**. Then close the add standalone snap-in window and the add/remove snap-in window.
5. Click the + to expand the certificates (local computer) console tree and look for the personal directory/folder. Expand the certificates folder.
6. Right-click on the certificate you want to backup and select **ALL TASKS > Export**.
7. Choose **Yes, export the private key** and **include all certificates in certificate path if possible**.
Warning: Do **not** select the delete private key option.
8. Leave the default settings and then enter your password if required.
9. Choose to save the file and then click **Finish**. You should receive an "export successful" message. The .pfx file is now saved to the location you selected.

Once you have the .pfx file, you will need to send it to the IAM team.

Separate the Private Key and SSL Certificate

You will need to separate your web server Private Key and SSL Server Certificate from the .pfx file created in the previous step. You can use the OpenSSL commands below to create the two files.

```
openssl pkcs12 -in certificate.pfx -nocerts -out private_key.pem -nodes
```

```
openssl pkcs12 -in certificate.pfx -nokeys -out certificate.cer
```

The newly generated .pem and .cer files will be used in the next step.






(Note: If you do not have access to OpenSSL, please open a CA ticket with the NTL.APP.VistA.Bene Travel 1_0 Dashboard group and ask for your ticket to be escalated to Tier 3.)

Cache/Site Configuration

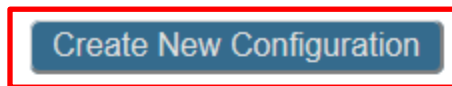
This part will need to be done at each Cache System Management Portal (which means that this will probably be done once per Site).

Cache SSL/TLS Configuration

In the Cache System Management Portal click 'SSL/TLS Configuration':

 Home	Configuration »	Users
 DeepSee	Security »	Roles
 System Operation	Licensing »	Resources
 System Explorer	Encryption »	Services
 System Administration	Enterprise Manager	Security Domains
		Applications »
		SSL/TLS Configurations
		X.509 Credentials
		System Security »
		Auditing »
		Security Advisor
		Mobile Phone
		Public Key Infrastructure

Click 'Create New Configuration':



The following is a list of SSL/TLS configurations:

Page size: Max rows: Results: 2 Page: [|<](#) [<<](#) **1** [>>](#) [>|](#) of 1

Name	Description	Enabled	Type		
dashboardsoi	Patch DGBT*1.0*32	Yes	Client	Edit	Delete
encrypt_only	Patch XOBW*1*4	Yes	Client	Edit	Delete

Enter the fields as shown below:

- Ensure that your configuration name is ‘dashboardssoi’.
- Under ‘This client’s credentials’
 - The ‘File containing this configuration’s X.509 certificate’ is the SSL certificate from the web server (.cer).
 - The ‘File containing associated private key’ is the private key file created earlier in this guide (.pem).

Save **Cancel** **Test**

Use the form below to edit an existing SSL/TLS configuration:

The screenshot shows a configuration form for an existing SSL/TLS configuration. The form is titled 'Configuration Name' and has a text box containing 'dashboardssoi'. Below this is a 'Description' field with 'Patch DGBT*1.0*32'. The 'Enabled' checkbox is checked. The 'Type' is set to 'Client' (radio button selected). The 'Peer certificate verification level' is set to 'None' (radio button selected). There are two 'Browse...' buttons for 'File containing trusted Certificate Authority X.509 certificate' and 'File containing Certificate Revocation List'. The 'This client's credentials' section is expanded, showing a note: 'Note: Only necessary if this client will be asked to authenticate itself to servers.' It contains two 'Browse...' buttons for 'File containing this configuration's X.509 certificate' and 'File containing associated private key'. The 'Private key type' is set to 'RSA' (radio button selected). The 'Password' section has three options: 'Enter new password', 'Clear password', and 'Leave as is' (radio button selected). The 'Cryptographic settings' section shows 'Protocols' with 'SSLv2' and 'SSLv3' unchecked and 'TLSv1' checked. The 'Enabled ciphersuites' field contains 'TLSv1:SSLv3:ADH:LOW:EXP:@STRENGTH'.

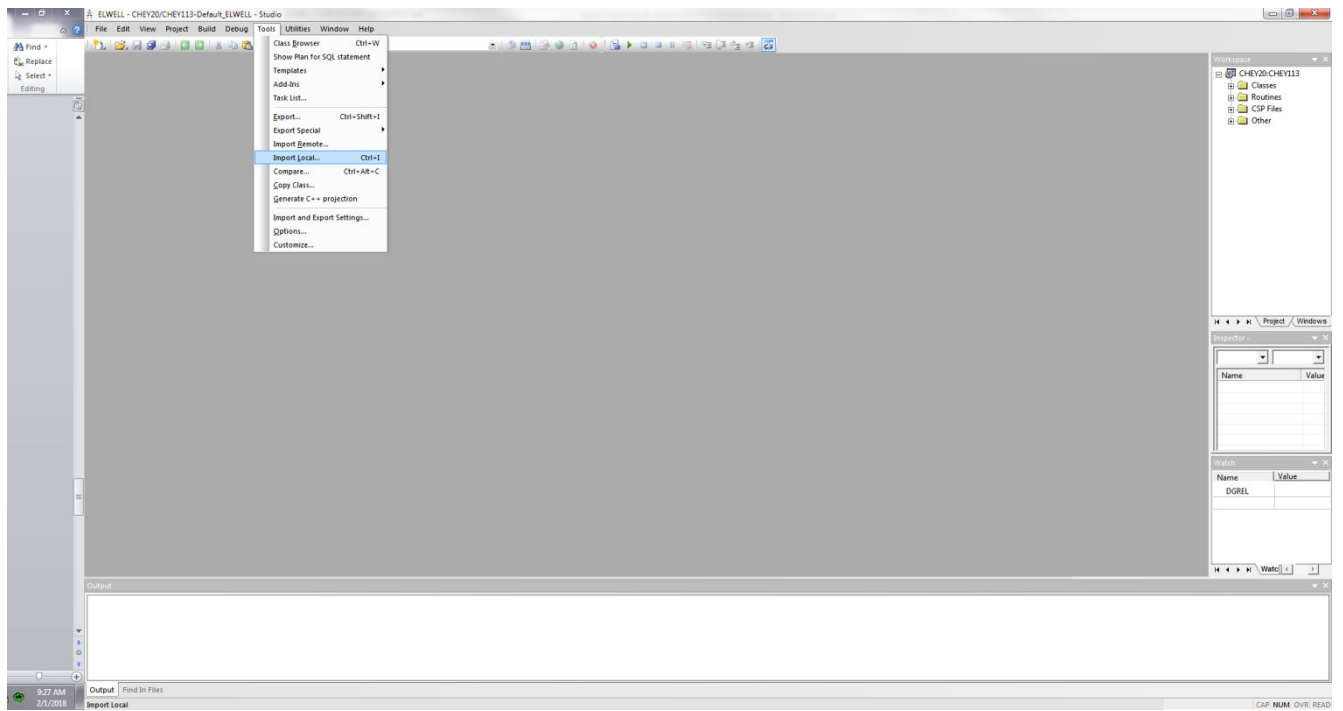
Click ‘Save’.

Import the XML file

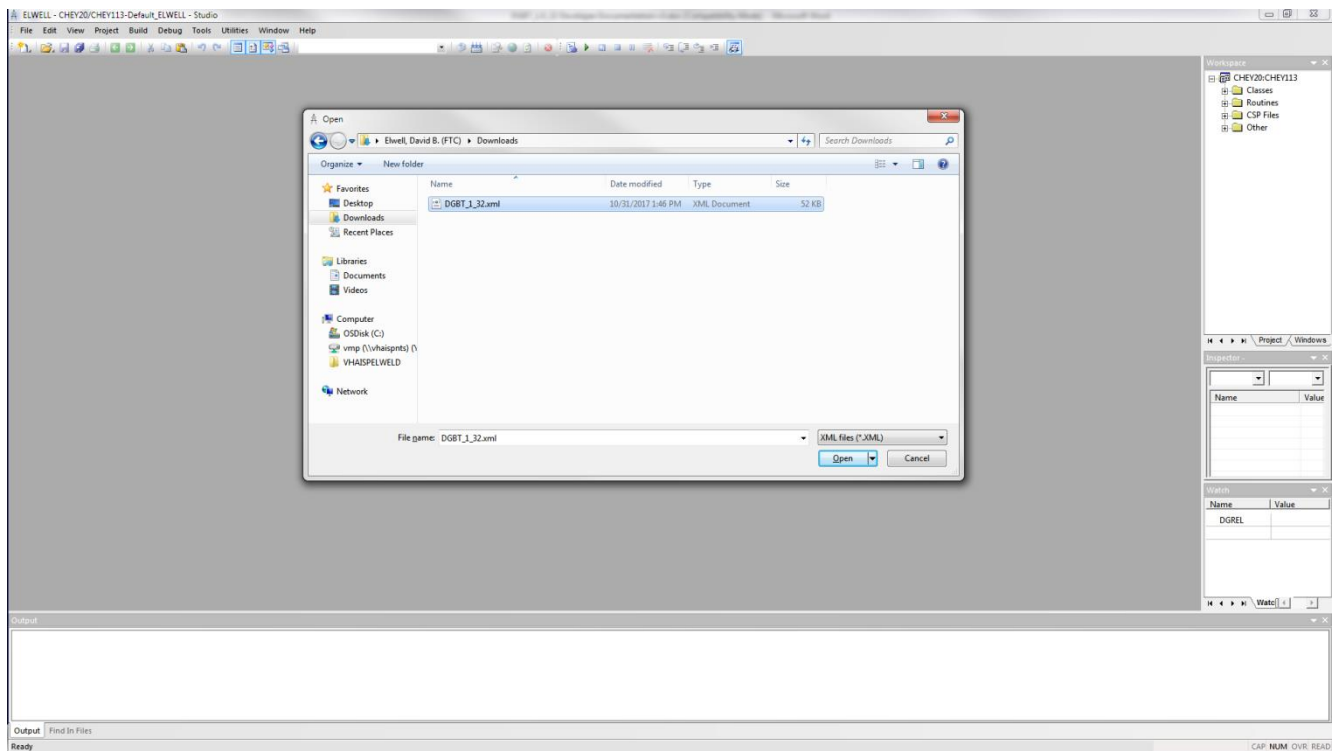
Use Caché Studio to import the source code XML.

Note: Caché Studio should be connected to your VistA server in your station’s namespace.

1. Click the **Tools** menu and select **Import Local**.



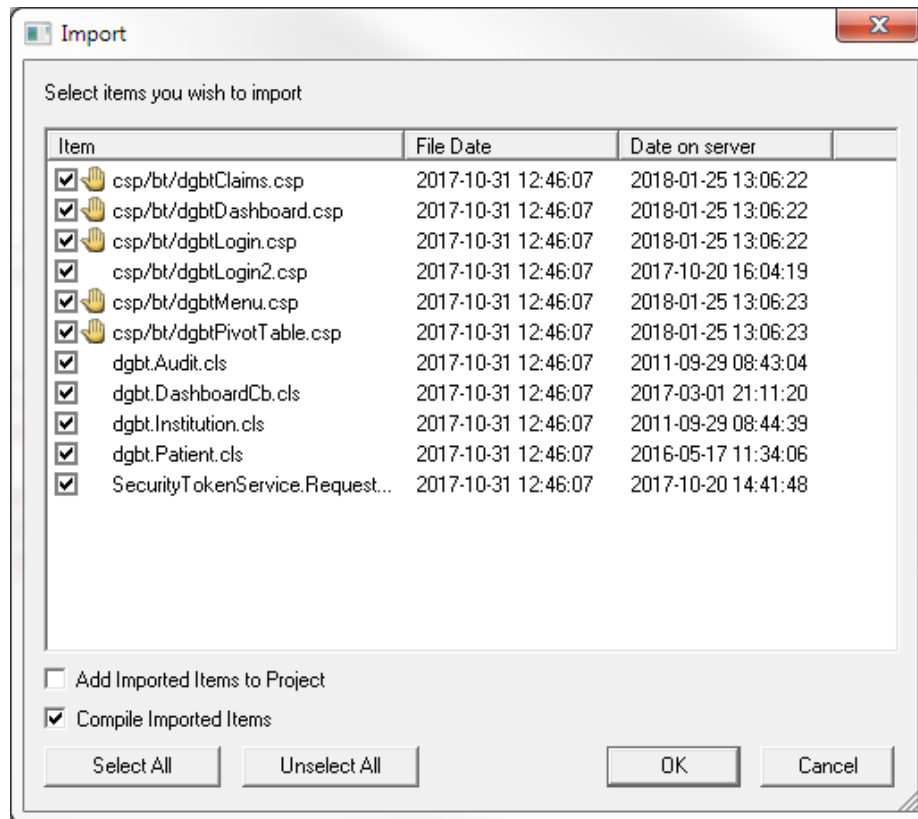
Caché>Studio>Tools>Import Local



Beneficiary Travel – Studio Open window

2. Browse to the DGBT_1_32.xml file retrieved from download.vista.med.va.gov.

3. Click the **Open** button.



Beneficiary Travel – Studio Import window

4. Ensure the **Add Imported Items to Project** checkbox is **not** selected and that **Compile Imported Items** is selected.
5. Click the **OK** button to import the **Beneficiary Travel Dashboard .csp and .cls** project files.

The End.