Configuring DBXL for Basic Authentication

If you have only Basic Authentication enabled on your SharePoint site, there are some additional steps required to enable InfoPath browser forms to call DBXL or other web services. InfoPath Form Services cannot impersonate the user when calling web services that only support Basic Authentication. It requires Windows Authentication be enabled at least on an extension site. Through IIS configuration, the extension site can be restricted to server-side communication. All external user authentications will still be done using Basic Authentication.

Certain DBXL-to-SharePoint functionality will be limited when using Basic Authentication. SharePoint mappings will need to use Single Sign-On (SSO). When DBXL publishes a form template to SharePoint, it will be created under the SSO configured credentials. User updates pushed to SharePoint from DBXL will also show as modified by the SSO identity.

Configuration requires:

- enabling Basic Authentication on the QdabraWebService virtual directory
- configuring an extension site to allow Windows Authentication.

ENABLING BASIC AUTHENTICATION FOR DBXL

In IIS manager, navigate to the web site where DBXL is installed. Select QdabraWebService and then double-click Authentication (Figure A1). Right-click Basic Authentication and select Edit (Figure A2). Enter your values used for the parent SharePoint site (Figure A3). Then right-click Basic Authentication and select Enable (Figure A4). Next, right-click Windows Authentication and select Disable (Figure A5).

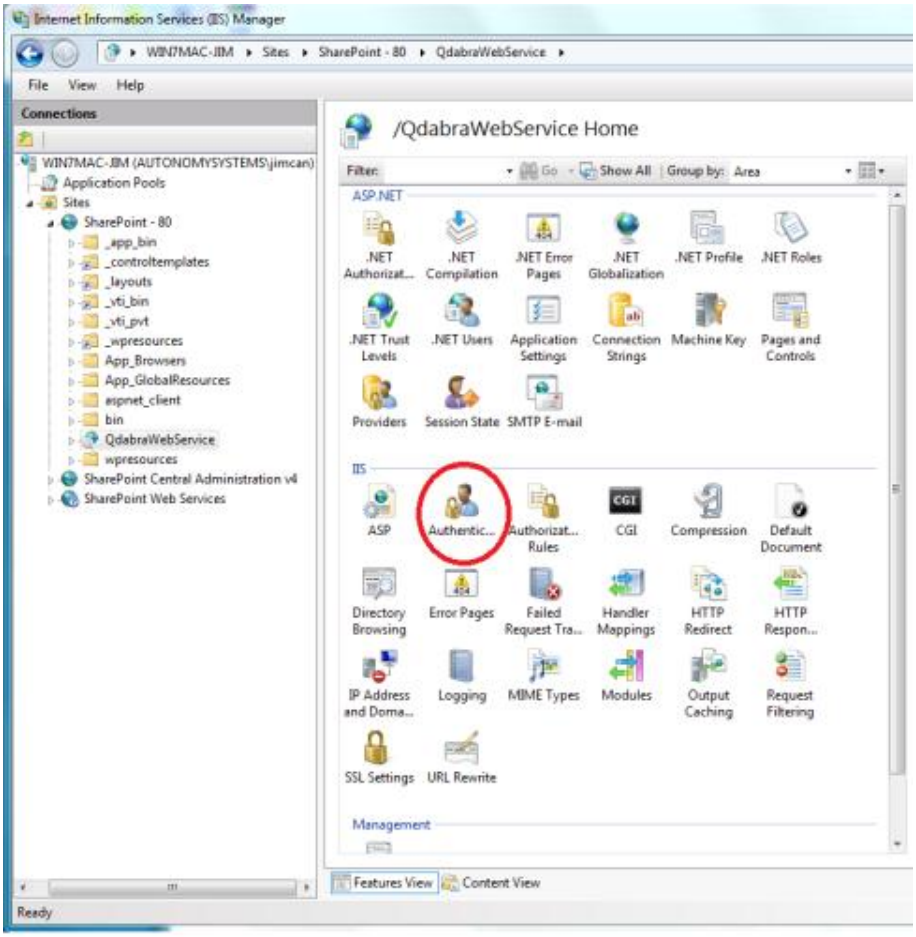

Figure A1.

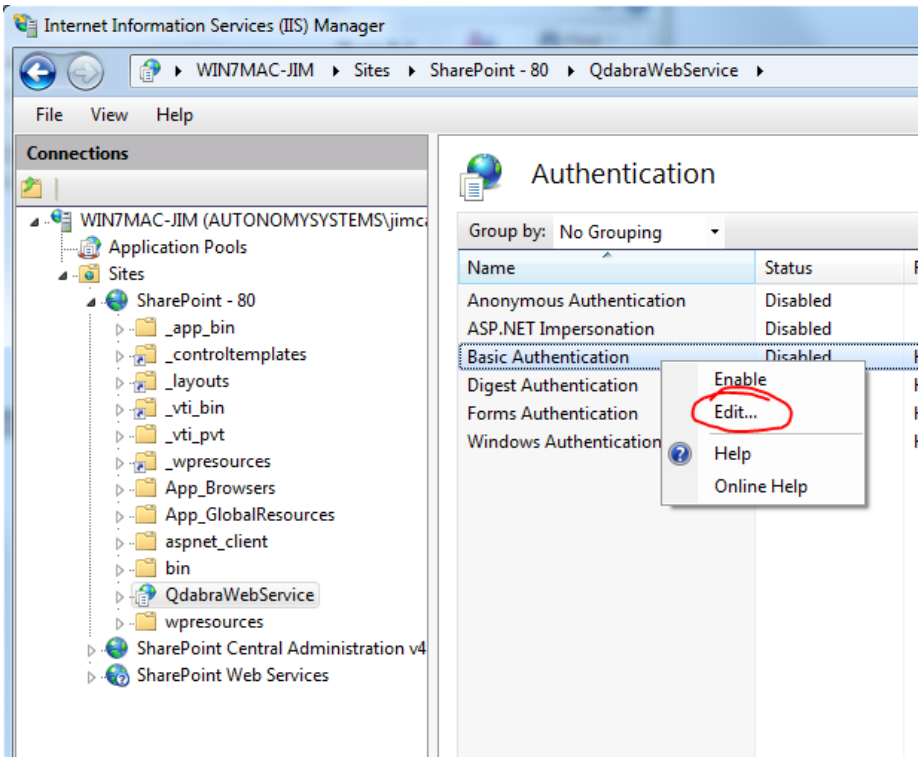

Figure A2.

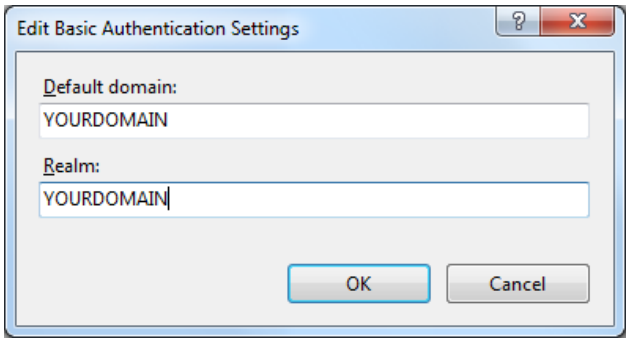

Figure A3.

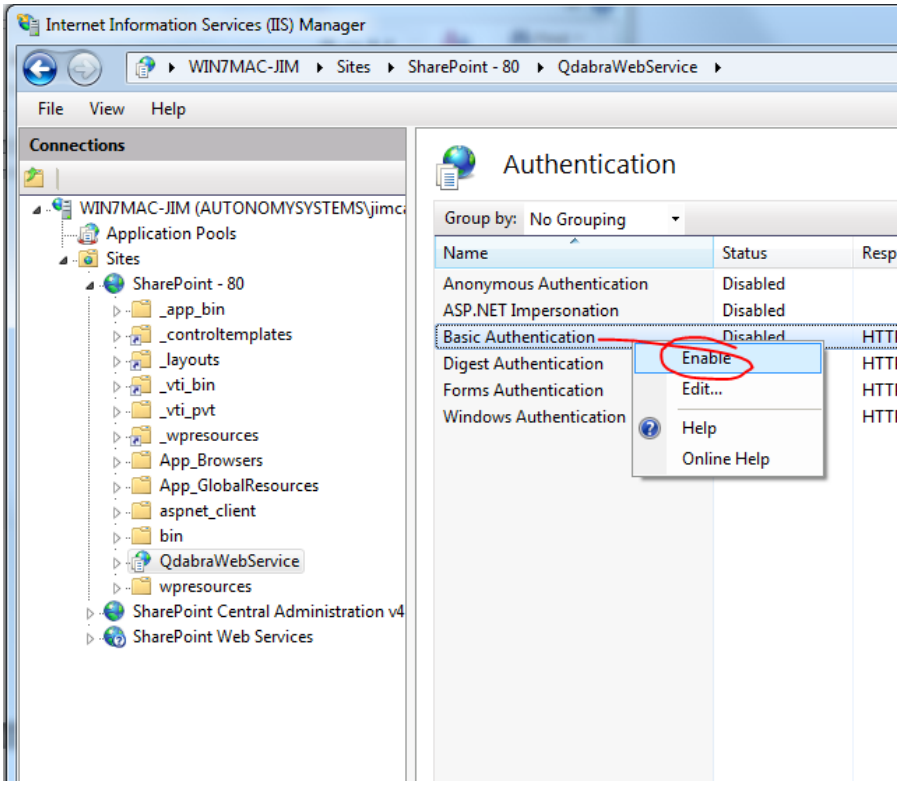

Figure A4.

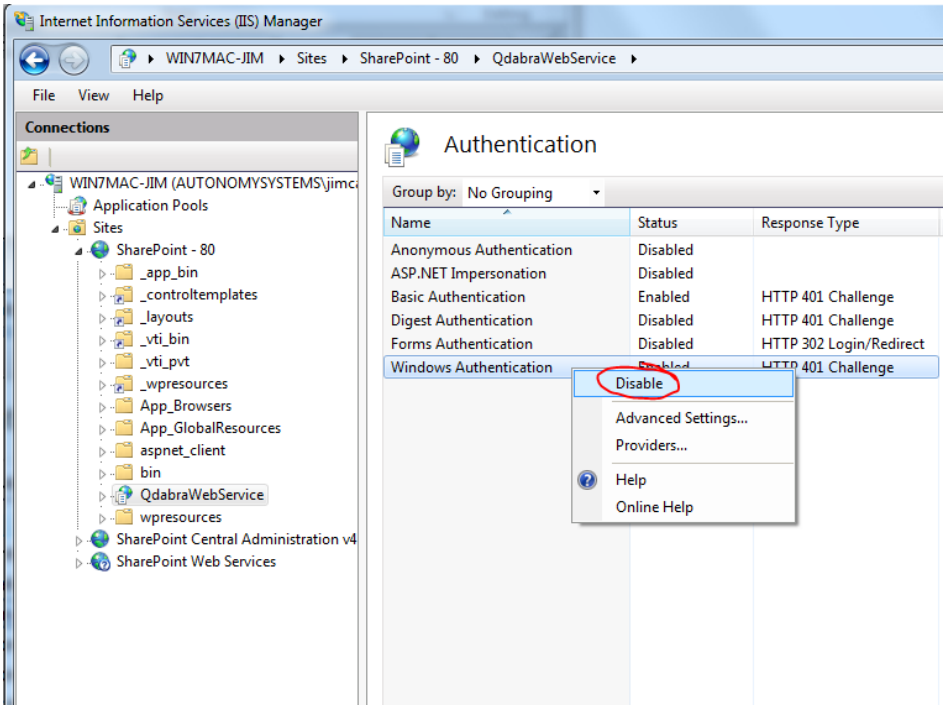

Figure A5.

CONFIGURING A WEB SITE EXTENSION

Extending the SharePoint site allows granting access to the same SharePoint site content and DBXL using an alternate authentication scheme. In this case, Windows Authentication will be used. After creating the web extension in SharePoint Central Administration, the QdabraWebService virtual directory will need to be created.

The QdabraWebService virtual directory must be added to the extended site.

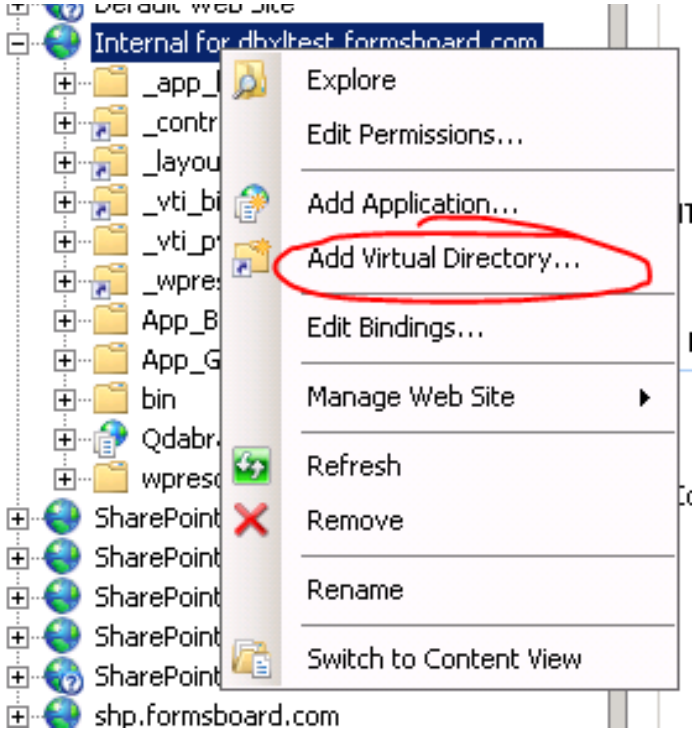

Figure B1.

The virtual directory will point to the physical QdabraWebService location used by the Basic Authentication site. Enter QdabraWebService for the alias, and the physical path to the QdabraWebService folder.

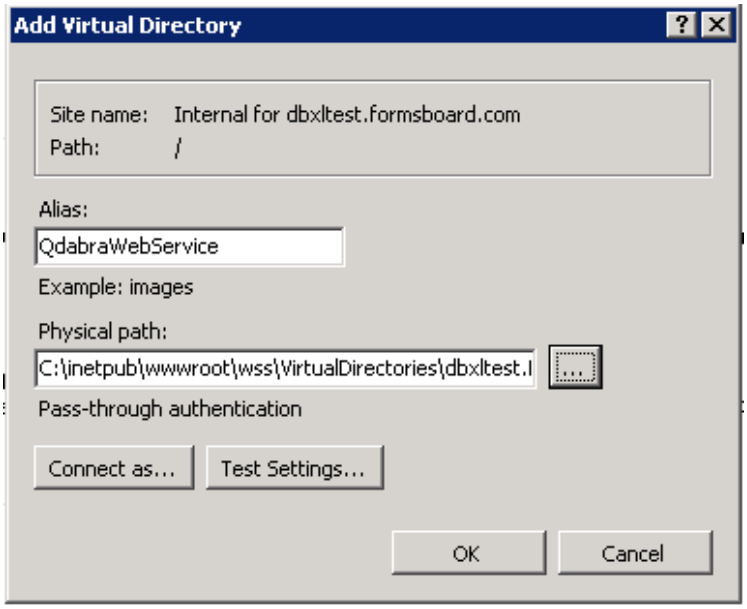

Figure B2.

Convert the QdabraWebService virtual directory to an application by right-clicking the folder and selecting Convert to Application.

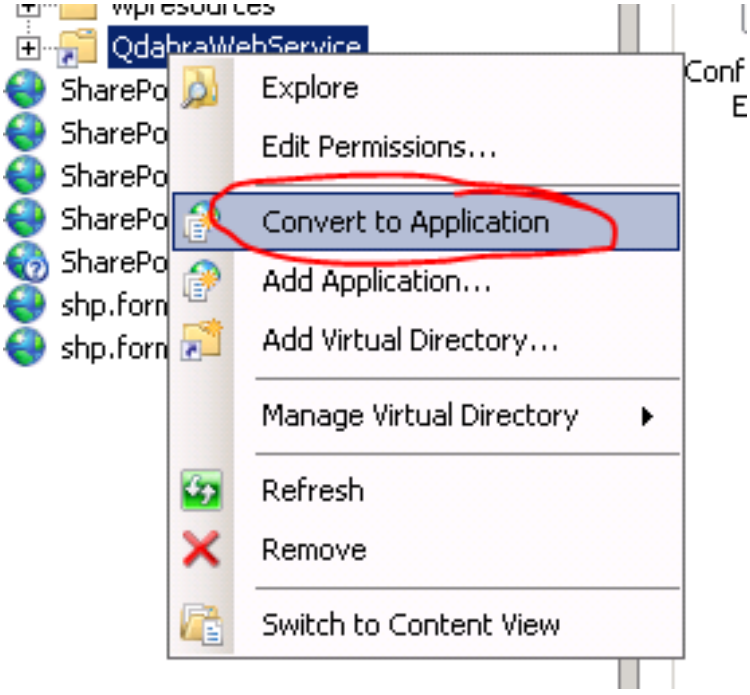

Figure B3.

At this point, the site is configured for Windows Authentication.

In my test scenario, the port number assigned was 22327. If you use UDC files containing a url to ***http://servername:22327/QdabraWebService/...***, InfoPath will transform it to the https://site.domain.com/QdabraWebService/... because it matches an alternate access mapping. This will cause the connection to fail because Windows Authentication is not enabled on that site.

To work around this problem, you need to add a port to the site which is not included in the Alternate Access Mappings. In this case, I added ported 22328 and updated the UDC files to reference http://servername:22328/QdabraWebService/...

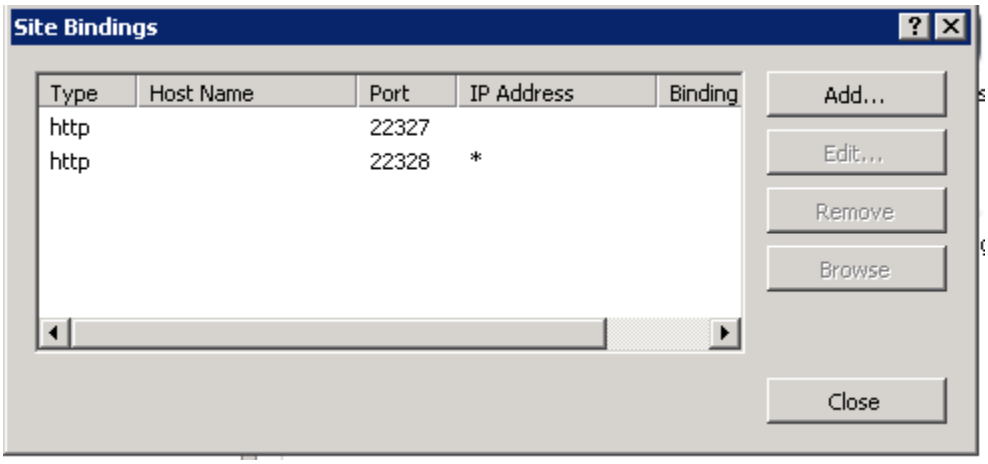

Figure B4.

SUPPORT

If you have questions about the information in this document, please contact us for assistance.

Licensed customers can contact us via **Support@Qdabra.com**.

Alternatively, please use the InfoPathDev.com Qdabra Product support forums to request help.