System Galaxy Procedure

LaunchPoint ◆ Adding a Signed Certificate to IIS

How to add a Signed Digital Certificate to the IIS Web Site for secure/encrypted connections with LaunchPoint Web Clients.

- Obtaining a signed SSL Certificate from a trusted Certificate Authority.
- Binding the signed SSL Certificate to IIS root (Default Web Site).
- Configuring a new LaunchPoint desktop shortcut to initiate a secure connection.

SG 11.8.5 (or higher)

Published JAN 2024

Table of Contents

Managing Digital Certificates for LaunchPoint On-Premises (MS-IIS)

This guide covers how to obtain a *signed Digital Certificate* and assign the Certificate to the IIS Default Web Site to support secure encrypted connections with the LaunchPoint web client on-premises deployment.

OUTLINE

The process for securing the communications for LaunchPoint is outlined below.

1. Submit a *Certificate Request* from the computer hosting IIS to a trusted Certificate Authority.
2. Download the *Signed Certificate* to an accessible folder on the computer hosting IIS.
3. Import & Bind the Certificate to the IIS Default Web Site.
4. Remove the old site binding to http/port 80 and Restart the IIS Web Site.
5. Create a new Desktop Startup Shortcut for each LaunchPoint client.
6. Verify the new Desktop Shortcut at each client to verify it opens the login page to the secure URL/HTTPS prefix.
7. (optional) Change Icon of the Desktop Shortcut to use the LaunchPoint logo.

REQUIREMENTS …

- **System Galaxy Software and core GCS Services must be installed** and operating on the *Galaxy Communication Server* – **which includes the *GCS Web API Service*** – in order to verify LaunchPoint will run correctly after the Digital Certificate is imported.
- **Microsoft IIS Component must be installed on the main communication server.**
  You can install IIS from the GCS Installation Media (ISO/USB).
- **SG LaunchPoint On-Premises must be installed on the server**.
- **You must obtain a signed Digital Certificate from a trusted Certificate Authority.**
  An unsigned or self-signed certificate will encounter *secure connection errors* and will not work in a production environment.
- **You must bind the signed Certificate to the root of the IIS website.**
- The *System Galaxy Communication Server* and *Web Client PCs* must be online on the LAN in order to verify LaunchPoint will run correctly after the signed Digital Certificate is installed.

Obtaining a Signed Digital Certificate

This section covers how to obtain the CSR Certificate.

IMPORTANT: Galaxy recommends you purchase the longest certificate lifespan possible. The LaunchPoint app communication will stop working when the Certificate expires.

ASSUMPTIONS

- The System Galaxy main communication server and core services are installed and are online and running – including the *GCS Web API Service* that is required by LaunchPoint.
- IIS has been installed on the appropriate computer that will host the IIS web server. This can be installed from the SG Installation Media (USB/ISO_main)
- The LaunchPoint has been installed on the computer after the IIS was installed.
- A signed certificate must be purchase from a *trusted Certificate Authority* to. Galaxy makes no recommendations as to which brand will provide the best security or best value.
- The Certificate Request CSR must be made from the same computer where IIS is installed.

1. The user will submit a **Certificate Signing Request (CSR)** from the computer where IIS is installed, to a *trusted Certificate Authority* of your choosing (such as Comodo, GoDaddy, Semantic, Verisign, etc.).
2. The *Certificate Authority* will issue a *signed Digital Certificate* (TLS/SSL Certificate).
3. The *digital certificate* must be downloaded onto the IIS web server and placed in a folder that you have permissions to access, such as My Documents or Downloads.
4. Proceed to the next section.

Importing a Certificate to IIS Default Web Site

This section describes how to add/bind a digital certificate to the IIS Web Site.

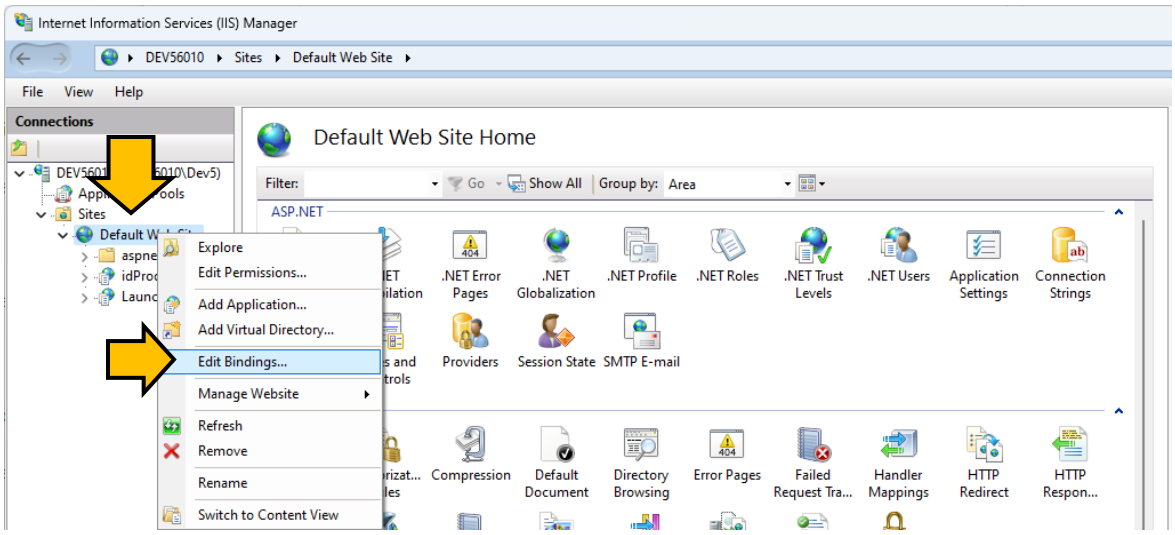
The process of adding the certificate to the IIS Site Binding will automatically import the certificate into the **Web Hosting Certificate Store** with a privacy key.

REQUIREMENTS

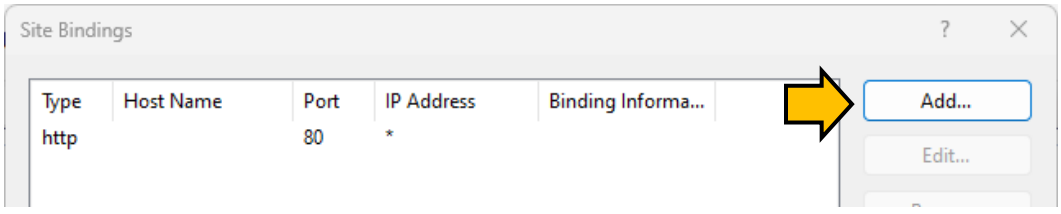
- The digital certificate must be signed by a trusted Certificate Authority. A self-signed or unsigned certificate will cause errors and cannot be used in a live/production environment.
- The *signed digital certificate* must already be downloaded to the computer hosting IIS to folder that the user has permissions to access, such as My Documents.

STEPS

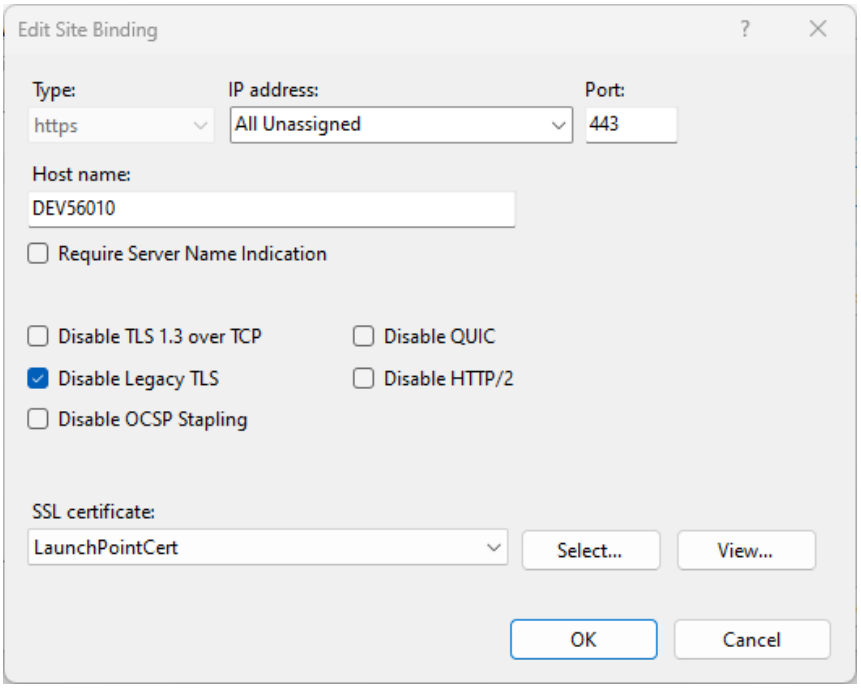
1. Open the ***Administrative Tools window*** (Windows Tools) on the computer that is hosting IIS. You can do this by, typing "Administrative Tools" into the Windows Search field on the task bar.
2. Double-click on ***Internet Information Services (IIS) Manager*** to open the IIS Manager window.
3. In the *IIS Connections Panel* (left panel), expand the branches until you will see the *Default Web Site*.
4. Right-click the ***Default Web Site branch*** and choose 'Edit Bindings…' from the menu.



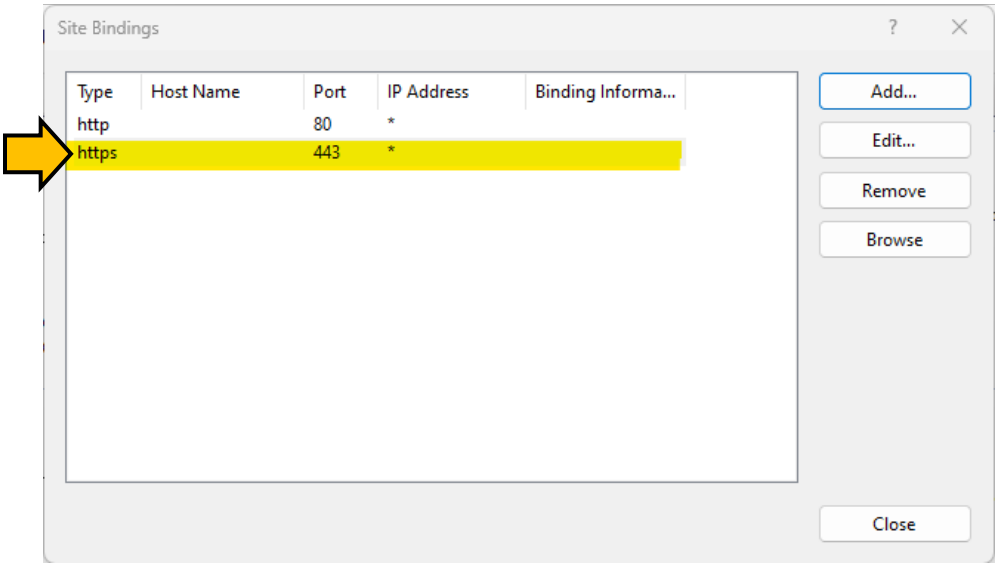
5. When the *Site Bindings window* opens, click the ADD button to open the Edit Bindings dialog.



6. In the *Edit Site Bindings* window, do the following …
   a. Set the **Type** field to "https".
   b. Set the **IP Address** field to "All Unassigned".
   c. Set the **Port** field to "443".
   d. Type the **Host Name** to the appropriate "friendly name".
   e. Set the '**Disable Legacy TLS**' checkbox to checked.
   f. Select the newly obtained certificate from the **SSL Certificate** droplist, that you purchased for IIS/LaunchPoint.
      - Clicking **VIEW** will display the file specifications of the selected certificate.
      - Clicking **SELECT** allows user to browse for the certificate file, if the certificate is not listed.
      -
   g. Click **OK** to add (bind) the chosen *SSL Certificate* to the Default Web Site.



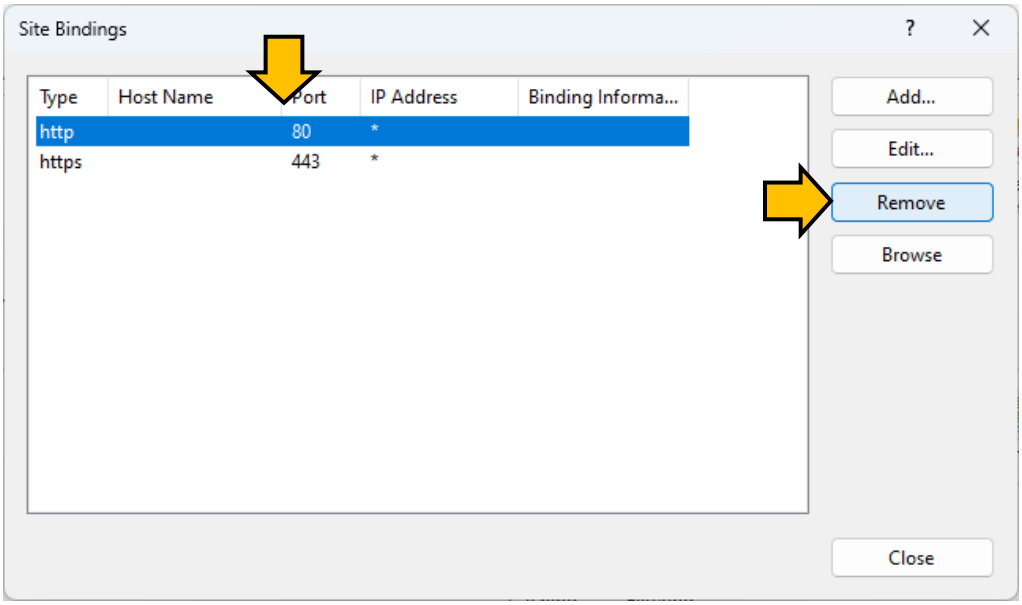
7. In the Site Bindings listview, the new secure port (https/port 443) is added to the list.



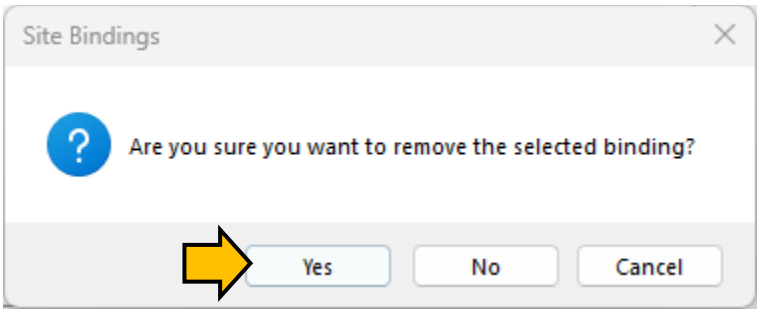
8. Proceed to the next section to remove the unsecure port.

Removing the Unsecure Binding

1. In the Site Binding screen, select (highlight) the **http/80** address
2. Click **Remove** button.



3. Click **YES** when prompted to confirm you want to delete the unsecured binding.

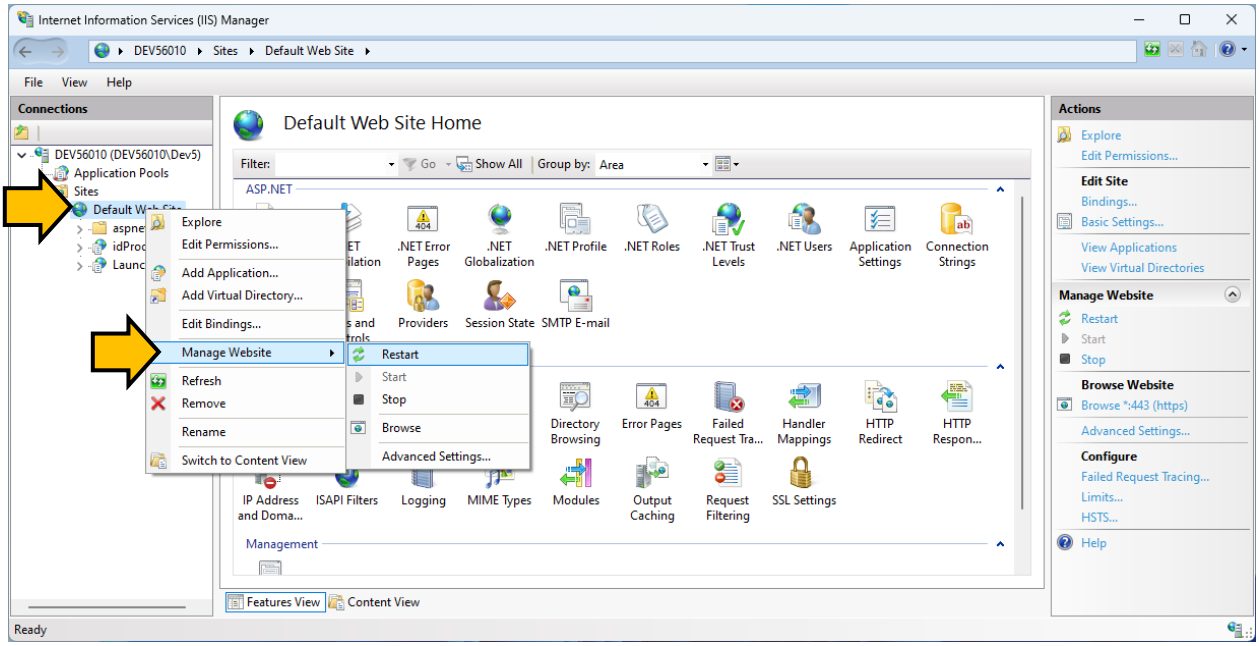


4. Click **Close** button to exit the Site Bindings screen.

Restart/Refresh the IIS Web Site

You must restart the IIS Default Web Site to refresh the new binding.

1. In the IIS Manager window, expand the Connection branches as shown
2. Right-click on the IIS Default Web Site
3. Choose 'Manage Website >' option and then chose 'Restart…' from the menu.



Creating a New Client Desktop Shortcut

You must create a new Client Desktop shortcut to use the new secure https address / port 443 on every client workstation that runs the LaunchPoint application. The old shortcuts must be deleted.

DELETE THE UNSECURE DESKTOP SHORTCUT

1. The recommended way to delete the *unsecure shortcut* from the client desktop, is to perform a <Shift+Delete> - as follows …

   a) Right-click the unsecure Desktop Shortcut (that points to Port 80).

   b) Press and hold the Shift key while selecting the option to Delete it from the popup menu.

   c) Click YES when prompted to confirm that you want to "permanently delete" the shortcut

   RESULT: The shortcut will be permanently deleted. It will not be in the trashcan, so no one can mistakenly restore it - plus you won't need to flush the customer's trashcan.

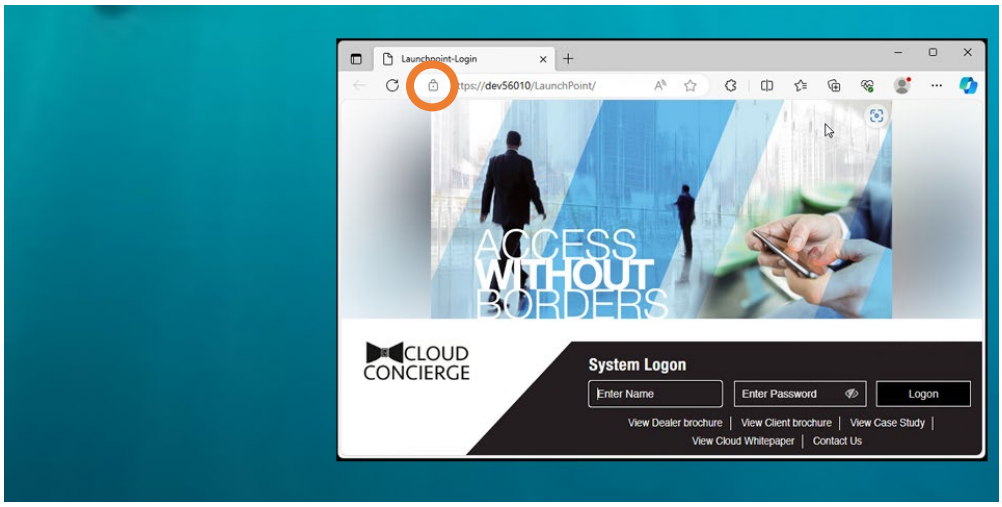
2. You need to do this at every Client PC that has the old shortcut.

CREATE THE NEW SECURE DESKTOP SHORTCUT

3. Open the preferred browser and reduce the screen size to allow the desktop to be visible.

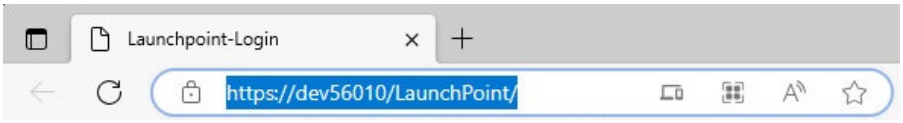
4. In the browser address bar, type the new LaunchPoint URL using the secure https prefix.
   ("https://your-server/LaunchPoint/")

   RESULT: The browser should display the *LaunchPoint Login page* with a **lock symbol** in the address bar.



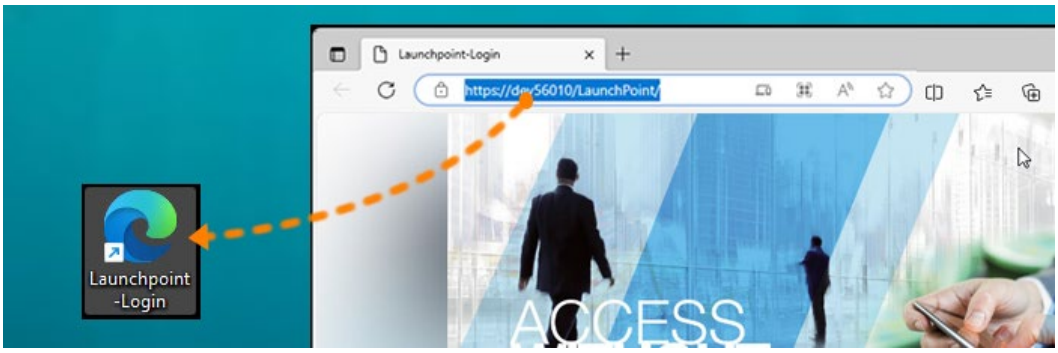
5. To create the new **Desktop Shortcut**, do the following …

   a) Select (highlight) the entire URL, including the https prefix.
   TIP: To make the https prefix to be visible, you can single-click inside the address bar if needed.



   b) With the full **URL** highlighted, drag-n-drop it from the browser onto the desktop.

   RESULT: The browser shortcut is automatically created for the secure LaunchPoint website.



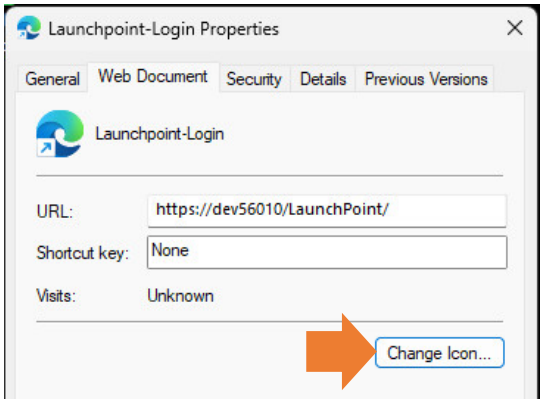
   c) Double-click the new LaunchPoint shortcut to verify it opens the secure "https" *LaunchPoint login page*.
   ("https://your-server/LaunchPoint/")

6. You will need to do these steps on every Client PC that needs the new Desktop Shortcut.

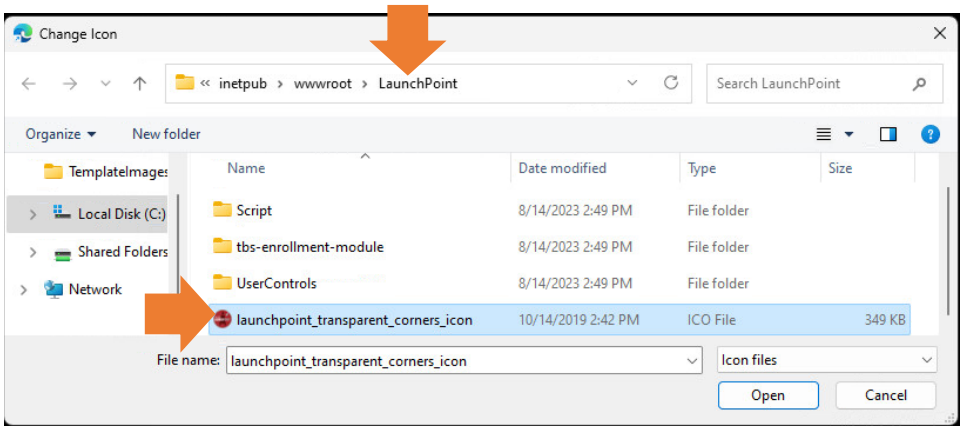
Link the LaunchPoint Icon to the Desktop Shortcut (optional)

When the new Desktop Shortcut is created, it will display the browser brand icon by default. You can restore the LaunchPoint icon as follows …

1. Right-click on the new LaunchPoint Desktop Shortcut.
2. Choose 'Properties' from the popup menu to open the *Properties* screen.
3. On the Web Document tab, click [Change Icon…] button.



4. On the Change Icon window, click Browse …
5. In the LaunchPoint web folder, scroll down to the "launchpoint_transparent_corners_icon" ICO file.
6. Double-click on the LaunchPoint ICO file to choose it.



7. Click OK in the Change Icon window to accept the new icon path.
8. Click APPLY in the *Properties screen* to save the new LaunchPoint icon.
9. Click OK to close the *Properties* screen.
   RESULT: The new secure Desktop Shortcut will use the LaunchPoint icon.
10. You will need to do these steps on every Client PC that needs the new Desktop Shortcut.