

Technical White Paper

Web Server Configuration

The following web server configuration instructions apply to UnitySync, Directify, emPass (IIS only), and Infocanon (IIS only). While we use UnitySync as an example throughout the document, the configuration is very similar for all programs. It will be clear in the instructions where and how they differ. If you have any questions at all, please contact support@dirwiz.com for clarification and assistance.

Table of Contents

Web Server Configuration.....	1
Internet Information Services (IIS) versions 8.5 or 10.....	2
Confirm needed Roles and Features are enabled in IIS.....	2
Add Virtual Directory.....	2
Configure Web Service Extensions.....	4
Enable All Unspecified CGI Modules.....	4
Configure Individual CGI extensions for IIS 8.5 or IIS 10.....	5
Handler Mappings.....	5
Edit Default Error Behavior.....	6
Access Your Program Using IIS 8.5 or IIS 10.....	6
Apache.....	8
Red Hat Enterprise Linux 6.x with Apache 2.2.x.....	8
Appendix.....	9
Appendix A: Program-specific .cgi files.....	10
Directify.....	10
emPass.....	10
InfoCanon.....	10
UnitySync.....	10

Internet Information Services (IIS) versions 8.5 or 10

Configuration steps for using Directory Wizards programs with IIS 10 are the same as in IIS 8.5. Please complete all steps and let us know if you have any questions at support@dirwiz.com.



NOTE: *If you do not already have IIS installed on your Windows server, please visit our knowledge base article for further guidance:*

<https://www.dirwiz.com/kb/3108>

If you are installing IIS, you will also want to select the Roles and Features described below at the same time. You will have the option to locate these specific items on the Role Services page of the wizard.

Confirm needed Roles and Features are enabled in IIS

1. Go to the Server Manager and select *IIS* in the left column of the window.
 - (a) Scroll through the pane on the right side of the window until you find *Roles and Features*.
 - i. Is *CGI* listed there? If so, it is enabled. If it is not, please continue.
 - ii. Is *ISAPI extensions* listed there? If so, they are enabled. If it is not, please continue.
 - iii. Is *Windows Authentication* listed there? If so, it is enabled. If not, please continue.
2. Click the *TASKS* drop-down just above the *Roles and Servers* section on the right and select *Add Roles and Features*.
 - (a) The Add Roles and Features Wizard will appear. Click *Next* if you are not already on the page to *Select installation type*.
 - (b) Select *Role-based or feature-based installation* and click *Next*.
 - (c) On the Server Selection page, click *Select a server from the server pool*, then find your server in the Server pool window below and click *Next*>.
 - (d) On the Server Roles page, expand down to click to select the roles you need:
 - i. *CGI* and/or *ISAPI extensions* can be selected under *Application Development (Web Server (IIS) > Web Server > Application Development)*
 - ii. *Windows Authentication* can be selected under *Security (Web Server (IIS) > Web Server > Security)*
 - (e) Then click *Next*>
 - (f) Click *Next*> on the next window, *Features*, to proceed.
 - (g) Finally, click *Install*.
 - (h) The next window will show you the installation progress. Once it completes, click *Close*.
 - (i) If you'd like to confirm the installation, go back to steps 1a and 1b to confirm *CGI* is now listed.

Add Virtual Directory

You must add a virtual directory for the program.

1. Start the IIS Manager. There are two ways to do this:

- (a) From the Start page, go to Server Manager, then highlight *IIS* in the left pane. Right-click the default server shown in the *Servers* section on the right side of the window, then select *Internet Information Services (IIS) Manager*.
- (b) OR from the Start Page, go to Windows Administrative Tools and double-click *Internet Information Services (IIS) Manager*.
2. In the IIS Manager window, expand the default server.
3. Now expand *Sites*.
3. Right-click on the *Default Web Site*.
4. Select *Add Virtual Directory...*
5. Type in the *Alias* you wish to use to access the program.

Use a descriptive name. For instance, if you are working with Directify or emPass, consider using the program name for the alias.



NOTE: In the example below, “*unitysync*” is used, resulting in the following URL:
<http://localhost/unitysync>

6. Select where you would like the virtual directory to point to. This should be the *cgi* folder in your program files.



NOTE: Make sure you use *c:\ProductName\cgi*. Pointing to the *cgi* folder is important for security reasons. DO NOT use simply *c:\ProductName*.

7. Click *OK*.
8. From the main window of the *IIS Manager*, highlight the virtual directory you just created.
 - (a) If you exited after creating your virtual directory, you may need to:
 - i. expand *Sites*
 - ii. then expand the *Default Web Site* to find the virtual directory you created
 - iii. now highlight your virtual directory
9. In the *Features View* menu that appears in the center pane, double-click *Authentication*. The icon for *Authentication* is found in the *IIS* section. Changes can be made in the *Actions* pane.
 - (a) For *UnitySync*:
 - i. Enable *Windows Authentication*.
 - ii. Disable *Anonymous Authentication*.



NOTE: Using this suggested authentication for *UnitySync* will result in an authentication window when you access the *UnitySync* user interface (UI) via *IIS*. If you would like to access the *UnitySync* UI without having to authenticate, you must visit also highlight the *Default Web Site* to *Enable Anonymous Authentication and Enable Windows Authentication*. Please note that changing this setting for the *Default Web Site* will affect all virtual directories, and ensure you want this behavior for all virtual directories before making the change.

- (b) For Directify:
 - i. Disable *Windows Authentication*.
 - ii. Enable *Anonymous Authentication*.
- (c) For emPass:
 - i. Disable *Windows Authentication*.
 - ii. Enable *Anonymous Authentication*.
 - 1. Now right-click on *Anonymous Authentication* and click *Edit...*
 - 2. A user will be selected and specified. You may keep this specific user or click *Set...* to change to another user. In either case, the user specified must be granted certain permissions in your emPass Central Server configuration. Please note what user you've selected as you'll need to perform another step in the emPass Central Server initial installation or upgrade process.



NOTE: *The security of your emPass password sync is ensured by the use of LDAP SSL, and no information is available via the emPass virtual directory.*

You have successfully added the virtual directory and configured authentication.

Configure Web Service Extensions

CGI programs must be allowed to execute. This can be done in one of two ways.

Enable All Unspecified CGI Modules

While this is the quickest way to enable CGI, you will only be able to execute *All Unspecified CGI Modules* if you are running IIS 8.5 or IIS 10 in ISAPI mode. This feature is not available if you are running IIS in Integrated mode.

If you are running IIS 8.5 or IIS 10 in Integrated mode, or if you prefer to configure individual CGI, proceed to [Configure Individual CGI extensions for IIS](#). If you would like to execute *All Unspecified CGI Modules*, continue below:

1. Start the *Information Services (IIS) Manager*.
2. Highlight your server, under the *Start Page* in the left navigation pane.
3. Under the *IIS* section in the main window pane, double-click *ISAPI and CGI restrictions*.

NOTE: *This icon might be found in the Security section.*



4. The window will change to show ISAPI and CGI extensions that are permitted on the web server. Click *Edit Feature Permissions...* (or *Edit Feature Settings...*) in the right pane.
5. Select *Allow unspecified CGI modules*, then click *OK*.

6. There won't be any indication that this is successful. If you'd like, you can go back into *Edit Feature Permissions...* (or *Edit Feature Settings...*) in the right pane and confirm the option remains checked.

You have successfully allowed all CGI to execute. Please proceed to [Handler Mappings](#) to continue.

Configure Individual CGI extensions for IIS 8.5 or IIS 10

1. Start the *Information Services (IIS) Manager*.
2. Highlight your server.
3. Under the *IIS* section in the main window pane, double-click *ISAPI and CGI restrictions*.
4. The window will change to show ISAPI and CGI extensions that are permitted on the web server. Click *Add...* in the right window pane.
5. In the Add ISAPI or CGI Restriction window:
 - a. Browse to the cgi directory for the program you are configuring.
 - b. In the lower right corner of the Browse window, use the drop-down to view All Files.
 - c. This step enables you to see the .cgi files you need to configure, as shown below.
6. Select one of the necessary .cgi files (as detailed in [Appendix](#)).
 - a. Once you've opened one of the .cgi files needed, fill in a *Description*. We suggest using the program and cgi file name – in our example, this is UnitySync config cgi.
 - b. Click the check box next to *Allow extension path to execute*.
 - c. Click *OK*.



NOTE: *There may be several .cgi files that you will need to allow depending on which program you are configuring for use with IIS, and you'll need to go through the previous steps 4 & 5 for each of them. Please refer to the Program-specific .cgi files listed in [Appendix A](#) for a complete list for the program you are configuring.*

7. Once you have added all of the necessary .cgi files, the Restrictions window will now show them with a status of *Allowed*. If any are listed as *Not Allowed*, it means you neglected to check *Allow extension path to execute*. You'll need to highlight those lines, right-click to *Edit...*, check the appropriate box, and then click *OK*.

You have successfully allowed individual CGI to execute. Please proceed to [Handler Mappings](#) to continue.

Handler Mappings

1. Return to the *Information Services (IIS) Manager*.
2. Double click the *Handler Mappings* icon found under either the *IIS* or *Server Components* section.
3. Right-click *CGI-exe*, then click *Edit Feature Permissions...* (or *Edit Feature Settings...*)

4. Make sure that *Execute* is checked. If it is not, select *Execute* then click *OK*.
5. Double-click *CGI-exe*. Make sure the *Request path* is **.cgi*. If it is not, fill in the *Request path* field with **.cgi* and click *OK*.

You have successfully set up Handler Mappings.

Edit Default Error Behavior

This configuration step allows detailed error messages to be presented when accessing the Program from other than the local server.

1. Return to the *Information Services (IIS) Manager* and select the primary server to open the server *Home* page.
2. Expand the default server and then *Sites* folder.
3. Click on the *Default Web Site* to select, then double-click the *Error Pages* icon in the *IIS* section.



NOTE: *If you have other items configured under the Default Web Site besides our products, you may elect to click on the specific virtual directory to apply the error behavior only to that one, but not all of your virtual directories. The directions that follow below are the same regardless of whether you elect to apply it to the Default Web Site or a specific virtual directory.*

4. Click *Edit Feature Settings...* in the right pane.
 - (a) The default setting for this error is *Detailed errors for local requests and custom error pages for remote requests*. This default setting will result in a generic error if you access the program from a remote server.
 - (b) Instead, select *Detailed errors* then click *OK* to save the selection.

You have successfully edited default error settings for all error types.

Access Your Program Using IIS 8.5 or IIS 10

Your IIS configuration is complete! To access your program, open a browser window and type in the alias address you selected in the [Add Virtual Directory](#) setup (i.e., <http://localhost/emPass>) and you should see the program interface.



NOTE: *When accessing Directify, you must also specify `.../config.cgi` or `.../directify.cgi`, or you will receive an HTTP Error 403.14 Forbidden (i.e., <http://localhost/directify/config.cgi>). Since `config.cgi` is the configuration window and `directify.cgi` is the user facing address, a default document is not configured upon installation. You can configure the default document yourself via instructions found in this knowledge base article:*

<https://www.dirwiz.com/kb/3015>

If you do not, and receive an error instead, please double check all configuration steps to ensure they have been completed. Then review step 2 of this knowledge base article for an additional potential solution:

<https://www.dirwiz.com/kb/436>

Please contact support@dirwiz.com if any questions remain.



IMPORTANT NOTE: *If you are configuring use via https://, please note that Directory Wizards products will not work properly if you are using self-signed certificates.*

Apache

Due to the highly configurable nature of Linux and the many versions, instructions for configuring Apache for use with UnitySync and Directify is difficult to articulate. As clients use our Linux version and request assistance with Apache configuration, we will add to this section with helpful hints and tips for configuration.

Red Hat Enterprise Linux 6.x with Apache 2.2.x



IMPORTANT NOTES

** These directions allow anonymous access to UnitySync admin pages. We **strongly recommend** adding some type of Apache authentication using the 'AuthType' parameters*

** Be sure the 'apache' user (or group) has full read/write access to the global and connections directories.*

** We recommend for security to enable Apache HTTPS*

1. Install Apache web server: `yum install httpd`
2. Edit the following file: /etc/httpd/conf/httpd.conf
3. Use this as a guide to modify your Apache environment:

```
Alias /unitysync/ "[Install Path]/cgi/"
```

```
<Directory "[Install Path]/cgi/">
```

```
AllowOverride None
```

```
Options None
```

```
Order allow,deny
```

```
Allow from all
```

```
Options +ExecCGI
```

```
AddHandler cgi-script .cgi
```

```
</Directory>
```

4. You should now be able to access UnitySync from your browser:

`http://[hostname]/unitysync`

Appendix

Appendix A: Program-specific .cgi files

Directify

- config.cgi
- directify.cgi

emPass

- empass.cgi

InfoCanon

- cgi-test.cgi
- config.cgi
- editor.cgi
- infocanon.cgi

UnitySync

- azure.cgi
- config.cgi
- csv.cgi
- kb.cgi
- ldap.cgi
- logview.cgi
- o365.cgi
- odbc.cgi
- proc.cgi
- smtp.cgi
- status.cgi