Training Guide Series

CYMA Employee Self Service (ESS) Installation Guide

June 2023

Contents

SECTION 1: IMPORTANT NOTES AND SYSTEM REQUIREMENTS 3

SECTION 2: NEW ESS INSTALLATIONS 4

SECTION 3: UPGRADE FROM CYMA 22.X AND EARLIER 6

SECTION 4: TROUBLESHOOTING AND ADDITIONAL NOTES 7

ADDITIONAL INFORMATION 11

SETTING UP ESS TO ALLOW EXTERNAL ACCESS 15

CYMA CONTACT INFORMATION 16

Section 1: Important Notes and System Requirements

Important Notes

1. NOTE: There are two versions of ESS V23. One works with Actian PSQL V12 or V13 and one that works with Actian Zen V15. Ensure the correct ESS version is installed for the correct version of the Actian database engine.

2. ESS Version 23.0 is designed to operate with CYMA Version 23 Payroll and HR software and only V23. ESS should be upgraded at the same time CYMA is upgraded.

3. CYMA and ESS do not need to be installed on the same computer, but if the ESS server is a different computer than CYMA, the Actian PSQL database engine Version 12.0 or greater must be installed on the computer which acts as the ESS server. You can install the Client, Workgroup or Server version of PSQL. If installing the Workgroup or Client, select the option to install as a service. If CYMA and ESS are on the same machine and if the database engine has been previously installed in order to operate CYMA, then no further action regarding the PSQL database is required.

4. Please seek the advice / assistance of CYMA or an IT professional before installing. This document assumes that the installer has a working knowledge of Internet Information Services (IIS) and an understanding of computer network communication.

System Requirements

Server:

- Windows Server OS that supports IIS 7 or later.
- IIS 7 or later.
- SSL Certificate (optional).

Client:

- Chrome (recommended)
- Firefox
- Microsoft Edge
- Safari
- Browser resolution 1280x800 or higher.

NOTE: Ensure browser is updated to the most current version.

Recommendations

Use SSL and purchase a secure certificate if ESS will be accessed from outside the company network.

Section 2: New ESS Installations

This section is for customers with an existing CYMA installation who are installing ESS for the first time.

1. Install IIS 7.x or later on the ESS Server (this may be the same machine that hosts CYMA) and ensure that both Application Development (You will have to expand the Application Development folder and select ASP.NET 4.8) and Static Content (under Common HTTP Features) are enabled.

2. If necessary, install the PSQL database engine on the ESS Server. If the ESS Server is the same machine as CYMA, and if PSQL is already installed, no action is necessary.

3. Install ESS as follows by choosing setup.exe. We recommend you choose the default location for installation files. The installation program will install ESS, Crystal Reports runtime components and the Microsoft .NET Framework 4.8. Reboot the server after the installation is complete.

4. Check the following:

    a. Ensure that the IIS User group has write privileges to the folder named “App_Data”, which is located within the “Attached” folder in the ESS installation location.

    b. Run IIS and verify that a **CYMA ESS for v23** application pool has been created.

    c. Check the Advanced Settings for the **CYMA ESS for v23** Application Pool:
        i. .NET Framework Version should be set to v4.0.
        ii. Enable 32-Bit Applications should be set to True.
        iii. Identity should be set to ApplicationPoolIdentity.

    NOTE: it is recommended that an application pool is setup for each portal needed. Only one application pool is created by the install.

5. Run the CYMA program and in System Manager go to Maintain - Company and check the ‘Use ESS’ checkbox for each company that you will setup in ESS.

6. Run the CYMA program and open Payroll - Maintain Employee dialog of all companies using ESS. This process will create any new company data files required by ESS.

7. In the PSQL Control Center verify that an entry exists for the main CYMA program (CYMASYS) and for each of your CYMA companies. These should have been created automatically by the CYMA installation. If entries do not exist, run the ‘Update SQL Database Connections’ utility on the host machine where the main CYMA program is installed.

8. The next step is to configure ESS to access CYMA data:

    a. Run IIS and select the CymaEmployeePortal website under “websites”.

    b. Double - click on Connection Strings under the ASP.NET section in the middle panel.

c. If the main CYMA program is located on a different server than ESS, edit the System Connection.

   i. Select the entry with the name of CYMASysConn. Click on Edit in the right panel.

   ii. In the Custom box, change localhost to the server's name or IP of the CYMA server.

d. To add additional Companies, create additional Connection Strings.

   i. Run IIS and select the CymaEmployeePortal website under "websites".

   ii. Double - click on Connection Strings under the ASP.NET section in the middle panel.

   iii. Click Add in the right panel.

   iv. The Name of the connection string will be <CompanyID>Conn. Example: DEMOConn

   v. Select the Custom option and type in the following: ServerDSN=CYMADEMO;HOST=localhost.

      Replace the ServerDSN value (after the =) with "CYMA<companyID>" and replace the HOST value with the server name or IP if ESS is installed on a different server.

e. To modify other settings

   i. Run IIS and select the CymaEmployeePortal website under "websites".

   ii. Double - click on Application Settings under the Management section in ASP.Net section.

   iii. For a list of all Settings and what they control see Application Settings under Additional Information.

Section 3: Upgrade from CYMA 22.x and Earlier

If you are currently using ESS, follow these steps to upgrade.

1. Make sure everyone is logged out of CYMA.
2. Upgrade CYMA following the instructions provided with the CYMA installation. The installation of CYMA will stop the PSQL service or services to ensure files needed by ESS are properly updated.
3. Upgrade ESS as follows:
    a. Save the existing web.config file from the directory where the existing ESS is installed. Due to differences between versions of ESS this file will need to be reconfigured.
    b. Uninstall the previous version of ESS.
    c. Run the Setup.exe.
    d. If you are not installing ESS in its default location then browse out to its existing location. Click Next.
    e. This will install:
        i. The ESS 23.0 program.
        ii. Crystal Report runtime components.
        iii. Microsoft .NET Framework 4.8
    f. Click Finish.
    g. Edit the new web.config following the instructions in Section 2: New Installs – Step 8. If any application settings were changed, those changes will need to be made again. See Application Settings in the Additional Information section for more information.
4. The ESS installation should have performed the following setup automatically. Verify the following:
    a. Ensure that the IIS User group has write privileges to the Attached folder.
    b. Ensure that the IIS User group has write privileges to the App_Data folder.
    c. Run IIS and verify that under Application Pools that a CYMA ESS v23 application pool has been created.
        i. Verify that the installed ESS Application under Advanced Settings has its Application Pool set to **CYMA ESS for v23**.
    d. Check the Advanced Settings for this **CYMA ESS for v23** Application Pool:
        i. .NET Framework Version should be set to v4.0.
        ii. Enable 32-Bit Applications should be set to True.
        iii. Identity should be set to ApplicationPoolIdentity.
5. Run the CYMA program and open the Maintain Employee dialog of any companies using ESS. This process will create any new company data files required by ESS.
6. Verify that ESS is working by logging in with a user name and password of an employee that has access.

Section 4: Troubleshooting and Additional Notes

Troubleshooting should be done at the IIS server. Detail error messages are not passed to the client machines. In many cases the user will see a message that states “an unexpected error has occurred”. If an error is encountered at a client computer, recreate the process at the IIS server to see the detailed error message. Most errors will be written to the Event Viewer on the Host computer. After any changes are made to IIS, the IIS service should be restarted prior to testing.

- Error 401
  - Possible cause is that Anonymous Authentication is not Enabled. In IIS, go to the website, double click on Authentication. Right Click on Anonymous Authentication and select Enable.
- Authentication
  - Forms authentication must be enabled.
- The website declined to show this webpage
  - This error will happen if default.aspx was not added to the default documents.
- An error has occurred while attempting to load the Crystal Reports runtime. Either the Crystal Reports registry key permissions are insufficient or the Crystal Reports runtime is not installed correctly.
  - This error will happen if you did not change the Application pool to allow 32bit applications.
- Could not load file or assembly 'CrystalDecisions.Web, Version=5.0.3700.0, Culture=neutral, PublicKeyToken=692fbea5521e1304' or one of its dependencies. The system cannot find the file specified.
  - This error will happen if the Crystal Components did not install. Install manually from the Support folder in the ESS install folder.
- Error 7011, or PSQL asks for a user name and password to create an ODBC/DSN.
  - In order to access DTI functionality through a terminal session a registry key needs to be changed.

    HKEY_LOCAL_MACHINE\SOFTWARE\Pervasive Software\Utilities Interface\Settings

    The value for Restricted Access On WTS client has a default value of 1 meaning access will be restricted. If the administrator changes this to 0, everyone will be able to run utilities as if they are logged on to the machine physically.

    It should be noted that changing this value to 0 gives all users full control of the DTI functions on the server.

    NOTE: Cases have been seen where this key is not in the registry but manually adding it resolves the problem.

    NOTE:
    Editing your registry is dangerous and can disable your operating system causing you to reinstall your software. CYMA will not be responsible for any mishap due to registry changes.
- Service Is Not Available
  - This error will happen when there are two web pages using different versions of ASP.net. To correct, you will need to set up a new application pool and then assign that application pool to the CYMA ESS application. In IIS 7, right click on the website, go to Manage Application - Advanced Settings.
- Error 500.19
  - ASP.NET is not installed for IIS.
- Error 500.19 in 64-bit server operating systems

  - There appears to be a known issue with enabling 32-bit applications in a 64-bit OS. This is not directly related to ESS and can be seen running the default website once you have set the Enable 32-bit Application flag to True. The information that follows comes from Microsoft forums:
    - To remove the compression scheme run the following command at a command prompt. Make sure you run the command prompt "As Administrator" not just logged in as an administrator. %windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpCompression /-[name='xpress']
    - NOTE: this will turn off HTTP compression for all sites on IIS. To turn compression ON again in IIS > (dbl-click icon) Compression, uncheck all boxes (if checked) > apply changes, then check all boxes > apply changes. Restart IIS. Then both HTTP compression & 32-bit work at the same time.
    - Note: to turn the compression scheme back on via command prompt run the following command %windir%\system32\inetsrv\appcmd.exe set config -section:system.webServer/httpCompression /+[name='xpress',doStaticCompression='false',dll='%windir%\system32\inetsrv\suscomp.dll']
- Error 503 after setting the Application Pool to enable 32-bit applications.
  - When this error is seen check the Event Viewer for more information. An error may show an error "The Module DLL C:\windows\system32\RpcProxy\RpcProxy.dll failed to load. The data is the error". This is sometimes seen in IIS 7.0 on an SBS server. The solution is to add a key in the application.config. To correct do the following:
    Edit c:\windows\system32\inetsrv\config\applicationhost.config

    In the section which has <globalmodules> add - **precondition="bitness64"** to the rpcproxy line so that you have the following:

    ```
    <add name="PasswordExpiryModule"
    image="C:\Windows\system32\RpcProxy\RpcProxy.dll" preCondition="bitness64" />
    ```

    In some cases you will need to also change the exppw key also to the following. This can be found in the Global Modules section and Modules section. Both need to be changed. If there is a path after the exppw leave that in and just add the precondition after.
    ```
    <add name="exppw" preCondition="bitness64" />
    ```

    Sometimes after this issue is corrected error 500.19 will be displayed when browsing. Follow the troubleshooting section for that issue.

- System.ArgumentOutOfRangeException: Year, Month, and Day parameters describe an un-representable DateTime.
  - This is most likely data damage and/or a date field was written incorrectly. If this comes up, the data will need to be corrected. Contact CYMA to have the data corrected.
- Cannot find File (code 12)
  - If this error happens when attempting to build the company dropdown, uninstall PSQL and reinstall on the server where IIS is installed.
  - This error will also display if you have installed CYMA Not-For-Profit edition and did not modify the web.config to show True for the NFPCompany setting. See Application Settings section for more info.

- Error in formula
    - This error will manifest itself in numerous ways, but if the error happens when running a report and it references the report directly, it is most likely due missing MFC components.
- Non-db file or corrupted db.
    - This error will happen if the DDFs have been corrupted. Also, if you attempt to browse the database through the PCC, nothing will display under the Tables folder.
    - To resolve the issue, follow these steps:
        - Stop Pervasive
        - Uninstall CYMA on the main server
        - Delete any files will an extension of DDF in the main CYMA directory
        - Reinstall CYMA.
- Error “No connection could be made because the target machine actively refused it”
    - The Host name was not properly set in the web.config file. See Section 2 Step 8 for more information.
- Security Exception - This can be caused by any number of problems. Some things to look for:
    - Change the Application Pool “Identity” option to “NetworkService”. This option is found in the advanced settings of the application pool.
    - Change the Application Pool, “Load Local User” option to “True”. This option is found in the advanced settings of the application pool.
- If the formatting of ESS appears to be missing, static content was not enabled. Read the IIS documentation from Microsoft to determine how to turn this on for your version of IIS.
- If an employee is having problems selecting a company or logging in. These problems can manifest in a few different ways.
    - The company doesn’t stay selected.
    - The company can be selected but the fields stay “greyed out”.
    - The company can be selected but the login doesn’t work even when 100% sure the user name and password are being entered correctly.

  The solution is to add portal.aspx to the default documents in IIS and move to the first location in the list.

  If this appears to only happen with newer versions of IE, try pressing the compatibility button next to the web address line. If this corrects the issue, compatibility mode can be turned on for all IE users by editing the Login.Master and ESS##.Master pages as follows:

  Before:

```
<!--[if lt IE 10]>
    <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
<![endif]-->
```

  After

```
    <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
```

  Stop and start IIS. Try a website that previously failed. You should no longer see the compatibility mode button in the browser and ESS should work.

- Crystal Reports – Load report failed – Access is denied. This error will happen when running reports within ESS. The issue is most likely caused by permissions on the Windows Temporary folder. Browse to %windows%\temp and make sure IIS_IUSRS has been added to the folder security. The user needs to have Modify, Read and Write access. NOTE: The IIS_IUSRS is found on the local machine and not the domain.
- Enter Staffing hours error “unable to store state. Access to the path 'C:\inetpub\wwwroot\debug\App_Data\state' is denied. Write permission for group IIS_IUSRS is not set on the APP_DATA folder in the main installation.

- Access to Path ‘C:\inetpub\wwwroot\CymaEmployeePortal\Attached is Denied: Write permissions for group IIS_IUSRS is not set on the Attached folder in the main installation.

Additional Information

Password Attempt Lockout

ESS has an option that allows setting of the number of password attempts allowed and how long the employee will be locked out. To change either setting, follow these steps.

1. In IIS, double-click on the configuration editor.
2. In the section dropdown box, select system.web/membership.
3. On the providers item line, click the box with three dots to the far right of the line. Select CYMAMembershipProvider in the box that displays.
4. The properties box at the bottom displays all options.
    a. Change the following options as desired:
        i. maxInvalidPasswordAttempts – this value is the maximum allowed invalid attempts. Once reached the user will not be able to log in until the time set in the passwordAttempWindow property. The default value is "99".
        ii. passwordAttempWindow – this value is the amount of time the employee will be locked out if the value in maxInvalidPasswordAttempts has been reached. This value is in minutes. The default value is 5.

Automation of Payroll Import and Calculation

CYMA has the option to allow the automation of importing and calculating of payroll entries. These options are located on the Employee Self Service page of PR Maintain - Configuration. The first option allows ESS entries to "bypass" the importing of web time entries step. If this option is selected, there is a further option to bypass the Generate & Calculate steps. If these options are selected and do not appear to be working in your ESS environment it is most likely due to an unregistered CymaX.ocx or the CYMA install path not set.

To correctly configure ESS to allow for automation, follow these steps:
If selecting the option to bypass the Generate/Calculate steps you must do the following:

1. CymaX.ocx must be registered
    - At the Admin command prompt: Change to the folder where CYMA is installed (C:\cyma\cyma4)
    - Run the following command - **regsvr32 cymax.ocx**

2. In the Web.config file add the cyma path application setting
    - From IIS Manager highlight the portal then double click on Application Settings
    - Select Add from the Actions panel
    - For Name field enter "CYMAPath"
    - For Value field enter the CYMA installation path (Ex: C:\Cyma\Cyma4)

3. Add the IIS_IUSERS group to each company folder, NOT system just company and include **write** permissions.
    a. Open File Explorer
    b. Locate the company folder (Ex: Cyma\Cyma4\Demo)
    c. Right click on the folder
    d. Select **Properties**
    e. Select the **Security** tab
    f. Click the **Edit** button
    g. Click the **Locations** button – Select the local computer then press OK
    h. Click the **Advanced** button
    i. Click the **Find Now** button
    j. Select the **IIS_IUSERS** group

k. Click the **OK** button
l. Click the **OK** button
m. Select the **Allow** check box for the **Write** permission
n. Click the **Apply** button
o. Click the **OK** button
p. Repeat steps b through o for each additional company folder.

Application Settings

Application Settings are found in IIS. These settings control some of the objects that can be customized by the end user.

- **CompanyLogo** - Image that the end user wants to see on the main screen above the login box. The default value is logo.png. The image file needs to be placed in the images folder within ESS. The image should be less than 130 pixels in height and 740 pixels in width.
- **CompanyName** - defines the text that displays in the webportal. This value is only used if the UseCompanyNameFromSystem is set to "False".
- **DbCommandTimeOut** - Gets or sets the wait time before terminating the attempt to execute a command and generating an error. This value should only be changed based on time out issues that can occur in some environments.
- **EmailBodyFile** – Enter the name of the .txt or .html file to be used when an employee clicks on the Forgot Password option on the main page. The file needs to be placed in the main ESS directory on the Web Server. This file will be used as the email that will be sent to the employee with their new PIN. To insert the PIN into the document, type "%0" where you want the PIN to display. For example, your statement might appear like this: Here is your new PIN: %0. When the employee receives the email, it would show: Here is your new PIN: 3228.

  Additional variables are:

  %CN = Company Name
  %EM = Employee ID
  %FN = First Name
  %LN = Last Name
  %CL = Client Name

- **EmailSubject** – Enter the text for the subject of the password reset email.
- **GoogleAnalyticsID** – If desired, an account with Google Analytics can be set up to allow tracking of website activity. Go to http://www.google.com/analytics/ for more information. The Google Analytics ID associated with the website should be used as the value for this key.
- **Mail<formname>** - These keys are manually entered by the user and used for adding Forms to the Email HR section on ESS. The Form name cannot contain spaces. The text following "mail" is the form name displayed Email HR dropdown in ESS. If an underline "_" is used, a space will be used when displaying in ESS. The value of the key is the relative path and file name of the form that is to be displayed in ESS. Forms associated with this key can be seen by all employees.
- **MainContentImage** – This is the image file that will display on the Home page for the employee. The default value is CYMAPayrollPortal-MainStage.gif. The image file needs to be placed in the images folder within the webportal.
- **MaxRecCnt** – Receiving the following - Microsoft JScript runtime error: Sys.WebForms.PageRequestManagerServerErrorException: An unknown error occurred while processing the request on the server. The status code returned from the server was: 12030 which means that ***"The Internet connection was aborted"***. This only seems to happen when many records are returned on some systems. The key is used for a possible workaround. **Note:** It is not known if the user limits the record count to 1000 for 2 users on the portal and the number of users increase to 5 if 1000 is too many. Changing of this setting should only be done with the direction of a CYMA consultant.
- **NFPCompany** – If company uses the Not-for-Profit version set to "True".
- **PinRequired** –If employees need to set up their account without needing a PIN this value can be set to "False". The use of a PIN creates stronger security and changing this value should be considered carefully. By default, this key is set to "True" and a PIN is required.

- **SuperMail<formname>** - These keys are manually entered by the user and used for adding Forms to the Email HR section on ESS. The Form name cannot contain spaces. The text following "mail" is the form name displayed Email HR dropdown in ESS. If an underline "_" is used, a space will be used when displaying in ESS. The value of the key is the relative path and file name of the form that is to be displayed in ESS. Forms associated with this key can only be seen by a supervisor.
- **UseCompanyNameFromSystem** – determine if ESS will display the company name from Maintain Company or if the user wants something specific. "True" uses the value from CYMA, "False" uses the value from the CompanyName key.
- **W2Years** – This is the number of years, prior to the current W2 year, which will show for W-2 printing. Example: If your current W2 year is set to 2009, in CYMAIV - Payroll - Maintain Configuration - Posting Information, then 2007, 2008 and 2009 will show in the webportal, provided the employee has data for those years. NOTE: if you set the value to "0" the option for W-2 will no longer display.
- **CYMAPath** – This is the path that is used for automation of import and calculations of payroll data. The value should the location of the CYMAX.ocx file, typically located in the main CYMAIV install directory. (Example: value=**c:\cyma\cyma4**)
- **UseTwoFactor** – This key is used to turn on Two Factor Authentication. ESS uses Google Authenticator as the provider of the codes. Set value to **true** to turn on the functionality.

Additional IIS settings

There are additional settings in IIS that can be changed based on user specific needs. These changes can be made in the IIS Configuration Editor for the specific website.

System.web/membership – select Providers, select CYMAMembershipProvider. There are two properties that can be changed:

- maxInvalidPasswordAttempts – this is the number of invalid attempts an employee can try before they are locked of trying to login. The default value is 99.
- passwordAttemptWindow – this is the time the employee is locked out until they can try again. The default value is 5. The value is in minutes.

Login Time out settings

Employees that are inactive within the website for a fixed number of minutes will be required to login again before navigating to a new page. The number of minutes before this occurs is configurable. To make the change follow these steps:

1. In IIS, click on website.
2. Double-click the Authentication icon.
3. Right-click Forms Authentication and select edit.
4. Change value in Authentication cookie time-out to the desired number.
5. Click OK

Additionally, there is a Session State timeout that can be changed. This setting defaults to 10 minutes, but can be changed to any value desired. To change the setting follow these steps:

1. In IIS, click on website.
2. Double-click Configuration Editor in the Management section.
3. In the section drop down, select system.web/sessionState.
4. Change value in timeout field to the desired value. The value is in the format HH:MM:SS
5. Click Apply in the upper right corner.

Setting up ESS to allow external access

General Information

There are many ways to allow access to ESS from the internet. These are optional steps and are not required, if employees will be accessing ESS only from the local network. As every situation is different and every piece of hardware has different options, these instructions are provided as a guideline. Please consult an IT professional if you need assistance with your setup.

DNS (Domain Name System)

DNS is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. DNS provides a way that a user can type in a more easily remembered name (ex. www.cyma.com) and it directs the user to an IP address associated with a server. DNS is usually provided by the same services that hosts a company's website.

Port Forwarding

Port Forwarding is a methodology that allows the configuration of internet traffic through a router. Routers need to be configured to allow traffic from the internet to the IIS server. The standard HTTP port is 80 and the standard HTTPS port is 443.

Secure Certificate

A secure certificate is an electronic document used to prove ownership of a public key. The certificate contains information about the key, the owner's identity and the entity that verified the certificate contents. It is installed and used to show the end user that the website is valid. A Secure Certificate can be purchased from a certificate authority.

CYMA Contact Information

CYMA Systems, Inc.

2330 West University Drive, Suite 4

Tempe, AZ 85281

(800) 292-2962

Fax: (480) 303-2969

E-mail: info@cyma.com

www.cyma.com

When contacting CYMA for technical support, please have the following information available:

- CYMA Account Number (if known)
- Windows Version
- Network Operating System (if applicable)
- CYMA Version

Any comments or suggestions you have regarding CYMA documentation can be sent to:

CYMA Systems, Inc.
Product Development/Documentation
2330 West University Drive, Suite 4
Tempe, AZ 85281
Fax: (480) 303-2969
www.cyma.com
E-mail: info@cyma.com