CYGNET

CygNet v9.5 Upgrade Procedure

Release Date: February 5, 2021

Revised: July 2, 2021

This document describes the procedures required to upgrade to v9.5 of CygNet SCADA and CygNet Measurement. Please note the following:

- Read this procedure in its entirety before beginning your upgrade.

- The baseline version for this upgrade procedure is v9.2. If your baseline is a version released prior to v9.2, you must first upgrade to v9.2 before beginning this upgrade.

- Upgrades from v9.2, v9.3, and/or v9.4 are supported by this document.

- The time estimates listed in this document are provided as a guide only, and the actual time to complete each step depends on the size and complexity of your system.

Contents

Revision History

The following revision has been made the CygNet v9.5 Upgrade Procedure on July 2, 2021.

- Added Step 4.20 Convert Older Canvas Screens to New Script Format

Before You Begin

This document outlines procedures for upgrading from CygNet v9.2, v9.3, or v9.4 to CygNet v9.5. The baseline version for this upgrade procedure is v9.2. If your baseline is a version released prior to v9.2, you must first upgrade to v9.2 before beginning this upgrade.

If you have a multi-host system running different version of CygNet, we recommend that you create an upgrade rollout plan for all hosts before starting. Appendix A contains information about running CygNet in a mixed-mode environment.

The amount of time it takes to perform the various upgrade tasks depends on the size and complexity of your system. Upgrade assistance can be obtained by contacting CygNet Support at the Software Support portal (login required), via phone 1-866-4CYGNET (1-866-429-4638) or via email at CygNet Support.

References in this document to "host server" mean the server machine where the CygNet site is running.

References in this document to the path "CygNet\" (e.g., **CygNet\Utilities** or **CygNet\Services**) use the name "CygNet" as an example to mean the folder where your CygNet host software is installed, for example, **C:\CygNet**.

References in this document to the "product source" or "source" mean the CygNet installation or upgrade files that you must download from the CygNet Download Site (login required). If you require the software on physical media (DVD), contact CygNet Support at the Software Support portal (login required), via phone 1-866-4CYGNET (1-866-429-4638) or via email at CygNet Support.

If your services for a site are on more than one server, run this upgrade on *all* applicable servers. For example, if you run FMS on a dedicated SQL Server, run the upgrade on that server as well. If you are running 64-bit components on a separate server, run the upgrade on all servers. See 64-bit CygNet Components below.

There are no additional or separate upgrade procedures for CygNet Webv9.5.

Download the Upgrade Files

Approximate time: 10 minutes.

1. Log in to the CygNet Download Site (login required).

2. Click **SOFTWARE** > **SCADA AND MEASUREMENT PRODUCTS**.

3. Click the **9.5** folder.

4. Download the **CygNetSCADA_95.zip** for v9.5.

5. Read and follow the instructions in the **!What's in the Zip_v95.txt** file.

6. Extract the zipped file to a folder on your CygNet Host machine. This is the "source" folder.

The upgrade begins in Step 4. Upgrade Host Software.

Product Lifecycle

For more information on the lifecycle of CygNet components, refer to the *CygNet Software Product Lifecycle Matrices* on the Software Support portal (login required).

CygNet Lifecycle Notice

CygNet Software follows a fixed product lifecycle policy and offers three years of support (two years of mainstream support followed by one year of limited support). Please contact your Account Manager or CygNet Sales (via email at CygNet Sales) for more information about your support options.

The following table lists the dates of support for the currently supported versions of CygNet Software.

CygNet Version	Release Date	Limited Support Begins	Limited Support Ends (End of Life)
9.5	February 5, 2021	February 5, 2023	February 5, 2024
9.4	February 28, 2020	February 28, 2022	February 28, 2023
9.3	July 19, 2019	July 19, 2021	July 19, 2022
9.2	December 14, 2018	December 14, 2020	December 14, 2021
9.1	July 20, 2018	July 20, 2020	July 20, 2021

The following CygNet versions have reached lifecycle milestones with the release of CygNet v9.5:

- **CygNet v9.3** will enter Limited Support on July 19, 2021 and will reach its End of Life on July 19, 2022.

- **CygNet v9.2** entered Limited Support on December 14, 2020 and will reach its End of Life on December 14, 2021.

- **CygNet v9.1** is in Limited Support effective July 20, 2020 and will reach its End of Life on July 20, 2021.

- **CygNet v9.0** reached its End of Life on December 19, 2020.

The following Windows operating systems are no longer supported with the release of CygNet v9.5:

- **Windows 7**

- **Windows 8**

- **Windows Server 2008**

- **Windows Server 2008 R2**

Refer to the Microsoft Lifecyle Policy for information about Windows operating system support.

Upgrade Assistance

Upgrade assistance is provided through prepaid professional service hours provided with your annual services subscription or through time-and-materials consulting services. If you need assistance in planning, upgrading, or deploying this release, please contact CygNet Support for more information about these options. Contact CygNet Support at the Software Support portal (login required), via phone 1-866-4CYGNET (1-866-429-4638) or via email at CygNet Support.

CygNet Documentation

The **CygNet Help** for CygNet v9.5 is available from https://softwaredocs.weatherford.com/cygnet/95/. Best viewed in Microsoft Edge or Google Chrome browser. Microsoft Internet Explorer 11 is not supported.

64-bit CygNet Components

CygNet Software now supports a 64-bit **Universal Interface Service (UIS),** 64-bit **EIE drivers**, and a 64-bit **Value History Service (VHS)**. The 64-bit drivers must be used with the 64-bit UIS.

There are four 64-bit utilities supported for handling larger data sets associated with 64-bit services:

- 64-bit Group Manager

- 64-bit Point Configuration Manager

- 64-bit VHS Check

- 64-bit VHS Import/Export Utility

Each utility can be installed for the first time from the APP/UTILS directory using the **CygNet Client Installer**. The **CygNet Host Updater** utility will automatically detect previously installed 64-bit components and upgrade all necessary executables and files. Follow the steps described in this document for *all* hosts where CygNet is installed.

Install 64-bit Services and Drivers

For information about installing 64-bit components in your CygNet system, refer to the **CygNet v9.5 64-bit Installation Guide** (refer to **CygNet Software** > **Additional CygNet Resources** topic in the **CygNet Help**). That document describes the supported services, drivers, installation notes, and required files for running 64-bit components. It describes how to install and configure 64-bit services and drivers in three possible scenarios:

- Upgrade existing UIS and/or VHS services and drivers from 32-bit to 64-bit

- Add new 64-bit UIS and/or VHS services and drivers to an existing CygNet site

- Install 64-bit UIS and/or VHS services and drivers on a separate independent server

Important Changes to the v9.5 Facility Service

CygNet v9.5 has been enhanced to support many more facility attributes, including additional table-driven attributes, additional free-form text attributes, and one large text attribute for use as a facility comment. All CygNet applications, clients, user interfaces, utilities, APIs, metadata, and schemas have been modified to reflect the new facility attributes.

To accommodate these changes the v9.5 Facility service database definition (FAC DDL) has been updated and a new column has been added to the Facility service database. After upgrading to v9.5, and the FAC.exe runs for the first time, the Facility service database is immediately "converted" and an earlier FAC.exe will not be able to read the modified database. Refer to the **CygNet v9.5 Release Notes** for more information about this enhancement.

Facility Service Replication in Mixed-Mode Hosts

Special consideration must be made when replicating between CygNet v9.5 and an older CygNet host. Refer to **Appendix A: Mixed-Mode Hosts** in the **CygNet v9.5 Upgrade Procedure** for more information about replicating in a mixed-mode environment and applying a recommended patch to allow an older Facility service and clients to interact with a v9.5 Facility service.

See Appendix A: Mixed-Mode Hosts.

1. Verify System Versions

The purpose of the steps in this section is to verify the version of your CygNet system(s). Your baseline must be v9.2 or later.

1.1 Verify Version Numbers of CygNet Services

Approximate time: 10 minutes.

1. Use **Windows Explorer** to browse to the **CygNet\Utilities** folder on the host server.

2. Start the **CygNet Version Info** utility by double-clicking the program executable (CVersionInfo.exe).

    a. Use the **Browse** button to select the folder that contains the service executable directories. The default is **CygNet**; however, if you are using split directories the folder name might be different.

    b. In the **File Spec** box, select ***.exe**;***.ocx**;***.dll**.

    c. Check **Include Subdirectories**.

    d. Click **List Files**.

    e. *Optional.* Click on the **File Version** header to sort the files.

    f. Verify that all service executables are at least product v9.2 or newer. If they are not v9.2 or newer, you must upgrade your system to v9.2 before continuing.

3. Click **Close** to exit the utility.

2. Back Up the System

The purpose of the steps in this section is to back up the system before performing data integrity checks. If an integrity check determines that you have an error, data might be lost when the corruption is fixed.

> **Note**: *We recommend performing a full service backup to clear transaction logs before proceeding with the steps in this section. Refer to the* **Backup and Restore** > **Service Backups on Demand** *topic in the CygNet Help for more information about performing service backups.*

2.1 Stop All Clients and Services on the Host Server

Approximate time: 5 minutes.

1. Close all CygNet client applications running on the host server.

2. Open the **CygNet Host Manager** utility (CHostMgr.exe).

3. Stop all services by highlighting each RSM configuration and clicking **Stop**. (Your services are stopped when the **Status** changes to STOPPED.)

4. Exit **CygNet Host Manager** by clicking **File**, then clicking **Exit CygNet Host Manager**.

2.2 Back Up the System

Approximate time: Depends on size of databases.

> **Note:** *For hosts configured with a Service data directory that is different from the Service executables directory, be sure to back up both directories.*

1. Copy all CygNet files and folders (Services, Support, and Utilities) to a backup location outside of the CygNet directory.

2. If you have a folder for your device template files (.dtf), also copy it to the backup location.

3. If you have external databases (e.g., for CygNet Measurement), contact your IT department about backing up those databases.

3. Verify Data Integrity

The purpose of the steps in this section is to validate the integrity of the data in your current system. The steps outlined in this section are <u>required</u>. They provide a method for you to identify any existing problems and to know that these problems are not a result of the upgrade. If any problems are found, <u>resolve</u> them before upgrading. Unresolved issues might be compounded if they are not fixed before upgrading.

Important: Tests in this section should be performed using your pre-upgrade toolset. The utility version must match the version of your pre-upgrade services. That is, do not perform tests with the new utilities provided on the product source.

3.1 Validate DDS Data File Using CygNet DDS Check

Approximate time: Depends on size of database.

This step requires the Device Definition Service (DDS) to be running.

1. If you have not done so already, use **CygNet Host Manager** to start the host server running the DDS.

2. Use **Windows Explorer** to browse to the **CygNet\Utilities** folder on the host server.

3. Start the **CygNet DDS Check Utility** by double-clicking the program executable (DdsCheck.exe).

   a. In the **DDS Service** field, type the name of your DDS, e.g. *MYSITE.DDS*.

   b. Verify that the **Check Devices, Data Groups, and DEIds** option is selected.

   c. Click **Perform Check**.

   d. If no errors are found, skip steps e., f., and g., and proceed to step 4.

   e. If errors are found, create a backup of the Dds.dat.edb, Dds.inx.edb, Dds.dat.pat, and Dds.inx.pat files. If you would like more information on the types of errors that the **CygNet DDS Check** utility has detected, please contact CygNet Support at the Software Support portal (login required), via phone 1-866-4CYGNET (1-866-429-4638) or via email at CygNet Support before performing the fix.

   f. Click **Perform Fix**. **Perform Fix** may permanently delete or modify information in the database. There is no undo.

   g. Click **Yes**.

4. Click **Close** to exit the utility.

3.2 Verify Services Are Operational

Approximate time: Depends on size of databases.

This step is to verify that all pre-upgrade services are fully operational before beginning the upgrade.

1. If they are not already running, use **CygNet Host Manager** to start all services.

2. Verify that each service is running in **CygNet Explorer**. (All service icons are green; all services show *Running* in the RSM.)

3. Close **CygNet Explorer**.

4. Upgrade Host Software

The purpose of the steps in this section is to upgrade the host software. This includes adding the new files to the host server and updating the service configuration files. The **CygNet Host Updater** utility performs the tasks of adding new files to your host server and APPS service. It also updates the timestamps of version management files.

4.1 Stop All Clients and Services on the Host Server

Approximate time: 5 minutes.

Note: *It is necessary to stop the MSS and disable automated polling independently of other services so that when the other services are restarted, polling does not resume until upgrade tasks are completed. You will be reminded after the upgrade is complete to restart the MSS and enable automated polling tasks in step 4.17 Restart the MSS and Activate Automated Polling.*

1. Use **CygNet Explorer** to deactivate any automated polling tasks and stop the MSS.

2. Close all CygNet client applications running on the host server.

3. Use **CygNet Host Manager** to **Stop** all services.

4. Exit **CygNet Host Manager** by clicking **File**, then select **Exit CygNet Host Manager**.

4.2 Run CygNet Host Updater

Approximate time: 10 minutes.

This step performs the upgrade to CygNet v9.5 using the **CygNet Host Updater** utility. The **CygNet Host Updater** utility is version specific. It compares the files in the product source to the host server and replaces the host server versions with the newer versions.

1. Use **Windows Explorer** to browse to the **CygNet\Utilities** folder in the product source.

2. Copy the **CygNet Host Updater** utility (CHostUpdater.exe) from the product source and paste it to the **CygNet\Utilities** folder on the host server. Indicate that you want to **Copy and Replace** the file.

3. Start the **CygNet Host Updater** utility on the host server by double-clicking the program executable (CHostUpdater.exe).

4. Verify that the title bar shows **CygNet v9.5 Host Updater**.

   a. Use the **Browse** button to select the source of the new files. This is the product source.

   b. Click **Load Files...**. The utility searches the host server for CygNet files and lists them in the **Found Install Folders** dialog box. If the search list does not include all folders (for example, folders on a different drive), you must use the **Add Install Folders >>** option to specify other folders.

   c. Make sure that all folders you want to be updated are checked. Conversely, make sure that any folder you do *not* want to be updated is *not* checked. For example, you might not want to update files that are in patch folders or you might not want to include your backup folder.

   d. Click **OK** to save the folders list. This will take a few minutes as the utility identifies the files to update.

   e. Click **Perform Update**. This will take several minutes as the utility processes files for update.

   f. Click **OK** when the update process is complete.

   g. Click **Close** to exit the **Process Status** dialog box.

5. Click **Close** to exit the **CygNet Host Updater** utility.

4.3 Install Any Patches

Important: This step is required only if v9.5 patches are available. If no patches are available, skip this step and pro-
ceed to step 4.4 Upgrade Microsoft .NET Framework 4.7.1 or Higher.

If you are upgrading to v9.5, and it is several months since v9.5 was released, or another CygNet version has been
released, there may be some v9.5 patches available for installation.

1. Check for any v9.5 patches on the CygNet Download Site (login required).

2. Click **SOFTWARE > SCADA AND MEASUREMENT PRODUCTS**.

3. Click the **9.5** folder.

4. Open the **Patches** folder.

5. Download the **95_Patch_Composite.zip** file.

6. Read and follow the instructions in the **95_Patch_Composite_Readme.html** file.

4.4 Upgrade Microsoft .NET Framework 4.7.1 or Higher

*Important: Many CygNet components (any executable deployed from the **\Bin** folder: Canvas, Canvas View, CygNet*
.NET API, Config File Manager, Redundancy Editor, and BSAP Configurable Data Group Migration utility; also
CygNet Measurement, CygNet Enterprise Objects, Enterprise Gateway, Business Object Builder, Note Feed
*Tool, and the Trend Tool) require **Microsoft .NET Framework 4.7.1** or higher. If you intend to use the .NET*
API or any of these applications, you must install .NET Framework 4.7.1 or higher.

*Refer to the **CygNet v9.5 System Requirements** for more information about the CygNet software require-*
ments. If .NET Framework 4.7.1 or higher is already installed, skip this step and proceed to step 4.5 Run
CygNet Config File Manager.

The Microsoft .NET Framework 4.7.1 is a highly compatible, in-place update to the Microsoft .NET Framework
4, 4.5, 4.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7.

1. Go to the download site to get the latest installer:

   Microsoft .NET Framework 4.7.1 (Web Installer) – https://www.microsoft.com/en-us/-
   download/details.aspx?id=56115

2. Install the .NET Framework on the host server where your CygNet Host, CygNet Enterprise Operations Platform,
   or CygNet Measurement application is running (if different from the CygNet host server) by following the
   installation instructions provided by Microsoft.

Note: Windows 10 Enterprise 2015 LTSC is limited to Microsoft .NET Framework .NET 4.6 and is therefore incom-
patible with CygNet v9.5.

*Note: CygNet Bridge for v9.5 (v4.3) requires **Microsoft .NET Framework 4.7.2 Developer Pack** or later, which*
can be downloaded from https://dotnet.microsoft.com/download/dotnet-framework/net472. Refer to the
***CygNet v9.5 System Requirements** for more information.*

4.5 Run CygNet Config File Manager

Approximate time: 5 minutes.

The **CygNet Config File Manager** utility is a tool used to update the keywords in the local service configuration files to those of the current version and remove any old keywords. The utility is version specific.

1. Use **Windows Explorer** to browse to the **CygNet\Bin** folder on the host server that was just upgraded.

2. Start the **CygNet Config File Manager** utility by double-clicking the program executable (ConfigFileMgr.exe). Verify that the **Migrate configuration files** box shows v9.5.

3. Click **Migrate configuration files**.

4. Type the **Service path** or click **Browse** to access the **Browse For Folder** dialog box. Select the folder where the configuration files are located on your local server, usually the **CygNet\Services** folder. The **CygNet Config File Manager** will search all folders under the selected path and find all the *.cfg files (with the exception of configuration files found in a service's backup folder, as specified in the BACKUP_PATH keyword). If a .cfg file conflict is detected, a **Conflict Resolver** dialog box will display for the user to choose the appropriate files to update.

5. Click **Migrate files** to start the migration.

6. A confirmation dialog box will display showing the changes made to the configuration files. Click **Save** to confirm or **Discard** to override the change. Click **Yes** to confirm the action.

7. Upon completion a success message will display. Click **OK** to close.

8. *Optional.* If replication is configured, we recommend that you enable and set a meaningful value for the **REPL_DELAY_MAX** keyword for all replicated services. A recommended value would be a longer time interval than you would expect any sync interval to take.

    a. Reopen the **CygNet Config File Manager** utility and select the **Edit local configuration files** option.

    b. Load the local configuration files for the replicated services.

    c. Find the **REPL_DELAY_MAX** keyword.

    d. Enable the keyword for all replicated services. Right-click the cell for the first service and select **Enable**. Then right-click the cell for the first service and select **Set row to value**.

    e. For each service edit the value to a longer time interval than you would expect any sync interval to take. You can use the **Set row to value** option if values are identical.

    f. Click **Finish** and **Save** the changes to the service configuration files.

9. Click **Exit** to quit the **CygNet Config File Manager**.

4.6 Enable Extended Logging Mode

Approximate time: Varies depending on number of services.

Important: This step is highly recommended for all users. It is related to changes made in CygNet v9.1 where in the unlikely event that a service encounters an unknown exception, the process will stop and the exception will be handled through the Windows Error Reporting service (WER). Previously, an unknown exception would have been logged and the process would continue running in a possibly unknown state. We recommend enabling Extended Logging Mode to retain log files after a restart and Automatic Service Recovery or Failover to restart services. See 4.11 Enable Automatic Service Recovery after you have restarted your services. Refer to the release note on page 18 of the CygNet v9.1 Release Notes for more information about this enhancement.

CygNet provides an extended logging mode for the retention and maintenance of log files after service restarts. We highly recommend you configure the *EXTENDED* logging option for the **LOGFILE_MODE** keyword in the service configuration (.cfg) file for each service. Refer to the **Logging > Configuring Logging** topic in the *CygNet Help* for more information about extended logging mode.

- Use the **CygNet Config File Manager** to mass modify the **LOGFILE_MODE** keyword and change the value to *EXTENDED* for all services. You can also manually edit each service configuration (.cfg) file, if preferred. For local configuration files, you must restart the service(s) for the changes to become effective. After changing the keyword(s) proceed to the next step.

4.7 Reindex the DDS

*Important: This step is **required** even if you are <u>not</u> using any of the CygNet OPC EIEs.*

Note: This step is required for every Device Definition Service (DDS) in your environment, regardless of its operational mode (in production or replicating).

Approximate time: 5 minutes.

In order to use a new index that was added to the v9.5 DDS to expose the Quality summary field that indicates the quality of the data in the data-group transaction for the OPC EIEs, the DDS service must be stopped and the DDS database definition file reindexed. This is done via the **ReIndexESE** (ReIndexEse.exe) command-line utility found in the **CygNet\Utilities** directory. This utility <u>must be run</u> under a user account with Administrator-level permissions. Be sure the new DDS database definition file (DDS.DDL) has been copied into your DDS service directory, replacing the previous version.

Refer to the release note in the CygNet Services, DDS section of the ***CygNet v9.5 Release Notes*** for more information about this enhancement.

1. Confirm the DDS service has been stopped along with the other services. See 4.1 Stop All Clients and Services on the Host Server.

2. Confirm the new DDS database definition file (DDS.DDL) has been copied into your DDS service directory.

3. Open a Command Prompt window:

    a. On the **Start** menu, click **Run** to access the **Run** dialog box.

    b. In the **Open** text box, type **Cmd** and then click **OK** to access the command window.

    > *Important: If your account does not have Administrator-level permissions, you can choose to run **Cmd** using the "Run as administrator" option (via an application shortcut (desktop icon or Start menu)) and provide valid administrative credentials.*

4. Navigate to the CygNet Utilities folder:

    a. If necessary, change the drive by typing the drive letter, for example, **C:** and then press **Enter**.

    b. Type **cd** and then press **Enter** to change to the root directory.

    c. Type **cd CygNet\Utilities** and press **Enter** to change to the CygNet Utilities directory.

5. Run the **ReIndexESE** utility by typing `ReIndexEse` and the path for the DDS service configuration file, and then press **Enter**. See the following example:

    ```
    ReIndexEse c=C:\CygNet\Services\DDS\Dds.cfg
    ```

6. If no errors are reported, the database definition file will be reindexed.

    > **Note**: Because **ReIndexESE** writes files to the directory from which it is run, look in the **CygNet\Utilities** directory for the generated files containing any errors.

7. Proceed to step 4.8 Reindex the PNT. After reindexing the PNT, you will restart all services, including the DDS. The new indexes can be used immediately after the restart.

4.8 Reindex the PNT

Important: *This step is required if you are upgrading from v9.1, v9.2, or v9.3 to v9.5. If you are upgrading from v9.4, skip this step and proceed to step 4.9 Restart the Services.*

Note: *This step is required for every Point (PNT) service in your environment, regardless of its operational mode (in production or replicating).*

Approximate time: 5 minutes.

In order to use the new indexes that were added to the PNT service for the Enhanced Alarm Configuration feature in v9.4, the PNT service must be stopped and the PNT database definition file reindexed. This is done via the **ReIndexESE** (ReIndexEse.exe) command-line utility found in the **CygNet\Utilities** directory. This utility must be run under a user account with Administrator-level permissions. Be sure the new PNT database definition file (PNT.DDL) has been copied into your PNT service directory, replacing the previous version.

1. Confirm the PNT service has been stopped along with the other services. See 4.1 Stop All Clients and Services on the Host Server.

2. Confirm the new PNT database definition file (PNT.DDL) has been copied into your PNT service directory.

3. Open a Command Prompt window:

   a. On the **Start** menu, click **Run** to access the **Run** dialog box.

   b. In the **Open** text box, type **Cmd** and then click **OK** to access the command window.

   > ***Important****: If your account does not have Administrator-level permissions, you can choose to run **Cmd** using the "Run as administrator" option (via an application shortcut (desktop icon or Start menu)) and provide valid administrative credentials.*

4. Navigate to the CygNet Utilities folder:

   a. If necessary, change the drive by typing the drive letter, for example, **C:** and then press **Enter**.

   b. Type **cd** and then press **Enter** to change to the root directory.

   c. Type **cd CygNet\Utilities** and press **Enter** to change to the CygNet Utilities directory.

5. Run the **ReIndexESE** utility by typing `ReIndexEse` and the path for the PNT service configuration file, and then press **Enter**. See the following example:

   ```
   ReIndexEse c=C:\CygNet\Services\PNT\Pnt.cfg
   ```

6. If no errors are reported, the database definition file will be reindexed.

   > **Note**: Because **ReIndexESE** writes files to the directory from which it is run, look in the **CygNet\Utilities** directory for the generated files containing any errors.

7. Proceed to step 4.9 Restart the Services to restart all services, including the DDS and the PNT. The new indexes can be used immediately after the restart.

4.9 Restart the Services

Approximate time: Varies depending on the number and size of services.

1. Start **CygNet Host Manager** from the **Start** menu or desktop icon.

2. Select the RSM for your Site.Service and click **Start**. Wait for the **Status** to indicate *RUNNING*.

3. Start your desired client application from the **Start** menu or the desktop icon. See the **Notes** below.

Notes:

- One of the tasks of the **CygNet Host Updater** is to load the new client application files to the APPS service and update the .rsp and .rsq file times. Since the APPS service is not running during the update, the files are written to a temporary storage location and then uploaded once the service is started. The temporary storage location is a folder named **Update** located under **CygNet\Services\APPS**. Once all of the files have been written to the APPS service, the folder is deleted.

  If you try to start a client application that uses version management while files are still being uploaded to the APPS service, an **Application Download Error** dialog box displays. This indicates that files are still being uploaded to the APPS service. It is recommended that you select **Wait** or **Cancel**. If you click **Wait**, another dialog box is presented that shows the update progress: **Waiting for service updating to complete...** Your client application will start in a few minutes. You can click **Stop** to return to the previous dialog box.

- The DDS and UIS services might start quickly; however, the size of the DDS database dictates the amount of time it takes for the UIS to load all of the devices. If you try to click on the UIS before it has loaded all of the devices, you'll get a "not ready" message.

4.10 Check GNS Folder Security

Approximate time: 5 minutes.

Important: This troubleshooting step is recommended for all users upgrading to v9.1 or later.

A security enhancement implemented in CygNet v9.1 might affect the ability of the General Notification Service (GNS) to send email notifications.

The enhancement requires that the service account under which the GNS is running be given explicit permission to the GNS executable folder or that the service account be part of the **Users** group and that the **Users** group has permission to the GNS executable folder. Note that it may not be sufficient to add the service account to the **Administrators** group.

If, after upgrading and restarting your services, you receive error "`SMTP Send Error: SMTP Message failed: Exit code: -2146232576`" in the Gns.log file, it is due to this permission issue, and you will need to change the permission for the service account to the GNS executable folder.

Alternatively, you can disable email sandboxing by setting the **SANDBOX_EMAIL_HANDLING** keyword in the GNS configuration file (Gns.cfg) to "No".

1. Stop the GNS using **CygNet Explorer**.

2. Start the **CygNet Config File Manager** (ConfigFileMgr.exe in the **CygNet\Bin** folder) and select **Edit local configuration files**.

3. Filter to the GNS and find the **SANDBOX_EMAIL_HANDLING** keyword in the **Shared Mail Settings** category. Disable or set the keyword to "No".

4. **Finish**, **Save**, and **Exit** to quit the **CygNet Config File Manager**.

5. Restart the GNS using **CygNet Explorer**.

6. Check that the GNS can send email notifications.

4.11 Enable Automatic Service Recovery

Approximate time: Varies depending on number of services.

Important: *This step is optional but highly recommended for all users. Enabling **Automatic Service Recovery** will automatically restart a service in the unlikely event that it fails. This step is related to changes made in CygNet v9.1 regarding how service failure is handled and is described in step 4.6 Enable Extended Logging Mode. Refer to the release note on page 18 of the **CygNet v9.1 Release Notes** for more information about this enhancement.*

CygNet provides an **Automatic Service Recovery** option for the local recovery of services in the unlikely event of an abnormal shutdown. We highly recommend you configure a restart action for each service. Automatic service recovery is configured in one of the following ways:

- Use the **RSM** to configure Automatic Service Recovery on a per-service basis. Individual service configuration allows a custom strategy for each service. Refer to the **Automatic Service Recovery** chapter in the *CygNet Help* for more information about how to configure Automatic Service Recovery.

- If you have Redundancy enabled, use the **CygNet Redundancy Editor** to make mass changes to the automatic service recovery settings for all redundant RSMs and their owned services. This option is *only* available if you have Redundancy configured for your services. Refer to the **Redundancy** > **Configuring Redundancy** > **CygNet Redundancy Editor** > **Configuring Auto-failover** > **Configuring Automatic Service Recovery** topic in the *CygNet Help* for more information about mass modification of service recovery settings.

4.12 Update the FMS Database for CygNet Measurement

Important: *This step is required only if you already have CygNet Measurement installed.*

If you do not have a pre-existing installation of CygNet Measurement, and intend to install it, complete your CygNet v9.5 software upgrade and then install CygNet Measurement v9.5 according to the procedure described in the CygNet Help documents. Then skip this step and proceed to step 4.13 Run the CygNet Service Migration Utility.

Approximate time: Varies depending on the size of the database, when it was last updated, and system hardware.

This step updates the database scheme of the FMS service for pre-existing installations of CygNet Measurement. The service will not operate correctly until the database update is performed. Once the database is updated, older versions of the FMS service will no longer be able to use this database.

1. Ensure that your FMS service is running.

2. Go to the **CygNet\Clients\CExplore** folder on the host server and open **CygNet Explorer** (CExplore.exe).

    a. In the service hierarchy, select your site and double-click **Flow Measurement Service (FMS)** to access the database update screen.

    b. Determine whether or not you would like to export a copy of the SQL statement being executed.

       - To export a copy, enter an export path into the **Path to export SQL statement** text box.

           Note: *Some operating systems do not support using certain export path locations as a file destination. In such cases, create a temporary folder (e.g. **C:\Temp**) and then enter that folder location into the text box as the file destination.*

       - To not export a copy, leave the **Path to export SQL statement** text box blank.

c. Update the database scheme, using the **Update DB** button (recommended) or the **Only Export SQL** button (not generally recommended).

> ***Note:*** *It is strongly recommended to use the **Update DB** option only, to ensure that your database tables will be properly updated.*

- Update the database scheme using **Update DB** (recommended). This process will update your system to v9.5 database version 1049, and the cycle may repeat, depending on the CygNet Measurement version you are updating from.

    i. Click **Update DB**.

    ii. Read the **Status:** statement and check the log to verify completion. Correct any listed errors before proceeding.

    iii. Repeat steps **i** and **ii** as many times as are required to complete the update of the database scheme. The following interim database version numbers may be helpful for reference purposes during the process.

    - v9.0 - 1044
    - v9.1 - 1045
    - v9.2 - 1046
    - v9.3 - 1047
    - v9.4 - 1048
    - v9.5 - 1049

- Update the database scheme via **Only Export SQL** (available as an option if applicable; not generally recommended). This is a multiple-part process, which also requires using the **Update DB** procedure.

    i. Generate and run the SQL script. This may only partially update your database and need to be repeated, depending on your current CygNet Measurement version.

        1. Enter an export path into the **Path to export SQL statement** text box.

        2. Click **Only Export SQL**.

        3. Stop your FMS service.

        4. Run the generated SQL script against your database.

        5. Restart your FMS service.

    ii. Update the database scheme using **Update DB**. This will update your system to v9.5 database version 1049.

        1. Follow the same steps described above for updating the database scheme using the **Update DB** button.

        2. Refresh your FMS service when complete.

d. Wait until the update is complete. You can refresh your FMS service to verify completion. When the FMS Node list appears upon refresh, the update is complete.

e. Once the update is complete, manually run the **Perform Database Maintenance** command for your FMS system. The **Update archived databases** command parameter must be set to **Yes** prior to running the command. This ensures that your archived data is consistent with the FMS database update.

4.13 Run the CygNet Service Migration Utility

Important: *While there are no new updates for CygNet v9.5, you should still run this utility when upgrading to v9.5.*

The **CygNet Service Migration Utility** (SvcMigration.exe) is a database service transformation tool. It enables CygNet to make database service-wide updates on a version-by-version basis.

Usually the update options displayed by the CygNet Service Migration Utility are required; affected services will not operate correctly if the changes aren't made. However, once you have made changes for a version on a given service, those changes do not need to be made again for that service. The list of available updates changes from CygNet version to version. Refer to the **System Administration** > **System Administration Utilities** > **CygNet Service Migration Utility** topic in the *CygNet Help* for more information about the updates listed in this table.

The following table lists the recent service-migration updates that have been added in CygNet v9.0 and v9.4.

Update	Introduced	Starting Version	Details
Migrate DDS transactions compression	9.0	7.3.0	Updates any records in the DDS database that are stored using a deprecated compression format.
Version-specific template file changes	9.4	8.5.0	Updates changes to template files to specify that **canSend**/**canRecv**/**uccSend**/**uccRecv**=true for the "Configurable Data Group" (**CfgDg**).

1. Ensure that all database services against which you plan to run the CygNet Service Migration Utility are running.

2. Go to the **CygNet\Utilities** folder on the host server and open the CygNet Service Migration Utility (SvcMigration.exe).

    a. At the **Site Service** box, select the Site.Service(s) to which this service migration applies. You have three options:

        - If you want to update <u>one or more specific</u> database services, click the **Browse** button and select a specific database service from the **Select Service** dialog box. In this scenario, you must check and update database services one at a time.

        - If you want to update <u>all database services for a specific site</u>, type the name of the site followed by a period and wildcard asterisk. For instance, you'd type *MYSITE*.*

        - If you want to update <u>all database services on a CygNet domain</u>, leave the **Site Service** field blank. Be aware that this means that all database services across all sites on the same domain will be affected.

    b. Using the **Select** check boxes, select only the service migration options you want to apply to the specified Site.Service(s).

    c. Click **Check** to preview the changes that the CygNet Service Migration Utility will make to your selected Site-Service(s).

    d. Closely review the service migration changes that will occur if you choose to update. When you are done, click **Done**.

    e. At the **CygNet Service Migration** dialog box, click **Update**. Doing so updates all migration items selected in the CygNet service check.

3. A dialog box appears asking, "Are you sure you want to migrate these *n* services?" If you are sure, click **Yes**. If you are unsure, click **No**.

4. A report appears informing you of all the service migration changes that occurred and whether the corrections were successful or not. Review the report for any exceptions, then click **Done**.

5. When you are finished, click **Close**.

4.14 Add New Table Entries to the TRS

Approximate time: 5 minutes.

This step adds any required new table entries to the Table Reference Service (TRS).

1. Make sure your TRS is running.

2. Use **Windows Explorer** to browse to the **CygNet\Utilities** folder on the host server.

3. Start the **CygNet TRS Import/Export** utility by double-clicking on the program executable (TrsLoad.exe).

    a. In the **Import** section, use the **Browse** button to select your TRS.

    b. In the **Import** section, use the **Browse** button to select the trs.csv file (located in the product source **Services\TRS** folder).

    c. Click **Import from CSV File to TRS**.

4. Click **Close** to exit the utility.

4.15 Validate All Active Device Template Files

Important: Validation ensures that your template is valid <u>as is</u>; it does not ensure that your template contains all of the functionality that is available with this release or fixes or enhancements. Compare your currently in-use templates with the templates provided with this release and make updates accordingly. <u>Do not</u> simply replace your currently in-use templates with those provided on the source image because you will lose any template customizations that you have made. Refer to the CygNet v9.5 product source for the latest CygNet templates or contact CygNet Support at the <u>Software Support portal</u> (login required), via phone 1-866-4CYGNET (1-866-429-4638) or via email at <u>CygNet Support</u>.

Important: If you installed the v9.5 patch composite in step <u>4.3 Install Any Patches</u>, and there are new device template files included in the .zip, each .dtf must be validated and repaired using the instructions in this step.

Approximate time: Varies depending on the number of device template files you must validate and the number of repairs you must make to outdated device template files.

This step validates currently in-use device template files for use in v9.5. Any issues found must be manually resolved <u>one at a time</u> before the device template file(s) can be reloaded into your DDS. Refer to the **Devices** > **Device Utilities** > **CygNet Device Template Manager Utility** topic in the *CygNet Help* for more information about validating and loading device template files.

1. Use **Windows Explorer** to browse to the **CygNet\Utilities** folder on the host server.

2. Start the **CygNet Device Template Manager** utility by double-clicking the program executable (DtfMgr.exe).

    a. Browse to and select the relevant **DDS Service**.

    b. Leave the **Template File Name** field blank. If you mistakenly browse to and select a device template file for this field, it overrides template validation for the DDS selected above.

    c. Click **Validate Template(s)**. Doing so identifies all invalid templates for the selected DDS.

    d. Take note of each invalid template and proceed to the next step. If all templates are valid, close the utility and proceed to step 4.16 Request the Device Configuration Data Groups.

3. Using CygNet Explorer, open the relevant DDS.

    a. Right-click in the DDS service pane.

    b. Select **Device Definitions**.

    c. Select an invalid template and click **Extract from DDS**.

    d. Do so for each invalid template noted above.

4. Return to the **CygNet Device Template Manager** utility and use the **Browse** button beside **Template File Name** to select an extracted invalid template.

    a. Click **Validate Template(s)**. Doing so displays issues with the extracted invalid template one at a time.

    b. For <u>each</u> issue that the **CygNet Device Template Manager** utility finds, manually edit and save the extracted device template file, then re-click **Validate Template(s)** in the **CygNet Device Template Manager** utility until no more issues are found for that template.

    c. Compare your valid extracted template to the latest CygNet version available to ensure that your template is current and has all of the available functionality offered by CygNet.

d. When no issues remain for a template and you've compared your valid version to the latest CygNet version and made any desired updates, return to the **CygNet Device Template Manager** utility, enter the name of a valid extracted template in the **Template File Name** field, and click **Load Template(s)**.

e. Save the newly validated template to a location that identifies it as a valid and current template.

f. Repeat steps a. through e. until all invalid templates are valid, current, and loaded into the relevant DDS.

5. Click **Close** to exit the utility.

4.16 Request the Device Configuration Data Groups

Important: You must always request the device configuration anytime there are configuration changes to the field device, driver, or firmware, or after modifying the device template file. If your remote devices do not have configuration data groups, skip this step and proceed to step 4.17 Restart the MSS and Activate Automated Polling.

Approximate time: Varies depending on the number of remote devices you have configured for your system.

1. Request the device configuration from remote devices prior to resuming normal poll schedules for any remote devices that have a "configuration" data group.

    The data group names will vary depending on your environment. For example, the "Process Configuration" data group on Eagle devices, the "ROC Config" data group on Emerson devices, the "Controller Version Information" data group on eProd and Lufkin SAM devices, the "RTU Config" data group on FB EFM 3000 and Flow Automation devices, the "Application Config" data group on Totalflow devices, and the "RTU Configuration" data group on Weatherford WellPilot DLQ/K-Series devices.

4.17 Restart the MSS and Activate Automated Polling

Approximate time: Varies depending on the number of remote devices and polling tasks you have configured for your system.

Note: You will need to restart the MSS and activate automated polling tasks, to resume polling after upgrade tasks are complete.

1. If not already running, use **CygNet Explorer** to restart the MSS.

2. Use **CygNet Explorer** to activate any automated polling tasks that you disabled in step 4.1 Stop All Clients and Services on the Host Server.

4.18 Remove the old CygNet.chm file on Host and Client Computers

Approximate time: <1 minute.

In CygNet v9.5 the CygNet Online Help is now available online at https://softwaredocs.weatherford.com/cygnet/95/.

Optional. If you want to remove the old CygNet.chm and other release documents from your host and client computers perform the following steps. Best practice recommends that you back up any files you wish to preserve, and then delete the following files and folders.

1. If you have a **\Docs** folder on your CygNet host or client computers delete the folder using Windows Explorer.

2. If you have a **\Help** folder on your CygNet host or client computers delete the folder using Windows Explorer.

3. If you have a **HELP** folder in your APPS, delete all files and the folder using CygNet Explorer or BSS Explorer.

Note: *Do not confuse the CygNet.chm with the CygNet.API.chm. CygNet.API.chm is the help file for the CygNet .NET API and can be found in the **\Bin** folder on your CygNet host or client computer and in the **BIN** folder in the APPS.*

4.19 Remove the old Canvas Help files on Host and Client Computers

Approximate time: <1 minute.

In CygNet v9.5 the Canvas Help is now part of the larger CygNet Online Help available online at https://softwaredocs.weatherford.com/cygnet/95/.

Optional. If you want to remove the old Canvas Help files from your host and client computers, perform the following steps. Best practice recommends that you back up any files you wish to preserve, and then delete the following files and folders.

- In prior versions of Canvas, the Canvas Help files were downloaded to the **Users\<CurrentUser>\AppData\Local\Canvas\Help** folder on the host server.

- If you have this folder on the computer where Canvas is installed, delete the files and folder using Windows Explorer.

4.20 Convert Older Canvas Screens to New Script Format

Approximate time: Varies depending on the number of screens to be converted.

Canvas supports pre-compiled assemblies. These files are embedded within the screen or object to allow for faster load time. To support this feature the Canvas screen format has been modified and the screen version incremented. The v9.5 Canvas applications have been modified to convert pre-v9.5 Canvas screens containing script when saved. In Canvas, a **Script Change Pending** message will warn you of the pending change. Older screens opened in Canvas View or Canvas View Lite will be converted on the fly, but not saved.

If you have a lot of older screens to convert, a CLI-based utility, **CanvasFileConverter**, is available to convert multiple Canvas screens to the updated script format. The CanvasFileConverter.exe utility is included in the v9.5 **Patch-2021-06-23-Canvas** available on the CygNet Download Site (login required).

Custom Canvas Controls

Note the following about custom Canvas controls:

- If your older screen contains a custom Canvas control, the control assemblies must be compiled against the v9.5 Canvas binaries before attempting to convert the screen to the new script format. Any screen that makes use of a custom Canvas control will fail to convert if the control is not first updated to the latest version of Canvas.

- Depending on where the CanvasFileConverter is being executed, the custom control assemblies need to be placed in the same folder. While Canvas currently allows for the custom control assemblies to reside in custom folders or subfolders, the CanvasFileConverter requires that the control assemblies be located in the same directory—along with all the Canvas and CygNet support binaries, typically **CygNet\Bin**.

CanvasFileConverter Input File

The CanvasFileConverter utility requires an input file that must be prepared in advanced of running the utility. The input file tells the utility the path to the file names of the screens to be converted. The input file can include a list of files, or a list of folders that contain the files. The utility supports converting files stored in a BSS, or in a local or network Windows file-system folder.

CanvasFileConverter Steps

1. Prepare the input file. See the command-line syntax in step 5 below; the `–files || –folders` parameter is described in the table below; or refer to more detailed instructions and examples in the Canvas Online Help.

2. Open a **Command Prompt** window.

3. Navigate to the directory where the CanvasFileConverter application is installed.

4. Optional. Type `canvasfileconverter` and press **Enter** to see user assistance for the utility.

5. Type the desired command(s) using the following syntax:

```
canvasfileconverter [-svc:<site.service>] [-files:<input file path> || -folders:<input file path>] [-topDirectoryOnly] [-backupPath:<path>]
```

The following table provides a brief description for each parameter. Refer to the Canvas Online Help for more detailed information and examples.

Parameter	Description
-svc	The name of the BSS hosting the files to be converted in site.service format.
-files || -folders	The name of an input file containing file names (.can and .cob) or folder names. The format of the input file differs for files and folders, and whether BSS-based or stored locally: • For files, the input file lists the names of the individual files to be converted. • For folders, the input file lists the names of the folders that contain the files to be converted. By default, all valid files within the specified folders and any related subfolders will be converted. The -topDirectoryOnly parameter can be used to limit folders. • If specifying a path to local files or folders, a fully qualified path is required. • If specifying a path to BSS-based files or folders, the name of the <site.service> must be specified in the -svc parameter.
-topdirectoryonly	Include this parameter to limit conversion to only the directory specified.
-backupPath	The local path to a backup location for the original files that have been converted. Backups will never be written back to the hosting BSS. If a -backupPath parameter is not specified, a new folder, named "Originals", will be created at the same path as specified in the -files or -folders parameter.

5. Upgrade Additional CygNet Products

This section addresses how to upgrade additional CygNet software products you have chosen to license for use with your CygNet Software installation.

5.1 Upgrade CygNet Bridge

Approximate time: Varies depending on complexity and number of companion components installed.

CygNet Bridge and its companion products (CygNet Mobile, CygNet Dispatch, and CygNet Bridge API) can be updated any time a new application version is released. Install new CygNet Bridge files as follows.

1. Stop **CygNet Bridge** in your IIS Manager.

2. From the **CygNet\Setup** folder in your source files, copy the new **CygNet Bridge Setup.exe** file to replace the previous version of the file on the web server hosting CygNet Bridge.

3. Open the CygNet Bridge installer (**CygNet Bridge Setup.exe**) and follow the prompts to install the new version of the software.

4. Start **CygNet Bridge** in your IIS Manager.

Refer to the **CygNet Bridge** chapter of the *CygNet Help* for more information about CygNet Bridge and its companion applications.

*Note: CygNet Bridge for v9.5 (v4.3) requires **Microsoft .NET Framework 4.7.2 Developer Pack** or later, which can be downloaded from https://dotnet.microsoft.com/download/dotnet-framework/net472. Refer to the **CygNet v9.5 System Requirements** for more information.*

5.2 Upgrade CygNet Mobile

Approximate time: 5 minutes

CygNet Mobile is contained in CygNet Bridge, therefore it can be updated any time a new version of the CygNet Bridge application is available. Whenever you update CygNet Bridge, the CygNet Bridge installer will update and modify CygNet Mobile if any changes or updates have been included.

The **CygNet Operator** app can be updated any time a new version of the CygNet Operator app is available. When a new version is available, search the iTunes App Store for iOS mobile devices, or Google Play Store for Android mobile devices, for "CygNet Operator" to install the latest version of the application.

Refer to the **CygNet Mobile** chapter of the *CygNet Help* for more information.

5.3 Upgrade CygNet Dispatch

Approximate time: 5 minutes

CygNet Dispatch can be updated any time the application is synchronized with the FMS service (via CygNet Bridge), and a newer version of the application is available on the host server. When you sync CygNet Dispatch, the software application version you are running is compared with the latest file version available on the host and, if a newer version is available, you will be notified and asked to allow an update.

On the host server, new CygNet Dispatch application files are made available as for most other CygNet client applications, using the latest version of the **CygNet Host Updater** utility. Manual file modifications may sometimes be a part of the process, depending on your system configuration.

Refer to the **CygNet Dispatch** chapter of the *CygNet Help* for more information.

5.4 Upgrade CygNet Bridge API

Approximate time: 5 minutes

CygNet Bridge contains the latest version of the CygNet Bridge API, therefore it can be updated any time a new version of the CygNet Bridge application is available. Whenever you update CygNet Bridge, the CygNet Bridge installer will update and modify the CygNet Bridge API if any changes or updates have been included in the new version.

Refer to the **CygNet Bridge API** chapter of the *CygNet Help* for more information.

Appendix A: Mixed-Mode Hosts

An environment where multiple CygNet hosts are running different versions of the software is called a mixed-mode environment or mixed-mode hosts.

Communication between mixed-mode hosts is supported, but careful consideration must be given when configuring host systems, especially when replicating data (or using CygNet Redundancy for failover) in a mixed-mode environment.

A.1 Mixed-Mode Hosts and Facility Service Replication

CygNet v9.5 has been enhanced to support additional facility attributes and the Facility service database definition has been updated accordingly. If you plan to replicate in a mixed-mode environment CygNet has prepared a required patch to update older CygNet services and clients to interact bi-directionally with a v9.5 Facility service.

Each version-specific patch updates the Facility service, clients, and component binaries, so that an older Facility service will replicate correctly from a v9.5 Facility service. After applying the patch, all patched v9.x Facility services will know how to replicate to the v9.5 Facility service, and patched v9.x clients will know how to read and write data to the v9.5 Facility service. If an older service or client interacts with a v9.5 service with the additional facility attributes defined, the older service and clients will remove the new attributes and associated values when replicating. You will not be able to replicate the new facility attributes until all CygNet hosts have been upgraded to v9.5.

We recommend that you avoid using the new facility attributes until all CygNet hosts have been upgraded to v9.5.

Apply the appropriate patch composite to the CygNet host running the older version.

CygNet Version	Composite Patch Name[1]	Optional FAC Patch Name
9.0	90_Patch_Composite.zip	Patch-2020-07-28_FacConnect.zip
9.1	91_Patch_Composite.zip	Patch-2020-07-29_FacVersion.zip
9.2	92_Patch_Composite.zip	Patch-2020-11-14_FacVersion.zip
9.3	93_Patch_Composite.zip	Patch-2020-11-06_FacVersion.zip
9.4	94_Patch_Composite.zip	Patch-2020-10-27_FAC_Version.zip

1. The 9x_Patch_Composite.zip contains each optional FAC patch.

Note: *If your CygNet host is older than v9.0, you must first upgrade to v9.0 or later before applying the appropriate patch.*

1. Patches are found on the CygNet Download Site (login required).

2. Click **SOFTWARE > SCADA AND MEASUREMENT PRODUCTS**.

3. Click the appropriate **9.x** folder for your CygNet host.

4. Open the **Patches** folder.

5. Download the **9x_Patch_Composite.zip** file (or the optional **Patch_2020_date_FacVersion.zip**).

6. Read and follow the instructions in the **9x_Patch_Composite_Readme.html** file.

A.2 Mixed-Mode Considerations

A mixed-mode situation typically occurs when a phased rollout of new software is planned for a multi-host system. The mixed-mode recommendations below assume that you are not already running in a mixed-mode environment.

- UIS and DDS versions must match if they are on the same host.

- The following procedures require you to upgrade these components on all hosts:

    - Address Resolution Service (Ars.exe)

    - ARS configuration file (Ars.cfg)

    - CygNet Version Manager (BSSVM.exe)

    - CygNet Client Installer Application (CInstall.exe)

    - CygNet Host Manager (CHostMgr.exe)

    - Data communication library (Dclnd.dll)

- The following procedures require you to upgrade these components on all clients on client PCs:

    - CygNet Version Manager (BSSVM.exe)

    - CygNet Client Installer/Launcher (CInstall.exe)

    - Data communication library (Dclnd.dll)

A.3 Upgrading Host Server Infrastructure for a Mixed-Mode Environment

Approximate time: 10 minutes.

1. Using **CygNet Host Manager**, stop the host.

2. From the CD Image, run the following applications on the host:

    - For both 32-bit and 64-bit operating systems, run **\System\CygVS2015Redist32.exe**.

    - If you are running 64-bit services on a 64-bit operating system, also run **\System64\CygVS2015Redist64.exe**.

        Note: *Both the 32-bit and 64-bit Redistributables can be installed on a 64-bit system.*

3. Copy **Ars.exe** from the product source **Services\ARS** folder to the **Services\ARS** folder on the host server.

4. Copy **CHostMgr.exe** from the product source **CygNet\Services** folder to the **CygNet\Services** folder on the host server.

5. Copy **Dclnd.dll** from the product source **CygNet\Support** folder to the **CygNet\Support** folder on the host server.

6. Merge the contents of **CygNet\Bin** folder and the **System\Telerik\WpfNoXaml** folder into a single temporary directory on the host server:

a. Copy the contents of the **CygNet\Bin** folder from the product source into a <u>temporary</u> folder on the host server. <u>Do not</u> overwrite the existing **CygNet\Bin** folder on the host server.

b. Copy the contents of the **System\Telerik\WpfNoXaml** folder from the product source to the <u>same</u> temporary folder used in step 6a.

7. Run **ConfigFileMgr.exe** from the <u>temporary</u> folder on the host server to update all ARS configuration files. Point the **ConfigFileMgr.exe** utility at only the **ARS** service folder. Repeat for all ARS services.

8. Copy **CHostUpdater.exe** from the product source **CygNet\Utilities** folder to a <u>temporary</u> folder on the host server. Do not overwrite the existing **CHostUpdater.exe** on the host server. For the purposes of this infrastructure upgrade, you must use the <u>source</u> **CHostUpdater.exe**.

9. Using **CHostMgr.exe**, start the host.

10. Using **CygNet Explorer**, replace **CInstall.exe** and **BSSVM.exe** in the **BSSVM** group in the APPS service with the product source **CInstall.exe** and **BSSVM.exe**. The files are in the source **CygNet\Clients** folder.

11. Using **CygNet Explorer**, upload **CygConn.exe** from the product source **CygNet\Utilities** folder to the UTILS group in the APPS service.

12. Update the ODBC driver on the host server:

a. Open **CHostUpdater.exe** found in the <u>temporary</u> folder you created in step 8 above.

b. Click **Browse...** to browse to the product source **CygNet\Support\ODBC** folder.

c. Select the product source **ODBC** folder and click **OK**.

d. Click **Load Files...**.

e. When the **Found Install Folders** dialog box opens, leave all default service folders selected and click **OK**.

f. Click **Perform Update**. Doing so overwrites your old (destination) **ODBC** folder with the new (product source) **ODBC** folder. Old files are removed, new files are added, and files are safely rearranged. All errors and warnings are displayed in the **Process Status** dialog box and are written to the CHostUpdater001.log file, which is located in the temporary folder from which **CHostUpdater.exe** was run.

g. When the process is complete, click **OK** and **Close** to exit **CHostUpdater.exe**.

Note: If you want to use 64-bit applications with CygNet ODBC you will need to install the 64-bit ODBC driver on the host server and create 64-bit DSNs.

13. Use **TouchBss.exe** to update the file times of all .rsp and .rsq files in the APPS service.